

# **Getaltheorie**

## **een introductie**

Bart Michels

# Inhoudsopgave

<b>Voorwoord</b>	<b>7</b>
<b>Inleiding</b>	<b>9</b>
0.1 Getallen . . . . .	9
0.2 Inductie en het welordeningsprincipe . . . . .	13
<b>Deel I. Elementaire getaltheorie</b>	<b>15</b>
<b>1 Deelbaarheid</b>	<b>16</b>
1.1 Rest en quotiënt . . . . .	17
1.2 Grootste gemene deler . . . . .	19
1.3 Kleinste gemene veelvoud . . . . .	20
1.4 De stelling van Bézout . . . . .	21
1.5 Algoritme van Euclides . . . . .	23
1.6 Lineaire Diophantische vergelijkingen . . . . .	25
Opgaven . . . . .	27
<b>2 Priemgetallen</b>	<b>28</b>
2.1 Priemontbinding . . . . .	28
2.2 Gevolgen van de hoofdstelling . . . . .	29
2.2.1 Rationale getallen . . . . .	32
2.3 Aritmetische functies . . . . .	33
2.3.1 Aantal delers . . . . .	33
2.3.2 Som van delers . . . . .	34
2.3.3 Totiëntfunctie . . . . .	35
2.3.4 Multiplicatieve functies . . . . .	36
Opgaven . . . . .	37
<b>3 Talstelsels</b>	<b>39</b>
3.1 Expansies van niet-gehele getallen . . . . .	40
Opgaven . . . . .	43
<b>4 Ad-hocmethodes voor diophantische vergelijkingen</b>	<b>44</b>
4.1 Ontbinden . . . . .	44
4.2 Ongelijkheden . . . . .	45
4.3 Extremenprincipe . . . . .	47
4.4 Vieta jumping . . . . .	47
Opgaven . . . . .	48
<b>5 Dirichlet-convolutie</b>	<b>50</b>
5.1 Inverteerbaarheid . . . . .	50
5.2 Multiplicativiteit . . . . .	52

5.3	Möbiusinversie . . . . .	53
5.3.1	Möbiusinversie in multiplicatieve vorm . . . . .	54
5.4	Toepassingen . . . . .	55
5.4.1	Expliciete formules voor aritmetische functies . . . . .	55
5.4.2	Elimineren van de floorfunctie . . . . .	57
5.5	Meer over multiplicativiteit . . . . .	58
	Opgaven . . . . .	60
<b>6</b>	<b>Intermezzo: low-budget ggd calculus</b>	<b>61</b>
6.1	Distributiviteit . . . . .	62
6.2	Associativiteit . . . . .	63
6.3	De ggd van meerdere getallen . . . . .	64
6.4	Additieve notatie . . . . .	65
6.5	Freshman's dream voor ggd's . . . . .	66
<b>7</b>	<b>Modulorekenen</b>	<b>68</b>
7.1	Congruentie . . . . .	68
7.2	Inverteerbaarheid . . . . .	71
7.3	Lineaire congruenties . . . . .	72
7.4	Stelsels congruenties: de Chinese reststelling (CRS) . . . . .	74
7.5	Kwadraatresten . . . . .	77
7.5.1	Toepassing: Diophantische vergelijkingen . . . . .	79
7.5.2	Pythagorese drietallen . . . . .	79
7.6	Stelling van Wilson . . . . .	80
	Opgaven . . . . .	81
<b>8</b>	<b>Exponentiële congruenties I</b>	<b>84</b>
8.1	Het ordelemma . . . . .	85
8.2	De kleine stelling van Fermat . . . . .	86
8.3	De stelling van Euler . . . . .	87
8.4	Ordes en periodieke expansies . . . . .	88
	Opgaven . . . . .	88
<b>9</b>	<b>Kwadraatresten</b>	<b>90</b>
9.1	Het Legendre-symbool . . . . .	90
9.1.1	Het criterium van Euler en multiplicativiteit . . . . .	90
9.2	Kwadratische reciprociteit . . . . .	91
9.2.1	Kleinste absolute resten: het lemma van Gauss . . . . .	91
9.2.2	Eisensteins weg naar kwadratische reciprociteit . . . . .	94
9.2.3	Systematisch bepalen van het Legendre-symbool . . . . .	96
9.3	Kwadratische congruenties . . . . .	96
9.3.1	Priemgetallen als moduli . . . . .	97
9.3.2	Priemmachten en het lemma van Hensel . . . . .	98
	Opgaven . . . . .	98
<b>10</b>	<b>Polynoomcongruenties</b>	<b>100</b>
10.1	Begrippen . . . . .	100
10.2	Factorisatiestellingen . . . . .	101

<b>11 Exponentiële congruenties II</b>	<b>103</b>
11.1 Lifting The Exponent . . . . .	103
11.1.1 Het geval $p = 2$ . . . . .	104
11.1.2 LTE in deelbaarheidsgedaante . . . . .	105
11.1.3 De klassieke Diophant . . . . .	105
11.2 Primitieve wortels . . . . .	106
11.2.1 Existentie . . . . .	106
11.2.2 Eigenschappen . . . . .	108
11.2.3 Indexrekenen . . . . .	109
11.3 Cyclotomische veeltermen . . . . .	109
11.3.1 Algebraïsche eigenschappen . . . . .	111
11.3.2 Toepassingen in de getaltheorie . . . . .	113
11.3.3 De stelling van Zsigmondy . . . . .	116
11.3.3.1 Bewijs van Zsigmondy . . . . .	116
11.3.3.2 Gevolgen . . . . .	118
11.4 Recapitulatie exponentiële congruenties . . . . .	118
11.4.1 LTE, Fermat, Euler, Bang, Zsigmondy, en Dirichlet . . . . .	119
11.4.2 Wieferich-priemgetallen . . . . .	120
11.4.3 $n$ -demachtsresten . . . . .	120
Opgaven . . . . .	120
<b>12 Binomiaalcongruenties</b>	<b>122</b>
12.1 De stelling van Lucas . . . . .	122
12.2 De stelling van Kummer . . . . .	122
12.3 De stelling van Wolstenholme . . . . .	123
Opgaven . . . . .	123
<b>13 Kwadratische vergelijkingen</b>	<b>124</b>
13.1 Completing the square . . . . .	124
13.2 Classificatie . . . . .	125
13.2.1 Discriminant 0: reductie tot kwadratische congruenties . . . . .	125
13.2.2 Sommen van kwadraten en Pell-typevergelijkingen . . . . .	126
13.2.3 Conclusies en praktische strategie . . . . .	127
13.3 Sommen van kwadraten . . . . .	127
13.3.1 Som van twee kwadraten: multiplicativiteit . . . . .	127
13.3.2 De twee-kwadratenstelling . . . . .	129
13.3.3 Drie en vier kwadraten . . . . .	131
13.3.4 Veralgemeningen . . . . .	132
13.3.4.1 Het probleem van Waring . . . . .	132
13.3.4.2 De veelhoeksgetalstelling van Fermat . . . . .	132
13.4 De kwadratische vorm $a^2 + nb^2$ . . . . .	132
13.4.1 Eindige afdaling . . . . .	132
13.4.2 Uniciteit . . . . .	133
13.5 Pell-vergelijkingen . . . . .	133
13.5.1 De norm in $\mathbb{Z}[\sqrt{d}]$ . . . . .	133
13.5.2 Bestaan van oplossingen . . . . .	134
13.5.3 Karakterisatie via minimale oplossingen . . . . .	135
13.5.4 Recurrente betrekkingen . . . . .	137
13.6 Pell-typevergelijkingen . . . . .	137

13.6.1	Karakterisatie en begrenzingsen . . . . .	138
13.6.2	Gedrag van minimale oplossingen . . . . .	139
13.6.3	Recurrente betrekkingen . . . . .	140
	Opgaven . . . . .	140
<b>14</b>	<b>Rationale en irrationale getallen</b>	<b>143</b>
14.1	Diophantische benadering . . . . .	143
14.1.1	Toepassingen van Diophantische benadering . . . . .	144
14.1.2	Irrationaliteit van reekssommen . . . . .	144
14.2	Kettingbreuken . . . . .	147
14.3	Pellvergelijkingen . . . . .	147
14.4	Irrationale en transcendente getallen . . . . .	147
14.5	De irrationaliteitsmaat . . . . .	147
14.5.1	Thue-Siegel-Roth . . . . .	148
14.5.2	Liouville-getallen . . . . .	148
	Opgaven . . . . .	148
<b>15</b>	<b>Veeltermen</b>	<b>149</b>
	Opgaven . . . . .	150
<b>16</b>	<b>Toepassingen</b>	<b>151</b>
16.1	Het Frobeniusgetal . . . . .	151
16.2	Perfecte en bevriende getallen . . . . .	152
16.2.1	De overvloedigheidsindex . . . . .	152
16.2.2	Een eerste karakterisatie . . . . .	153
16.2.3	Enkele congruenties . . . . .	154
16.3	Het probleem van Josephus . . . . .	154
16.4	Magische vierkanten . . . . .	154
16.4.1	De Latijnse strategie . . . . .	155
16.4.1.1	Diagonalen . . . . .	158
16.4.1.2	De Siamese methode . . . . .	160
16.4.2	Conway's LUX-methode . . . . .	161
16.4.3	Kroneckerproduct . . . . .	161
16.5	Lineaire recursies . . . . .	161
16.5.1	Periodiciteit . . . . .	161
16.6	De rij van Fibonacci . . . . .	161
16.6.1	De Pisanoperiode . . . . .	161
16.6.2	Deelbaarheidsrijen . . . . .	162
16.6.3	Sterke deelbaarheidsrijen . . . . .	162
	Opgaven . . . . .	162
<b>17</b>	<b>Algoritmen</b>	<b>164</b>
17.1	Algoritme van Euclides . . . . .	164
17.2	Modulaire machtsverheffing . . . . .	164
17.3	Factorisatie . . . . .	164
17.3.1	Dixon's algoritme . . . . .	164
17.4	Priemgetallen . . . . .	164
17.4.1	Lucas-Lehmer . . . . .	164
17.4.2	Miller-Rabin . . . . .	164
17.5	RSA-encryptie . . . . .	164

17.5.1	Diffie-Hellman protocol . . . . .	164
17.6	Primitieve wortels . . . . .	164
17.7	Sommen van kwadraten . . . . .	164
17.8	Pellvergelijkingen . . . . .	164
17.8.1	Chakravala methode . . . . .	164
	Opgaven . . . . .	165
<b>Opgaven deel I</b>		<b>166</b>
 <b>Deel II. Algebra</b>		<b>176</b>
<b>18</b>	<b>Modulorekenen revisited</b>	<b>177</b>
18.1	De ring $\mathbb{Z}/m\mathbb{Z}$ . . . . .	177
18.1.1	Bewerkingen in $\mathbb{Z}/m\mathbb{Z}$ . . . . .	177
18.1.2	Ringen . . . . .	180
18.1.3	Quotiëntringen . . . . .	181
18.2	De groep $(\mathbb{Z}/m\mathbb{Z})^\times$ . . . . .	183
18.2.1	Inverteerbaarheid in $\mathbb{Z}/m\mathbb{Z}$ . . . . .	183
18.2.2	Groepen . . . . .	184
18.2.3	Orde van een element . . . . .	186
18.2.4	Eigenschappen van de orde: het ordelemma . . . . .	187
18.3	Interactie . . . . .	188
18.3.1	Morfismen . . . . .	188
18.3.2	Som en product van structuren . . . . .	190
18.3.3	Direct product . . . . .	190
18.4	De Chinese reststelling . . . . .	191
18.5	Veeltermringen . . . . .	192
18.5.1	Factorisatiestellingen . . . . .	192
18.6	Cyclische groepen . . . . .	192
18.7	Het veld $\mathbb{F}_p$ . . . . .	192
	Opgaven . . . . .	192
<b>19</b>	<b>Ringuitbreidingen van <math>\mathbb{Z}</math></b>	<b>193</b>
19.1	Case study: de Ramanujan-Nagell vergelijking . . . . .	193
19.2	Mordell-vergelijkingen . . . . .	193
	Opgaven . . . . .	193
<b>20</b>	<b>De <math>p</math>-adische getallen</b>	<b>194</b>
	Opgaven . . . . .	194
<b>Opgaven deel II</b>		<b>195</b>
 <b>Deel III. Analyse</b>		<b>196</b>
<b>21</b>	<b>Zonder naam</b>	<b>197</b>
21.1	Zonder naam . . . . .	197
	Opgaven . . . . .	198

<b>22 Befaamde vermoedens</b>	<b>199</b>
22.1 Sommen van priemgetallen . . . . .	199
22.2 Priemhiaten . . . . .	199
Opgaven . . . . .	200
<b>Opgaven deel III</b>	<b>201</b>
<b>Bijlagen</b>	<b>202</b>
<b>A Notaties</b>	<b>203</b>
A.1 Sommatieteken . . . . .	203
A.2 Discrete functies . . . . .	205
<b>B Nuttige stellingen</b>	<b>207</b>
B.1 Ontbindingen . . . . .	207
B.2 Inclusie-exclusie . . . . .	207
B.3 Ongelijkheden . . . . .	210
B.4 Lineaire recursies . . . . .	211
B.5 Varia . . . . .	212
<b>C Complexe getallen</b>	<b>214</b>
<b>D Verzamelingen</b>	<b>216</b>
D.1 Binaire relaties . . . . .	216
D.1.1 Equivalentierelaties . . . . .	218
D.2 Groepen . . . . .	220
D.3 Nevenklassen . . . . .	220
D.4 De stelling van Lagrange . . . . .	220
<b>Hints</b>	<b>222</b>
<b>Antwoorden</b>	<b>231</b>
<b>Referenties</b>	<b>238</b>
<b>Lijst van symbolen</b>	<b>239</b>
<b>Index</b>	<b>240</b>

# Voorwoord

Bij het introduceren van een nieuw vakgebied heeft men de onhebbelijke gewoonte om zich de existentiële vraag te stellen in de vorm

*Wat is getaltheorie?*

De grenzen van een wiskundige discipline zijn, indien niet helemaal onbekend, in elk geval heel vaag. Een ontwijkend antwoord in de stijl van

*Who is but the form following the function of what, and what I am is a man in a mask.*

*(V in V for Vendetta)*

lijkt nog het meest geschikt: wat er echt toe doet is niet wát getaltheorie is, maar hóe ze is en wat we er over weten.

Een droge geschiedenis staat misschien ook niet mis. Tenslotte is getaltheorie, na meetkunde waarschijnlijk het oudste deelgebied in de wiskunde. In het oude Griekenland, in Italië, India, China en nog vele andere landen vinden we bronnen van de eerste wiskundigen die gehele getallen bestudeerden. Zo hebben we Euclides (265 - 200 v.C.) in Griekenland, Fibonacci (c. 1170 - c. 1250) in Italië, Brahmagupta (598 - 668) en Bhāskara (1114 - 1185) als vertegenwoordigers van India en onze Chinese vriend Sun Tzu (c. 400 - c. 473) met zijn alom bekende Chinese reststelling.

Het wonderbaarlijke aan getaltheorie is dat ze niet, of toch tot op een zeker niveau, steunt op andere domeinen uit de wiskunde, zoals analyse of meetkunde. Dat maakt haar zo zuiver en in essentie zo eenvoudig. ‘In essentie’, want heel wat problemen uit de getaltheorie zijn pas heel laat opgelost of zijn dat nog steeds niet. Het bewijs van de laatste stelling van Fermat heeft 350 jaar op zich laten wachten, tot de Britse wiskundige Andrew Wiles in 1993 een bewijs publiceerde. Het vermoeden van Catalan werd pas bewezen in 2002 door onze Roemeense collega Preda Mihăilescu, maar liefst 158 jaar nadat onze landgenoot Eugène Catalan het vermoeden in 1844 formuleerde. Het vermoeden van Goldbach, het probleem van Brocard, het abc-vermoeden, het vermoeden van Collatz, het probleem van Waring, het vermoeden van Andrica, van Collatz, ... zijn slechts enkele van de talloze onbewezen hypothesen en onopgeloste problemen:

*There are many questions which fools can ask that wise men cannot answer.*

*(George Polya)*

Voor het oplossen van dit soort raadsels is er natuurlijk eerst wat kennis nodig, en wie weet kan je na het lezen van deze niet-meer-zo-beknopte introductie wel het bewijs van een van die hersenkrakers op jouw naam zetten.

Maar laat je vooral niet overdonderen. Er is hier massaal veel in te vinden dat het erg lang zal duren eer je alles goed en wel hebt gelezen en begrepen.

*Useful communication is useful because of what it does not contain.*



(Qiaochu Yuan<sup>1</sup>)

Akkoord. Helaas heb ik zowat de neiging om alles tot in detail uit te schrijven zonder ook maar één mysterie te verzwijgen. Ter compensatie doe ik mijn best om alles gestructureerd te houden, met dien verstande dat dit toelaat aan de lezer om de *useful* delen vlot zelf te selecteren. Selecteren? Ja! Het is zeker niet nodig om alles in de volgorde te lezen zoals het hier is opgebouwd. Integendeel, het zou te gek zijn om je te verdiepen in pakweg Dirichlet convolutie zonder ook maar iets te hebben gelezen over modulorekenen. Een goede keuze is om deze volgorde te hanteren: Hoofdstuk 1 en Hoofdstuk 2 t.e.m. de hoofdstelling van de rekenkunde, een beetje uit het weinig theoretische Hoofdstuk 4 en vervolgens Hoofdstuk 7. Als beginnend problem-solver kan je daar al een heel eind mee. Wil je meer weten, dan raad ik je aan om het deel over aritmetische functies te lezen in Hoofdstuk 2 gevolgd door Hoofdstuk 8. Daarna zie je maar. Hoofdstuk 16 over toepassingen is misschien wel eens leuk, en bevat massa's dingen die bijna geen voorkennis vragen. De reden waarom ik toch alles in deze volgorde heb geplaatst is om een sluitende opbouw te geven van alle resultaten - althans, het is voor mijzelf een geruststelling dat alles in de (een) juiste volgorde staat.

Je zal ook merken dat er heel wat dingen nog onafgewerkt zijn, zeker naar het einde van de hoofdstukken toe. Of die dingen ooit vervolledigd worden blijft een moeilijke vraag. Vaak heb ik gewoon de titel van een hoofdstuk of paragraaf gemaakt als geheugensteun, met de bedoeling om daar ooit eens wat over te schrijven. Heb je zelf suggesties – een leuke stelling, een raadseltje dat kan opgelost worden met getaltheorie, een of andere observatie die roept om veralgemening, een moeilijk probleem (opgelost of onopgelost), een quote om dit alles wat mee te versieren, laat maar weten. Ook verbeteringen van typo's en spellingsfouten zijn welkom.

---

<sup>1</sup><http://math.stackexchange.com/a/216578/43288>

# Inleiding

## 0.1 Getallen

*Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.*

*(Leopold Kronecker)*

We doorlopen enkele eigenschappen van natuurlijke, gehele, rationale en reële getallen. Veel van deze eigenschappen zijn erg intuïtief, maar voor de geïnteresseerde lezer geven we hier en daar een bewijs; de ongeïnteresseerde lezer kan zich beperken tot het vertrouwd worden met enkele notaties en definities. Wat we hier formuleren als eigenschappen zijn op hun beurt stellingen die voortvloeien uit veel fundamentele wiskunde, en we doen dan ook geen poging om alles axiomatisch op te bouwen.

Daarom hier geen formele definitie van natuurlijke getallen.

### Notatie 0.1.

We noteren  $\mathbb{N} = \{0, 1, 2, 3, \dots\}$  voor de verzameling van de natuurlijke getallen.

We schrijven ook  $\mathbb{N}^+ = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \dots\}$ .<sup>2</sup>

### Eigenschap 0.2. Welordeningsprincipe over $\mathbb{N}$

Elke niet-lege deelverzameling van  $\mathbb{N}$  heeft een minimaal element.

De voorwaarde dat de deelverzameling niet-leeg is uiteraard nodig. Vaak zal het niet-leeg zijn meteen duidelijk zijn, maar het loont toch de moeite om deze voorwaarde te controleren bij het toepassen van deze stelling.

Ook voor gehele getallen geven we geen formele definitie. Intuïtief vormen de gehele getallen de verzameling van verschillen tussen twee natuurlijke getallen.

### Notatie 0.3.

We noteren  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$  voor de verzameling van gehele getallen.

We schrijven ook  $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$ .

De rationale getallen komen intuïtief overeen met quotiënten van gehele getallen.

---

<sup>2</sup>Er zijn hopeloos veel conventies in de omgang. We vermijden bewust de notatie  $\mathbb{N}_0$  omdat de betekenis hiervan wijzigt van auteur tot auteur: sommigen noteren  $\mathbb{N}_0 = \{0, 1, \dots\}$ , anderen  $\mathbb{N}_0 = \{1, 2, \dots\}$ . Over de betekenis van  $\mathbb{N}^+$  bestaat nagenoeg geen twijfel.

**Notatie 0.4.**

We noteren  $\mathbb{Q}$  voor de verzameling van rationale getallen.

De reële getallen tenslotte vullen de gaten op die de rationale getallen overlaten: men kan ze beschouwen als limieten van rijen die uit rationale getallen bestaan.<sup>3</sup>

**Notatie 0.5.**

We noteren  $\mathbb{R}$  voor de verzameling van reële getallen.

Een deelverzameling  $V$  van  $\mathbb{R}$  noemt men *naar boven begrensd* als er een reëel getal bestaat dat minstens zo groot is als elk element van  $V$ . Analoog noemt men  $V$  *naar onder begrensd* als er een reëel getal bestaat dat hoogstens zo groot is als elk element van  $V$ . Een verzameling die zowel naar boven als naar onder begrensd is noemt men kortweg *begrensd*. Een reëel getal  $m$  dat aan zo'n eigenschap voldoet noemt men een *bovengrens* respectievelijk *ondergrens* voor  $V$ . We zeggen ook ' $V$  is naar boven (resp. onder) begrensd door  $m$ .'

Een naar boven begrensde deelverzameling heeft niet noodzakelijk een maximum. Zo is bijvoorbeeld het interval  $[0, 1[$  naar boven begrensd, maar heeft geen maximum (het bevat 1 niet). Wel hebben we de volgende eigenschap (zonder bewijs hier):

**Eigenschap 0.6. Supremumprincipe over  $\mathbb{R}$** 

Elke niet-lege deelverzameling  $V$  van  $\mathbb{R}$  die naar boven begrensd is heeft een kleinste bovengrens, het *supremum* genaamd, en wordt genoteerd  $\sup V$ .

Merk op dat indien  $r$  een ondergrens is voor  $V$ , dan is  $-r$  een bovengrens voor  $-V$  (de verzameling van tegengestelden van elementen van  $V$ ). Het minimum van de verzameling van bovengrenzen van  $-V$  is dan het maximum van de verzameling van ondergrenzen voor  $V$ . Uit het supremumprincipe volgt dus:

**Eigenschap 0.7. Infimumprincipe over  $\mathbb{R}$** 

Elke niet-lege deelverzameling  $V$  van  $\mathbb{R}$  die naar onder begrensd is heeft een grootste ondergrens, het *infimum* genaamd, en wordt genoteerd  $\inf V$ .

**Stelling 0.8.**

De gehele getallen zijn naar boven begrensd, noch naar onder begrensd.

*Bewijs.*

We bewijzen de eerste eigenschap, de tweede gaat analoog. Veronderstel dat  $\mathbb{Z}$  toch naar boven begrensd is, en  $\sup \mathbb{Z} = s$ . Omdat  $s$  de kleinste bovengrens is, is  $s - 1$  geen bovengrens. Er is dus een  $z \in \mathbb{Z}$  met  $s - 1 < z$ . Dan is  $s < z + 1$ , wat in tegenstrijd is met de veronderstelling dat  $s$  een bovengrens is voor  $\mathbb{Z}$ :  $z + 1$  is immers een geheel getal dat per veronderstelling kleiner of gelijk aan  $s$  is.  $\square$

<sup>3</sup>Men noemt  $\mathbb{R}$  om die reden de *Cauchy-completering* van  $\mathbb{Q}$ .

**Stelling 0.9.**

Voor elk reëel getal  $r$  bestaat er een geheel getal  $z < r$ , en een geheel getal  $z > r$ .

*Bewijs.*

We bewijzen de eerste eigenschap, de tweede is analoog. Veronderstel dat ze niet geldt, dus dat er een zeker reëel getal  $r$  bestaat met de eigenschap dat  $z \geq r$  voor alle  $z \in \mathbb{Z}$ . Dan zou  $\mathbb{Z}$  naar boven begrensd zijn door  $r$ , een tegenstrijdigheid.  $\square$

Het supremumprincipe laat ons toe om het welordeningsprincipe over  $\mathbb{N}$  te veralgemenen tot  $\mathbb{Z}$ .

**Stelling 0.10.** Extremumprincipe over  $\mathbb{Z}$ 

Elke niet-lege deelverzameling van  $\mathbb{Z}$  die naar onder begrensd is heeft een kleinste element. Elke niet-lege deelverzameling van  $\mathbb{Z}$  die naar boven begrensd is heeft een grootste element.

*Bewijs.*

Stel dat  $V \subseteq \mathbb{Z}$  naar onder begrensd is door  $r \in \mathbb{R}$ . Wegens de vorige stelling bestaat er een geheel getal  $z < r$ . Dan is  $v - z > v - r \geq 0$  voor alle  $v \in V$ , dus  $V - z \subseteq \mathbb{N}$ . Wegens het welordeningsprincipe over  $\mathbb{N}$  heeft  $V - z$  een kleinste element  $n$ . Dan heeft  $V$  ook een kleinste element, namelijk  $n + z$ .

Stel nu dat  $V$  naar boven begrensd is door  $r \in \mathbb{R}$ . Dan is  $-V$  naar onder begrensd door  $-r$ , dus heeft  $-V$  een kleinste element  $k$  wegens het eerste deel van het bewijs. Bijgevolg heeft  $V$  als grootste element  $-k$ .  $\square$

Uit Stelling 0.9 volgt in het bijzonder dat voor een willekeurig reëel getal  $r$ , de verzameling van gehele getallen die groter dan of gelijk zijn aan  $r$  niet leeg is. Die verzameling heeft wegens de vorige stelling dus een kleinste element (ze is immers naar onder begrensd, door  $r$ ).

**Notatie 0.11.**

Voor  $r \in \mathbb{R}$  noteren we  $\lceil r \rceil$  voor het kleinste geheel getal groter of gelijk aan  $r$ . Men zegt ook wel ‘ceiling  $r$ ’ en  $\lceil \cdot \rceil$  wordt soms de *ceilingfunctie* genoemd. We zeggen ook “ $r$  naar boven afgerond is  $\lceil r \rceil$ ”.

Bijvoorbeeld,  $\lceil 3 \rceil = 3$ ,  $\lceil 2.4 \rceil = 3$  en  $\lceil -1.3 \rceil = -1$ .

Analoog bestaat er voor elk reëel getal  $r$  een grootste geheel getal dat kleiner of gelijk aan  $r$  is.

**Notatie 0.12.**

Voor  $r \in \mathbb{R}$  noteren we  $\lfloor r \rfloor$  voor het grootste geheel getal kleiner of gelijk aan  $r$ . Men zegt ook wel ‘floor  $r$ ’ of het *geheel deel* van  $r$  en  $\lfloor \cdot \rfloor$  wordt de *entierfunctie*<sup>4</sup>, *trapfunctie* of *floorfunctie* genoemd. We zeggen ook “ $r$  naar beneden afgerond is  $\lfloor r \rfloor$ ”.

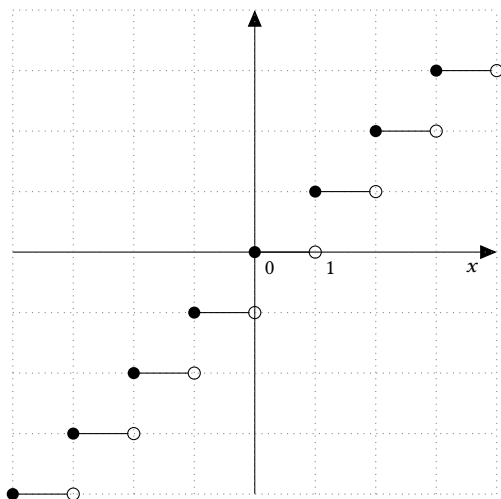
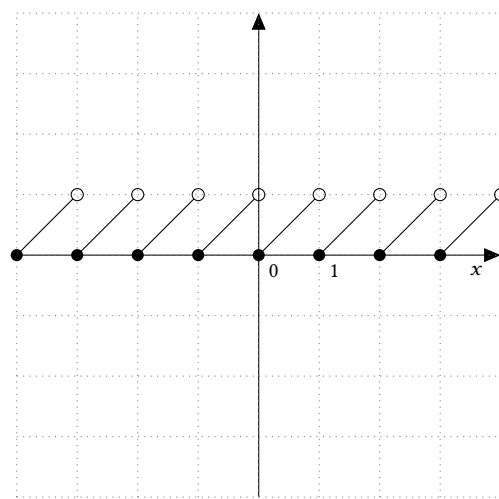
We spreken ook van het ‘gedeelte voor de komma’ van  $r$ , zoals blijkt uit de decimale notatie:  $\lfloor 3 \rfloor = 3$ ,  $\lfloor 2.4 \rfloor = 2$  en  $\lfloor -1.3 \rfloor = -2$ .

Aan de hand van het geheel deel definieert men het *fractioneel deel* van een reëel getal.

**Definitie 0.13.** Fractioneel deel

Voor  $r \in \mathbb{R}$  definiëren we het *fractioneel deel* als  $\{r\} = r - \lfloor r \rfloor$ .<sup>5</sup> De functie  $\{\cdot\}$  noemt men ook de *zaagtandfunctie*.

We spreken ook van het ‘gedeelte na de komma’ van  $r$ :  $\{3\} = 0$ ,  $\{2.4\} = 0.4$  en  $\{-1.3\} = 0.7$ . De benamingen ‘trap’ en ‘zaagtand’ worden gemotiveerd door de grafiek van hun functies:

Grafiek van  $\lfloor x \rfloor$ Grafiek van  $\{x\}$ 

We bekijken enkele verdere eigenschappen van  $\lfloor \cdot \rfloor$ .  $\lfloor x \rfloor$  is per definitie het grootste geheel getal kleiner of gelijk aan  $x$ . Dus  $\lfloor x \rfloor + 1 > x$ . We hebben dus de ongelijkheden

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Veronderstel nu omgekeerd dat er een geheel getal  $z$  is zo dat  $z \leq x < z + 1$ . Dan is  $z$  een geheel getal kleiner of gelijk aan  $x$ , en dus hoogstens  $\lfloor x \rfloor$ . Uit  $z + 1 > x$  volgt dat  $z + 1 > \lfloor x \rfloor$ , zodat  $z > \lfloor x \rfloor - 1$ . Combinatie van de ongelijkheden  $z \leq \lfloor x \rfloor$  en  $z > \lfloor x \rfloor - 1$  leert ons dat  $z = \lfloor x \rfloor$ . Samenvattend,

<sup>4</sup>Naar het Franse *entier*, wat *geheel* betekent.

<sup>5</sup>Soms noteert men  $\{r\}$  als  $r \bmod 1$ , om redenen die in Hoofdstuk 1 duidelijk worden.

**Stelling 0.14.**

Voor elk reëel getal  $x$  bestaat er een uniek geheel getal  $z$  waarvoor  $z \leq x < z + 1$ , dat bovendien gelijk is aan  $\lfloor x \rfloor$ .

Met een volledig analoge redenering bewijst men:

**Stelling 0.15.**

Voor elk reëel getal  $x$  bestaat er een uniek geheel getal  $z$  waarvoor  $z - 1 < x \leq z$ , dat bovendien gelijk is aan  $\lceil x \rceil$ .


Floor en ceil hebben nog meer eigenschappen. De meeste volgen min of meer rechtstreeks uit de definitie.

**Voorbeeld 0.16.** Bewijs dat  $\lfloor -x \rfloor = -\lceil x \rceil$  voor alle  $x \in \mathbb{R}$ .

*Oplossing.*

Voor een geheel getal  $z$  geldt dat  $z \leq -x$  als en slechts als  $-z \geq x$ . Het grootste geheel getal  $z$  waarvoor  $z \leq -x$  is dus het tegengestelde van het kleinste geheel getal  $y$  waarvoor  $y \geq x$ . Symbolisch,  $\lfloor -x \rfloor = -\lceil x \rceil$ .  $\square$

**Opgave 0.17.** Hoe ziet de grafiek van  $\lceil \cdot \rceil$  eruit? H

**Opgave 0.18.** Bewijs dat  $\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor$  voor  $x, y > 0$ . 

**Opgave 0.19.** (VWO 2013 ronde 1 vraag 22) Hoeveel van de volgende gelijkheden gelden voor alle reële getallen  $x \geq 1$  en  $y \geq 1$ ? H

$$\lfloor x + \lfloor y \rfloor \rfloor = \lfloor \lfloor x \rfloor + y \rfloor$$

$$\lfloor x - \lfloor y \rfloor \rfloor = \lfloor \lfloor x \rfloor - y \rfloor$$

$$\lfloor x \cdot \lfloor y \rfloor \rfloor = \lfloor \lfloor x \rfloor \cdot y \rfloor$$

$$\lfloor x : \lfloor y \rfloor \rfloor = \lfloor \lfloor x \rfloor : y \rfloor$$

- (A) 0            (B) 1            (C) 2            (D) 3            (E) 4

## 0.2 Inductie en het welordeningsprincipe

Op het welordeningsprincipe over  $\mathbb{N}$  steunt het zogenaamde inductieprincipe over  $\mathbb{N}$ . Met “een predikaat  $P$  gedefinieerd over  $\mathbb{N}$ ” bedoelen we een uitspraak  $P(n)$  die afhankelijk is van het natuurlijk getal  $n$ . De waarheidswaarde van  $P$  kan verschillen van getal tot getal. Bijvoorbeeld, “ $P(n)$  betekent  $n \geq 5$ ”. Dit predikaat is vals voor  $n = 0, 1, 2, 3, 4$  en waar voor alle andere natuurlijke getallen.

**Eigenschap 0.20.** Inductieprincipe over  $\mathbb{N}$

Zij  $P$  een predikaat gedefinieerd over  $\mathbb{N}$ . Als  $P(0)$  geldt, en indien voor alle  $k \in \mathbb{N}$  uit  $P(k)$  volgt dat ook  $P(k + 1)$ , dan is  $P(n)$  waar voor alle  $n \in \mathbb{N}$ .

In deze context noemt men  $P(0)$  de inductiebasis. Het bewijzen dat  $P(k + 1)$  een gevolg is van  $P(k)$  gebeurt in de zogenaamde inductiestap. Tijdens het bewijs van de inductiestap noemt men  $P(k)$  de inductiehypothese.  $P(k)$  is als het ware een veronderstelling, waaruit  $P(k + 1)$  moet worden bewezen.

**Voorbeeld 0.21.** Bewijs dat  $0 + 1 + 2 + \dots + n = \frac{n(n+1)}{2}$  voor alle  $n \in \mathbb{N}$ .

*Oplossing.*

De uitspraak  $P(n)$  is hier “ $0 + 1 + 2 + \dots + n$  is gelijk aan  $\frac{n(n+1)}{2}$ ”.

*Inductiebasis.* We moeten bewijzen dat  $P(0)$  geldt. Inderdaad: de som in het linkerlid is dan 0, en het rechterlid is  $\frac{0 \cdot 1}{2} = 0$ .

*Inductiehypothese.* Veronderstel dat  $k \in \mathbb{N}$ , en dat  $P(k)$  waar is.

*Inductiestap.* We bewijzen dat ook  $P(k + 1)$  waar is, op voorwaarde dat  $P(k)$  waar is. Uit de inductiehypothese weten we dat  $0 + 1 + \dots + k = \frac{k(k+1)}{2}$ . Tellen we hier aan beide kanten  $k + 1$  bij:  $0 + \dots + k + (k + 1) = \frac{k(k+1)}{2} + k + 1$ .  $P(k + 1)$  zal bewezen zijn indien deze laatste uitdrukking gelijk is aan  $\frac{(k+1)((k+1)+1)}{2}$ . Inderdaad:  $\frac{k(k+1)}{2} + k + 1 = \frac{k(k+1)+2(k+1)}{2} = \frac{(k+2)(k+1)}{2} = \frac{(k+1)((k+1)+1)}{2}$ . Het inductieprincipe over  $\mathbb{N}$  zegt nu dat  $P(n)$  waar is voor alle  $n \in \mathbb{N}$ .  $\square$

Zoals we reeds lieten uitschijnen kan het inductieprincipe bewezen worden uit het welordeningsprincipe.

*Bewijs.*

Zij  $P$  een predikaat waarvoor  $P(0)$  geldt en  $P(k + 1)$  volgt uit  $P(k)$ . We bewijzen dat  $P(n)$  voor alle  $n \in \mathbb{N}$ . Veronderstel dat het niet zo is, en zij  $V$  de verzameling van natuurlijke getallen  $n$  waarvoor  $P(n)$  een valse uitspraak is. Bij veronderstelling is  $V$  niet leeg, en bevat  $V$  wegens het welordeningsprincipe een kleinste element  $k$ . Dan is  $k \neq 0$ , want er is gegeven dat  $P(0)$  waar is. Omdat  $k > 0$  is  $k - 1$  ook een natuurlijk getal. Omdat  $k$  minimaal werd gekozen en  $k - 1 < k$ , is  $P(k - 1)$  wel waar. Maar dan zou ook  $P(k - 1 + 1) = P(k)$  waar zijn, en we hadden juist verondersteld dat  $P(k)$  vals is! Er is maar één verklaring, en dat is dat zulke  $k$  niet bestaat, of dus dat  $V$  toch leeg is.

Omdat  $V$  leeg is, is  $P(n)$  waar voor alle  $n \in \mathbb{N}$ .  $\square$

Als inductiebasis kan men ook  $P(k)$  bewijzen voor een zekere  $k > 0$ . Het inductieprincipe zegt dan dat  $P(n)$  waar is voor alle  $n \geq k$ . Over de uitspraken  $P(0), P(1), \dots, P(k - 1)$  kan er dan echter niets besloten worden. Wat ook kan is als inductiebasis  $P(z)$  bewijzen voor een zekere  $z \in \mathbb{Z}$ . Als men dan bovendien bewijst dat  $P(n + 1)$  uit  $P(n)$  volgt voor alle  $n \geq z$ , dan kan men met het inductieprincipe besluiten dat  $P(n)$  voor alle  $n \geq z$ . Het volstaat immers het predikaat te hernoemen zo dat de inductiehypothese terug bij 0 komt te liggen: indien men liever  $P(z)$  als inductiebasis neemt, beschouw dat het predikaat  $Q$  met  $Q(n) = P(n + z)$ . De uitspraak “ $P(z)$  is waar” wordt hiermee “ $Q(0)$  is waar”, en “ $P(n + 1)$  volgt uit  $P(n)$  voor alle  $n \geq z$ ” vertaald zich als “ $Q(n + 1)$  volgt uit  $Q(n)$  voor alle  $n \geq 0$ ”.

I

# Elementaire getaltheorie



De begrippen die de basis vormen van de getaltheorie zijn deler en veelvoud. Stel  $a$  en  $b$  zijn gehele getallen met  $b \neq 0$ . Bij deling van  $a$  door  $b$  noemen we  $a$  het *deeltal* en  $b$  de *deler*.

**Definitie 1.1.** Deler en veelvoud

Zij  $a, b \in \mathbb{Z}$ . We zeggen dat  $a$  deelbaar is door  $b$  als er een  $k \in \mathbb{Z}$  bestaat waarvoor  $a = kb$ . We zeggen ook “ $b$  is een *deler* van  $a$ ”, “ $a$  is een *veelvoud* van  $b$ ”, of kortweg “ $b$  deelt  $a$ ”. We noteren:  $b \mid a$ .

Zo geldt bijvoorbeeld dat  $7 \mid 21$  omdat er een geheel getal  $k$  bestaat waarvoor  $21 = 7k$ , namelijk  $k = 3$ . Ook voor het tegenovergestelde fenomeen bestaat er een symbool. Als  $a$  niet deelbaar is door  $b$  noteren we

$$b \nmid a.$$

Als een getal een veelvoud is van 2 noemen we dat getal “even”. In het andere geval noemen we het getal “oneven”. Zo is 8 bijvoorbeeld even, en is  $-3$  oneven.

**Gevolgen 1.2.**

1. 0 is deelbaar door elk geheel getal dat niet 0 is. In het bijzonder is 0 even.
2. Als  $a, b \in \mathbb{Z}_0$  en  $b \mid a$ , dan geldt dat  $|b| \leq |a|$ .
3. Als  $a, b \in \mathbb{Z}_0$  zo dat  $b \mid a$  en  $a \mid b$ , dan geldt dat  $a = \pm b$ .
4. Als  $a, b \in \mathbb{Z}_0$  dezelfde delers hebben, dan is  $a = \pm b$ .

*Bewijs.*

1. Voor elk geheel getal  $a \neq 0$  bestaat er een getal  $k$  zo dat  $0 = ka$ , namelijk  $k = 0$ . Dus 0 is een even getal, want het is deelbaar door 2.
2. Als  $b \leq a$ , dan is  $a = kb$ , en omdat  $a \neq 0$  is  $|k| \geq 1$ . Nu geldt dat

$$|b| = \frac{|a|}{|k|} \leq \frac{|a|}{1} = |a|.$$

3. Uit het tweede gevolg weten we dat  $|b| \leq |a|$  en dat  $|a| \leq |b|$ , dus moet noodzakelijk  $|a| = |b|$ . Bijgevolg is  $a = \pm b$ .
4.  $a$  is een deler van zichzelf, dus omdat  $a \mid a$  geldt dan  $a \mid b$ . Om een anlogre reden geldt dat  $b \mid a$ . Uit het derde gevolg weten we dat  $a = \pm b$ .

□

**Stelling 1.3.** Deelbaarheid is transitief

Als  $a, b \in \mathbb{Z}_0$  en  $c \in \mathbb{Z}$  zo dat  $a \mid b$  en  $b \mid c$ , dan geldt  $a \mid c$ .

*Bewijs.*

Omdat  $b \mid c$  bestaat er een geheel getal  $k$  waarvoor  $c = kb$ . Omdat  $a \mid b$  bestaat er een tweede geheel getal  $x$  waarvoor  $b = xa$ . Dit vullen we in in de eerste gelijkheid, zodat  $c = kxa$ . Dus  $c$  is deelbaar door  $a$ , want er bestaat een geheel getal  $y$  waarvoor  $c = ya$ , namelijk  $y = kx$ .  $\square$

**Opgave 1.4.** Zij  $x, y \in \mathbb{Z}$  zo dat  $3 \mid x$  en  $3 \mid x + y$ . Is dan ook  $3 \mid y$ ?

**Opgave 1.5.** Zij  $a, b, c \in \mathbb{Z}$  zo dat  $5 \mid a$ ,  $7 \mid c$  en  $-10 \mid b$ . Toon aan dat  $5 \mid ac + b$ .

**Opgave 1.6.** Stel dat  $a, b \in \mathbb{Z}$  zo dat  $91 \mid a$  en  $56 \mid b$ . Bewijs dat  $14 \mid 12a + 3b$ .

**Definitie 1.7.** Lineaire combinatie

Als  $x, y \in \mathbb{Z}$ , noemen we  $ax + by$  een lineaire combinatie van  $a$  en  $b$ .

Bijvoorbeeld,  $4a - 5b$ ,  $-3b$  en  $0$  zijn lineaire combinaties van  $a$  en  $b$ .

**Stelling 1.8.**

Als  $d \mid a$  en  $d \mid b$ , dan deelt  $d$  elke lineaire combinatie van  $a$  en  $b$ .

*Bewijs.*

Uit  $d \mid a$  en  $d \mid b$  volgt dat  $a = md$  en  $b = nd$ . Dus  $ax + by = mdx + ndy = (mx + ny)d$ . Bijgevolg is  $ax + by$  deelbaar door  $d$  voor alle mogelijke waarden van  $x$  en  $y$ .  $\square$

Aantonen dat een getal  $n$  deelbaar is door een getal  $d$  gaat vrij eenvoudig, je hoeft maar een gepaste  $k \in \mathbb{Z}$  te vinden waarvoor  $n = kd$ . Bewijzen dat geen zo'n  $k$  bestaat ligt iets moeilijker.

**Voorbeeld 1.9.** Toon aan dat 100 niet deelbaar is door 7.

*Oplossing.*

Indien wel, zou er een  $k \in \mathbb{Z}$  zijn met  $7k = 100$ .  $k$  moet dan minstens 15 zijn, want als  $k \leq 14$  is  $7k \leq 98$ , wat kleiner is dan 100. Maar als  $k \geq 15$  is  $7k \geq 105$ , wat groter is dan 100. Bijgevolg bestaat geen zo'n  $k$ .

*Opmerking.*

Je zou misschien willen zeggen: "natuurlijk,  $\frac{100}{7}$  is geen geheel getal!" Wie zegt dat  $\frac{100}{7}$  niet geheel is? Intuïtief is dat misschien duidelijk, maar het geldt pas echt als bewezen van zodra je bijvoorbeeld kan aantonen dat het tussen twee gehele getallen ligt. En dat is essentieel wat in het voorbeeld werd gedaan. Verderop stellen we een veel praktischere voorwaarde op om te bewijzen dat een getal ondeelbaar is door een ander.

## 1.1 Rest en quotiënt

Ook als  $a$  geen deler is van  $b$  valt er iets nuttigs te vertellen over  $a$  en  $b$ .

**Definitie 1.10.** Rest en quotiënt

Zij  $a$  en  $b$  gehele getallen met  $b \neq 0$ . Gehele getallen  $q$  en  $r$  waarvoor  $a = bq + r$  en  $0 \leq r < |b|$  noemen we respectievelijk het *quotiënt* en de *rest* bij deling van  $a$  door  $b$ . Voor de rest zeggen we ook wel “ $a$  modulo  $b$  is  $r$ ” en noteren we  $a \bmod b = r$ .

De voorwaarde  $0 \leq r < |b|$  is hier van kapitaal belang, en mag nooit vergeten worden om te controleren of een getal wel de juiste rest is. Bijvoorbeeld, bij deling van 19 door 6 is het quotiënt 3 en de rest 1, want  $19 = 3 \cdot 6 + 1$  en  $0 \leq 1 < 6$ . De rest van een getal  $a$  bij deling door 2 noemen we ook de *pariteit* van  $a$ . De pariteit van een getal is dus steeds 0 of 1. De pariteit van een even getal is dus 0, en van een oneven getal zullen we zien dat het pariteit 1 heeft.

**Opgave 1.11.** Bepaal een rest en quotiënt bij deling van

- A. 6 door 10.
- B.  $-100$  door 7.
- C. 5 door  $-8$ .
- D.  $-50$  door  $-9$ .

De uitspraak “hét quotiënt en dé rest” wordt gerechtvaardigd door de volgende stelling:

**Stelling 1.12.** Unicité van rest en quotiënt

Voor alle gehele getallen  $a$  en  $b$  met  $b \neq 0$  bestaat er juist één koppel gehele getallen  $(q, r)$  waarvoor  $a = q \cdot b + r$  en  $0 \leq r < |b|$ .

We bewijzen eerst de uniciteit van rest en quotiënt.

**Opgave 1.13.** (Unicité van rest en quotiënt) Veronderstel dat er twee quotiënten zijn met bijhorende rest, zeg  $(q_1, r_1)$  en  $(q_2, r_2)$ .

- A. Toon aan dat  $r_1 - r_2$  deelbaar is door  $b$ .
- B. Toon aan dat  $r_1$  en  $r_2$  niet beide groter dan of gelijk aan 0 en kleiner dan  $|b|$  kunnen zijn.

Bijgevolg zijn rest en quotiënt uniek.

Nog te bewijzen is dat er steeds een quotiënt en een rest bestaan. Dit lijkt natuurlijk vanzelfsprekend, maar toch kan je dit als wiskundige niet aannemen zonder bewijs. Sterker nog, heel Hoofdstuk 7 steunt erop dat er een rest en een quotiënt bestaat.

**Voorbeeld 1.14.** Bewijs dat bij deling van  $a$  door  $b$  met  $b > 0$  er een rest en een quotiënt bestaan.

*Oplossing.*

Het getal  $\frac{a}{b}$  is een reëel getal. Dit ligt dus tussen twee opeenvolgende gehele getallen. In symbolen, er bestaat een geheel getal  $q$  zo dat  $q \leq \frac{a}{b} < q + 1$ . Dus  $bq \leq a < bq + b$  (merk op dat we hier de voorwaarde  $b > 0$  gebruiken), wat we kunnen schrijven als  $0 \leq a - qb < b$ . Stellen we nu  $r = a - qb$ , dan hebben we getallen  $q$  en  $r$  waarvoor  $a = qb + r$  en  $0 \leq r < b$ . Aan de twee voorwaarden is voldaan, dus bestaan er een quotiënt en een rest.

**Opgave 1.15.** Bewijs zelf dat er ook een rest en een quotiënt bestaan bij deling van  $a$  door  $b$  met  $b < 0$ . HA

Zoals eerder beloofd een praktische voorwaarde voor deelbaarheid.

**Eigenschap 1.16.** Praktische voorwaarde voor deelbaarheid

$b \mid a$  als en slechts als  $a$  rest 0 heeft bij deling door  $b$ .

*Bewijs.*

$b \mid a$  als en slechts als er een  $q \in \mathbb{Z}$  bestaat met  $a = qb$ . Dit laatste drukt precies uit dat  $a$  rest 0 heeft bij deling door  $b$ .  $\square$

We hernemen het eerdere voorbeeld.

**Voorbeeld 1.17.** Toon aan dat 100 niet deelbaar is door 7.

*Oplossing.*

Aangezien  $100 = 14 \cdot 7 + 2$  heeft 100 rest 2 bij deling door 7. Daar  $2 \neq 0$  is wegens bovenstaande eigenschap 7 geen deler van 100.

Deze eigenschap laat in praktisch alle gevallen toe om onze intuïtie te laten spreken.

## 1.2 Grootste gemene deler

Twee gehele getallen hebben altijd gemeenschappelijke delers. Zo hebben 6 en 10 precies vier gemeenschappelijke delers, namelijk  $-2, -1, 1$  en  $2$ .  $1$  en  $-1$  zijn delers van alle gehele getallen.

**Definitie 1.18.** Grootste gemene deler

De grootste gemene deler  $d$  van twee gehele getallen  $a$  en  $b$ , die niet beide 0 zijn, is het grootste geheel getal dat een deler is van zowel  $a$  als  $b$ . We noteren  $\text{ggd}(a, b)$ .

Bijvoorbeeld:  $\text{ggd}(6, 10) = 2$ ,  $\text{ggd}(0, 5) = 5$ ,  $\text{ggd}(-12, -16) = 4$ . Merk op dat het noodzakelijk is dat  $a$  en  $b$  niet beide 0 zijn, anders zou er geen grootste gemene deler bestaan, want 0 is deelbaar door elk geheel getal groter dan 0. We kunnen de grootste gemene deler ook definiëren voor meer dan twee getallen.

**Definitie 1.19.** Grootste gemene deler, meerdere getallen

De grootste gemene deler van een aantal gehele getallen is het grootste geheel getal dat een deler is van elk van die getallen. We noteren  $\text{ggd}(a_1, \dots, a_n)$ .

Bijvoorbeeld:  $\text{ggd}(15, -12, 3) = 3$ . Merk op dat de grootste gemene deler altijd een positief getal is. We zullen vaak geïnteresseerd zijn in getallen waarvoor de grootste gemene deler 1 is.

**Definitie 1.20.** Relatief priem

Als  $\text{ggd}(a, b) = 1$  dan noemen we  $a$  en  $b$  *onderling ondeelbaar*, *copriem* of *relatief priem*.  
 Als  $a_1, a_2, \dots, a_n$  gehele getallen zijn waarvoor  $\text{ggd}(a_i, a_j) = 1$  voor alle  $i \neq j$ , dan noemen we de getallen  $a_1, a_2, \dots, a_n$  *paarsgewijs relatief priem*.

*Opmerking.*

“ $a_1, \dots, a_n$  zijn paarsgewijs relatief priem” betekent niet hetzelfde als  $\text{ggd}(a_1, \dots, a_n) = 1$ . Zo is bijvoorbeeld  $\text{ggd}(2, 3, 9) = 1$ , maar de getallen 2, 3, 9 zijn niet paarsgewijs relatief priem want  $\text{ggd}(3, 9) \neq 1$ . Paarsgewijs relatief priem houdt dus in dat de grootste gemene deler van elke twee getallen gelijk is aan 1 (en dus i.h.b.  $\text{ggd}(a_1, \dots, a_n) = 1$ ).

### 1.3 Kleinste gemene veelvoud

Twee gehele getallen hebben gemeenschappelijke veelvouden. Zo zijn bijvoorbeeld  $ab$  en  $3ab$  gemeenschappelijke veelvouden van  $a$  en  $b$ .

**Definitie 1.21.** Kleinste gemene veelvoud

Het *kleinste gemene veelvoud*  $k$  van twee gehele getallen  $a$  en  $b$  is het kleinste geheel getal groter dan 0 dat een veelvoud is van  $a$  en  $b$ . We noteren  $\text{kgv}(a, b) = k$ .

Bijvoorbeeld:  $\text{kgv}(8, 6) = 24$ ,  $\text{kgv}(-2, 5) = 10$ ,  $\text{kgv}(-10, -18) = 90$ . De voorwaarde dat  $k > 0$  is noodzakelijk, zoniet zou het kleinste gemene veelvoud steeds 0 zijn, want 0 is een veelvoud van elk geheel getal. Merk op dat het kleinste gemene veelvoud dus niet bestaat als één van de getallen 0 is. Want 0 heeft maar één veelvoud, 0. Net zoals bij de grootste gemene deler kunnen we de definitie eenvoudig uitbreiden.

**Definitie 1.22.** Kleinste gemene veelvoud, meerdere getallen

Het kleinste gemene veelvoud van een aantal gehele getallen is het kleinste natuurlijk getal groter dan 0 dat een veelvoud is van elk van die getallen. We noteren  $\text{kgv}(a_1, \dots, a_n)$ .

Bijvoorbeeld:  $\text{kgv}(12, 5, -6) = 60$ .

**Stelling 1.23.**

Als  $a \mid c$  en  $b \mid c$ , dan  $\text{kgv}(a, b) \mid c$ .

*Bewijs.*

Stel  $\text{kgv}(a, b) = k$ , en  $q$  en  $r$  zijn het quotiënt en de rest van  $c$  bij deling door  $k$ , dus  $r < k$ . Dan is  $c = qk + r$ . Omdat  $a \mid c$  en  $a \mid k$ , is  $c = ma$  en  $k = xa$ , zodat  $r = c - qk = a(m - qx)$ . Dus  $a \mid r$ . Op een volledig analoge manier vind je dat  $b \mid r$ .  $r$  is dus een veelvoud van  $a$  en van  $b$ . Maar  $r < k$  en  $k$  is het kleinste strikt positief getal dat een veelvoud is van  $a$  en van  $b$ . De enige mogelijkheid is dus dat  $r = 0$ , zodat  $k \mid c$ .  $\square$

*Opmerking.*

Misschien was je zelf niet meteen op het idee gekomen op de rest en het quotiënt van  $c$  bij deling door  $k$  te bekijken. Aan een oefening als deze gaat dan ook heel wat geklungel vooraf,

tot je bij de juiste werkwijze terecht komt. Je moet dus niet te snel opgeven, maar soms toch eens een andere methode uitproberen. Hier waren er nog relatief weinig mogelijkheden. Om te bewijzen dat een getal  $x$  deelbaar is door  $y$  zijn er enkele opties:

- Uit de gegevens leidt je af dat  $x = ky$  voor een zeker geheel getal  $k$ .
- Je toont aan dat als een getal een deler is van  $y$ , dan ook een deler is van  $x$ .
- Je probeert te bewijzen dat de rest bij deling van  $x$  door  $y$  gelijk is aan 0. Hoe dat dan precies gebeurt kan verschillen van oefening tot oefening.

Er zijn nog tal van alternatieve methodes, maar hiermee heb je toch al drie relevante. In het algemeen moet je heel vaak gebruik maken van lineaire combinaties. In de volgende hoofdstukken kom je uiteenlopende stellingen tegen die ook hulp kunnen bieden.

## 1.4 De stelling van Bézout

**Stelling 1.24.** Stelling van Bézout<sup>6</sup>

Als  $a$  en  $b$  gehele getallen zijn is  $\text{ggd}(a, b)$  een lineaire combinatie van  $a$  en  $b$ .

Ook hier gaan we ervan uit dat  $a$  en  $b$  niet beide 0 zijn. Je zal merken dat we zoiets later ook stilzwijgend zullen veronderstellen. Je mag er dus steeds van uit gaan dat aan de beperkende voorwaarden voldaan is.

**Opgave 1.25.** (Bewijs van de stelling van Bézout) Noem  $V$  de verzameling van alle lineaire combinaties van  $a$  en  $b$ .

A. Toon aan dat  $V$  minstens één getal bevat dat groter is dan 0.

Bijgevolg heeft  $V$  een kleinste strikt positief element, zeg  $d$ . Noem  $q$  het quotiënt en  $r$  de rest van  $a$  bij deling door  $d$ .

B. Toon aan dat  $r$  een lineaire combinatie is van  $a$  en  $b$ .

C. Toon aan dat  $r = 0$ .

We hebben dus dat  $d \mid a$ . Analoog geldt dat  $d \mid b$ .  $d$  is dus een gemeenschappelijke deler van  $a$  en  $b$ . Stel dat  $c$  ook een gemeenschappelijke deler is van  $a$  en  $b$ .

D. Toon aan dat  $c \mid d$ , en dat  $c \leq d$ .

Bijgevolg is  $d$  de grootste gemene deler van  $a$  en  $b$ , en is de grootste gemene deler te schrijven als lineaire combinatie.

---

<sup>6</sup>Naar étienne Bézout. Voor het eerst geformuleerd door de Fransman Bachet in de 17e eeuw

**Gevolg 1.26.**

1. Als  $c \mid a$  en  $c \mid b$ , dan  $c \mid \text{ggd}(a, b)$ .
2.  $\text{ggd}(a, b)$  is de kleinst mogelijke strikt positieve lineaire combinatie van  $a$  en  $b$ .
3. Elk veelvoud van  $\text{ggd}(a, b)$  is een lineaire combinatie van  $a$  en  $b$ .

*Bewijs.*

1.  $c$  deelt elke lineaire combinatie van  $a$  en  $b$ , dus  $c$  deelt ook  $\text{ggd}(a, b)$ .
2.  $\text{ggd}(a, b)$  deelt  $a$  en  $b$ , dus  $\text{ggd}(a, b)$  deelt elke lineaire combinatie  $ax + by$  van  $a$  en  $b$ . Bijgevolg geldt dat als  $ax + by > 0$ , dan  $\text{ggd}(a, b) \leq ax + by$ . (Gevolg 1.2.2.)
3. Stel bijvoorbeeld  $c = k \cdot \text{ggd}(a, b)$ , dan is  $c = k(xa + yb)$  voor bepaalde getallen  $x$  en  $y$ , zodat  $c = kx \cdot a + ky \cdot b$ . Hiermee is  $c$  dus een lineaire combinatie van  $a$  en  $b$ . □

**Voorbeeld 1.27.** Bewijs dat  $\text{ggd}(a, b) = \text{ggd}(a, b - na)$  voor elk geheel getal  $n$ .*Oplossing.*

We tonen aan dat  $d$  een deler is van  $\text{ggd}(a, b - na)$  als en slechts als  $d$  een deler is van  $\text{ggd}(a, b)$ . Als  $d \mid \text{ggd}(a, b)$ , dan  $d \mid a$  en  $d \mid b$ , zodat  $d \mid 1 \cdot b - n \cdot a = b - na$ , dus  $d \mid \text{ggd}(a, b - na)$ .

Als  $d \mid \text{ggd}(a, b - na)$ , dan  $d \mid n \cdot a + 1 \cdot (b - na) = b$  dus  $d \mid \text{ggd}(a, b)$ . (Hier gebruikten we dus tweemaal Stelling 1.8 en Gevolg 1.26.2.)

De getallen  $\text{ggd}(a, b)$  en  $\text{ggd}(a, b - na)$  hebben dezelfde delers en zijn dus gelijk wegens Gevolg 1.2.4.

*Opmerking.*

Behalve het feit dat  $a$  en  $b$  niet beide nul zijn, hadden we hier geen enkele beperkende voorwaarde voor deze eigenschap. Dat maakt ze heel krachtig, zoals je zal merken bij het algoritme van Euclides.

Het volgende lemma zal nog nuttig blijken.

**Lemma 1.28.**

Stel dat  $\text{ggd}(a, b) = 1$  en  $a \mid bc$ . Dan is  $a \mid c$ .

*Bewijs.*

Omdat  $\text{ggd}(a, b) = 1$  bestaan er  $x$  en  $y$  zo dat  $ax + by = 1$ . Dus  $axc + byc = c$ .

Omdat  $a \mid bc$  is  $bc = ka$ . Dan is  $axc + yka = c$ , of dus  $(xc + yk)a = c$ . Dus  $a \mid c$ . □

*Opmerking.*

De cruciale stap in dit bewijs was om in de eerste gelijkheid links en rechts te vermenigvuldigen met  $c$ . Dit komt nogal uit de lucht gevallen, maar eigenlijk is het een logische zet. We willen namelijk bekomen dat  $a \mid c$ , dus  $c = \dots \cdot a$ . Het is dus ergens wel voor de hand liggend dat we  $c$  afzonderen aan één kant van het gelijkheidsteken, zonder dat er extra factoren bij staan.

**Opdracht 1.29.** Stel dat  $a \mid c$ ,  $b \mid c$  en  $\text{ggd}(a, b) = 1$ . Bewijs dat  $ab \mid c$ .*Opmerking.*

Deze oefening en de volgende lijken heel vanzelfsprekend. Je denkt misschien: dat klopt toch, zoiets moet je toch niet bewijzen? Inderdaad, maar voor een wiskundige kan je met intuïtie niets bewijzen. Geef trouwens toe dat een bewijsje als het vorige heel mooi is als je

het netjes opschrijft en de intuïtie achterwege laat. Probeer dat dus ook te doen en maak enkel gebruik van eigenschappen die je tot nu toe bent tegengekomen, zonder zelf eigenschappen te verzinnen.

**Opgave 1.30.** Stel dat  $\text{ggd}(a, b) = 1$ . Toon aan dat  $\text{ggd}(a, c) = \text{ggd}(a, bc)$ .

**Opgave 1.31.** Stel  $d$  is een geheel getal.

A. Bewijs dat  $\text{ggd}(da, db) = d \cdot \text{ggd}(a, b)$ .

Stel nu  $g = \text{ggd}(a, b)$ .

B. Bewijs dat  $\text{ggd}\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ .

De stelling van Bézout kan worden veralgemeend naar meerdere getallen.

**Stelling 1.32.** Stelling van Bézout, algemeen geval

Als  $a_1, a_2, \dots, a_n$  gehele getallen zijn, dan kan  $\text{ggd}(a_1, a_2, \dots, a_n)$  geschreven worden als lineaire combinatie van  $a_1, a_2, \dots, a_n$ .

**Opgave 1.33.** Bewijs.

H

## 1.5 Algoritme van Euclides

Het algoritme van Euclides is een techniek om de grootste gemene deler van twee getallen te bepalen. Het maakt gebruik van het principe uit Voorbeeld 1.27. Als  $r$  de rest is bij deling van  $b$  door  $a$ , dan geldt dat  $\text{ggd}(a, b) = \text{ggd}(a, r)$ . Want uit Voorbeeld 1.27 weten we dat  $\text{ggd}(a, b) = \text{ggd}(a, b - na)$  ook geldt als  $n$  het quotiënt is bij deling van  $b$  door  $a$ . En dan is  $b - na = r$ .

Om  $\text{ggd}(a, b)$  te berekenen voor gegeven getallen  $a$  en  $b$  met  $a < b$  bereken je de rest  $r$  bij deling van  $b$  door  $a$  en je zoekt dan  $\text{ggd}(a, r)$ . Door dit te herhalen bekom je steeds kleinere getallen totdat er  $\text{ggd}(d, 0)$  komt te staan. Dan geldt dat  $\text{ggd}(a, b) = d$ . Zo vinden we bijvoorbeeld

$$\text{ggd}(459, 342) = \text{ggd}(117, 342) = \text{ggd}(117, 108) = \text{ggd}(9, 108) = \text{ggd}(9, 0) = 9.$$

Deze werkwijze kunnen we ook noteren in het zogenaamde rekenschema van Euclides. Eerst noteren we het grootste van de twee getallen links in het midden en daarnaast het kleinste.

459	342				

Vervolgens bepalen we het quotiënt bij deling van het grootste door het kleinste, 1. Dat noteren we boven de deler. Dan berekenen we het product van het quotiënt met de deler,  $1 \cdot 342 = 342$ , en dat noteren we onder het deeltal.

	1				
459	342				
342					

Dan trekken we het bekomen product af van het deeltal,  $459 - 342 = 117$ , en we hebben de rest.



	1				
459	342	117			
342					

Dit proces herhalen we, met de rest als nieuwe deler en de vorige deler als deeltal.

	1	2			
459	342	117	108		
342	234				

We blijven dit herhalen totdat er 0 als rest komt te staan.

	1	2	1	12	
459	342	117	108	9	0
342	234	108	108		

De laatste deler, 9, is dan de grootste gemene deler.

Schematisch:

**Gevolg 1.34.**

Met het rekenschema van Euclides kan men de grootste gemene deler schrijven als lineaire combinatie. Deze techniek noemen we het uitgebreid algoritme van Euclides.

We hernemen het voorgaande voorbeeld.

**Voorbeeld 1.35.** Schrijf  $9 = \text{ggd}(459, 342)$  als lineaire combinatie van 459 en 342.

*Oplossing.*

Als we de eerste deling uitvoeren bekommen we dat de rest gelijk is aan

$$117 = 1 \cdot 459 - 1 \cdot 342.$$

Dit verschil werken we niet uit en laten we zo staan. Bij de tweede deling vinden we als rest  $108 = 1 \cdot 342 - 2 \cdot 117$ . Hierin vervangen we 117 door  $1 \cdot 459 - 1 \cdot 342$  en we schrijven 108 als lineaire combinatie van 459 en 342, namelijk

$$108 = 1 \cdot 342 - 2 \cdot 117 = 1 \cdot 342 - 2 \cdot (1 \cdot 459 - 1 \cdot 342) = 3 \cdot 342 - 2 \cdot 459.$$

We doen hetzelfde voor 9 en we vinden

$$9 = 1 \cdot 117 - 1 \cdot 108 = 1 \cdot (1 \cdot 459 - 1 \cdot 342) - 1 \cdot (3 \cdot 342 - 2 \cdot 459) = 3 \cdot 459 - 4 \cdot 342.$$

We hebben 9 dus geschreven als lineaire combinatie van 459 en 342.

Het zal niet steeds nodig zijn om het rekenschema van Euclides te gebruiken om de grootste gemene deler te schrijven als lineaire combinatie. Soms zal je op zicht een lineaire combinatie kunnen bedenken, maar dit algoritme geeft een algemene manier waar je steeds op kan vertrouwen. Zo is bijvoorbeeld de grootste gemene deler van twee opeenvolgende getallen gewoon hun verschil:  $\text{ggd}(28, 29) = 1 \cdot 29 - 1 \cdot 28$ . En daarmee heb je meteen een lineaire combinatie.

Dat je hier steeds op mag vertrouwen wordt duidelijk in de volgende oefening:

**Opgave 1.36.** Toon aan dat je met het algoritme van Euclides steeds de grootste gemene deler bekomt.

- A. Toon aan dat je na een eindig aantal stappen steeds 0 als rest bekomt.
- B. Toon aan dat de voorlaatste rest een veelvoud is van de grootste gemene deler.
- C. Toon aan dat de voorlaatste rest een deler is van elke voorgaande rest.
- D. Toon aan dat die voorlaatste rest de grootste gemene deler is.

## 1.6 Lineaire Diophantische vergelijkingen

Een Diophantische vergelijking is een heel algemeen begrip.

### Definitie 1.37. Diophantische vergelijking

Een *Diophantische vergelijking* is een vergelijking in één of meerdere variabelen waarbij we zoeken naar gehele of natuurlijke oplossingen voor die variabelen.

Een Diophantische vergelijking kan allerlei vormen aannemen. Zo zijn

$$p^{7x^2+3} - a^2 = 2^n$$

en

$$\frac{(a!)^{b!}}{b^a} = x^y + y^x$$

Diophantische vergelijkingen. Voorlopig zijn we iets minder ambitieus:

### Definitie 1.38. Lineaire Diophantische vergelijking

Een *lineaire Diophantische vergelijking* is een vergelijking van de vorm  $ax + by = c$ , waarbij  $a, b, c \in \mathbb{Z}$  en we oplossingen in gehele getallen zoeken voor  $x$  en  $y$ .

### Stelling 1.39.

De lineaire Diophantische vergelijking  $ax + by = c$  heeft een oplossing als en slechts als  $\text{ggd}(a, b) \mid c$ . Indien  $(x_0, y_0)$  een oplossing is worden alle oplossingen gegeven door

$$x = x_0 + \frac{kb}{\text{ggd}(a, b)} \quad \text{en} \quad y = y_0 + \frac{ka}{\text{ggd}(a, b)}, \quad k \in \mathbb{Z}.$$

### Opgave 1.40. Bewijs.

Stel dat zo'n Diophantische vergelijking een oplossing heeft.

- A. Toon aan dat  $\text{ggd}(a, b) \mid c$ .

Indien er een oplossing is, geldt dus dat  $\text{ggd}(a, b) \mid c$ . Bijgevolg kunnen we  $c$  schrijven als lineaire combinatie van  $a$  en  $b$ . Via het uitgebreid algoritme van Euclides bepalen we dan getallen  $x_0$  en  $y_0$  zo dat  $ax_0 + by_0 = c$ . Dit geeft al één oplossing voor  $x$  en  $y$ . Stel nu  $d = \text{ggd}(a, b)$ .

Stel dat  $x$  en  $y$  oplossingen zijn. We kunnen zeggen dat  $x = x_0 + m$  en  $y = y_0 - n$ .

- B. Toon aan dat  $am = bn$ .

C. Toon aan dat  $\frac{b}{d} \mid m$ .

Bijgevolg is  $m = \frac{kb}{d}$ .

D. Toon aan dat  $n = \frac{ka}{d}$ .

De algemene oplossing is dus  $x = x_0 + \frac{kb}{d}$  en  $y = y_0 + \frac{ka}{d}$ , waar  $k$  elk geheel getal mag zijn. Voor  $k = 0$  bekomen we opnieuw de oorspronkelijke oplossing die we vonden via het rekenschema van Euclides.

*Opmerking.*

Omdat  $d \mid a, b, c$  hadden we ook  $a = da_0$ ,  $b = db_0$  en  $c = dc_0$  kunnen stellen, zodat we de vergelijking  $a_0x + b_0y = c_0$  bekwamen, met  $\text{ggd}(a_0, b_0) = 1$ . Dat is wat we in de praktijk zullen doen bij het oplossen van zo'n vergelijking, maar hier zou dat de oefening niet bijzonder eenvoudiger hebben gemaakt.

#### **Gevolg 1.41.**

1. De grootste gemene deler van twee getallen  $a$  en  $b$  kan op oneindig veel manieren worden geschreven als lineaire combinatie.
2. We kunnen de grootste gemene deler  $d$  van twee strikt positieve of twee strikt negatieve getallen  $a$  en  $b$  schrijven als  $ax + by$  met  $x > 0$  en  $y < 0$ , of met  $x < 0$  en  $y > 0$ .

*Bewijs.*

1. De waarde van  $k$  in de algemene oplossing mag elk geheel getal zijn.
2. Stel dat  $a, b > 0$ . In de algemene oplossing,  $x = x_0 + \frac{kb}{d}$  en  $y = y_0 + \frac{ka}{d}$ , kunnen we  $k$  een voldoende grote waarde geven, zodat  $x > 0$  en  $y < 0$ , of een voldoende kleine waarde, zodat  $x < 0$  en  $y > 0$ . Voor  $a, b < 0$  kunnen we analoog tewerk gaan.

□

De voorwaarde dat  $a$  en  $b$  hetzelfde teken hebben is noodzakelijk in Gevolg 1.41.2. Want als bijvoorbeeld  $b \leq 0$  en  $a > 0$ , dan zou het verhogen van  $k$  ervoor zorgen dat  $x$  kleiner wordt of gelijk blijft, terwijl  $y$  ook kleiner wordt. En dan kunnen we niet met zekerheid zeggen dat het mogelijk is om  $x > 0$  en  $y < 0$  te verkrijgen.

**Voorbeeld 1.42.** Bepaal alle oplossingen van de vergelijking  $72x - 30y = 18$ .

*Oplossing.*

We beginnen met het ons zelf niet te moeilijk te maken. We kunnen delen door 6 en het rekenwerk zal heel wat lichter zijn:  $12x - 5y = 3$ . (Merk op dat we er hierdoor steeds voor zorgen dat de grootste gemene deler van de coëfficiënten bij  $x$  en  $y$  steeds 1 zal zijn.)

We schrijven eerst  $\text{ggd}(12, -5)$ , of dus  $\text{ggd}(12, 5)$ , als lineaire combinatie van 12 en 5 via het rekenschema van Euclides. We laten het minteken even weg om zeker te zijn dat we geen fouten maken met mintekens, dat maakt het rekenwerk eenvoudiger.

	2	2	1	
12	5	2	1	0
10	4	2		

We vinden  $\text{ggd}(12, 5) = 1 = 1 \cdot 5 - 2 \cdot 2 = 1 \cdot 5 - 2 \cdot (1 \cdot 12 - 2 \cdot 5) = -2 \cdot 12 + 5 \cdot 5$ . Om de getallen  $x_0$  en  $y_0$  te vinden moeten we  $\text{ggd}(12, -5)$  wel schrijven als lineaire combinatie met  $-5$ , en niet met 5. Dus  $1 = -2 \cdot 12 - 5 \cdot (-5)$ .

Om 3 te schrijven als lineaire combinatie vinden we dan  $3 = 3 \cdot 1 = -6 \cdot 12 - 15 \cdot (-5)$ .

We hebben dus dat  $x_0 = -6$  en  $y_0 = -15$ .

De algemene oplossing is dan  $x = x_0 + \frac{k \cdot (-5)}{1} = -6 - 5k$  en  $y = y_0 - \frac{k \cdot 12}{1} = -15 - 12k$ , met  $k$  een willekeurig geheel getal.

*Opmerking.*


Als je liever niet zo veel mintekens ziet, mag je natuurlijk ook  $k$  vervangen door  $-t$ , zodat je  $x = 5t - 6$  en  $y = 12t - 15$  hebt, of zelfs door  $-t - 2$  zodat er  $x = 5t + 4$  en  $y = 12t + 9$  komt te staan. Al die notaties zijn goed, want ze geven dezelfde oplossingen. Maar bijvoorbeeld de substitutie  $k = 2t + 1$  is niet goed. Hiermee zal je enkel oneven waarden van  $k$  kunnen krijgen. Om dezelfde reden is  $k = 5t + 4$  ook niet goed, want daarmee krijg je alleen waarden van  $k$  die rest 4 hebben bij deling door 5. De waarde  $k = 1$  bijvoorbeeld kan je zo nooit bekomen.


**Opgave 1.43.** Bepaal alle gehele getallen  $m$  en  $n$  waarvoor  $50m - 28n = -16$ .


**Opgave 1.44.** Bepaal alle oplossingen voor  $p$  en  $q$  van de vergelijking  $-35p + 84q = 65$ .

Voor een leuke praktische toepassing van dit soort vergelijkingen verwijzen we naar Subsectie 16.1.


## Opgaven hoofdstuk 1

**Opgave 1.45.** (JWO 2007 finale vraag 3) Wat is het kleinste getal  $\overline{xyz}$  bestaande uit drie verschillende cijfers  $x, y$  en  $z$  elk verschillend van 0 zo dat het gemiddelde van de getallen  $\overline{xyz}, \overline{xzy}, \overline{yxz}, \overline{yzx}, \overline{zxy}, \overline{zyx}$  een natuurlijk getal is dat eindigt op 0? 

**Opgave 1.46.** (VWO 1991 finale vraag 1) Toon aan dat het getal, gevormd door 1991 keer het cijfer 1 na elkaar te schrijven, niet priem is. 


**Opgave 1.47.** (VWO 2013 ronde 2 vraag 17) Als je  $10!$  deelt door  $9! - 1$  krijg je als rest  H  
(A) 0                      (B) 1                      (C) 8                      (D) 9                      (E) 10

**Opgave 1.48.** Bewijs dat  $\text{ggd}(3a, 6a + 1) = 1$ .

**Opgave 1.49.** (IMO 1959 dag 1 vraag 1) Bewijs dat de breuk  $\frac{21n+4}{14n+3}$  voor geen enkel natuurlijk getal  $n$  vereenvoudigbaar is. 

**Opgave 1.50.** Bewijs dat  $\text{ggd}(2n^2 - 1, n + 1) = 1$ .

**Opgave 1.51.** Toon aan dat  $\text{kgv}(n, n + 1) = n^2 + n$ .

**Opgave 1.52.** Stel dat  $\text{ggd}(a, b) = 1$ . Bewijs dat  $\text{ggd}(a + b, a - b) \in \{1, 2\}$ . 

**Opgave 1.53.** Stel dat  $\text{ggd}(a, b) = 1$ . Bewijs dat  $\text{ggd}(a + b, a^2 - ab + b^2) \in \{1, 3\}$ .

**Opgave 1.54.** Bewijs dat voor natuurlijke getallen  $x$  en  $y$  geldt dat  $17 \mid 2x + 3y$  als en slechts als  $17 \mid 9x + 5y$ .

**Opgave 1.55.** (NWO 1982 ronde 2 vraag 4) Stel  $n = 9^{753}$ . Bepaal  $\text{ggd}(n^2 + 2, n^3 + 1)$ .

**Opgave 1.56.** Stel  $a > 1$  en  $m, n > 0$ . Toon aan dat  $\text{ggd}(a^m - 1, a^n - 1) = a^{\text{ggd}(m, n)} - 1$ .  H

**Definitie 2.1.** Priemgetal

Een *priemgetal* is een natuurlijk getal met precies twee positieve delers.

Bijgevolg zijn deze delers steeds 1 en zichzelf. Als  $p$  een priemgetal is zeggen we ook wel “ $p$  is priem”. De kleinste tien priemgetallen zijn 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. 1 is geen priemgetal, want het heeft slechts één positieve deler. Als een priemgetal  $p$  een deler is van een getal  $n$ , dan zeggen we ook wel “ $p$  is een priemdelers van  $n$ ”.

**Definitie 2.2.** Samengesteld getal

Een *samengesteld getal* is een natuurlijk getal groter dan 1 dat geen priemgetal is.

1 is per definitie noch priem, noch samengesteld. 1 en  $-1$  worden ook wel *eenheden* van  $\mathbb{Z}$  genoemd.

**Voorbeeld 2.3.** Als  $p$  en  $q$  verschillende priemgetallen zijn, bewijs dat  $\text{ggd}(p, q) = 1$ .

*Oplossing.*

Er geldt dat  $\text{ggd}(p, q) \mid p$ , dus  $\text{ggd}(p, q) = 1$  of  $\text{ggd}(p, q) = p$ . Want 1 en  $p$  zijn de enige delers van  $p$ . Anderzijds geldt dat  $\text{ggd}(p, q) \mid q$ , dus  $\text{ggd}(p, q) = 1$  of  $\text{ggd}(p, q) = q$ . De enige mogelijkheid is dus dat  $\text{ggd}(p, q) = 1$ .

**Opgave 2.4.** Zij  $p$  een priemgetal. Toon aan dat  $p \mid \binom{p}{a}$  voor elke  $a$  met  $0 < a < p$ .

## 2.1 Priemontbinding

**Stelling 2.5.** Hoofdstelling van de rekenkunde

Elk natuurlijk getal  $n$  groter dan 1 is te schrijven als het product van priemgetallen,  $p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$  waarbij  $p_1, p_2, \dots, p_r$  verschillende priemgetallen zijn en  $a_1, a_2, \dots, a_r$  natuurlijke getallen groter dan 0. Deze schrijfwijze is bovendien uniek, op de volgorde van de factoren na.

**Definitie 2.6.** Priemontbinding

De schrijfwijze

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$$

noemen we de *priemontbinding* of *priemfactorisatie* van  $n$ .

Bijvoorbeeld, de priemontbinding van 48 is  $2^4 \cdot 3$ . De priemfactorisatie van 1050 is  $2 \cdot 3 \cdot 5^2 \cdot 7$ . Vaak wordt deze stelling als dieper liggende reden gebruikt dat 1 niet tot de priemgetallen wordt gerekend. Want indien 1 wel een priemgetal was, dan zou de priemontbinding niet uniek zijn. Dan zouden bijvoorbeeld zowel  $2^4 \cdot 3$ ,  $1 \cdot 2^4 \cdot 3$  als  $1^{13} \cdot 2^4 \cdot 3$  verschillende priemontbindingen zijn van 48.

Het bewijs van de hoofdstelling bestaat uit twee delen: bewijzen dat er zo'n priemontbinding bestaat, en bewijzen dat ze uniek is. Dit lijkt allemaal vanzelfsprekend, maar er vergelijkbare situaties denkbaar waarin de priemontbinding niet uniek is (Opgave 2.53) of zelfs niet bestaat (Hoofdstuk 19). Er is dus wel degelijk iets bijzonders aan de hand met  $\mathbb{Z}$  dat er voor zorgt dat alles probleemloos verloopt.

**Opgave 2.7.** Bewijs dat er voor elk natuurlijk getal  $n$  met  $n > 1$  een ontbinding bestaat in priemgetallen.

We bewijzen dit via volledige inductie.

Basisstap. Er bestaat een priemontbinding voor  $n = 2$ , want 2 is een priemgetal.

Inductiestap. Veronderstel dat  $n > 2$  en dat alle getallen kleiner dan  $n$  en groter dan 1 een priemontbinding hebben.

- A. Toon aan dat  $n$  een priemontbinding heeft als  $n$  een priemgetal is.
- B. Toon aan dat  $n$  een priemontbinding heeft als  $n$  een samengesteld getal is.

Het bewijs volgt nu via volledige inductie.

**Opgave 2.8.** Bewijs dat de priemontbinding uniek is.

Stel  $n$  is het kleinste natuurlijk getal groter dan 1 dat geen unieke priemontbinding heeft. Dus  $n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$ , met  $p_1 \leq p_2 \leq \cdots \leq p_r$  en  $q_1 \leq q_2 \leq \cdots \leq q_s$ . (Dit is niet de normale manier om een priemontbinding te noteren, maar je zal merken waarom deze manier zo handig is.)

- A. Toon aan dat  $q_s$  niet in de rij  $p_1, p_2, \dots, p_r$  voorkomt.

$q_s$  is een deler van  $n$  en dus van  $p_1 \cdot p_2 \cdots p_r$ .

- B. Toon aan dat  $q_s$  een deler is van  $p_2 \cdot p_3 \cdots p_r$ .
- C. Herhaal deze werkwijze en toon aan dat  $q_s$  een deler moet zijn van  $p_r$ .

Bijgevolg is het onmogelijk dat  $n$  geen unieke priemontbinding heeft, want anders zou  $q_s = p_r$  maar we hadden al aangetoond dat  $q_s$  niet in de rij  $p_1, p_2, \dots, p_r$  voorkomt. Aangezien er geen kleinste getal  $n$  is zonder unieke priemontbinding, is er dus geen enkel getal zonder unieke priemontbinding.

## 2.2 Gevolgen van de hoofdstelling

**Gevolg 2.9.**

1. De grootste gemene deler van twee natuurlijke getallen is het product van alle priemfactoren met hun kleinst voorkomende exponent. In formulevorm, als  $x$  en  $y$  natuurlijke getallen zijn met  $x = n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$  en  $y = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$ , dan geldt

$$\text{ggd}(x, y) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_r^{\min(a_r, b_r)}.$$

2. Het kleinste gemene veelvoud van twee natuurlijke getallen is het product van alle priemfactoren met hun hoogst voorkomende exponent. In formulevorm, als  $x$  en  $y$  natuurlijke getallen zijn met  $x = n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$  en  $y = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$ , dan geldt

$$\text{kgv}(x, y) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_r^{\max(a_r, b_r)}.$$

*Bewijs.*

1. Een getal met een factor  $p_i^k$  met  $k > \min(a_i, b_i)$  zal geen deler zijn van  $x$  en  $y$ , aangezien de exponent van  $p_i$  dan niet bij zowel  $x$  en  $y$  minstens  $k$  kan zijn. De priemontbinding is immers uniek.
2. Een getal waarvoor de exponent van  $p_i$  in de priemontbinding strikt kleiner is dan  $\max(a_i, b_i)$ , kan niet deelbaar zijn door  $p_i^{\max(a_i, b_i)}$ , en dus niet door zowel  $p_i^{a_i}$  als  $p_i^{b_i}$ . □

**Stelling 2.10.** Euclides

Er bestaan oneindig veel priemgetallen.

Eigenlijk is dit niet precies wat Euclides bewees. Euclides geloofde hoogst waarschijnlijk niet eens in het bestaan van een oneindige verzameling, een absurd begrip in zijn tijd. Hij bewees echter dat, indien er een eindig aantal priemgetallen is, er toch nog een ander priemgetal kan worden gevonden. In moderne termen betekent dit zo goed als hetzelfde, en zijn bewijs is dan ook nog steeds bruikbaar, ondanks de verschillende semantiek:

**Opgave 2.11.** Bewijs dat er oneindig veel priemgetallen bestaan.

Veronderstel dat er slechts een eindig aantal priemgetallen bestaat. Noem die priemgetallen  $p_1, p_2, \dots, p_n$ . Beschouw nu het getal  $x = 1 + p_1 p_2 \cdots p_n$ .

- A. Toon aan dat  $x$  geen priemgetal kan zijn.
- B. Toon aan dat  $x$  niet deelbaar kan zijn door een priemgetal  $p_i$ .

Bijgevolg heeft  $x$  geen priemontbinding, wat niet kan wegens de hoofdstelling van de rekenkunde. Het is dus onmogelijk dat er slechts een eindig aantal priemgetallen bestaat.

**Opgave 2.12.** Bereken de grootste gemene deler en het kleinste gemene veelvoud van

- A. 75 en 60.
- B. 1000 en 350.
- C.  $30^{40}$  en  $40^{30}$ .
- D.  $123^{456}$  en  $456^{123}$ .

**Stelling 2.13.**

Er geldt dat  $\text{ggd}(a, b) \cdot \text{kgv}(a, b) = ab$  voor natuurlijke getallen  $a$  en  $b$ .

*Bewijs.*

Als oefening. □

**Opgave 2.14.** Toon aan dat  $\text{kgv}(x^n, y^n) = (\text{kgv}(x, y))^n$  voor elk natuurlijk getal  $n$ . Geldt A hetzelfde voor de grootste gemene deler?

**Opgave 2.15.** Toon aan dat  $n$  met  $n > 1$  een volkomen kwadraat is als en slechts alle priemfactoren van  $n$  tot een even macht voorkomen in de priemontbinding.

**Definitie 2.16.**  $p$ -adische valuatie

Als  $n \in \mathbb{Z}_0$  en  $p$  is een priemgetal noteren we  $v_p(n)$  voor het aantal priemfactoren  $p$  in de priemontbinding van  $|n|$ .<sup>7</sup> (Ook wel: *p-adische valuatie* van  $n$ .) Indien  $v_p(n) = k$  noteren we ook  $p^k \parallel n$ .

Zo is  $v_2(-1) = 0$ ,  $v_5(50) = 2$  en  $v_7(2) = 0$ .

**Opgave 2.17.** (Valuatie is additief) Bewijs dat  $v_p(ab) = v_p(a) + v_p(b)$  voor priemgetallen  $p$  en  $a, b \in \mathbb{Z}_0$ .

**Lemma 2.18.**

Er geldt dat  $\text{ggd}(\text{kgv}(a, b), \text{kgv}(a, c)) = \text{kgv}(a, \text{ggd}(b, c))$  voor gehele getallen  $a, b, c$ .

*Bewijs.*

We beschouwen eerst slechts één priemgetal  $p$ . Stel dat  $v_p(a) = x$ ,  $v_p(b) = y$  en  $v_p(c) = z$ . We tonen nu aan dat  $p$  in het linker- en rechterlid tot een gelijke macht voorkomt.

In het linkerlid is de exponent van  $p$  gelijk aan  $\min(\max(x, y), \max(x, z))$ . Hier passen we gewoon het eerste en tweede gevolg van de hoofdstelling van de rekenkunde toe. Immers, de exponent van  $p$  in  $\text{kgv}(a, b)$  is  $\max(x, y)$ , en in  $\text{kgv}(a, c)$  is die  $\max(x, z)$ . Als we dan de grootste gemene deler van deze twee getallen nemen, komt  $p$  daarin voor tot de kleinst voorkomende macht:  $\min(\max(x, y), \max(x, z))$ .

In het rechterlid is de exponent van  $p$  gelijk aan  $\max(x, \min(y, z))$ , om een gelijkaardige reden. We moeten nu dus aantonen dat  $\min(\max(x, y), \max(x, z)) = \max(x, \min(y, z))$ . We kunnen veronderstellen dat  $y \leq z$ , want de gelijkheid is symmetrisch in  $y$  en  $z$ . Het rechterlid is dan gelijk aan  $\max(x, y)$ .

We bekijken nu het linkerlid. Omdat  $y \leq z$ , kan  $\max(x, y)$  niet groter zijn dan  $\max(x, z)$ . Stel bijvoorbeeld dat  $\max(x, y) = x$  en dat  $x > \max(x, z)$ . Dan moet  $x > z$  en  $x > x$ , wat een belachelijke tegenstrijdigheid is.

In het geval dat  $\max(x, y) = y$  en  $y > \max(x, z)$  geldt dat  $y > x$  en  $y > z$ . Maar we hadden gesteld dat  $y \leq z$  dus ook dit is onmogelijk.

<sup>7</sup>De  $v$  is een Griekse letter nu, en geen  $v$ , maar je moet al heel proper schrijven om het verschil te zien...



Bijgevolg is  $\max(x, y) \leq \max(x, z)$ , zodat het linkerlid gelijk is aan  $\max(x, y)$ . Linker- en rechterlid zijn dus gelijk, waaruit we besluiten dat  $p$  in de twee leden van de oorspronkelijke gelijkheid tot dezelfde macht voorkomt.

Deze redenering geldt voor elk priemgetal  $p$ . Dus de twee leden hebben dezelfde priemontbinding, en zijn dus gelijk.  $\square$

**Lemma 2.19.**

Er geldt dat  $\text{kgv}(\text{ggd}(a, b), \text{ggd}(a, c)) = \text{ggd}(a, \text{kgv}(b, c))$  voor gehele getallen  $a, b, c$ .

**Opgave 2.20.** Bewijs.

H

**Stelling 2.21.** Formule van Legendre

Er geldt dat

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Merk op dat de som gewoon een eindig aantal termen heeft, omdat de termen met  $p^k > n$  steeds 0 zijn.

*Bewijs.*

Als oefening  $\square$

**Stelling 2.22.** Postulaat van Bertrand

Voor elk natuurlijk getal  $n > 1$  bestaat er een priemgetal  $p$  met  $n < p < 2n$ .

Dit verassende resultaat, sinds 1850 ook gekend als de stelling van Tshebysjev, werd in 1845 als vermoeden geformuleerd door de Fransman Joseph Bertrand. Het werd voor het eerst bewezen in 1850 door Pafnoeti Tshebysjev, in Hoofdstuk 21 geven we een eenvoudiger bewijs van de Hongaar Paul Erdős. Het bewijs is elementair en steunt op niet meer dan wat hieraan vooraf gaat.

Een klassieke toepassing van het Postulaat van Bertrand die we niet kunnen achterhouden:

**Opgave 2.23.** Vind alle natuurlijke getallen  $n$  waarvoor  $n!$  een kwadraat is.

### 2.2.1 Rationale getallen

**Eigenschap<sup>8</sup> 2.24.**

Een rationaal getal is een getal van de vorm  $\frac{a}{b}$  met  $a \in \mathbb{Z}$  en  $b \in \mathbb{Z}_0$ .  $\mathbb{Q}$  is de verzameling van rationale getallen.

Wie rationaal zegt, zegt irrationaal.

**Definitie 2.25. Irrationaal getal**

Een irrationaal getal is een reëel getal dat niet rationaal is.

De volgende stelling geeft ons meer controle over de rationale getallen.

**Stelling 2.26. Eenduidigheid van rationale getallen**

Elk rationaal getal kan op een unieke manier geschreven worden als  $\frac{a}{b}$  met  $a \in \mathbb{Z}$  en  $b \in \mathbb{N}^+$  zo dat  $\text{ggd}(a, b) = 1$ .

Zo'n breuk noemen we onvereenvoudigbaar, aangezien ze niet verder kan worden vereenvoudigd.

**Opgave 2.27.** Bewijs Stelling 2.26.

Een typische toepassing van deze stelling is:

**Opgave 2.28.** Zij  $n \in \mathbb{N}$  geen volkomen kwadraat. Bewijs dat  $\sqrt{n}$  irrationaal is.

**Opgave 2.29.** Zij  $p$  een priemgetal. Bewijs dat voor natuurlijke getallen  $n \in \mathbb{N}^+$  geldt dat  $\log_p(n) \in \mathbb{Q}$  als en slechts als  $n$  een macht van  $p$  is.

**Opgave 2.30.** Bepaal van de volgende getallen of ze rationaal zijn:

- A.  $\sqrt{5}/\sqrt[3]{15}$
- B.  $\sqrt{3} + \sqrt{5}$
- C.  $\sqrt{2} + \sqrt{8} - \sqrt{18}$

## 2.3 Aritmetische functies

Een aritmetische functie is, in zijn algemeenste definitie, een functie van  $\mathbb{N}^+$  naar  $\mathbb{C}$ . We bekijken enkele typische voorbeelden.

### 2.3.1 Aantal delers

**Opgave 2.31.** Bepaal het aantal positieve delers van

- A.  $2^{10}$ .
- B.  $3^{10}$ .
- C.  $2 \cdot 3 \cdot 5 \cdot 7$ .

A

---

<sup>8</sup>We formuleren dit bewust als eigenschap. Aan een strenge definitie van rationale getallen wagen we ons hier niet.

- D.  $4 \cdot 3 \cdot 5$ .
- E.  $4 \cdot 9 \cdot 25$ .

**Stelling 2.32.**

Als  $n$  een natuurlijk getal is met priemontbinding  $p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ , dan is het aantal positieve delers  $\tau(n)$  van  $n$  gelijk aan

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_r + 1).$$

**Opgave 2.33.** Toon de formule voor  $\tau(n)$  aan.

**Opgave 2.34.** Welke natuurlijke getallen hebben precies 101 positieve delers? A

**Opgave 2.35.** Toon aan dat een natuurlijk getal groter dan 0 een oneven aantal delers heeft als en slechts als dat getal een volkomen kwadraat is.

### 2.3.2 Som van delers

**Opgave 2.36.** Bepaal de som van de positieve delers van A

- A.  $2^5$ .
- B.  $3^5$ .
- C.  $2 \cdot 3 \cdot 5$ .
- D.  $4 \cdot 3 \cdot 5$ .
- E.  $4 \cdot 9 \cdot 25$ .

**Stelling 2.37.**

Als  $n$  een natuurlijk getal is met priemontbinding  $p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ , dan is de som  $\sigma(n)$  van de positieve delers van  $n$  gelijk aan

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{a_r+1} - 1}{p_r - 1}$$

of dus

$$(1 + p_1 + p_1^2 + \cdots + p_1^{a_1})(1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdots (1 + p_r + p_r^2 + \cdots + p_r^{a_r}).$$

**Opgave 2.38.** Toon de formule voor  $\sigma(n)$  aan.

**Opgave 2.39.** Welke natuurlijke getallen hebben 31 als som van hun positieve delers?

**Opgave 2.40.** Zij  $n > 1$  een oneven natuurlijk getal. Toon aan dat som van de positieve delers van  $n$  oneven is als en slechts als  $n$  een volkomen kwadraat is.

### 2.3.3 Totiëntfunctie

#### Definitie 2.41. Totiënt

De totiënt (ook wel: *indicator*) van een natuurlijk getal  $n \in \mathbb{N}^+$  is het aantal natuurlijke getallen in de verzameling  $\{1, \dots, n\}$  die relatief priem zijn met  $n$ . We noteren  $\varphi(n)$ . De functie  $\varphi$  wordt ook de Euler totiënt functie of kortweg phi functie genoemd.

**Opgave 2.42.** Bepaal de totiënt van

A

- A.  $2^5$ .
- B.  $3^5$ .
- C.  $pq$  met  $p$  en  $q$  verschillende priemgetallen.
- D.  $p^2q$ .
- E.  $p, q, r$  met ook  $r$  priem.
- F.  $p^m q^n$  met  $m, n \geq 1$ .

Analoog aan  $\tau$  en  $\sigma$  hebben we een expliciete formule voor  $\varphi$ .

#### Stelling 2.43.

Als  $n > 1$  en  $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_r^{a_r}$ , dan is

$$\varphi(n) = (p_1 - 1)p_1^{a_1 - 1} \cdot (p_2 - 1)p_2^{a_2 - 1} \cdot \dots \cdot (p_r - 1)p_r^{a_r - 1}.$$

Een intuïtief argument voor deze formule gaat als volgt: als  $p$  een priemdelers van  $n$  is, is de 'kans' dat een getal in  $\mathbb{N}_{\leq n}^+$  deelbaar is door  $p$  gelijk aan  $\frac{1}{p}$ . De kans dat een dergelijk getal niet deelbaar is door  $p$  is  $1 - \frac{1}{p}$ . Om rekening te houden met alle priemgetallen, moeten we deze kansen vermenigvuldigen (hier zit de onzuiverheid in het bewijs) zodat

$$\varphi(n) = n \cdot \prod_{p|n} \frac{p-1}{p},$$

dit is de voorspelde formule. In Hoofdstuk 7 zal de Chinese reststelling toelaten om dit bewijs te formaliseren, weliswaar zonder het begrip 'kans'.

We kunnen deze redenering nu wel al ombuigen tot een bewijs met het inclusie-exclusieprincipe (Stelling B.4).

*Bewijs.*

Noteer voor een priemdelers  $p$  van  $n$ ,  $A_p$  als de verzameling van getallen in  $\mathbb{N}_{\leq n}^+$  die deelbaar zijn door  $p$ . Dus  $\varphi(n) = n - \left| \bigcup_{p|n} A_p \right|$ . Voor verschillende priemgetallen  $p_1, \dots, p_k$  geldt, aangezien  $\text{kgv}(p_1, \dots, p_k) = p_1 \cdot \dots \cdot p_k$ , dat  $\left| \bigcap_{l=1}^k A_{p_l} \right| = \frac{n}{p_1 \cdot \dots \cdot p_k}$ . Zij nu  $p_1, \dots, p_k$  de verschillende priemdelers van  $n$ . Het inclusie-exclusieprincipe zegt dat

$$n - \left| \bigcup_{p|n} A_p \right| = n - \sum_{l=1}^k (-1)^{l+1} \sum_{\substack{S \subseteq \mathbb{N}_{\leq k}^+ \\ |S|=l}} \frac{n}{\prod_{j \in S} p_j}$$

wat kan worden ontbonden als

$$\varphi(n) = n \cdot \prod_{j=1}^k \left(1 - \frac{1}{p_j}\right).$$

□

**Opgave 2.44.** Toon aan dat  $\varphi(n)$  even is voor  $n > 2$ .

**Opgave 2.45.** Bepaal alle natuurlijke getallen  $a$  zo dat  $\varphi(a) = 8$ .

**Opgave 2.46.** Bepaal alle natuurlijke getallen  $n$  zo dat  $\varphi(\varphi(\varphi(n)))$  een priemgetal is. H

Zoals je misschien hebt gemerkt zijn de bewijzen van de formules voor  $\tau$ ,  $\sigma$  en  $\varphi$  heel sterk combinatorisch. Er bestaat een techniek, *Dirichlet convolutie*, die toelaat om minder combinatorische (maar ook minder intuïtieve) bewijzen te geven, die misschien wel rigoureuzer lijken.

### 2.3.4 Multiplicatieve functies

Een bijzondere klasse van aritmetische functies vormen de *multiplicatieve* en *additieve* functies.

#### Definitie 2.47. Multiplicativiteit

Een functie  $f : \mathbb{N}^+ \rightarrow \mathbb{C}$  noemt men *multiplicatief* als  $f(ab) = f(a) \cdot f(b)$  voor alle coprieme  $a, b \in \mathbb{N}^+$ , en als  $f(1) \neq 0$ .<sup>9</sup> Indien de gelijkheid geldt voor alle keuzes van  $a$  en  $b$  noemen we  $f$  *totaal multiplicatief*.

Minder belangrijk, maar een even handig begrip is:

#### Definitie 2.48. Additiviteit

We noemen  $f$  *additief* als  $f(a + b) = f(a) + f(b)$  voor alle coprieme  $a, b \in \mathbb{N}^+$  en *totaal additief* als dit geldt voor alle  $a, b$ .

In wat volgt bekijken we enkel de multiplicatieve functies in detail.

**Opgave 2.49.** Als  $f$  een multiplicatieve functie is, wat zijn dan de mogelijke waarden voor  $f(1)$ ?

**Opgave 2.50.** Toon aan dat alle waarden van een multiplicatieve functie  $f$  gekend zijn, van zodra we  $f(n)$  kennen voor alle machten van priemgetallen.

Dit principe houdt onder andere in dat twee multiplicatieve functies gelijk zijn zodra ze gelijk zijn voor machten van priemgetallen.

<sup>9</sup>De voorwaarde  $f(1) \neq 0$  drukt uit dat  $f(n)$  niet voor alle  $n$  nul is. Soms wordt ze weggelaten in de definitie.

**Stelling 2.51.**

$\tau$ ,  $\sigma$  en  $\varphi$  zijn multiplicatief, maar niet totaal multiplicatief.

*Bewijs.*

Dit volgt onmiddellijk uit de expliciete formule: Als  $m = p_1^{a_1} \cdots p_r^{a_r}$  en  $n = q_1^{b_1} \cdots q_s^{b_s}$  met alle  $p_k, q_l$  verschillend, dan is

$$\tau(mn) = \prod_{k=1}^r (a_k + 1) \prod_{k=1}^s (b_k + 1) = \tau(m)\tau(n).$$

Een analoge redenering geldt voor  $\sigma$  en  $\varphi$ . Dat ze niet totaal multiplicatief zijn zien we bijvoorbeeld aan  $\tau(4) \neq \tau(2)^2$ ,  $\sigma(4) \neq \sigma(2)^2$  en  $\varphi(4) \neq \varphi(2)^2$ .  $\square$

## Opgaven hoofdstuk 2

**Opgave 2.52.** Toon aan dat er oneindig veel natuurlijke getallen bestaan die niet kunnen worden geschreven in de vorm  $n^2 + p$  met  $p$  een priemgetal. H

**Opgave 2.53.** Zij  $S = \{1\} \cup 2\mathbb{N}$ , de verzameling die bestaat uit 1 en de positieve veelvouden van 2. We noemen een element van  $S$  een *priemgetal (van  $S$ )* als het precies 2 (positive) delers in  $S$  heeft. Voorbeelden zijn 2 en 6. A

- Bewijs dat elk element van  $S$  een ontbinding heeft in priemgetallen van  $S$ .
- Bepaal alle priemgetallen van  $S$ .
- Geef een voorbeeld van een getal met twee verschillende priemontbindingen.
- Als  $a, b \in S$ , bestaan dan  $q, r \in S \cup \{0\}$  met  $b = qa + r$  en  $r < b$ ?
- Als  $p, a, b \in S$  met  $p$  priem en  $p \mid ab$ , is dan noodzakelijk  $p \mid a$  of  $p \mid b$ ?

**Opgave 2.54.** Vind alle priemgetallen  $p, q$  en  $r$  zo dat  $p \mid q - r$  en  $p \mid q + r$ .

**Opgave 2.55.** (CanMO 1978 vraag 2) Vind alle koppels  $(a, b)$  van natuurlijke getallen die voldoen aan  $2a^2 = 3b^3$ . H

**Opgave 2.56.** (IrMO 2007 dag 1 vraag 1) Vind alle koppels priemgetallen  $(p, q)$  zo dat  $p \mid q + 6$  en  $q \mid p + 7$ .

**Opgave 2.57.** (NWO 2007 vraag 4) Voor hoeveel natuurlijke getallen  $1 \leq n \leq 100$  is  $n^n$  een volkomen kwadraat?

**Opgave 2.58.** (IrMO 2007 dag 2 vraag 4) Vind het aantal nullen op het einde van  $2007!$ , en vind ook het laatste cijfer dat niet 0 is.

**Opgave 2.59.** Definieer voor elk natuurlijk getal  $n$  het getal  $p(n)$  als de grootste oneven deler van  $n$ . Bewijs dat H

$$\frac{1}{2^k} \cdot \sum_{n=1}^{2^k} \frac{p(n)}{n} > \frac{2}{3}.$$

**Opgave 2.60.** (USAMO 1972 vraag 1) Toon aan dat voor natuurlijke getallen  $a$ ,  $b$  en  $c$  geldt dat

$$\text{ggd}(a, b, c)^2 \cdot \text{kgv}(a, b) \cdot \text{kgv}(b, c) \cdot \text{kgv}(c, a) = \text{kgv}(a, b, c)^2 \cdot \text{ggd}(a, b) \cdot \text{ggd}(b, c) \cdot \text{ggd}(c, a).$$

**Opgave 2.61.** (BaMO 1989 vraag 1) Vind alle natuurlijke getallen die de som zijn van de kwadraten van hun vier kleinste positieve delers. H

**Opgave 2.62.** Zij  $a \in \mathbb{N}$  geen kwadraat. Bewijs dat de vergelijking  $n! + a = b^2$  een eindig aantal oplossingen  $(n, b)$  heeft.

**Vermoeden 2.63.** Probleem van Brocard

De enige oplossingen  $(n, b)$  van  $n! + 1 = b^2$  zijn  $(4, 5)$ ,  $(5, 11)$  en  $(7, 71)$ .

**Opgave 2.64.** Toon aan dat het product van de positieve delers van een natuurlijk getal  $n$  gelijk is aan  $n^{\frac{\tau(n)}{2}}$ . H

**Opgave 2.65.** Stel  $n > 0$ . Toon aan dat het aantal koppels natuurlijke getallen  $(x, y)$  dat voldoet aan  $\text{kgv}(x, y) = n$  gelijk is aan  $\tau(n^2)$ . H

**Opgave 2.66.** Toon aan dat voor natuurlijke getallen  $p$  en  $k$  met  $p$  priem geldt dat H

$$\text{ggd}(\sigma(p^k), \sigma(p^{2k})) = 1.$$

**Opgave 2.67.** Vind alle natuurlijke getallen  $n > 1$  waarvoor  $\varphi(n) \mid n$ . H

**Opgave 2.68.** Vind alle natuurlijke getallen  $n > 1$  waarvoor  $\varphi(\varphi(n)) \mid n$ . H

**Opgave 2.69.** (IMOSL 2004 vraag 9) Bewijs dat er oneindig veel natuurlijke getallen  $a$  bestaan zo dat de vergelijking  $\tau(an) = n$  geen natuurlijk getal  $n$  als oplossing heeft.

*Er zijn 10 soorten mensen op aarde. Zij die binair kennen en zij die geen binair kennen.*

We maken even formeel wat we bedoelen met uitdrukkingen als “11” en “3.14”. Voor algemene reële getallen ligt de zaak iets moeilijker, maar die spelen dan ook geen grote rol in de hoofdstukken die volgen.

Een getalstelsel of talstelsel is informeel gezegd een manier om getallen voor te stellen. Men zou bijvoorbeeld voor elk getal een nieuw symbool kunnen bedenken. Bijvoorbeeld 0 voor nul, 1 voor een, 2 voor twee, ..., 9 voor negen, ★ voor tien, □ voor elf, ⊗ voor twaalf en ga maar door. Dit blijkt echter niet zo’n efficiënte methode te zijn: zelf bij de meest creatieve geesten raakt de inspiratie voor het bedenken van nieuwe symbolen al gauw op. Iedereen weet wel beter, we schrijven gewoon twee symbolen naast elkaar van zodra onze voorraad is uitgeput. In plaats van steeds te werken met de tien symbolen 0, 1, ..., 9 kunnen we met elk natuurlijk aantal (groter dan één) symbolen werken.

Een talstelsel wordt bepaald door een natuurlijk getal  $b > 1$ , de basis. Een voorbeeld is het decimale talstelsel met basis tien. Een getal wordt voorgesteld door een eindige sequentie cijfers of symbolen, waarbij er keuze is tussen  $b$  symbolen. De  $b$  cijfers of symbolen hebben waarden 0, 1, ...,  $b - 1$ . Als we een natuurlijk getal  $n$  voorstellen in basis  $b$  als  $a_m a_{m-1} \cdots a_0$ , waarbij  $a_0, \dots, a_m$  symbolen zijn (al dan niet verschillend), betekent dit dat

$$n = \sum_{k=0}^m a_k \cdot b^k.$$

We stellen de waarde van een symbool dus gelijk aan de waarde die het voorstelt (van tautologie gesproken!). De voorwaarde is wel dat  $a_m \neq 0$  als  $n \neq 0$ , m.a.w. we schrijven nooit een 0 als eerste symbool, tenzij voor het voorstellen van 0. Om duidelijk te maken dat  $n$  in basis  $b$  staat geschreven, noteert men vaak  $(a_m a_{m-1} \cdots a_0)_b$ . Om dit niet te verwarren met het product  $a_m \cdot a_{m-1} \cdots a_0$  schrijft men ook wel  $\overline{a_m a_{m-1} \cdots a_0}_b$ .

Veel gebruikte basissen zijn twee, zestien en uiteraard tien. Het talstelsel met basis twee noemt men ook wel binair, en de symbolen die worden gebruikt zijn gewoon 0 en 1. Het talstelsel met basis zestien noemt men het hexadecimale, en meestal gebruikt men de cijfers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 en de hoofdletters A, B, C, D en E als symbolen.

Bijvoorbeeld,  $135_{10} = 10000111_2 = 12000_3$  en  $C5_{16} = 197_{10}$ . Als de basis niet wordt gegeven als index veronderstelt men dat de basis tien is, tenzij de context een andere basis suggereert. Gewoonlijk wordt de index ook in basis tien genoteerd, zoals we hier deden.<sup>10</sup>

**Opgave 3.1.** Tien heeft de eigenschap dat, wanneer je het schrijft in zijn eigen basis, er een 1 A en een 0 staat. Wat maakt tien zo speciaal?

**Opgave 3.2.** Bewijs dat  $(a_m \cdots a_0)_b < b^{m+1}$  voor alle  $b > 1$ .

De volgende stelling is wel het minste dat je kan verwachten. Ze houdt bijvoorbeeld in dat  $10 \neq 11$ .

<sup>10</sup>En dus niet  $C5_{16_{10}}$  of  $C5_{16_{10_{10}}}$  ... Je moet ergens een keuze maken!



**Stelling 3.3.**

Elk natuurlijk getal kan op een unieke manier worden geschreven in basis  $b$ , als  $b > 1$ .

**Opgave 3.4.** Bewijs.

Het bewijs bestaat uit twee delen. Bewijzen dat er steeds voorstelling bestaat, en bewijzen dat die uniek is. Eerst tonen we, via inductie, aan dat er steeds minstens één manier is.

Basisstap. Voor  $n = 0$  is er duidelijk zo'n manier, namelijk gewoon  $(0)_b$ .

Inductiestap. Veronderstel nu dat het klopt voor alle getallen kleiner dan  $n$ . Noem  $q$  het quotiënt en  $a_0$  de rest van  $n$  bij deling door  $b$ .

A. Toon aan dat  $q < n$ .

Stel dus  $q = (a'_m \cdots a'_0)_b$ .

B. Toon aan dat  $n = (a'_m \cdots a'_0 a_0)_b$ .

Dus  $n$  heeft een voorstelling.

Veronderstel nu dat een natuurlijk getal  $n$  op twee manieren kan worden geschreven in basis  $b$ , zeg  $n = (a_x \cdots a_0)_b = (a'_y \cdots a'_0)_b$ . Dan is er een kleinste getal  $k$  zo dat  $a_k \neq a'_k$ , ofwel is  $x \neq y$  omdat het aantal symbolen verschilt. Stel eerst dat  $a_k > a'_k$ .

C. Bewijs dat  $(a_x \cdots a_0)$  en  $(a'_y \cdots a'_0)_b$  een verschillende rest hebben bij deling door  $b^{k+1}$ , en dus onmogelijk gelijk kunnen zijn.

D. Bewijs dat  $x \neq y$  ook niet mogelijk is.

Bijgevolg is de representatie uniek.

**3.1 Expansies van niet-gehele getallen**

De vraag rijst of we elk reëel getal in elk talstelsel kunnen voorstellen, en of die schrijfwijze uniek is. Om duidelijk te stellen wat we hiermee bedoelen is het noodzakelijk om precies vast te leggen wat het betekent om een niet-geheel getal voorstellen in een basis (zeg  $b$ ).

**Definitie 3.5.**

Zij  $b > 1$  een natuurlijk getal,  $n, m \in \mathbb{N}$  en  $a_n, \dots, a_0, a_{-1}, \dots, a_{-m} \in \{0, \dots, b-1\}$ . We noteren

$$\begin{aligned} (a_n a_{n-1} \dots a_0 . a_{-1} \dots a_{-m})_b &= a_n b^n + a_{n-1} b^{n-1} + \dots + a_0 + a_{-1} b^{-1} + \dots + a_{-m} b^{-m} \\ &= \sum_{k=-m}^n a_k b^k. \end{aligned}$$

Met deze notatie is bijvoorbeeld  $\frac{17}{8} = 2.125_{10} = 2.1_8 = 2.02_4 = 10.001_2$ .

Met deze notatie kunnen we uiteraard enkel rationale getallen voorstellen. Er zijn dus getallen (zoals  $\sqrt{2}$ ) die we op deze manier in geen enkele basis kunnen voorstellen. Om hieraan te verhelpen laten we oneindig lange uitdrukkingen toe:

**Definitie 3.6.**

Zij  $b > 1$  een natuurlijk getal,  $n \in \mathbb{N}$  en  $a_n, a_{n-1}, \dots, a_0, a_{-1}, a_{-2} \dots \in \{0, \dots, b-1\}$ . We noteren

$$\begin{aligned} (a_n a_{n-1} \dots a_0 . a_{-1} a_{-2} \dots)_b &= a_n b^n + a_{n-1} b^{n-1} + \dots + a_0 + a_{-1} b^{-1} + a_{-2} b^{-2} + \dots \\ &= \sum_{k=-\infty}^n a_k b^k. \end{aligned}$$

Kunnen we hiermee nu elk reëel getal voorstellen in elke basis  $b > 2$ ? Uiteraard niet; om te beginnen moeten we toelaten een minteken voor de uitdrukking te plaatsen... Maar wat als we dat toelaten?

**Stelling 3.7.**

Zij  $x \in \mathbb{R}$  en  $b \in \mathbb{N}$ ,  $b > 1$ . Dan bestaan  $n \in \mathbb{Z}$ ,  $a_n, a_{n-1}, \dots, a_0, a_{-1}, a_{-2} \dots \in \{0, \dots, b-1\}$  en  $s \in \{-1, 1\}$  waarvoor  $x = s \cdot \sum_{k=-\infty}^n a_k b^k$ .

**Opgave 3.8.** Bewijs.

Stel eerst dat  $x \geq 0$ . We construeren  $a_n, a_{n-1}, \dots$ . Noem  $n$  het grootste geheel getal waarvoor  $b^n < x$  en stel  $a_n = \lfloor \frac{x}{b^n} \rfloor$ .

A. Toon aan dat  $a_n \in \{0, \dots, b-1\}$ .

B. Toon aan dat  $0 \leq x - a_n b^n < b^n$ .

Veronderstel nu dat  $a_n, \dots, a_k$  bepaald zijn en dat  $0 \leq x - (a_n b^n + \dots + a_k b^k) < b^k$ . We construeren  $a_{k-1}$  en tonen met het oog op inductie aan dat een analoge eigenschap blijft gelden. Stel dus  $a_{k-1} = \lfloor \frac{x - a_n b^n - \dots - a_k b^k}{b^{k-1}} \rfloor$

C. Toon aan dat  $a_{k-1} \in \{0, \dots, b-1\}$  en dat  $0 \leq x - (a_n b^n + \dots + a_{k-1} b^{k-1}) < b^{k-1}$ .

Aldus construeren we recursief  $a_n, a_{n-1}, \dots$

D. Toon aan dat  $x = \sum_{k=-\infty}^n a_k b^k$ .

E. Toon ten slotte aan dat de stelling ook geldt voor  $x \leq 0$ .

De enige onbeantwoorde vraag is uniciteit. Deze is alles behalve gegarandeerd. om te beginnen kunnen we vooraan de uitdrukking naar believen nullen toevoegen:  $003.4_5 = 0000003.4_5$ . Indien de uitdrukking eindig is kunnen we ook achteraan nullen toevoegen:  $3_4 = 003.000_4$ . Is dit alles? Nee: aangezien  $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots = 1$  hebben we bijvoorbeeld

$$0.111\dots_2 = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots = 1_2.$$

Ook is  $2.3999\dots_{10} = 2.4_{10}$ .

**Opgave 3.9.** Zij  $b \in \mathbb{N}$ ,  $b > 1$ . Als  $x \in \mathbb{R}$  een oneindige representatie in basis  $b$  heeft die vanaf een bepaald punt enkel uit symbool  $b-1$  bestaat, toon dan aan dat  $x$  ook een eindige representatie heeft.

Wel blijkt dat dit de enige problemen zijn die kunnen optreden: ofwel voegen we vooraan of achteraan nullen toe, ofwel eindigt de representatie met een oneindige herhaling van het symbool  $b-1$ :

**Stelling 3.10.**

Zij  $x \in \mathbb{R}$ ,  $x \neq 0$  en  $b \in \mathbb{N}$ ,  $b > 1$ . Dan kan  $x$  op unieke wijze worden voorgesteld als

$$x = s \cdot \sum_{k=-\infty}^n a_k b^k$$

met  $s \in \{-1, 1\}$ , alle  $a_k \in \{0, \dots, b-1\}$  en  $n \in \mathbb{Z}$ , waarbij  $a_n \neq 0$  en er willekeurig kleine  $k$  zijn waarvoor  $a_k \neq b-1$ .

Merk op dat het achteraan toevoegen van nullen wordt opgeslorpt in het feit dat we enkel oneindige representaties beschouwen, en dat we rekening houden met het vooraan toevoegen van nullen door te eisen dat  $a_n \neq 0$ .

**Opgave 3.11.** Bewijs.

H

A. Toon aan dat  $x$  minstens één zo'n representatie heeft.

Beschouw nu twee representaties van  $x$ .

B. Toon aan dat deze noodzakelijk gelijk zijn.

De unieke representatie uit de vorige stelling zullen we vanaf nu benoemen met de *representatie van  $x$  in basis  $b$* . We veralremenen tot slot enkele eerdere notaties:

**Notatie 3.12.**

Zij  $x \in \mathbb{R}$ ,  $x > 0$  en  $x = \sum_{k=-\infty}^n a_k b^k$  de representatie van  $x$  in basis  $b \in \mathbb{N}$ ,  $b > 1$ . We noteren

$$\begin{cases} x = (a_n \dots a_0 . a_{-1} \dots)_b & \text{als } n \geq 0 \\ x = (0.0 \dots 0 a_n a_{n-1} \dots)_b & \text{als } n < 0. \end{cases}$$

Dit soort oneindige representaties lijkt op het eerste zicht misschien omslachtig om iets mee aan te vangen. Het interessante eraan is dat de rationale getallen zeer herkenbare representaties hebben. We bekijken enkele voorbeelden.

**Voorbeeld 3.13.** Bepaal de decimale ontwikkeling van  $\frac{1}{3}$ .

*Oplossing.*

We gaan te werk zoals in het bewijs van Stelling 3.7: het grootste geheel getal  $n$  waarvoor  $10^n < \frac{1}{3}$  is  $-1$ . Stel dus  $a_{-1} = \left\lfloor \frac{\frac{1}{3}}{10^{-1}} \right\rfloor = \left\lfloor \frac{10}{3} \right\rfloor = 3$ . Wat overblijft is  $\frac{1}{3} - 3 \cdot 10^{-1} = \frac{1}{30}$ . We stellen nu  $a_{-2} = \left\lfloor \frac{\frac{1}{30}}{10^{-2}} \right\rfloor = 3$ . Wat overblijft is  $\frac{1}{30} - 3 \cdot 10^{-2} = \frac{1}{300}$ . Het is niet moeilijk om in te zien dat die uiteindelijk leidt tot  $a_k = 3$  voor alle  $k < 0$ . Dus  $\frac{1}{3} = 0.33 \dots_{10}$ .

**Notatie 3.14.**

We noteren  $(a_n \dots a_0.a_{-1} \dots \overline{a_k \dots a_{k-p+1}})_b$  indien  $a_{n-p} = a_n$  voor alle  $n \leq k$ .

Zo is bijvoorbeeld  $\frac{1}{3} = 0.\overline{3}$ , maar ook  $\frac{1}{3} = 0.33\overline{33}$ . Het spreekt voor zich dat we de voorkeur geven aan een zo kort mogelijk notatie; hier dus  $0.\overline{3}$ .

**Voorbeeld 3.15.** Stel  $x = 0.\overline{25}$ . Toon aan dat  $x$  rationaal is en bepaal  $a, b \in \mathbb{Z}$  waarvoor  $x = \frac{a}{b}$ .

*Oplissing.*


In reekssomnotatie is  $x = \sum_{k=-\infty}^{-1} (5 \cdot 10^{2k} + 2 \cdot 10^{2k+1})$ . Hieruit volgt dat  $100x = \sum_{k=-\infty}^{-1} (5 \cdot 10^{2(k+1)} + 2 \cdot 10^{2(k+1)+1}) = 25 + \sum_{k=-\infty}^{-2} (5 \cdot 10^{2(k+1)} + 2 \cdot 10^{2(k+1)+1}) = x + 25$ . Dus  $99x = 25$ , zodat  $x = \frac{25}{99} \in \mathbb{Q}$ .


**Stelling 3.16.**

Zij  $x \in \mathbb{R}$ ,  $x > 0$  en  $b \in \mathbb{N}$ ,  $b > 1$ . Zij  $x = \sum_{k=-\infty}^n a_k b^k$  de representatie van  $x$  in basis  $b$ . Dan is  $x \in \mathbb{Q}$  als en slechts als  $K \in \mathbb{Z}$  en  $p \in \mathbb{N}^+$  bestaan met de eigenschap dat  $a_{k-p} = a_k$  voor alle  $k < K$ , m.a.w. de representatie van  $x$  is *uiteindelijk periodiek* met periode (hoogstens)  $p$ .

**Opgaven hoofdstuk 3**

**Opgave 3.17.** Bepaal de mogelijke basissen  $a > 8$  als  $(35_a + 24_a) \cdot 20_a = 1081_a$ .

**Opgave 3.18.** (IMC 2014 dag 2 vraag 1) Noteer voor  $x \in \mathbb{N}^+$  en  $n \in \mathbb{N}$  met  $d_n(x)$  het  $n$ -de getal in de decimale ontwikkeling van  $x$ , i.e.  $d_n(x) \in \{0, \dots, 9\}$  en  $x = \sum_{n=1}^{\infty} d_n(x) 10^{n-1}$ . Veronderstel dat er voor een bepaalde natuurlijke rij  $(a_n)$  slechts eindig veel nullen voorkomen in de rij  $(d(a_n))$ . Bewijs dat er oneindig veel natuurlijke getallen niet voorkomen in de rij  $(a_n)$ . 

**Opgave 3.19.** Bestaat er een irrationaal getal  $x$  en een gehele rij  $(a_n)$  waarvoor 

$$\lim_{n \rightarrow \infty} |a_n - n! \cdot x| = 0 ?$$

# Ad-hocmethodes voor diophantische vergelijkingen

*In het rijk van de geest is een methode te vergelijken met een kruk.  
De ware denker loopt vrij.*

*(Godfried Bomans)*

## 4.1 Ontbinden

Ontbinden is het omzetten van een som naar een product. Het is een handige techniek om Diophantische vergelijkingen op te lossen. Het voordeel van de notatie als product is dat de factoren een getal opdelen in delers, en zoals je ondertussen wel weet draait het in de getaltheorie allemaal om delers. Voorbeelden van ontbindingen zijn  $(a^2 - b^2) = (a - b)(a + b)$  en  $ab + a + b + 1 = (a + 1)(b + 1)$ .

In de appendix achteraan vind je het binomium van Newton en nog enkele ontbindingen. Soms zal je echter oefeningen tegenkomen waarbij de ontbinding niet voor de hand ligt, en waar je misschien niet op het idee zal komen om te ontbinden. Het is echter aan te raden om toch steeds te proberen, want zoals je in de volgende oefening zal merken zijn er nogal wat ontbindingen die niet vanzelfsprekend zijn.

**Opgave 4.1.** Ontbind in factoren.

- A.  $ab - a - b + 1$
- B.  $3m + 4n - 2mn - 6$
- C.  $y + x^2 + xy + y^2 + x^3 + x^2y$
- D.  $a^4 + 4b^4$
- E.  $a^3 + b^3 + c^3 - 3abc$

**Opgave 4.2.** Vind alle priemgetallen  $p$  zo dat  $p + 1$  een volkomen kwadraat is.

H

**Opgave 4.3.** Vind alle gehele getallen  $a$  en  $b$  zo dat  $ab = a + b$ .

H

**Definitie 4.4.** Mersennepriemgetal

Een priemgetal van de vorm  $2^n - 1$  noemen we een Mersennepriemgetal.

**Opgave 4.5.** Stel dat  $2^n - 1$  een priemgetal is. Toon aan dat  $n$  een priemgetal is.

H

**Definitie 4.6.** Fermat-priemgetal

Een priemgetal van de vorm  $2^m + 1$  noemen we een Fermat-priemgetal.

**Opgave 4.7.** Stel dat  $2^m + 1$  een priemgetal is. Toon aan dat  $m$  een macht van 2 is.

H

## 4.2 Ongelijkheden

Ongelijkheden kunnen voorkomen op verschillende manieren. Een eerste toepassing is het uitsluiten van deelbaarheid. Als  $a, b \in \mathbb{N}^+$  zo dat  $a \mid b$ , dan geldt dat  $a \leq b$ . Dus als je twee getallen  $x, y > 0$  hebt zodanig dat  $x > y$ , is het onmogelijk dat  $x \mid y$ .

**Voorbeeld 4.8.** Vind alle natuurlijke getallen  $n$  zo dat  $2^{n+1}$  deelbaar is door  $5^n + 1$ .

*Oplossing.*

Voor  $n = 0$  hebben we  $5^n + 1 \mid 2^{n+1}$ , want  $2 \mid 2$ .

Stel nu  $n \geq 1$ . Dan is  $5^n + 1 > 5^n > 4^n = 2^{2n} \geq 2^{n+1}$ . Dan kan  $5^n + 1$  dus geen deler zijn van  $2^{n+1}$ . De enige oplossing is  $n = 0$ .

*Opmerking.*

We hebben hier de ‘ketting’ van ongelijkheden  $5^n + 1 > 5^n > 4^n = 2^{2n} \geq 2^{n+1}$  gebruikt. Er zijn natuurlijk nog andere mogelijkheden. Je had het bijvoorbeeld ook kunnen bewijzen met

$$5^{n+1} + 1 > 5^n = 5 \cdot 5^{n-1} > 4 \cdot 5^{n-1} \geq 4 \cdot 2^{n-1} = 2^{n+1}.$$

Dat maakt dus niet uit. Het belangrijkste is dat je heel strikt bewijst dat het ene groter is dan het andere, en dat elk stapje in de keten duidelijk is. Maak vooral dat je er niet slordig overgaat zonder de ongelijkheid nauwkeurig aan te tonen. En in het geval dat alle tekens die je in de ketting plaatst groter-of-gelijk-aan tekens zijn, moet je nog bewijzen dat gelijkheid onmogelijk is, of, nagaan wanneer dat wel nog mogelijk is. Als je er dan nog niet uit geraakt, kan je misschien beter een andere ketting vormen, of eventueel een extra waarde van  $n$  apart nagaan zodat je meer kan doen met de ongelijkheid. Bijvoorbeeld,  $5^n > 4^n$  is niet waar voor  $n = 0$ , maar wel voor  $n \geq 1$ . We zijn dus eerst het geval  $n = 0$  nagegaan zodat we  $n \geq 1$  konden stellen. Dat is wat heel vaak zal voorkomen als je ongelijkheden gebruikt: eerst een voorwaarde stellen en dan pas verder doen. Vergeet dan niet om de overige gevallen af te gaan.

**Opgave 4.9.** Vind alle natuurlijke getallen  $n$  waarvoor  $2^n + 1 \mid 2n + 1$ .

**Opgave 4.10.** Vind alle natuurlijke getallen  $m$  waarvoor  $7^n \mid 9^n - 1$ .

Het kan ook gebeuren dat een Diophantische vergelijking geen oplossingen heeft omdat het ene lid steeds groter is dan het andere, mits te voldoen aan bepaalde voorwaarden. Het volstaat dan van de ongelijkheid te bewijzen om aan te tonen dat er geen oplossingen zijn. Immers, twee getallen waarvan het ene groter is dan het andere, kunnen onmogelijk gelijk zijn.

**Voorbeeld 4.11.** Vind alle natuurlijke getallen  $a$ ,  $b$  en  $c$  zo dat  $a! + b! = c!$ .



*Oplossing.*

Als  $a, b < 2$  zijn er slechts enkele mogelijkheden na te gaan, en we krijgen de oplossingen  $(0, 0, 2)$ ,  $(0, 1, 2)$ ,  $(1, 0, 2)$  en  $(1, 1, 2)$  voor  $(a, b, c)$ . Stel nu dat  $a, b > 1$ . We kunnen veronderstellen dat  $a \leq b$ , aangezien het wisselen van  $a$  en  $b$  ook een oplossing geeft. Als we nu oplossingen vinden, moeten we er achteraf wel rekening mee houden dat we  $a$  en  $b$  mogen wisselen.

Omdat  $c! = a! + b!$  is  $c$  groter dan  $b$ . Dan is

$$c! \geq (b+1)! = (b+1) \cdot b! > (1+1) \cdot b! \geq a! + b!,$$

dus is het onmogelijk dat  $a! + b! = c!$  omdat  $c!$  steeds groter is. De enige oplossingen zijn dus die oplossingen die eerder al waren vermeld.

*Opmerking.*

Bij de ketting van ongelijkheden hadden we nog juist één groter-dan teken. Gelukkig maar, anders konden we niet besluiten dat  $c!$  steeds groter is.

**Opgave 4.12.** Vind alle natuurlijke getallen  $n$  zo dat  $n + 1 = 2^n$ .

**Opgave 4.13.** (CanMO 1983 vraag 1) Vind alle natuurlijke getallen  $w, x, y, z$  die voldoen aan  $w! = x! + y! + z!$ .

**Opgave 4.14.** Vind alle natuurlijke getallen  $a, b$  en  $c$  zo dat  $a^a + b^b = c^c$ .

**Opgave 4.15.** (JBaMO 2010 vraag 2) Vind alle natuurlijke getallen  $n \geq 1$  zo dat  $n \cdot 2^{n+1} + 1$  een kwadraat is.

Ongelijkheden kunnen ook gebruikt worden om te bewijzen dat een getal geen volkomen kwadraat is. Hierbij steunen we op het principe dat er nooit een geheel getal  $x$  bestaat zo dat  $a^2 < x^2 < (a+1)^2$ , op voorwaarde dat  $a \geq 0$ . Om een analoge reden geldt dat als  $a^2 < x^2 < (a+2)^2$ , dan  $x = a+1$ . Hetzelfde geldt natuurlijk ook voor derdemachten, en  $n$ -de machten, als  $n > 0$ . Ja, ook voor  $n = 1$ , want er liggen namelijk geen gehele getallen tussen  $a$  en  $a+1$ .

**Voorbeeld 4.16.** Vind alle gehele getallen  $n$  zo dat  $n^2 + 1$  een volkomen kwadraat is.

*Oplossing.*

$n = 0$  geeft al een oplossing. Stel eerst  $n > 0$ . Dan is  $n^2 < n^2 + 1 < n^2 + 2n + 1 = (n+1)^2$ . Dan kan  $n^2 + 1$  dus geen volkomen kwadraat zijn. Stel nu  $n < 0$ . Dan is  $n^2 < n^2 + 1 < n^2 - 2n + 1 = (n-1)^2$ . Ook hier is  $n^2 + 1$  onmogelijk een volkomen kwadraat.

*Opmerking.*

De ongelijkheid  $n^2 + 1 < n^2 + 2n + 1$  is alleen geldig als  $n < 0$ , en  $n^2 + 1 < n^2 - 2n + 1$  alleen als  $n < 0$ . Het was dus nodig om gevalsonderscheid te maken.

**Opgave 4.17.** Vind alle gehele getallen  $x$  en  $y$  zo dat  $\frac{x}{y-1} = \frac{y+1}{x+1}$ .

**Opgave 4.18.** (Q-E-D Competitie juni 2012)

- Vind alle natuurlijke getallen  $n$  waarvoor geldt dat  $n^2 + 12n + 20$  een volkomen kwadraat is.
- Vind alle natuurlijke getallen  $n$  waarvoor geldt dat  $n^4 + 2n^3 + 2n^2 + 2n + 1$  een volkomen kwadraat is.

### 4.3 Extremenprincipe

Het extremenprincipe wordt soms ook omschreven door “descente infinie” of, uit het Frans vertaald, oneindige afdaling. Het is een techniek om aan te tonen dat een vergelijking geen oplossingen heeft. We schetsen eerst met een voorbeeld hoe de techniek in zijn werk gaat.

**Voorbeeld 4.19.** Vind alle gehele getallen  $a$  en  $b$  waarvoor  $a^2 = 3b^2$ .

*Oplossing.*

Om te beginnen hebben we de oplossing  $a = b = 0$ . Stel nu dat  $a, b > 0$ , en dat  $a$  de kleinste waarde is waarvoor er een bijbehorende waarde van  $b$  bestaat. merk op dat  $a > b$ .

Er geldt dat  $3 \mid a^2$ , dus moet  $3 \mid a$ . Stel dus  $a = 3x$ . We kunnen de vergelijking herschrijven als  $9x^2 = 3b^2$ , of dus  $3x^2 = b^2$ .

Stellen we nu  $a_0 = b$  en  $b_0 = x$ , dan hebben we een nieuwe oplossing  $(a_0, b_0)$  waarvoor  $a_0^2 = 3b_0^2$ .

Maar  $a_0 = b < a$  en  $a$  was de kleinste waarde waarvoor er een  $b$  bestaat. Dat is dus onmogelijk, want  $a_0$  is nog kleiner en heeft ook een waarde  $b_0$ .

Hieruit kunnen we besluiten dat er geen kleinste waarde voor  $a$  is als  $a > 0$ , dus is er ook geen andere oplossing.

*Opmerking.*

Bij deze oefening is het erg omslachtig om het extremenprincipe toe te passen. Je had deze waarschijnlijk opgelost door de priemontbinding van beide leden te bekijken, en op te merken dat 3 in het linkerlid tot een even macht voorkomt en in het rechterlid tot een oneven macht, waardoor gelijkheid onmogelijk is als  $a, b > 0$ . Deze oefening diende dan ook alleen maar om het principe duidelijk te maken.

Bij dit voorbeeld kozen we een minimale waarde, en toonden aan dat er toch nog een kleinere waarde bestaat. Soms kan het ook zijn dat je een maximale waarde kiest. Het getal waarvoor je het maximum beschouwt hoeft ook niet noodzakelijk simpelweg één van de onbekenden te zijn. Wat ook kan is de som van twee getallen, of hun product, of de som van hun kwadraten, om maar enkele voorbeelden te geven. Hier hadden we bijvoorbeeld de som  $a + b$  als minimale waarde kunnen nemen: de nieuwe oplossing  $(a_0, b_0)$  geeft dan een som  $a_0 + b_0 = b + \frac{a}{3} < a + b$ , dus bestaat er nog een kleinere som. Nu lijkt het misschien moeilijk om te weten voor welke waarde je een extremum kiest, maar vaak zal dat duidelijk worden eens je je op het probleem hebt gestort. Merk trouwens op dat we het extremenprincipe stilzwijgend al toepasten bij het bewijs dat de priemontbinding uniek is.

**Opgave 4.20.** Bewijs dat er geen strikt positieve gehele getallen  $x$  en  $y$  zijn die voldoen aan  $x^2 + 2y^2 = 4xy$ .

**Opgave 4.21.** Vind alle gehele getallen  $x$ ,  $y$  en  $z$  zijn die voldoen aan  $x^3 + 3y^2 = 9z^2$ .

### 4.4 Vieta jumping

Vieta jumping of root flipping is een techniek die specifiek is voor een bepaald soort problemen in de getaltheorie. Ze zijn duidelijk herkenbaar, maar vaak niet bepaald gemakkelijk. De werkwijze is echter altijd ongeveer gelijkaardig. Je herschrijft een vergelijking als een kwadratische vergelijking in één van de variabelen, en haalt daaruit een tweede oplossing van de vergelijking. Dan kies je een bepaalde waarde die je minimaliseert, en je probeert daarop het extremenprincipe toe te passen.

Laten we dit eens verduidelijken met een voorbeeld.



**Voorbeeld 4.22.** Zij  $x$  en  $y$  natuurlijke getallen zo dat  $xy \mid x^2 + y^2 + 1$ . Bewijs dat  $x^2 + y^2 + 1 = 3xy$ .

*Oplossing.*

Stel  $x^2 + y^2 + 1 = kxy$ , en bekijk een vaste waarde van  $k$ . Noem  $S_k$  de verzameling van alle koppels  $(x, y)$  die voldoen.

Dus  $x^2 - ky \cdot x + y^2 + 1 = 0$ . Als  $x$  een oplossing geeft voor zekere  $y$  en  $k$ , dan geeft ook  $x' = ky - x = \frac{y^2+1}{x}$  een oplossing: uit  $x' = ky - x$  volgt dat  $x' \in \mathbb{Z}$  en uit  $x' = \frac{y^2+1}{x}$  volgt dat  $x' > 0$ .

Merk dus op dat, als  $(x, y) \in S_k$ , dan ook  $(ky - x, y) \in S_k$  en analoog  $(x, kx - y) \in S_k$ .

Noem nu  $a$  de kleinste waarde van  $x$  waarvoor er een  $y$  bestaat zodat  $(x, y) \in S_k$ . Noem  $b$  de kleinste waarde van  $y$  waarvoor  $(a, y) \in S_k$ .

Dan is  $a \leq b$ , want anders zou  $a$  niet de kleinste waarde van  $x$  geven: immers, als  $(a, b) \in S_k$ , dan  $(b, a) \in S_k$  maar  $b < a$  en  $a$  was de kleinste...

Omdat  $(a, b) \in S_k$  is dus  $(a, \frac{a^2+1}{b}) \in S_k$ .

Als  $b > 1$  is  $\frac{a^2+1}{b} \leq \frac{b^2+1}{b} = b + \frac{1}{b} < b + 1$ . Dus  $\frac{a^2+1}{b} = b$  zodat  $a^2 + 1 = b^2$ , wat niet kan als  $a > 0$ , contradictie.

Bijgevolg moet  $b = 1$  zodat  $a = 1$ , en dan is  $k = 3$ . □

We zullen nu eens duidelijk maken wat Vieta jumping eigenlijk is. De naam Vieta jumping is genoemd naar de Franse wiskundige François Viète. Hij stelde formules op voor de coëfficiënten van veeltermen in functie van de nulpunten van de veelterm, waaronder die voor de som en het product bij een kwadratische vergelijking. Het grootste deel van de oplossing steunt op deze formules voor de som en het product, en de gelijkheid  $ky - x = \frac{y^2+1}{x}$ . De techniek bestond er vooral uit om uit een oplossing  $(x, y)$  andere oplossingen te creëren:  $(y, x)$ ,  $(ky - x, y)$ ,  $(y, ky - x)$ ,  $(x, kx - y)$  en  $(kx - y, x)$ . Deze bleken niet allemaal nodig te zijn, maar leveren wel een waaier van mogelijkheden. Zoals je hebt gemerkt is hier ook het extremenprincipe bij komen kijken. Het minimaliseren van  $x$  en  $y$  was ook een cruciale stap en lijkt misschien ver gezocht, hoewel zoiets in het algemeen vaak meer informatie kan geven. Immers, over een kleinste getal kan je al iets meer zeggen dan over een willekeurig getal, namelijk precies het feit dat het het kleinste is.

**Opgave 4.23.** Vind alle natuurlijke getallen  $n$  waarvoor er  $x, y \in \mathbb{N}$  bestaan zo dat


$$\frac{(x + y + 1)^2}{xy + 1} = n.$$

## Opgaven hoofdstuk 4

**Opgave 4.24.** (JWO 2010 finale vraag 2) Vind alle gehele getallen  $a$  en  $b$  waarvoor  $\frac{1}{a} - \frac{1}{b} = 6$ . 

**Opgave 4.25.** Zij  $p$  een priemgetal. Vind alle  $a, b \in \mathbb{N}$  zo dat  $pa + pb = ab$ .

**Opgave 4.26.** Vind alle priemgetallen  $p$  en natuurlijke getallen  $n$  zo dat  $8^p + 27^p = p^n$ .

**Opgave 4.27.** Bepaal de grootste waarde van  $a + b$  als  $a$  en  $b$  natuurlijke getallen zijn met  $\frac{1}{a} + \frac{1}{b} = \frac{1}{20}$ . 

**Opgave 4.28.** (JWO 2004 finale vraag 4) Vind alle  $a, b \in \mathbb{N}$  zo dat

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{2004}.$$

**Opgave 4.29.** (Q-E-D Competitie augustus 2012). Voor welke natuurlijke getallen  $n$  is  $n^4 + 4^n$  een priemgetal? H

**Opgave 4.30.** (Q-E-D Competitie augustus 2012). Voor welke natuurlijke getallen  $n$  is  $2^{2^n-2} + 1$  een priemgetal? H

**Opgave 4.31.** Vind alle priemgetallen  $p$  en  $q$  zo dat  $p^2 + 7pq + q^2$  een volkomen kwadraat is. H

**Opgave 4.32.** (APMC 2006 dag 2 vraag 1) Een geheel getal  $d > 6$  is mooi als voor alle gehele getallen  $x, y$  geldt dat  $d \mid (x + y)^5 - x^5 - y^5$  als en slechts als  $d \mid (x + y)^7 - x^7 - y^7$ . H

A. Is 29 mooi?

B. Is 2006 mooi?

C. Bewijs dat er oneindig veel mooie getallen zijn.

**Opgave 4.33.** Zij  $a, b, c, d \in \mathbb{N}^+$  met  $ab = cd$ . Bewijs dat  $a^2 + b^2 + c^2 + d^2$  geen priemgetal is. ✿

**Opgave 4.34.** (VWO 2009 finale vraag 2) Een natuurlijk getal heeft vier natuurlijke delers: 1, zichzelf en twee echte delers. Dat getal vermeerderd met 9 is gelijk aan 7 keer de som van de echte delers. Bewijs dat dat getal uniek is en zeg welk getal we zochten. H

**Opgave 4.35.** (IMOSL 2002 vraag 10) Zij  $n \geq 2$  een natuurlijk getal, met delers  $1 = d_1 < d_2 < \dots < d_k = n$ . Bewijs dat  $d_1d_2 + d_2d_3 + \dots + d_{k-1}d_k$  altijd kleiner is dan  $n^2$  en bepaal wanneer het een deler is van  $n^2$ . H

**Opgave 4.36.** (Polen MO 2013 finale vraag 1) Vind alle gehele getallen  $x, y$  zo dat  $x^4 + y = x^3 + y^2$ . H

**Opgave 4.37.** (WiNA 2010) Bepaal de priemgetallen  $p$  waarvoor zowel  $\frac{p+1}{2}$  als  $\frac{p^2+1}{2}$  volkomen kwadraten zijn. ✿ H

**Opgave 4.38.** Bepaal de gehele oplossingen van  $3a^2 + 3b^2 + 19ab = 0$ . ✿

**Opgave 4.39.** (IMO 1988 dag 2 vraag 3) Gegeven zijn positieve gehele getallen  $a$  en  $b$  waarvoor geldt dat  $ab + 1$  een deler is van  $a^2 + b^2$ . Bewijs dat  $\frac{a^2+b^2}{ab+1}$  het kwadraat van een geheel getal is. H

**Opgave 4.40.** (IMO 2007 dag 2 vraag 2) Stel  $a$  en  $b$  zijn gehele getallen groter dan 0, zo dat  $4ab - 1$  een deler is van  $(4a^2 - 1)^2$ . Toon aan dat  $a = b$ . H

**Opgave 4.41.** Vind alle  $n \in \mathbb{N}$  waarvoor  $324 + 455^n$  een priemgetal is. ✿ HA

Het convolutieproduct is een bewerking tussen functies. In principe is het niet meer dan een verkorte notatie, maar het zal toelaten enkele interessante eigenschappen eenvoudig af te leiden.

**Definitie 5.1.**

We definiëren de functies  $\text{id}$ ,  $\mathbf{1}$  en  $\varepsilon$  door  $\text{id}(n) = n$ ,  $\mathbf{1}(n) = 1$  en

$$\varepsilon(n) = \begin{cases} 1 & \text{als } n = 1. \\ 0 & \text{als } n \neq 1. \end{cases}$$

De functies  $\text{id}$ ,  $\mathbf{1}$  en  $\varepsilon$  zijn totaal multiplicatief.

**Definitie 5.2.** Dirichlet-convolutie

Voor twee aritmetische functies  $f, g$ , niet noodzakelijk multiplicatief, definiëren we het *Dirichlet convolutieproduct*  $f * g$  als de functie met voorschrift

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right),$$

waarbij de som loopt over de positieve delers  $d$  van  $n$ .

**Stelling 5.3.**

Het Dirichlet-convolutieproduct is commutatief en associatief, en heeft als neutraal element  $\varepsilon$ .

Om die reden noemt men  $\varepsilon$  ook wel de (*Dirichlet-*)convolutie-eenheid.

**5.1 Inverteerbaarheid**

**Definitie 5.4.** Dirichlet-inverse

Een aritmetische functie  $f$  noemen we *inverteerbaar* als er een functie  $g$  bestaat met  $g * f = \varepsilon$ .  $g$  noemt men de *Dirichlet-inverse* van  $f$ , of kortweg inverse. Soms noteert men  $g = f^{-1}$ .

**Opgave 5.5.** Toon aan dat een Dirichlet-inverse, als ze bestaat, uniek is.

**Opgave 5.6.** Zij  $f$  inverteerbaar. Toon aan dat  $f^{-1}$  inverteerbaar is en  $(f^{-1})^{-1} = f$ .

Welke functies zijn inverteerbaar? In elk geval niet allemaal, zo is bijvoorbeeld de constante functie 0 zeker niet inverteerbaar. Verrassend genoeg blijkt het niet-nul zijn van  $f(1)$  nodig en voldoende voor het inverteerbaar zijn van  $f$ .

**Stelling 5.7.** Criterium voor inverteerbaarheid

Een aritmetische functie  $f$  is inverteerbaar als en slechts als  $f(1) \neq 0$ .

*Bewijs.*

Als  $f$  inverteerbaar is, is  $f(1) \cdot f^{-1}(1) = (f * f^{-1})(1) = \varepsilon(1) = 1$ , dus  $f(1) \neq 0$ . De andere richting van het bewijs is constructief: het is vaak de methode waarop een inverse wordt geconstrueerd. Zij dus  $f(1) \neq 0$ . De inverse  $g$  moet voldoen aan het stelsel

$$\begin{cases} f(1)g(1) = 1 \\ f(1)g(2) + f(2)g(1) = 0 \\ f(1)g(3) + f(3)g(1) = 0 \\ f(1)g(4) + f(2)g(2) + f(4)g(1) = 0 \\ \dots \\ \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = 0 \\ \dots \end{cases}$$

waarbij  $g(1), g(2), g(3), \dots$  de onbekenden zijn. Uit de eerste vergelijking volgt dat  $g(1) = \frac{1}{f(1)}$ . De tweede vergelijking geeft  $g(2) = -\frac{g(1)f(2)}{f(1)} = -\frac{f(2)}{f(1)^2}$ . Invullen in de derde vergelijking geeft dan een formule voor  $g(3)$ . Algemeen vinden we  $g(n)$  door

$$g(n) = -\frac{1}{f(1)} \sum_{d|n, d>1} f(d)g\left(\frac{n}{d}\right),$$

wat  $g(n)$  uniek bepaalt. Zo zien we dat er een inverse bestaat, namelijk de functie  $g$  die recursief wordt gedefinieerd door

$$\begin{cases} g(1) = \frac{1}{f(1)} \\ g(n) = -\frac{1}{f(1)} \sum_{d|n, d>1} f(d)g\left(\frac{n}{d}\right). \end{cases}$$

Merk op dat deze constructie nogmaals de uniciteit van de inverse impliceert. □

We bekijken nog enkele belangrijke gevolgen van inverteerbaarheid.

**Gevolg 5.8.** Schrappingswet voor convoluties

Als  $f, g, h$  aritmetische functies zijn zo dat  $h(1) \neq 0$  en  $f * h = g * h$ , dan is  $f = g$ .

*Bewijs.*

Omdat  $h(1) \neq 0$  bestaat  $h^{-1}$ . Links en rechts convolueren met  $h^{-1}$  geeft  $(f * h) * h^{-1} = (g * h) * h^{-1}$ , dus  $f = g$  aangezien  $*$  associatief is en  $\varepsilon$  als neutraal element heeft.  $\square$

## 5.2 Multiplicativiteit

**Stelling 5.9.**

Als  $f$  en  $g$  multiplicatief zijn is  $f * g$  ook multiplicatief.

*Bewijs.*

Als oefening.  $\square$

Let er op dat Stelling 5.9 enkel toelaat te besluiten dat  $f * g$  multiplicatief is. Als  $f$  en  $g$  *totaal* multiplicatief zijn, betekent dit niet noodzakelijk dat  $f * g$  ook *totaal* multiplicatief is. De volgende oefening toont hier meteen twee voorbeelden van.

**Opgave 5.10.** Bewijs dat  $1 * 1 = \tau$  en  $1 * \text{id} = \sigma$ .

**Opgave 5.11.** Noem  $\chi_{\text{sq}}$  de karakteristieke functie van de kwadraten. Is  $\chi_{\text{sq}}$  multiplicatief? Is  $1 - \chi_{\text{sq}}$  multiplicatief?

**Stelling 5.12.**

Als  $f$  multiplicatief is, is  $f$  inverteerbaar en is  $f^{-1}$  ook multiplicatief.

*Bewijs.*

In een eerdere oefening werd aangetoond dat  $f(1) = 1$  voor multiplicatieve  $f$ , dus die zijn inverteerbaar. De multiplicativiteit van  $g = f^{-1}$ , of dus  $g(ab) = g(a)g(b)$  voor  $\text{ggd}(a, b) = 1$  bewijzen we met inductie op het product  $ab$ . Als het product 1 is, is het duidelijk: dan is  $a = b = 1$  en dus  $g(a) = g(b) = g(ab) = \frac{1}{f(1)} = 1$ . Veronderstel nu dat het waar is voor alle producten kleiner dan  $ab$ , met  $\text{ggd}(a, b) = 1$ . We hebben

$$\sum_{d|ab} f(d)g\left(\frac{ab}{d}\right) = \varepsilon(ab) = \varepsilon(a)\varepsilon(b) = \sum_{x|a} f(x)g\left(\frac{a}{x}\right) \sum_{y|b} f(y)g\left(\frac{b}{y}\right).$$

Aangezien  $\text{ggd}(a, b) = 1$  is in het linkerlid  $d = xy$  met  $x | a$  en  $y | b$ ,  $\text{ggd}(x, y) = 1$ . Dus

$$\sum_{x|a, y|b} f(xy)g\left(\frac{ab}{xy}\right) = \sum_{x|a, y|b} f(x)f(y)g\left(\frac{a}{x}\right)g\left(\frac{b}{y}\right)$$

Gebruiken we de multiplicativiteit van  $f$  en de inductiehypothese, dan kunnen we het linkerlid herschrijven als

$$g(ab) + \sum_{\substack{x|a, y|b \\ xy > 1}} f(x)f(y)g\left(\frac{a}{x}\right)g\left(\frac{b}{y}\right).$$

De term  $g(ab)$  is dus gelijk aan de term voor  $x = y = 1$  in het rechterlid, dat is  $f(1)^2 g(a)g(b) = g(a)g(b)$ .  $\square$

**Gevolg 5.13.**

Als  $f * g = h$ , dan zijn deze drie functies multiplicatief zodra twee van hen dat zijn.

**Opgave 5.14.** Bewijs als oefening.

### 5.3 Möbiusinversie

**Definitie 5.15.** Kwadraatvrij en kwadraatvol

Een natuurlijk getal  $n \in \mathbb{N}^+$  noemen we *kwadraatvrij* als geen enkele priemfactor in de priemontbinding tot een macht hoger dan 1 voorkomt. Of equivalent, als  $n$  niet deelbaar is door een kwadraat groter dan 1. Een natuurlijk getal dat niet kwadraatvrij is, heet *kwadraatvol*

**Definitie 5.16.** Möbiusfunctie

Voor  $n \in \mathbb{N}^+$  definiëren we de Möbiusfunctie  $\mu$  met

$$\mu(n) = \begin{cases} 0 & \text{als } n \text{ niet kwadraatvrij is.} \\ (-1)^k & \text{als } n \text{ het product is van } k \text{ verschillende priemgetallen.} \end{cases}$$

Per definitie is dus  $\mu(1) = 1$  en  $\mu(p) = -1$  voor priemgetallen  $p$ .

**Stelling 5.17.**

$\mu$  is multiplicatief.

**Opgave 5.18.** Bewijs.

De volgende convolutie ligt aan de basis van de Möbiusinversie:

**Lemma 5.19.**

Er geldt dat  $\mu * 1 = \varepsilon$ .

*Bewijs.*

Aangezien  $\mu$  en  $1$  multiplicatief zijn is ook  $\mu * 1$  multiplicatief. Het volstaat dus om de gelijkheid te bewijzen voor machten van priemgetallen. Dat beide functies gelijk zijn in 1 is duidelijk. Zij nu  $p$  een priemgetal en  $n \in \mathbb{N}^+$ . Dan is  $\varepsilon(p^n) = 0$ . Er geldt

$$(\mu * 1)(p^n) = \sum_{d|p^n} \mu(d) \cdot 1 = \mu(1) + \mu(p) + 0 + \dots + 0 = 1 - 1 = 0,$$

zodat  $(\mu * 1)(p^n) = \varepsilon(p^n)$ .  $\square$

**Gevolg 5.20.**

Als  $n > 1$  geldt

$$\sum_{d|n} \mu(d) = 0.$$

Indien  $n = 1$  is deze som 1.

**Opgave 5.21.** Zij  $n$  het product van  $m$  verschillende priemgetallen. Leid uit  $\sum_{d|n} \mu(d) = 0$  af dat

$$\sum_{k=1}^m (-1)^k \binom{m}{k} = 0,$$

d.i., een bijzonder geval van het binomium van Newton.

**Stelling 5.22.** Möbius-inversiestelling

Als  $f, g : \mathbb{N}^+ \rightarrow \mathbb{C}$  functies zijn, dan geldt dat  $f = \mu * g$  als en slechts als  $g = \mathbf{1} * f$ .

*Bewijs.*

Indien  $f = \mu * g$  is  $\mathbf{1} * f = \mathbf{1} * (\mu * g) = (\mathbf{1} * \mu) * g = \varepsilon * g = g$ . Omgekeerd, indien  $g = \mathbf{1} * f$  is  $\mu * g = \mu * (\mathbf{1} * f) = (\mu * \mathbf{1}) * f = \varepsilon * f = f$ .  $\square$

De Möbius-inversiestelling laat zich ook uitdrukken met de zogenaamde Möbius-inversieformule:

**Gevolg 5.23.** Möbius-inversieformule

Als  $f, g$  aritmetische functies zijn waarvoor

$$g(n) = \sum_{d|n} f(d),$$

dan is

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

**Opgave 5.24.** Bewijs dat

$$\sum_{d|n} \mu(d) \tau\left(\frac{n}{d}\right) = 1 \quad \text{en} \quad \sum_{d|n} \mu(d) \sigma\left(\frac{n}{d}\right) = n$$

voor elk natuurlijk getal  $n$ .

**5.3.1 Möbiusinversie in multiplicatieve vorm**

De Möbius-inversieformule kent ook een multiplicatieve variant. Het bewijs ervan kan helaas niet met het convolutieproduct gegeven worden.<sup>11</sup>

<sup>11</sup>Een verklaring hiervoor is het gebrek aan commutativiteit van de multiplicatieve variant van het convolutieproduct.

**Stelling 5.25.** Möbius-inversieformule, multiplicatieve vorm

Als  $f, g$  aritmetische functies zijn waarvoor

$$g(n) = \prod_{d|n} f(d),$$

dan is

$$f(n) = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}.$$

**Opgave 5.26.** Bewijs.

*Opmerking.*

De Möbius-inversieformule alsook zijn multiplicatieve variant zijn ook geldig voor niet aritmetische functies, op voorwaarde dat de beeldverzameling aan de volgende eisen voldoet:<sup>12</sup>

- De optelling en vermenigvuldiging zijn associatief en commutatief.
- De vermenigvuldiging is distributief t.o.v. de optelling.
- De optelling heeft een neutraal element, en elk element heeft een inverse voor de optelling.
- De vermenigvuldiging heeft een neutraal element.

Voor de multiplicatieve variant komt er een voorwaarde bij:

- Elk element heeft een invers element voor de vermenigvuldiging.

Dit garandeert dat een negatieve exponent ten gevolge van  $\mu$  zinvol is. Een voorbeeld van een dergelijke verzameling is  $\mathbb{C}[x]$ , de verzameling van veeltermen over  $\mathbb{C}$ . Voor de bijkomende vijfde eigenschap is er  $\mathbb{C}(x)$ , de verzameling van rationale functies over  $\mathbb{C}$ .

**Opgave 5.27.** Bewijs dat voor elk natuurlijk getal  $n > 0$

$$\sigma(n) = \sum_{d|n} \varphi(d) \tau\left(\frac{n}{d}\right).$$

**Opgave 5.28.** Bewijs dat voor elk natuurlijk getal  $n > 0$

$$\prod_{d|n} d^{\mu(d) \tau\left(\frac{n}{d}\right)} = \frac{1}{n}.$$

## 5.4 Toepassingen

### 5.4.1 Expliciete formules voor aritmetische functies

Een enigszins verrassende convolutie is de volgende:

<sup>12</sup>Onder de eerste vier voorwaarden noemt men die verzameling een *commutatieve ring (met eenheid)*.



**Stelling 5.29.**

Er geldt dat  $1 * \varphi = \text{id}$ , of anders gezegd, voor elk natuurlijk getal  $n > 0$  geldt er dat

$$\sum_{d|n} \varphi(d) = n.$$

Aangezien het doel is om de formule voor  $\varphi$  opnieuw te bewijzen steunen we niet op die formule.

*Bewijs.*

We tellen het aantal breuken in  $\{\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}\}$  op twee manieren. Enerzijds zijn dit er gewoon  $n$ . Anderzijds kunnen we elke breuk vereenvoudigen. Een breuk zal dan noemer  $d$  hebben als de teller niet groter was dan  $d$  en relatief priem met  $d$ . Zo zijn er  $\varphi(d)$ . Omdat elke breuk als noemer een deler van  $n$  heeft, is het aantal breuken precies  $\sum_{d|n} \varphi(d)$ .  $\square$

*Opmerking.*

Strikt genomen hebben we nog niets gezien over rationale getallen en het vereenvoudigen van breuken. Voor een rechtvaardiging van dit bewijs verwijzen we naar Stelling 2.26.

Ter illustratie van enkele nieuwe technieken geven we nog een zuiver algebraïsch bewijs:

*Bewijs.*

$$\begin{aligned} \sum_{d|n} \varphi(d) &= \sum_{d|n} \sum_{\substack{k \leq d \\ \text{ggd}(k,d)=1}} 1 \\ &= \sum_{d|n} \sum_{k \leq d} \sum_{f|k,d} \mu(f) \\ &= \sum_{f|n} \mu(f) \sum_{\substack{d \\ f|d|n}} \sum_{f|k} 1 \\ &= \sum_{f|n} \mu(f) \sum_{\substack{d \\ f|d|n}} \frac{d}{f} \\ &= \sum_{f|n} \mu(f) \sum_{g|\frac{n}{f}} g && (d = gf) \\ &= \sum_{f|n} \mu(f) \sigma\left(\frac{n}{f}\right) \\ &= (\mu * \sigma)(n) \\ &= \text{id}(n). \end{aligned}$$

$\square$

Zoals je kan zien hebben we de voorwaarde  $\text{ggd}(k, d) = 1$  weggewerkt door een extra sommatie  $\sum_{f|\text{ggd}(k,d)} \mu(f) = \varepsilon(\text{ggd}(k, d))$ . We konden daardoor gewoon sommeren over alle  $k \leq d$ . Daarna hebben we de volgorde van de sommaties omgekeerd: de mogelijke waarden van  $f$  zijn delers van  $d$ , wat op zijn beurt een deler van  $n$  is. Als we de sommatie over  $f$  voorop plaatsen moeten we dus sommeren over de delers van  $n$ .  $\mu(f)$  kwam enkel voor als er  $k$  en  $d$

zijn met  $k \leq d$  zodat  $f \mid k, d$ . Sommeren we eerst over  $d$ , dan zijn de mogelijke waarden van  $d$  precies die waarvoor  $f \mid d$  en  $d \mid n$ .  $k$  kan op zijn beurt enkel waarden kleiner of gelijk aan  $d$  aannemen die veelvoudig zijn van  $f$ .

Uit deze convolutie volgt ook de formule voor  $\varphi$ :

*Bewijs.*

$\varphi * 1 = \text{id}$  is  $\varphi = \text{id} * \mu$ , zodat  $\varphi$  multiplicatief is. Voor een priemmacht  $p^n$  volgt uit de definitie van  $\varphi$  gemakkelijk dat  $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$ . (Als alternatief kan je de zopas bekomen formule uitbuiten d.m.v.  $\varphi(p^n) = \sum_{d \mid p^n} \mu(d) \cdot \frac{p^n}{d} = p^n - \frac{p^n}{p} + 0 + \dots + 0 = (p-1)p^{n-1}$ .) De algemene formule voor  $\varphi$  volgt nu uit de multiplicativiteit.  $\square$

De identiteit kent nog een mooi bewijs, op voorwaarde dat we al weten dat  $\varphi$  multiplicatief is. (Dit bewijs past niet in de opbouw die we hierboven gaven omdat het net de multiplicativiteit van  $\varphi$  is die met de laatste stelling bewezen werd.)

*Bewijs.*

Via inductie. Voor  $n = 1$  is het duidelijk, stel nu dat het geldt voor  $1, \dots, n-1$ . Zij  $p^k \parallel n$  met  $m = p^k m$ . We hebben

$$\sum_{d \mid n} \varphi(d) = \sum_{\substack{d \mid n \\ p^k \mid d}} \varphi(d) + \sum_{\substack{d \mid n \\ p^k \nmid d}} \varphi(d)$$

In de eerste som is  $d = p^k f$  met  $f \mid m$  en  $\varphi(d) = \varphi(p^k)\varphi(f)$  wegens de multiplicativiteit. Wegens de inductiehypothese is nu  $\sum_{\substack{d \mid n, p^k \mid d}} \varphi(d) = \varphi(p^k) \sum_{f \mid m} \varphi(f) = (1 - \frac{1}{p}) \cdot p^k m = (1 - \frac{1}{p})n$ . In de tweede som is  $d \mid \frac{n}{p}$ , dus die som is wegens de inductiehypothese  $\frac{n}{p}$ . Optellen levert  $(1 - \frac{1}{p})n + \frac{n}{p} = n$ .  $\square$

## 5.4.2 Elimineren van de floorfunctie

Onder het motto 'oefening baart kunst' maak ik hier niet te veel woorden aan vuil.

**Opgave 5.30.** Bewijs dat voor  $n \geq 1$ ,

$$\sum_{k=1}^n \left\lfloor \frac{n}{k} \right\rfloor = \sum_{k=1}^n \tau(k).$$

**Opgave 5.31.** Bewijs dat voor  $n \geq 1$ ,

$$\sum_{k=1}^n \left\lfloor \frac{n}{k} \right\rfloor \varphi(k) = \frac{n(n+1)}{2}.$$

**Opgave 5.32.** Bewijs dat voor  $n \geq 1$ ,

$$\sum_{k=1}^n \left\lfloor \frac{n}{k} \right\rfloor \mu(k) = 1.$$

**Opgave 5.33.** Bewijs dat voor  $n \geq 1$ ,

$$\sum_{k=1}^n \left\lfloor \frac{n}{k} \right\rfloor \lambda(k) = \lfloor \sqrt{n} \rfloor.$$

## 5.5 Meer over multiplicativiteit

### Definitie 5.34. Radicaal

Het radicaal van een natuurlijk getal  $n \in \mathbb{N}^+$  is het product van alle priemdelers van  $n$ . We noteren  $\text{rad}(n)$ .

**Opgave 5.35.** (Veralgemeende convoluties) Zij voor alle  $n \in \mathbb{N}$   $S(n) = S_n$  een verzameling van delers van  $n$ . Definieer een bewerking  $*_S$  op aritmetische functies door

$$(f *_S g)(n) = \sum_{d \in S_n} f(d)g\left(\frac{n}{d}\right)$$

Zoals voor de gewone  $*$  is ook  $*_S$  distributief t.o.v. optelling. Onder welke voorwaarden op  $S$

- A. is  $*_S$  commutatief?
- B. heeft  $*_S$  een neutraal element?
- C. is  $*_S$  associatief?

Een triviaal voorbeeld van  $S$  waarbij al deze voorwaarden voldaan zijn, is  $S_n = \emptyset$ . Iets minder triviaal is  $S_n = \{1, n\}$ . Hieruit blijkt dat  $d \mid n$  niet impliceert dat  $S_d \subset S_n$ .

We noemen een deelverzameling  $V \subset \mathbb{N}$  *multiplicatief verzadigd* als ze gesloten is onder delen en vermenigvuldigen.<sup>13</sup>

- D. Toon aan dat als  $*_S$  associatief is en  $V \subset \mathbb{N}$  multiplicatief verzadigd,  $*_{S \cap V}$  associatief is (met  $(S \cap V)_n = S_n \cap V$ ).

Voorbeelden: de verzameling van  $k$ de machten ( $k \geq 0$ ), de getallen die copriem zijn met een vast getal, de getallen waarvan de priemdelers tot een vaste verzameling priemgetallen behoren. Als  $V$  en  $W$  multiplicatief verzadigd zijn, dan ook  $V \cap W$ . Als bovendien  $\text{ggd}(V, W) = 1$  (d.w.z. elk getal uit  $V$  is copriem met elk getal uit  $W$ ), dan is  $VW$  multiplicatief verzadigd.<sup>14</sup>

- E. Zij  $k > 1$  en stel  $S_n = \{d : d^k \mid n\}$ . Welke van bovenstaande eigenschappen heeft  $*_S$ ?

**Opgave 5.36.** (Multiplicativiteit en restrictie) We gebruiken de notaties en terminologie uit Opgave 5.35 (maar het is niet nodig om die gemaakt te hebben). We zeggen dat  $*_S$  multiplicativiteit bewaart als  $f *_S g$  multiplicatief is zodra  $f$  en  $g$  dat zijn.<sup>15</sup>

- A. Toon aan dat  $*_S$  multiplicativiteit bewaart a.s.a.  $S_{mn} = S_m S_n$  voor  $\text{ggd}(m, n) = 1$ .
- B. Toon aan dat als  $*_S$  en  $*_T$  multiplicativiteit bewaren,  $*_{S \cap T}$  multiplicativiteit bewaart.

We noemen een niet-lege deelverzameling  $V \subset \mathbb{N}$  *primitief* als  $mn \in V$  en  $\text{ggd}(m, n) = 1$  impliceert dat  $m, n \in V$ .

<sup>13</sup>Een niet-lege multiplicatief verzadigde verzameling bevat dus steeds 1.

<sup>14</sup>Multiplicatieve verzadigdheid blijft ook behouden onder (willekeurige) oneindige doorsnedes en producten van paarsgewijs coprieme verzamelingen.

<sup>15</sup>Bij definitie is  $f(1) = 1$  als  $f$  multiplicatief is. Als  $S$  multiplicativiteit bewaart, is dus  $S_1 = \{1\}$ . I.h.b. is  $S_n$  niet voor alle  $n$  leeg.

- C. Toon aan dat als  $*_S$  multiplicativiteit bewaart en  $V$  primitief is,  $*_{S \cap V}$  multiplicativiteit bewaart.

Voorbeelden: de verzameling van  $k$ de machten ( $k \geq 0$ ), de getallen die copriem zijn met een vast getal, de getallen met hoogstens  $k$  priemdelers ( $k$  vast), de getallen waarvan de priemdelers tot een vaste verzameling priemgetallen behoren. Als  $V$  en  $W$  primitief zijn, dan ook  $V \cap W$ .<sup>16</sup>

Er zijn multiplicatief verzadigde (zie Opgave 5.35) verzamelingen die niet primitief zijn; bvb. de machten van  $n$  met  $n > 1$  niet priem, de natuurlijke getallen congruent (zie Hoofdstuk 7) met 1 modulo een vast getal  $n$ , of meer algemeen, die congruent zijn met een inverteerbare  $k$ -de machtsrest modulo  $n$  ( $k, n$  vast).

- D. Zij  $f$  een multiplicatieve functie. Toon aan dat

$$g(n) = \sum_{\substack{d^3|n \\ d \text{ oneven}}} f(n/d^3)$$

multiplicatief is.

**Definitie 5.37.** Indicatorfunctie

Zij  $V \subset \mathbb{N}$ . Noteer met  $1_V$  de indicatorfunctie van  $V$ :

$$1_V(n) = \begin{cases} 1 & \text{als } n \in V \\ 0 & \text{als } n \notin V. \end{cases}$$

We noteren ook  $1_{sq}$  voor de karakteristieke functie van de kwadraten.  $1_{sq}$  is multiplicatief, maar niet totaal multiplicatief.

**Opgave 5.38.** Wanneer is  $1_V$  multiplicatief? Totaal multiplicatief? A

**Opgave 5.39.** Zij  $V \in \mathbb{N}$  zo dat  $1_V$  multiplicatief is, en stel dat  $*_S$  multiplicativiteit bewaart. A  
Bewijs dat  $*_{S \cap V}$  multiplicativiteit bewaart (hetgeen we uit Opgave 5.36 al wisten voor meer algemene  $V$ ).

**Voorbeeld 5.40.** Zij  $f$  een multiplicatieve functie. Toon aan dat

$$\sum_{d^2|n} f(d)$$

multiplicatief is.

*Oplissing.*

Dit kan uiteraard door rechtstreekse controle. Een conceptueler alternatief: de resultaten uit Opgave 5.36 of Opgave 5.39 zijn niet rechtstreeks toepasbaar aangezien niet gesommeerd wordt over  $f(d^2)$ . We proberen de som om te vormen naar eentje waarbij dat wel het geval is, m.a.w. we willen aantonen dat er een multiplicatieve functie  $g$  bestaat met  $g(n^2) = f(n)$ . Het is straightforward om na te gaan dat  $g(n^2) = f(n)$ , en bijvoorbeeld  $g(n) = 0$  als  $n$  geen kwadraat is (de waarden van  $g$  in niet-kwadraten doen er niet toe), een multiplicatieve functie

<sup>16</sup>Primitiviteit blijft ook behouden onder (willekeurige) oneindige doorsnedes.

definieert (bijv. omdat het de unieke multiplicatieve functie is bepaald door  $g(p^{2n}) = f(p^n)$  en  $g(p^{2n+1}) = 0$ ). We kunnen dit ook inzien m.b.v. Opgave 5.41: we tonen aan dat er een multiplicatieve  $h$  bestaat met  $h \mid \text{id}^\infty$  en  $h(n^2) = n$ ; daaruit volgt dan dat  $g = (f \circ h) \cdot \mathbf{1}_{\text{sq}}$  multiplicatief is. Inderdaad: we kunnen  $h$  terug vastleggen op priem machten. Alternatief:

**Opgave 5.41.** (Samenstelling van multiplicatieve functies) Als  $f$  en  $g$  aritmetische functies zijn en  $g(\mathbb{N}^+) \subset \mathbb{N}^+$ , dan is de samenstelling  $f \circ g$  betekenisvol.

- A. Toon aan dat de samenstelling van multiplicatieve functies niet noodzakelijk multiplicatief is.
- B. Zij  $f$  en  $g$  multiplicatief,  $g(\mathbb{N}^+) \subset \mathbb{N}^+$  en stel dat  $\text{ggd}(a, b) = 1 \implies \text{ggd}(g(a), g(b)) = 1$ . Bewijs dat  $f \circ g$  multiplicatief is.

Noteren we  $a \mid b^\infty$  als een natuurlijk getal  $n$  bestaat met  $a \mid b^n$ , dan geldt i.h.b.: Als  $g(n) \mid n^\infty$  voor alle  $n$  (kort:  $g \mid \text{id}^\infty$ ), dan is  $f \circ g$  multiplicatief.

## Opgaven hoofdstuk 5

**Opgave 5.42.** Op hoeveel manieren kan een natuurlijk getal geschreven worden als product van A

- A. 3 natuurlijke getallen?
- B.  $k \geq 1$  natuurlijke getallen?

Schrijf je resultaten als convolutie.

**Opgave 5.43.** Zij  $f$  een totaal multiplicatieve functie en  $g$  inverteerbaar. Bewijs dat  $(fg)^{-1} = fg^{-1}$ . ✿

**Opgave 5.44.** Bewijs dat voor  $n \geq 1$ , ✿

$$\sum_{d|n} \mu(d)\sigma(d) = (-1)^{\omega(n)} \prod_{p|n} p.$$

**Opgave 5.45.** (Voorbeeld van niet-associativiteit) Aan welke bekende functies zijn ✿ A

$$\sum_{d^2|n} \mu(d) \quad \text{en} \quad \sum_{d^2|n} \mu\left(\frac{n}{d}\right)$$

gelijk?

**Opgave 5.46.** Bewijs voor  $n \geq 1$  dat ✿ H

$$\sum_{d|n} \tau^3(d) = \left( \sum_{d|n} \tau(d) \right)^2.$$

## calculus

Heel wat eigenschappen van de grootste gemene deler zijn eenvoudig te bewijzen wanneer we beschikken over de hoofdstelling van de rekenkunde, d.i., unieke factorisatie in priemfactoren. Unieke factorisatie wordt soms als een ‘zware’ eigenschap beschouwd, en vaak geeft men dan ook de voorkeur aan een bewijs van een zekere eigenschap die niet steunt op unieke ontbinding in priemgetallen.

Hetzelfde geldt voor het bestaan van unieke rest en quotiënt. Dit is in feite wat aan de basis ligt voor de unieke factorisatie, in die zin dat (zonder tot in details te treden) de unieke factorisatie er min of meer rechtstreeks uit volgt.<sup>17</sup> De voorkeur gaat dan ook naar een bewijs dat geen gebruik maakt van het bestaan van rest en quotiënt.

Merk hierbij op dat het bewijs van de stelling van Bézout cruciaal steunt op het bestaan van (unieke) rest en quotiënt. Als we rest en quotiënt laten vallen, laten we maar best ook meteen de stelling van Bézout vallen.

Je kan je afvragen of dit allemaal wel zin heeft, m.a.w., of de definitie van de grootste gemene deler niet steunt op begrippen als ‘rest en quotiënt’ of ‘priemgetal’. Dit is niet het geval: de grootste gemene deler is simpelweg gedefinieerd als de grootste gemeenschappelijke deler. ‘Een deler zijn’ is op zijn beurt gedefinieerd enkel a.d.h.v. de vermenigvuldiging in  $\mathbb{Z}$ .

Omdat er in deze sectie nogal wat ggd’s zullen opduiken voeren we tijdelijk een beknoptere notatie in (die overigens door sommige auteurs altijd wordt gebruikt):

**Notatie 6.1.**

We noteren (tijdelijk) kortweg  $(a, b)$  voor  $\text{ggd}(a, b)$ .

Merk vooraf op dat de grootste gemene deler van twee (of meer) gehele getallen  $a_1, \dots, a_n$  enkel bestaat wanneer minstens één van de getallen niet 0 is. We zullen naar deze voorwaarde kortweg referen als “ $\text{ggd}(a_1, \dots, a_n)$  bestaat”.

Je vraagt je misschien af, nu we zoveel eigenschappen links laten liggen, waar we dan *wel* nog op kunnen steunen. Het antwoord is eenvoudig: praktisch niets. Hoe hard je ook mag proberen, als je iets zinvols zou willen bewijzen zal je hoe dan ook op een of andere manier gebruik maken van rest en quotiënt. Zijn we dan te restrictief? Niet echt. Het probleem zit in de definitie van de grootste gemene deler als de ‘grootste gemeenschappelijke deler’. ‘Grootste’ is een begrip dat met de opgelegde restricties weinig relevantie heeft en waar dus weinig mee valt aan te vangen.<sup>18</sup> Een oplossing bestaat erin de definitie van de grootste

<sup>17</sup>In algebraïsche termen: elk Euclidisch domein is een UFD.

<sup>18</sup>Intuïtief gesproken hebben we de eigenschappen van de natuurlijke orderrelatie op  $\mathbb{Z}$  zopas aan de kant gezet, terwijl de oude definitie van de ggd net gebaseerd is op die orderrelatie. Het is dan ook niet verwonderlijk dat we meer kunnen aanvangen wanneer we onze definitie van de ggd baseren op een andere (partiële) orderrelatie: deelbaarheid!

gemene deler te herzien. Dit kan als volgt: “Als  $a, b \in \mathbb{Z}$  niet beide 0 zijn, dan noemen we  $d$  een grootste gemene deler van  $a$  en  $b$  als  $d$  een gemeenschappelijke deler is van  $a$  en  $b$ , en voor elke gemeenschappelijke deler  $c$  van  $a$  en  $b$  geldt dat  $c \mid d$ .” Een equivalente manier om dit te formuleren is: “ $d$  is een grootste gemene deler van  $a$  en  $b$  als en slechts als voor alle  $c \in \mathbb{Z}$  geldt dat  $c \mid a, b$  als en slechts als  $c \mid d$ .”

Deze definitie roept toch enkele vragen op:

- Als we de ggd op deze manier definiëren, kunnen we dan besluiten dat  $\text{ggd}(a, b)$  altijd bestaat als  $a$  en  $b$  niet beide 0 zijn?
- Als er een grootste gemene deler bestaat, is die dan uniek?

Het antwoord op de eerste vraag is negatief: om met deze definitie aan te tonen dat een grootste gemene deler van  $a$  en  $b$  bestaat moet je toch weer gebruik maken van rest of quotiënt of andere structurele eigenschappen van  $\mathbb{Z}$  die we hier niet wensen te gebruiken. We zullen er daarom vanaf nu zonder meer van uit gaan dat er steeds een grootste gemene deler bestaat, *maar steunen op geen enkele andere eigenschap van ggd's!*

**Axioma 6.2.**

Als  $a, b \in \mathbb{Z}$  niet beide 0 zijn, dan bestaan een grootste gemene deler van  $a$  en  $b$ .

Deze aanname lijkt misschien dubieus of verwarrend; het punt is dat het voortbouwen op dit alternatief stel axioma's een heel andere en op unieke manier waardevolle theorie met zich meebrengt.<sup>19</sup>

Het antwoord op de tweede vraag is dan weer positief, of toch in zekere zin:

**Opgave 6.3.** Toon aan dat, met de nieuwe definitie van een grootste gemene deler, een grootste gemene deler van  $a, b \in \mathbb{Z}$  (niet beide 0) uniek is op het teken na. H

Merk terloops op dat we heel bewust “*een* grootste gemene deler” en niet “*de* grootste gemene deler” zeggen. We gebruiken vanaf nu het lidwoord “de” om aan te geven dat het om de positieve grootste gemene deler gaat.

**Opgave 6.4.** (Commutativiteit) Bewijs dat  $(a, b) = (b, a)$  voor alle  $a, b \in \mathbb{Z}$  indien  $(a, b)$  bestaat.

**Opgave 6.5.** Bewijs dat  $(a, 1) = 1$  voor alle  $a \in \mathbb{Z}$ .

We bekijken een aantal meer interessante eigenschappen. Een typische eigenschap van de grootste gemene deler die niet steunt op alles wat we hier als taboe beschouwen, is de zogeheten distributiviteit.

## 6.1 Distributiviteit

<sup>19</sup>In de algebra wordt men soms geconfronteerd met structuren waarin enkel het *bestaan* van een ggd is gegarandeerd, en alles wat we in dit hoofdstuk aan gekkenwerk doen is dan rechtstreeks overdraagbaar.

**Eigenschap 6.6.** Distributieve eigenschap van de ggd

Zij  $z \in \mathbb{Z}_0$  en stel dat  $(a, b)$  bestaat. Dan is  $(az, bz) = |z| \cdot (a, b)$ .

*Bewijs.*

Merk op dat  $\frac{(az, bz)}{|z|} \in \mathbb{Z}$  aangezien  $z \mid az, bz$ . We bewijzen dat  $\frac{(az, bz)}{|z|}$  en  $(a, b)$  dezelfde delers hebben; in dat geval zijn ze gelijk (want beide zijn positief):

$$d \mid \frac{(az, bz)}{|z|} \Leftrightarrow dz \mid (az, bz) \Leftrightarrow dz \mid az \text{ en } dz \mid bz \Leftrightarrow d \mid a \text{ en } d \mid b \Leftrightarrow d \mid (a, b).$$

□

Om de voorwaarde dat de ggd bestaat niet steeds te moeten meezeulen beschouwen we vanaf nu enkel gehele getallen die niet 0 zijn. Het loont de moeite om bij de eigenschappen toch even stil te staan wat er verandert indien bepaalde optredende variabelen 0 worden.

**Gevolg 6.7.**

Stel dat  $(a, b) = 1$  en  $a \mid bc$ , dan is  $a \mid c$ .

*Bewijs.*

Vroeger hebben we dit als volgt bewezen: Omdat  $(a, b) = 1$  bestaan er  $x$  en  $y$  zo dat  $ax + by = 1$ .

Dus  $axc + byc = c$ . Omdat  $a \mid bc$  is  $a \mid c$ .

Gebruik makend van de distributieve eigenschap kan dit heel wat korter (en zonder gebruik te maken van de stelling van Bézout):

$$a \mid bc \Rightarrow a \mid (bc, ac) = (a, b) \mid c = |c|.$$

□

## 6.2 Associativiteit

**Eigenschap 6.8.** Associatieve eigenschap van de ggd

Zij  $a, b, c \in \mathbb{Z}_0$ . Dan is  $(a, (b, c)) = ((a, b), c)$ .

(Merk op dat  $(a, b) \neq 0 \neq (b, c)$  zodat  $(a, (b, c))$  en  $((a, b), c)$  bestaan. Deze “sanity check” zullen we voortaan niet steeds meer uitvoeren; we laten ze over aan de kritische lezer.)

*Bewijs.*

We hebben

$$\begin{aligned} d \mid (a, (b, c)) &\Leftrightarrow d \mid a \text{ en } d \mid (b, c) \\ &\Leftrightarrow d \mid a \text{ en } (d \mid b \text{ en } d \mid c) \\ &\Leftrightarrow (d \mid a \text{ en } d \mid b) \text{ en } d \mid c \\ &\Leftrightarrow d \mid (a, b) \text{ en } d \mid c \\ &\Leftrightarrow d \mid ((a, b), c). \end{aligned}$$

□



**Gevolg 6.9.**

Als  $(a, b) = 1$ , dan is  $(ac, b) = (c, b)$ .

*Bewijs.*

Met behulp van associativiteit en distributiviteit vinden we:

$$(ac, b) = (ac, b \cdot (c, 1)) = (ac, (bc, b)) = ((ac, bc), b) = (c \cdot (a, b), b) = (c, b).$$

□

**Gevolg 6.10. Multiplicativiteit van de ggd**

Als  $(a, b) = 1$ , dan is  $(ab, c) = (a, c)(b, c)$ .

*Bewijs.*

Met behulp van associativiteit en distributiviteit vinden we:

$$\begin{aligned} (a, c)(b, c) &= (a \cdot (b, c), c \cdot (b, c)) \\ &= ((ab, ac), (bc, c^2)) \\ &= (ab, (ac, (bc, c^2))) \\ &= (ab, ((ac, bc), c^2)) \\ &= (ab, (c, c^2)) \\ &= (ab, c). \end{aligned}$$

□

Een verrassende toepassing van de multiplicativiteit is de volgende:

**Gevolg 6.11.**

Stel dat  $a \mid c$ ,  $b \mid c$  en  $(a, b) = 1$ , dan is  $ab \mid c$ .

*Bewijs.*

$a \mid (a, c)$  en  $b \mid (b, c)$ , dus  $ab \mid (a, c)(b, c) = (ab, c)$  zodat  $ab \mid c$ .

□

**6.3 De ggd van meerdere getallen**

In het bewijs van de associatieve eigenschap zien we dat  $d = ((a, b), c)$  een getal is met de eigenschap dat  $e \mid d \Leftrightarrow e \mid a, b, c$ . Als we dus een grootste gemene deler van meerdere getallen definiëren als in

**Definitie 6.12.**

We noemen  $d \in \mathbb{Z}$  een grootste gemene deler van  $a_1, \dots, a_n$  (niet allen 0) indien  $e \mid d \Leftrightarrow e \mid a_1, \dots, a_n$ .

dan zien we dat zo'n grootste gemene deler inderdaad bestaat voor  $n = 3$ : indien bijvoorbeeld  $a \neq 0$  is  $d = ((a, b), c)$  een kandidaat-ggd. Indien  $a = b = 0$  maar  $c \neq 0$  kunnen we  $d = (a, (b, c))$  nemen.

**Opgave 6.13.** Toon aan dat een grootste gemene deler van meerdere getallen (volgens de nieuwe definitie), indien die bestaat, uniek is op het teken na.

**Notatie 6.14.**

We noteren  $(a_1, \dots, a_n)$  voor de unieke positieve grootste gemene deler van  $a_1, \dots, a_n$ .

Voor twee getallen hebben we in deze nieuwe beschouwing axiomatisch aangenomen dat een ggd bestaat. We zouden dit nu opnieuw kunnen aannemen voor meerdere getallen, met een hoop extra axioma's tot gevolg. Dit blijkt (gelukkig) niet nodig:

**Opgave 6.15.** Indien  $a_1, \dots, a_n \in \mathbb{Z}$  niet allen 0 zijn, toon aan dat ze een grootste gemene deler hebben.

Uit het bewijs van de associatieve eigenschap blijkt dat  $(a, (b, c)) = (a, b, c) = ((a, b), c)$ .

**Opgave 6.16.** Probeer in te zien waarom meer algemeen geldt dat we extra ggd-haakjes binnen ggd-haakjes mogen negeren zonder dat het resultaat wijzigt.

**Opgave 6.17.** Overtuig jezelf ervan dat de distributieve eigenschap ook geldig is voor meerdere variabelen, in de vorm:

$$(za_1, \dots, za_n) = |z| \cdot (a_1, \dots, a_n).$$

## 6.4 Additieve notatie

**Notatie 6.18.**

We noteren  $a \dot{+} b = (a, b)$ ,  $a \dot{+} b \dot{+} c = (a, b, c)$  en analoog voor meer variabelen.

Hiermee wordt de distributieve eigenschap:

$$(a \dot{+} b)c = ac \dot{+} bc$$

en de associatieve eigenschap:

$$(a \dot{+} b) \dot{+} c = a \dot{+} b \dot{+} c = a \dot{+} (b \dot{+} c)$$

De grootste gemene deler gedraagt zich dus als een optelling! Of toch bijna, want we hebben ook de minder natuurlijke rekenregels

$$a \dot{+} 1 = 1 \quad \text{en} \quad a \dot{+} a = |a| \quad \forall a \in \mathbb{Z}_0.$$

Let dus op en laat je niet verleiden om bijvoorbeeld  $3a \dot{+} 3b$  te herschrijven als  $(a \dot{+} a \dot{+} a) \dot{+} (b \dot{+} b \dot{+} b) = a \dot{+} b$ :  $3a$  is immers helemaal niet hetzelfde als  $a \dot{+} a \dot{+} a$ .

**Opgave 6.19.** Werk de haakjes weg, er voor het gemak van uitgaande dat alle getallen verschillend zijn van 0: A

- A.  $(a \dot{+} b)(c \dot{+} d)$
- B.  $(a \dot{+} b \dot{+} c)(d \dot{+} e)$
- C.  $(a \dot{+} b)^2$
- D.  $(a \dot{+} b)^3$

## 6.5 Freshman's dream voor ggd's

**Lemma 6.20.**

Indien  $(a, b)$  bestaat is  $(a \dot{+} b)^n = a^n \dot{+} a^{n-1}b \dot{+} \dots \dot{+} ab^{n-1} \dot{+} b^n$ .

**Opgave 6.21.** Bewijs als oefening.

H

**Eigenschap 6.22.** Freshman's dream voor ggd's

Voor  $n \in \mathbb{N}^+$  en  $a, b \in \mathbb{Z}_0$  is

$$(a \dot{+} b)^n = a^n \dot{+} b^n.$$

*Bewijs.*

Wegens het voorgaande lemma, distributiviteit en commutativiteit hebben we:

$$\begin{aligned} (a \dot{+} b)^{2n} &= a^{2n} \dot{+} a^{2n-1}b \dot{+} \dots \dot{+} ab^{2n-1} \dot{+} b^{2n} \\ &= a^n(a^n \dot{+} a^{n-1}b \dot{+} \dots \dot{+} ab^{n-1} \dot{+} b^n) \dot{+} b^n(a^n \dot{+} a^{n-1}b \dot{+} \dots \dot{+} ab^{n-1} \dot{+} b^n) \\ &= (a^n \dot{+} b^n) \cdot (a^n \dot{+} a^{n-1}b \dot{+} \dots \dot{+} ab^{n-1} \dot{+} b^n) \\ &= (a^n \dot{+} b^n)(a \dot{+} b)^n. \end{aligned}$$

Links en rechts delen door (het niet-0 getal)  $(a \dot{+} b)^n$  levert  $(a \dot{+} b)^n = a^n \dot{+} b^n$ .  $\square$

Dit bewijs komt wellicht over als hocus-pocus. Om dit te compenseren, en als afsluiter van dit hoofdstuk, presenteren we nog enkele alternatieve bewijzen van freshman's dream voor ggd's.

Merk vooraf op dat het wegens  $(za, zb) = |z|(a, b)$  volstaat om te bewijzen dat indien  $(a, b) = 1$ , dan  $(a^n, b^n) = 1$ . Stel dus dat  $a, b \in \mathbb{Z}$  en  $(a, b) = 1$ .

*Bewijs.*

We gebruiken het resultaat van Gevolg 6.9: als  $(a, b) = 1$  is  $(ac, b) = (c, b)$ . Passen we dit toe met  $c = a$ , dan hebben we  $(a^2, b) = 1$ . Daarom is (opnieuw wegens het gevolg)  $(a^2, b^2) = (a^2, b \cdot b) = (a^2, b) = 1$ . Omdat  $b$  copriem is met  $a^2$ , kunnen we nog een factor  $b$  toevoegen zonder dat de ggd wijzigt:  $(a^2, b^3) = 1$ . Het veralgemenen van deze techniek tot een bewijs laten we als oefening.  $\square$

**Opgave 6.23.** Stel dat  $(a, b) = 1$ . Gebruik bovenstaande suggestie om aan te tonen dat  $(a^n, b^m) = 1$  voor alle  $m, n > 0$ . H

De volgende bewijzen passen niet echt in deze sectie omdat ze gebruik maken van de stelling van Bézout, maar omwille van hun elegantie kunnen ze we niet achterhouden:

*Bewijs.*

Wegens Bézout vinden we  $x, y \in \mathbb{Z}$  met  $ax + by = 1$ . Verheffen we dit tot de  $2n - 1$ -de macht (elke hogere exponent werkt ook) en werken we alles uit, dan staat er in het linkerlid een aantal termen met een factor  $a^n$  en een aantal termen met een factor  $b^n$ . We krijgen dus een lineaire combinatie van  $a^n$  en  $b^n$  die 1 is, dus  $(a^n, b^n) = 1$ .  $\square$

Nog een laatste alternatief bewijs van freshman's dream.

*Bewijs.*

Het is niet zo moeilijk om in te zien (bijvoorbeeld zoals in een van de vorige bewijzen) dat indien  $(a, b) = 1$ , dan ook  $(a^2, b^2) = 1$ . Per inductie volgt dan meteen dat  $(a^{2^m}, b^{2^m}) = 1$  voor  $m \geq 0$ . Er bestaan dus  $x, y \in \mathbb{Z}$  met  $a^{2^m}x + b^{2^m}y = 1$ . Kiezen we  $m$  zo groot dat  $2^m > n$ , dan staat hier een lineaire combinatie van  $a^n$  en  $b^n$  die 1 is:  $a^n \cdot a^{2^m-n}x + b^n \cdot b^{2^m-n}y = 1$ . Dus  $(a^n, b^n) = 1$  wegens Bézout.  $\square$

## 7.1 Congruentie

### Definitie 7.1. Congruentie

Twee gehele getallen  $a$  en  $b$  zijn *congruent modulo* een geheel getal  $c$  als ze dezelfde rest hebben bij deling door  $c$ . We noteren  $a \equiv b \pmod{c}$ . Het getal  $c$  wordt de *modulus* van de congruentie genoemd.

We zeggen “ $a$  is congruent met  $b$  modulo  $c$ ”, “ $a$  en  $b$  zijn congruent modulo  $c$ ” of korter, “ $a$  is  $b$  modulo  $c$ ”. Indien  $a$  en  $b$  niet congruent zijn noteren we  $a \not\equiv b$ .

Bijvoorbeeld:  $5 \equiv 17 \pmod{3}$ ,  $8 \equiv 12 \pmod{4}$ . Indien de modulus uit de context duidelijk is zegt men kort “ $a$  is congruent met  $b$ ” en noteert men  $a \equiv b$  zonder  $c$  te vermelden. Ook samenstellingen van gelijkheden en congruenties worden gebruikt, bijvoorbeeld

$$(-2)^2 = 4 \equiv 1 = (-1)^2 \equiv 7 \pmod{3}.$$

Als een getal  $a$  deelbaar is door  $c$  kunnen we wegens Eigenschap 1.16 noteren  $a \equiv 0 \pmod{c}$ .

### Definitie 7.2. Restklasse

Een restklasse modulo een geheel getal  $c$  is een verzameling van alle gehele getallen die bij deling door  $c$  dezelfde rest hebben, of dus congruent zijn modulo  $c$ .

Er zijn precies  $|c|$  restklassen modulo  $c$ . Het begrip ‘restklasse’ zal in voorlopig niet tot zijn volledige recht komen.<sup>20</sup> Vaak is het gewoon een handig woord om beknopt iets uit te drukken.

<sup>20</sup>In deel 2 bekijken we de restklassen als objecten op zichzelf. Verassend genoeg blijkt deze licht verschillende invalshoek heel wat krachtiger te zijn.

**Stelling 7.3.** Eigenschappen van congruenties

De volgende eigenschappen gelden voor congruenties modulo  $c$ .

1.  $a \equiv b$  als en slechts als  $a - b \equiv 0$ .
2. Als  $a \equiv b$  en  $d \equiv e$ , dan is  $a + d \equiv b + e$ .
3. Als  $a \equiv b$ , dan  $na \equiv nb$  voor elk geheel getal  $n$ .
4. Als  $a \equiv b$  en  $d \equiv e$ , dan geldt  $ad \equiv be$ .
5. Als  $a \equiv b$  dan is  $a^n \equiv b^n$  voor elk natuurlijk getal  $n > 0$ .

*Bewijs.*

We bewijzen alleen de eerste eigenschap en laten de rest als oefening.

Het bewijs bestaat uit twee delen.

Deel 1: als  $a \equiv b \pmod{c}$  dan  $a - b \equiv 0 \pmod{c}$ .

Stel  $a = q_1c + r_1$  en  $b = q_2c + r_2$  met  $0 \leq r_1, r_2 < |c|$ . Omdat  $a \equiv b \pmod{c}$  weten we dat  $r_1 = r_2$ , want dat volgt uit de definitie van congruentie. Dan is  $a - b = q_1c - q_2c = (q_1 - q_2)c$ . Dus  $a - b \equiv 0 \pmod{c}$ .

Deel 2: als  $a - b \equiv 0 \pmod{c}$  dan  $a \equiv b \pmod{c}$ .

Omdat  $a - b \equiv 0 \pmod{c}$  is  $a - b = kc$ . Stel  $a = qc + r$  met  $0 \leq r < |c|$ . Dan is  $b = a - kc = (q - k)c + r$ .  $b$  heeft dus dezelfde rest als  $a$ , dus  $a \equiv b \pmod{c}$ .  $\square$

Het is belangrijk om te weten dat het congruentiesymbool niets meer is dan een korte notatie. Het kan vaak handig zijn om deze notatie te verlaten en  $a \equiv b \pmod{c}$  te schrijven als  $a = b + kc$ . Het schrijven in de vorm  $a = b + kc$  noemen we “verborgen modulo rekenen”. Merk op dat Stelling 7.3.1 toelaat om dit te doen, omdat  $a \equiv b$  equivalent is met  $a - b \equiv 0$  en dus met  $c \mid a - b$ .

**Opgave 7.4.** Bewijs zelf eigenschappen 2 tot en met 5.

**Opgave 7.5.** Toon telkens aan met een voorbeeld dat het omgekeerde van de eigenschappen 2, 3, 4 en 5 niet steeds waar is.

**Voorbeeld 7.6.** Bereken de rest bij deling van  $25 \cdot 8^9$  door 7 en zeg steeds welke eigenschappen je gebruikt.

*Oplossing.*

Er geldt dat  $25 \equiv 4 \pmod{7}$ . Nu berekenen we  $8^9 \pmod{7}$ . Er geldt dat  $8 \equiv 1 \pmod{7}$ , dus wegens eigenschap 5 geldt  $8^9 \equiv 1^9 \pmod{7}$ , dus  $8^9 \equiv 1 \pmod{7}$ .

Uit eigenschap 3 volgt nu  $25 \cdot 8^9 \equiv 4 \cdot 1 \pmod{7}$ . De uiteindelijke rest zal dus 4 zijn.

**Opgave 7.7.** Bereken de rest bij deling door 3 van

- A.  $77 \cdot 88$
- B.  $25^4$
- C.  $-11^{10}$
- D.  $31^{32} \cdot 32^{31}$

en zeg steeds welke eigenschappen je gebruikt.

*Opmerking.*

Je wordt uitdrukkelijk gevraagd om bij te houden welke eigenschappen je gebruikt. Dat is omdat je goed zou weten waar je precies mee bezig bent en een idee krijgt van hoe je de eigenschappen kan gebruiken. En vooral, dat je geen eigenschappen uit je mouw schudt.

**Opgave 7.8.** Bereken de rest van  $2014^{2015}$  bij deling door

- A. 7
- B. -8
- C. -9
- D. 10

en zeg ook hier steeds welke eigenschappen je gebruikt.

**Opgave 7.9.** Bepaal het kleinste natuurlijk getal  $n$  zo dat  $\frac{9^{20}+n}{41}$  een natuurlijk getal is.

**Voorbeeld 7.10.** Bereken  $4^{12} \bmod 12$ .

*Oplossing.*

We bekijken eerst  $4^2 \bmod 12$ , wat gelijk is aan 4. Er geldt dus dat  $4^2 \equiv 4 \pmod{12}$ . Dus ook  $4^3 = 4^2 \cdot 4 \equiv 4 \cdot 4 = 4^2 \equiv 4 \pmod{12}$ . Dit kunnen we analoog uitbreiden voor grotere exponenten, en we kunnen dus besluiten dat  $4^n \equiv 4 \pmod{12}$  voor elk natuurlijk getal  $n > 0$ . Dus ook  $4^{12} \equiv 4 \pmod{12}$ .

*Opmerking.*

Als we streng zijn hadden we  $4^n \equiv 4 \pmod{12}$  moeten bewijzen via inductie, maar omdat het hier zo vanzelfsprekend is lieten we dat even weg. Hou dus wel in gedachten dat het 'analoog uitbreiden' een vorm van inductie is, en dat je in principe bij zo'n werkwijze moet vermelden dat je het met inductie kan bewijzen.

Met dit voorbeeld heb je nog een extra techniek om modulair te rekenen. Er zijn natuurlijk nog heel wat andere manieren, maar van zodra je wat inzicht hebt verkregen in het modulo rekenen zal je die vanzelf ontdekken.

**Opgave 7.11.** Bereken

- A.  $3^8 \bmod 6$ .
- B.  $9^{20} \bmod (-36)$ .
- C.  $5^{32} \bmod 40$ .
- D.  $7^{2000} \bmod (-42)$ .

**Opgave 7.12.** Bewijs dat een natuurlijk getal deelbaar is door 9 als en slechts als de som van H zijn cijfers deelbaar is door 9.

**Opgave 7.13.** Stel  $a \neq b$ . Bewijs dat voor  $n > 0$  geldt dat  $a^n - b^n$  deelbaar is door  $a - b$ , zonder H gebruik te maken van de algemene ontbinding van  $a^n - b^n$ .

**Lemma 7.14.**

$a \equiv b \pmod{c}$  is equivalent met  $ad \equiv bd \pmod{cd}$  voor elk geheel getal  $d \neq 0$ .

*Bewijs.*

$a \equiv b \pmod{c}$  is gelijkwaardig met  $a - b = kc$ , wat gelijkwaardig is met  $ad - bd = kcd$  en dus met  $ad \equiv bd \pmod{cd}$ .  $\square$

Merk op dat dit zo'n situatie is waar het verborgen modulo rekenen zijn voordelen heeft. Verborgen modulo rekenen komt van pas bij het veranderen van de modulus, zoals in bovenstaande eigenschap. Doorgaans zal je daarmee, of met een van de volgende resultaten wel op weg kunnen:

**Opgave 7.15.** Stel dat  $x \equiv y \pmod{n}$  en  $d \mid n$ . Bewijs dat  $x \equiv y \pmod{d}$ .

**Opgave 7.16.** Gegeven zijn getallen  $m, n, x, y$  waarvoor  $x \equiv y \pmod{n}$  en  $x \equiv y \pmod{m}$ . Toon aan dat  $x \equiv y \pmod{\text{kgv}(m, n)}$ .

**Opgave 7.17.** Bewijs dat er oneindig veel priemgetallen van de vorm  $4k + 3$  bestaan.

**Opgave 7.18.** Bewijs dat er oneindig veel priemgetallen van de vorm  $6k + 5$  bestaan.

## 7.2 Inverteerbaarheid

In congruenties kunnen we bijna alles doen wat we ook met gelijkheden mogen doen: optellen, vermenigvuldigen en machtsverheffen. Wat nog ontbreekt is delen en "worteltrekken". Het begrip *inverse* biedt een goed alternatief voor het "delen".

**Definitie 7.19.** Inverteerbaar

Een getal  $x$  noemen we een *inverse* van  $a$  modulo  $b$  als  $ax \equiv 1 \pmod{b}$ . We noteren  $x \equiv a^{-1}$ . Indien  $a$  een inverse heeft noemen we  $a$  *inverteerbaar* modulo  $b$ .

Bijvoorbeeld, 5 is een inverse van 8 modulo 13 want  $5 \cdot 8 = 40 \equiv 1 \pmod{13}$ . Maar merk op dat ook bijvoorbeeld  $5 + 13 = 18$  en  $5 - 13 = -8$  inversen zijn van 5 modulo 13. Een inverse is dus, als ze bestaat, zeker niet uniek.

Er geldt

$$ax \equiv 1 \pmod{b} \Leftrightarrow ax = 1 - yb \Leftrightarrow ax + by = 1$$

voor een zekere  $y \in \mathbb{Z}$ . Het bestaan van een inverse is dus equivalent aan het bestaan van oplossingen van de Diophantische vergelijking

$$ax + by = 1 \tag{1}$$

in  $x$  en  $y$ . De volgende stelling volgt daarom onmiddellijk uit Stelling 1.39.



**Stelling 7.20.** Criterium voor inverteerbaarheid

$a$  heeft een inverse modulo  $b$  als en slechts als  $\text{ggd}(a, b) = 1$ . Alle inversen van  $a$  zijn bovendien onderling congruent modulo  $b$ .

Het vinden an een inverse is dus equivalent aan het oplossen van een lineaire Diophantische vergelijking. Omdat we daar een algemene methode voor hebben, hebben we meteen ook een methode om een inverse te vinden.

**Lemma 7.21.** Schrappingswet voor congruenties

Als  $\text{ggd}(d, m) = 1$ , dan is  $x \equiv y \pmod{m}$  equivalent met  $dx \equiv dy \pmod{m}$ .

Met andere woorden, we mogen links en rechts ‘delen’ door  $d$  op voorwaarde dat  $d$  een inverse heeft. Hetzelfde geldt niet steeds als  $d$  geen inverse heeft. Zo is bijvoorbeeld  $2 \cdot 3 \equiv 2 \cdot 5 \pmod{4}$ , maar  $3 \not\equiv 5 \pmod{4}$ .

*Bewijs.*

Er geldt  $x \equiv y \pmod{m} \Leftrightarrow m \mid x - y$ . Als  $\text{ggd}(d, m) = 1$  is dit op zijn beurt equivalent met  $m \mid d(x - y) \Leftrightarrow dx \equiv dy \pmod{m}$ .  $\square$

Een alternatief bewijs gebruikt wat we ondertussen weten over inverteerbaarheid:

*Bewijs.*

Als  $x \equiv y \pmod{m}$ , dan is uiteraard  $dx \equiv dy \pmod{m}$  (eigenschap 3 van congruenties). Veronderstel nu omgekeerd dat  $dx \equiv dy \pmod{m}$ . Aangezien  $\text{ggd}(d, m) = 1$  heeft  $d$  een inverse modulo  $m$ , zeg  $e$ . Uit  $dx \equiv dy$  volgt dat  $edx \equiv edy$  zodat  $1 \cdot x \equiv 1 \cdot y$  (eigenschap 4), dus  $x \equiv y$ .  $\square$

### 7.3 Lineaire congruenties

**Voorbeeld 7.22.** Vind alle  $n \in \mathbb{N}$  met  $0 \leq n < 17$  zo dat  $6n \equiv 8 \pmod{17}$ .

*Oplossing.*

6 heeft een inverse modulo 17, bijvoorbeeld 3. Wegens eigenschap 3 van congruenties geldt dat  $3 \cdot 6n \equiv 3 \cdot 8 \pmod{17}$ , dus  $n \equiv 24 \pmod{17}$ . Dan moet  $n = 24 \pmod{17} = 7$ .

We kunnen dus de inverse van  $a$  gebruiken, indien die bestaat, om (2) op te lossen. Indien men de inverse zomaar kan bedenken is het oplossen van (2) dus helemaal niet moeilijk. Lemma 7.21 zegt dat de bekomen congruentie inderdaad equivalent is aan de oorspronkelijke. Als we een vergelijking, zeg  $6n = 8$  oplossen, dan delen we links en rechts door 6. Wat we eigenlijk doen is links en rechts vermenigvuldigen met  $\frac{1}{6}$ :

$$6n = 8 \Leftrightarrow \frac{1}{6} \cdot 6n = \frac{1}{6} \cdot 8 \Leftrightarrow n = \frac{8}{6}.$$

Dat is ook wat we doen bij congruenties, het enige verschil is dat de inverse van een getal nu afhangt van de modulus:

$$6n \equiv 8 \Leftrightarrow 6^{-1} \cdot 6n \equiv 6^{-1} \cdot 8 \Leftrightarrow n \equiv 6^{-1} \cdot 8 \pmod{17}.$$

Vandaar de volgende notatie:

**Notatie 7.23.**

Indien  $\text{ggd}(a, m) = 1$  noteren we  $\frac{1}{a}$  voor  $a^{-1}$  in congruenties modulo  $m$ . Ook schrijven we  $\frac{b}{a}$  in plaats van  $b \cdot a^{-1}$ .

Indien  $\text{ggd}(a, m) = 1$  is dit perfect toegestaan. De inverse is immers uniek modulo  $m$ , dus hebben de notaties  $\frac{1}{a}$  en  $\frac{b}{a}$  geen dubbelzinnige betekenis. We veralgemenen ook nog de notatie  $a^{-1}$ :

**Notatie 7.24.**

Indien  $\text{ggd}(a, m) = 1$  en  $n \in \mathbb{N}^+$  noteren we  $a^{-n}$  voor  $(a^{-1})^n$  in congruenties modulo  $m$ .

De volgende lemma's volgen onmiddellijk uit de definitie.

**Lemma 7.25.**

Als  $a$  inverteerbaar is, dan ook  $a^{-1}$  en  $(a^{-1})^{-1} \equiv a$ .

**Lemma 7.26.**

$a$  en  $b$  zijn inverteerbaar als en slechts  $ab$  inverteerbaar is. In dat geval is

$$(ab)^{-1} \equiv a^{-1}b^{-1}.$$

Dit drukt onder andere uit dat we breuken mogen vermenigvuldigen door tellers en noemers te vermenigvuldigen, immers,

$$\frac{a}{b} \cdot \frac{c}{d} \equiv a \cdot b^{-1} \cdot c \cdot d^{-1} \equiv ac \cdot (bd)^{-1} \equiv \frac{ac}{bd}.$$

Zo is ook

$$\frac{1}{\frac{1}{a}} \equiv \frac{1}{a^{-1}} \equiv (a^{-1})^{-1} \equiv a.$$

De volgende gevolgen voelen heel natuurlijk aan.

**Gevolg 7.27.**

Er geldt dat  $a^{-n} \equiv (a^n)^{-1} \pmod{m}$  als  $n \in \mathbb{N}$  en  $\text{ggd}(a, m) = 1$ .

**Gevolg 7.28.**

Als  $\text{ggd}(a, m) = 1$  geldt dat  $a^x \cdot a^y \equiv a^{x+y}$  en  $(a^x)^y \equiv a^{xy} \pmod{m}$  voor alle  $x, y \in \mathbb{Z}$ .

Analoog aan lineaire Diophantische vergelijkingen hebben we lineaire congruenties.

**Definitie 7.29.** Lineaire congruentie

Een *lineaire congruentie* is een congruentie van de vorm

$$ax \equiv b \pmod{c} \quad (2)$$

waarbij  $a$ ,  $b$  en  $c$  constant zijn en we oplossingen in gehele getallen zoeken voor  $x$ .

Als  $x_0$  een oplossing is van de lineaire congruentie (2) kunnen we een hele verzameling oplossingen vinden door bij  $x$  een veelvoud van  $c$  op te tellen. We zullen ons daarom beperken tot oplossingen in het interval  $[0, |c| - 1]$ . Omdat we zo de vergelijking reduceren tot de resten modulo  $c$ , zeggen we dat we “oplossingen zoeken modulo  $c$ ”. Een oplossing modulo  $c$  ligt dus steeds in dat interval. We “delen de algemene oplossing door  $c$ ”.

**Stelling 7.30.**

De lineaire congruentie (2) heeft oplossingen als en slechts als  $\text{ggd}(a, c) \mid b$ . Indien er een oplossing is, dan zijn er precies  $\text{ggd}(a, c)$  oplossingen modulo  $c$ .

*Bewijs.*

Het vinden van oplossingen van (2) is equivalent aan het vinden van oplossingen van

$$ax + cy = b. \quad (3)$$

Wegens Stelling 1.39 is er een oplossing als en slechts als  $\text{ggd}(a, c) \mid b$ . Indien er een oplossing  $x_0$  is, dan wordt de algemene oplossing gegeven door  $x_0 + \frac{kc}{d}$  met  $d = \text{ggd}(a, c)$ . Omdat we enkel geïnteresseerd zijn in de  $x$  in het interval  $[0, c - 1]$  zal  $k \in \{1, \dots, d\}$ , na reductie modulo  $c$  alle verschillende oplossingen geven modulo  $c$ . Er zijn precies  $d$  zo'n waarden voor  $k$ .  $\square$

Als  $a$  geen inverse heeft kan de congruentie via Lemma 7.14 gereduceerd worden tot een congruentie waarin dat wel het geval is:

**Voorbeeld 7.31.** Vind alle natuurlijke getallen  $0 \leq n < 12$  met  $9n \equiv 6 \pmod{12}$ .

*Oplossing.*

Er geldt dat  $3n \equiv 2 \pmod{4}$  als en slechts als  $9n \equiv 6 \pmod{12}$ , want  $3n = 4k + 2$  als en slechts als  $9n = 12k + 6$ .

We zoeken nu een inverse van 3 modulo 4, bijvoorbeeld 3. Dan geldt  $3 \cdot 3n \equiv 2 \cdot 3 \pmod{4}$ , of dus  $n \equiv 2 \pmod{4}$ .

Omdat  $0 \leq n < 12$  zijn de oplossingen dus 2, 6, 10.

*Opmerking.*

Om de congruentie te vereenvoudigen gingen we over op verborgen modulo rekenen. Hier merk je dus dat je, soms, niet of moeilijk verder geraakt als je bij de nieuwe notatie blijft.

## 7.4 Stelsels congruenties: de Chinese reststelling (CRS)

Net zoals er stelsels van vergelijkingen zijn, zijn er ook stelsels van congruenties. De *Chinse reststelling* bespreekt de oplossingen van zo'n stelsel.

**Stelling 7.32.** Chinese reststelling

Als  $m_1, m_2, \dots, m_n$  paarsgewijs relatief priem gehele getallen zijn, en  $a_1, a_2, \dots, a_n$  zijn willekeurige gehele getallen, dan bestaan er oneindig veel  $x \in \mathbb{Z}$  zo dat  $x \equiv a_k \pmod{m_k}$  voor elke  $k$ . Alle oplossingen voor  $x$  zijn bovendien congruent modulo  $m_1 m_2 \cdots m_n$ .

**Voorbeeld 7.33.** We nemen het drietal gehele getallen  $(m_1, m_2, m_3) = (3, 5, -8)$  die paarsgewijs relatief priem zijn, en de gehele getallen  $(a_1, a_2, a_3) = (4, 0, 2)$ . We hebben nog geen systematische manier om een getal te vinden dat voldoet, maar na even zoeken vinden we dat 10 voldoet aan de drie voorwaarden:  $10 \equiv 4 \pmod{3}$ ,  $10 \equiv 0 \pmod{5}$  en  $10 \equiv 2 \pmod{-8}$ .

**Opgave 7.34.** (Chinese reststelling) Stel  $y = m_1 m_2 \cdots m_n$ .

A. Toon aan dat voor elke  $k$  er getallen  $p_k$  en  $q_k$  bestaan zo dat  $p_k m_k + \frac{q_k y}{m_k} = 1$ .

Stel nu  $r_k = \frac{q_k y}{m_k}$ .

B. Toon aan dat  $r_k \equiv 1 \pmod{m_k}$  en dat  $r_k \equiv 0 \pmod{m_l}$  als  $k \neq l$ .

C. Toon aan dat  $x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$  voldoet aan de voorwaarde.

D. Toon aan dat er oneindig veel oplossingen zijn voor  $x$ .

Vervolgens bewijzen we dat alle oplossingen voor  $x$  congruent zijn modulo  $y$ . Zij  $x_1$  en  $x_2$  twee oplossingen.

E. Toon aan dat  $m_k \mid x_1 - x_2$  voor elke  $k$ .

F. Toon aan dat  $x_1 \equiv x_2 \pmod{y}$ .

Dit bewijs schetst meteen ook het algoritme voor het vinden van oplossingen. We stellen  $y = m_1 \cdots m_n$  en  $M_k = \frac{y}{m_k}$ . Aangezien  $\text{ggd}(m_k, M_k) = 1$  heeft elke  $M_k$  een inverse  $q_k$  modulo  $m_k$ . Een oplossing wordt dan gegeven door

$$x = \sum_{k=1}^n a_k q_k M_k.$$

**Opgave 7.35.** Toon aan dat er voor elk natuurlijk getal  $n > 0$  een getal  $m$  bestaat zo dat  $n + 1 \mid m$  en  $n \mid m + 1$ . HA

**Opgave 7.36.** Vind alle gehele getallen  $x$  zo dat  $5x \equiv 3 \pmod{7}$  en  $6x \equiv 8 \pmod{10}$ .

De Chinese reststelling kan men uitbreiden met een meer algemene voorwaarde voor het bestaan van gehele oplossingen  $x$  die voldoen aan  $x \equiv a_i \pmod{m_i}$  voor elke  $i$ .

De precieze voorwaarde luidt als volgt:

**Stelling 7.37.** Chinesese reststelling, veralgemening

Als  $m_1, m_2, \dots, m_n$  en  $a_1, a_2, \dots, a_n$  rijen gehele getallen zijn, dan heeft het stelsel congruenties  $x \equiv a_k \pmod{m_k}$  een oplossing als en slechts als

$$a_k \equiv a_l \pmod{\text{ggd}(m_k, m_l)}$$

voor alle  $k$  en  $l$ .

Als het stelsel een oplossing heeft, dan heeft het oneindig veel oplossingen die bovendien congruent zijn modulo  $\text{kgv}(m_1, m_2, \dots, m_n)$ .

**Opgave 7.38.** (Veralgemeende Chinese reststelling) De stelling bevat 'als en slechts als', en bestaat dus uit twee delen, die we apart zullen bewijzen.

A. Stel dat  $x \equiv a_k \pmod{m_k}$  voor elke  $k$ . Toon aan dat

$$a_k \equiv a_l \pmod{\text{ggd}(m_k, m_l)}$$

voor alle  $k$  en  $l$ .

Hiermee is het eerste deel reeds voltooid. Vervolgens bewijzen we dat er oneindig veel oplossingen bestaan, onderling congruent modulo  $\text{kgv}(m_1, \dots, m_n)$ , indien voor alle  $k$  en  $l$  geldt dat  $a_k \equiv a_l \pmod{\text{ggd}(m_k, m_l)}$ . We bewijzen dit via volledige inductie op  $n$ . Basisstap. We tonen de stelling aan voor  $n = 2$ .

- B. Toon aan dat er gehele getallen  $q_1, q_2, r, s, t$  bestaan zo dat  $a_1 = q_1 s m_1 + q_2 t m_2 + r$  en  $a_2 = q_2 s m_1 + q_1 t m_2 + r$ .
- C. Toon aan dat  $x = q_1 t m_2 + q_2 s m_1 + r$  voldoet.
- D. Toon aan dat er oneindig veel oplossingen bestaan en dat die onderling congruent zijn modulo  $\text{kgv}(m_1, m_2)$ .

Hiermee is de basisstap voltooid.

Inductiestap. We veronderstellen dat de stelling telkens waar is voor een stelsel van  $j$  congruenties, met  $j \leq n$ . Beschouw nu zo'n stelsel van  $j + 1$  congruenties.

Wegens de inductiehypothese zijn de laatste twee congruenties  $x \equiv a_n \pmod{m_n}$  en  $x \equiv a_{n+1} \pmod{m_{n+1}}$  gelijkwaardig met  $x \equiv b_n \pmod{p_n}$  voor een bepaalde waarde van  $b_n$ , en met  $p_n = \text{kgv}(m_n, m_{n+1})$ , want de stelling is waar voor  $n = 2$ . (We vervingen de laatste twee congruenties dus door één.) Stel nu  $a_k = b_k$  en  $m_k = p_k$  voor alle  $k$  met  $0 \leq k < n$ .

We willen de inductiehypothese nogmaals toepassen, maar deze keer op het stelsel congruenties  $x \equiv b_k \pmod{p_k}$ . Daarvoor moeten we er eerst zeker van zijn dat aan de voorwaarde  $b_k \equiv b_l \pmod{\text{ggd}(p_k, p_l)}$  is voldaan.

E. Toon aan dat de voorwaarde geldt voor alle  $k, l$  met  $k, l < n$ .

Het wordt dus een probleem wanneer  $l = n$ . Nu bewijzen we nog voor alle  $k < n$  dat  $b_k \equiv b_n \pmod{\text{ggd}(p_k, p_n)}$ . We bekijken daarvoor een vaste waarde van  $k$ .

F. Toon aan dat

$$b_n \equiv a_n \pmod{\text{ggd}(p_k, m_n)} \quad \text{en} \quad b_{n+1} \equiv a_{n+1} \pmod{\text{ggd}(p_k, m_{n+1})}.$$

G. Toon aan dat

$$b_n \equiv b_k \pmod{\text{ggd}(p_k, m_n)} \quad \text{en} \quad b_{n+1} \equiv b_k \pmod{\text{ggd}(p_k, m_{n+1})}.$$

H. Toon aan dat

$$b_n \equiv b_k \pmod{\text{kgv}(\text{ggd}(p_k, m_n), \text{ggd}(p_k, m_{n+1}))}.$$

Wie zich nog Lemma 2.19 herinnert, heeft misschien opgemerkt dat

$$\text{kgv}(\text{ggd}(p_k, m_n), \text{ggd}(p_k, m_{n+1})) = \text{ggd}(p_k, \text{kgv}(m_n, m_{n+1})) = \text{ggd}(p_k, p_n).$$

Bijgevolg geldt dat  $b_n \equiv b_k \pmod{\text{ggd}(p_k, p_n)}$ . Hierdoor kunnen we de inductiehypothese toepassen, en weten we dat het stelsel oneindig veel oplossingen heeft, die bovendien congruent zijn modulo  $\text{kgv}(p_1, p_2, \dots, p_n)$ . We zijn bijna klaar:

I. Toon aan dat de oplossingen congruent zijn modulo  $\text{kgv}(m_1, m_2, \dots, m_{n+1})$ .

Ziezo, daarmee is de kous af. Wegens volledige inductie geldt de stelling nu voor elk natuurlijk getal  $n$ .

**Opgave 7.39.** (BSMC 2008 vraag 4) Bewijs dat er voor elk natuurlijk getal  $k$  oneindig veel natuurlijke getallen  $n$  bestaan zo dat

$$\frac{n - \tau(n^r)}{r}$$

een geheel getal is voor elke  $r \in \{1, 2, \dots, k\}$ .

## 7.5 Kwadraatresten

### Definitie 7.40. Kwadraatrest

We zeggen dat  $a$  een *kwadraatrest* is modulo  $b$  als er een geheel getal  $x$  bestaat zo dat  $x^2 \equiv a \pmod{b}$ . We zeggen ook kort “ $a$  is een kwadraat modulo  $b$ .” Een niet-kwadraatrest modulo  $b$  is een getal dat geen kwadraat is modulo  $b$ .

Bijvoorbeeld, 23 is een kwadraatrest modulo 7 want  $3^2 = 9 \equiv 23 \pmod{7}$ . 0 is een kwadraatrest modulo elk geheel getal.

We zullen vanaf nu ook spreken over het aantal kwadraatresten modulo  $b$ . Hiermee bedoelen we het aantal onderling incongruente kwadraatresten, of dus het aantal kwadraatresten “na reductie modulo  $b$ ”. Of nog, het aantal kwadraatresten in het interval  $[0, |b| - 1]$ . We zullen voorlopig nog niet diep indaan op kwadraatresten. Hoofdstuk 9 is daaraan toegewijd.

**Lemma 7.41.**

2 is geen kwadraatrest modulo 3.

*Bewijs.*

We bekijken eerst wat alle mogelijke kwadraatresten zijn modulo 3. Als  $a \equiv b \pmod{3}$ , dan geldt  $a^2 \equiv b^2 \pmod{3}$ . Voor elk geheel getal  $a$  bestaat er een getal  $b$  met  $0 \leq b < 3$  waarvoor  $a \equiv b \pmod{3}$ , namelijk de rest van  $a$  bij deling door 3.

Het volstaat dus om de resten van  $0^2$ ,  $1^2$  en  $2^2$  te berekenen, want elk ander geheel getal heeft een kwadraat dat congruent is met één van deze kwadraten.

We zien dat deze resten steeds 0 of 1 zijn. Het is dus onmogelijk dat 2 een kwadraatrest is modulo 3.  $\square$

**Opgave 7.42.** Toon aan dat 0 en 1 de enige kwadraatresten zijn modulo 4.

*Opmerking.*

Met “0 en 1 zijn de enige kwadraatresten modulo 4” bedoelen we dus dat dit de enige kwadraatresten zijn na reductie modulo 4. Of dus, dat 0 en 1 de enige “resten van kwadraten” zijn modulo 4.

**Stelling 7.43.**

Er zijn precies  $\frac{p+1}{2}$  kwadraten modulo een oneven priemgetal  $p$ .

**Opgave 7.44.** Bewijs dat dit inderdaad zo is.

- Toon aan dat het volstaat om het aantal verschillende resten van  $a^2$  met  $0 \leq a < p$  te bekijken.
- Wanneer geldt dat  $a^2 \equiv b^2$  als  $0 \leq a, b < p$ ?
- Toon nu aan dat het aantal verschillende resten gelijk is aan  $\frac{p+1}{2}$ .

**Opgave 7.45.** Vind alle kwadraatresten modulo 5.

Analoog aan kwadraatresten definiëren we  $n$ -demachtsresten in het algemeen.

**Definitie 7.46.**  $n$ -demachtsrest

We noemen  $a$  een  $n$ -demachtsrest modulo  $b$  als er een getal  $x$  bestaat zo dat  $x^n \equiv a \pmod{b}$ .

**Opgave 7.47.** Vind alle derdemachtsresten modulo 7.

**Opgave 7.48.** Toon aan dat  $n^2 + 1$  nooit deelbaar is door 3.

**Opgave 7.49.** Stel dat  $3 \mid a^2 + b^2$ . Toon aan dat  $9 \mid a^2 + b^2$ .

### 7.5.1 Toepassing: Diophantische vergelijkingen

**Voorbeeld 7.50.** Vind alle gehele getallen  $m$  en  $n$  zo dat  $n^2 + 1 = 4m \cdot (m + 1)$ .

*Oplossing.*

Omdat het linkerlid en rechterlid gelijke gehele getallen zijn hebben ze dezelfde rest bij deling door 2. Dat betekent dat  $n$  niet even kan zijn, anders zou  $n^2 + 1 \equiv 1 \pmod{4}$  terwijl  $4m \cdot (m + 1) \equiv 0 \pmod{4}$ . Dus  $n$  is oneven.

We bekijken nu de vergelijking modulo 4, dat wil zeggen: we beschouwen de (mogelijke) resten van beide leden bij deling door 4. Omdat  $n$  oneven is, is  $n^2 \equiv 1 \pmod{4}$  en dus  $n^2 + 1 \equiv 2 \pmod{4}$ . Het rechterlid is echter congruent met 0 modulo 4. Er zijn dus geen oplossingen, omdat het linkerlid en rechterlid onmogelijk dezelfde rest kunnen hebben bij deling door 4.

*Opmerking.*

Het lijkt misschien vreemd om de vergelijking modulo 4 te beschouwen, omdat daar eigenlijk geen reden toe was. Bij het oplossen van een dergelijke vergelijking kan het best gebeuren dat je de vergelijking eerst modulo andere getallen beschouwt, en niet meteen besluiten kan trekken. Het is dus belangrijk van niet meteen op te geven en te blijven proberen.

Hier was 4 nog een vrij logische keuze omdat het rechterlid deelbaar is door 4, en dus congruent is met 0. Dat verkleint het aantal gevallen omdat er dan voor het rechterlid maar één mogelijkheid is. Het is dus niet steeds zo dat er slechts één geval te controleren valt:

**Voorbeeld 7.51.** Vind alle gehele getallen  $x$  en  $y$  waarvoor  $2x^2 + 1 = 5y^2 + 2$ .

*Oplossing.*

We beschouwen de vergelijking modulo 5, aangezien het aantal mogelijke resten van het rechterlid dan sterk wordt gereduceerd. We bekijken eerst wat de mogelijke kwadraatresten zijn modulo 5:  $0^2 \equiv 0$ ,  $1^2 \equiv 1$ ,  $2^2 \equiv 4$ ,  $3^2 \equiv 4$ ,  $4^2 \equiv 1$ . Meer resten hoeven we niet te berekenen. De mogelijke resten zijn dus 0, 1 en 4.

Dus  $2x^2 + 1$  kan modulo 5 enkel congruent zijn met  $2 \cdot 0 + 1 = 1$ ,  $2 \cdot 1 + 1 = 3$  en  $2 \cdot 4 + 1 \equiv 4$ . Het linkerlid is echter congruent met 2 modulo 5. Dat betekent dat er geen oplossingen zijn.

**Opgave 7.52.** Vind alle natuurlijke getallen  $n$  en priemgetallen  $p, q$  zo dat  $p^2 + q^2 = 2^n$ .

**Opgave 7.53.** Vind alle gehele getallen  $a$  en  $n$  met  $n \geq 0$  zo dat  $a \cdot (a + 2) = 3^n - 2$ .

### 7.5.2 Pythagorese drietallen

**Definitie 7.54.** Pythagorees drietal

Een natuurlijk drietal  $(a, b, c)$  waarvoor  $a^2 + b^2 = c^2$  noemen we een *Pythagorees drietal*. Indien geldt dat  $\text{ggd}(a, b, c) = 1$  noemen we het drietal “primitief”.



**Stelling 7.55.**

Alle primitieve Pythagorese drietallen zijn van de vorm

$$(2xy, x^2 - y^2, x^2 + y^2) \quad \text{of} \quad (x^2 - y^2, 2xy, x^2 + y^2)$$

met  $\text{ggd}(x, y) = 1$ .

**Opgave 7.56.** Vind alle primitieve Pythagorese drietallen  $(a, b, c)$ .

A. Toon aan dat  $a$  en  $b$  niet tegelijk oneven kunnen zijn.

Veronderstel nu dat  $a$  even is. We kunnen dit veronderstellen omdat de gelijkheid symmetrisch is in  $a$  en  $b$ . Dan moeten we er achteraf wel rekening mee houden dat ook  $b$  even kon zijn.

B. Toon aan dat  $\text{ggd}(c + b, c - b) = 2$ .

C. Toon aan dat er getallen  $x$  en  $y$  bestaan zodat  $c + b = 2x^2$ ,  $c - b = 2y^2$  en  $\text{ggd}(x, y) = 1$ .

D. Toon aan dat  $a = 2xy$ ,  $b = x^2 - y^2$  en  $c = x^2 + y^2$ .

Alle primitieve drietallen zijn dus van de vorm

$$(2xy, x^2 - y^2, x^2 + y^2) \quad \text{of} \quad (x^2 - y^2, 2xy, x^2 + y^2)$$

naar gelang  $a$  of  $b$  even is.

Het is helaas niet zo dat ook elk niet-primitief drietal van die vorm is.

**Opgave 7.57.** Vind een Pythagorees drietal  $(a, b, c)$  met  $b$  oneven, dat niet van de vorm  $A$   $(2xy, x^2 - y^2, x^2 + y^2)$  is.

We kunnen uiteraard wel alle niet-primitieve drietallen afleiden uit een primitief drietal, door  $a$ ,  $b$  en  $c$  te vermenigvuldigen met een vast getal.

## 7.6 Stelling van Wilson

De stelling van Wilson bewijst vaak zijn nut. Problemen waarin Wilson van pas komt zijn echter vaak eenvoudig herkenbaar.

**Stelling 7.58.** Stelling van Wilson

Als  $p$  een priemgetal is, dan geldt

$$(p - 1)! \equiv -1 \pmod{p}.$$

**Opgave 7.59.** (Stelling van Wilson) Het is eenvoudig te controleren dat de stelling geldt voor  $p > 2$ . Veronderstel nu dat  $p > 2$ .

A. Vind alle gehele getallen  $a$  met  $0 \leq a < p$  zo dat  $a^2 \equiv 1 \pmod{p}$ .

B. Toon aan dat voor elk geheel getal  $a$  met  $0 \leq a < p$  dat niet voldoet aan  $a^2 \equiv 1$ , er een ander geheel getal  $b$  met  $0 \leq b < p$  bestaat zo dat  $ab \equiv 1 \pmod{p}$ , en dat zo'n getal  $b$  steeds bij precies één getal  $a$  hoort.

C. Toon aan dat  $(p-1)! \equiv -1 \pmod{p}$ .

**Opgave 7.60.** Toon aan dat  $p! + p$  deelbaar is door  $p^2$  als  $p$  een priemgetal is.

**Stelling 7.61.**

Als  $p$  een oneven priemgetal is  $k$  is een natuurlijk getal met  $k \leq p$ , dan is

$$(k-1)! \cdot (p-k)! \equiv (-1)^k \pmod{p}.$$

*Bewijs.*

Er geldt dat

$$\prod_{\substack{n=1-k \\ n \neq 0}}^{p-k} n \equiv (p-1)!$$

omdat alle factoren in het linkerlid één aan één congruent zijn met een factor in het rechterlid. Nu is het linkerlid gelijk aan  $(-1)^{k-1}(k-1)! \cdot (p-k)!$  en het rechterlid is congruent met  $-1$ . Dus

$$(-1)^{k-1}(k-1)! \cdot (p-k)! \equiv -1$$

en hieruit volgt de stelling. □

**Opgave 7.62.** Bereken  $1! \cdot 2! \cdot \dots \cdot 10! \pmod{11}$ .

**Gevolg 7.63.**

Als  $p$  een oneven priemgetal is, dan is

$$\left( \left( \frac{p-1}{2} \right)! \right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

*Bewijs.*

Dit volgt door  $k = \frac{p+1}{2}$  te stellen in de vorige stelling. □

**Stelling 7.64.**

$-1$  is een kwadraat modulo een priemgetal  $p$  als en slechts als  $p = 2$  of  $p \equiv 1 \pmod{4}$ .

**Opgave 7.65.** Bewijs.

## Opgaven hoofdstuk 7

**Opgave 7.66.** Voor een natuurlijk getal wordt de alternerende som van zijn cijfers verkregen door de cijfers afwisselend op te tellen en af te trekken, beginnend bij het laatste cijfer. Zo is de alternerende som van 946254 gelijk aan  $4 - 5 + 2 - 6 + 4 - 9$ . Bewijs dat een natuurlijk getal deelbaar is door 11 als en slechts als de alternerende som van zijn cijfers deelbaar is door 11.

**Opgave 7.67.** (BrMO 2003 ronde 1 vraag 1) Gegeven dat H

$$34! = 95232799cd96041408476186096435ab000000,$$

bepaal de cijfers  $a$ ,  $b$ ,  $c$  en  $d$ .

**Opgave 7.68.** (JWO 2011 finale vraag 3) Een natuurlijk getal is prima als ieder deel van het getal, bestaande uit opeenvolgende cijfers ervan, zelf een priemgetal is. Bepaal alle primagetallen. H

**Opgave 7.69.** (CanMO 1973 vraag 3) Bewijs dat als  $p$  en  $p + 2$  priemgetallen zijn groter dan 3, dat 6 een deler is van  $p + 1$ .

**Opgave 7.70.** (CanMO 1980 vraag 1) Als  $a679b$  een vijfcijferig getal is dat deelbaar is door 72, bepaal dan  $a$  en  $b$ .

**Opgave 7.71.** We beschouwen het getal  $7^{555}$  en berekenen de som van zijn cijfers. Van deze som berekenen we opnieuw de som van zijn cijfers. Dit herhalen we tot we een getal bekomen van slechts één cijfer. Wat is dat cijfer?

**Opgave 7.72.** (VWO 2000 finale vraag 1) Een natuurlijk getal van zeven verschillende cijfers is deelbaar door elk van zijn cijfers. Welke cijfers kunnen niet in dat getal voorkomen? H

**Opgave 7.73.** Twee priemgetallen  $p$  en  $q$  met  $q = p + 2$  noemen we een priemtweeling.

A. Vind tien priemtweelingen.

Drie priemgetallen  $p$ ,  $q$  en  $r$  met  $r = q + 2 = p + 4$  noemen we een priemdrieling.

B. Vind alle priemdrielingen.

**Opgave 7.74.** (VWO 2009 finale vraag 1) Op 29/09/2009 komen precies 2009 Belgen samen om het record handjes schudden te verbreken. Iedereen schudt een ander precies één keer de hand. Twee van de aanwezigen zijn Thomas en Nathalie. Nathalie zei op het einde dat ze vijf keer zoveel Vlamingen als Brusselaars de hand had gegeven. Thomas antwoordde met "Ik heb precies drie keer zoveel Walen als Brusselaars een hand geschud". Uit welk gewest komt Nathalie en uit welk gewest komt Thomas? H






**Opgave 7.75.** (VWO 2010 finale vraag 1) Op hoeveel nullen eindigt  $101^{100} - 1$ ? H

**Opgave 7.76.** Bepaal alle natuurlijke getallen  $n$  zo dat  $2^n \mid 3^n - 1$ .

**Opgave 7.77.** (VWO 2013 finale vraag 1) Een getal van zes cijfers is evenwichtig wanneer alle cijfers verschillend zijn van nul en de som van de eerste drie cijfers gelijk is aan de som van de laatste drie cijfers. Bewijs dat de som van alle evenwichtige getallen van zes cijfers deelbaar is door 13. H

**Opgave 7.78.** Bepaal het laatste cijfer van  $4^2 + 4^4 + 4^8 + 4^{16} + \dots + 4^{2^{101}}$  H

**Opgave 7.79.** Zij  $a$ ,  $b$ ,  $d$ ,  $n$  natuurlijke getallen zo dat  $a$  de inverse is van  $n$  en  $b$  de inverse van  $n + 1$  modulo  $d$ . Bewijs dat  $(a + 1)^2$  de inverse is van  $(b - 1)^2$  modulo  $d$ .

- Opgave 7.80.**  $n$  waterleliebladen liggen in een vijver, geranschikt in een cirkel. Een kikker  A bevindt zich op een van de bladen en springt langs de cirkel van blad naar blad, waarbij hij telkens  $k$  bladen overslaat. Hoeveel bladen kan de kikker maximaal bereiken?
- Opgave 7.81.** Toon aan dat er 19 opeenvolgende natuurlijke getallen bestaan die elk deelbaar zijn door de 17-de macht van een natuurlijk getal.
- Opgave 7.82.** Bewijs dat de vergelijking  $x^2 + y^2 = 2^k$  precies vier oplossingen in gehele getallen heeft, voor elk natuurlijk getal  $k$ .
- Opgave 7.83.** (JWO 2002 finale vraag 2) Bewijs dat er geen enkel getal bestaande uit meerdere  gelijke cijfers na elkaar een kwadraat is.
- Opgave 7.84.** Vind alle oplossingen in gehele getallen van  $x^2 + 4 = y^5$ .
- Opgave 7.85.** Vind alle priemgetallen die geschreven kunnen worden als  $a^4 + b^4 + c^4 - 3$ , waarbij  $a, b, c$  zelf priemgetallen zijn.
- Opgave 7.86.** Zij  $n$  een natuurlijk getal zo dat  $N = 2 + 2\sqrt{28n^2 + 1}$  een natuurlijk getal is. Bewijs dat  $N$  een volkomen kwadraat is.
- Opgave 7.87.** (BrMO 1 2007 vraag 6) Zij  $n$  een geheel getal. Als  $2 + 2\sqrt{1 + 12n^2}$  een geheel getal is, bewijs dan dat het een volkomen kwadraat is.
- Opgave 7.88.** (Klassieker) Bepaal alle natuurlijke getallen  $x, y$  en  $z$  zo dat  $3^x + 4^y = 5^z$ . 
- Opgave 7.89.** Vind alle  $n \in \mathbb{N}$  waarvoor  $\frac{n!-1}{2n+7} \in \mathbb{N}$ . 
- Opgave 7.90.** Kunnen 18 opeenvolgende gehele getallen in twee groepen worden verdeeld  H A zodanig dat het product van de getallen in elk van de groepen hetzelfde is?

**Definitie 8.1.** Orde

Als  $a, b \in \mathbb{Z}_0$  noemen we de kleinste  $n \in \mathbb{N}^+$  waarvoor  $a^n \equiv 1 \pmod{b}$ , indien  $n$  bestaat, de orde van  $a$  modulo  $b$ . We noteren  $n = \text{ord}_b(a)$  (soms  $O_b(a)$ ).

Merk op dat de voorwaarde  $n > 0$  noodzakelijk is, anders zou de orde steeds 0 zijn. Nu rest nog de vraag wanneer er een orde bestaat.

**Stelling 8.2.**

$a$  heeft een orde modulo  $b$  als en slechts als  $\text{ggd}(a, b) = 1$ .

**Opgave 8.3.** Bewijs.

A. Bewijs dat als  $a$  een orde heeft modulo  $b$ , dan  $\text{ggd}(a, b) = 1$ .

Stel nu  $\text{ggd}(a, b) = 1$ . We bewijzen dat  $a$  een orde heeft modulo  $b$ .

B. Toon aan dat er natuurlijke getallen  $k$  en  $l$  bestaan met  $k > l$  zo dat  $a^k \equiv a^l \pmod{b}$ .

C. Toon aan dat er een natuurlijk getal  $n > 0$  bestaat zo dat  $a^n \equiv 1 \pmod{b}$ .

Bijgevolg bestaat er ook een kleinst mogelijke waarde voor  $n$  en heeft  $a$  een orde.

**Gevolg 8.4.**

Als  $\text{ord}_n(a) = t$  dan geldt  $a^k \equiv a^{k+t}$  voor alle  $k \in \mathbb{Z}$ , en  $t$  is het kleinste getal groter dan 0 waarvoor dit geldt. M.a.w, de rij van resten van  $a^k$  modulo  $n$  is periodiek met periode  $t$ .

We nemen als voorbeeld  $n = 11$  en  $t = 3$ . Bekijken we de resten van  $3, 3^2, 3^3, \dots$  dan vinden we de rij  $3, 9, 5, 4, 1, 3, 9, 5, 4, 1, \dots$ . De rij is periodiek met periode 5, dus  $\text{ord}_{11}(3) = 5$ . Eigenlijk hadden we al mogen stoppen met resten berekenen van zodra er een 1 verscheen. Immers, voor de zesde term geldt  $3^6 \equiv 3^5 \cdot 3 \equiv 1 \cdot 3 = 3$ . Zo zal dan  $3^7 \equiv 3^2$ , enzovoort.

**Gevolg 8.5.**

Als  $\text{ord}_n(a) = t$  dan is  $a^{-1} \equiv a^{t-1}$ .

We hebben dus een andere (vrij omslachtige) methode om de inverse te bepalen. Zo zien we dat  $3^4 \equiv 4 \pmod{11}$ , dus 4 is de inverse van 3. Inderdaad,  $3 \cdot 4 = 12 \equiv 1$ .

## 8.1 Het ordelemma

### Stelling 8.6. Ordelemma

Als  $n = \text{ord}_b(a)$ , dan geldt dat  $a^m \equiv 1 \pmod{b}$  als en slechts als  $n \mid m$  voor alle  $m \in \mathbb{Z}$ .

**Opgave 8.7.** Bewijs het ordelemma.

### Gevolg 8.8.

Zij  $a, b, x, y$  gehele getallen en zij  $n = \text{ord}_b(a)$ . Dan geldt  $a^x \equiv a^y \pmod{b}$  als en slechts als  $x \equiv y \pmod{n}$ .

*Bewijs.*

Omdat  $\text{ggd}(a, b) = 1$  is  $\text{ggd}(a^{-y}, b) = 1$  zodat wegens Lemma 7.21 en Gevolg 7.28 geldt dat  $a^x \equiv a^y$  als en slechts als  $a^{x-y} \equiv 1$ . Wegens de vorige stelling is dit equivalent met  $n \mid x - y$ .  $\square$

Het volgende lemma zegt iets over de orde van het product van gehele getallen met dezelfde modulus.

### Lemma 8.9.

Zij  $a, b, n \in \mathbb{Z}$  en  $\text{ord}_n(a) = k$ ,  $\text{ord}_n(b) = l$  zo dat  $\text{ggd}(k, l) = 1$ . Dan is  $\text{ord}_n(ab) = kl$ .

*Bewijs.*

Stel  $x = \text{ord}_n(ab)$ . Er geldt  $(ab)^{kl} = (a^k)^l (b^l)^k \equiv 1$ , dus  $x \mid kl$  wegens het ordelemma. Stel  $kl = mx$ . Noem  $g = \text{ggd}(k, m)$ , dan is

$$1 \equiv (ab)^{\frac{xm}{g}} = (ab)^{\frac{kl}{g}} = (a^k)^{\frac{l}{g}} b^{\frac{kl}{g}} \equiv b^{\frac{kl}{g}}$$

zodat  $l \mid \frac{kl}{g}$  wegens het ordelemma. Omdat  $\text{ggd}(k, l) = 1$  moet dan  $l \mid \frac{l}{g}$  dus  $g = 1$ .

Analoog moet  $\text{ggd}(l, m) = 1$ , zodat  $m = 1$  omdat  $m \mid kl$ . Dus  $kl = x$ .  $\square$

### Lemma 8.10.

Zij  $a, k, n \in \mathbb{Z}$ . Dan is  $\text{ord}_n(a) = \text{ord}_n(a^k)$  als en slechts als  $\text{ggd}(k, \text{ord}_n(a)) = 1$ .

**Opgave 8.11.** Bewijs.

We kunnen, onder bepaalde voorwaarden, ordes met verschillende moduli combineren:

**Lemma 8.12.**

Zij  $a, n, m$  gehele getallen met  $\text{ggd}(m, n) = 1$ ,  $\text{ord}_m(a) = x$  en  $\text{ord}_n(a) = y$ . Dan is  $\text{ord}_{mn}(a) = \text{kgv}(x, y)$ .

**Opgave 8.13.** Bewijs.

*Opmerking.*

De voorwaarde  $\text{ggd}(m, n) = 1$  is voldoende, maar niet noodzakelijk opdat de gelijkheid zou gelden. Een voorbeeld waar de gelijkheid ook geldt is  $m = n = 11$  en  $a = 3$ . We komen hier later op terug om dit verder te analyseren, wanneer we het hebben over Wieferich-priemgetallen.

**Opgave 8.14.** Stel dat  $\text{ggd}(a, b) = 1$  en dat  $p$  en  $q$  verschillende priemgetallen zijn.

A

- A. Als  $a^p \equiv a^q \pmod{b}$ , geldt dan noodzakelijk dat  $a \equiv 1 \pmod{b}$ ?
- B. Als  $a^p \equiv a^q \equiv 1 \pmod{b}$ , geldt dan noodzakelijk dat  $a \equiv 1 \pmod{b}$ ?

**8.2 De kleine stelling van Fermat****Stelling 8.15.** Kleine stelling van Fermat

Als  $p$  een priemgetal is en  $p \nmid a$ , dan is

$$a^{p-1} \equiv 1 \pmod{p}.$$

**Opgave 8.16.** (Kleine stelling van Fermat) Beschouw de getallen  $x_k = ka$  voor  $1 \leq k \leq p-1$ 

- A. Toon aan dat  $x_k \equiv x_l \pmod{p}$  onmogelijk is als  $k \neq l$ .

Beschouw nu de resten van de getallen  $x_k$  modulo  $p$ . Wegens het vorige zijn die dus allemaal verschillend.

- B. Toon aan dat die resten de getallen  $1, 2, \dots, p-1$  zijn, in een willekeurige volgorde.
- C. Definieer nu  $y = x_1 x_2 \cdots x_{p-1}$ . Toon aan dat  $y \equiv (p-1)! \pmod{p}$ .
- D. Bewijs dat  $a^{p-1} \equiv 1 \pmod{p}$ .

**Gevolg 8.17.**

Voor elk geheel getal  $a$  en elk priemgetal  $p$  geldt dat  $a^p \equiv a \pmod{p}$ .

*Bewijs.*

Eenvoudig gevalsonderscheid. □

**Gevolg 8.18.**

Voor elk priemgetal  $p$  geldt dat  $\text{ord}_p(a) \mid p - 1$ .

*Bewijs.*

Dit volgt meteen uit het ordelemma en de stelling van Fermat □

**Opgave 8.19.** Toon aan dat  $1^{10} + 2^{10} + \dots + 9999^{10}$  deelbaar is door 11. H

**Opgave 8.20.** Vind alle priemgetallen  $p$  en  $a, b \in \mathbb{N}$  zo dat  $2^p + a^{p-1} = p^b$ .

**Opgave 8.21.** (BrMO 1 2007 vraag 1) Vind vier priemgetallen kleiner dan 100 die delers zijn van  $3^{32} - 2^{32}$ .

### 8.3 De stelling van Euler

Een grote beperking van de stelling van Fermat is dat ze enkel geldt voor priemgetallen. Je zou je kunnen afvragen of er ook voor samengestelde getallen een gelijkaardige eigenschap geldt. Daar geeft de stelling van Euler een antwoord op.

**Stelling 8.22.** Stelling van Euler

Als  $a, n \in \mathbb{Z}$  met  $\text{ggd}(a, n) = 1$  en  $n > 0$ , dan is

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Vooraleer we tot een bewijs komen presenteren we een eigenschap die in andere situaties ook best nuttig kan zijn.

**Lemma 8.23.** Lifting lemma

Als  $p$  een priemgetal is,  $k > 0$  en  $a \equiv b \pmod{p^k}$ , dan geldt dat

$$a^{p^n} \equiv b^{p^n} \pmod{p^{k+n}}$$

voor elk natuurlijk getal  $n$ .

**Opgave 8.24.** Toon deze eigenschap aan. H

**Opgave 8.25.** (Bewijs van de stelling van Euler) We bewijzen eerst via inductie dat de stelling geldt voor  $n = p^k$  met  $p$  priem en  $k > 0$ .

A. Toon aan dat de stelling geldt voor  $k = 1$ .

Veronderstel nu dat de stelling geldt voor  $k$ . Dan is  $a^{\varphi(p^k)} = m \cdot p^k + 1$ .

B. Toon aan dat  $\varphi(p^{k+1}) = p \cdot \varphi(p^k)$ .

C. Toon aan dat  $a^{\varphi(p^{k+1})} \equiv 1 \pmod{p^{k+1}}$ .



Wegens inductie geldt de stelling nu voor elke  $n = p^k$ .

Stel  $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ .

D. Toon aan dat  $a^{\varphi(n)} \equiv 1 \pmod{p_i^{a_i}}$  voor elke  $i$ .

E. Toon aan dat  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

Nogal langdradig en onelegant... Nochtans is het best wel een interessante techniek: de stelling eerst te bewijzen voor priem machten en pas daarna voor algemene getallen.

Bovenstaand bewijs maakt zwaar gebruik van de expliciete formule voor  $\varphi(n)$ , maar we kunnen ook zonder:

**Opgave 8.26.** Bewijs de stelling van Euler analoog aan die van Fermat.

Merk trouwens op dat de stelling van Euler een uitbreiding is van die van Fermat, in de zin dat ze die omvat: als  $n$  priem is, is  $\varphi(n) = n - 1$ .

### Gevolg 8.27.

Voor elk natuurlijk getal  $n > 1$  geldt dat  $\text{ord}_n(a) \mid \varphi(n)$ .

*Bewijs.*

Dit volgt meteen uit het ordelemma en de stelling van Euler. □

## 8.4 Ordes en periodieke expansies

### Opgaven hoofdstuk 8

**Opgave 8.28.** Veralgemeen Gevolg 8.4 naar het geval  $\text{ggd}(a, n) \neq 1$ , m.a.w. bestudeer de periodiciteit van de rij  $1, a, a^2, \dots \pmod{n}$ .

**Opgave 8.29.** (VWO 1992 finale vraag 1) Bepaal voor elk natuurlijk getal  $n$  het grootste natuurlijk getal  $k$  zo dat  $2^k \mid 3^n + 1$ . 🔗

**Opgave 8.30.** (JWO 2008 finale vraag 1) 🔗

A. Kan een getal dat enkel uit zevens bestaat deelbaar zijn door 99?

B. Motiveer of een getal uitsluitend bestaand uit negens deelbaar kan zijn door 7777777.

**Opgave 8.31.** Bewijs dat voor natuurlijke getallen  $n$  geldt dat  $7 \mid n^3 + 3^n$  als en slechts als  $7 \mid n^3 \cdot 3^n + 1$ .

**Opgave 8.32.** Als  $a, b \in \mathbb{Z}$  en  $n > 1$  zo dat  $\text{ggd}(ab, n) = 1$  en  $n \mid a^n - b^n$ , bewijs dat  $a - b$  deelbaar is door de kleinste priemdelers van  $n$ .

**Opgave 8.33.** (Polen MO 1998 ronde 1 vraag 1) Bewijs dat er onder de getallen  $50^n + (50n + 1)^n$ , met  $n \in \mathbb{N}$ , oneindig veel samengestelde getallen zijn.

**Opgave 8.34.** Stel dat  $\text{ggd}(m, n) = 1$ . Toon aan dat  $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$ .

**Opgave 8.35.** Vind alle natuurlijke oplossingen van  $2^x + 7 = y^2$ .



**Opgave 8.36.** Bepaal alle natuurlijke getallen  $a, b$  zo dat

$$(a + 19b)^{18} + (a + b)^{18} + (19a + b)^{18}$$

een volkomen kwadraat is.

**Opgave 8.37.** Zij  $a, b \in \mathbb{N}$  zo dat  $2a - 1$ ,  $2b - 1$  en  $a + b$  priemgetallen zijn. Bewijs dat  $a + b$  een deler is van  $a^a + b^b$  noch  $a^b + b^a$ .



**Opgave 8.38.** Stel  $p > 5$  is een priemgetal. Toon aan dat alle delers van  $\frac{6^p - 1}{5}$  van de vorm  $kp + 1$  zijn.

**Opgave 8.39.** Als  $a, b, n > 0$  natuurlijke getallen zijn zo dat  $a \neq b$ , bewijs dan dat



$$2n \mid \varphi(a^n + b^n).$$

**Opgave 8.40.** (IMO 1999 dag 2 vraag 1) Bepaal alle paren natuurlijke getallen  $n$  en priemgetallen  $p$  waarvoor  $n < 2p$  en  $n^{p-1} \mid (p-1)^n + 1$ .



**Opgave 8.41.** Bepaal de drie laatste cijfers van het getal  $2003^{2002^{2001}}$ .

**Opgave 8.42.** (LIMO 2007) Zij  $n$  een natuurlijk getal,  $p$  een priemgetal en  $d$  een deler van  $(n+1)^p - n^p$ . Bewijs dat  $d \equiv 1 \pmod{p}$ .

## 9.1 Het Legendre-symbool

### Definitie 9.1. Legendre-symbool

Is  $a \in \mathbb{Z}$  en  $p$  een oneven priemgetal, dan definiëren we het *Legendre-symbool* of *kwadratisch karakter* door

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{als } p \mid a \\ 1 & \text{als } a \text{ een kwadraatrest is modulo } p \\ -1 & \text{als } a \text{ geen kwadraatrest is modulo } p. \end{cases}$$

### Eigenschappen 9.2.

Voor alle  $a, k \in \mathbb{Z}$  en oneven priemgetallen  $p$  is

$$\left(\frac{a + kp}{p}\right) = \left(\frac{a}{p}\right),$$

en als  $p \nmid a$  is

$$\left(\frac{a^2}{p}\right) = 1.$$

*Bewijs.*

Als oefening. □

**Opgave 9.3.** Toon aan dat

$$\sum_{k=1}^p \left(\frac{k}{p}\right) = 0$$

als  $p$  een oneven priemgetal is.

### 9.1.1 Het criterium van Euler en multiplicativiteit

**Stelling 9.4.** Criterium van Euler

Er geldt dat

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

**Opgave 9.5.** Bewijs het criterium van Euler.

- A. Bewijs het criterium in het geval dat  $p \mid a$ .
- B. Bewijs het criterium in het geval dat  $a$  een kwadraatrest is modulo  $p$ .

Veronderstel nu dat  $a$  geen kwadraatrest is modulo  $p$ .

- C. Toon aan dat voor elk getal  $x$  met  $0 < x < p$  er een  $y$  met  $0 < y < p$  bestaat zo dat  $xy \equiv a \pmod{p}$ .
- D. Toon aan dat  $a^{\frac{p-1}{2}} \equiv (p-1)! \pmod{p}$ .

Wegens de stelling van Wilson geldt nu dat  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ . Dus ook in dit geval geldt het criterium van Euler.

**Gevolg 9.6.** Het Legendre-symbool is totaal multiplicatief

Het Legendre symbool voldoet aan

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \quad \text{en} \quad \left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n$$

voor alle  $a, b \in \mathbb{Z}$  en  $n \in \mathbb{N}^+$ .

Het criterium van Euler laat ons een ‘properder’ bewijs toe van Stelling 7.64.

**Opgave 9.7.** Bewijs dat  $-1$  een kwadraatrest is modulo een priemgetal  $p$  als en slechts als  $p = 2$  of  $p \equiv 1 \pmod{4}$ .

**Opgave 9.8.** Stel dat  $p$  een priemgetal is en  $p \nmid ab$ . Bewijs dat als  $p$  een deler is van  $a^2 + b^2$ , dan  $p \equiv 1 \pmod{4}$ .

**Stelling 9.9.**

Er bestaan oneindig veel priemgetallen van de vorm  $4k + 1$ .

*Bewijs.*

Als oefening. □

## 9.2 Kwadratische reciprociteit

### 9.2.1 Kleinste absolute resten: het lemma van Gauss

**Definitie 9.10.** Kleinste absolute rest

Bij deling van  $a$  door  $b$  noemen we de *kleinste absolute rest* het geheel getal  $r$  waarvoor er een  $q \in \mathbb{Z}$  bestaat zo dat  $a = qb + r$ , en  $r \in ]-\frac{|b|}{2}, \frac{|b|}{2}]$ .

Bijvoorbeeld, bij deling van 14 door 5 is die rest  $-1$ , want  $-1$  ligt in het interval  $]-\frac{5}{2}, \frac{5}{2}]$ . Als we 19 delen door 8 is die deze rest gelijk aan 3, want 3 ligt in het interval  $]-4, 4]$ .

Merk op dat dit interval halfopen is, omdat deze rest anders niet steeds uniek gedefinieerd zou zijn. Bijvoorbeeld, bij deling van 10 door 4 is de kleinste absolute rest gelijk aan 2, omdat dat in het interval  $]-2, 2]$  ligt. Maar als het interval volledig gesloten was, dan zou ook  $-2$  een mogelijke waarde geweest zijn.

**Opgave 9.11.** Bepaal de kleinste absolute rest bij deling van

- A. 6 door 10.
- B.  $-100$  door 7.
- C. 5 door  $-8$ .
- D.  $-50$  door  $-9$ .

De volgende stelling zegt precies wat je zou verwachten.

**Stelling 9.12.** Unicité van de kleinste absolute rest

Bij deling van  $a$  door  $b$  bestaat er een kleinste absolute rest, die bovendien uniek is.

**Opgave 9.13.** Bewijs.

**Lemma 9.14.** Lemma van Gauss

Zij  $p$  een oneven priemgetal en  $a \in \mathbb{Z}$  met  $p \nmid a$ . Beschouw de getallen  $a, 2a, \dots, \frac{p-1}{2}a$  en hun kleinste absolute resten modulo  $p$ . Zij  $n$  het aantal negatieve resten, dan is

$$\left(\frac{a}{p}\right) = (-1)^n.$$

**Opgave 9.15.** (Lemma van Gauss) Stel  $y = a \cdot 2a \cdot \dots \cdot \frac{p-1}{2}a$ . Noteer met  $d(x)$  de absolute waarde van de kleinste absolute rest van  $x$  bij deling door  $p$ .

- A. Toon aan dat  $y \equiv (-1)^n \cdot d(a) \cdot d(2a) \cdot \dots \cdot d\left(\frac{p-1}{2}a\right) \pmod{p}$ .
- B. Toon aan dat  $d(va) = d(wa)$  met  $1 \leq v, w \leq \frac{p-1}{2}$  alleen kan als  $v = w$ .
- C. Toon aan dat de getallen  $d(a), d(2a), \dots, d\left(\frac{p-1}{2}a\right)$  gelijk zijn aan de getallen  $1, 2, \dots, \frac{p-1}{2}$ , in een willekeurige volgorde.
- D. Toon aan dat  $a^{\frac{p-1}{2}} \equiv (-1)^n$ .

Het lemma van Gauss volgt nu uit het criterium van Euler.

**Stelling 9.16.** Kwadratisch karakter van 2

Er geldt dat  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ , en 2 is een kwadraat modulo een oneven priemgetal  $p$  als en slechts als  $p \equiv \pm 1 \pmod{8}$ .

**Opgave 9.17.** Bewijs.

- A. Toon aan dat  $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$  als  $p \equiv 1 \pmod{4}$ .
- B. Toon aan dat  $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$  als  $p \equiv 3 \pmod{4}$ .
- C. Bewijs nu dat  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$  en dat  $\left(\frac{2}{p}\right) = 1$  als en slechts als  $p \equiv \pm 1 \pmod{8}$ .

**Voorbeeld 9.18.** Bereken  $\left(\frac{73}{13}\right)$ .

*Oplossing.*

We hebben  $\left(\frac{73}{13}\right) = \left(\frac{73-5 \cdot 13}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{2^3}{13}\right) = \left(\frac{2}{13}\right) = (-1)^{\frac{13-1}{4}} = (-1)^3 = -1$ .

*Opmerking.*

De truc bestond er uit om het Legendre symbool te herleiden tot iets met een macht van 2. Dat is een techniek die je vaak zal nodig hebben: het symbool herleiden tot een getal met een eenvoudige priemontbinding, liefst met zo klein mogelijke priemfactoren. Omdat we tot nu toe geen handige techniek hebben om  $\left(\frac{q}{p}\right)$ , met  $q$  priem, te berekenen hebben we voorlopig niet veel andere mogelijkheden dan een macht van 2.

**Opgave 9.19.** Bereken het Legendre symbool

- A.  $\left(\frac{51}{7}\right)$ .
- B.  $\left(\frac{15}{17}\right)$ .
- C.  $\left(\frac{-6}{19}\right)$ .
- D.  $\left(\frac{-53}{23}\right)$ .

**Opgave 9.20.** Vind analoge uitdrukkingen aan  $\left(\frac{2}{p}\right)$ , maar dan voor  $\left(\frac{3}{p}\right)$  met  $p > 3$ .

- A. Toon aan dat  $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$  als  $p \equiv 1 \pmod{3}$ .
- B. Toon aan dat  $\left(\frac{3}{p}\right) = (-1)^{\frac{p+1}{2}}$  als  $p \equiv 2 \pmod{3}$ .

Indien je deze gelijkheden uit het hoofd wil kennen, kan het handiger zijn om

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p \pm 1}{6}}$$

te onthouden. Hier is er geen twijfel mogelijk wanneer het  $(-1)^{\frac{p-1}{2}}$  of  $(-1)^{\frac{p+1}{2}}$  is, want van  $(-1)^{\frac{p \pm 1}{6}}$  is er telkens maar één gedefinieerd. Maar wees gerust, je zal deze gelijkheden veel eenvoudiger zelf kunnen opstellen van zodra we de kwadratische reciprociteit hebben gezien.

**Voorbeeld 9.21.** Bereken  $\left(\frac{10}{13}\right)$ .

*Oplossing.*

Er geldt dat  $\left(\frac{10}{13}\right) = \left(\frac{-3}{13}\right) = \left(\frac{-1}{13}\right) \cdot \left(\frac{3}{13}\right) = (-1)^{\frac{13-1}{2}} \cdot (-1)^{\frac{13-1}{6}} = (-1)^6 \cdot (-1)^2 = 1$ .

*Opmerking.*

Er zijn natuurlijk nog andere manieren om tot de oplossing te komen. Je had ook kunnen opmerken dat  $10 + 2 \cdot 13 = 36$ , zodat  $\left(\frac{10}{13}\right) = \left(\frac{36}{13}\right) = 1$ . Of  $10 - 2 \cdot 13 = -16$ , zodat  $\left(\frac{10}{13}\right) = \left(\frac{-16}{13}\right) = \left(\frac{-1}{13}\right) = 1$ . Of nog leuker:  $\left(\frac{10}{13}\right) = \left(\frac{10 \cdot 2^2}{13}\right) = \left(\frac{40}{13}\right) = \left(\frac{1}{13}\right) = 1$ . Massa's aan mogelijkheden dus.

**Opgave 9.22.** Bereken het Legendre symbool

- A.  $\left(\frac{5}{37}\right)$ .
- B.  $\left(\frac{-20}{31}\right)$ .
- C.  $\left(\frac{856}{331}\right)$ .
- D.  $\left(\frac{12345}{2017}\right)$ .

**Opgave 9.23.** Bewijs dat 3 een kwadraatrest is modulo een priemgetal  $p$  als en slechts als  $p \equiv 1 \pmod{12}$ ,  $p \equiv -1 \pmod{12}$ ,  $p = 2$  of  $p = 3$ .

**Opgave 9.24.** Zij  $n$  oneven en  $p$  een priemdelers van  $2^n - 1$ . Bewijs dat  $p \equiv \pm 1 \pmod{8}$ .

## 9.2.2 Eisensteins weg naar kwadratische reciprociteit

Om de wet van de kwadratische reciprociteit te kunnen bewijzen hebben we eerst een bekend lemma nodig.

### Lemma 9.25. Lemma van Eisenstein

Als  $p$  een oneven priemgetal is en  $a \in \mathbb{Z}$  oneven zo dat  $p \nmid a$ , dan geldt

$$\left(\frac{a}{p}\right) = (-1)^{\alpha(a,p)}$$

met

$$\alpha(a, p) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor.$$

**Opgave 9.26.** Bewijs het lemma van Eisenstein.

Stel  $u_1 = a, u_2 = 2a, \dots, u_{\frac{p-1}{2}} = \frac{p-1}{2}a$ . Noem  $r_k$  rest van  $u_k$  bij deling door  $p$ . Noem  $b_1, b_2, \dots, b_m$  de resten kleiner dan  $\frac{p}{2}$  en  $c_1, c_2, \dots, c_n$  de resten die groter zijn dan  $\frac{p}{2}$ . Stel  $U = \sum u_k$  en  $R = \sum r_k$ .

A. Toon aan dat  $U \equiv \alpha(a, p) + R \pmod{2}$ .

Bekijk de getallen  $b_1, b_2, \dots, b_m$  en  $p - c_1, p - c_2, \dots, p - c_n$ .

B. Toon aan dat die getallen gelijk zijn aan  $1, 2, \dots, \frac{p-1}{2}$ , in willekeurige volgorde.

Noem  $S$  hun som.

C. Toon aan dat  $U \equiv n + R \pmod{2}$ .

D. Bewijs dat  $\left(\frac{a}{p}\right) = (-1)^{\alpha(a,p)}$ .

**Opgave 9.27.** Gebruik het Lemma van Eisenstein om aan te tonen dat  $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$  als  $p \equiv 1 \pmod{4}$ , en dat  $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$  als  $p \equiv 3 \pmod{4}$ .

**Stelling 9.28.** Wet van de kwadratische reciprociteit

Voor twee verschillende oneven priemgetallen  $p$  en  $q$  geldt dat

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Deze wet is heel krachtig omdat ze toelaat om complexere Legendre symbolen te berekenen.

**Opgave 9.29.** (Kwadratische reciprociteit) We zullen aantonen dat

$$\alpha(p, q) + \alpha(q, p) = \frac{(p-1)(q-1)}{4}.$$

Beschouw de rechthoek met breedte  $\frac{p}{2}$  en hoogte  $\frac{q}{2}$ , zoals op de figuur. De roosterpunten liggen telkens een afstand 1 uit elkaar.

- Toon aan dat er geen roosterpunten op de diagonaal liggen.
- Toon aan dat het aantal roosterpunten binnen de onderste driehoek gelijk is aan  $\alpha(q, p)$ .
- Toon aan dat het aantal roosterpunten binnen de bovenste driehoek gelijk is aan  $\alpha(p, q)$ .
- Toon aan dat

$$\alpha(p, q) + \alpha(q, p) = \frac{(p-1)(q-1)}{4}.$$

- Bewijs dat  $\left(\frac{q}{p}\right) \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ .

Hiermee is de wet bewezen.

**Voorbeeld 9.30.** Toon aan dat 3 een kwadraatrest is modulo een oneven priemgetal  $p > 3$  als en slechts als  $p \equiv \pm 1 \pmod{12}$ .

*Oplossing.*

De wet van de kwadratische reciprociteit zegt ons dat

$$\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)(3-1)}{4}} \cdot \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right).$$

Als het product  $(-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{3}\right)$  gelijk is aan 1, zijn beide factoren ofwel 1 ofwel  $-1$ . Stel eerst dat ze beide 1 zijn. Dan is  $p \equiv 1 \pmod{4}$  en  $p \equiv 1 \pmod{3}$ , wat wegens de Chinese reststelling gelijkwaardig is met  $p \equiv 1 \pmod{12}$ .

Stel nu dat ze beide  $-1$  zijn. Dan is  $p \equiv 3 \pmod{4}$  en  $p \equiv 2 \pmod{3}$  wat wegens de Chinese reststelling betekent dat  $p \equiv -1 \pmod{12}$ . Hiermee is de eigenschap aangetoond.

**Opgave 9.31.** Voor welke priemgetallen heeft de congruentie  $x^2 \equiv -3 \pmod{p}$  een oplossing?

**Opgave 9.32.** Stel dat  $p$  en  $q$  verschillende priemgetallen zijn zo dat minstens één van de vorm  $4k+1$  is. Bewijs dat  $q$  een kwadraatrest is modulo  $p$  als en slechts als  $p$  een kwadraatrest is modulo  $q$ .



### 9.2.3 Systematisch bepalen van het Legendre-symbool

Kwadratische reciprociteit laat ons toe om systematisch elk Legendre-symbool te bepalen. Met ‘systematisch’ bedoelen we zonder elegant nadenken zoals in Opgave 9.22. Beschouw  $n \in \mathbb{Z}$  en  $p$  een oneven priemgetal,  $p \nmid n$ . Als  $n < 0$  kunnen we het Legendre-symbool opsplitsen en het criterium van Euler gebruiken voor de factor  $-1$ . Als  $n$  even is kunnen we factoren 2 afsplitsen en daarvan het Legendre-symbool bepalen met Stelling 9.16. Stel nu  $n > 0$  oneven. Indien  $n > p$  bepalen we de rest  $r$  van  $n$  bij deling door  $p$ . Deze rest heeft in elk geval kleinere priemfactoren dan  $p$ . We kunnen het Legendre-symbool bepalen voor elk van die priemfactoren met kwadratische reciprociteit; dan komen er Legendre-symbolen te staan met kleinere priemgetallen in de “noemer”. Als we voor elk van de factoren dit proces blijven herhalen bekomen we steeds kleinere oneven priemgetallen tot er alleen nog 3 als noemer staat; en modulo 3 kunnen we gemakkelijk Legendre-symbolen berekenen.

We illustreren deze inzichtsloze methode:

**Voorbeeld 9.33.** Bepaal  $\left(\frac{-98}{17}\right)$ .

*Oplossing.*

We splitsen de factoren  $-1$  en  $2$  af:

$$\left(\frac{-98}{17}\right) = \left(\frac{-1}{17}\right) \left(\frac{2}{17}\right) \left(\frac{49}{17}\right) = (-1)^{\frac{17-1}{2}} (-1)^{\frac{17^2-1}{2}} \left(\frac{49}{17}\right) = 1 \cdot 1 \cdot \left(\frac{49}{17}\right).$$

We doen alsof we niet weten dat 49 een kwadraat is en gaan systematisch verder. We bepalen de rest van 49 modulo 17, die is 15:

$$\left(\frac{49}{17}\right) = \left(\frac{15}{17}\right) = \left(\frac{3}{17}\right) \left(\frac{5}{17}\right) = (-1)^{\frac{(17-1)(3-1)}{4}} \left(\frac{17}{3}\right) (-1)^{\frac{(17-1)(5-1)}{4}} \left(\frac{17}{5}\right).$$

Vereenvoudigd,  $\left(\frac{17}{3}\right) \cdot \left(\frac{17}{5}\right)$ . We bepalen eerst  $\left(\frac{17}{5}\right)$ :

$$\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{2}} = -1.$$

Verder is

$$\left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1.$$

Het antwoord is dus  $(-1) \cdot (-1) = 1$ . (Zoals te voorspellen was omdat  $49 = 7^2$ .)

Aangezien  $-1$  en  $2$  speciale gevallen zijn die de kwadratische reciprociteit niet behandeld, worden de stellingen hieromtrent respectievelijk het eerste en tweede supplement genoemd. De kwadratische reciprociteit en zijn twee supplementen laten tesamen toe om systematisch elk Legendre-symbool te bepalen.

## 9.3 Kwadratische congruenties

Analoog aan lineaire congruenties zijn er kwadratische congruenties.

**Definitie 9.34.** Kwadratische congruentie

Een kwadratische congruentie is een congruentie van de vorm

$$ax^2 + bx + c \equiv 0 \pmod{m} \quad (1)$$

waarbij  $a, b, c$  en  $m$  constant zijn en we gehele oplossingen zoeken voor  $x$ .

Opnieuw bedoelen we met “het aantal oplossingen modulo  $m$ ” het aantal oplossingen na reductie modulo  $m$ . We beschouwen enkel  $m \in \mathbb{N}^+$  omdat de congruentie voor negatieve moduli op precies hetzelfde neerkomt.

**Lemma 9.35.**

Zij  $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ , dan is  $x$  een oplossing van (1) als en slechts als  $x$  een oplossing van elk van de congruenties

$$ax^2 + bx + c \equiv 0 \pmod{p_k^{a_k}}.$$

*Bewijs.*

Triviaal. □

Als we de priemontbinding van  $m$  kennen is het probleem dus vereenvoudigd tot het vinden van oplossingen modulo machten van priemgetallen.

**9.3.1 Priemgetallen als moduli****Lemma 9.36.**

Als  $p$  een oneven priemgetal is en  $p \nmid a$  kan de congruentie

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

Herleid worden tot

$$y^2 \equiv d \pmod{p} \quad (2)$$

met  $y \equiv x + \frac{b}{2a}$  en  $d \equiv \frac{b^2 - 4ac}{4a^2}$ .

*Bewijs.*

Dit volgt meteen door  $x \equiv y - \frac{b}{2a}$  te substitueren. □

Indien  $p \mid a$  is de congruentie lineair, zodat de oplossingen eenvoudig kunnen worden bepaald. Het aantal oplossingen van (2) hangt af van het kwadratisch karakter van  $d$  modulo  $p$ .

**Stelling 9.37.**

Als  $p$  een oneven priemgetal is en  $p \nmid a$  heeft de congruentie

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

precies  $1 + \left(\frac{b^2 - 4ac}{p}\right)$  oplossingen modulo  $p$ .

*Bewijs.*

Als oefening. □

Het geval waar  $m$  een oneven priemgetal is beschouwen we als afgehandeld. We gaan verder met  $p^k$ ,  $p$  oneven.

**Stelling 9.38.****Stelling 9.39.**

Als  $m = p^k$  en  $p \mid a$  is de congruentie (1) te herleiden tot een kwadratische congruentie modulo  $p^{k-1}$ . Als  $p \nmid a$  kan de congruentie herleid worden tot

$$y^2 \equiv d \pmod{p^k}.$$

**9.3.2 Priemmachten en het lemma van Hensel****Opgaven hoofdstuk 9**

**Opgave 9.40.** Bewijs dat ✿

$$\left(\frac{\frac{p-1}{2}}{p}\right) = (-1)^{\frac{(p-1)(p+5)}{8}}.$$

**Opgave 9.41.** Zij  $m$  en  $n$  natuurlijke getallen. Bewijs dat  $4mn - m - n$  nooit een volkomen kwadraat is.

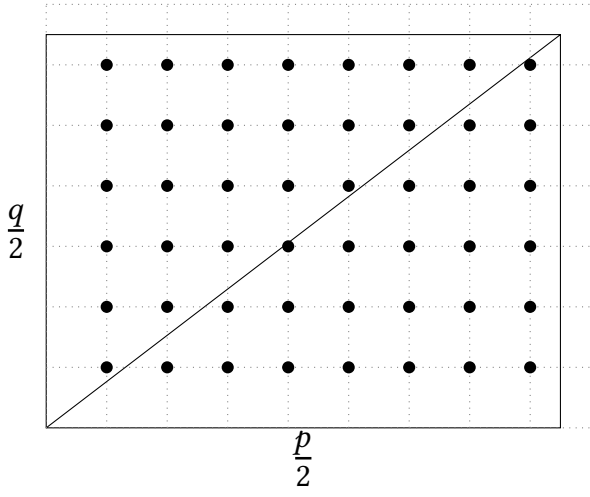
**Opgave 9.42.** Zijn  $a, b, c \in \mathbb{N}$  paarsgewijs relatief priem met  $c^2 = a^2 - ab + b^2$ . Zij  $p$  een priemdelers van  $c$ . Bewijs dat  $p \equiv 1 \pmod{6}$ .

**Opgave 9.43.** Bewijs dat  $16$  een achtste macht is modulo elk priemgetal  $p$ .

**Opgave 9.44.** (Polen MO 2013 vraag 2) Zij  $a$  en  $b$  gehele getallen zo dat  $6a \mid 3 + a + b^2$ . Bewijs dat  $a < 0$ .

**Opgave 9.45.** Voor welke natuurlijke getallen  $n$  bestaat er een natuurlijk getal  $m$  zo dat

$$2^n - 1 \mid m^2 + 9?$$



# 10 Polynoomcongruenties

## Definitie 10.1.

Een veelterm  $f$  over  $\mathbb{Z}$  is een veelterm met gehele coëfficiënten. We noteren  $f \in \mathbb{Z}[x]$  voor een veelterm in de variabele  $x$ . Analoog hebben we  $\mathbb{Q}[x]$ ,  $\mathbb{R}[x]$  en  $\mathbb{C}[x]$ .

## Definitie 10.2. Monische veelterm

Een veelterm  $f \in \mathbb{C}[x]$  waarvan de hoogste graadscoëfficiënt 1 is noemt men monisch.

## Lemma 10.3.

Als  $f, g \in \mathbb{Q}[x]$  monisch zijn en  $fg \in \mathbb{Z}[x]$ , dan zijn  $f, g \in \mathbb{Z}[x]$ .

**Opgave 10.4.** We bewijzen Lemma 10.3.

Stel  $f(x) = x^k + a_{k-1}x^{k-1} + \dots + a_0$  en  $g(x) = x^l + b_{l-1}x^{l-1} + \dots + b_0$ . Noem  $m$  en  $n$  de kleinste natuurlijke getallen zo dat  $mf$  en  $ng$  gehele coëfficiënten hebben. Stel  $a_k = 1$  en  $b_l = 1$ . Stel dat  $mn > 1$  en zij  $p$  een priemdelers van  $mn$ .

A. Bewijs dat er  $s$  en  $t$  bestaan zo dat  $p \nmid ma_s$  en  $p \nmid nb_t$ .

Kies nu voor  $s$  en  $t$  telkens de grootste onder de mogelijke waarden.

B. Toon aan dat de coëfficiënt van  $x^{s+t}$  in  $mng$  niet deelbaar is door  $p$ .

Dit is echter onmogelijk omdat  $p \mid mn$  en  $fg \in \mathbb{Z}[x]$ . Dus  $mn = 1$ , zodat  $f, g \in \mathbb{Z}[x]$ .

## 10.1 Begrippen

We breiden de betekenis van enkele begrippen uit tot het modulorekenen.

## Definitie 10.5. Nulpunt modulo $m$

Als  $f \in \mathbb{Z}[x]$  zeggen we dat  $n$  een nulpunt van  $f$  is modulo  $m$  als  $f(n) \equiv 0 \pmod{m}$ .

**Definitie 10.6.** Nulveelterm

Als  $f \in \mathbb{Z}[x]$  zo dat alle coëfficiënten van  $f$  deelbaar zijn door  $m$  noemen we  $f$  een nulveelterm modulo  $m$ . We noteren  $f \equiv 0 \pmod{m}$ .

Als we het hebben over het aantal nulpunten modulo  $m$ , dan bedoelen we zoals gewoonlijk het aantal nulpunten na reductie modulo  $m$ . Een veelterm heeft dus hoogstens  $|m|$  nulpunten modulo  $m$ .

**Definitie 10.7.** Veeltermcongruentie

Twee veeltermen  $f, g \in \mathbb{Z}[x]$  noemen we congruent modulo  $m$  als  $f - g \equiv 0 \pmod{m}$ . We noteren dan  $f \equiv g \pmod{m}$ .

We zullen ook soms de notatie  $f(x) \equiv g(x)$  gebruiken in plaats van  $f \equiv g$ . Deze notatie is dubbelzinnig, want ze zou ook kunnen inhouden dat voor het geheel getal  $x$  geldt dat  $f(x) \equiv 0$ . Indien de veranderlijke, bijvoorbeeld  $x$ , geen expliciete betekenis heeft in de huidige context wordt in zo'n situaties steeds  $f \equiv g$  bedoeld.

Er volgt dat veeltermen de basiseigenschappen van congruenties voor gehele getallen overerven:

**Stelling 10.8.** Eigenschappen van veeltermcongruenties

Als  $a, b, c, d \in \mathbb{Z}[x]$  en  $m \in \mathbb{Z}$  zo dat  $a \equiv b$  en  $c \equiv d \pmod{m}$ , dan geldt:

1.  $a + c \equiv b + d$ .
2.  $ac \equiv bd$ .
3.  $a^n \equiv b^n$  voor elke  $n \in \mathbb{N}^+$ .

**Opgave 10.9.** Bewijs.

H

**Definitie 10.10.** Graad van een veelterm

De *graad* van  $f(x)$  modulo  $m$  is de hoogst voorkomende exponent van  $x$ , waarbij de coëfficiënt niet deelbaar is door  $m$ . Een nulveelterm modulo  $m$  heeft per definitie geen graad modulo  $m$ .

Bijvoorbeeld, de graad van  $3 + 6x + 30x^2 - 12x^3$  modulo 5 is 3, modulo 4 is die 2, modulo 2 is die 0 en modulo 3 heeft de veelterm geen graad: het is de nulveelterm.

**10.2 Factorisatiestellingen**

**Stelling 10.11.**

Als  $f \in \mathbb{Z}[x]$  graad  $k > 0$  heeft en  $n$  is een nulpunt van  $f$  modulo  $m$ , dan bestaat er een veelterm  $g \in \mathbb{Z}[x]$  van graad  $k - 1$  zo dat  $f(x) \equiv (x - n) \cdot g(x) \pmod{m}$ .

*Bewijs.*

Stel  $f = a_0 + a_1x + \dots + a_kx^k$ , dan is

$$f \equiv a_0 - a_0 + a_1(x - n) + \dots + a_k(x^k - n^k)$$

omdat  $a_0 + a_1n + \dots + a_kn^k \equiv 0$ . Elke veelterm  $a_1(x - n), a_2(x^2 - n^2), \dots, a_k(x^k - n^k)$  kan wegens Stelling B.2 ontbonden worden door een factor  $(x - n)$  voorop te zetten. Dus ook hun som  $f$  kan ontbonden worden in de vorm  $(x - n) \cdot g(x)$ . Tenslotte is  $\deg g = n - 1$  omdat  $a_k \neq 0$ .  $\square$

**Stelling 10.12.**

Als  $p$  een priemgetal is heeft een veelterm van graad  $n$  modulo  $p$  hoogstens  $n$  nulpunten modulo  $p$ .

**Opgave 10.13.** Bewijs.

We bewijzen dat elke veelterm van graad  $n$  die  $n + 1$  nulpunten heeft modulo  $p$  toch een nulveelterm is modulo  $p$ . Noem  $f$  zo'n veelterm.

- Toon aan dat  $f \equiv a(x - x_1)(x - x_2) \cdots (x - x_n)$  voor gehele getallen  $x_k$  die onderling incongruent zijn modulo  $p$  en met  $a \in \mathbb{Z}$ .
- Toon aan dat  $f$  toch geen graad heeft.

De vorige stelling laat een alternatief bewijs voor de stelling van Wilson toe.

**Opgave 10.14.** (Stelling van Wilson m.b.v. Stelling 10.12) Zij  $p$  een priemgetal. Beschouw de veelterm

$$f(x) = (x - 1)(x - 2) \cdots (x - (p - 1)) - x^{p-1} + 1.$$

- Toon aan dat  $f$  hoogstens van graad  $p - 2$  is modulo  $p$ .
- Toon aan dat  $f$  een nulveelterm is modulo  $p$ .
- Vind nu een handige  $x$  om uit  $f(x) \equiv 0 \pmod{p}$  de stelling van Wilson af te leiden.

**Stelling 10.15.**

Als  $p$  een priemgetal is,  $d \in \mathbb{N}$  en  $d \mid p - 1$ , dan heeft de veelterm  $x^d - 1$  precies  $d$  nulpunten modulo  $p$ .

**Opgave 10.16.** Bewijs.

Stel  $p - 1 = dk$  en  $f(x) = 1 + x^d + (x^d)^2 + \dots + (x^d)^{k-1}$ .

- Toon aan dat  $x^{p-1} - 1 = (x^d - 1)f(x)$  precies  $dk$  nulpunten heeft modulo  $p$ .
- Toon aan dat  $x^d - 1$  precies  $d$  nulpunten heeft modulo  $p$ .

### 11.1 Lifting The Exponent

Uit Lemma 8.23 weten we dat  $a \equiv b \pmod{p^k}$  ( $k \geq 1$ ) impliceert dat  $a^p \equiv b^p \pmod{p^{k+1}}$ . Lifting The Exponent pluist dit fenomeen verder uit door te onderzoeken wat de grootste macht van  $p$  is die  $a^n - b^n$  deelt.

#### Lemma 11.1.

Als  $p$  een priemgetal is,  $p \nmid n$ ,  $x, y$  en  $p \mid x - y$ , dan geldt

$$v_p(x^n - y^n) = v_p(x - y).$$

**Opgave 11.2.** Bewijs.

H

#### Stelling 11.3. Het eigenlijke LTE

Als  $p$  een oneven priemgetal is zo dat  $p \nmid x, y$  en  $p \mid x - y$ , en  $n$  is een natuurlijk getal, dan geldt

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

**Opgave 11.4.** (Lifting The exponent) We bewijzen dit via inductie op  $v_p(n)$ .

Basisstap. We tonen het aan als  $v_p(n) = 1$ . Stel dus  $n = pb$  zo dat  $p \nmid b$ .

- Toon aan dat  $v_p(x^n - y^n) = v_p(x^p - y^p)$ .
- Toon aan dat

$$p \mid \sum_{k=0}^{p-1} x^k y^{p-k-1}.$$

Vervolgens tonen we aan dat

$$p^2 \nmid \sum_{k=0}^{p-1} x^k y^{p-k-1}. \quad (1)$$

Stel daarvoor  $y = x + mp$ .

- Toon aan dat  $x^k y^{p-k-1} \equiv x^{p-1} + kmpx^{p-2} \pmod{p^2}$ .
- Toon (1) aan.
- Toon aan dat  $v_p(x^n - y^n) = v_p(x - y) + 1$ .

Hiermee is de basisstap voltooid.

Inductiestap. Veronderstel dat het lemma geldt voor  $v_p(n) = a$  met  $a > 0$ . We tonen het lemma nu aan voor  $v_p(n) = a + 1$ . Stel dus  $n = p^{a+1}b$  zo dat  $p$  geen deler is van  $b$ .



- F. Toon aan dat  $v_p(x^n - y^n) = v_p(x^{p^{a+1}} - y^{p^{a+1}})$ .
- G. Toon aan dat  $v_p(x^n - y^n) = v_p(x^{p^a} - y^{p^a}) + 1$ .
- H. Bewijs dat  $v_p(x^n - y^n) = v_p(x - y) + v_p(n)$ .

Het is nu bewezen via inductie.

**Gevolg 11.5.**

Als  $n$  oneven is,  $p$  oneven,  $p \nmid x, y$  en  $p \mid x + y$ , dan is

$$v_p(x^n + y^n) = v_p(x + y) + v_p(n).$$

**11.1.1 Het geval  $p = 2$**

**Stelling 11.6.** LTE voor het geval  $p = 2$

Als  $x$  en  $y$  oneven zijn zo dat  $4 \mid x - y$ , dan geldt

$$v_2(x^n - y^n) = v_2(x - y) + v_2(n)$$

voor elk natuurlijk getal  $n$ .

Merk op dat de voorwaarde hier niet  $2 \mid x - y$  maar  $4 \mid x - y$  is. Onder andere daarom is het nodig om het geval  $p = 2$  apart te beschouwen.

**Opgave 11.7.** Bewijs LTE als  $p = 2$ .

Stel  $n = 2^a b$  met  $b$  oneven.

- A. Toon aan dat  $v_2(x^n - y^n) = v_2(x^{2^a} - y^{2^a})$ .

Er geldt dat

$$x^{2^a} - y^{2^a} = (x - y) \cdot \prod_{i=0}^{a-1} (x^{2^i} + y^{2^i}).$$

- B. Toon aan dat  $x^{2^i} + y^{2^i} \equiv 2 \pmod{4}$  voor  $i \geq 0$ .
- C. Bewijs dat  $v_2(x^n - y^n) = v_2(x - y) + v_2(n)$ .

Ook Stelling 11.6 geldt nu als bewezen.

**Gevolg 11.8.**

Voor oneven  $n \in \mathbb{N}$  geldt dat als  $x$  en  $y$  oneven zijn en  $4 \mid x + y$ , dan

$$v_2(x^n + y^n) = v_2(x + y) + v_2(n).$$

Het vierde lemma is een variatie op lemma 3. Het behandelt nog steeds het geval  $p = 2$ , maar de voorwaarden zijn anders.

**Stelling 11.9.** Uitbreiding op het geval  $p = 2$

Als  $x$  en  $y$  oneven zijn en  $n$  even, dan

$$v_2(x^n - y^n) = v_2(x + y) + v_2(x - y) + v_2(n) - 1.$$

**Opgave 11.10.** Bewijs.

Stel  $n = 2^a b$  met  $b$  oneven.

- A. Toon aan dat  $v_2(x^n - y^n) = v_2(x^{2^a} - y^{2^a})$ .
- B. Toon aan dat  $4 \mid x^2 - y^2$ .
- C. Toon aan dat  $v_2(x^n - y^n) = v_2(x^2 - y^2) + a - 1$ .
- D. Bewijs dat  $v_2(x^n - y^n) = v_2(x + y) + v_2(x - y) + v_2(n) - 1$ .

Ook het vierde lemma is nu bewezen.

### 11.1.2 LTE in deelbaarheidsgedaante

LTE kent een quasi-equivalente vorm, waarbij verassend genoeg geen congruenties worden gebruikt.

**Opgave 11.11.** Stel  $a, b$  zijn gehele getallen met  $a \neq b$  en  $\text{ggd}(a, b) = 1$ . In Opgave 1.52 en Opgave 1.53 zagen we reeds dat  $\text{ggd}(a + b, a - b) \mid 2$  en  $\text{ggd}(a^2 + ab + b^2, a - b) \mid 3$ . Toon nu algemeen aan dat

$$\text{ggd}\left(\frac{a^n - b^n}{a - b}, a - b\right) \mid n$$

voor  $n > 1$ .

**Opgave 11.12.** Zij  $a, b \in \mathbb{Z}$  met  $a \neq b$  en  $n > 1$ . Bewijs dat

$$\text{ggd}\left(\frac{a^n - b^n}{a - b}, a - b\right) = \text{ggd}(nd^{n-1}, a - b)$$

waarbij  $d = \text{ggd}(a, b)$ .

**Stelling 11.13.** LTE in deelbaarheidsgedaante

### 11.1.3 De klassieke Diophant

LTE is de laatste jaren erg populair gebleken in olympiades. Wie destijds het geluk had om LTE te kennen had vaak een mooie voorsprong. Wellicht heeft men nu door dat LTE bij de meeste problem-solvers bekend is geraakt; mogelijks de verklaring waarom de LTE-hype nu aan zijn einde lijkt te zijn gekomen.

**Opgave 11.14.** (BxMO 2010 vraag 4) Bepaal alle viertallen  $(a, b, p, n)$  van natuurlijke getallen groter dan 0 zo dat  $p$  een priemgetal is en  $a^3 + b^3 = p^n$ .

**Opgave 11.15.** (EMC 2012 vraag 1) Vind alle natuurlijke getallen  $a, b, n > 0$  en priemgetallen  $p$  waarvoor geldt dat  $a^{2013} + b^{2013} = p^n$ .

**Opgave 11.16.** (Frankrijk 2012 dag 1 vraag 3) Vind alle viertallen  $(p, a, b, c)$  met  $p$  priem en  $a, b, c > 0$  gehele getallen zo dat geldt dat  $a^p + b^p = p^c$ .

## 11.2 Primitieve wortels

Uit het ordelemma en de stelling van Euler volgt dat een getal hoogstens orde  $\varphi(n)$  heeft modulo  $n$ . De vraag rijst of er ook getallen bestaan die precies orde  $\varphi(n)$  hebben.

### Definitie 11.17. Primitieve wortel

We noemen  $a$  een primitieve wortel modulo  $n$  als  $\text{ord}_n(a) = \varphi(n)$ .

**Opgave 11.18.** Toon aan dat  $2^{2 \cdot 3^{n-1}} \equiv 1 + 3^n \pmod{3^{n+1}}$  en dat 2 een primitieve wortel is modulo  $3^n$ , voor  $n \geq 1$ .

### 11.2.1 Existentie

#### Stelling 11.19. Nodige voorwaarde voor primitieve wortels

Als  $n$  een primitieve wortel heeft, dan is  $n = 1, 2, 4, n = p^k$  of  $n = 2p^k$  met  $p$  priem en  $k > 0$ .

**Opgave 11.20.** Stel  $n = p_1^{e_1} \cdots p_k^{e_k}$ . Bewijs dat er slechts een primitieve wortel kan bestaan modulo  $n$  als  $\text{ggd}(\varphi(p_1^{e_1}), \dots, \varphi(p_k^{e_k})) = 1$ . Leid hier de vorige stelling uit af.

Het is duidelijk dat er inderdaad primitieve wortels zijn modulo 1, 2 en 4. In wat volgt bewijzen we dat er ook primitieve wortels zijn modulo  $p^k$  en  $2p^k$  met  $p$  een oneven priemgetal.

#### Lemma 11.21.

Als  $p$  een oneven priemgetal is en  $q$  is een priemdelers van  $p$  zo dat  $q^k \mid p - 1$ , dan bestaat er een getal met orde  $q^k$  modulo  $p$ .

**Opgave 11.22.** Bewijs zelf eens.

#### Stelling 11.23.

Als  $p$  een oneven priemgetal is,  $d \in \mathbb{N}$  en  $d \mid p - 1$  dan bestaat er een getal met orde  $d$  modulo  $p$ . In het bijzonder bestaat er een primitieve wortel modulo  $p$ .

*Bewijs.*

Stel  $d = q_1^{e_1} \cdots q_k^{e_k}$ . Om getallen te construeren met orde  $q_i^{e_i}$  gebruiken we Lemma 11.21, en om een getal te construeren waarvan de orde  $d$  is gebruiken we Lemma 8.9.  $\square$

**Gevolg 11.24.**

Als  $d \in \mathbb{N}$  en  $d \mid p - 1$  bestaan er  $\varphi(d)$  onderling incongruente getallen van orde  $d$ .

*Bewijs.*

De vergelijking  $x^d - 1 = 0$  heeft precies  $d$  nulpunten modulo  $p$ . Er bestaat een getal  $g$  van orde  $d$ , dus zullen de getallen  $1, g, g^2, \dots, g^{d-1}$  alle oplossingen zijn van deze vergelijking. Elk getal van orde  $d$  is een oplossing van deze vergelijking en dus van de vorm  $g^k$ . Lemma 8.10 zegt dat  $g^k$  ook orde  $d$  heeft als en slechts als  $\text{ggd}(k, d) = 1$ . Er zijn zo  $\varphi(d)$  waarden van  $k$ , dus ook  $\varphi(d)$  getallen van orde  $d$ .  $\square$

Er bestaan dus ook  $\varphi(p - 1)$  primitieve wortels modulo  $p$ , maar hier komen we later algemener op terug. We breiden het bestaan van primitieve wortels uit naar  $p^k$ .

**Lemma 11.25.**

Als  $w$  een primitieve wortel is modulo een oneven priemgetal  $p$  en  $w^{p-1} \not\equiv 1 \pmod{p^2}$ , dan is  $w^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$  voor alle  $k > 0$ .

**Opgave 11.26.** Bewijs.

H

**Stelling 11.27.**

Zij  $w$  een primitieve wortel modulo een oneven priemgetal  $p$ . Dan is  $w$  of  $w + p$  een primitieve wortel modulo  $p^k$  voor alle  $k > 0$ .

*Bewijs.*

Als oefening.  $\square$

Er rest nog het geval  $2p^k$ . Ook hier zullen primitieve wortels bestaan.

**Opgave 11.28.** Bewijs dat er een primitieve wortel bestaat modulo  $2n$  als er een bestaat modulo  $n$ , voor elke oneven  $n > 0$ .

- A. Stel  $w$  is oneven en een primitieve wortel modulo  $n$ . Toon aan dat  $w$  een primitieve wortel is modulo  $2n$ .
- B. Stel  $w$  is even, en is een primitieve wortel modulo  $n$ . Toon aan dat  $w + n$  een primitieve wortel is modulo  $2n$ .

De volgende stelling volgt meteen:

**Stelling 11.29.**

Er bestaat een primitieve wortel modulo  $2p^k$  met  $p$  priem.

**11.2.2 Eigenschappen**

Het bestaan van primitieve wortels is dus gegarandeerd, maar er is nog geen efficiënte manier bekend om primitieve wortels te vinden modulo priemgetallen.

De volgende eigenschap karakteriseert primitieve wortels. Soms wordt ze als definitie gebruikt.

**Stelling 11.30.**

$w$  is een primitieve wortel modulo  $n$  als en slechts als de resten van  $w, w^2, \dots, w^{\varphi(n)}$  bij deling door  $n$  allemaal verschillend zijn.

*Bewijs.*

Wegens Gevolg 8.4 is dit een equivalente formulering van  $\text{ord}_n(w) = \varphi(n)$ . □

**Gevolg 11.31.**

Als  $w$  een primitieve wortel is zijn de resten van  $w, w^2, \dots, w^{\varphi(n)}$  precies de getallen in  $\{1, \dots, n\}$  die relatief priem zijn met  $n$ . Elke andere primitieve wortel moet dus van de vorm  $w^k$  zijn.

**Stelling 11.32.**

Indien er een primitieve wortel bestaat modulo  $n$ , zijn er precies  $\varphi(\varphi(n))$  primitieve wortels.

*Bewijs.*

Indien  $w$  een primitieve wortel is, is wegens Lemma 8.10 elke primitieve wortel van de vorm  $w^k$  met  $\text{ggd}(k, \varphi(n)) = 1$ . □

Primitieve wortels zijn heel handige getallen omdat ze toestaan om berekeningen en bewijzen te vereenvoudigen. Ze laten ons zelfs een derde bewijs van de stelling van Wilson toe.

**Opgave 11.33.** (Stelling van Wilson met primitieve wortels) Stel dat er een primitieve wortel bestaat modulo  $n$  en zij  $A$  de verzameling van natuurlijke getallen in  $\{1, \dots, n\}$  relatief priem met  $n$ . Toon aan dat

$$\prod_{a \in A} a \equiv -1 \pmod{n},$$

en leidt hieruit de stelling van Wilson af.

**Stelling 11.34.** Product van primitieve wortels

Het product van alle primitieve wortels modulo  $p$  is congruent met 1 modulo  $p$ .

**Opgave 11.35.** Bewijs.

H

**Stelling 11.36.** Som van primitieve wortels

De som van alle primitieve wortels modulo  $p$  is congruent met  $\mu(p-1)$  modulo  $p$ .

**Opgave 11.37.** Bewijs.



**Opgave 11.38.** Zij  $p$  een priemgetal. Bewijs dat de som van de vjdemachten van  $1, 2, \dots, p-1$  deelbaar is door  $p$ .

**Opgave 11.39.** Toon aan dat als  $a$  een primitieve wortel is modulo  $n$  met  $n > 2$ , dan  $n \mid a^{\frac{\varphi(n)}{2}} + 1$ .

**Opgave 11.40.** Bepaal de grootste gemene deler van de getallen van de vorm  $n^{13} - n$ .

### 11.2.3 Indexrekenen

**Definitie 11.41.** Index

Zij  $n$  een natuurlijk getal met een primitieve wortel  $w$  en  $a \in \mathbb{Z}$  met  $\text{ggd}(a, n) = 1$ . Het unieke natuurlijke getal  $k \in \{0, \dots, \varphi(n) - 1\}$  waarvoor  $w^k \equiv a \pmod{n}$  noemen we de *index* van  $k$  modulo  $n$  t.o.v de *basis*  $w$ .

## 11.3 Cyclotomische veeltermen

*Gebaseerd op [5]*

Cyclotomische veeltermen zijn een bijzonder soort veeltermen in  $\mathbb{Z}[x]$ . Ze hebben heel wat interessante eigenschappen.

**Definitie 11.42.** Eenheidswortel

Een complex getal  $\zeta$  waarvoor  $\zeta^n = 1$  noemen we een  $n$ -de eenheidswortel.

De  $n$ -de eenheidswortels zijn precies  $e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \dots, e^{\frac{2\pi i(n-1)}{n}}$ .

**Definitie 11.43.** Orde van een eenheidswortel

Als  $\zeta$  een  $n$ -de eenheidswortel is, noemen we de kleinste  $k \in \mathbb{N}^+$  waarvoor  $\zeta^k = 1$  de *orde* van  $\zeta$ . We noteren  $\text{ord}(\zeta)$ .

De volgende eigenschap komt je vast bekend voor.

**Lemma 11.44.** Ordelemma voor eenheidswortels

Als  $\zeta$  een  $n$ -de eenheidswortel is, dan is  $\zeta^k = \zeta^l$  als en slechts als  $k \equiv l \pmod{\text{ord}(\zeta)}$ , voor alle  $k, l \in \mathbb{Z}$ .

*Bewijs.*

$\zeta^k = \zeta^l$  als en slechts als  $\zeta^{k-l} = 1$ . Stel  $\text{ord}(\zeta) = x$  en  $k - l = qx + r$  met  $0 \leq r < x$ .

Er volgt dat  $\zeta^r = 1$ , dus  $r = 0$ . □

**Definitie 11.45.** Primitieve eenheidswortel

Een  $n$ -de eenheidswortel  $\zeta$  noemen we primitief als  $\text{ord}(\zeta) = n$ . We noemen  $\zeta$  een primitieve  $n$ -eenheidswortel.

In het bijzonder is  $e^{\frac{2\pi i}{n}}$  steeds primitief.

**Lemma 11.46.** Criterium voor primitiviteit

Een  $n$ -de eenheidswortel  $\zeta$  is primitief als en slechts als de verzameling  $\{\zeta, \zeta^2, \dots, \zeta^n\}$  alle  $n$ -de eenheidswortels bevat.

*Bewijs.*

Dit volgt meteen uit Lemma 11.44. □

**Lemma 11.47.**

Zij  $k \in \mathbb{Z}$  en  $\zeta$  een primitieve  $n$ -eenheidswortel. Dan is  $\zeta^k$  ook primitief als en slechts als  $\text{ggd}(k, n) = 1$ .

*Bewijs.*

Als oefening. □

Merk op dat heel wat eigenschappen van de orde van eenheidswortels lijken op eigenschappen van de orde in modulorekenen... Toeval? Helemaal niet; zie Hoofdstuk 18.

**Gevolg 11.48.** Aantal primitieve eenheidswortels

Er zijn precies  $\varphi(n)$  primitieve  $n$ -eenheidswortels.

**Definitie 11.49.** Cyclotomische veelterm

De  $n$ -de cyclotomische veelterm is de monische veelterm

$$\Phi_n(x) = \prod_{\text{ord}(\zeta)=n}^n (x - \zeta),$$

waarbij het product loopt over alle primitieve  $n$ -eenheidswortels.

**Gevolg 11.50.**

$\Phi_n(x)$  heeft graad  $\varphi(n)$ .

*Bewijs.*

Dit volgt uit Gevolg 11.48. □

**11.3.1 Algebraïsche eigenschappen**

We bekijken enkele voorbeelden van cyclotomische veeltermen. We beginnen met  $n = 1$ . 1 is de enige 1-de machtswortel van 1 met orde 1, dus  $\Phi_1(x) = x - 1$ .

De enige vierkantswortel van 1 met orde 2 is  $-1$ , dus  $\Phi_2(x) = x - (-1) = x + 1$ .

Er zijn juist  $\varphi(4) = 2$  primitieve 4-demachtswortels van 1, namelijk  $i$  en  $-i$ . Dus  $\Phi_4(x) = (x - i)(x + i) = x^2 + 1$ .

Het bepalen van cyclotomische veeltermen wordt een stuk eenvoudiger met:

**Stelling 11.51.**

Er geldt dat

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

*Bewijs.*

Aangezien elke  $n$ -de eenheidswortel  $\zeta$  een unieke orde heeft komt elke factor  $(x - \zeta)$  één keer voor in het rechterlid. Omdat het product van al die factoren  $(x - \zeta)$  precies  $x^n - 1$  is, geldt de gelijkheid. □

Merk op dat, aangezien beide leden dezelfde graad hebben, deze stelling een nieuw bewijs levert voor

$$\sum_{d|n} \varphi(d) = n.$$

We kunnen nu gemakkelijk cyclotomische veeltermen bepalen. Bekijk een priemgetal  $p$ . Dan is  $\Phi_p(x)\Phi_1(x) = x^p - 1$ , dus:



**Gevolg 11.52.**

Voor priemgetallen  $p$  is

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}.$$

Hoe zit het dan met  $\Phi_p(1)$ ? Is die wel gedefinieerd? Het antwoord is ja, maar de notatie van  $\Phi_p(x)$  als breuk is misleidend. Met die breuk wordt bedoeld dat  $\Phi_p$  de quotiëntveelterm is bij deling van  $x^p - 1$  door  $x - 1$ . Dus

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Vandaar  $\Phi_p(1) = p$ .

We kunnen Stelling 11.51 en Gevolg 11.52 gebruiken om  $\Phi_n$  te bepalen voor  $n$  die geen priemgetal zijn. Bijvoorbeeld,

$$\Phi_6(x) = \frac{x^6 - 1}{\Phi_3(x)\Phi_2(x)\Phi_1(x)} = \frac{x^6 - 1}{(x+1)(x^3 - 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1.$$

**Opgave 11.53.** Zij  $p > 2$  priem. Bewijs dat  $\Phi_{2p}(x) = \Phi_p(-x)$ .

**Stelling 11.54.**

De cyclotomische veelterm  $\Phi_n$  heeft gehele coëfficiënten.

*Bewijs.*

Via inductie. Voor  $n = 1$  is het duidelijk. Stel dat het waar is voor alle natuurlijke getallen kleiner dan  $n$ . Omdat

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)}$$

is  $\Phi_n \in \mathbb{Q}[x]$  als quotiënt van rationale veeltermen. Omdat

$$\Phi_n \cdot \prod_{\substack{d|n \\ d \neq n}} \Phi_d \in \mathbb{Z}[x]$$

geldt nu wegens Lemma 10.3 dat ook  $\Phi_n \in \mathbb{Z}[x]$ . □

**Gevolg 11.55.**

Als  $a \in \mathbb{Z}$  en  $n \in \mathbb{N}$ , dan is  $\Phi_n(a) \mid a^n - 1$ .

**Stelling 11.56.**

Er geldt dat

$$\Phi_n(x) = \prod_{d|n} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}$$

voor alle  $x \in \mathbb{C}$  die geen  $n$ -de eenheidswortel zijn.

*Bewijs.*

De gelijkheid geldt voor alle  $x \in \mathbb{C}$  waarvoor  $x^n \neq 1$  wegens Stelling 5.25 en Stelling 11.51.  $\square$

*Opmerking.*

We zullen de voorwaarde  $x^n \neq 1$  in het vervolg niet steeds vermelden, en gewoon veronderstellen dat hieraan voldaan is.

**Gevolg 11.57.**

Er geldt dat  $\Phi_n(x) > 0$  voor alle  $x > 1$  en  $n \in \mathbb{N}^+$ .

**Lemma 11.58.**

Zij  $p$  een priemgetal en  $n \in \mathbb{N}^+$ , dan geldt

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{als } p \mid n \\ \frac{\Phi_n(x^p)}{\Phi_n(x)} & \text{als } p \nmid n. \end{cases}$$

*Bewijs.*

Als oefening.  $\square$

**Gevolg 11.59.**

Als  $p$  priem is en  $k, n \in \mathbb{N}^+$  hebben we

$$\Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}) & \text{als } p \mid n \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})} & \text{als } p \nmid n. \end{cases}$$

*Bewijs.*

Herhaaldelijk toepassen van Lemma 11.58.  $\square$

**11.3.2 Toepassingen in de getaltheorie**

**Lemma 11.60.**

Zij  $p$  een priemgetal. Als de veelterm  $x^n - 1$  een dubbele wortel heeft modulo  $p$ , m.a.w. als er  $a \in \mathbb{Z}$  en  $Q \in \mathbb{Z}[x]$  bestaan waarvoor

$$x^n - 1 \equiv (x - a)^2 Q(x) \pmod{p},$$

dan is  $p \mid n$ .

*Bewijs.*

We werken modulo  $p$ . Uit  $a^n \equiv 1$  volgt dat  $p \nmid a$ . Stellen we  $y = x - a$ , dan geldt

$$(a + y)^n - 1 \equiv y^2 f(y + a).$$

Beide veeltermen zijn congruent en hebben dus onder andere congruente coëfficiënten bij de eerstegraadsterm. In het rechterlid is die coëfficiënt 0, en in het linkerlid is die  $na^{n-1}$ . Dus  $p \mid na^{n-1}$ , zodat  $p \mid n$ . □

Nu zijn de meeste ‘saai’ eigenschappen achter de rug. Hoog tijd om de cyclotomische veeltermen met getaltheorie te vermengen.

**Lemma 11.61.**

Zij  $a \in \mathbb{Z}$ ,  $n, d \in \mathbb{N}$  zo dat  $d \mid n$  en  $d < n$ . Als  $p$  een gemeenschappelijke priemdelers is van  $\Phi_n(a)$  en  $\Phi_d(a)$ , dan geldt  $p \mid n$ .

*Bewijs.*

Als oefening. □

**Stelling 11.62.**

Zij  $n \in \mathbb{N}$  en  $a \in \mathbb{Z}$ . Elke priemdelers  $p$  van  $\Phi_n(a)$  voldoet aan  $p \equiv 1 \pmod{n}$  of  $p \mid n$ .

**Opgave 11.63.** Bewijs.

$p$  is geen delers van  $a$ , aangezien  $p \mid \Phi_n(a) \mid a^n - 1$  wegens Gevolg 11.55. Stel  $\text{ord}_p(a) = k$ .

- A. Toon aan dat  $k \mid n$ .
- B. Bewijs dat uit  $k = n$  volgt dat  $p \equiv 1 \pmod{n}$ .
- C. Bewijs dat uit  $k < n$  volgt dat  $p \mid n$ .

Een spectaculair gevolg:

**Stelling 11.64.**

Als  $n \in \mathbb{N}^+$  bestaan er oneindig veel priemgetallen van de vorm  $kn + 1$ .

**Opgave 11.65.** Bewijs.

H

Het lijkt aannemelijk dat voor natuurlijke getallen  $a$  en  $b$  met  $\text{ggd}(a, b) = 1$  er oneindig veel priemgetallen bestaan die congruent zijn met  $b$  modulo  $a$ . Inderdaad:

**Stelling 11.66.** Stelling van Dirichlet, kwalitatieve vorm

Als  $a, b \in \mathbb{N}^+$  met  $\text{ggd}(a, b) = 1$  zijn er oneindig veel priemgetallen van de vorm  $ka + b$ .

Het bewijs maakt – zover ik weet – zwaar gebruik van complexe analyse en stellen we uit tot Hoofdstuk 21.

**Stelling 11.67.**

Als  $n, m \in \mathbb{N}$  en  $a \in \mathbb{Z}$  zo dat  $\text{ggd}(\Phi_n(a), \Phi_m(a)) > 1$ . Dan is  $\frac{m}{n} = p^k$  met  $k \in \mathbb{Z}$  en  $p$  een priemgetal. Indien bovendien  $m \neq n$  is die grootste gemene deler ook van de vorm  $p^l$ ,  $l \in \mathbb{N}^+$ .

**Opgave 11.68.** Bewijs.

Zij  $p$  een priemdelers van  $\text{ggd}(\Phi_n(a), \Phi_m(a))$ . Stel  $m = p^s x$  en  $n = p^t y$  met  $s, t \geq 0$  en  $p \nmid xy$ . We moeten aantonen dat  $x = y$ .

- A. Toon aan dat  $p \mid \Phi_x(a^{p^s})$  en  $p \mid \Phi_y(a^{p^t})$ .
- B. Bewijs dat  $p \mid \Phi_x(a)$  en  $p \mid \Phi_y(a)$ .

Veronderstel nu dat  $x > y$ . Stel  $g = \text{ggd}(x, y)$ .

- C. Toon aan dat  $p \mid a^g - 1$ .
- D. Toon aan dat  $p$  toch een deler zou zijn van  $x$ .

Bijgevolg geldt  $x = y$ . Deze redenering konden we toepassen op elke priemdelers van  $\text{ggd}(\Phi_n(a), \Phi_m(a))$ , dus hebben we, indien  $\frac{m}{n} \neq 1$ , noodzakelijk steeds hetzelfde priemgetal.

**Opgave 11.69.** (IMOSL 2006) Vind alle gehele oplossingen van de vergelijking

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

**Stelling 11.70.**

De primitieve wortels modulo  $p$  zijn de nulpunten van  $\Phi_{p-1}$  modulo  $p$ .

**Opgave 11.71.** Bewijs.

H

Het vinden van primitieve wortels is dus equivalent aan het oplossen van de congruentie  $\Phi_{p-1}(x) \equiv 0 \pmod{p}$ .

### 11.3.3 De stelling van Zsigmondy

**Stelling 11.72.** Stelling van Zsigmondy

Zij  $a, b \in \mathbb{N}^+$  met  $\text{ggd}(a, b) = 1$  en  $n \in \mathbb{N}$ ,  $n > 1$ . Dan bestaat er een priemgetal dat een deler is van  $a^n - b^n$  en niet van  $a^k - b^k$  voor alle  $k \in \{1, 2, \dots, n-1\}$ , behalve in de gevallen

1.  $2^6 - 1^6$ .
2.  $n = 2$  en  $a + b$  is een macht van 2.

Anders gezegd: er bestaat een priemgetal  $p$  dat geen deler is van  $a$  en  $b$  en waarvoor  $a/b$  orde  $n$  heeft modulo  $p$ . Een dergelijk priemgetal noemen we een primitieve priemdeler van  $a^n - b^n$ . Een getal dat het product is van primitieve priemdelers en een deler is van  $a^n - b^n$  noemen we meer algemeen een primitieve deler.

De volgende stelling veralgemeent de stelling van Zsigmondy voor sommen:

**Gevolg 11.73.** Stelling van Zsigmondy voor sommen

Zij  $a, b \in \mathbb{N}^+$  met  $\text{ggd}(a, b) = 1$  en  $n \in \mathbb{N}$ ,  $n > 1$ . Dan bestaat er een priemgetal dat een deler is van  $a^n + b^n$  en niet van  $a^k + b^k$  voor alle  $k \in \{1, 2, \dots, n-1\}$ , behalve in het geval  $2^3 + 1^3$ .

*Bewijs.*

Als oefening. □

#### 11.3.3.1 Bewijs van Zsigmondy

*Gebaseerd op [2, 10]*

**Definitie 11.74.** Radicaal

Het radicaal van een natuurlijk getal  $n \in \mathbb{N}^+$  is het product van alle priemdelers van  $n$ . We noteren  $\text{rad}(n)$ .

Bijvoorbeeld,  $\text{rad}(1000) = 10$  en  $\text{rad}(180) = 30$ .

Het volgende lemma geeft voor nulpunten van cyclotomische veeltermen modulo een priemgetal hun orde modulo dat priemgetal. Het blijkt essentieel in het bewijs voor de stelling van Zsigmondy.

**Lemma 11.75.**

Als  $p$  een priemgetal is,  $n = p^\alpha q > 0$  en  $a$  gehele getallen waarvoor  $p \nmid q$  en  $p \mid \Phi_n(a)$ , dan is  $\text{ord}_p(a) = q$ .

**Opgave 11.76.** Bewijs.

Zij nu  $a, b, n$  zoals in de stelling. We proberen te bewijzen dat er inderdaad een primitieve priemdelers te vinden is.

**Reductie tot cyclotomische veeltermen**

We proberen de stelling te formuleren aan de hand van cyclotomische veeltermen. Bij het controleren of een priemdelers van  $a^n - b^n$  primitief is kunnen we een kleine vereenvoudiging doorvoeren:

**Opgave 11.77.** Om te controleren of  $p \mid a^n - b^n$  primitief is, bewijs dat het volstaat om de waarden van  $k$  te bekijken die delers zijn van  $n$ .

Merk op dat we  $a^n - 1$  op een natuurlijke manier kunnen ontbinden als  $\prod_{d|n} \Phi_d(a)$ . Om algemener  $a^n - b^n$  op zo'n manier te ontbinden hebben we een analogon van cyclotomische veeltermen nodig, met twee variabelen.

Een eenvoudig antwoord wordt gegeven door

$$\Psi_k = b^{\varphi(k)} \Phi_k\left(\frac{a}{b}\right).$$

Merk op dat  $\Psi_k \in \mathbb{Z}$ . Noteer ook  $z_k = a^k - b^k$  voor  $k \in \mathbb{N}$ .

**Opgave 11.78.** Toon aan dat

H

$$\Psi_k = \prod_{d|n} z_k^{\mu(d)} \quad \text{en} \quad z_k = \prod_{d|k} \Psi_d.$$

Als  $z_n = n = p_1^{a_1} \cdots p_r^{a_r}$  waarbij  $p_{s_1}, \dots, p_{s_t}$  de primitieve priemdelers van  $z_n$  zijn, stel dan

$$P_n = p_{s_1}^{a_{s_1}} \cdots p_{s_t}^{a_{s_t}}.$$

We moeten aantonen dat  $P_n > 1$ .

**Opgave 11.79.** Bewijs dat  $P_n \mid \Psi_n$ , d.i.: de primitieve priemdelers van  $z_n$  zijn (met hun hele H multipliciteit) bevat in de factor  $\Psi_n$ .

Stel nu  $\Psi_n = \lambda_n P_n$ . In wat volgt proberen we  $\lambda_n$  naar boven af te schatten en vervolgens  $P_n$  naar onder af te schatten, d.i. bewijzen dat  $P_n > 1$ .

**Een bovengrens voor  $\lambda_n$** **Opgave 11.80.**

- Toon aan dat  $\Psi_n \mid \frac{z_n}{z_d}$  voor elke deler  $d < n$  van  $n$ .
- Bewijs dat  $\text{rad}(\lambda_n) \mid n$ .
- Toon aan dat  $\text{ggd}(\lambda_n, P_n) = 1$ .

Stel dat  $p$  een priemdelers van  $\lambda_n$  is. Stel  $n = p^\alpha q$  met  $p^\alpha \parallel n$ . We noteren nu ook meer algemeen

$$\Psi_n(x, y) = y^{\varphi(n)} \Phi_n\left(\frac{x}{y}\right).$$

D. Bewijs dat uit  $p \mid \lambda_n$  volgt dat  $p \mid \Psi_q$ .

Als  $p \nmid \Psi_q$  voor alle keuzes van  $p$  geldt dus  $\lambda_n = 1$ . Veronderstel nu dat  $p$  een priemdelers van  $\lambda_n$  is waarvoor  $p \mid \Psi_q$ .

E. Bewijs dat  $p$  uniek bepaald is als de grootste priemdelers van  $n$ .

Stel dus  $\lambda_n = p^\beta$ .

F. Bewijs dat  $\beta = 1$ .

### Een ondergrens voor $P_n$

**Opgave 11.81.** Om te besluiten dat  $P_n > 1$  onderscheiden we drie gevallen.

A. Bewijs dat  $P_n > 1$  als  $\lambda_n = 1$ .

B. Toon aan dat  $P_n > 1$  als  $\lambda_n$  priem is en  $a - b > 1$ , tenzij  $n = 2$  en  $a + b$  een macht van 2 is.

Stel nu dat  $\lambda_n = p$  priem is en  $a - b = 1$ . Stel dat toch  $P_n = 1$ .

C. Bewijs dat  $p > 2$ .

Stel  $n = p^\alpha q$  met  $p \nmid q$ .

D. Bewijs dat  $p = \Psi_{pq}(a^{p^{\alpha-1}}, b^{p^{\alpha-1}})$  toch groter is dan  $p$ .

Dus  $\alpha = 1$ .

E. Bewijs dat  $p = \frac{\Psi_q(a^p, b^p)}{\Psi_q}$  gelijk is aan 3.

F. Toon aan dat  $n = 6$ ,  $a = 2$  en  $b = 1$ .

### 11.3.3.2 Gevolgen

**Stelling 11.82.**

## 11.4 Recapitulatie exponentiële congruenties

In dit hoofdstuk is er zo veel aan bod gekomen dat het bos bijna niet meer door de bomen te zien is. Daarom presenteren we een samenvatting in verband met exponentiële congruenties, die je meer inzicht zou moeten geven in wat er allemaal precies aan de hand is.

### 11.4.1 LTE, Fermat, Euler, Bang, Zsigmondy, en Dirichlet

Herinner je de volgende eigenschap (Lemma 8.23): als  $a \equiv b \pmod{p^k}$ , dan is voor alle  $n \geq 0$  ook  $a^{p^n} \equiv b^{p^n} \pmod{p^{k+n}}$ . Dit verhogen van de modulus doet misschien denken aan het Lifting The Exponent Lemma. Inderdaad: LTE zegt meer precies dat  $v_p(a^{p^n} - b^{p^n}) = n + v_p(a - b)$ . Als dus  $v_p(a - b) \geq k$  is wegens LTE zeker  $v_p(a^{p^n} - b^{p^n}) \geq n + k$ . LTE zegt dus nog meer dan die ene eigenschap, het geeft aan hoe groot de modulus precies mag worden opdat de congruentie zou gelden.

Of toch bijna, want als  $p = 2$  moeten we bij LTE eisen dat  $4 \mid a - b$ . M.a.w. als  $p = 2$  laat LTE a priori enkel toe om die ene eigenschap te besluiten wanneer  $4 \mid a - b$ , of dus als  $k \geq 2$ .

Deze eigenschap en LTE zijn voorbeelden van congruenties (of toch een vermoede congruentie wat LTE betreft) waarbij al aan een zekere congruentie moet voldaan zijn om iets zinnigs te kunnen besluiten. Een ander type eigenschappen zijn die waar we uit het niets een congruentie cadeau krijgen, zoals de stelling van Euler (met als bijzonder geval de kleine stelling van Fermat). We bekijken nog even wat Euler zegt voor priem machten: als  $p \nmid a$ , dan is  $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$ . Kiezen we nu  $n \geq 0$ , dan volgt uit die ene eigenschap van daarnet dat  $(a^{(p-1)p^{k-1}})^{p^n} \equiv 1 \pmod{p^{k+n}}$ . Merk op dat dit gewoon de stelling van Euler toegepast is met als modulus  $p^{k+n}$ . Dit is trouwens hoe dat eerste bewijs van de stelling van Euler in mekaar zat: uit de kleine stelling van Fermat ( $a^{p-1} \equiv 1 \pmod{p}$ ) besloten we dat Euler's stelling geldt voor priem machten. (Door de congruentie te herschrijven als een deelbaarheidsrelatie konden we de stelling dan uiteindelijk ook besluiten voor algemene natuurlijke getallen.)

Merk op dat LTE, grof gesproken, bij vaste  $a \in \mathbb{Z}$  aangeeft hoe groot een priem macht  $p^k$  kan zijn om nog aan een zekere congruentie  $a^n \equiv 1 \pmod{p^k}$  te voldoen, wanneer de exponent  $n$  vast ligt. Een andere vraag die we kunnen stellen is hoe klein de exponent  $n$  kan zijn, wanneer nu niet de exponent, maar wel de modulus  $p^k$  vast ligt. Deze kleinste  $n$  (die niet 0 is) is uiteraard gewoon de orde van  $a$  modulo  $p^k$ . Dit leidde dan tot het begrip *primitieve wortels*: modulo  $p^k$  bestaat er een getal met orde  $\varphi(p^k)$ . (Tenzij voor  $p = 2$ , dan geldt het enkel voor  $k \leq 2$ .) De discussie omtrent indexrekenen die hierop volgde maakte duidelijk dat de meeste geheimen omtrent de ordes van getallen modulo  $p^k$  uitgeklaard zijn: voor  $d \mid \varphi(p^k)$  zijn er precies  $\varphi(d)$  elementen van orde  $d$  modulo  $p^k$ . (In het bijzonder zijn er precies  $\varphi(\varphi(p^k))$  primitieve wortels modulo  $p^k$ .)

Over de ordes van getallen modulo priem machten weten we dus al tamelijk wat. Een analoge, maar veel moeilijker te beantwoorden vraag is of er, gegeven natuurlijke getallen  $a$  en  $n$ , een priem macht  $p^k$  bestaat zo dat de orde van  $a$  modulo  $p^k$  gelijk is aan  $n$ . Als  $n$  zelf een priemgetal is, is het antwoord eenvoudig:

**Opgave 11.83.** Zij  $a, n \in \mathbb{N}^+$  en  $n$  priem. Toon aan dat er een priemgetal  $p$  bestaat zo dat  $\text{ord}_p(a) = n$ . H

**Opgave 11.84.** Zij  $n$  een priemgetal. Bewijs dat er oneindig veel priemgetallen  $p \equiv 1 \pmod{n}$  bestaan. H

Voor algemene  $n$  ligt het iets moeilijker. De stelling van Bang (die een speciaal geval is van de stelling van Zsigmondy) zegt dat er altijd een priemgetal  $p$  bestaat met  $\text{ord}_p(a) = n$  (op een aantal randgevallen na). Maar de stelling van Zsigmondy zegt meer dan dit. We betrekken LTE er weer even bij. LTE gaf, gegeven een exponent  $n$ , de grootst mogelijke priem macht als modulus in de congruentie  $a^n - b^n \equiv 0 \pmod{p^k}$ . Als we ons nu omgekeerd afvragen of er voor elke  $a$  en  $b$  bij een gegeven  $n$  er een priemgetal  $p$  bestaat zo dat  $n$  de kleinste exponent is waarvoor  $p \mid a^n - b^n$ , dan geeft de stelling van Zsigmondy hierop een positief antwoord (onder



bepaalde randvoorwaarden). Merk dus op dat voor  $b = 1$  deze vraagstelling overeenkomt met die i.v.m. ordes, waar we het net over hadden.

**Opgave 11.85.** Zij  $n \in \mathbb{N}^+$ . Bewijs dat er oneindig veel priemgetallen  $p \equiv 1 \pmod{n}$  bestaan.

Merk op dat we dit laatste resultaat ook iets rechtstreeks hebben bewezen met behulp van eigenschappen van cyclotomische veeltermen, maar het kan interessant zijn om het in de context van Zsigmondy nog eens te herbekijken.

Nu we het toch over dit soort eigenschappen hebben herhalen we nog eens de eerdervernoemde stelling van Dirichlet (zonder bewijs): als  $\text{ggd}(m, n) = 1$  zijn er oneindig veel priemgetallen  $p \equiv m \pmod{n}$ . Probeer deze niet te bewijzen, het bewijs hiervan vereist (voor zover we weten) nogal wat geavanceerde analytische getaltheorie.

### 11.4.2 Wieferich-priemgetallen

Merk op dat Zsigmondy onder bepaalde voorwaarden priemgetallen geeft waarvoor  $n$  de kleinste exponent is zo dat  $p \mid a^n - b^n$ . Zsigmondy garandeert niet dat  $p^2$  dan geen deler kan zijn van  $a^n - b^n$ . M.a.w., het zou kunnen dat de kleinste  $n$  waarvoor  $p \mid a^n - b^n$  onmiddellijk de kleinste  $n$  is waarvoor  $p^2 \mid a^n - b^n$ . We krijgen er als het ware gratis een extra factor  $p$  bij. Maar kan dit wel voorkomen? Beschouwen we even het bijzonder geval  $a = 2$  en  $b = 1$ , dan leidt dit tot een interessant type priemgetallen:

**Definitie 11.86.** Wieferich-priemgetal<sup>21</sup>

Een *Wieferich-priemgetal* is een priemgetal waarvoor  $p^2 \mid 2^{p-1} - 1$ .

Merk op dat we - in tegenstelling tot wat de discussie hierboven zou suggereren - dit soort priemgetallen niet hebben gedefinieerd als die waarvoor de schijnbaar sterkere voorwaarde  $\text{ord}_p(2) = \text{ord}_{p^2}(2)$  voldaan is.

**Opgave 11.87.** Zij  $p > 2$  een priemgetal met  $\text{ord}_p(2) = \text{ord}_{p^2}(2)$ . Toon aan dat  $p$  een Wieferich-priemgetal is.

‘Schijnbaar sterker’, want in feite zijn deze twee definities toch equivalent:

**Lemma 11.88.**

Toon aan dat een priemgetal  $p$  Wieferich is als en slechts als  $\text{ord}_p(2) = \text{ord}_{p^2}(2)$ .

**Opgave 11.89.** Bewijs zelf eens. H

Bestaan er wel Wieferich-priemgetallen? Tot op heden zijn er precies twee Wieferich-priemgetallen bekend: 1093 en 3511.

We herinneren even aan Lemma 8.12: als  $a, n, m \in \mathbb{Z}$  met  $\text{ggd}(m, n) = 1$ ,  $\text{ord}_m(a) = x$  en  $\text{ord}_n(a) = y$ , dan is  $\text{ord}_{mn}(a) = \text{kgv}(x, y)$ .


### 11.4.3 $n$ -demachtsresten


## Opgaven hoofdstuk 11

**Opgave 11.90.** Zij  $p$  en  $q$  oneven priemgetallen met  $q = 2p + 1$ . Bewijs dat  $-4$  een primitieve wortel is modulo  $q$ . ❁

<sup>21</sup>Naar de Duitse wiskundige Arthur Wieferich (1884-1954)

**Opgave 11.91.** Zij  $p, q \geq 5$  priemgetallen zo dat  $p = 2q + 1$ . Bewijs dat  $-3$  een primitieve wortel is modulo  $p$ .

**Opgave 11.92.** Zij  $p$  een priemgetal. Vind alle natuurlijke getallen  $n$  met de eigenschap dat er geen geheel getal  $x$  bestaat zo dat  $x^n - 1$  deelbaar is door  $p$  maar niet door  $p^2$ . 

**Opgave 11.93.** Noteer met  $\Phi'_n$  de afgeleide van  $\Phi_n$ . Bewijs dat voor  $n > 1$ , 

- A.  $\Phi'_n(0) = -\mu(n)$ ;
- B.  $\Phi'_n(1) = \frac{1}{2}e^{\Lambda(n)}\varphi(n)$ .

**Opgave 11.94.** (IMOSL 2002) Zij  $p_1, p_2, \dots, p_n$  verschillende priemgetallen groter dan 3. Bewijs dat  $2^{p_1 \cdots p_n} + 1$  minstens  $4^n$  positieve delers heeft.

**Opgave 11.95.** Voor welke priemgetallen  $p$  is


- A.  $p^2 \mid a^{p-1} - 1$  voor alle  $a \in \mathbb{Z}$  met  $p \nmid a$ ?
- B.  $p^2 \mid a^{p-1} - 1$  voor alle  $a \in \{1, \dots, p-1\}$ ?


**Opgave 11.96.** Zij  $p$  en  $q$  priemgetallen en  $a \in \mathbb{Z}$  zo dat

$$q \mid 1 + a + \cdots + a^{p-1}.$$

Bewijs dat  $q = p$  of  $q \equiv 1 \pmod{p}$ , en dat  $p \mid 1 + a + \cdots + a^{p-1}$  a.s.a.  $a \equiv 1 \pmod{p}$ .

**Opgave 11.97.** Zij  $F_n$  het  $n$ -de Fibonacci-getal. Bewijs dat voor elk priemgetal  $p > 7$  geldt dat  $F_p \equiv \binom{p}{5} \pmod{p}$ .

**Opgave 11.98.** (WiNA 2014) Zij  $p = 4n + 1$  een priemgetal, bewijs dat  $p \mid n^n - 1$ . 

**Opgave 11.99.** (IMOSL 1991 vraag 18) Vind de hoogste waarde van  $k$  zo dat 

$$1991^k \mid 1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

Over exponentiële congruenties weten we nu toch al tamelijk wat. Een andere klasse van congruenties zijn ‘binomiaalcongruenties’.

### 12.1 De stelling van Lucas

#### Stelling 12.1. Stelling van Lucas

Zij  $m, n \geq 0$  met  $m = (m_k m_{k-1} \dots m_0)_p$  en  $n = (n_k n_{k-1} \dots n_0)_p$  de ontwikkelingen in basis  $p$  (eventueel zijn een aantal van de eerste cijfers 0). Dan is

$$\binom{n}{m} \equiv \prod_{j=0}^k \binom{n_j}{m_j} \pmod{p}.$$

### 12.2 De stelling van Kummer

De stelling van Kummer geeft de hoogste macht van  $p$  die een deler is van  $\binom{n}{m}$ . Herinner je de formule van Legendre:  $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$ .

**Opgave 12.2.** Bewijs dat

$$v_p \binom{n}{m} = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=1}^{\infty} \left\lfloor \frac{m}{p^k} \right\rfloor - \sum_{k=1}^{\infty} \left\lfloor \frac{n-m}{p^k} \right\rfloor$$

voor  $m, n \geq 0$ .

Het resultaat uit de vorige oefening is niet erg nuttig aangezien het berekenen van de sommen in het rechterlid niet erg eenvoudig is. Handiger is de volgende vorm van Legendre's formule:

#### Stelling 12.3. Formule van Legendre, alternatieve vorm

Noem voor  $n \in \mathbb{N}$   $s_p(n)$  de som van de cijfers wanneer  $n$  in basis  $p$  wordt geschreven. Dan is voor alle  $n \in \mathbb{N}$

$$v_p(n!) = \frac{n - s_p(n)}{p - 1}.$$

**Opgave 12.4.** Bewijs zelf eens.

H

Dit geeft een alternatieve formule voor  $v_p \binom{n}{m}$ , namelijk

$$v_p \binom{n}{m} = \frac{s_p(m) + s_p(n-m) - s_p(n)}{p-1}.$$

Kummer ging nog verder en vereenvoudigde de uitdrukking  $\frac{s_p(m) + s_p(n-m) - s_p(n)}{p-1}$ :

**Stelling 12.5.** Stelling van Kummer

Zij  $m, n \geq 0$  met  $m = (m_k m_{k-1} \dots m_0)_p$  en  $n = (n_k n_{k-1} \dots n_0)_p$  de ontwikkelingen in basis  $p$  (eventueel zijn een aantal van de eerste cijfers 0). Dan is  $v_p \binom{n}{m}$  gelijk aan het aantal indices  $j \leq k$  waarvoor  $n_j < m_j$ .

**Opgave 12.6.** (Stelling van Kummer) Stel  $r = n - m = (r_k \dots r_0)_p$ . Stel  $c_j = 0$  als  $n_j \geq m_j$  en 1 als  $n_j < m_j$ . Stel ook  $c_{-1} = 0$ .

- Bewijs dat  $n_j = m_j + r_j + c_{j-1} - pc_j$  voor  $0 \leq j \leq k$ .
- Bewijs dat  $s_p(m) + s_p(n - m) + s_p(m) = (p - 1)(c_0 + \dots + c_k) + c_k$
- Besluit Kummer's stelling.

**12.3 De stelling van Wolstenholme****Stelling 12.7.** Stelling van Wolstenholme

Zij  $p > 3$  een priemgetal. Dan is


$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

**Definitie 12.8.** Wolstenholme-priemgetal

Een *Wolstenholme-priemgetal* is een priemgetal  $p > 7$  waarvoor

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}.$$

**Opgaven hoofdstuk 12**

**Opgave 12.9.** Zij  $p$  een priemgetal. Bewijs dat  $\binom{2p}{p} \equiv 2 \pmod{p}$ . 

**Opgave 12.10.** Zijn  $n$  en  $q$  natuurlijke getallen met  $n \geq 5$  en  $2 \leq q \leq n$ . Bewijs dat  $q - 1$  een H deler is van  $\left\lfloor \frac{(n-1)!}{q} \right\rfloor$ .

In dit hoofdstuk bespreken we de oplossingen van kwadratische Diophantische vergelijkingen. In het bijzonder de zogenaamde Pell-vergelijkingen en de mogelijkheid om een natuurlijk getal te schrijven als de som van kwadraten.

### 13.1 Completing the square

**Voorbeeld 13.1.** Bepaal de gehele oplossingen van  $x^2 - 2xy + 2y^2 + x - y = 1$ .

*Oplossing.*

We herkennen  $x^2 - 2xy + y^2 = (x - y)^2$ . Daartoe schrijven we  $(x - y)^2 + y^2 + x - y = 1$ . We proberen nu  $(x - y)^2 + x - y$  te doen lijken op een kwadraat. Algemeen is  $a^2 + a = \frac{1}{4}(4a^2 + 4a + 1 - 1) = \frac{1}{4}((2a + 1)^2 - 1)$ . Daarom vermenigvuldigen we alles met 4:  $4(x - y)^2 + 4y^2 + 4(x - y) = 4$ , of dus  $(2x - 2y + 1)^2 + 4y^2 = 5$ .

Er zijn niet erg veel manieren om 5 te schrijven als som van twee kwadraten, enkel  $(\pm 1)^2 + (\pm 2)^2 = 5$ . Er moet dus gelden dat  $2y = \pm 2$  enerzijds en  $2x - 2y + 1 = \pm 1$  anderzijds. Dit geeft als oplossingen  $(1, 1)$ ,  $(0, 1)$ ,  $(-1, -1)$ ,  $(-2, -1)$ .

Bij het zien van  $a^2 + a$  is het een goede reflex om te denken aan  $(2a + 1)^2$ . Analoog moet  $a^2 - a$  je doen denken aan  $(2a - 1)^2$ . Meer algemeen kunnen we  $a^2 + ab$  handig herschrijven door te vermenigvuldigen met 4:  $4a^2 + 4ab = (2a + b)^2 - b^2$ .

Dit herschrijven is wat men *completing the square* noemt, vrij vertaald, *vervolledigen van het kwadraat*.

**Voorbeeld 13.2.** Bepaal de gehele oplossingen van  $3x^2 + 2xy + 2y^2 - 5x + y =$ .

*Oplossing.*

We proberen de term  $2xy$  weg te werken door die te verwerken in een kwadraat. Een mogelijkheid is om  $x^2 + 2xy + y^2 = (x + y)^2$  te gebruiken. Het nadeel is dat we dan met drie kwadratische termen ( $2x^2$ ,  $(x + y)^2$  en  $y^2$ ) opgescheept zitten. Interessanter is om alles met 3 te vermenigvuldigen:  $9x^2 + 6xy + \dots = \dots$ . Dit lijkt op  $(3x + y)^2$ , immers,  $9x^2 + 6xy + y^2 = (3x + y)^2$ . Concreet wordt de vergelijking dus  $(3x + y)^2 + 5y^2 - 15x + 3y =$ .

Nu werken we de  $-15x$  weg. Om iets van de vorm  $a^2 + ba$  te verkrijgen vullen we  $-15x$  aan met  $-5y$ , we bekommen  $-5(3x + y)$ . Dus:

$$(3x + y)^2 + y^2 - 15x + 3y = (3x + y)^2 - 5(3x + y) + y^2 + 8y.$$

Completing the square levert na vermenigvuldigen met 4,

$$(6x + 2y - 5)^2 + 4y^2 + 12y =$$

## 13.2 Classificatie

### Definitie 13.3. Kwadratische Diophantische vergelijking

Een kwadratische Diophantische vergelijking in twee variabelen is een vergelijking van de vorm  $ax^2 + bxy + cy^2 + dx + ey + f = 0$ , waarbij  $a, b, c, d, e, f \in \mathbb{Z}$  parameters zijn en we oplossingen in  $\mathbb{Z}$  zoeken voor  $x$  en  $y$ .

We zullen proberen een algemene methode te vinden om een dergelijke vergelijking op te lossen. Deze paragraaf kan best saai lijken, ze is dan ook slechts bedoeld om formeel te bespreken hoe je in de verschillende gevallen te werk kan gaan om oplossingen te vinden, en dient als motivatie voor de zogenaamde Pell-vergelijkingen.

Hoe meer parameters 0 zijn, hoe eenvoudiger de vergelijking wordt.

#### Het geval $a = c = 0$

Als bovendien  $b = 0$  is dit gewoon een lineaire vergelijking. Die kunnen we in principe algemeen bespreken en oplossen. Veronderstel  $b \neq 0$ . Dan is de vergelijking gelijkwaardig met

$$\begin{aligned} b^2xy + bdx + bde + bf &= 0 \\ \Leftrightarrow (bx + e)(by + d) &= de - bf. \end{aligned}$$

Het probleem is dan gereduceerd tot het achterhalen van de delers van  $de - bf$ , dus in dit geval kunnen we de vergelijking in principe ook oplossen.

#### Het geval $a \neq 0$

Veronderstel nu dat  $a$  en  $c$  niet beide 0 zijn, stel bijvoorbeeld dat  $a \neq 0$ . We proberen de vergelijking te schrijven als som van kwadraten.

$$\begin{aligned} 4a^2x^2 + 4abxy + 4acy^2 + 4adx + 4aey + 4af &= 0 \\ \Leftrightarrow (2ax + by + d)^2 + (4ac - b^2)y^2 + (4ae - 2bd)y + 4af - d^2 &= 0. \end{aligned}$$

We hebben alle termen met  $x$  binnen een kwadraat gebracht. De vergelijking heeft nu de vorm  $(2ax + by + d)^2 = Dy^2 + Ay + B$ . We proberen nu met de overige termen een kwadraat te vormen, of iets wat er op lijkt.  $D = b^2 - 4ac$  noemen we de *discriminant* van de kwadratische vergelijking.

### 13.2.1 Discriminant 0: reductie tot kwadratische congruenties

Veronderstel eerst dat  $D = 0$ . Als bovendien  $A = 0$  is de vergelijking heel eenvoudig: naar gelang  $B$  een kwadraat is of niet krijgen we geen oplossingen, of 1 of 2 lineaire vergelijkingen  $2ax + by + d = \pm \sqrt{B}$ . Dit geval geldt als besproken. Als  $A \neq 0$  stellen we  $z = 2ax + by + d$ , zodat  $Ay = z^2 - B$ . We zullen proberen de oplossingen te parametriseren aan de hand van  $z$ .

We hebben het stelsel

$$\begin{aligned} & \begin{cases} 2ax + by + d = z \\ Ay = z^2 - B \end{cases} \\ \Leftrightarrow & \begin{cases} 2aAx + bAy + Ad = Az \\ Ay = z^2 - B \end{cases} \\ \Leftrightarrow & \begin{cases} 2aAx = -bz^2 + Az + bB - Ad \\ Ay = z^2 - B. \end{cases} \end{aligned}$$

Het probleem reduceert zich dan tot het vinden van alle  $z \in \mathbb{Z}$  waarvoor

$$\begin{cases} -bz^2 + Az + bB - Ad \equiv 0 \pmod{2aA} \\ z^2 - B \equiv 0 \pmod{A}. \end{cases}$$

Dit stelsel congruenties kan in principe steeds opgelost worden met behulp van de theorie over kwadratische congruenties en de Chinese reststelling. (Merk hierbij op dat de tweede congruentie automatisch uit de eerste zal volgen indien  $\text{ggd}(A, b) = 1$ , of dus  $\text{ggd}(4ae, b) = 1$ .) In het bijzonder zijn er steeds geen of oneindig veel oplossingen. Dit is echter niet het interessante geval waar we naartoe willen.

### 13.2.2 Sommen van kwadraten en Pell-typevergelijkingen

Veronderstel  $D \neq 0$ . We proberen het rechterlid in de vorm van een kwadraat te brengen. We stellen opnieuw  $z = 2ax + by + d$ . De vergelijking wordt  $Dz^2 = D^2y^2 + ADy + DB$ . Merk op dat  $A = 2bd - 4ae$  steeds even is, we moesten dus niet vermenigvuldigen met  $4D$  zoals voorheen, om het rechterlid te herschrijven. Stel  $A = 2C$ , zodat  $Dz^2 = (Dy + C)^2 + DB - C^2$ . Of nog,

$$(Dy + C)^2 - Dz^2 = C^2 - DB.$$

Zodra we deze vergelijking algemeen hebben opgelost zal het niet meer zo moeilijk zijn om daar de koppels  $(y, z)$  uit te halen die aanleiding geven tot een gehele  $x$ . Essentieel hebben we het laatste geval dus herleid tot de gedaante

$$u^2 - Dz^2 = F,$$

met  $D = b^2 - 4ac$ . Indien  $D = k^2$  een kwadraat is valt de vergelijking te ontbinden als  $(u - kz)(u + kz) = F$ . Voor elke deler van  $F$  geeft dit een stelsel van twee vergelijkingen in  $x$  en  $y$ . Niet echt een boeiend geval dus. Als  $D < 0$  krijgen we  $u^2 + |D|z^2 = F$ . Zo'n vergelijking heeft steeds een eindig aantal oplossingen in  $u$  en  $z$ . In het bijzonder hebben we de vergelijking

$$u^2 + z^2 = F.$$

De vraag is dan welke getallen  $F$  de som zijn van twee kwadraten.

Elk koppel  $(u, z)$  geeft dan op zijn beurt een  $2 \times 2$ -stelsel in  $x$  en  $y$ , waaruit de oplossingen moeten volgen.

Ook interessant is wanneer  $D > 0$  geen kwadraat is.

**Definitie 13.4.** Pell-vergelijking

Een *Pell-vergelijking* is een vergelijking van de vorm  $x^2 - dy^2 = 1$ , waarbij  $d \in \mathbb{N}$  een parameter is die geen volkomen kwadraat is, en men oplossingen zoekt voor  $x$  en  $y$ .

Meer algemeen definiëren we:

**Definitie 13.5.** Pell-typevergelijking

Een *Pell-typevergelijking* is een vergelijking van de vorm  $x^2 - dy^2 = a$  met  $a$  en  $d$  constanten,  $a \neq 0$  en  $d \in \mathbb{N}$  geen kwadraat.

**13.2.3 Conclusies en praktische strategie**

Merk dus op dat we het gedrag van de vergelijking al vanaf het begin kunnen voorspellen, naargelang het teken van  $D = b^2 - 4ac$ .<sup>22</sup> Als  $D < 0$  krijgen we iets met een som van kwadraten (of toch in het bijzondere geval  $D = -1$ ). Als  $D = 0$  krijgen we een stelsel kwadratische congruenties, en als  $D > 0$  een Pell-(type)vergelijking.

In sommige gevallen zal je al meteen kunnen besluiten dat er geen oplossingen zijn door de vergelijking modulo een goed gekozen getal te beschouwen. Een goede keuze is dan  $D$  of een deler daarvan: uit de equivalente vormen zien we dat het aantal te onderscheiden gevallen dan sterk wordt gereduceerd, en de vraag is dan of  $F$  een kwadraatrest is. Modulo een priemgetal  $p > 2$  heeft  $F$  een kans van  $\frac{p+1}{2p} \approx \frac{1}{2}$  om een kwadraatrest te zijn. De moeite waard dus om te proberen.

Indien  $D = 0$  loont het de moeite om de vergelijking al meteen modulo  $A = 2bd - 4ae$  te bekijken. We hadden in dat geval immers een stelsel congruenties, onder andere modulo  $A$ . Met een beetje geluk heeft dat stelsel geen oplossingen.

**13.3 Sommen van kwadraten**

*Gebaseerd op [1]*

Van een natuurlijk getal  $n$  zeggen we dat het de som is van twee kwadraten als de vergelijking  $a^2 + b^2 = n$ , een gehele oplossing in  $a$  en  $b$  heeft. Analoog hebben we sommen van drie kwadraten, enzovoort. Merk op dat ook 0 de som is van twee kwadraten.

**13.3.1 Som van twee kwadraten: multiplicativiteit**

<sup>22</sup>In een algebraïsche context wordt  $ax^2 + bxy + cy^2 + dx + ey + f$  een (niet-homogene) *binair kwadratische vorm* genoemd.



**Stelling 13.6.** Brahmagupta-Fibonacci

Als een natuurlijk getal het product is van twee sommen van twee kwadraten, dan is dat getal ook te schrijven als de som van twee kwadraten.

*Bewijs.*

Dit volgt vrijwel onmiddellijk uit de identiteit van Brahmagupta-Fibonacci

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Inderdaad, na de haakjes uit te werken zien we dat beide leden gelijk zijn. □

Merk op dat we evengoed kunnen schrijven

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ab + bc)^2.$$

Deze stelling is meteen uitbreidbaar naar meerdere getallen.

**Gevolg 13.7.**

Als  $n_1, n_2, \dots, n_m$  natuurlijke getallen zijn die kunnen worden geschreven als de som van twee kwadraten, dan kan ook hun product  $n_1 n_2 \cdots n_m$  worden geschreven als de som van twee kwadraten.

Het volstaat om inductie toe te passen op het aantal factoren.

**Lemma 13.8.**

Stel dat  $\in \mathbb{N}$  zo dat  $2n$  de som is van twee kwadraten. Dan is ook  $n$  de som van twee kwadraten.

**Opgave 13.9.** Bewijs.

**Lemma 13.10.**

Als een natuurlijk getal  $n$  op twee manieren te schrijven is als de som van twee kwadraten als  $n = a^2 + b^2 = c^2 + d^2$  met  $|a| \neq |c| \neq |b|$ , dan is  $n$  ook het product van twee sommen van twee kwadraten die beide groter dan 1 zijn.

De voorwaarde  $|a| \neq |c| \neq |b|$  drukt uit dat die twee manieren niet uit elkaar volgen door omwisseling van  $a$  en  $b$  of tekens te wijzigen.

**Opgave 13.11.** Bewijs.

Zij  $n$  zoals in de opgave en veronderstel  $a, b, c, d \geq 0$ . Stel  $x = \frac{a+c}{2}$  en  $y = \frac{b+d}{2}$ .

A. Toon aan dat  $x$  en  $y$  natuurlijke getallen zijn, eventueel na omwisselen van  $c$  en  $d$ .

B. Toon aan dat  $\frac{x}{y} = \frac{y-b}{x-c}$ .

Stel nu  $\text{ggd}(x, y) = r$ ,  $x = pr$ ,  $y = qr$  en  $\text{ggd}(x - c, y - b) = s$ .

- C. Toon aan dat  $x - c = qs$  en  $y - b = ps$ .
- D. Toon aan dat  $a = pr + qs$  en  $b = qr - ps$ .
- E. Schrijf  $n$  als het product van twee sommen van twee kwadraten, beide groter dan 1.

De methode uit het bewijs staat bekend als de *factorisatiemethode van Euler*.

**Opgave 13.12.** Zij  $p$  een priemgetal. Bewijs dat de vergelijking  $x^2 + y^2 = p$  steeds precies 0 of 4 gehele oplossingen  $(x, y)$  heeft.

### 13.3.2 De twee-kwadratenstelling

#### Stelling 13.13. Kerststelling van Fermat

Een oneven priemgetal  $p$  kan worden geschreven als de som van twee kwadraten als en slechts als  $p \equiv 1 \pmod{4}$ .

**Opgave 13.14.** (Kerststelling van Fermat) Zij  $p$  een priemgetal.

- A. Toon aan dat een priemgetal  $p \equiv 3 \pmod{4}$  niet kan worden geschreven als de som van twee kwadraten.

Stel nu  $p \equiv 1 \pmod{4}$ .

- B. Toon aan dat er een getal  $v$  met  $0 \leq v < p$  bestaat zo dat  $p \mid v^2 + 1$ .

Bijgevolg is  $v^2 + 1 = kp$ .

- C. Toon aan dat  $0 < k < p$ .

Vervolgens zullen we bewijzen dat als  $xp$  de som van twee kwadraten is en  $0 < x < p$ , er dan een natuurlijk getal  $y$  bestaat met  $0 < y < x$  zo dat ook  $yp$  de som van twee kwadraten is. Dan kunnen we, beginnend met  $k$ , steeds kleinere getallen  $x$  vinden waarvoor  $xp$  de som van twee kwadraten is, totdat  $x = 1$ .

Veronderstel nu dus dat  $a^2 + b^2 = xp$ . Noem  $c$  en  $d$  de kleinste absolute resten van respectievelijk  $a$  en  $b$  bij deling door  $x$ .

- D. Toon aan dat  $c^2 + d^2 = yx$  en dat  $0 < y < x$ .
- E. Schrijf  $x^2yp$  als de som van twee kwadraten  $m^2 + n^2$ .
- F. Toon aan dat  $m$  en  $n$  beide deelbaar zijn door  $x$ .

Bijgevolg is  $\left(\frac{m}{x}\right)^2 + \left(\frac{n}{x}\right)^2 = yp$ , en hebben we een oplossing voor een kleinere waarde  $y$ .

In deze context wordt de techniek uit dit bewijs *finite descent* of *descente finie* (eindige afdaling) genoemd, in contrast met oneindige afdaling. We zullen die methode nog tegenkomen.

**Stelling 13.15.** Twee-kwadratenstelling

Een natuurlijk getal  $n$  groter dan 0 kan worden geschreven als de som van twee kwadraten als en slechts als alle priemdelers van de vorm  $4k + 3$  in de priemontbinding van  $n$  tot een even macht voorkomen.

Bijvoorbeeld, 15 is niet de som van twee kwadraten want 3 komt tot een oneven macht voor. En inderdaad, er zijn maar enkele gevallen te proberen, en  $15 - 0^2$ ,  $15 - 1^2$ ,  $15 - 2^2$ ,  $15 - 3^2$  leveren nooit een kwadraat op. In 45 komt die factor 3 wel met een even exponent voor, en inderdaad:  $45 = 3^2 + 6^2$ .

**Opgave 13.16.** (Twee-kwadratenstelling) Stel eerst dat  $n = x^2 + y^2$  en  $p = 4k + 3$  is een priemdeeler van  $n$ .

A. Toon aan dat  $p$  tot een even macht voorkomt in de priemontbinding van  $n$ .

Hiermee is het eerste deel bewezen. Nu bewijzen we omgekeerd dat elk getal  $n$  dat hieraan voldoet kan geschreven worden als de som van twee kwadraten.

B. Bewijs dat  $2^a$ ,  $p^b$  en  $q^{2c}$  elk de som zijn van twee kwadraten als  $p \equiv 1 \pmod{4}$  en  $q \equiv 3 \pmod{4}$ .

C. Bewijs dat  $n$  de som is van twee kwadraten.

**Opgave 13.17.** Gebruik de identiteit van Brahmagupta-Fibonacci om  $p^2$  en  $p^3$  op twee essentieel verschillende manieren te schrijven als de som van twee kwadraten, met  $p = a^2 + b^2$  een priemgetal.

**Opgave 13.18.** Vind alle priemgetallen  $p$  waarvoor er natuurlijke getallen  $a, b, n$  bestaan zo dat  $a^2 + b^2 = p^3$  en  $a - b = n^3$ .

**Opgave 13.19.** (IrMO 2005 dag 1 vraag 1) Bewijs dat  $2005^{2005}$  de som van twee volkomen kwadraten is, maar niet de som van twee volkomen derdemachten.

**Opgave 13.20.** Zij  $q = 4k + 3$  een priemgetal. Toon aan dat de vergelijking  $x^2 + y^2 = q^{2n}$  voor elke  $n \in \mathbb{N}$  precies vier oplossingen  $(x, y)$  heeft.

**Stelling 13.21.**

Zij  $n$  een natuurlijk getal is waarvan  $p_1, p_2, \dots, p_r$  de priemdelers van de vorm  $4k + 1$  zijn met bijbehorende exponenten  $a_1, a_2, \dots, a_r$ . Als  $n$  de som is van twee kwadraten, dan is het aantal oplossingen van de vergelijking  $x^2 + y^2 = n$  precies

$$r_2(n) = 4 \cdot \prod_{i=1}^r (a_i + 1).$$

Het bewijs steunt op eigenschappen van Gaussiaanse gehele getallen en wordt hier niet vermeld.

### 13.3.3 Drie en vier kwadraten

De vraag stelt zich welke natuurlijke getallen de som zijn van 3, 4 of meer kwadraten. Voor 4 kwadraten is het antwoord eenvoudig:

**Stelling 13.22.** Vier-kwadratenstelling van Langrange<sup>23</sup>

Elk natuurlijk getal is de som van vier kwadraten.

De reden waarom het geval van vier kwadraten veel eenvoudiger is als dat van drie, is de identiteit

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) &= (aA + bB + cC + dD)^2 \\ &+ (aB - bA + cD - dC)^2 \\ &+ (aC - bD - cA + dB)^2 \\ &+ (aD - dA + bC - cB)^2,\end{aligned}$$

ook wel bekend als de vier-kwadratenidentiteit van Euler. De identiteit impliceert dat het product van twee sommen van vier kwadraten terug een som van vier kwadraten is. Voor sommen van drie kwadraten bestaat geen dergelijke identiteit. Inderdaad: bijvoorbeeld 3 en 5 zijn de som van drie kwadraten, maar  $3 \cdot 5 = 15$  is dat niet. We zullen later zien welke getallen dat wel zijn.

Analoog als in het geval van twee kwadraten hebben we:

**Lemma 13.23.**

Zij  $n \in \mathbb{N}$  zo dat  $2n$  de som van vier kwadraten is. Dan is ook  $n$  de som van vier kwadraten.

**Opgave 13.24.** Bewijs.

**Opgave 13.25.** (Vier-kwadratenstelling) Wegens Euler's identiteit volstaat het om aan te tonen dat het geldt voor priemgetallen.

A. Bewijs dat 2, en de priemgetallen van de vorm  $4k + 1$  de som zijn van vier kwadraten.

Stel  $p \equiv 3 \pmod{4}$  is een priemgetal. Het bewijs gaat via eindige afdaling zoals in het bewijs van de Kerststelling.

B. Toon aan dat er getallen  $v$  en  $w$  met  $\lfloor \frac{-p}{2} \rfloor < v, w \leq \lfloor \frac{p}{2} \rfloor$  bestaan zo dat  $p \mid v^2 + w^2 + 1$ .

Bijgevolg is  $v^2 + w^2 + 1 = kp$ .

C. Toon aan dat  $0 < k < p$ .

Stel nu dat  $0 < x < p$  en dat  $xp$  de som van vier kwadraten is. We zoeken een  $y$  met  $0 < y < x$  waarvoor ook  $yp$  dat is.

Noem opnieuw  $e, f, g, h$  de kleinste absolute resten van respectievelijk  $a, b, c, d$  bij deling door  $x$ . Stel eerst dat  $x$  oneven is.

<sup>23</sup>Ook bekend als het vermoeden van Bachet, voor het eerst bewezen door Lagrange in 1770.

- D. Toon aan dat  $e^2 + f^2 + g^2 + h^2 = yx$  en dat  $0 < y < x$ .
- E. Schrijf  $x^2yp$  als de som van vier kwadraten  $k^2 + l^2 + m^2 + n^2$  en toon aan  $k, l, m, n$  deelbaar zijn door  $x$ .

Bijgevolg is ook  $yp$  de som van vier kwadraten. Stel nu dat  $x$  even is. We kunnen nu niet met zekerheid zeggen dat  $0 < y < x$  in  $e^2 + f^2 + g^2 + h^2 = yx$ , immers, het ongelukkige geval  $e = f = g = h = \frac{x}{2}$  kan zich voordoen. Uit het vorige lemma weten we gelukkig dat ook  $\frac{xp}{2}$  de som van vier volkomen kwadraten is, en dus kunnen we  $y = \frac{x}{2} < x$  nemen.

**Stelling 13.26.**

Een natuurlijk getal is de som van drie kwadraten als en slechts als het niet van de vorm  $4^k \cdot (8m + 7)$  is.

Deze stelling vindt zijn oorsprong bij Legendre. Zijn bewijs was echter onvolledig en werd later voltooid door Gauss. De ene richting van de stelling is goed doenbaar, de andere richting bewijzen we hier niet.

**Opgave 13.27.** Toon aan dat een getal  $n$  van de vorm  $4^k \cdot (8m + 7)$  niet kan worden geschreven als de som van drie kwadraten.

- A. Toon aan dat het waar is voor oneven getallen  $n$ .
- B. Bewijs dat het ook waar is voor even getallen  $n$ .

### 13.3.4 Veralgemeningen

*I remember once going to see him when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways."*


(Hardy over Ramanujan)

#### 13.3.4.1 Het probleem van Waring

#### 13.3.4.2 De veelhoeksgetalstelling van Fermat

### 13.4 De kwadratische vorm $a^2 + nb^2$

#### 13.4.1 Eindige afdaling

**Opgave 13.28.** Zij  $p$  een priemgetal en  $\left(\frac{-3}{p}\right) = 1$ . Bewijs dat  $p$  van de vorm  $a^2 + 3b^2$  is. 

Interessant om te vermelden in deze context is het volgende resultaat:

**Stelling 13.29.** Stelling van Kaplansky

Zij  $p$  een priemgetal.

1. Is  $p \equiv 1 \pmod{16}$ , dan is  $p$  van de vorm  $x^2 + 32y^2$  als en slechts als  $p$  van de vorm  $x^2 + 64y^2$  is.
2. Is  $p \equiv 9 \pmod{16}$ , dan is  $p$  van precies één van bovenstaande gedaantes.

### 13.4.2 Uniciteit

**Opgave 13.30.** Zij  $p = a^2 + 2b^2$  een priemgetal. Toon aan dat  $a$  en  $b$  uniek zijn op hun teken na. ❀

## 13.5 Pell-vergelijkingen

Gebaseerd op [3, 4, 9]

Stel  $d > 0$  is geen kwadraat. We kunnen de vergelijking  $x^2 - dy^2 = a$  ontbinden als  $(x + y\sqrt{d})(x - y\sqrt{d}) = a$ . Om hiervan de zinvolheid te verduidelijken voeren we enkele nieuwe begrippen in.

### 13.5.1 De norm in $\mathbb{Z}[\sqrt{d}]$

**Notatie 13.31.**

De verzameling  $\mathbb{Z}[\sqrt{d}]$  is de verzameling van alle reële getallen van de vorm  $x + y\sqrt{d}$  met  $x, y \in \mathbb{Z}$ .

**Stelling 13.32.**

De som en het product van elementen uit  $\mathbb{Z}[\sqrt{d}]$  zitten terug in die verzameling.<sup>24</sup>

*Bewijs.*

Het bewijs is niet meer dan een rechtstreekse controle:

$$(x_1 + y_1\sqrt{d}) + (x_2 + y_2\sqrt{d}) = (x_1 + x_2) + (y_1 + y_2)\sqrt{d}$$

en

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}.$$

□

De volgende stelling is een gevolg van het feit dat  $d$  geen kwadraat is.

---

<sup>24</sup>Men noemt  $\mathbb{Z}[\sqrt{d}]$  *gesloten* onder optelling en vermenigvuldiging.

**Stelling 13.33.**

Voor elk getal  $z \in \mathbb{Z}[\sqrt{d}]$  bestaan er unieke  $x, y \in \mathbb{Z}$  waarvoor  $z = x + y\sqrt{d}$ .

*Bewijs.*

Als oefening. □

Dankzij deze unieke notatie zijn de volgende functies goed gedefinieerd.

**Definitie 13.34. Toevoeging**

Het *toegevoegde* van van  $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$  definiëren we als  $x - y\sqrt{d}$ . We noteren  $\bar{z} = x - y\sqrt{d}$ .

Men gaat eenvoudig na dat toevoeging multiplicatief is: voor alle  $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$  geldt dat  $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$ . In de uitwerking van het product hierboven zien we immers dat wanneer  $y_1$  en  $y_2$  van teken veranderen, de eerste term in het rechterlid gelijk blijft en de tweede van teken verandert.

**Definitie 13.35. Norm**

De *norm* van  $z \in \mathbb{Z}[\sqrt{d}]$  definiëren we als  $N(z) = z \cdot \bar{z}$ .

Er volgt dat  $N(x + y\sqrt{d}) = x^2 - dy^2$ . Merk op dat de norm negatief kan zijn. Uit de multiplicativiteit van de toevoeging volgt dat ook de norm multiplicatief is:  $N(z_1 z_2) = N(z_1)N(z_2)$ . De vergelijking  $x^2 - dy^2 = a$  is dus equivalent met de vergelijking  $N(z) = a$  over  $\mathbb{Z}[\sqrt{d}]$ .

**Opgave 13.36.** Stel  $z = 14 + 6\sqrt{5}$ , zodat  $z \in \mathbb{Z}[\sqrt{5}], \mathbb{Z}[\sqrt{20}], \mathbb{Z}[\sqrt{45}], \mathbb{Z}[\sqrt{180}]$ .

- A. Wat is  $N(z)$  in elk van die verzamelingen?
- B. Verklaar waarom we kortweg  $N(z)$  noteren, zonder  $d$  te vermelden in de notatie zoals bijvoorbeeld d.m.v.  $N_d(z)$ .

**Opgave 13.37.** Stel dat  $z \in \mathbb{Z}[\sqrt{d}]$  met  $N(z) = 1$ . Bewijs dat ook  $z^{-1} \in \mathbb{Z}[\sqrt{d}]$  en dat  $N(z^{-1}) = 1$ .

**13.5.2 Bestaan van oplossingen**

Het bestaan van oplossingen in het algemeen hebben we te danken aan Lagrange:

**Stelling 13.38.**

Elke Pell-vergelijking  $x^2 - dy^2 = 1$  heeft een oplossing.

**Opgave 13.39.** Bewijs.

Uit het gevolg van Dirichlet's benaderingsstelling vinden we oneindig veel koppels  $(p, q)$  met  $\left| \sqrt{d} - \frac{p}{q} \right| < \frac{1}{q^2}$ .

- A. Bewijs dat voor zulke koppels geldt dat  $|p^2 - dq^2| < 2\sqrt{d} + 1$ .
- B. Bewijs dat er verschillende  $z_1 = p_1 + q_1\sqrt{d}$  en  $z_2 = p_2 + q_2\sqrt{d}$  bestaan met dezelfde norm  $n$ , zodanig dat  $p_1 \equiv p_2 \pmod{n}$  en  $q_1 \equiv q_2 \pmod{n}$ .

Veronderstel zonder verlies van algemeenheid dat  $z_1 < z_2$ .

- C. Bewijs dat  $z = \frac{z_1}{z_2} \in \mathbb{Z}[\sqrt{d}]$ , en dat  $N(z) = 1$ .

**13.5.3 Karakterisatie via minimale oplossingen**

De Pell-vergelijking  $N(z) = 1$  heeft als triviale oplossing  $z = \pm 1$ . Als we echter de kleinste niet-triviale oplossing groter dan 1 kennen laat de volgende stelling toe om alle oplossingen te kennen.

**Stelling 13.40.**

Als  $z_0$  het kleinste element uit  $\mathbb{Z}[\sqrt{d}]$  is met  $z_0 > 1$  en  $N(z_0) = 1$ , dan worden alle oplossingen van  $N(z) = 1$  gegeven door  $z = \pm z_0^n$  met  $n \in \mathbb{Z}$ .

*Bewijs.*

Zij  $z > 0$  een oplossing van  $N(z) = 1$  en  $z_0 > 1$  de kleinste oplossing, het geval  $z < 0$  gaat analog. Dan bestaat er een unieke  $k \in \mathbb{Z}$  waarvoor  $z_0^k \leq z < z_0^{k+1}$ . Bekijk nu het getal  $z_1 = zz_0^{-k}$ . Dat zit ook in  $\mathbb{Z}[\sqrt{d}]$ . Er geldt dat  $1 \leq z_1 < z_0$  en  $N(z_1) = N(z)N(z_0)^{-k} = 1$ . Omdat  $z_0$  het kleinste element groter dan 1 was waarvoor  $N(z_0) = 1$ , moet dus  $z_1 = 1$ . Dus  $z = z_0^k$ . Uit de multiplicativiteit van de norm volgt dat al deze getallen inderdaad voldoen.  $\square$

Voor een element  $z$  met norm 1 is  $z^{-1} = \bar{z}$ . We kunnen de oplossingen dus evengoed schrijven als  $z = \pm z_0^n$  of  $z = \pm \bar{z}_0^n$ , met  $n \in \mathbb{N}$ .

Deze stelling geeft ons alle oplossingen op voorwaarde dat we de kleinste oplossing kennen. Het is echter nog niet zeker of er ook steeds een oplossing is, en of er een kleinste oplossing bestaat. Het zou misschien kunnen dat er een oneindige rij  $z_1, z_2, \dots > 1$  bestaat die strikt dalend is en waarvoor  $N(z_k) = 1$  voor alle  $k$ . In dat geval hebben we niet zeker een kleinste oplossing.

We kennen ook nog geen praktische methode om een kleinste oplossing te vinden. We proberen daarom het 'klein' zijn van  $x + y\sqrt{d}$  te herleiden tot het 'klein' zijn van  $x$  en  $y$ . We noemen een element  $z$  kortweg minimaal als het het kleinste element groter dan 1 is met norm 1.



**Stelling 13.41.**

Zij  $x, y \in \mathbb{Z}$ . Als  $x + y\sqrt{d}$  minimaal is, dan zijn  $x, y \in \mathbb{N}^+$ .

*Bewijs.*

Uit  $(x + y\sqrt{d})(x - y\sqrt{d}) = 1$  volgt dat  $x - y\sqrt{d} < 1$ . Dus  $x - y\sqrt{d} < x + y\sqrt{d}$ , zodat  $y > 0$ . Omdat  $x + y\sqrt{d} > 0$  is ook  $x - y\sqrt{d} > 0$ . Dit kan alleen als  $x > 0$ .  $\square$

De minimale oplossing moet dus enkel worden gezocht onder de elementen met positieve ‘coëfficiënten’.

**Gevolg 13.42.**

Als  $x_0, y_0$  de minimale oplossing is voor  $x^2 - dy^2 = 1$ , dan worden alle gehele oplossingen gegeven door  $x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$ ,  $n \in \mathbb{Z}$ .

Merk op dat de gelijkheid  $x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$  de waarden van  $x$  en  $y$  uniek bepaalt, aangezien de schrijfwijze in de vorm  $a + b\sqrt{d}$  uniek is. Om  $x$  en  $y$  precies te kennen leiden we uit  $z = x + y\sqrt{d}$  af dat  $x = \frac{z+\bar{z}}{2}$  en  $y = \frac{z-\bar{z}}{2\sqrt{d}}$ . Zo wordt de oplossing  $x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$ :

$$x = \pm \frac{(x_0 + y_0\sqrt{d})^n + (x_0 - y_0\sqrt{d})^n}{2} \quad \text{en} \quad y = \pm \frac{(x_0 + y_0\sqrt{d})^n - (x_0 - y_0\sqrt{d})^n}{2\sqrt{d}}$$

(omdat toevoeging multiplicatief is) waarbij het  $\pm$ -teken voor  $x$  en  $y$  hetzelfde moet worden gekozen. Met het binomium van Newton worden deze uitdrukkingen ook nog (voor het geval met  $n \geq 0$  en het plusteken)

$$x = \frac{1}{2} \sum_{k=0}^n x_0^{n-k} y_0^k \binom{n}{k} \left( \sqrt{d}^k + (-\sqrt{d})^k \right)$$

$$\text{en} \quad y = \frac{1}{2\sqrt{d}} \sum_{k=0}^n x_0^{n-k} y_0^k \binom{n}{k} \left( \sqrt{d}^k - (-\sqrt{d})^k \right)$$

waaraan te zien is dat  $x$  en  $y$  inderdaad geheel zijn.

*Opmerking.*

De uitspraak “ $x_0, y_0$  is de minimale oplossing” betekent dat  $x_0 + y_0\sqrt{d}$  minimaal is. Echter, aangezien dan  $y_0\sqrt{d} = \sqrt{x_0^2 - 1}$  en omdat de functie  $x + \sqrt{x^2 - 1}$  stijgend is, is  $x_0 + y_0\sqrt{d}$  minimaal als en slechts als  $x_0$  (of  $y_0$ ) positief en zo klein mogelijk is (maar nog steeds groter dan 1, respectievelijk 0). Het minimaal zijn van  $x + y\sqrt{d}$  is dus volledig herleid tot het klein zijn van  $x$  en/of  $y$ . Hieruit volgt ook dat indien er een oplossing is, er een minimale oplossing is.

**Voorbeeld 13.43.** Los de vergelijking  $x^2 - 2y^2 = 1$  op in  $\mathbb{Z}$ .

*Oplossing.*

De kleinste positieve oplossing blijkt  $(3, 2)$  te zijn. Alle oplossingen zijn dus van de vorm

$$x = \pm \frac{(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n}{2} \quad \text{en} \quad y = \pm \frac{(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n}{2\sqrt{2}}$$

met  $n \in \mathbb{Z}$ . Bijvoorbeeld  $n = 2$  geeft (met het plusteken)  $(x, y) = (17, 12)$ ,  $n = 3$  geeft  $(99, 70)$ .

### 13.5.4 Recurrente betrekkingen

Vaak vraagt men om te bewijzen dat een bepaalde vergelijking oneindig veel oplossingen heeft. Indien de vergelijking te herschrijven is als een Pell-vergelijking kan je meteen zeggen dat dat inderdaad zo is. Er is echter een meer elementaire manier, die gebaseerd is op de oplossingsgedaante  $z = \pm z_0^n$ . We hernemen het voorbeeld van hierboven:

**Voorbeeld 13.44.** Bewijs dat de vergelijking  $x^2 - 2y^2 = 1$  oneindig veel oplossingen in natuurlijke getallen heeft.

*Oplossing.*

We bewijzen het volgende: als  $(x, y)$  een oplossing is, dan is ook  $(3x+4y, 2x+3y)$  een oplossing. Inderdaad, na uitwerken zien we dat  $(3x + 4y)^2 - 2(2x + 3y)^2 = x^2 - 2y^2$ . Aangezien  $(3, 2)$  een oplossing is vinden we een rij van oplossingen  $(x_{n+1}, y_{n+1}) = (3x_n + 4y_n, 2x_n + 3y_n)$  met  $(x_0, y_0) = (3, 2)$ . Dat deze oplossingen allemaal verschillend zijn, zien we aan het feit dat  $x_n$  strikt stijgt:  $x_{n+1} = 3x_n + 4y_n > x_n$ , van zodra  $x_n > 0$ .  $\square$

Merk op dat deze oplossing geen theorie over Pell-vergelijkingen gebruikt! De manier waarop ze werd bedacht is de volgende. Als  $x + y\sqrt{d}$  norm 1 heeft, dan heeft  $(x + y\sqrt{d})(x_0 + y_0\sqrt{d})$  ook norm 1, met  $(x_0, y_0)$  een willekeurige oplossing. Uitwerken geeft  $(x_0x + dy_0y, y_0x + x_0y)$  als oplossing. Dit is wat hierboven werd gedaan, met  $(x_0, y_0) = (3, 2)$  en  $d = 2$ .

Zo zal je, indien je al een niet-triviale oplossing kent, heel elementair kunnen bewijzen dat er oneindig veel oplossingen zijn. Men bekomt dus een nieuwe oplossing door twee oude oplossingen 'samen te stellen'. Een alternatief is om een oplossing met zichzelf samen te stellen, de recursie wordt dan  $(x_{n+1}, y_{n+1}) = (x_n^2 + dy_n^2, 2x_ny_n)$ .

Merk terloops op dat deze methode niets zinvols oplevert je enkel uitgaat van de oplossing  $(x_0, y_0) = (1, 0)$ .

Tot slot nog een opmerking over de algemene oplossing  $z = \pm z_0^n$ ,  $n \in \mathbb{Z}$ . Aangezien  $z_0$  positieve coëfficiënten heeft, zullen we als  $n \geq 0$  met het plusteken enkel oplossingen in natuurlijke getallen bekomen. Dit blijkt onder meer uit de recursie  $(x_{n+1}, y_{n+1}) = (x_0x_n + dy_0y_n, y_0x_n + x_0y_n)$ . Voor  $n \geq 0$  en met het minteken bekomen we dan precies de oplossingen met  $x, y < 0$ . Verder weten we dat  $z_0^{-1} = \bar{z}_0$ . Met  $n \leq 0$  en het plusteken bekomen we dus precies de oplossingen met  $y < 0 < x$ . Nemen we het minteken, dan hebben we  $x < 0 < y$ . De vier te onderscheiden gevallen met plus- en mintekens zitten dus bevat in het  $\pm$ -teken en de negatieve exponent. We kunnen dit echter omzeilen door de algemene oplossing te noteren met

$$x = \pm \frac{(x_0 + y_0\sqrt{d})^n + (x_0 - y_0\sqrt{d})^n}{2} \quad \text{en} \quad y = \pm \frac{(x_0 + y_0\sqrt{d})^n - (x_0 - y_0\sqrt{d})^n}{2\sqrt{d}}$$

met  $n \geq 0$ , en waarbij deze keer het  $\pm$ -teken onafhankelijk mag worden gekozen voor  $x$  en  $y$ . Zo zijn we van de negatieve exponenten verlost en behouden we toch alle oplossingen.

**Opgave 13.45.** (Baltic Way 1990 vraag 13) Bewijs dat de vergelijking  $x^2 - 7y^2 = 1$  oneindig veel oplossingen in natuurlijke getallen heeft.

### 13.6 Pell-typevergelijkingen

Een Pell-type vergelijking  $x^2 - dy^2 = a$  (of  $N(z) = a$ ) heeft niet steeds een oplossing, neem als voorbeeld  $x^2 - 3y^2 = -1$  of  $x^2 - 2y^2 = 5$ . We noemen  $x^2 - dy^2 = 1$  de corresponderende Pell-vergelijking. In deze sectie is steeds  $a \neq 0, 1$ .

### 13.6.1 Karakterisatie en begrenzingen

We kunnen de algemene oplossing opnieuw karakteriseren als we de ‘kleine’ oplossingen kennen:

#### Stelling 13.46.

Zij  $z$  een oplossing van  $N(z) = a$  en  $z_0$  de minimale oplossing van de corresponderende Pell-vergelijking. Zij  $z_1, z_2, \dots$  de elementen in  $[1, z_0[$  met norm  $a$ . Dan is  $z = \pm z_m z_0^k$  voor unieke  $m \in \mathbb{N}^+$  en  $k \in \mathbb{Z}$ .

*Bewijs.*

Stel dat  $z > 0$ , het andere geval gaat analoog. Bekijk de unieke  $k \in \mathbb{Z}$  waarvoor  $z_0^k \leq z < z_0^{k+1}$ . Dan is  $1 \leq z z_0^{-k} < z_0$ , en bijgevolg  $z z_0^{-k} = z_m$  voor zekere  $m$ . De uniciteit volgt uit het feit dat  $z_1, z_2, \dots$  in het interval  $[1, z_0[$  liggen en dus geen factor  $z_0^l$  met  $l \geq 1$  kunnen verschillen.  $\square$

Merk op dat niets zegt over het aantal  $z_1, z_2, \dots$ . Misschien zijn het er oneindig veel, of slechts 1. We noemen  $z_1, z_2, \dots$  de minimale oplossingen van de Pell-typevergelijking.

#### Stelling 13.47. Bovengrens voor de kleinste minimale oplossing

Stel dat de Pell-typevergelijking  $x^2 - dy^2 = a$  een oplossing heeft, en zij  $z_0$  de minimale oplossing van  $x^2 - dy^2 = 1$ . Dan is er een oplossing met  $|y| \leq \frac{z_0+1}{2\sqrt{dz_0}} \sqrt{|a|}$ .

*Bewijs.*

Idee van het bewijs: voor een oplossing  $z = x + y\sqrt{d}$  van  $N(z) = a$  geldt dat  $2\sqrt{d}|y| = |z - \bar{z}| = |z - \frac{a}{z}| \leq |z| + \left|\frac{a}{z}\right|$ .  $|y|$  zal dus tamelijk klein zijn wanneer  $z \approx \sqrt{|a|}$ . Zij nu  $z_1 > 0$  met norm  $a$ , en kies  $m \in \mathbb{Z}$  zo dat  $\sqrt{\frac{|a|}{z_0}} \leq z_0^m z_1 < \sqrt{|a|} z_0$ . Dan is  $x + y\sqrt{d} = z = z_0^m z_1$  een element met norm  $a$  (dat relatief dicht bij  $\sqrt{|a|}$  ligt) en met

$$2\sqrt{d}|y| \leq |z| + \left|\frac{a}{z}\right| \leq \max_{\sqrt{\frac{|a|}{z_0}} \leq t < \sqrt{|a|} z_0} \left(t + \frac{|a|}{t}\right) = \frac{z_0 + 1}{\sqrt{z_0}} \sqrt{|a|},$$

aangezien  $t + \frac{|a|}{t}$  dalend is voor  $0 < t < \sqrt{|a|}$  en stijgend voor  $t > \sqrt{|a|}$ .  $\square$

*Opmerking.*

Deze stelling zegt niet dat elke minimale oplossing voldoet aan  $|y| \leq \frac{z_0+1}{2\sqrt{dz_0}} \sqrt{|a|}$ . Ze is dan ook niet nuttig om alle oplossingen te bepalen. Het nut ervan is dat ze toelaat om te bewijzen dat een Pell-typevergelijking geen oplossingen heeft: het volstaat dan om te controleren dat er geen oplossingen zijn met  $0 \leq y \leq \frac{z_0+1}{2\sqrt{dz_0}} \sqrt{|a|}$ .

**Opgave 13.48.** Als  $a > 0$  lijkt de ongelijkheid  $|z - \frac{a}{z}| \leq |z| + \left|\frac{a}{z}\right|$  uit het bewijs erg onnauwkeurig. Vreemd genoeg blijkt het omzeilen van deze ongelijkheid niet zo'n veel scherper resultaat op te leveren. Toon analoog aan dat je voor  $a > 0$  op zijn best kan bewijzen dat er een oplossing is met  $|y| \leq \frac{z_0-1}{2\sqrt{dz_0}} \sqrt{a}$ . A

*Opmerking.*

Een erg grote verbetering geeft dit niet voor het geval  $a > 0$ , tenzij  $z_0$  klein is. Veelal zal die

tweede bovengrens niets meer vertellen, maar hij is misschien toch de moeite om te vermelden.

Merk op dat we geen zo'n bovengrens hadden voor gewone Pell-vergelijkingen. Neem als voorbeeld  $x^2 - 991y^2 = 1$ . De kleinste niet-triviale oplossing is<sup>25</sup>

$$y = 12055735790331359447442538767$$

met een nog grotere waarde voor  $x$ . Geef toe, als je niets kende van Pell-vergelijkingen en de eerste  $12 \cdot 10^{27}$  natuurlijke getallen had gecontroleerd zou je gaan geloven dat die vergelijking geen oplossingen heeft, niet?

**Stelling 13.49.** Bovengrens voor minimale oplossingen

Elke minimale oplossing van  $x^2 - dy^2 = a$  voldoet aan  $|y| \leq \frac{\max(|a|, z_0) + 1}{2\sqrt{d}}$ .

*Bewijs.*

Zij  $z$  minimaal. Er geldt  $2\sqrt{d}|y| = |z - \bar{z}| \leq z + \frac{|a|}{z}$ . De functie  $f(t) = t + \frac{|a|}{t}$  is dalend voor  $0 < t < \sqrt{|a|}$  en stijgend voor  $t > \sqrt{|a|}$ . Aangezien  $z \in [1, z_0]$  kunnen we verder vergroten tot  $\max(z_0 + \frac{|a|}{z_0}, 1 + |a|)$ . We onderscheiden twee gevallen: als  $z_0 \leq |a|$  is  $z_0 \in [1, |a|]$  en dus  $f(z_0) \leq f(1) = f(|a|)$ , zodat  $z_0 + \frac{|a|}{z_0} \leq 1 + |a|$ . Als  $z_0 \geq |a|$  is  $z_0 + \frac{|a|}{z_0} \leq z_0 + 1$ . Combineren we deze twee gevallen, dan blijkt dat  $2\sqrt{d}|y| \leq \max(|a|, z_0) + 1$ .  $\square$

In het bijzonder leren we hieruit dat er hoogstens een eindig aantal minimale oplossingen is.

### 13.6.2 Gedrag van minimale oplossingen

We bekijken enkele voorbeelden van Pell-typevergelijkingen die het gedrag van minimale oplossingen illustreren.

**Voorbeeld 13.50.** Bepaal alle gehele oplossingen van  $x^2 - 7y^2 = 2$ .

*Oplossing.*

De corresponderende Pell-vergelijking heeft als minimale oplossing  $8 + 3\sqrt{7}$ . We moeten enkel nog de minimale oplossingen  $z = x + y\sqrt{7}$  bepalen van  $N(z) = 2$  waarvoor dus  $|y| \leq \frac{\max(|a|, z_0) + 1}{2\sqrt{d}}$ .

We hebben  $|a| < z_0 < 16$  en  $\sqrt{7} > 2$  zodat  $|y| < \frac{17}{4}$ . Het volstaat dan om te controleren of  $-4, \dots, 4$  aanleiding geven tot een minimale oplossing. Enkel  $y = \pm 1$  geeft een oplossing, en alleen  $3 + 1 \cdot \sqrt{7}$  blijkt in het interval  $[1, 8 + 3\sqrt{7}]$  te liggen. Alle oplossingen worden dus gegeven door  $x + y\sqrt{7} = \pm(3 + \sqrt{7})(8 + 3\sqrt{7})^n$ ,  $n \in \mathbb{Z}$ . Een expliciete uitdrukking voor  $x$  en  $y$  kan je vinden door deze uitdrukking (voor  $n \geq 0$ ) uit te schrijven met het binomium van Newton en de coëfficiënten af te lezen.

In dit voorbeeld was er slechts één minimale oplossing. Dat is niet altijd het geval.

**Voorbeeld 13.51.** Bepaal alle gehele oplossingen van  $x^2 - 10y^2 = 9$ .

*Oplossing.*

De minimale oplossing van  $x^2 - 10y^2 = 1$  is  $19 + 6\sqrt{10}$ . We bepalen de minimale oplossingen van de Pell-typevergelijking, met dus  $|y| \leq \frac{\max(|a|, z_0) + 1}{2\sqrt{d}} = 3 + \sqrt{10}$ . We bekijken dus  $y \in \{-6, \dots, 6\}$ . De mogelijke minimale oplossingen blijken  $(\pm 3, 0)$ ,  $(\pm 7, \pm 2)$ , en  $(\pm 13, \pm 4)$ .

<sup>25</sup> *A First Course in Algebra*, J. Rotman

Enkel  $3$ ,  $7 + 2\sqrt{10}$  en  $13 + 4\sqrt{10}$  liggen in het interval  $[1, 19 + 6\sqrt{10}]$ . Alle oplossingen worden dus gegeven door  $\pm 3 \cdot (19 + 6\sqrt{10})^n$ ,  $\pm (7 + 2\sqrt{10})(19 + 6\sqrt{10})^n$  en  $\pm (13 + 4\sqrt{10})(19 + 6\sqrt{10})^n$ ,  $n \in \mathbb{Z}$ .

Merk op dat de minimale oplossing van de Pell-vergelijking hier aanleiding geeft tot  $\pm 3 \cdot (19 + 6\sqrt{10})^n$ , aangezien  $9 = 3^2$ . Er bleken echter nog meer oplossingen te zijn.

Je zou verder kunnen vermoeden dat minimale oplossingen steeds positieve coëfficiënten hebben, zoals dat bij Pell-vergelijkingen was. Dat is helaas niet waar: zowel  $4 + \sqrt{5}$  als  $4 - \sqrt{5}$  zijn minimale oplossingen van de Pell-typevergelijking  $x^2 - 5y^2 = 11$ . (De minimale oplossing van  $x^2 - 5y^2 = 1$  is  $9 + 4\sqrt{5}$ .)

Dergelijke minimale oplossingen hoeven ook niet steeds samen met hun toegevoegde voor te komen: zo is  $5 - \sqrt{2}$  een minimale oplossing van  $x^2 - 2y^2 = 23$ , maar  $5 + \sqrt{2}$  is dat niet (het is groter dan  $3 + 2\sqrt{2}$ ). ( $5 + \sqrt{2}$  is afkomstig van de minimale oplossing  $11 - 7\sqrt{2} \approx 1.1$  aangezien  $5 + \sqrt{2} = (11 - 7\sqrt{2})(3 + 2\sqrt{2})$ .)

De  $x$ -waarde kan ook best negatief zijn. Zo is  $-1 + \sqrt{5}$  een minimale oplossing van  $x^2 - 5y^2 = -4$ .

### 13.6.3 Recurrente betrekkingen

Zoals bij Pell-vergelijkingen kunnen we ook hier soms gemakkelijk (t.t.z. zonder al die theorie) beargumenteren dat een vergelijking oneindig veel oplossingen heeft.


**Voorbeeld 13.52.** Toon aan dat de vergelijking  $x^2 - 2y^2 = 23$  oneindig veel natuurlijke oplossingen heeft.

*Oplossing.*

Als  $(x, y)$  een oplossing is, dan blijkt na uitwerken dat ook  $(3x + 4y, 2x + 3y)$  een oplossing is. Aangezien  $(5, 1)$  een oplossing is vinden we een rij van oplossingen  $(x_{n+1}, y_{n+1}) = (3x_n + 4y_n, 2x_n + 3y_n)$  met  $(x_0, y_0) = (5, 1)$ . Dat deze oplossingen allemaal verschillend zijn, zien we aan het feit dat  $x_n$  strikt stijgt:  $x_{n+1} = 3x_n + 4y_n > x_n$ , van zodra  $x_n > 0$ .  $\square$

Uiteraard is deze oplossing helemaal gebaseerd op de oplossingsverzameling  $(5 + \sqrt{2})(3 + 2\sqrt{2})^n$ , waaruit de recursie  $(x_{n+1}, y_{n+1}) = (3x_n + 4y_n, 2x_n + 3y_n)$  volgt. Dezelfde redenering gaat op voor eenderwelke Pell-typevergelijking. Het kan soms wel iets lastiger worden om aan te tonen dat alle geconstrueerde oplossingen verschillend zijn, indien de gekozen beginoplossing een minteken bevat. Indien er geen extra voorwaarden aan verbonden zijn kan je simpelweg plustekens nemen en je van de minimaliteit van de beginoplossing niets aantrekken. (Herinner je eraan dat de minimale oplossing van de Pell-vergelijking steeds positieve coëfficiënten heeft.) Als er echter een extra voorwaarde is moet je misschien noodgedwongen en beginoplossing met een minteken nemen. Om dan aan te tonen dat alle oplossingen verschillend zijn zal je een of andere truc moeten uitvinden. Het kan soms ook nuttig zijn om dan de recursie  $(x_{n+1}, y_{n+1}) = (x_n^2 + dy_n^2, 2x_n y_n)$  te gebruiken, indien deze de bijkomende voorwaarden bewaart. Hierbij is de rij van  $x$ -waarden in elk geval stijgend van zodra  $|x| > 1$ .

## Opgaven hoofdstuk 13

**Opgave 13.53.** Bewijs dat de vergelijking  $a^2 - 15b^2 = 3$  geen gehele oplossingen heeft.  H

**Opgave 13.54.** (NWO 1994 finale vraag 3)

- A. Bewijs dat elk veelvoud van 6 te schrijven is als de som van vier derdemachten van gehele getallen.

- B. Bewijs dat elk geheel getal te schrijven is als de som van vijf derdemachten van gehele getallen.

**Opgave 13.55.** (VWO 2003 finale vraag 4) In het vlak beschouwt men het rooster van alle punten met gehele coördinaatgetallen. Indien met een getal  $r$  goed kiest gaat de cirkel met middelpunt  $(0, 0)$  en met straal  $r$  door een aantal roosterpunten. (Bijvoorbeeld, de cirkel met  $r = 2\sqrt{2}$  gaat door vier punten). Bewijs dat er voor elk natuurlijk getal  $n$  een reëel getal  $r$  bestaat, zo dat de cirkel met straal  $r$  en middelpunt  $(0, 0)$  door minstens  $n$  roosterpunten gaat.

**Opgave 13.56.** Een driehoeksgetal is een geheel getal van de vorm  $\frac{k \cdot (k+1)}{2}$ . Bewijs dat elk natuurlijk getal de som is van drie driehoeksgetallen.

**Opgave 13.57.** (VWO 2005 finale vraag 3) Een getal is goed als het kan geschreven worden als de som van twee verschillende strikt positieve kwadraten. Een getal is beter als dit op minstens twee manieren kan, en best als dit op minstens vier manieren kan.

- A. Bewijs dat het product van twee goede getallen goed is.  
 B. Bewijs dat 5 goed is, 2005 beter en  $2005^2$  best.

**Opgave 13.58.** (LIMO 2014 vraag 8)

- A. Bepaal alle  $(x, y) \in \mathbb{Z}^2$  zodanig dat  $|3x^2 - 7xy + 3y^2 - 6| \leq 1$ .  
 B. Bepaal alle  $(x, y, z) \in \mathbb{Z}^3$  zodanig dat

$$|x^4 + y^4 + z^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2| \leq 4.$$

**Opgave 13.59.** (MOAWOA 2014 vraag 3) Bewijs dat voor alle  $n \in \mathbb{N}$  er oneindig veel koppels  $(x, y) \in \mathbb{N}^2$  zijn zo dat  $x \mid n + y^2$  en  $y \mid n + x^2$ .

**Opgave 13.60.** Bewijs dat er oneindig veel  $n \in \mathbb{N}$  zijn zo dat  $n$ ,  $n + 1$  en  $n + 2$  alle drie de som van twee kwadraten zijn.

**Opgave 13.61.** Vind alle driehoeken waarvan de zijden opeenvolgende natuurlijke getallen zijn en waarvan de oppervlakte ook natuurlijk is.

**Opgave 13.62.** Zij  $A = \{n^2 - 1 : n \in \mathbb{N}^+\}$ . Bewijs dat voor elke  $a \in A$  oneindig veel koppels  $(b, c)$  in  $A$  te vinden zijn met  $b = ac$ .

**Opgave 13.63.** Bewijs dat er oneindig veel gehele getallen  $n$  zijn waarvoor zowel  $2n + 1$  als  $3n + 1$  kwadraten zijn en zo dat  $n$  een veelvoud is van 40.

**Opgave 13.64.** Bewijs dat er oneindig veel natuurlijke koppels  $(x, y)$  bestaan waarvoor  $\frac{x+1}{y} + \frac{y+1}{x} = 4$ .

**Opgave 13.65.** (USAMO 1986 vraag 3) Bepaal het kleinste natuurlijk getal  $n > 1$  zo dat het rekenkundig gemiddelde van de getallen  $1^2, 2^2, \dots, n^2$  zelf een kwadraat is.

**Opgave 13.66.** Bewijs dat  $5x^2 + 4$  of  $5x^2 - 4$  een kwadraat is als en slechts als  $x$  een Fibonaccigetal is.

**Opgave 13.67.** Vind alle  $n \in \mathbb{N}$  zo dat  $\binom{n}{k-1} = 2\binom{n}{k} + \binom{n}{k+1}$  voor een zeker natuurlijk getal  $k < n$ .

**Opgave 13.68.** Zij  $a \in \mathbb{N}$  en  $x$  en  $y$  gehele getallen zo dat  $|x^2 - (a^2 - 1)y^2| < 2a + 2$ . Bewijs dat  $|x^2 - (a^2 - 1)y^2|$  een kwadraat is.

**Opgave 13.69.** Bewijs dat de vergelijking  $x^2 - dy^2 = -1$  oplosbaar is als en slechts als  $c^2 - dy^2 = -4$  dat is.

**Opgave 13.70.** Zij  $p$  een priemgetal. Bewijs dat de vergelijking  $x^2 - py^2 = -1$  een gehele oplossing heeft als en slechts als  $p = 2$  of  $p \equiv 1 \pmod{4}$ .

**Opgave 13.71.** Zij  $p$  een priemgetal van de vorm  $4k + 3$ . Bewijs dat precies één van de vergelijkingen  $x^2 - py^2 = \pm 2$  een gehele oplossing heeft.

**Opgave 13.72.** Toon aan dat een Pell-vergelijking  $x^2 - dy^2 = 1$  een oplossing heeft met H

$$0 < |y| < 16^{1024^{d^3}}.$$

**Opgave 13.73.** Vind alle  $n \in \mathbb{N}$  waarvoor  $3^n - 2$  een kwadraat is.

**Opgave 13.74.** Bewijs dat als  $\frac{x^2+1}{y^2} + 4$  een kwadraat is, dit gelijk is aan 9.

**Opgave 13.75.** (MOAWOA 2015 Vraag 2) Zij  $n > 1$  een natuurlijk getal. Bewijs dat er natuurlijke getallen  $a, b, c > 0$  bestaan zo dat  $a + b = n$  en  $|ab - c^2| \leq 4$ .

**Opgave 13.76.** Zij  $p \equiv 3 \pmod{4}$  een priemgetal. Bewijs dat de vergelijking ✿

$$|x^2 - py^2| = \frac{p-1}{2}$$

een gehele oplossing heeft.

# 14 Rationale en irrationale getallen

## 14.1 Diophantische benadering

### Stelling 14.1.

Als  $\alpha$  irrationaal is, dan bestaat er voor elk reëel getal  $r \in [0, 1]$  en elk reëel getal  $\varepsilon > 0$  een getal  $q \in \mathbb{N}$  zo dat  $|\{q\alpha\} - r| < \varepsilon$ .

Anders uitgedrukt, als  $\alpha$  irrationaal is kan het gedeelte na de komma van  $q\alpha$  willekeurig dicht bij elk reëel getal  $r \in [0, 1]$  komen te liggen, voor  $q \in \mathbb{N}$ .<sup>26</sup>

**Opgave 14.2.** We bewijzen Stelling 14.1.

Kies  $n$  zo groot dat  $n > \frac{1}{\varepsilon}$ . We verdelen het interval  $[0, 1]$  in  $n$  intervallen van lengte  $\frac{1}{n}$ . Beschouw nu de  $n + 1$  getallen  $0, \{\alpha\}, \dots, \{n\alpha\}$ .

- Toon aan dat er zeker twee van die getallen in hetzelfde deelinterval van lengte  $\frac{1}{n}$  liggen.
- Toon aan dat er getallen  $a \in \mathbb{N}^+$  en  $b \in \mathbb{Z}$  bestaan waarvoor  $0 < a\alpha + b < \frac{1}{n}$ .

Stel dat  $r$  in het interval  $[\frac{m}{n}, \frac{m+1}{n}]$  ligt.

- Bewijs dat er een  $k \in \mathbb{N}^+$  bestaat zo dat  $k(a\alpha + b)$  ook in het interval  $[\frac{m}{n}, \frac{m+1}{n}]$  ligt.

Dan geldt dat  $|ka\alpha + bk - r| < \frac{1}{n}$ . Omdat  $0 < ka\alpha + bk < 1$  en  $bk \in \mathbb{Z}$  zal  $\{ka\alpha\} = ka\alpha + bk$ . Er geldt dus  $|\{ka\alpha\} - r| < \frac{1}{n} < \varepsilon$ .

### Gevolg 14.3.

Als  $\alpha$  irrationaal is,  $r \in \mathbb{R}$  en  $\varepsilon > 0$ , dan bestaan er  $q \in \mathbb{N}^+$  en  $p \in \mathbb{Z}$  zo dat  $|q\alpha - p - r| < \varepsilon$ .

*Bewijs.*

We kunnen de vorige stelling toepassen op  $\{r\}$ , zodat  $q \in \mathbb{N}$  bestaat waarvoor  $|\{q\alpha\} - \{r\}| < \varepsilon$ . Stellen we  $p = \lfloor q\alpha \rfloor - \lfloor r \rfloor$ , dan geldt  $|q\alpha - p - r| < \varepsilon$ .  $\square$

Nemen we in het bijzonder  $r = 0$ , dan vinden we  $\frac{p}{q} \in \mathbb{Q}$  waarvoor  $|\alpha - \frac{p}{q}| < \frac{\varepsilon}{q} \leq \varepsilon$ . Een irrationaal getal wordt dus willekeurig goed benaderd door rationale getallen. Het benaderen van reële getallen door rationale getallen noemt men Diophantische benadering. Een sterker resultaat is het volgende:

<sup>26</sup>Men zegt dat de verzameling van fractionele delen  $\{q\alpha\}$  *dicht* is in  $[0, 1]$ .



**Stelling 14.4.** Benaderingsstelling van Dirichlet

Zij  $\alpha$  een irrationaal getal en  $n \in \mathbb{N}^+$ . Dan bestaan er  $p \in \mathbb{Z}$  en  $q \in \{1, \dots, n\}$  waarvoor

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{(n+1)q}.$$

**Opgave 14.5.** Bewijs Dirichlet's benaderingsstelling.

**Gevolg 14.6.**

Als  $\alpha \in \mathbb{R}$  bestaan er oneindig veel koppels  $(p, q) \in \mathbb{Z} \times \mathbb{N}^+$  waarvoor  $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$ .

*Bewijs.*

Als  $\alpha = \frac{a}{b}$  rationaal is, kies dan  $p = ka$ ,  $q = kb$  met  $k \in \mathbb{N}^+$ . Als  $\alpha$  irrationaal is, neem dan  $n_1 \in \mathbb{N}^+$ . Wegens de vorige stelling bestaan er  $p_1 \in \mathbb{Z}$  en  $q_1 \leq n_1$  met  $\left| \alpha - \frac{p_1}{q_1} \right| < \frac{1}{(n_1+1)q_1} < \frac{1}{q_1^2}$ . Kies dan  $n_2$  zo groot dat  $\frac{1}{n_2} < \left| \alpha - \frac{p_1}{q_1} \right|$ . We vinden analoog  $p_2$  en  $q_2$  met  $\left| \alpha - \frac{p_2}{q_2} \right| < \frac{1}{(n_2+1)q_2} < \frac{1}{n_2}$ , dus is zeker  $(p_1, q_1) \neq (p_2, q_2)$ . Zo vinden we oneindig veel koppels.  $\square$

**14.1.1 Toepassingen van Diophantische benadering****14.1.2 Irrationaliteit van reekssommen**

Vaak stelt men zich de vraag of een bepaald reëel getal, pakweg  $\sqrt{3}$ ,  $\pi$ ,  $e$ ,  $e^2$ ,  $e^\pi$ ,  $e + \pi$ , ... irrationaal is. Om dit te onderzoeken loont het vaak de moeite om het betreffende getal te schrijven als reekssom:

$$\sum_{n=1}^{\infty} \frac{1}{a_n}$$

met  $a_n \in \mathbb{Z}$ . Een verder interessante eigenschap van rationale getallen is de volgende:

**Eigenschap 14.7.**

Als  $n, p, q \in \mathbb{Z}$  met  $q \neq 0$ , dan is het fractioneel deel van  $n \cdot \frac{p}{q}$  ofwel 0, ofwel ten minste  $\frac{1}{q}$ .

Stel nu dat we een reekssom hebben gegeven waarvan we wensen aan te tonen dat het irrationaal is, bijvoorbeeld  $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ . Stel dat  $e \in \mathbb{Q}$ , dus  $e = \frac{p}{q}$ . Dan zou ofwel  $ae \in \mathbb{Z}$  of  $\{a \cdot e\} \geq \frac{1}{q}$  voor  $a \in \mathbb{N}$ . We kiezen zulke  $a$  nu op zo'n manier dat een hoop termen van de reekssom geheel worden. Nemen we bijvoorbeeld  $a = k!$  voor zekere  $k$ ; dan vinden we

$$k!e = \sum_{n=0}^k \frac{k!}{n!} + \sum_{n=k+1}^{\infty} \frac{k!}{n!}.$$

De eerste som is nu een geheel getal. De tweede som is wegens het veronderstelde minstens  $\frac{1}{q}$ . De strategie is nu om aan te tonen dat er een  $k \in \mathbb{N}$  bestaat waarvoor die tweede som tóch

kleiner is dan  $\frac{1}{q}$ ; deze tegenstrijdigheid leidt dan tot de conclusie dat  $e$  irrationaal is. Merk op dat voor  $n > k$ ,

$$\frac{k!}{n!} = \frac{1}{n(n-1)\cdots(k+1)} \leq \frac{1}{(k+1)^{n-k}}$$

waarbij de ongelijkheid strikt is voor  $n > k + 1$ . Dus

$$\sum_{n=k+1}^{\infty} \frac{k!}{n!} < \sum_{n=k+1}^{\infty} \frac{1}{(k+1)^{n-k}} = \frac{1}{k}.$$

Het volstaat nu om  $k \geq q$  te kiezen. We besluiten:

**Stelling 14.8.**

$e$  is irrationaal.

Bovenstaand bewijs hebben we te danken aan Joseph Fourier. Wat het zo interessant maakt is dat het inspirerend is om de irrationaliteit van andere getallen te bewijzen. Stel dat  $(a_n)$  een rij natuurlijke getallen is, en dat we willen bewijzen dat  $x = \sum_{n=1}^{\infty} \frac{1}{a_n}$  irrationaal is. Analoog als in het bewijs van Fourier vermenigvuldigen we  $x$  met een geheel getal  $a$  op zo'n manier dat de eerste  $k$  termen in de som geheel worden. In het geval van  $a_n = n!$  konden we  $a = k!$  nemen. In het algemeen moeten we voor  $a$  een veelvoud nemen van  $\text{kgv}(a_1, \dots, a_k)$ . We nemen even voor het gemak  $a = a_1 a_2 \cdots a_k$ . We hopen nu voor elke  $q \in \mathbb{N}$  een  $k \in \mathbb{N}$  te vinden waarvoor

$$\sum_{n=k+1}^{\infty} \frac{a_1 a_2 \cdots a_k}{a_n} < \frac{1}{q}.$$

**Opgave 14.9.** Zij  $(a_n)$  een strikt stijgende rij natuurlijke getallen zo dat



$$\lim_{n \rightarrow \infty} \frac{a_{n+1}}{a_1 a_2 \cdots a_n} = \infty.$$

Bewijs dat  $\sum_{n=1}^{\infty} \frac{1}{a_n}$  convergeert naar een irrationaal getal.

**Opgave 14.10.** Zij  $(a_n)$  een stijgende rij natuurlijke getallen zo dat



$$\lim_{n \rightarrow \infty} a_n^{2^{-n}} = \infty.$$

Bewijs dat  $\sum_{n=1}^{\infty} \frac{1}{a_n}$  convergeert naar een irrationaal getal.

De overkoepelende strategie valt als volgt samen te vatten:

**Stelling 14.11.**

Zij  $(a_n)$  een rij niet-nul gehele getallen waarvoor  $\sum_{n=1}^{\infty} \frac{1}{a_n}$  convergeert en

$$\liminf_{k \rightarrow \infty} \left| \sum_{n=k+1}^{\infty} \frac{\text{kgv}(a_1, \dots, a_k)}{a_n} \right| = 0.$$

Dan is  $\sum_{n=1}^{\infty} \frac{1}{a_n}$  irrationaal.

**Voorbeeld 14.12.** Zij  $(x_n)$  een rij waarvan elke term  $\pm 1$  is. Bewijs dat



$$\sum_{n=0}^{\infty} \frac{x_n}{n!}$$

irrationaal is.

*Oplossing.*

In Fourier's bewijs dat  $e$  irrationaal is blijkt dat

$$\liminf_{k \rightarrow \infty} \left| \sum_{n=k+1}^{\infty} \frac{k!}{n!} \right| = 0.$$

Bijgevolg is

$$\liminf_{k \rightarrow \infty} \left| \sum_{n=k+1}^{\infty} \frac{\text{kgv}(x_1 \cdot 1!, \dots, x_k \cdot k!)}{x_n \cdot n!} \right| \leq \liminf_{k \rightarrow \infty} \left| \sum_{n=k+1}^{\infty} \frac{k!}{x_n \cdot n!} \right| \leq \liminf_{k \rightarrow \infty} \left| \sum_{n=k+1}^{\infty} \frac{k!}{n!} \right| = 0$$

zodat  $\sum_{n=0}^{\infty} \frac{1}{x_n \cdot n!}$  irrationaal is. □

Het is evenwel mogelijk het bewijs van Fourier aan te passen en zonder veel moeite dezelfde conclusie trekken. Wat je dan zal doen komt in essentie neer op bovenstaande oplossing. Het voordeel van wat we hier toonden is dat het bewijs iets overzichtelijker wordt (en we geen dubbel rekenwerk moeten doen!) door te gebruiken van wat we reeds weten over  $\liminf_{k \rightarrow \infty} \left| \sum_{n=k+1}^{\infty} \frac{\text{kgv}(1, \dots, k)}{n!} \right|$ .

**Opgave 14.13.** Probeer de volgende veralgemening van Opgave 14.10 aan te tonen: A

Zij  $(a_n)$  een stijgende rij natuurlijke getallen en  $c > 1$  zo dat

$$\lim_{n \rightarrow \infty} a_n^{c^{-n}} = \infty.$$

Dan convergeert  $\sum_{n=1}^{\infty} \frac{1}{a_n}$  naar een irrationaal getal.

Wat loopt er mis? Kan je een voorbeeld van zo'n rij geven waarvoor de voorwaarde uit Stelling 14.11 niet van toepassing is?

*Opmerking.*

Voor zover ik weet is de claim uit bovenstaande opgave een openstaand probleem.<sup>27</sup>

<sup>27</sup>Zie <http://math.stackexchange.com/questions/1385325>

## 14.2 Kettingbreuken

## 14.3 Pellvergelijkingen

## 14.4 Irrationale en transcendente getallen

### Definitie 14.14. Algebraïsch

Een *algebraïsch getal* is een complex getal dat een nulpunt is van een niet-nul veelterm met gehele coëfficiënten.

**Opgave 14.15.** Toon aan dat elk rationaal getal algebraïsch is.

### Definitie 14.16. Transcendent

Een *transcendent getal* is een complex getal dat niet algebraïsch is.

### Stelling 14.17. Stelling van Gelfond-Schneider

Zij  $a, b \in \mathbb{C} \setminus \{0, 1\}$ ,  $a$  algebraïsch en  $b$  irrationaal. Dan is  $a^b$  transcendent.

**Opgave 14.18.** Bewijs dat  $\sqrt{2}^{\sqrt{2}}$  irrationaal is.

## 14.5 De irrationaliteitsmaat

### Definitie 14.19. Irrationaliteitsmaat

Zij  $x \in \mathbb{R}$  en  $M$  de verzameling van  $m \in \mathbb{R}$  waarvoor er slechts eindig veel relatief priem koppels  $(p, q) \in \mathbb{Z}^2$  bestaan met

$$0 < \left| x - \frac{p}{q} \right| < \frac{1}{q^m}.$$

Het infimum van  $M$  wordt de *irrationaliteitsmaat van  $x$*  genoemd:  $\mu(x) = \inf M$ .

### Stelling 14.20.

Voor  $x \in \mathbb{Q}$  is  $\mu(x) = 1$ .

**Opgave 14.21.** Bewijs.

**Stelling 14.22.**

Als  $x$  irrationaal is, is  $\mu(x) \geq 2$ .

*Bewijs.*

Dit is precies Gevolg 14.6. □

**14.5.1 Thue-Siegel-Roth****14.5.2 Liouville-getallen****Opgaven hoofdstuk 14**

**Opgave 14.23.** Zij  $(x_n)$  een rij natuurlijke getallen zo dat  $\sin x_n$  strikt daalt en nadert naar 0. ✿ A  
Is dan noodzakelijk  $\sqrt[n]{\sin x_n} \rightarrow 1$ ?

**Opgave 14.24.** Bestaat er een irrationaal getal  $\alpha$  waarvoor de verzameling  $\{2^n \alpha : n \in \mathbb{N}\}$  ✿  
niet dicht is in  $[0, 1]$ ?

**Opgave 14.25.** Zij  $(a_n)$  een strikt stijgende rij natuurlijke getallen. Bewijs dat  $\sum_{n=1}^{\infty} \frac{2^{a_n}}{a_n!}$  con- ✿  
vergeert naar een irrationaal getal.

# 15 Veeltermen

## Definitie 15.1. Eenheidsveelterm

Zij  $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  of  $\mathbb{C}$ . We noemen een veelterm  $P \in \mathbb{K}[x]$  een *eenheidsveelterm over  $\mathbb{K}$*  als er een veelterm  $Q \in \mathbb{K}[x]$  bestaat met  $PQ = 1$ .

De constante veeltermen 1 en  $-1$  zijn eenheidsveeltermen over  $\mathbb{Z}$ . Als  $n \in \mathbb{Z}$  en  $|n| > 1$  is  $n$  is geen eenheidsveelterm over  $\mathbb{Z}$ . Wel over  $\mathbb{Q}, \mathbb{R}$  en  $\mathbb{C}$ , want  $n \cdot \frac{1}{n} = 1$  en  $\frac{1}{n} \in \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ . Het begrip eenheidsveelterm hangt dus af van de gekozen verzameling  $\mathbb{K}$ .

Merk op dat, aangezien  $\deg PQ = \deg P + \deg Q$ , een eenheidsveelterm noodzakelijk een constante veelterm is.

## Definitie 15.2. Irreducibel

Zij  $\mathbb{K} = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$  of  $\mathbb{C}$ . We noemen een veelterm  $P \in \mathbb{K}[x]$  *irreducibel over  $\mathbb{K}$*  als er geen niet-eenheidsveeltermen  $Q, R \in \mathbb{K}[x]$  bestaan met  $QR = P$ . Of nog, als  $QR = P$  enkel kan indien  $Q$  of  $R$  een eenheidsveelterm is.

## Stelling 15.3. Rationale worteltest

Zij  $\frac{p}{q}$  een rationale wortel van  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ , met dus  $p, q \in \mathbb{Z}$  en  $\text{ggd}(p, q) = 1$ . Dan is  $p \mid a_0$  en  $q \mid a_n$ .

In het bijzonder geldt:

## Gevolg 15.4. Gehele worteltest

Zij  $n$  een gehele wortel van  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ . Dan is  $n \mid a_0$ .

## Stelling 15.5. Criterium van Eisenstein

Zij  $P = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ . Als er een priemgetal  $p$  bestaat waarvoor  $p \mid a_0, a_1, \dots, a_{n-1}$  en  $p^2 \nmid a_0$ , dan is  $P$  irreducibel.

**Stelling 15.6.** Lemma van Gauss

Zij  $P \in \mathbb{Z}[x]$  irreducibel. Dan is  $P$  irreducibel over  $\mathbb{Q}$ .

Het omgekeerde is niet waar: zo is bijvoorbeeld  $2x \in \mathbb{Z}[x]$  irreducibel over  $\mathbb{Q}$ , maar niet over  $\mathbb{Z}$ :  $2$  en  $x$  zijn geen eenheidsveeltermen over  $\mathbb{Z}$ , maar  $2$  is wel een eenheidsveelterm over  $\mathbb{Q}$ . De omgekeerde richting geldt wel indien de ggd van alle coëfficiënten  $1$  is: dan is het immers onmogelijk dat de veelterm in kwestie deelbaar is door een gehele  $\mathbb{Q}$ -eenheidsveelterm die geen  $\mathbb{Z}$ -eenheidsveelterm is (de enige zulke eenheidsveeltermen zijn  $\pm 1$ ).

## Opgaven hoofdstuk 15

**Opgave 15.7.** Bewijs dat  $x^n + x + 3$  irreducibel is over  $\mathbb{Q}$  voor  $n \geq 1$ .



## 16.1 Het Frobeniusgetal

**Definitie 16.1.** Frobeniusgetal

Het *Frobeniusgetal* van  $a_1, \dots, a_n \in \mathbb{N}$  met  $\text{ggd}(a_1, \dots, a_n) = 1$  is het grootste natuurlijk getal dat niet kan worden geschreven als lineaire combinatie van die getallen, waarbij enkel positieve coëfficiënten zijn toegelaten. We noteren  $g(a_1, \dots, a_n)$ .

Om te beginnen is het al niet vanzelfsprekend dat het Frobeniusgetal steeds bestaat indien  $\text{ggd}(a_1, \dots, a_n) = 1$ .

**Stelling 16.2.**

Als  $\text{ggd}(a_1, \dots, a_n) = 1$  dan bestaat het Frobeniusgetal  $g(a_1, \dots, a_n)$ .

**Opgave 16.3.** Bewijs.

Voor  $n = 2$  is een exacte formule bekend, maar zelfs voor  $n = 3$  wacht de wereld nog steeds op een algemene oplossing.

**Stelling 16.4.**

Het Frobeniusgetal van twee getallen  $a$  en  $b$  is gelijk aan  $ab - a - b$ .

**Opgave 16.5.** Bewijs dat  $g(a, b) = ab - a - b$  als  $\text{ggd}(a, b) = 1$ .

Noteer voor een willekeurig getal  $n$ ,  $n = ax + by$  met  $a$  en  $b$  niet noodzakelijk positief.

- A. Toon aan dat we, voor voldoende grote waarden van  $n$ , positieve  $x$  en  $y$  kunnen kiezen.

Er bestaat dus een maximum.

- B. Toon aan dat  $g(a, b) < ab$ .
- C. Toon aan dat  $g(a, b) < (a - 1)(b - 1)$ .
- D. Toon aan dat  $(a - 1)(b - 1) - 1$  niet kan geschreven worden als  $ax + by$  met  $x, y \geq 0$ .



**Stelling 16.6.**

Als  $\text{ggd}(a, b) = 1$ , dan kunnen precies  $\frac{1}{2}(g(a, b) + 1)$  natuurlijke getallen niet worden geschreven als lineaire combinatie met positieve coëfficiënten.

**Opgave 16.7.** Bewijs.

H

## 16.2 Perfecte en bevriende getallen

**Definitie 16.8.** Perfect getal

Een *perfect getal* of *volmaakt getal* is een natuurlijk getal dat gelijk is aan de som van zijn positieve delers, zichzelf niet inbegrepen. In symbolen:  $\sigma(n) = 2n$ .

Dit begrip was al bekend aan de oude grieken. Ze identificeerden de eerste perfecte getallen: 6, 28, 496 en 8182. Enkele enthousiaste middeleeuwers merkten op dat ook

33550336, 8589869056 en 137438691328

perfect zijn. De zoektocht naar perfecte getallen zet zich vandaag de dag nog steeds voort. Twee verwante begrippen dringen zich op:

**Definitie 16.9.** Overvloedig en gebrekkig

We noemen een natuurlijk getal  $n \in \mathbb{N}^+$  overvloedig als  $\sigma(n) > 2n$  en gebrekkig als  $\sigma(n) < 2n$ .

**Opgave 16.10.** Bestaan er perfecte volkomen kwadraten?

H

### 16.2.1 De overvloedigheidsindex

De mate van overvloedigheid vatten we samen in de verhouding  $\frac{\sigma(n)}{n}$ :

**Definitie 16.11.** Overvloedigheidsindex

De overvloedigheidsindex van  $n$  is  $I(n) = \frac{\sigma(n)}{n}$ .

De perfecte getallen zijn dus juist die met overvloedigheidsindex 2.

Als  $n = \prod p_k^{a_k}$  hebben we

$$I(n) = \frac{\sigma(n)}{n} = \prod \frac{p^{a_k+1} - 1}{p^{a_k}(p - 1)} = \prod \frac{p - p^{-a_k}}{p - 1}.$$

Merk op dat alle factoren in het product strikt groter dan 1 zijn. Hoe groter  $a_k$ , hoe groter de factor. Het toevoegen van priemfactoren zal de overvloedigheidsindex dus strikt groter maken:

**Stelling 16.12.**

Als  $a \mid b$  en  $a \neq b$  is  $I(a) < I(b)$ .

**Opgave 16.13.** Bewijs dat 6 het enige perfecte getal is dat deelbaar is door 6.

**16.2.2 Een eerste karakterisatie****Stelling 16.14.** Stelling van Euclides-Euler

De even perfecte getallen zijn de getallen van de vorm  $2^k(2^{k+1} - 1)$  met  $2^{k+1} - 1$  een priemgetal.

**Opgave 16.15.** Bewijs als oefening.

H

Schrijf  $n = 2^k m$  met  $m$  oneven.

A. Toon aan dat  $2^{k+1} - 1 \mid m$

Stel  $x = \frac{m}{2^{k+1}-1}$ .

B. Toon aan dat  $\sigma(m) = m + x$ .

C. Besluit dat  $m$  priem is en dat  $m = 2^{k+1} - 1$ .

D. Toon tot slot aan dat omgekeerd ook elk getal van de vorm  $2^k(2^{k+1} - 1)$  met  $2^{k+1} - 1$  priem, perfect is.

Het bepalen van even perfecte getallen is dus gereduceerd tot het vinden van Mersennepriemgetallen. Hoe zit het met oneven perfecte getallen? Dat is heel wat lastiger. Nog geen enkel oneven perfect getal is gekend. Het is zelfs niet eens geweten of er wel oneven perfecte getallen bestaan. Wel is men er in geslaagd heel wat voorwaarden op te leggen aan dewelke een oneven perfect getal zou moeten voldoen.

**Stelling 16.16.** Stelling van Frenicle-Euler

Een oneven perfect getal  $n$  is van de vorm  $p^k m^2$  met  $p$  een priemgetal,  $p \nmid m$  en  $p \equiv k \equiv 1 \pmod{4}$ .

In het bijzonder leren we hieruit dat  $n \equiv 1 \pmod{4}$ .

**Opgave 16.17.** Bewijs.

H

Zij  $n = \prod p_k^{a_k}$  perfect en oneven.

A. Bewijs dat er een unieke  $k$  is waarvoor  $\sigma(p_k^{a_k})$  even is.

Stel zonder verlies van algemeenheid  $k = 1$ . (We gaan er hier niet van uit dat  $p_1$  de kleinste priemdelers is, we hernoemen gewoon.)

B. Toon aan dat  $p_1 \equiv 1 \pmod{4}$ .

C. Toon aan dat voor  $k > 1$ ,  $a_k$  even is.

D. Bewijs tenslotte dat  $a_1 \equiv 1 \pmod{4}$ .

**Definitie 16.18.** Euler-priemgetal

Zij  $n = p^k m^2$  een oneven perfect getal. We noemen  $p$  het *Euler-priemgetal* van  $n$ .

Merk op dat  $p$  uniek bepaald is omdat  $k$  oneven is.

**Opgave 16.19.** Kan een oneven perfect getal deelbaar zijn door 105? ✿ H

**Opgave 16.20.** Kan een oneven perfect getal deelbaar zijn door 825? ✿ H

**Opgave 16.21.** Kan een oneven perfect getal deelbaar zijn door  $5313 = 3 \cdot 7 \cdot 11 \cdot 23$ ? ✿ H

### 16.2.3 Enkele congruenties

**Lemma 16.22.**

Een perfect getal is niet congruent met 2 modulo 3.

**Opgave 16.23.** Bewijs als oefening. H

**Stelling 16.24.** Stelling van Touchard

Een oneven perfect getal is congruent met 1 modulo 12 of met 9 modulo 36.

*Bewijs.*

Zij  $n$  oneven en perfect. Wegens Frenicle-Euler is  $n \equiv 1 \pmod{4}$  en wegens het vorige lemma is  $n \not\equiv 2 \pmod{3}$ . Als  $n \equiv 1 \pmod{3}$  is wegens de Chinese reststelling  $n \equiv 1 \pmod{12}$ . Als  $n \equiv 0 \pmod{3}$  is (opnieuw wegens Frenicle-Euler)  $9 \mid n$ , en dus wegens CRS  $n \equiv 9 \pmod{36}$ .  $\square$

**Stelling 16.25.**

Een oneven perfect getal is congruent met 1 modulo 12, 117 modulo 468 of 81 modulo 324.

**Opgave 16.26.** Bewijs. H

## 16.3 Het probleem van Josephus

### 16.4 Magische vierkanten

Al meer dan 2,5 millennium zijn sommige mensen gek genoeg om gefascineerd te zijn door verrassende getallenpatronen. Veruit het meest fascinerende type objecten zijn zonder twijfel de zogeheten magische vierkanten: getallen die op zo'n manier worden gerangschikt in een vierkant dat bepaalde sommen steeds dezelfde uitkomst opleveren. Onderstaand magisch vierkant, *Melencolica I* genaamd, werd opgesteld door Albrecht Dürer in, jawel, 1514:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Reken maar na: de som van de getallen op elke rij is 34. Hetzelfde geldt voor de kolommen en diagonalen. Ook de vier getallen op de hoeken of de vier getallen in het midden sommeren tot 34. Of de 2 en 3 bovenaan leveren samen met de 14 en 15 onderaan 34 op, en evenzo is  $5 + 9 + 8 + 12 = 34$ . Iemand met wat gevoel voor rotatie-symmetrie merkt misschien ook op dat  $3 + 9 + 14 + 8 = 34$  en dat  $2 + 5 + 15 + 12 = 34$ . Om nog te zwijgen van  $3 + 5 + 12 + 14$  en  $9 + 15 + 2 + 8 \dots$  Gek, niet? Wat dit magisch vierkant extra elegant maakt is dat de voorkomende getallen precies 1 tot en met 16 zijn.

**Definitie 16.27.** Magisch Vierkant

Een *magisch vierkant van orde*  $n \in \mathbb{N}^+$  is een  $n \times n$  matrix met gehele getallen waarvoor de som van de getallen op de rijen en kolommen dezelfde is.

Soms (en dat is wat wij ook vaak zullen doen) stelt men de eis dat de voorkomende getallen precies  $1, \dots, n^2$  of  $0, \dots, n^2 - 1$  zijn, of eist men dat de diagonalen ook sommeren tot hetzelfde getal. Zoals je ziet stellen we dus niet al te veel eisen in onze definitie van een magisch vierkant, althans niet zo veel als wat we terugvinden in Melencolica I.

**Definitie 16.28.** Magische constante

De som van de getallen op een rij (of kolom) in een magisch vierkant noemen we de *magische constante* van het vierkant.

Er roepen zich meteen enkele vragen op: kunnen we voor elke  $n \in \mathbb{N}^+$  de getallen  $1, \dots, n^2$  in een magisch vierkant van orde  $n$  rangschikken? Welke getallen kunnen optreden als magische constante? Hoeveel magische vierkanten zijn er van orde  $n$  met getallen  $1, \dots, n^2$ ?

**Opgave 16.29.** Bewijs dat de som van de getallen in een  $n \times n$  magisch vierkant steeds deelbaar is door  $n$ .

**Opgave 16.30.** Bewijs dat de magische constante van een magisch vierkant met getallen  $1, \dots, n^2$  enkel  $\frac{n^3+n}{2}$  kan zijn.

### 16.4.1 De Latijnse strategie

We bekijken nog een voorbeeld van een magisch vierkant geconstrueerd door Ramanujan:

22	12	18	87
88	17	9	25
10	24	89	16
19	86	23	11

Leuk om hierbij op te merken is dat Ramanujan's geboortedatum precies 22/12/1887 is. Wat valt er op? De getallen lijken in groepjes van 4 te horen, op basis van hun grootte. We duiden de verschillende groepen even aan met kleur:<sup>28</sup>

<sup>28</sup>Er wordt nagedacht over een kleurenblind-vriendelijker alternatief.

$$\begin{array}{cccc}
22 & 12 & 18 & 87 \\
88 & 17 & 9 & 25 \\
10 & 24 & 89 & 16 \\
19 & 86 & 23 & 11
\end{array}$$

Merk op dat in elke kolom, elke rij en elke diagonaal precies één getal van iedere kleur staat. Iets preciezer, we kunnen het magisch vierkant als volgt schrijven als een som van matrices:

$$\begin{pmatrix} 22 & 12 & 18 & 87 \\ 88 & 17 & 9 & 25 \\ 10 & 24 & 89 & 16 \\ 19 & 86 & 23 & 11 \end{pmatrix} = \begin{pmatrix} 22 & 9 & 16 & 86 \\ 86 & 16 & 9 & 22 \\ 9 & 22 & 86 & 16 \\ 16 & 86 & 22 & 9 \end{pmatrix} + \begin{pmatrix} 0 & 3 & 2 & 1 \\ 2 & 1 & 0 & 3 \\ 1 & 2 & 3 & 0 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

en we zien dat in de eerste matrix in elke rij en kolom elk van de vier getallen 9, 16, 22, 86 één keer voorkomt. In de tweede matrix bevat elke rij en kolom precies één van de getallen 0, 1, 2, 3.

**Opgave 16.31.** Probeer in te zien hoe we hieruit kunnen besluiten dat de som van de twee matrices een magisch vierkant oplevert.

Merk verder op dat indien twee posities links gelijke getallen bevatten, de overeenkomstige posities rechts nooit ook gelijke getallen bevatten, en vice versa.

**Opgave 16.32.** Probeer in te zien waarom dit, samen met het feit dat de getallen 9, 16, 22, 86 ‘ver genoeg’ uit elkaar liggen, maakt dat het bekomen magische vierkant geen twee dezelfde getallen bevat.

**Opgave 16.33.** Gebruik dit inzicht om een magisch vierkant te maken met jouw geboortedatum in plaats van die van Ramanujan. (In het ongelukkige geval dat het volgnummer van je geboortedag en -maand gelijk zijn of dat het om een andere reden niet lijkt te lukken, neem dan een andere datum of wat dan ook.)

Ter illustratie eentje van mijzelf:

$$\begin{pmatrix} 7 & 12 & 19 & 95 \\ 94 & 20 & 11 & 8 \\ 14 & 9 & 93 & 17 \\ 18 & 92 & 10 & 13 \end{pmatrix} = \begin{pmatrix} 7 & 11 & 17 & 92 \\ 92 & 17 & 11 & 7 \\ 11 & 7 & 92 & 17 \\ 17 & 92 & 7 & 11 \end{pmatrix} + \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

Merk op dat er wat moest worden gesleuteld aan de rechtse matrix (omdat 7 en 12 te dicht bij elkaar liggen), maar het principe blijft hetzelfde. Het soort matrix dat de getallen 0, 1, 2, 3 bevat noemen we een Latijns vierkant:

**Definitie 16.34.** Latijns vierkant

Een latijns vierkant van orde  $n \in \mathbb{N}^+$  is een  $n \times n$  rooster met  $n$  verschillende symbolen zo dat elke rij en elke kolom elk symbool precies één keer bevat.

Als symbolen gebruiken we doorgaans de getallen  $0, \dots, n-1$  of  $1, \dots, n$ , waarbij de voorkeur soms gaat naar  $0, \dots, n-1$ . Met deze definitie kunnen we bovenstaande observaties neerschrijven:

**Stelling 16.35.**

Zij  $A = (a_{rk})$  en  $B = (b_{rk})$   $n \times n$  Latijnse vierkanten met symbolen  $0, \dots, n-1$ . Stel dat  $a_{r_1k_1} = a_{r_2k_2} \implies b_{r_1k_1} \neq b_{r_2k_2}$ , m.a.w., gelijke getallen in  $A$  geven op de overeenkomstige posities in  $B$  nooit ook gelijke getallen. Dan is  $nA + B$  een magisch vierkant met getallen  $0, \dots, n^2 - 1$ .

Een voorbeeld is het volgende 10e-eeuwse magisch vierkant, Chautisa Yantra genaamd, gevonden in een Indische Parshvanath Jain tempel:

$$\begin{pmatrix} 7 & 12 & 1 & 14 \\ 2 & 13 & 8 & 11 \\ 16 & 3 & 10 & 5 \\ 9 & 6 & 15 & 4 \end{pmatrix} = 4 \cdot \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{pmatrix} + \begin{pmatrix} 3 & 4 & 1 & 2 \\ 2 & 1 & 4 & 3 \\ 4 & 3 & 2 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Merk wel op dat het rechtse Latijns vierkant de getallen 1, 2, 3, 4 en niet 0, 1, 2, 3 bevat. Dit zorgt er dan ook voor dat het bekomen magisch vierkant de getallen  $1, \dots, 4^2$  en niet  $0, \dots, 4^2 - 1$  bevat, maar het optellen van een vast getal op elke positie in een magisch vierkant verandert uiteraard niets aan het al dan niet magisch zijn ervan. Hetzelfde geldt duidelijkerwijs voor Latijnse vierkanten.

**Definitie 16.36.**

Twee  $n \times n$  Latijnse vierkanten  $A = (a_{rk})$  en  $B = (b_{rk})$  noemen we complementair indien  $a_{r_1k_1} = a_{r_2k_2}$  en  $b_{r_1k_1} = b_{r_2k_2}$  impliceert dat  $r_1 = r_2$  en  $k_1 = k_2$ .

Om met voorgaande strategie magische vierkanten te construeren volstaat het dus complementaire Latijnse vierkanten te vinden. We bekijken nog een inspirerend voorbeeld:

$$\begin{pmatrix} 16 & 23 & 0 & 7 & 14 \\ 22 & 4 & 6 & 13 & 15 \\ 3 & 5 & 12 & 19 & 21 \\ 9 & 11 & 18 & 20 & 2 \\ 10 & 17 & 24 & 1 & 8 \end{pmatrix} = 5 \cdot \begin{pmatrix} 0 & 4 & 3 & 2 & 1 \\ 1 & 0 & 4 & 3 & 2 \\ 2 & 1 & 0 & 4 & 3 \\ 3 & 2 & 1 & 0 & 4 \\ 4 & 3 & 2 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 3 & 1 & 4 & 2 \\ 1 & 4 & 2 & 0 & 3 \\ 2 & 0 & 3 & 1 & 4 \\ 3 & 1 & 4 & 2 & 0 \\ 4 & 2 & 0 & 3 & 1 \end{pmatrix}$$

Het patroon in het eerste Latijns vierkant is wel duidelijk: de cijfers liggen als het ware op (dalende) rechten die bovenaan doorlopen wanneer ze onderaan uit het vierkant verdwijnen. Dit is ook wat in het tweede vierkant aan de hand is, alleen lopen de rechten hier dubbel zo stijl omlaag. Indien we nu beide Latijnse vierkanten op elkaar zouden leggen, lijkt het alsof elke rechte in het linkse vierkant op precies één positie in de matrix snijdt met een rechte in het rechtse vierkant. Om dit vlot te kunnen inzien proberen we in formules te beschrijven wat de elementen van de Latijnse vierkanten precies zijn.

**Opgave 16.37.** Probeer in te zien waarom in het eerste Latijns vierkant ( $A$ ) geldt dat  $a_{rk} = (r - k) \bmod 5$  en in het tweede ( $B$ )  $b_{rk} = (r - 2k) \bmod 5$  (als we de rijen en kolommen beginnen nummeren vanaf 0).

In feite maakt het niet zo veel uit of deze formules nu overeenkomen met het meetkundige patroon dat we zien. Wat vooral belangrijk is, is of deze formules Latijnse vierkanten opleveren, en of ze complementair zijn.

**Opgave 16.38.** Ga na dat dit inderdaad het geval is.

We bekijken dit nu iets algemener, waarbij we toelaten dat de matricelementen, meetkundig gezien, rechten met een willekeurige richtingscoëfficiënt vormen:

**Stelling 16.39.**

Zij  $n \in \mathbb{N}^+$  en  $p_1, q_1, m_1, p_2, q_2, m_2 \in \mathbb{Z}$ . Definieer  $n \times n$  matrices  $A$  en  $B$  door

$$a_{rk} = (p_1r + q_1k + m_1) \bmod n \text{ en } b_{rk} = (p_2r + q_2k + m_2) \bmod n.$$

Dan geldt:

1.  $A$  is Latijns als en slechts als  $\text{ggd}(p_1q_1, n) = 1$ , en analoog voor  $B$ .
2. Als  $A$  en  $B$  Latijns zijn geldt:  $A$  en  $B$  zijn complementair als en slechts als

$$\text{ggd}(p_1q_2 - p_2q_1, n) = 1.$$

**Opgave 16.40.** Bewijs als oefening.

In feite geldt de implicatie “ $\text{ggd}(p_1q_2 - p_2q_1, n) = 1 \Rightarrow A, B$  complementair” ook indien  $A$  en  $B$  niet beide Latijns zijn.

Merk op dat de constanten  $m_1$  en  $m_2$  uit de vorige stelling er niet toe doen. De vraag is nu voor welke waarden van  $n$  er zo'n getallen  $p_1, q_1, p_2, q_2$  te vinden zijn. Het antwoord is eenvoudig: als  $n$  oneven is kunnen we bijvoorbeeld  $(p_1, q_1) = (1, 1)$  en  $(p_2, q_2) = (1, 2)$  nemen. Indien  $n$  even is, impliceert  $\text{ggd}(p_1q_1p_2q_2, n) = 1$  dat  $p_1, q_1, p_2, q_2$  oneven zijn, zodat  $\text{ggd}(p_1q_2 - p_2q_1, n) = 1$  onmogelijk is.

**Gevolg 16.41.**

Zij  $n \in \mathbb{N}^+$  oneven. Dan bestaat een magisch vierkant van orde  $n$  met getallen  $1, \dots, n^2$ .

**Opgave 16.42.** Bepaal een expliciete uitdrukking voor de elementen van het aldus geconstrueerde magisch vierkant met parameters  $p_1 = q_1 = p_2 = 1, q_2 = 2, m_1 = m_2 = 0$ . A

Deze strategie faalt dus helemaal om magische vierkanten te construeren van even orde met getallen  $1, \dots, n^2$ . We bekijken daarom later nog enkele andere methoden.

### 16.4.1.1 Diagonalen

Iets dat we tot nu toe onder de mat hebben geveegd is de voorwaarde dat de diagonalen ook sommeren tot de magische constante. Je zou je kunnen afvragen of deze Latijnse strategie daar toevallig rekening mee houdt. Vanaf nu veronderstellen we dat  $n$  oneven is, omdat de Latijnse strategie anders toch geen zin heeft.

**Opgave 16.43.** Probeer in te zien waarom het voldoende is dat de getallen op de diagonalen van de complementaire Latijnse vierkanten telkens alle  $n$  verschillend zijn.

**Stelling 16.44.**

Stel dat  $A$  een  $n \times n$  Latijns vierkant is met  $a_{rk} = (pr + qk + m) \bmod n$ . Dan geldt:

1. De elementen op de nevensdiagonaal zijn verschillend a.s.a.  $\text{ggd}(p - q, n) = 1$ .
2. De elementen op de hoofddiagonaal zijn verschillend a.s.a.  $\text{ggd}(p + q, n) = 1$ .

**Opgave 16.45.** Bewijs.

**Opgave 16.46.** Stel dat  $n$  niet deelbaar is door 3. Bepaal twee complementaire Latijnse vierkanten waarvoor de diagonaalelementen telkens alle  $n$  verschillend zijn. Wat gaat er mis indien  $3 \mid n$ ? A

Gelukkig is de voldoende voorwaarde uit de vorige stelling een iets te sterke eis, en zijn de diagonalen ook onder zwakkere voorwaarden in orde:

**Stelling 16.47.**

Zij  $A$  en  $B$  complementaire Latijnse  $n \times n$  vierkanten met getallen  $0, \dots, n - 1$ . Dan is  $nA + B$  magisch met goede diagonaalsommen zodra elk van de vier diagonalen ofwel

1. de getallen  $0, \dots, n - 1$  bevat
2. enkel het getal  $\frac{n-1}{2}$  bevat.

**Opgave 16.48.** Bewijs. H

Het is een eenvoudige controle om na te gaan dat aan de voorwaarden voldaan is indien bijvoorbeeld  $a_{rk} = (r - k + \frac{n-1}{2}) \bmod n$ . Indien  $3 \nmid n$  kunnen we zoals eerder opgemerkt  $b_{rk} = (r + 2k) \bmod n$  of  $c_{rk} = (2r + k) \bmod n$  nemen, en deze drie Latijnse vierkanten zijn dan twee aan twee complementair. Om het geval  $3 \mid n$  te behandelen bekijken we meteen algemener waar de parameters aan moeten voldoen opdat de diagonaalsommen goed zouden uitkomen. De voorwaarde dat het Latijns vierkant  $a_{rk} = (pk + qr + m) \bmod n$  de juiste diagonaalsommen zou hebben luidt:

$$\sum_{k=0}^{n-1} ((p + q)k + m) \bmod n = \sum_{k=0}^{n-1} (pk + q(n - 1 - k) + m) \bmod n = \frac{n^2 - n}{2}.$$

Het loont de moeite om meer algemeen sommen van de vorm  $\sum_{k=0}^{n-1} (ak + b) \bmod n$  te bestuderen.

**Opgave 16.49.** Zij  $n \in \mathbb{N}^+$  (niet noodzakelijk oneven) en  $a, b \in \mathbb{Z}$  met  $\text{ggd}(a, n) = 1$ . Toon aan dat  $\sum_{k=0}^{n-1} (ak + b) \bmod n = \frac{n^2 - n}{2}$ . H

Iets algemener geldt:



**Stelling 16.50.**

Zij  $n \in \mathbb{N}^+$  (niet noodzakelijk oneven) en  $a, b \in \mathbb{Z}$  met  $\text{ggd}(a, n) = d$ . Dan is

$$\sum_{k=0}^{n-1} (ak + b) \bmod n = \frac{n^2 - nd}{2} + n \cdot (b \bmod d).$$

**Opgave 16.51.** Toon aan.

H

In het geval  $\text{ggd}(p + q, n) = 3$  geldt dus

$$\sum_{k=0}^{n-1} ((p + q)k + m) \bmod n = \frac{n^2 - 3n}{2} + n \cdot (m \bmod 3).$$

Opdat dit gelijk zou zijn aan  $\frac{n^2 - n}{2}$  moet  $n \cdot (m \bmod 3) = n$ , of dus  $m \equiv 1 \pmod{3}$ .  
Analoog is, indien  $\text{ggd}(p - q, n) = 3$ ,

$$\sum_{k=0}^{n-1} (pk + q(n - 1 - k) + m) \bmod n = \frac{n^2 - 3n}{2} + n \cdot (m \bmod 3)$$

zodat dit gelijk is aan  $\frac{n^2 - n}{2}$  als en slechts als  $m \equiv 1 \pmod{3}$ .

We keren nu terug naar de situatie waarbij we gepaste complementaire Latijnse vierkanten probeerden construeren. Een eerste vierkant dat rekening houdt met de diagonalen is  $a_{rk} = (r + k + \frac{n+1}{2}) \bmod n$ , en een hieraan complementair vierkant is bijvoorbeeld  $b_{rk} = (r + 2k + m) \bmod n$ . Indien  $3 \nmid n$  maakt de waarde van  $m$  niets uit voor de diagonalen; die zijn dan immers altijd in orde. Indien  $3 \mid n$  weten we uit bovenstaande berekeningen dat we  $m \equiv 1 \pmod{3}$  moeten kiezen. Een mogelijkheid is uiteraard  $m = 1$ . We bekijken even de resultaten voor  $n = 3, 5, 7, 9$ :

### 16.4.1.2 De Siamese methode

Het linkse Latijnse vierkant is zo geconstrueerd dat op de hoofddiagonaal telkens alle  $n$  verschillende getallen staan, en op de nevendiaagonaal steeds het getal  $\frac{n-1}{2}$ . Het rechtse vierkant is zo geconstrueerd dat op de nevendiaagonaal  $n$  verschillende getallen staan (daar  $\text{ggd}(1-2, n) = 1$ ) en op de hoofddiagonaal ook indien  $\text{ggd}(1+2, n) = 1$ . Indien  $3 \mid n$  staan op de hoofddiagonaal van het rechtse vierkant inderdaad elk getal  $\equiv 1 \pmod{3}$  precies één keer, zoals we ook beredeneerd hebben in het bewijs dat de diagonaalsom goed uitkomt (vooral in het geval  $n = 9$  is dit goed te zien):

$$\begin{pmatrix} 7 & 0 & 5 \\ 2 & 4 & 6 \\ 3 & 8 & 1 \end{pmatrix} = 3 \cdot \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 16 & 23 & 0 & 7 & 14 \\ 22 & 4 & 6 & 13 & 15 \\ 3 & 5 & 12 & 19 & 21 \\ 9 & 11 & 18 & 20 & 2 \\ 10 & 17 & 24 & 1 & 8 \end{pmatrix} = 5 \cdot \begin{pmatrix} 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 0 & 2 & 4 \\ 2 & 4 & 1 & 3 & 0 \\ 3 & 0 & 2 & 4 & 1 \\ 4 & 1 & 3 & 0 & 2 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 29 & 38 & 47 & 0 & 9 & 18 & 27 \\ 37 & 46 & 6 & 8 & 17 & 26 & 28 \\ 45 & 5 & 7 & 16 & 25 & 34 & 36 \\ 4 & 13 & 15 & 24 & 33 & 35 & 44 \\ 12 & 14 & 23 & 32 & 41 & 43 & 3 \\ 20 & 22 & 31 & 40 & 42 & 2 & 11 \\ 21 & 30 & 39 & 48 & 1 & 10 & 19 \end{pmatrix} = 7 \cdot \begin{pmatrix} 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 5 & 0 & 2 & 4 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 & 0 \\ 3 & 5 & 0 & 2 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & 5 & 0 & 2 \\ 5 & 0 & 2 & 4 & 6 & 1 & 3 \\ 6 & 1 & 3 & 5 & 0 & 2 & 4 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 46 & 57 & 68 & 79 & 0 & 11 & 22 & 33 & 44 \\ 56 & 67 & 78 & 8 & 10 & 21 & 32 & 43 & 45 \\ 66 & 77 & 7 & 9 & 20 & 31 & 42 & 53 & 55 \\ 76 & 6 & 17 & 19 & 30 & 41 & 52 & 54 & 65 \\ 5 & 16 & 18 & 29 & 40 & 51 & 62 & 64 & 75 \\ 15 & 26 & 28 & 39 & 50 & 61 & 63 & 74 & 4 \\ 25 & 27 & 38 & 49 & 60 & 71 & 73 & 3 & 14 \\ 35 & 37 & 48 & 59 & 70 & 72 & 2 & 13 & 24 \\ 36 & 47 & 58 & 69 & 80 & 1 & 12 & 23 & 34 \end{pmatrix} = 9 \cdot \begin{pmatrix} 5 & 6 & 7 & 8 & 0 & 1 & 2 & 3 & 4 \\ 6 & 7 & 8 & 0 & 1 & 2 & 3 & 4 & 5 \\ 7 & 8 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 8 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 0 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 0 & 1 \\ 3 & 4 & 5 & 6 & 7 & 8 & 0 & 1 & 2 \\ 4 & 5 & 6 & 7 & 8 & 0 & 1 & 2 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 5 & 7 & 0 & 2 & 4 & 6 & 8 \\ 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 0 \\ 3 & 5 & 7 & 0 & 2 & 4 & 6 & 8 & 1 \\ 4 & 6 & 8 & 1 & 3 & 5 & 7 & 0 & 2 \\ 5 & 7 & 0 & 2 & 4 & 6 & 8 & 1 & 3 \\ 6 & 8 & 1 & 3 & 5 & 7 & 0 & 2 & 4 \\ 7 & 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 \\ 8 & 1 & 3 & 5 & 7 & 0 & 2 & 4 & 6 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 \end{pmatrix}$$

## 16.4.2 Conway's LUX-methode

## 16.4.3 Kroneckerproduct

## 16.5 Lineaire recursies

### 16.5.1 Periodiciteit

## 16.6 De rij van Fibonacci

### 16.6.1 De Pisanoperiode

**Stelling 16.52.**

Zij  $p$  een priemgetal waarvoor 5 een kwadraatrest is. Dan is de pisanoperiode modulo  $p$  een deler van  $p - 1$ .

Men kan het volgende aantonen:

**Stelling 16.53.**

Zij  $p$  een priemgetal waarvoor 5 geen kwadraatrest is. Dan is de pisanoperiode modulo  $p$  een deler van  $p^2 - 1$ .

**16.6.2 Deelbaarheidsrijen****Definitie 16.54.** Deelbaarheidsrij

Een gehele rij  $(a_n)$  noemen we een *deelbaarheidsrij* indien voor alle  $m, n > 0$  geldt dat als  $m \mid n$ , dan  $a_m \mid a_n$ .

**16.6.3 Sterke deelbaarheidsrijen****Stelling 16.55.**

Zij  $(a_n)$  een gehele rij met  $a_0 = 0$  en  $a_n \equiv a_{n-m} \pmod{a_m}$  voor alle  $n > m > 0$ . Dan is  $\text{ggd}(a_m, a_n) = a_{\text{ggd}(m,n)}$  voor alle  $m, n > 0$ .

**Definitie 16.56.** Sterke deelbaarheidsrij


Een gehele rij  $(a_n)$  noemen we een *sterke deelbaarheidsrij* indien  $\text{ggd}(a_m, a_n) = a_{\text{ggd}(m,n)}$  voor alle  $m, n > 0$ .






Merk op dat elke sterke deelbaarheidsrij automatisch een deelbaarheidsrij is.

**Opgaven hoofdstuk 16**

**Opgave 16.57.** We zouden volledig analoog ook het Frobeniusgetal van een oneindige verzameling kunnen definiëren, op voorwaarde dat de ggd van al die getallen 1 is. Waarom niet? Toon aan dat als  $S$  een oneindige verzameling is met  $\text{ggd}(S) = 1$ , er een eindige deelverzameling van  $S$  bestaat met ggd 1.

**Opgave 16.58.** (IMC 2014 dag 1 vraag 4) Zij  $n > 6$  een perfect getal en  $p_1^{e_1} \cdots p_k^{e_k}$  zijn priemontbinding met  $p_1 < \dots < p_k$ . Bewijs dat  $e_1$  even is.

**Opgave 16.59.** (Sint-Petersburg 2014) We noemen een natuurlijk getal  $n$  bijna perfect als de som van zijn positieve gehele delers, zichzelf niet inbegrepen, gelijk is aan  $n - 1$ . Vind alle bijna perfecte getallen  $n$  met de eigenschap dat ook  $n^k$  bijna perfect is, voor een zekere gehele  $k > 1$ . 

- Opgave 16.60.** Zij  $n$  een even perfect getal. Bewijs dat het product van zijn delers een macht van  $n$  is. 
- Opgave 16.61.** Als  $n \in \mathbb{N}^+$  en  $\sigma(n) = 2n + 1$ , bewijs dat  $n$  een oneven kwadraat is. 
- Opgave 16.62.** Zij  $n \in \mathbb{N}^+$  en  $a, b \in \mathbb{Z}$ . Bepaal  $\sum_{k=0}^{n-1} \left\lfloor \frac{ak+b}{n} \right\rfloor$ . H A
- Opgave 16.63.** Toon aan dat een lineaire recursie van recursiediepte  $k$  na een tijdje periodiek wordt modulo  $n \in \mathbb{N}$  met periode hoogstens  $n^k$ .
- Opgave 16.64.** Zij  $F_n$  het  $n$ de Fibonaccigetal. Bewijs dat  $F_n^2 - 28$  nooit priem is zodra  $n > 5$ . 
- Opgave 16.65.** (LIMO 2012) Vind alle koppels  $(m, n)$  van natuurlijke getallen waarvoor  $F_n = 2^{2^m} + 1$ .  

**17.1** Algoritme van Euclides**17.2** Modulaire machtsverheffing**17.3** Factorisatie**17.3.1** Dixon's algoritme**17.4** Priemgetallen**Stelling 17.1.**

Zij  $n \in \mathbb{N}$  en  $p = 2^n + 1$ . Als  $p \mid 3^{\frac{p-1}{2}} + 1$ , dan is  $p$  een priemgetal.

Merk op dat deze stelling slechts in één richting geldt. Het is zeker niet zo dat voor elk Fermatpriemgetal  $p$  geldt dat  $p \mid 3^{\frac{p-1}{2}} + 1$ , neem bijvoorbeeld  $p = 3$ .

**17.4.1** Lucas-Lehmer**Stelling 17.2.**

Definieer een rij  $(s_n)$  recursief d.m.v.  $s_0 = 4$  en  $s_{n+1} = s_n^2 - 2$ . Dan is  $2^p - 1$  een priemgetal als en slechts als  $s_{p-2} \equiv 0 \pmod{2^p - 1}$ .

**17.4.2** Miller-Rabin**17.5** RSA-encryptie**17.5.1** Diffie-Hellman protocol**17.6** Primitieve wortels**17.7** Sommen van kwadraten**17.8** Pellvergelijkingen**17.8.1** Chakravala methode

De volgende stelling hebben we te danken aan Lagrange:


**Stelling 17.3.**


De Chakravala methode geeft steeds na een eindig aantal stappen een gehele oplossing.

**Opgaven hoofdstuk 17**

# Opgaven deel I


Een hele reeks nog ongecategoriseerde en onbeoordeelde oefeningen. Ze staan niet noodzakelijk in volgorde van moeilijkheidsgraad: sommigen zijn heel eenvoudig, anderen zijn belachelijk (maar écht belachelijk) moeilijk.


**Opgave I.4.** Vind alle getallen van de vorm  $123456789123 \dots$  die volkomen kwadraten zijn. 


**Opgave I.5.** Zij  $a, m \in \mathbb{N}^+$ . Bewijs dat er oneindig veel  $n \in \mathbb{N}^+$  bestaan zo dat  $m \mid \tau(na^n + 1)$ . 


**Opgave I.6.** Zij  $(a_n)$  een rij natuurlijke getallen waarvoor  $\text{ggd}(a_n, a_m) = \text{ggd}(n, m)$  voor  $n \neq m$ .  
Bewijs dat  $a_n = n$  voor alle  $n$ . 

**Opgave I.7.** Bewijs dat  $n + 3$  en  $n^2 + 3$  niet tegelijk derdemachten kunnen zijn als  $n \in \mathbb{N}$ .


**Opgave I.8.** Bewijs dat  $n + 3$  en  $n^2 + 3n + 3$  niet tegelijk derdemachten kunnen zijn als  $n \in \mathbb{N}$ . 

**Opgave I.9.** Noteer met  $p_k$  het  $k$ -de priemgetal. Bewijs dat  $p_1 p_2 \cdots p_n + 1$  voor geen enkele  $n > 0$  een kwadraat is. 


**Opgave I.10.** Vind alle priemgetallen  $p, q$  en  $m \in \mathbb{N}$  met  $1 + 2^m p^2 = q^5$ . 


**Opgave I.11.** (USAMO 1998 vraag 5) Bewijs dat voor ieder natuurlijk getal  $n \geq 2$ , er een verzameling  $S$  van  $n$  gehele getallen bestaat zo dat  $(a - b)^2 \mid ab$  voor iedere verschillende  $a, b \in S$ .  H


**Opgave I.12.** (JWO 2009 finale vraag 2) Zoek het kleinste natuurlijk getal  $n$  zo dat  $2003 \cdot 2005 \cdot 2007 \cdot 2009 + n$  een volkomen kwadraat is.  H


**Opgave I.13.** (JWO 2013 finale vraag 1) Bepaal het natuurlijk getal  $n$  zodanig dat  H

$$\left(\frac{2013}{1} - 1\right) \cdot \left(\frac{2013}{3} - 1\right) \cdot \left(\frac{2013}{5} - 1\right) \cdots \left(\frac{2013}{1005} - 1\right) = 4^n.$$

**Opgave I.14.** Stel dat  $a \in \mathbb{N}^+$  zo dat  $2a + 1$  en  $3a + 1$  beide kwadraten zijn. Bewijs dat  $5a + 3$  niet priem is. 

**Opgave I.15.** Bewijs dat  $n!$  op precies één nul minder eindigt als  $3^{n!} - 1$ , voor  $n \geq 4$ . 

**Opgave I.16.** Zij  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  een functie die voor elke  $q \in \mathbb{N}^+$  periodiek is met periode (een deler van)  $q$ . Is  $f$  dan een veelterm? 

**Opgave I.17.** Noteer met  $p_n$  het  $n$ -de priemgetal. Vind alle  $n$  met  $p_n + p_{n+1} = 1 + p_{n+2}$ . 

**Opgave I.18.** Zij  $a, b, c, d \in \mathbb{R}$  met  $ad \neq bc$ . Bewijs dat er gehele  $x, y$  bestaan zo dat ✿

$$|(ax + by)(cx + dy)| \leq \frac{1}{2} |ad - bc|.$$

**Opgave I.19.** Bewijs dat  $512^3 + 675^3 + 720^3$  geen priemgetal is. ✿

**Opgave I.20.** (PEN A67) Zij  $A = \{a_1, \dots, a_n\}$  een deelverzameling van  $\mathbb{N}^+$ . Bewijs dat

$$\text{kgv}(A) = \prod_{k=1}^n \alpha_k^{(-1)^k}$$

waarbij

$$\alpha_k = \prod_{\substack{S \subseteq \mathbb{N}_{\leq n}^+ \\ |S|=k}} \text{ggd}\{a_l : l \in S\}.$$

**Opgave I.21.** (China TST 2014) Zij  $k \in \mathbb{N}^+$ . Bewijs dat er een  $n \in \mathbb{N}^+$  is zo dat  $k! + (2k)! + \dots + (nk)!$  een priemdelers groter dan  $k!$  heeft. ✿

**Opgave I.22.** Zij  $p > 2$  een priemgetal en  $rp + 1 \mid p^p - 1$ . Bewijs dat  $r$  even is. ✿

**Opgave I.23.** De getallen  $1, 2, \dots, 2013^2$  worden rij per rij in een  $2013 \times 2013$  rooster geschreven. Vervolgens kleurt men de getallen in de rijen en kolommen die een kwadraat bevatten. Hoeveel getallen worden niet gekleurd? ✿

**Opgave I.24.** Zij  $n \in \mathbb{N}$  oneven. Bepaal het aantal factoren 2 van  $\left\lfloor (1 + \sqrt{3})^n \right\rfloor$ . ✿ HA

**Opgave I.25.** Noem een priemgetal paars als het van de vorm  $|3^a - 2^b|$  is, en kleurrijk als het van de vorm  $|3^a \pm 2^b|$  is. ✿

A. Vind het kleinste niet-paarse priemgetal.

B. Bewijs dat er oneindig veel niet-kleurrijke priemgetallen bestaan.

**Opgave I.26.** Zij  $a, b$  verschillende reële getallen zo dat  $a^n - b^n \in \mathbb{Z}$  voor alle  $n \in \mathbb{N}^+$ . Zijn  $a$  en  $b$  dan noodzakelijk geheel? ✿ A

**Opgave I.27.** Bewijs dat voor geen enkele  $n \in \mathbb{N}$  er  $x, y \in \mathbb{N}$  bestaan waarvoor ✿

$$\sqrt{n} + \sqrt{n+1} < \sqrt{x} + \sqrt{y} < \sqrt{4n+2}.$$

**Opgave I.28.** Het getal  $2^{29}$  heeft precies 9 cijfers. Welk cijfer ontbreekt? ✿ HA

**Opgave I.29.** De functie  $f : \mathbb{N} \rightarrow \mathbb{Z}$  voldoet aan  $m + n \mid f(m) + f(n)$  voor alle  $m, n \in \mathbb{N}$ . Bewijs dat  $m - n \mid f(m) - f(n)$  voor alle  $m, n \in \mathbb{N}$ . ✿

**Opgave I.30.** Bepaal alle functies  $f : \mathbb{N} \rightarrow \mathbb{Z}$  die voldoen aan  $m + n \mid f(m) + f(n)$  voor alle  $m, n \in \mathbb{N}$ . ✿



**Opgave I.31.** Noteer met  $F_n$  het  $n$ -de Fibonaccigetal. Bewijs dat  $5^k \mid F_{5^k}$  voor  $k \in \mathbb{N}$ . ✿

**Opgave I.32.** Noteer  $T_n = \sum_{k=1}^n \frac{1}{k \cdot 2^k}$ . Bepaal alle priemgetallen  $p$  waarvoor ✿

$$\sum_{k=1}^{p+2} \frac{T_k}{k+1} \equiv 0 \pmod{p}.$$

**Opgave I.33.** Zij  $p$  een priemdelers van  $2^{2^n} + 1$ .

A. Bewijs dat  $p \equiv 1 \pmod{2^{n+1}}$ .

B. Bewijs dat  $p \equiv 1 \pmod{2^{n+2}}$ .

**Opgave I.34.** Wat is (als het bestaat) het grootste natuurlijk getal dat op slechts één manier kan worden geschreven als de som van vijf niet-nul kwadraten? (Permutatie van de kwadraten wordt niet meegerekend.) ✿ A

**Opgave I.35.** Bewijs dat er voor elke  $k \in \mathbb{N}$  drie opeenvolgende priemgetallen  $p < q < r$  bestaan met  $r - q > k$  en  $q - p > k$ . ✿

**Opgave I.36.** Bewijs dat de vergelijking  $2a^4 + 2a^2b^2 + b^4 = c^2$  geen gehele oplossingen heeft met  $a \neq 0$ . ✿

**Opgave I.37.** Vind alle  $n, k \in \mathbb{N}$  waarvoor  $(n-1)! + 1 = n^k$ . ✿

**Opgave I.38.** Zij  $a, b, c \in \mathbb{Z}$  met  $c \neq 0$  en  $\text{ggd}(a, b, c) = 1$ . Bewijs dat er een  $n \in \mathbb{N}$  bestaat met  $\text{ggd}(an + b, c) = 1$ . (Zonder gebruik te maken van de stelling van Dirichlet.) ✿

**Opgave I.39.** Zij  $p$  een oneven priemgetal. Bewijs dat ✿

$$\sum_{k=1}^p k^{2p-1} \equiv \frac{p(p+1)}{2} \pmod{p^2}.$$

**Opgave I.40.** Zij  $n > 1$  en  $a, b$  zo dat  $0 < a, b < n$ . Bewijs dat  $\text{ggd}\left(\binom{n}{a}, \binom{n}{b}\right) > 1$ . ✿

**Opgave I.41.** Als  $n \geq 1$ , bewijs dat ✿ H

$$\prod_{k=1}^n \left(4 - \frac{2}{k}\right)$$

een even natuurlijk getal is.

**Opgave I.42.** Bewijs dat  $2^{15} - 2^3$  een deler is van  $a^{15} - a^3$  voor alle  $a \in \mathbb{Z}$ . ✿ H

**Opgave I.43.** Wanneer is de som van drie opeenvolgende natuurlijke derdemachten terug een derdemacht? ✿ A

**Opgave I.44.** Bewijs dat voor  $n > 0$ , ✿ H

$$1 - \frac{1}{2^n} < \sum_{k=1}^n \frac{\varphi(k)}{k} \ln \frac{2^k}{2^k - 1} < 1.$$

**Opgave I.45.** Vind alle triples priemgetallen  $p, q, r$  waarvoor  $p(p + q) = r + 120$ . ✿ HA

**Opgave I.46.** Zij  $p > 2$  een priemgetal. Bewijs dat de congruentie  $x^2 + y^2 + z^2 \equiv 1 \pmod{p}$  ✿  
precies  $p^2 + \left(\frac{-1}{p}\right) \cdot p$  oplossingen heeft.

**Opgave I.47.** Vind alle  $x \in \mathbb{R}$  waarvoor  $8x^3 - 20$  en  $2x^5 - 2$  vokomen kwadraten zijn. ✿ HA

**Opgave I.48.** Bewijs dat de vergelijking  $x^3 = y^2 + 6$  geen gehele oplossingen heeft. ✿ H

**Opgave I.49.** Zij  $a, b \in \mathbb{Z}$  met  $\text{ggd}(a, b) = 1$ . Bewijs dat de verzameling  $\{ak + b : k \in \mathbb{N}\}$  een ✿  
deelverzameling  $\{c_1, \dots, c_n\}$  van paarsgewijs relatief priem getallen heeft voor elke  $n > 0$ . (Zonder gebruik te maken van de stelling van Dirichlet.)

**Opgave I.50.** Zij  $a \in \mathbb{N}^+$ . Bewijs dat de congruentie ✿

$$a^2 + \text{ggd}(a, b)^2 \equiv 0 \pmod{b \cdot \text{ggd}(a, b)}$$

een eindig en even aantal natuurlijke oplossingen voor  $b$  heeft.

**Opgave I.51.** Door de cijfers 2, 2, 3, 3, 4, 4, 5, 5, 6, 6, 7, 7, 8, 8, 9, 9 in twee groepen te delen en ✿  
ze in een bepaalde volgorde naast elkaar te plaatsen mag je twee getallen vormen. Kan je ervoor zorgen dat het ene getal het dubbele is van het andere, als je elk van de cijfers precies één keer gebruikt?

**Opgave I.52.** Zij  $n \geq 2$ . ✿ H

A. Bewijs dat er voor elke oneven  $a \in \mathbb{Z}$  unieke  $m \in \{0, \dots, 2^{n-2} - 1\}$  en  $k \in \{0, 1\}$  zijn met  $a \equiv (-1)^k \cdot 3^m \pmod{2^n}$ .

B. Bewijs dat het aantal kwadraten modulo  $2^n$  gelijk is aan  $\frac{1}{3}(2^{n-1} + 4)$  als  $n$  even is en  $\frac{1}{3}(2^{n-1} + 5)$  als  $n$  oneven is (voor  $n \geq 1$ ).

**Opgave I.53.** Als  $r$  en  $s$  gehele getallen zijn met  $11s = 13r$ , is  $r + s$  dan steeds deelbaar door ✿  
8?

**Opgave I.54.** Vind alle  $x, y, z \in \mathbb{N}^+$  waarvoor  $x^2 + y^2 + x + y + 1 = xyz$ . ✿

**Opgave I.55.** Bewijs dat  $3^n - 5 \cdot 2^n$  geen priemgetal is voor oneindig veel  $n \in \mathbb{N}$ . ✿ H

**Opgave I.56.** Vind alle priemgetallen  $p, q$  waarvoor zowel  $2p - 1$ ,  $2q - 1$  als  $2pq - 1$  kwadraten ✿  
zijn.

**Opgave I.57.** Als  $n$  een natuurlijk getal is met 60 delers en als  $7n$  80 delers heeft, hoeveel keer ✿  
is  $n$  dan deelbaar door 7?

**Opgave I.58.** Zij  $k, m, n > 0$  zo dat  $k^{m+n} = nm^n$ . Bewijs dat  $m = k$  en  $n = k^k$ . ✿

**Opgave I.59.** Bepaal de natuurlijke getallen  $x$  en  $y$  als  $x^3 - 5x + 10 = 2^y$ . ✿ A

**Opgave I.60.** Bewijs dat er oneindig veel natuurlijke getallen  $n$  zijn waarvoor  $\left\lfloor 2^n \cdot \sqrt{2} \right\rfloor$  geen ✿  
priemgetal is.

**Opgave I.61.** (China TST 2014) Bewijs dat voor gehele  $k, N > 0$ , ✿

$$\left( \frac{1}{N} \sum_{n=1}^N (\omega(n))^k \right)^{\frac{1}{k}} \leq k + \sum_{p^n \leq N} \frac{1}{p^n}$$

waarbij de som in het rechterlid loopt over alle priem machten kleiner of gelijk aan  $N$ .

**Opgave I.62.** Vind de kleinste  $n > 0$  zo dat  $79n + 1 = 2^a 3^b$  voor zekere  $a, b \in \mathbb{N}$ . ✿

**Opgave I.63.** Vind alle priemgetallen  $p, q$  waarvoor  $p^q + q^p$  een kwadraat is. ✿

**Opgave I.64.** Zij  $m$  en  $n$  gehele getallen met  $3m^2 + 3 = 4n^2 + n$ . Bewijs dat  $m - n$  een kwadraat is. ✿

**Opgave I.65.** Zij  $x, y \in \mathbb{Z}_0$  met  $\text{ggd}(x(x+1), y) = 1$ . Stel dat  $\text{ord}_y(x) = 3$ , wat is dan  $\text{ord}_y(x+1)$ ? ✿

**Opgave I.66.** Noteer met  $p(n)$  het product van de priemgetallen kleiner dan  $n$ . Bepaal alle  $n > 3$  waarvoor  $p(n) = 2n + 16$ . ✿

**Opgave I.67.** (USAMO 1999 vraag 3) Zij  $p > 2$  een priemgetal en  $a, b, c, d \in \mathbb{Z}$  niet deelbaar door  $p$  zo dat ✿ 🌐

$$\left\{ \frac{ra}{p} \right\} + \left\{ \frac{rb}{p} \right\} + \left\{ \frac{rc}{p} \right\} + \left\{ \frac{rd}{p} \right\} = 2$$

voor alle  $r \in \mathbb{Z}$  met  $p \nmid r$ . Bewijs dat tenminste twee van de getallen  $a + b, a + c, a + d, b + c, b + d, c + d$  deelbaar zijn door  $p$ .

**Opgave I.68.** Zij  $S$  de verzameling van rationale getallen van de vorm ✿ 🌐

$$\frac{(a_1^2 + a_1 - 1)(a_2^2 + a_2 - 1) \cdots (a_n^2 + a_n - 1)}{(b_1^2 + b_1 - 1)(b_2^2 + b_2 - 1) \cdots (b_n^2 + b_n - 1)}$$

met  $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in \mathbb{N}^+$ . Bewijs dat er oneindig veel priemgetallen in  $S$  zijn.

**Opgave I.69.** Zij  $x, y > 0$  gehele getallen met  $2xy \mid x^2 + y^2 - x$ . Bewijs dat  $x$  een kwadraat is. ✿

**Opgave I.70.** Zij  $m, n \in \mathbb{Z}_0$  met  $\text{ggd}(m, n) = 1$ . Zij  $a \in \mathbb{Z}$  met  $\text{ggd}(a, mn) = 1$ . Bewijs dat ✿ H

$$\text{ord}_{mn}(a) = \text{kgv } \text{ord}_m(a), \text{ord}_n(a).$$

Is de voorwaarde  $\text{ggd}(m, n) = 1$  noodzakelijk?

**Opgave I.71.** Vind het grootste natuurlijk getal  $n$  waarvoor  $\omega(n) + \varphi(n) = \pi(n) + 1$ . ✿ A

**Opgave I.72.** Zij  $p > 2$  een priemgetal. Hoeveel oplossingen modulo  $p$  heeft  $a^2 \equiv bc \pmod{p}$ ? ✿ A

**Opgave I.73.** Bewijs dat  $35 \mid 24^n + 12^n - 17^n - 19^n$  voor elke  $n \in \mathbb{N}$ . ✿

**Opgave I.74.** Waar of vals? Voor elke  $n \in \mathbb{N}$  bestaan er  $n$  opeenvolgende natuurlijke getallen die elk deelbaar zijn door de som van hun cijfers. ✿ A

**Opgave I.75.** Bewijs dat voor  $m, n, q \in \mathbb{N}^+$ ,



$$\sum_{m|q} \sum_{n|q} \frac{\mu(m)\mu(n)}{mn} \text{ggd}(m, n) = \frac{\varphi(q)}{q}.$$

**Opgave I.76.** Zij  $a, b, c \in \mathbb{N}$  paarsgewijs relatief priem en zo dat  $a^2 + b^2 + c^2 \mid abc$ . Bewijs dat



$$\frac{abc}{a^2 + b^2 + c^2}$$

even is.

**Opgave I.77.** Toon aan dat een natuurlijk getal dat enkel uit de cijfers 0 en 6 bestaat, geen kwadraat kan zijn.



**Opgave I.78.** (INMO 2014 vraag 2) Zij  $n \in \mathbb{N}^+$ . Bewijs dat



$$\left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \left\lfloor \frac{n}{n} \right\rfloor + \lfloor \sqrt{n} \rfloor$$

even is.

**Opgave I.79.** (RMO 2013 vraag 2) Vind alle drietallen  $(p, q, r)$  van priemgetallen waarvoor  $pq = r + 1$  en  $2(p^2 + q^2) = r^2 + 1$ .



**Opgave I.80.** Zij  $p \equiv 7 \pmod{8}$  een priemgetal. Bewijs dat



$$\sum_{r=1}^{\frac{p-1}{2}} r \binom{r}{p} = 0.$$

**Opgave I.81.** Bepaal het laatste niet-nul cijfer van  $\binom{1027}{41}$ .



**Opgave I.82.** Geen van de getallen in de rij  $a, a + d, a + 2d, \dots$  is deelbaar door  $n$ . Bewijs dat  $\text{ggd}(d, n) = 1$ .



**Opgave I.83.** Noem  $a(k)$  het aantal enen in de binaire schrijfwijze van  $k$ . Als  $n > 0$ , bewijs dat



$$\sum_{k=0}^{2^n-1} (-1)^{a(k)} \cdot 2^k$$

minstens  $n!$  delers heeft.

**Opgave I.84.** Zij  $x, y, n \in \mathbb{N}^+$  zo dat  $(n + 1)x^2 - (n - 1)y^2 = n$ . Bewijs dat  $2n$  een kwadraat is.



**Opgave I.85.** (RMO 1992 vraag 2) Stel dat  $a, b, c \in \mathbb{N}$  relatief priem zijn en  $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$ . Bewijs dat  $a + b$  een kwadraat is.



**Opgave I.86.** Noem een natuurlijk getal een semi-priemmacht als het hoogstens twee verschillende priemfactoren heeft. Kan elke  $q \in \mathbb{Q}^+$  worden geschreven in de vorm ✿ A

$$q = \frac{1}{n_1} + \cdots + \frac{1}{n_k}$$

met  $n_1, \dots, n_k$  semi-priem machten?

**Opgave I.87.** Bewijs dat  $3^m + 3^n + 1$  geen kwadraat kan zijn voor  $m, n \in \mathbb{N}$ . ✿

**Opgave I.88.** Zij  $p \equiv 7 \pmod{8}$  een priemgetal. Bewijs dat ✿

$$\sum_{n=1}^p \left\lfloor \frac{n(n+1)}{p} \right\rfloor = \frac{2p^2 + 3p + 7}{6}.$$

**Opgave I.89.** Bewijs dat  $2^k$  voor  $k \geq 3$  kan worden geschreven in de vorm  $a^2 + 7b^2$  met  $a, b$  oneven. ✿

**Opgave I.90.** Zij  $m \in \mathbb{N}$  oneven. Noteer met  $p(n)$  de grootste oneven deler van  $n$ . We definiëren een rij  $(a_n)$  via  $a_{n+1} = p(m + a_n)$ , met  $a_1 \in \{1, \dots, m-1\}$  oneven. Definieer ook de rij  $(b_n)$  met  $b_1 = \frac{a_1}{m}$  en  $b_{n+1} = 2^k b_n - 1$ , waarbij  $k$  minimaal wordt gekozen zo dat  $b_{n+1} > 0$ . Bewijs dat  $(a_n)$  en  $(b_n)$  periodiek zijn met dezelfde periode. ✿

**Opgave I.91.** Bewijs dat  $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$  een natuurlijk getal is enkel als  $n = 1$ . ✿

**Opgave I.92.** Bewijs dat  $x^8 \equiv 16 \pmod{p}$  oplosbaar is voor elk priemgetal  $p$ . ✿

**Opgave I.93.** (PEN J8) Bewijs dat de verzameling van rationale getallen  $\frac{\varphi(n)}{n}$  dicht is in  $[0, 1]$ .

**Opgave I.94.** Vind alle gehele getallen van de vorm  $\frac{x^3-y}{xy+1}$  met  $x, y \in \mathbb{N}$ . 🟩

**Opgave I.95.** (PEN J9) Bewijs dat de verzameling van rationale getallen  $\frac{\varphi(n+1)}{n}$  dicht is in  $\mathbb{R}^+$ .

**Opgave I.96.** Zij  $x, y \in \mathbb{Z}$  zo dat  $\frac{4x^2-1}{4x^2-y^2} = k \in \mathbb{Z}$ . Bewijs dat  $k = 1$ .

**Opgave I.97.** Zij  $p = a^2 + 4b^2$  een priemgetal,  $a, b \in \mathbb{N}$ . Bewijs dat de Pell-typevergelijking  $x^2 - py^2 = a$  een gehele oplossing heeft. ✿










**Opgave I.98.** Vind alle priemgetallen waarvoor  $\frac{2^{p-1}-1}{p}$  een kwadraat is. ✿

**Opgave I.99.** Vind alle Fibonaccigetallen die van de vorm  $2^{2^n} + 1$  zijn. ✿

**Opgave I.100.** Zij  $a, b \in \mathbb{Z}$ . Bewijs dat ✿

$$\left(a + \frac{1}{2}\right)^n + \left(b + \frac{1}{2}\right)^n$$

geheel is voor slechts een eindig aantal  $n \in \mathbb{N}$ .

- Opgave I.101.** Bewijs dat de verzameling van rationale getallen  $\frac{\varphi(n+2)}{\varphi(n)}$  dicht is in  $\mathbb{R}^+$ . 
- Opgave I.102.** Zij  $a, b \in \mathbb{N}^+$  met  $(ab)^{n-1} + 1 \mid a^n + b^n$ . Bewijs dat  $\frac{a^n + b^n}{(ab)^{n-1} + 1}$  een volkomen  $n$ -de macht is.  
- Opgave I.103.** Vind alle  $x, y \in \mathbb{N}$  waarvoor  $5xy(x^2 + y^2)^{\frac{3}{2}}$  de som van vier gehele vijfdemachten is. 
- Opgave I.104.** (CanMO 1971 vraag 6) Toon aan dat voor alle  $n \in \mathbb{Z}$ ,  $n^2 + 2n + 12$  geen veelvoud is van 121.
- Opgave I.105.** (IrMO 2006 dag 1 vraag 1) Zijn er gehele getallen  $x, y, z$  die voldoen aan  $z^2 = (x^2 + 1)(y^2 - 1) + n$  als  $n = 2006$ ? Wat als  $n = 2007$ ?
- Opgave I.106.** (BrMO 1 2006 vraag 1) Zij  $n$  een natuurlijk getal groter dan 6. Bewijs dat als zowel  $n - 1$  als  $n + 1$  priem zijn, dat  $n^2(n^2 + 16)$  deelbaar is door 720. Is het omgekeerde waar?
- Opgave I.107.** (VWO 2001 finale vraag 1) Toon aan dat voor elk natuurlijk getal  $n > 1$  geldt dat  $(n - 1)^2 \mid n^{n-1} - 1$ . 
- Opgave I.108.** (USAMO 1979 vraag 1) Vind alle 14-tallen van (niet noodzakelijk verschillende) natuurlijke getallen waarvoor de som van de vierdemachten 1599 is. 
- Opgave I.109.** Zij  $p \geq 5$  een priemgetal. Bewijs dat  $7^p - 6^p - 1$  deelbaar is door 43. 
- Opgave I.110.** Zijn  $a$  en  $b$  natuurlijke getallen zo dat  $2^n a + b$  een volkomen kwadraat is voor alle natuurlijke getallen  $n$ . Bewijs dat  $a = 0$ .
- Opgave I.111.** (VWO 1990 finale vraag 2) Als  $a > b$  twee priemgetallen zijn met minstens twee cijfers, bewijs dan dat  $240 \mid a^4 - b^4$ , en dat 240 de grootst mogelijke waarde hiervoor is. 
- Opgave I.112.** Zij  $P(x)$  een niet-constante veelterm met gehele coëfficiënten. Bewijs dat er oneindig veel natuurlijke getallen  $n$  bestaan waarvoor  $|P(n)|$  geen priemgetal is.
- Opgave I.113.** Zij  $n = 2^m k + 1$  een natuurlijk getal zo dat  $k < 2^m$ ,  $k$  oneven is en er een getal  $a$  bestaat waarvoor  $a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ . Bewijs dat  $n$  een priemgetal is.
- Opgave I.114.** (USAMO 1986 vraag 3) Bepaal het kleinste natuurlijk getal  $n > 1$  zo dat het rekenkundig gemiddelde van de getallen  $1^2, 2^2, \dots, n^2$  zelf een kwadraat is. 
- Opgave I.115.** Stel  $n > 0$  is een veelvoud van 8 met precies  $m$  verschillende priemdelers. Hoeveel oplossingen modulo  $n$  heeft de congruentie  $x^2 \equiv 1 \pmod{n}$  dan? Druk je antwoord uit in functie van  $m$  alleen.
- Opgave I.116.** (BaMO 2003 vraag 1) Kan men 4004 natuurlijke getallen vinden zodanig dat de som van elke 2003 van deze getallen niet deelbaar is door 2003?

**Opgave I.117.** Vind het grootste natuurlijk getal  $a$  zo dat  $a \mid p^{2010} - q^{2010}$  voor alle priemgetallen  $p$  en  $q$  zo dat  $p$  minstens 2010 cijfers en  $q$  minstens 1020 cijfers heeft. ❄

**Opgave I.118.** (BaMO 1988 vraag 4) Gegeven is de rij  $x_n = 2^n + 49$ . Vind alle natuurlijke getallen  $n$  zodanig dat  $x_n$  en  $x_{n+1}$  elk het product zijn van precies twee verschillende priemgetallen met hetzelfde verschil.

## Open problemen

De volgende opgaven zijn vermoedelijk niet extreem moeilijk, maar er is nog geen oplossing van bekend. Of tenminste, geen oplossing die steunt op elementair rekenwerk. Mogelijks gebruikt hun eenvoudigste oplossing een eigenschap uit een volgend deel, dus zoek je ook niet te pletter.

**Opgave I.119.** Zij  $p$  een priemgetal en  $k \in \mathbb{N}^+$ . Bewijs dat  $\frac{p^{2k}-1}{p^2-1}$  geen kwadraat kan zijn. ❄

**Opgave I.120.** Zij  $p > 3$  een priemgetal. Bewijs dat de constante term van ❄

$$\left(1 + x + \frac{1}{x}\right)^p - 1$$

deelbaar is door  $p^2$ .

**Opgave I.121.** Toon aan dat de vergelijking  $x^2 - y^{10} + z^5 = 6$  geen gehele oplossingen heeft. ❄

**Opgave I.122.** Zij  $p$  een priemdelers van  $2^{2^n} + 1$ , en stel dat  $p \equiv 1 \pmod{2^{n+3}}$ . Is 2 dan een vierdemacht modulo  $p$ ? ❄

**Opgave I.123.** Bewijs dat  $99^{100} + 100^{101} + 101^{99} + 1$  geen priemgetal is. ❄

**Opgave I.124.** Voor welke priemgetallen  $p$  en natuurlijke getallen  $m$  heeft  $p$  een oneven orde modulo  $\text{rad}\left(\frac{p^m-1}{p-1}\right)$ ? ❄

**Opgave I.125.** Zij  $a, b \in \mathbb{N}^+$  relatief priem. Bewijs dat voor elke  $n > 0$ , ❄

$$\frac{1}{a} + \frac{1}{a+b} + \frac{1}{a+2b} + \cdots + \frac{1}{a+nb} \notin \mathbb{N}.$$

**Opgave I.126.** Los  $p^a + 1 = 2q^b$  op voor  $a, b \geq 2$  en oneven priemgetallen  $p, q$ . ❄

**Opgave I.127.** Als  $q \in \mathbb{N}$  oneven is en  $2^q \pm 2^{\frac{q+1}{2}} + 1$  een priemgetal, is  $q$  dan noodzakelijk een priemgetal? ❄

**Opgave I.128.** Voor welke natuurlijke getallen  $q$  is  $\sigma(q) - q \mid q - 1$ ? ❄

**Opgave I.129.** Vind alle Fibonaccigetallen die de som van twee derdemachten groter dan 0 zijn. ❄

**Opgave I.130.** Vind alle functies  $f : \mathbb{N}^+ \rightarrow \mathbb{N}^+$  met de eigenschap dat voor alle  $a, b > 0$  waarvoor  $a + b$  een kwadraat is, ook  $f(a) + f(b)$  een kwadraat is. ❀

**Opgave I.131.** Bestaan er gehele  $a, b > 1$  waarvoor  $a^4 \equiv 1 \pmod{b^2}$  en  $b^4 \equiv 1 \pmod{a^2}$ ? ❀

**Opgave I.132.** Voor welke natuurlijke  $x$  zijn er  $x$  opeenvolgende gehele getallen waarvan de som een priemgetal is? ❀

**Definitie I.133.** Thabit-priemgetal

Een *Thabit* is een priemgetal van de vorm  $3 \cdot 2^n - 1$ .

**Opgave I.134.** Zij  $p = 3 \cdot 2^n - 1$  een Thabit-priemgetal met  $n$  oneven. Bewijs dat 5 een primitieve wortel is modulo  $p$  als en slechts als  $n \equiv 3, 7 \pmod{8}$ . ❀

**Opgave I.135.** Welke veeltermen  $P$  voldoen aan  $P(n) > 0$  en  $\varphi(n) \mid \varphi(P(n))$  voor alle  $n \in \mathbb{N}^+$ ? ❀

**Opgave I.136.** Vind alle gehele  $x, y$  met  $x^3 + 5 = y^5$ . ❀

**Opgave I.137.** Voor welke  $n \in \mathbb{N}$  is  $n^7 + 7$  een volkomen kwadraat? ❀

**Opgave I.138.** Bewijs dat  $(x^2 + ay^2)(u^2 + bv^2) = p^2 + cq^2$  een niet-triviale oplossing heeft voor alle keuzes van  $a, b, c$ . ❀

**Opgave I.139.** Zijn Wieferich-priemgetallen de enige oplossingen voor ❀

$$2^{n-1} \equiv 1 \pmod{n^2} ?$$

**Opgave I.140.** Wat kan je zeggen over de waarde van ❀

$$\sum_{d|q^n-1} \mu\left(\frac{q^n-1}{d}\right) q^{\text{ord}_d(q)} ?$$

Beschouw eventueel eerst de gevallen waarbij  $q$  priem is of een priemmacht is.



# II

## Algebra

*I believe that in mathematics nothing is a trick, if seen from a sufficiently high level.*

(Qiaochu Yuan)

In wat volgt geven we een alternatieve opbouw van modulorekenen. De eigenschappen van congruenties die we in het begin van Hoofdstuk 7 hebben bewezen, zullen we hier (voor even toch) heel bewust niet gebruiken. De bedoeling is om een volledig zelfstandige opbouw te geven.

### 18.1 De ring $\mathbb{Z}/m\mathbb{Z}$

We voeren opnieuw het begrip congruentie in. Het subtiele verschil zit er in dat we hier geen getallen apart beschouwen, maar steeds de hele restklasse waartoe een getal behoort. Met het oog op rekenen met restklassen voeren we een nieuwe notatie in.

#### Notatie 18.1.

Voor  $m \in \mathbb{Z}_0$  noteren we  $\mathbb{Z}/m\mathbb{Z}$  voor de verzameling van restklassen modulo  $m$ .

Herinner je de volgende eigenschappen:

#### Eigenschappen 18.2.

Voor  $m \in \mathbb{Z}_0$  en  $a, b \in \mathbb{Z}$  geldt:

1. Er zijn  $|m|$  restklassen modulo  $m$
2.  $a$  en  $b$  hebben dezelfde rest bij deling door  $m$  als en slechts als  $a - b$  een veelvoud is van  $m$ .

#### Notatie 18.3.

We noteren  $[a]_m = a + m\mathbb{Z}$  voor de restklasse modulo  $m$  waar  $a$  toe behoort, of kortweg  $[a]$  als er geen verwarring mogelijk is.

#### 18.1.1 Bewerkingen in $\mathbb{Z}/m\mathbb{Z}$

We voeren nu formeel twee nieuwe bewerkingen in.

**Definitie 18.4.**

Voor  $a, b \in \mathbb{Z}$  definiëren we  $[a]_m \oplus [b]_m = [a + b]_m$  en  $[a]_m \otimes [b]_m = [ab]_m$ .

Wacht, niet zo snel: wat we hier definiëren is een bewerking tussen verzamelingen, restklassen, maar de definitie gebeurt aan de hand van één enkel getal dat daartoe behoort? Betekent dit dat die definitie niet afhangt van welk getal we kozen? Goede vraag! Zo'n definitie heeft inderdaad pas zin als we bewijzen dat ze niet afhankelijk is van de *representanten*  $a$  en  $b$ . Laten we dit dus toch maar eens nagaan. Herinner je eraan dat we algemeen  $V + W = \{v + w : v \in V \text{ en } w \in W\}$  noteren (indien die laatste optelling betekenisvol is), analoog voor vermenigvuldiging.

**Lemma 18.5.**

Zij  $m \in \mathbb{Z}_0$  en  $a, b, c \in \mathbb{Z}$ . Dan geldt: (de restklassen zijn modulo  $m$ )

1.  $[a] = [b]$  als en slechts als  $b - a = km$  voor zekere  $k \in \mathbb{Z}$ .
2. Als  $m \mid b$ , dan is  $[a + b] = [a]$ .
3. De definitie van  $\oplus$  hangt niet af van de keuze van de representanten.
4. De definitie van  $\otimes$  hangt niet af van de keuze van de representanten.

*Bewijs.*

1. Aangezien  $b \in [b]$  is dan  $b \in [a]$ , dus  $b = a + km$ .
2. Stel  $b = km$ . Als  $x \in [a + b]$ , dan is  $x = a + b + lm$  voor zekere  $l \in \mathbb{Z}$ . Dan is  $x = (k + l)m$ , dus  $x \in [a]$ . Omgekeerd, als  $x \in [a]$  is  $x = a + lm$ . Blijkbaar is dan  $x = a + b + (l - k)m$ , dus  $x \in [a + b]$ .
3. Wat we moeten nagaan is dat, als  $[a] = [b]$ , dan  $[a] \oplus [c] = [b] \oplus [c]$ , of dus  $[a + c] = [b + c]$ . (Analoog geldt dan dat de keuze van de representant van  $[c]$  geen verschil maakt.) Aangezien  $b = a + km$  is inderdaad  $[a + c] = [b + c + km] = [b + c]$  wegens het vorige.
4. We moeten nagaan dat, als  $[a] = [b]$ , dan  $[ac] = [bc]$ . Inderdaad:  $[ac] = [(b + km)c] = [bc + kc \cdot m] = [bc]$ .

□

Het ligt voor de hand dat  $\oplus$  en  $\otimes$  niets anders zijn dan de 'gewone' optelling en vermenigvuldiging van verzamelingen. Merk daartoe eerst op dat  $m\mathbb{Z} + am\mathbb{Z} = m\mathbb{Z}$  voor  $a \in \mathbb{Z}$ : het linkerlid is de verzameling van sommen  $mk + aml$  met  $k, l$  willekeurig. Dit is in elk geval een deelverzameling van  $m\mathbb{Z}$ . Dat elk element van  $m\mathbb{Z}$  wel degelijk kan bereikt worden, kunnen we zien door  $l = 0$  te kiezen. Analoog is  $(m\mathbb{Z})(m\mathbb{Z}) = m\mathbb{Z}$ .

**Stelling 18.6.**

Zij  $m \in \mathbb{Z}_0$  en  $a, b \in \mathbb{Z}$ . Dan geldt: (de restklassen zijn modulo  $m$ )

1.  $[a + b] = [a] + [b]$ . (Deze optelling van restklassen is niet noodzakelijk  $\oplus$ !)
2.  $[ab] = [a][b]$ .

*Bewijs.*

1. We hebben  $[a] + [b] = (a + m\mathbb{Z}) + (b + m\mathbb{Z})$ . Deze optelling is commutatief en associatief, dus dit is ook  $(a + b) + (m\mathbb{Z} + m\mathbb{Z}) = (a + b) + m\mathbb{Z} = [a + b]$ .
2. Het rechterlid is  $(a + m\mathbb{Z})(b + m\mathbb{Z})$ . Aangezien deze vermenigvuldiging distributief is, is dit gelijk aan

$$ab + a \cdot (m\mathbb{Z}) + b \cdot (m\mathbb{Z}) + (m\mathbb{Z})(m\mathbb{Z}) = ab + am\mathbb{Z} + bm\mathbb{Z} + m\mathbb{Z} = ab + m\mathbb{Z} = [ab].$$

□

Voila! We kunnen dus gerust  $[a] \oplus [b] = [a] + [b]$  en  $[a] \otimes [b] = [a] \cdot [b]$  schrijven.

Even samenvatten: we hebben een optelling en vermenigvuldiging gedefinieerd op de verzameling van restklassen modulo  $m$ , op zo'n manier dat deze bewerkingen in essentie de optelling en vermenigvuldiging uit  $\mathbb{Z}$  zijn. Er volgt dat deze bewerkingen de eigenschappen van die van  $\mathbb{Z}$  overerven:

**Gevolg 18.7.**

In  $\mathbb{Z}/m\mathbb{Z}$  gelden de volgende eigenschappen:

1. De optelling is associatief:  $\forall a, b, c \in \mathbb{Z}/m\mathbb{Z} : (a + b) + c = a + (b + c)$ .
2. De optelling is commutatief:  $\forall a, b \in \mathbb{Z}/m\mathbb{Z} : a + b = b + a$ .
3. De optelling heeft een neutraal element:  
 $\exists e \in \mathbb{Z}/m\mathbb{Z} : \forall a \in \mathbb{Z}/m\mathbb{Z} : a + e = a = e + a$ .
4. Elk element heeft een inverse voor de optelling:  
 $\forall a \in \mathbb{Z}/m\mathbb{Z} : \exists b \in \mathbb{Z}/m\mathbb{Z} : a + b = e = b + a$ .
5. De vermenigvuldiging is associatief:  $\forall a, b, c \in \mathbb{Z}/m\mathbb{Z} : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ .
6. De vermenigvuldiging is commutatief:  $\forall a, b \in \mathbb{Z}/m\mathbb{Z} : a \cdot b = b \cdot a$ .
7. De vermenigvuldiging heeft een neutraal element:  
 $\exists e \in \mathbb{Z}/m\mathbb{Z} : \forall a \in \mathbb{Z}/m\mathbb{Z} : a \cdot e = a = e \cdot a$ .
8. De vermenigvuldiging is distributief t.o.v. de optelling:  
 $\forall a, b, c \in \mathbb{Z}/m\mathbb{Z} : a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ .

*Bewijs.*

We tonen enkel de laatste aan, de rest gaat met eenzelfde redenering. We hebben

$$[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [ab + ac] = [ab] + [ac] = [a] \cdot [b] + [b] \cdot [c].$$

□

Klaarblijkelijk is  $[0]$  een neutraal element voor de optelling en  $[1]$  voor de vermenigvuldiging. Het is a priori denkbaar dat er nog meer zo'n neutrale elementen zijn, maar daar komen we later op terug. (Je zou kunnen zeggen dat ook bijvoorbeeld  $[m]$  een neutraal element voor de optelling is, maar dit is natuurlijk gewoon hetzelfde element als  $[0]$ .)

Als we nu analoog als in Hoofdstuk 7 een begrip 'congruentie' invoeren, dan hebben we gratis de volgende eigenschappen:

**Gevolg 18.8.**

1.  $a \equiv b$  als en slechts als  $a - b \equiv 0$ .
2. Als  $a \equiv b$  en  $d \equiv e$ , dan is  $a + d \equiv b + e$ .
3. Als  $a \equiv b$ , dan  $na \equiv nb$  voor elk geheel getal  $n$ .
4. Als  $a \equiv b$  en  $d \equiv e$ , dan geldt  $ad \equiv be$ .
5. Als  $a \equiv b$  dan is  $a^n \equiv b^n$  voor elk natuurlijk getal  $n > 0$ .

*Bewijs.*

$[a] = [b]$  als en slechts als  $a \equiv b$ . Alle eigenschappen volgen nu uit het feit dat  $[a] + [b] = [a + b]$  en  $[ab] = [a] \cdot [b]$ . □

### 18.1.2 Ringen

Wat men in de algebra graag doet is zoiets veralgemenen van  $\mathbb{Z}$  naar andere verzamelingen.

**Definitie 18.9.**

Een *ring* is een verzameling  $R$  voorzien van twee bewerkingen,  $\oplus$  en  $\otimes$  die aan de volgende eigenschappen voldoen:

1.  $R$  is *gesloten onder*  $\oplus$ : als  $a, b \in R$ , dan behoort  $a \oplus b$  terug tot  $R$ .
2.  $\oplus$  is commutatief en associatief, en heeft een neutraal element.
3.  $R$  is *gesloten onder*  $\otimes$ : als  $a, b \in R$ , dan behoort  $a \otimes b$  terug tot  $R$ .
4.  $\otimes$  is associatief en heeft een neutraal element.
5.  $\otimes$  is distributief t.o.v.  $\oplus$ .

We zeggen ook dat  $(R, \oplus, \otimes)$  een ring is. (Soms voor het gemak zonder haakjes.)

We zullen deze bewerkingen voortaan ook gewoon optelling en vermenigvuldiging noemen.  $\mathbb{Z}$ , met de gebruikelijke optelling en vermenigvuldiging is het typevoorbeeld van een ring. En niet zomaar een ring.

**Definitie 18.10.**

Een commutatieve ring is een ring waarvoor de vermenigvuldiging commutatief is.

Andere voorbeelden van commutatieve ringen zijn  $\mathbb{Q}$  en  $\mathbb{R}$ .

*Opmerking.*

De voorwaarde dat de vermenigvuldiging een neutraal element heeft wordt soms weggelaten in de definitie van een ring. Men spreekt dan van een ring *met of zonder eenheid*. We zullen hier de conventie aanhouden dat elke ring steeds een neutraal element voor de vermenigvuldiging heeft.

Nogal vervelend om steeds te moeten zeggen “*een* neutraal element” en “*een* inverse”.

**Stelling 18.11.**

Zij  $(R, +, \cdot)$  een ring, dan geldt:

1. Er is een uniek neutraal element voor de optelling en vermenigvuldiging.
2. Elk element heeft een unieke inverse voor de optelling.

*Bewijs.*

1. Stel dat  $e$  en  $f$  neutrale elementen zijn. We moeten bewijzen dat  $e = f$ . Enerzijds is  $e + f = f$ , want  $e$  is een neutraal element. Anderzijds is  $e + f = e$ , want  $f$  is een neutraal element. Dus  $e = f$ . Volledig analoog voor de vermenigvuldiging.
2. Stel dat  $b$  en  $c$  beide inversen zijn van  $a$ . Uit  $b + a = e$  volgen nu achtereenvolgens:  
 $(b + a) + c = e + c \Rightarrow b + (a + c) = c \Rightarrow b + e = c$ , dus  $b = c$ .

□

**Notatie 18.12.**

Zij  $(R, +, \cdot)$  een ring. Voor  $a \in R$  noteren we het unieke inverse voor de optelling als  $-a$ . We schrijven ook  $a + (-b) = a - b$ .

Het neutraal element voor de optelling wordt vaak met 0 genoteerd.

**Definitie 18.13.**

Zij  $R$  een ring. We noemen een deelverzameling  $S$  van  $R$  een *deelring* als  $S$  opnieuw een ring is onder dezelfde optelling en vermenigvuldiging als die van  $R$ .

Niet zomaar elke deelverzameling van  $R$  zal een ring zijn: de voorwaarde dat  $S$  gesloten is onder optelling en vermenigvuldiging legt een grote beperking op.

**Voorbeeld 18.14.** Zij  $R$  een ring met neutraal element voor de optelling 0. Dan zijn  $\{0\}$  en  $R$  deelringen van  $R$ .

De deelring  $\{0\}$  noemt men *triviaal*, er is dan ook weinig interessants over te zeggen. Met een *echte* deelring bedoelen we een die noch  $\{0\}$  noch  $R$  zelf is.

**Opgave 18.15.** Bepaal alle deelringen van  $\mathbb{Z}$ .

HA

### 18.1.3 Quotiëntringen

We veralgemenen nu de constructie van  $\mathbb{Z}/m\mathbb{Z}$  naar algemene ringen.

**Definitie 18.16.**

Zij  $R$  een ring. Een *ideaal* van  $R$  is een deelring  $I$  met de eigenschap dat  $R \cdot I = I \cdot R = I$ , of dus:  $\forall r \in R, i \in I : r \cdot i, i \cdot r \in I$ .

**Voorbeeld 18.17.** Als  $m \in \mathbb{Z}$  is  $m\mathbb{Z}$  een ideaal van  $\mathbb{Z}$ .

**Definitie 18.18.**

Zij  $I$  een ideaal van  $R$ . We noemen twee elementen  $a, b \in R$  *congruent modulo*  $I$  als  $a - b \in I$ . We noteren  $a \equiv b \pmod{I}$ .

Deze definitie van congruentie over  $\mathbb{Z}$  verschilt subtiel van de vroegere: de congruentie is hier modulo een verzameling, niet modulo een getal, maar het is wel duidelijk dat deze twee relaties op hetzelfde neerkomen. (Zie Hoofdstuk D voor een definitie van relaties.)

Merk ook op dat we hier congruentie definiëren als “het verschil  $a - b$  zit in  $I$ ”, terwijl we dit in  $\mathbb{Z}$  definieerden als “dezelfde rest hebben modulo een getal”. In  $\mathbb{Z}$  komen deze twee definities natuurlijk op hetzelfde neer.

**Lemma 18.19.**

Congruentie modulo een ideaal  $I$  is een equivalentierelatie. De equivalentieklasse van  $a$  is  $a + I$ .

*Bewijs.*

Als oefening. □

Dit verklaart de volgende definities:

**Definities 18.20.**

Zij  $R$  een ring en  $I$  een ideaal van  $R$ . Voor  $a \in R$  noteren we  $[a]_I = [a]_{\equiv} = a + I$  en  $R/I = R/\equiv$ , met  $\equiv$  congruentie modulo  $I$ .  $R/I$  noemen we de *quotiëntring*  $R$  modulo  $I$  (ook wel: *factoring*).

Vandaar de notatie  $\mathbb{Z}/m\mathbb{Z}$  die we eerder hebben gezien. Analoog als toen bewijst men de volgende eigenschappen:

**Lemma 18.21.**

Zij  $I$  een ideaal van  $R$  en  $a, b \in R$ . Dan geldt: (de restklassen zijn modulo  $I$ )

1.  $[a] = [b]$  als en slechts als  $b - a \in I$ .
2. Als  $b \in I$ , dan is  $[a + b] = [a]$ .
3.  $[a + b] = [a] + [b]$ .
4.  $[a \cdot b] = [a] \cdot [b]$ .

**Opgave 18.22.** Bewijs als oefening.

Dit verklaart meteen de naam quotiëntring, het was immers a priori niet duidelijk dat  $R/I$  wel degelijk een ring is:

**Gevolg 18.23.**

Een quotiëntring  $R/I$  vormt een ring onder optelling en vermenigvuldiging van de restklassen als verzamelingen. Is  $R$  commutatief, dan ook  $R/I$ .

*Opmerking.*

De constructie van  $R/I$  verschilt hier lichtelijk met die van  $\mathbb{Z}/m\mathbb{Z}$ . Hier definiëren we voor het gemak de optelling en vermenigvuldiging in  $R/I$  aan de hand van de bewerkingen met verzamelingen, zonder eerst formeel twee nieuwe bewerkingen in te voeren en nadien te moeten controleren of die goed gedefinieerd zijn.

**18.2 De groep  $(\mathbb{Z}/m\mathbb{Z})^\times$** **18.2.1 Inverteerbaarheid in  $\mathbb{Z}/m\mathbb{Z}$** 

We weten dat de vermenigvuldiging in  $\mathbb{Z}$  en  $\mathbb{Z}/m\mathbb{Z}$  (meer algemeen in een ring) een neutraal element heeft. Niet zomaar elk element is echter inverteerbaar. Analoog als in Hoofdstuk 7 volgt uit de stelling van Bézout:

**Eigenschap 18.24.**

Zij  $m \in \mathbb{Z}_0$ .  $[a] \in \mathbb{Z}/m\mathbb{Z}$  heeft een inverse voor de vermenigvuldiging als en slechts als  $\text{ggd}(a, m) = 1$ .

We spreken kortweg van “inverteerbaar zijn”, waarbij verondersteld wordt dat het om de vermenigvuldiging gaat.

**Notatie 18.25.**

We noteren  $(\mathbb{Z}/m\mathbb{Z})^\times$  voor de verzameling van inverteerbare elementen in  $\mathbb{Z}/m\mathbb{Z}$ .

Bij definitie van de totiëntfunctie is  $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(|m|)$ . Meer algemeen definiëren we:

**Notatie 18.26.**

Zij  $R$  een ring. We noteren  $R^\times$  voor de verzameling van inverteerbare elementen in  $R$ .

Zo is bijvoorbeeld  $\mathbb{Z}^\times = \{-1, 1\}$ .

De som van twee inverteerbare elementen is niet noodzakelijk terug inverteerbaar. Zo is in  $\mathbb{Z}/2\mathbb{Z}$   $[1]$  inverteerbaar, maar  $[1] + [1]$  is dat niet. Hoe zit het met hun product?



**Lemma 18.27.**

Als  $R$  een ring is, is  $R^\times$  gesloten onder vermenigvuldiging.

*Bewijs.*

Als  $a$  een inverse heeft, zeg  $b$  en  $c$  heeft een inverse  $d$ , dan is  $ac$  inverteerbaar. Inderdaad, als  $e$  het unieke neutraal element in  $R$  is, dan is  $(ac)(db) = a((cd)b) = a(eb) = ab = e$ , dus  $ac$  is inverteerbaar.  $\square$

**18.2.2 Groepen**

De structuur van  $R^\times$  is die van wat men een *groep* noemt.

**Definitie 18.28.**

Een *groep* is een verzameling  $G$  uitgerust met een bewerking  $*$  die aan de volgende eigenschappen voldoet:

1.  $G$  is gesloten onder  $*$ .
2.  $*$  is associatief:  $\forall a, b, c \in G : (a * b) * c = a * (b * c)$ .
3.  $*$  heeft een neutraal element:  $\exists e \in G : \forall a \in G : a * e = a = e * a$ .
4. Elk element in  $G$  heeft een inverse voor  $*$ :  $\forall a \in G : \exists b \in G : b * a = e = a * b$ .

We zeggen dat  $G$  een groep vormt onder  $*$ , of kort, dat  $(G, *)$  een groep is. (Soms voor het gemak zonder haakjes.)

In het bijzonder geldt:

**Gevolg 18.29.**

Een ring  $R$  vormt een groep onder zijn optelling.  $R^\times$  vormt een groep onder vermenigvuldiging.

*Bewijs.*

Voor de optelling volgt dit rechtstreeks uit de definitie, elk element is immers inverteerbaar voor  $+$ . Voor de vermenigvuldiging geldt dit ook, want we hebben zopas bewezen dat het product van twee inverteerbare elementen terug inverteerbaar is. Bovendien is de inverse van een inverteerbaar element terug inverteerbaar: als  $a$  inverse  $a^{-1}$  heeft, dan heeft  $a^{-1}$  inverse  $a$ . Alle andere eigenschappen volgen uit de definitie van een ring.  $\square$

Voor een ring wisten we al dat een neutraal element en een inverse voor de optelling uniek zijn. Het bewijs voor groepen is volledig analoog.

**Stelling 18.30.**

In een groep  $G$  geldt:

1. Er is een uniek neutraal element
2. Elk element heeft een unieke inverse.

**Opgave 18.31.** Bewijs zelf als oefening.

Merk op dat de groepsbewerking niet commutatief hoeft te zijn.

**Definitie 18.32.**

Een groep met een commutatieve groepsbewerking is een *abelse groep* of *commutatieve groep*.

**Notaties 18.33.**

Vaak zullen we de groepsbewerking ‘vermenigvuldiging’ noemen, en de bewerking niet altijd noteren. We schrijven dan  $a \cdot a = a^2$ ,  $a \cdot a \cdot a = a^3$ , enzovoort. We stellen ook  $a^1 = a$ . Wegens de associativiteit is deze notatie niet dubbelzinnig. In dit geval spreken we van de *multiplicatieve notatie*. Het unieke neutraal element noemen we vaak  $e$  of 1, en de unieke inverse van  $a$  noteren we als  $a^{-1}$ . We stellen ook nog  $a^0 = e$ .

Soms leent de situatie zich meer tot de zogenaamde *additieve notatie*, denk bijvoorbeeld aan de additieve groep van een ring. In dat geval noemen we de bewerking ‘optelling’ en schrijven we wel steeds het symbool daarvoor. We noteren dan  $a + a = 2a$ ,  $a + a + a = 3a$ , enzovoort. We stellen ook  $1a = a$ . Het unieke neutraal element noteren we vaak als 0, de unieke inverse van  $a$  als  $-a$ . We stellen ook nog  $0a = 0$ .

*Opmerking.*

Er is geen enkel bezwaar tegen om andere notaties te gebruiken. Zo kan je bijvoorbeeld het neutraal element in additieve notatie 1 noemen. Doorgaans wordt dit niet gedaan omdat gelijkheden als  $a + 1 = a$  niet zo natuurlijk aanvoelen.

**Opgave 18.34.** Bewijs dat in een groep geldt dat  $(ab)^{-1} = b^{-1}a^{-1}$  voor alle  $a, b$ .

**Opgave 18.35.** Bewijs dat in een groep,  $(a^{-1})^{-1} = a$  voor alle  $a$ .

**Notaties 18.36.**

In een groep noteren we  $a^{-n} = (a^{-1})^n$  voor  $n > 1$ . In additieve notatie schrijven we  $(-n)a = -na = -(na)$ .

Merk op dat we hiervoor in beide gevallen enkel de meest rechtse van de notaties al hadden ingevoerd.

**Opgave 18.37.** Toon aan dat  $a^{-n} = (a^n)^{-1}$ .

**Opgave 18.38.** Toon aan dat  $a^m a^n = a^{m+n}$  voor willekeurige  $m, n \in \mathbb{Z}$ .

**Definitie 18.39.**

Zij  $G, \cdot$  een groep en  $H$  een deelverzameling van  $G$ . Als  $H, \cdot$  ook een groep is noemen we  $H$  een *deelgroep* van  $G$ .

**18.2.3 Orde van een element**

In Hoofdstuk 7 hebben we bewezen:

**Eigenschap 18.40.**

Als  $m \in \mathbb{Z}_0$  en  $a \in \mathbb{Z}$  met  $\text{ggd}(a, m) = 1$ , dan is er een kleinste natuurlijk getal  $n > 0$  waarvoor  $a^n \equiv 1 \pmod{m}$ .

Je ziet het misschien al gebeuren, in een groep vertaalt dit zich als volgt:

**Definitie 18.41. Eindige groep**

Zij  $G$  een groep. Als  $G$  een eindig aantal elementen heeft, noemen we  $|G|$  de *orde* van  $G$ .  $G$  noemen we een *eindige groep*.

Niet overtuigd? Misschien klinkt het volgende bekender:

**Stelling 18.42.**

Zij  $G$  een eindige groep en  $a \in G$ . Er is een kleinste natuurlijk getal  $n > 0$  waarvoor  $a^n = e$ .  $n$  noemen we de *orde van  $a$  in  $G$* . We noteren  $\text{ord}(a)$  of  $|a|$ .

Het bewijs is volledig analoog als in Hoofdstuk 7:

*Bewijs.*

Aangezien  $G$  eindig is, zijn er wegens het duivenhokprincipe verschillende natuurlijke getallen  $m, n$  waarvoor  $a^m = a^n$ . Veronderstel dat  $m > n$ , dan is  $a^m a^{-m} = a^n a^{-m}$ , dus  $a^{n-m} = e$ . Het volstaat nu om de kleinst mogelijke exponent te beschouwen waarvoor dit geldt, het welordeningsprincipe over  $\mathbb{N}$  garandeert dat die bestaat.  $\square$

Het leuke is nu dat de orde van een element wel degelijk verband houdt met de orde van een groep, zij het niet zomaar een groep.

**Definitie 18.43.**

Zij  $G$  een groep en  $a \in G$ . We stellen  $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, a^0, a, a^2, \dots\}$  en noemen dit de groep *voortgebracht door  $a$* .

Mogelijks is  $\langle a \rangle$  een oneindige verzameling. Dat het een groep is, volgt meteen uit de definitie.

**Definitie 18.44.**

Een groep  $G$  is *cyclisch* als  $G = \langle a \rangle$  voor een zekere  $a \in G$ .

**Opgave 18.45.** Bewijs dat elke cyclische groep abels is.

We hebben:

**Gevolg 18.46.**

Zij  $G$  een eindige groep en  $a \in G$ . De orde van  $\langle a \rangle$  is gelijk aan de orde van  $a$  in  $G$ .

*Bewijs.*

Stel dat  $a$  orde  $n$  heeft. We gaan na dat  $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ . Stel dat  $k \geq 0$ . Noem  $r$  de rest van  $k$  bij deling door  $n$ , dan is  $a^k = a^r$ , hetgeen in die verzameling zit.

Ook zit  $a^{-k}$  in die verzameling, want  $a^{-k} = a^{-r} = a^{n-r}$ . □

**18.2.4 Eigenschappen van de orde: het ordelemma**

**Opgave 18.47.** Zij  $G$  een groep,  $H \leq G$  en  $a \in H$ . Toon aan dat de orde van  $a$  als element van  $H$  dezelfde is als wanneer we het beschouwen als element van  $G$ .

Vandaar noteren we kortweg  $\text{ord}(a)$  en niet  $\text{ord}_G(a)$  of iets dergelijks. We komen nu tot een verassend resultaat.

**Stelling 18.48.**

Zij  $G$  een eindige groep en  $a \in G$ . De orde van  $a$  is een deler van  $|G|$ .

*Bewijs.*

De orde van  $a$  is gelijk aan  $|\langle a \rangle|$ . Dit is een deler van  $|G|$  wegens de stelling van Lagrange. □

Zoals je ziet maakt de stelling van Lagrange dit bijna triviaal. Een onmiddellijk gevolg is:

**Gevolg 18.49. Stelling van Euler**

Zij  $m \in \mathbb{N}^+$  en  $\text{ggd}(a, m) = 1$ , dan is  $[a]^{\varphi(m)} = [1]$ .

*Bewijs.*

De orde van  $[a]$  is een deler van  $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$ . Bijgevolg is  $[a]^{\varphi(m)} = [1]$ . □

En dat zonder ook maar een keer een congruentie te moeten noteren.

**Opgave 18.50.** Bewijs dat  $(\mathbb{Z}/m\mathbb{Z}, +)$  steeds cyclisch is.

**Opgave 18.51.** Zij  $p$  een priemgetal. Bewijs dat elke groep van orde  $p$  cyclisch is.

Volledig analoog als bij het modulorekenen volgt een hoop eigenschappen van ordes.

**Stelling 18.52.** Het ordelemma

Zij  $G$  een groep en  $a \in G$ . Dan is  $a^n = e$  voor  $n \in \mathbb{N}$  als en slechts als  $\text{ord}(a) \mid n$ .

*Bewijs.*

Noem  $q$  het quotiënt en  $r$  de rest van  $n$  bij deling door  $\text{ord}(a)$ . Er geldt dat  $a^n = (a^{\text{ord}(a)})^q a^r = ea^r = a^r$ , dus  $a^r = e$ . Maar  $0 \leq r < \text{ord}(a)$ , dus moet noodzakelijk  $r = 0$ .  $\square$

## 18.3 Interactie

Veelal zijn we niet enkel geïnteresseerd in de structuur van een enkele groep of ring, maar is ook het verband tussen verschillende groepen of ringen van belang. Soms komt het voor dat twee groepen of twee ringen essentieel dezelfde structuur hebben; men spreekt van *isomorfe* structuren.

### 18.3.1 Morfismen

Algemeen zijn morfismen afbeeldingen tussen verzamelingen met bewerkingen of relaties die compatibel zijn met de structuur van die verzamelingen. Om zo'n vage definitie toch wat kracht bij te zetten doen we de moeite om bij elke nieuwe structuur precies te definiëren wat een morfisme juist is.

**Definitie 18.53.**

Zij  $G$  en  $H$  groepen. Een afbeelding  $f : G \rightarrow H$  is een *groeps morfisme* of *groepshomomorfisme* als  $f(ab) = f(a)f(b)$  voor alle  $a, b \in G$ .

De notatie  $f(ab) = f(a)f(b)$  behoeft een beetje uitleg: in het linkerlid staat de functiewaarde van een product. de bewerking tussen  $a$  en  $b$  ginds is die van  $G$ . Rechts staat het product van twee functiewaarden, de bewerking is die uit  $H$ . Voor het gemak noteren we de bewerkingen gewoon niet.

*Opmerking.*

*morfisme* en *homomorfisme* zijn synoniemen, ook in samenstellingen met 'groep' of 'ring'. Om de leesbaarheid te bevorderen zullen we vooral *morfisme* gebruiken.

**Voorbeeld 18.54.**  $\ln$  is een groeps morfisme van de groep  $(\mathbb{R}^+, \cdot)$  naar  $(\mathbb{R}, +)$ .

**Definities 18.55.**

Een *groepsisomorfisme* is een groeps morfisme dat een bijectie is. Een *groepsautomorfisme* is een isomorfisme van een groep naar zichzelf. Twee groepen noemen we *isomorf* als er een groepsisomorfisme bestaat van de ene naar de andere. We noemen  $G \cong H$ .

$\ln$  is klaarblijkelijk een groepsisomorfisme. Analoge definities gaan op voor ringen:

**Definities 18.56.**

Zij  $(R, \oplus, \otimes)$  en  $(S, \boxplus, \boxtimes)$  ringen. Een afbeelding  $f : R \rightarrow S$  is een *ringmorfisme* als  $f$  een groepsomorfisme is van  $(R, \oplus)$  naar  $(S, \boxplus)$ , en als  $f(a \otimes b) = f(a) \boxtimes f(b)$  voor alle  $a, b \in R$ .  $f$  is een *ringisomorfisme* als het bovendien een bijectie is, en een *ringautomorfisme* als  $R = S$ . We noemen  $R$  en  $S$  *isomorf* als er een isomorfisme bestaat van  $R$  naar  $S$ , en noteren  $R \cong S$ .

Naast erg goede Scrabble-woorden (met ‘ringisomorfisme’ kan je een woord over de hele breedte leggen) zijn dit ook heel zinvolle begrippen in de wiskunde.

**Voorbeeld 18.57.** Bewijs dat  $(\mathbb{Z}/5\mathbb{Z})^\times, \cdot) \cong (\mathbb{Z}/4\mathbb{Z}, +)$  en geef een groepsisomorfisme.

*Oplossing.*

Om te beginnen gaan we na of beide groepen evenveel elementen hebben. Inderdaad:

$$|(\mathbb{Z}/5\mathbb{Z})^\times| = \varphi(5) = 4 = |\mathbb{Z}/4\mathbb{Z}| :$$

er is hoop. Merk op dat  $(\mathbb{Z}/5\mathbb{Z})^\times$  cyclisch is:  $[2]^0 = [1]$ ,  $[2]^1 = [2]$ ,  $[2]^2 = [4]$  en  $[2]^3 = [3]$ . Het isomorfisme ligt nu voor de hand: Definieer  $f([2^0]) = 0$ ,  $f([2^1]) = 1$ ,  $f([2^2]) = 2$  en  $f([2^3]) = 3$ . Dat dit wel degelijk een morfisme is gaat men eenvoudig na met hun zogenaamde Cayley-tabellen:

$\cdot$	$[2^0]$	$[2^1]$	$[2^2]$	$[2^3]$	$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[2^0]$	$[2^0]$	$[2^1]$	$[2^2]$	$[2^3]$	$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2^1]$	$[2^1]$	$[2^2]$	$[2^3]$	$[2^0]$	$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2^2]$	$[2^2]$	$[2^3]$	$[2^0]$	$[2^1]$	$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[2^3]$	$[2^3]$	$[2^0]$	$[2^1]$	$[2^2]$	$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Een Cayley-tabel van een groep is een tabel waarin het resultaat van de groepsbewerking voor alle koppels groeps-elementen af te lezen is. Als een afbeelding tussen groepen de ene Cayley-tabel op de andere afbeeldt, dan is die afbeelding meteen een isomorfisme:  $f(a \cdot b) = f(a) + f(b)$ , en de afbeelding is bijectief.  $\square$

We weten al dat  $\mathbb{Z}/m\mathbb{Z}$  steeds cyclisch is. Ook  $\mathbb{Z}$  is cyclisch, want elk element is te schrijven als  $1 + \dots + 1$  of het tegengestelde daarvan. Het leuke is nu dat het begrip ‘isomorfisme’ ons toelaat om in zekere zin alle cyclische groepen te kennen.

**Stelling 18.58.**

Een cyclische groep is ofwel isomorf met  $(\mathbb{Z}/n\mathbb{Z}, +)$  voor zekere  $n \in \mathbb{N}^+$ , ofwel met  $(\mathbb{Z}, +)$ .

Men zegt ook:  $\mathbb{Z}/n\mathbb{Z}$  en  $\mathbb{Z}$  vormen alle cyclische groepen ‘op een isomorfisme na’.

*Bewijs.*

Zij  $G$  cyclisch, en stel dat  $G$  eindig is. Dan is  $G = \{e, a, a^2, \dots, a^{n-1}\}$  voor zekere  $a \in G$ . Definieer nu  $f(a^k) = [k]_n$ . Deze definitie hangt niet af van de exponent  $k$ : als  $a^l = a^k$ , dan is noodzakelijk  $n \mid k - l$  omdat  $a$  orde  $n$  heeft, en dus  $[k]_n = [l]_n$ . De afbeelding is duidelijk bijectief. Er geldt dat  $f(a^k \cdot a^l) = f(a^{k+l}) = [k+l] = [k] + [l] = f(a^k) + f(a^l)$ , dus  $f$  is een morfisme.

Stel nu dat  $G$  oneindig is en voortgebracht wordt door  $a$ . Dan zijn alle elementen  $a^k$  met  $k \in \mathbb{Z}$  verschillend, zoniet zou  $\langle a \rangle$  eindig zijn. Definieer dus  $f(a^k) = k$ .  $f$  is een bijectie, en uiteraard een morfisme:  $f(a^k \cdot a^l) = f(a^{k+l}) = k + l = f(a^k) + f(a^l)$ .  $\square$

We hernemen het voorgaande voorbeeld. We wisten dat  $(\mathbb{Z}/5\mathbb{Z})^\times$  cyclisch is. Aangezien die groep orde 4 heeft, volgt onmiddellijk dat hij isomorf is met  $\mathbb{Z}/4\mathbb{Z}$ .

**Notatie 18.59.**

Voor  $n \in \mathbb{N}^+$  schrijven we  $C_n$  voor een niet nader gespecificeerde cyclische groep van orde  $n$ , en  $C_\infty$  voor een niet nader gespecificeerde oneindige cyclische groep.

Deze notatie is eerder van formeel belang. We schrijven bijvoorbeeld  $(\mathbb{Z}/5\mathbb{Z})^\times \cong C_4$  om duidelijk te maken dat  $(\mathbb{Z}/5\mathbb{Z})^\times$  een cyclische groep van orde 4 is. Wat  $C_4$  precies is, doet er niet toe. Alle cyclische groepen van dezelfde orde zijn toch onderling isomorf.

**Opgave 18.60.** Bepaal op een isomorfisme na alle groepen van orde 4. Met welke bekende HA groepen zijn ze isomorf?

**18.3.2 Som en product van structuren****18.3.3 Direct product**

Met twee groepen kan men een nieuwe groep construeren als volgt:

**Definitie 18.61.**

Zij  $G$  en  $H$  groepen (die niks met elkaar te maken hoeven te hebben). Het *direct product*  $G \times H$  is de groep bestaande uit alle koppels  $(g, h)$  met  $g \in G$  en  $h \in H$ , en met bewerking gedefinieerd door  $(a, b)(c, d) = (ab, cd)$ .

**Opgave 18.62.** Ga na dat het direct product van twee groepen een groep is.

**Gevolg 18.63.**

Voor groepen  $A, B, C$  geldt:

1.  $A \times B \cong B \times A$ . Het isomorfisme wordt gegeven door  $(a, b) \mapsto (b, a)$ .
2. als  $A \cong C$ , dan  $A \times B \cong C \times B$ . Als het isomorfisme tussen  $A$  en  $C$   $a$  op  $c$  afbeeldt, dan stellen we  $(a, b) \mapsto (c, b)$ .

**Voorbeeld 18.64.** Bewijs dat  $(\mathbb{Z}/8\mathbb{Z})^\times \cong C_2 \times C_2$ .

*Oplossing.*

Stel  $C_2 = (e, a)$ . De caleytabellen van beide groepen zijn

$\cdot$	[1]	[3]	[5]	[7]		$+$	(0, 0)	(0, 1)	(1, 1)	(1, 0)
[1]	[1]	[3]	[5]	[7]		(0, 0)	(0, 0)	(0, 1)	(1, 1)	(1, 0)
[3]	[3]	[1]	[7]	[5]		(0, 1)	(0, 1)	(0, 0)	(1, 0)	(1, 1)
[5]	[5]	[7]	[1]	[3]		(1, 1)	(1, 1)	(1, 0)	(0, 0)	(0, 1)
[7]	[7]	[5]	[3]	[1]		(1, 0)	(1, 0)	(1, 1)	(0, 1)	(0, 0)

Een mogelijk isomorfisme is dus  $([1], [3], [5], [7]) \mapsto ((0, 0), (0, 1), (1, 1), (1, 0))$ . □

Vanzelfsprekend kunnen we het direct product uitbreiden naar meerdere groepen.

**Definitie 18.65.** Direct product van groepen

Voor groepen  $G_1, \dots, G_n$  definiëren we het *direct product*  $G_1 \times \dots \times G_n$  analoog als de groep op het cartesisch product met geïnduceerde componentsgewijze bewerkingen.

Klaarblijkelijk is  $(A \times B) \times C \cong A \times B \times C \cong A \times (B \times C) \cong A \times B \times D$  als  $C \cong D$ . Analoge eigenschappen gelden uiteraard voor meerdere groepen.

**Notatie 18.66.**

We schrijven  $G \times G = G^2$ ,  $G \times G \times G = G^3$ , enzovoort.

**Definitie 18.67.** Direct product van ringen

Zij  $R$  en  $S$  ringen (niet noodzakelijk met dezelfde bewerkingen). Het *direct product*  $R \times S$  is de ring op het cartesisch product met geïnduceerde componentsgewijze bewerkingen.

Het spreekt voor zich dat we ook deze definitie kunnen veralgemenen naar meerdere ringen, met analoge eigenschappen voor isomorfismen.

## 18.4 De Chinese reststelling

We proberen de Chinese reststelling te veralgemenen. Om te beginnen hebben we een nieuwe notie van ‘relatief priem’ nodig.



**Definitie 18.68.** Coprieme idealen

Zij  $R$  een commutatieve ring en  $I, J$  idealen van  $R$ . We noemen  $I$  en  $J$  *copriem* of *comaximaal* als  $I + J = R$ .

## 18.5 Veeltermringen

### 18.5.1 Factorisatiestellingen

## 18.6 Cyclische groepen

**Stelling 18.69.**

Zij  $G$  een eindige groep van orde  $n$ . De volgende uitspraken zijn gelijkwaardig:

1.  $G$  is cyclisch.
2. Voor elke deler  $d$  van  $n$  heeft de vergelijking  $x^d = e$  precies  $d$  oplossingen.
3. Voor elke deler  $d$  van  $n$  zijn er juist  $\varphi(d)$  elementen van orde  $d$ .

**Opgave 18.70.** Bewijs.

Als we aantonen dat 2 uit 1, 3 uit 2 en 1 uit 3 volgt is het bewezen.

- A. Toon aan dat 2 uit 1 volgt, meer bepaald dat  $x = g^k$  voldoet aan  $x^d = e$  als en slechts als  $\frac{n}{d} \mid k$ .

Veronderstel 2. Noem  $A(d)$  het aantal elementen van orde  $d$ .

- B. Toon aan dat  $d = \sum_{c \mid d} A(c)$  voor alle  $d \mid n$ .

- C. Toon aan dat  $A(d) = \varphi(d)$  voor alle  $d \mid n$ .

Veronderstel nu 3. Dan zijn er  $\varphi(n)$  elementen van orde  $n$ . Daar  $\varphi(n) \geq 1$  is er een element  $g$  van orde  $n$ . Daar  $|\langle g \rangle| = n$  en  $\langle g \rangle \leq G$  is  $\langle g \rangle = G$ , dus  $G$  is cyclisch.

**Gevolg 18.71.**


Zij  $G = \langle g \rangle$  een cyclische groep van orde  $n$ . Dan bezit  $G$  voor elke deler  $d$  van  $n$  juist één deelgroep van orde  $d$ . Die deelgroep wordt voortgebracht door  $g^{\frac{n}{d}}$ .

## 18.7 Het veld $\mathbb{F}_p$


### Opgaven hoofdstuk 18


**Opgave 18.72.** Zij  $G$  een groep en  $A$  en  $B$  cyclische deelgroepen van  $G$ . Bewijs dat  $A \cap B$  ook cyclisch is.

**Opgave 18.73.** (VJO 2006) Zij  $G$  een eindige groep van orde  $n$ . Bewijs dat elk element van  $G$  een kwadraat is als en slechts als  $n$  oneven is. 

**Opgave 18.74.** (VJO 1993) Bepaal of er een niet-triviaal homomorfisme bestaat van  $(\mathbb{Q}, +)$  naar  $(\mathbb{Z}, +)$ . 

**19.1 Case study: de Ramanujan-Nagell vergelijking****19.2 Mordell-vergelijkingen**

**Opgave 19.1.** Bewijs dat  $n^3 + 7$  geen volkomen kwadraat kan zijn voor  $n \in \mathbb{N}$ . 

**Opgave 19.2.** Vind alle natuurlijke oplossingen van  $8^x + 17 = y^2$ . 

**Opgaven hoofdstuk 19**

In afwachting van de nodige tijd en enthousiasme om dit hoofdstuk vorm te geven, raden we de geïnteresseerde lezer aan een kijkje te nemen in een boek als [6]. Voor andere suggesties kan je rondneuzen op de volgende links:


<http://math.stackexchange.com/questions/1336798>

<http://math.stackexchange.com/questions/73565>

<http://math.stackexchange.com/questions/1298669>

### Opgaven hoofdstuk 20

## Opgaven deel II

**Opgave II.1.** Noteer met  $L_n$  de lengte van een zijde in een regelmatige  $n$ -hoek ingeschreven in een cirkel met straal 1 (en  $L_2 = 2$ ). Vind alle oplossingen van  $L_a^2 + L_b^2 = L_c^2$ .  A

# III

## Analyse

# 21 Zonder naam

We geven hier geen volledig overzicht van analytische getaltheorie, met bewijzen al zeker niet. Het doel van dit hoofdstuk is om de lezer vertrouwd te maken met enkele nieuwe notaties en enkele technieken aan te leren voor asymptotische afschattingen en deze toe te passen in gevarieerde oefeningen. Voor een meer diepgaande inleiding tot analytische getaltheorie verwijzen we naar [8]. Voor de volledigheid vermelden we wel enkele interessante resultaten die tot dusver zijn bewezen.

## 21.1 Zonder naam

Zoals eerder beloofd geven we Erdős' bewijs van het postulaat van Bertrand. Het grondidee van het bewijs is dat een bepaald getal, afhankelijk van  $n$  steeds een priemdelers moet hebben tussen  $n$  en  $2n$ , omdat andere priemdelers het getal nooit groot genoeg kunnen maken. Dit werkt helaas niet zomaar voor elk natuurlijk getal, maar Erdős kwam op het geniale idee om de centrale binomiaalcoëfficiënten te bestuderen.

### Definitie 21.1. Primoriaal

Voor een reëel getal  $x \geq 2$  definiëren we de *primoriaal* als het product van de priemgetallen kleiner of gelijk aan  $x$ . We noteren  $x\#$ .

Zo is  $6.99\# = 2 \cdot 3 \cdot 5$ ,  $2.5\# = 2$  en  $7\# = 2 \cdot 3 \cdot 5 \cdot 7$ .

### Lemma 21.2.

Er geldt dat  $x\# < 4^x$  voor alle  $x > 2$ .

### Opgave 21.3. Bewijs.

A. Toon aan dat het volstaat om alleen natuurlijke getallen  $x > 1$  te bekijken.

We bewijzen het nu via volledige inductie op  $x$ .

Basisstap. Voor  $x = 2$  is het eenvoudig te controleren.

Inductiestap. Veronderstel dat het waar is voor natuurlijke getallen kleiner dan  $x$ .

B. Toon aan dat ook  $x\# < 4^x$  als  $x$  even is.

Stel nu  $x = 2m + 1$  oneven.

C. Toon aan dat  $\binom{2m+1}{m} < 4^m$

D. Toon aan dat  $(2m + 1)\# < 4^m \cdot (m + 1)\#$ .

Wegens de inductiehypothese geldt nu  $(2m + 1)\# < 4^m \cdot 4^{m+1} = 4^{2m+1}$ .

**Opgave 21.4.** (Postulaat van Bertrand) Om te beginnen schatten we de centrale binomiaalcoëfficiënten af naar onder.

A. Toon aan dat

$$\frac{4^n}{2n} \leq \binom{2n}{n}$$

voor  $n > 0$ .

Vervolgens zoeken we een bovengrens voor machten van priemgetallen die de binomiaalcoëfficiënt delen. Noteer voor een priemgetal  $p$  en  $n \in \mathbb{N}$ ,  $R(p, n) = v_p \binom{2n}{n}$ .

B. Toon aan dat  $p^{R(p,n)} \leq 2n$ .

C. Toon aan dat  $R(p, n) = 0$  als  $\frac{2}{3}n < p \leq n$ .

We hebben nu genoeg bagage om het bewijs af te ronden. Veronderstel dat er een tegenvoorbeeld  $n$  is voor het postulaat van Bertrand.

D. Toon aan dat elke priemdelers  $p$  van  $\binom{2n}{n}$  voldoet aan  $p \leq \frac{2}{3}n$ .

E. Bewijs dat

$$\frac{4^n}{2n} < (2n)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n}.$$

Deze ongelijkheid is equivalent met  $n \cdot \frac{\ln 4}{3} < (\sqrt{2} + 1) \ln(2n)$ . Men kan nagaan dat de functie in het rechterlid concaaf is, zodat dit enkel geldt voor voldoende kleine waarden van  $n$ . Er blijkt dat de ongelijkheid niet meer geldt als  $n > 467$ . Een mogelijk tegenvoorbeeld moet dus kleiner zijn dan 468. Maar voor  $n < 468$  is het eenvoudig te controleren dat er geen tegenvoorbeelden zijn. Bijgevolg geldt het postulaat als bewezen.

#### Stelling 21.5. Priemgetalstelling

Er geldt dat  $\pi(n) \sim \frac{n}{\log n}$ .


#### Stelling 21.6. Stelling van Dirichlet, kwantitatieve vorm


Zij  $a, b \in \mathbb{N}^+$  met  $\text{ggd}(a, b) = 1$ . Dan is

$$\sum_{\substack{p \leq x \\ p \equiv b \pmod{a}}} \frac{1}{p} = \frac{1}{\varphi(a)} \ln \ln x + O_a(1).$$

In het bijzonder volgt hieruit, zoals eerder vermeld, dat er oneindig veel priemgetallen congruent met  $b$  modulo  $a$  zijn.

## Opgaven hoofdstuk 21

**Opgave 21.7.** Noteer met  $p_n$  het  $n$ de priemgetal. Bewijs dat  $p_n + p_{n+1} > p_{n+2}$  voor  $n \geq 2$ . 

**Opgave 21.8.** Vind alle natuurlijke oplossingen voor  $n! = 2^a - 2^b$ . 

**Opgave 21.9.** (PUMA 2015 Vraag 6) Noteer voor een natuurlijk getal  $n > 1$  met  $d_n$  de op een na grootste deler van  $n$ . Definieer de rij  $(a_n)$  door  $a_1 = 1$ ,  $a_2 = 0$  en

$$a_{n+1} = \frac{d_n^5 a_n + a_{d_n}}{d_n^5 + 1}$$

voor  $n \geq 2$ . Bewijs dat  $a_n \rightarrow 1$ .

### 22.1 Sommen van priemgetallen

**Vermoeden 22.1.** Sterk vermoeden van Goldbach

Elk even natuurlijk getal groter dan 2 is te schrijven als de som van twee priemgetallen.

**Vermoeden 22.2.** Zwak vermoeden van Goldbach

Elk oneven natuurlijk getal groter dan 7 is te schrijven als de som van drie priemgetallen.

De benaming is als volgt te verklaren:

**Opgave 22.3.** Toon aan dat het zwakke vermoeden van Goldbach volgt uit het sterke vermoeden.

**Stelling 22.4.** Vinogradov, 1937

Het zwakke vermoeden van Goldbach is geldig voor voldoende grote getallen. Meer bepaald is het aantal manieren waarop  $n$  kan worden geschreven als de som van drie priemgetallen  $\Omega(n^2/\log^3 n)$ .

**Stelling 22.5.** Borozdin

Het zwakke vermoeden van Goldbach is geldig voor getallen groter dan  $3^{3^{15}}$ .

**Stelling 22.6.** Helfgott, 2013

Het zwakke vermoeden van Goldbach is waar.

### 22.2 Priemhiaten



**Vermoeden 22.7.** Tweelingpriemvermoeden

Er zijn oneindig veel koppels priemgetallen  $p$  en  $q$  met  $q = p + 2$ .

**Vermoeden 22.8.** De Polignac, 1849

Voor elk even natuurlijk getal  $n$  zijn er oneindig veel priemhiaten gelijk aan  $n$ .

Merk op dat het niet veel zin heeft om te spreken over oneven priemhiaten.

**Stelling 22.9.** Zhang, 2013

Er is een natuurlijk getal  $n < 7 \cdot 10^7$  zo dat er oneindig veel priemhiaten gelijk zijn aan  $n$ .

**Stelling 22.10.** Polymath Project, 2014

Er is een natuurlijk getal  $n \leq 246$  zo dat er oneindig veel priemhiaten gelijk zijn aan  $n$ .

**Stelling 22.11.** Brun, 1915

De reeks (of som?)

$$\sum_p \frac{1}{p}$$

convergeert, waarbij de som loopt over de priemgetallen die lid zijn van een priem-tweeling. Meer bepaald is het aantal priemtweelingen kleiner dan  $n$  asymptotisch

$$O(n/\log^2 n).$$

## Opgaven hoofdstuk 22

**Opgave 22.12.** Aan welk bekend vermoeden link je de volgende uitspraak? *Elk natuurlijk getal groter dan 1 is het gemiddelde van twee (niet noodzakelijk verschillende) priemgetallen.* ❁

# Opgaven deel III

# Bijlagen

Hier vind je symbolen en formules die regelmatig worden gebruikt in de cursus. Je wordt verondersteld van die te kennen, maar voor wie er nog niet mee vertrouwd is, is er hier een kort overzicht. Indien je iets vreemds tegenkomt is de kans dus groot dat er hier een verklaring voor te vinden is.

### A.1 Sommatieteken

Een sommatieteken is een verkorte schrijfwijze van een som.

#### Notatie A.1.

Als  $f$  een functie is en  $a$  en  $b$  gehele getallen met  $a \leq b$ , noteren we

$$f(a) + f(a+1) + \cdots + f(b-1) + f(b)$$

verkort als

$$\sum_{k=a}^b f(k).$$

Hierbij noemen we  $k$  de index,  $a$  de ondergrens en  $b$  de bovengrens.

Bijvoorbeeld:

$$\sum_{k=-3}^5 k^2 = (-3)^2 + (-2)^2 + (-1)^2 + 0^2 + 1^2 + 2^2 + 3^2 + 4^2 + 5^2.$$

De letter  $k$  mag eventueel een andere letter zijn, zolang deze maar geen andere betekenis heeft in de context. De notatie

$$\sum_{b=a}^b f(b)$$

is dus fout: aangezien  $b$  al een betekenis heeft, mag die niet als index worden genomen. Als ondergrens of bovengrens kan ook oneindig worden genomen. Bijvoorbeeld:

$$\sum_{i=-\infty}^{-5} \frac{2}{i^2}.$$

## Eigenschappen A.2.

1. Je kan de grenzen veranderen als je ook de functie verandert. Bijvoorbeeld:

$$\sum_{k=a}^b f(k) = \sum_{k=a+1}^{b+1} f(k-1)$$

en

$$\sum_{k=a}^b f(k) = \sum_{k=0}^{b-a} f(a+k).$$

2. De distributieve eigenschap blijft behouden. Als  $c$  een getal is, onafhankelijk van  $k$ , dan is

$$\sum_{k=a}^b c \cdot f(k) = c \cdot \sum_{k=a}^b f(k).$$

3. Ook associativiteit blijft behouden. We kunnen de som

$$\sum_{k=a}^b (f(k) + g(k))$$

schrijven als

$$\sum_{k=a}^b f(k) + \sum_{k=a}^b g(k).$$

4. De commutativiteit blijft natuurlijk ook behouden. Een gevolg is dat we de index in omgekeerde richting kunnen laten lopen:

$$\sum_{k=a}^b f(k) = \sum_{k=a}^b f(a+b-k).$$

Enkele bekende sommen zijn

$$\sum_{a=1}^n a = \frac{n \cdot (n+1)}{2} \quad \text{en} \quad \sum_{k=1}^n k^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}.$$

Men hoeft niet steeds expliciet de onder- en bovengrens te noteren. Ook toegestaan is het sommeren over een verzameling. Als  $V = \{1, 2, 3\}$  is

$$\sum_{k \in V} k^2 = \sum_{k=1}^3 k^2.$$

Ook kan je extra voorwaarden onder of boven het sommatieteken schrijven. Meestal doet men dit onderaan, bijvoorbeeld

$$\sum_{\substack{-10 \leq a < 101 \\ a \text{ oneven} \\ a \neq 51}} f(a).$$

Wanneer de som leeg is, dan is de som bij afspraak gelijk aan 0. Een som kan leeg zijn als bijvoorbeeld de bovengrens kleiner is dan de ondergrens, of als de som van de elementen uit

een lege verzameling wordt genomen. Bijvoorbeeld,

$$\sum_{\substack{a=0 \\ a \text{ oneven} \\ \frac{a}{2} \in \mathbb{Z}}}^{456} f(a) = 0.$$

Een multiplicatieteken doet hetzelfde voor een product.

**Notatie A.3.**

Als  $f$  een functie is en  $a$  en  $b$  gehele getallen met  $a \leq b$ , noteren we

$$f(a) \cdot f(a+1) \cdots f(b-1) \cdot f(b)$$

als

$$\prod_{k=a}^b f(k).$$

Analoge eigenschappen gelden voor het product. Als het product leeg is, dan is het bij afspraak gelijk aan 1.

## A.2 Discrete functies

**Definitie A.4. Faculteit**

De *faculteit* van een natuurlijk getal  $n \in \mathbb{N}^+$  is het product van alle natuurlijke getallen in  $\{1, \dots, n\}$ . We noteren

$$n! = \prod_{k=1}^n k.$$

We definiëren ook  $0! = 1$ .

Bijvoorbeeld:  $2! = 2$ ,  $4! = 24$ ,  $5! = 120$ .

**Definitie A.5. Binomiaalcoëfficiënt**

De *binomiaalcoëfficiënt*

$$\binom{a}{b}$$

met  $a, b \in \mathbb{N}$  en  $b \leq a$  is een rationaal getal gelijk aan

$$\frac{a!}{b! \cdot (a-b)!}.$$

Bijvoorbeeld:  $\binom{3}{2} = 3$ ,  $\binom{7}{5} = 15$ ,  $\binom{1}{0} = 1$ .

**Eigenschap A.6.**

Er is symmetrie:

$$\binom{a}{b} = \binom{a}{a-b}.$$

**Eigenschap A.7. Formule van Stifel-Pascal**

Voor alle  $a, b \in \mathbb{N}$  met  $b \leq a$  is

$$\binom{a}{b} + \binom{a+1}{b} = \binom{a+1}{b+1}.$$

Het bewijs van deze identiteit is niet meer dan een rechtstreekse verificatie.

**Eigenschap A.8.**

Als  $a, b \in \mathbb{N}$  met  $b \leq a$  is  $\binom{a}{b} \in \mathbb{N}$ .

*Bewijs.*

Via inductie op de som  $a + b$ . Als  $a + b = 0$  klopt het: dan is  $a = b = 0$  en dus  $\binom{a}{b} = 1 \in \mathbb{N}$ . Stel dat het waar is voor alle sommen kleiner dan  $s$  en zij  $a + b = s$  met  $b \leq a$ . Als  $a = 0$  of  $b = 0$  volgt het gestelde rechtstreeks uit de definitie. Als  $a, b > 1$  is  $\binom{a}{b} = \binom{a}{b-1} + \binom{a-1}{b-1} \in \mathbb{N}$  wegens de inductiehypothese voor  $s - 1$  en  $s - 2$ .  $\square$

**B.1 Ontbindingen****Stelling B.1.** Binomium van Newton

Het binomium van Newton geeft een algemene uitwerking van  $(a + b)^n$  met  $n \in \mathbb{N}$ ,

$$(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

als  $a + b \neq 0$ .

Bijvoorbeeld,

$$(a + b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$$

en

$$(a - 1)^5 = a^5 - 5a^4 + 10a^3 - 10a^2 + 5a - 1.$$

**Stelling B.2.**

Voor  $n \in \mathbb{N}$  en  $a, b \in \mathbb{R}_0$  geldt

$$a^n - b^n = (a - b) \cdot \sum_{k=0}^{n-1} a^k b^{n-k-1}.$$

Bijvoorbeeld,

$$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4)$$

en

$$a^3 - 2^3 = (a - 2)(a^2 + 2a + 4).$$

**B.2 Inclusie-exclusie**

Zij  $A_1, A_2, \dots, A_n$  eindige verzamelingen. Het inclusie-exclusieprincipe geeft een algemene formule om het aantal elementen in de unie  $A_1 \cup A_2 \cup \dots \cup A_n$  te tellen, in functie van het aantal elementen in de doorsnedes, zoals  $A_1 \cap A_2, A_2 \cap A_n, A_1 \cap A_2 \cap A_3, A_2 \cap \dots \cap A_n$ , enzovoort. Vaak is het veel eenvoudiger om het aantal elementen in de doorsnede van verzamelingen te tellen, en dan biedt inclusie-exclusie een handige uitweg.

We bekijken het geval  $n = 2$ :



**Stelling B.3.**

Als  $A_1$  en  $A_2$  eindig zijn, dan is  $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ .

*Bewijs.*

We tellen het aantal elementen van  $A_1 \cup A_2$ . Dat doen we door het aantal elementen van  $A_1$  op te tellen bij het aantal elementen van  $A_2$ . We moeten hier het aantal elementen dat we tweemaal hebben geteld van aftrekken, dat is  $|A_1 \cap A_2|$ . Dus  $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ .

□

**Stelling B.4. Veralgemeend inclusie-exclusieprincipe**

Zij  $A_1, \dots, A_n$  eindige verzamelingen. Dan is

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{k=1}^n (-1)^{k+1} \alpha_k$$

waarbij

$$\alpha_k = \sum_{\substack{S \subseteq \mathbb{N}^+ \\ |S|=k \\ |S| \leq n}} \left| \bigcap_{l \in S} A_l \right|.$$

*Bewijs.*

Via inductie op  $|\bigcup_{k=1}^n A_k|$ . Voor  $|\bigcup_{k=1}^n A_k| = 0$  is het duidelijk, dan zijn alle  $A_k$  leeg en is ook het rechterlid nul. Veronderstel dat het waar is voor  $|\bigcup_{k=1}^n A_k| = m$ , we bewijzen het voor  $m + 1$ . Zij willekeurig  $x \in \bigcup_{k=1}^n A_k$ . Veronderstel dat  $x$  tot precies  $p$  verzamelingen  $A_k$  behoort. Stel  $B_k = A_k \setminus \{x\}$ , zodat  $|\bigcup_{k=1}^n B_k| = m$  en de inductiehypothese leert dat

$$|B_1 \cup B_2 \cup \dots \cup B_n| = \sum_{k=1}^n (-1)^{k+1} \beta_k$$

met

$$\beta_k = \sum_{\substack{S \subseteq \{1, 2, \dots, n\} \\ |S|=k}} \left| \bigcap_{l \in S} B_l \right|.$$

Stel analoog

$$\alpha_k = \sum_{\substack{S \subseteq \{1, 2, \dots, n\} \\ |S|=k}} \left| \bigcap_{l \in S} A_l \right|.$$

Merk op dat  $|A_1 \cup A_2 \cup \dots \cup A_n| = 1 + |B_1 \cup B_2 \cup \dots \cup B_n|$ . Als we kunnen aantonen dat

$$\sum_{k=1}^n (-1)^{k+1} \alpha_k = 1 + \sum_{k=1}^n (-1)^{k+1} \beta_k$$

is de inductiestap voltooid.

Nu is  $\alpha_k = \binom{p}{k} + \beta_k$  voor  $k \leq p$  en  $\alpha_k = \beta_k$  voor  $k > p$ , dus

$$\begin{aligned} \sum_{k=1}^n (-1)^{k+1} \alpha_k &= \sum_{k=1}^p (-1)^{k+1} \binom{p}{k} + \sum_{k=1}^n (-1)^{k+1} \beta_k \\ &= 1 + \sum_{k=1}^n (-1)^{k+1} \beta_k. \end{aligned}$$

□

Een alternatief maar omslachtiger bewijs gaat via inductie op het aantal verzamelingen.<sup>29</sup> Het is echter veel intuïtiever en kan als verklaring dienen voor de factor  $(-1)^{k+1}$  die in de som optreedt.

*Bewijs.*

Via inductie op het aantal verzamelingen  $n$ . We weten al dat de stelling geldt voor  $n = 2$ , veronderstel dat de stelling geldt voor  $n = 2, \dots, n = m$ , we bewijzen dat het ook waar is voor  $n = m + 1$ . Er geldt dat

$$\left| \bigcup_{k=1}^{m+1} A_k \right| = \left| A_{m+1} \cup \bigcup_{k=1}^m A_k \right|.$$

Wegens de inductiehypothese voor  $n = 2$  is

$$\begin{aligned} \left| \bigcup_{k=1}^{m+1} A_k \right| &= |A_{m+1}| + \left| \bigcup_{k=1}^m A_k \right| - \left| A_{m+1} \cap \bigcup_{k=1}^m A_k \right| \\ &= |A_{m+1}| + \left| \bigcup_{k=1}^m A_k \right| - \left| \bigcup_{k=1}^m (A_{m+1} \cap A_k) \right|. \end{aligned}$$

Stel  $B_k = A_{m+1} \cap A_k$ . Noteer

$$\alpha_{k,n} = \sum_{\substack{S \subseteq \{1,2,\dots,n\} \\ |S|=k}} \left| \bigcap_{l \in S} A_l \right|$$

en analoog

$$\beta_{k,n} = \sum_{\substack{S \subseteq \{1,2,\dots,n\} \\ |S|=k}} \left| \bigcap_{l \in S} B_l \right|$$

voor natuurlijke getallen  $k, n$  met  $k \leq n$ .

Door de inductiehypothese voor  $n = m$  toe te passen op de doorsneden  $\bigcup_{k=1}^m A_k$  en  $\bigcup_{k=1}^m B_k$  geldt

$$\left| \bigcup_{k=1}^{m+1} A_k \right| = |A_{m+1}| + \sum_{k=1}^m (-1)^{k+1} \alpha_{k,m} - \sum_{k=1}^m (-1)^{k+1} \beta_{k,m}.$$

<sup>29</sup>Een voordeel hiervan is dat het zich laat veralgemenen tot willekeurige maten  $\mu$ , juist omdat er nergens wordt verwezen naar het aantal elementen van de betrokken verzamelingen. Het volstaat dan om  $|A|$  telkens te vervangen door  $\mu(A)$ .

Er geldt

$$\begin{aligned}
(-1)^{k+2} \alpha_{k+1,m} - (-1)^{k+1} \beta_{k,m} &= (-1)^{k+2} \left( \sum_{\substack{S \subseteq \mathbb{N}_{\leq m} \\ |S|=k+1}} \left| \bigcap_{l \in S} A_l \right| + \sum_{\substack{S \subseteq \mathbb{N}_{\leq m} \\ |S|=k}} \left| \bigcap_{l \in S} (A_{m+1} \cap A_l) \right| \right) \\
&= (-1)^{k+2} \left( \sum_{\substack{S \subseteq \{1, \dots, m+1\} \\ |S|=k+1 \\ m+1 \notin S}} \left| \bigcap_{l \in S} A_l \right| + \sum_{\substack{S \subseteq \{1, 2, \dots, m+1\} \\ |S|=k+1 \\ m+1 \in S}} \left| \bigcap_{l \in S} A_l \right| \right) \\
&= (-1)^{k+2} \sum_{\substack{S \subseteq \{1, \dots, m+1\} \\ |S|=k+1}} \left| \bigcap_{l \in S} A_l \right| \\
&= (-1)^{k+2} \alpha_{k+1,m+1}
\end{aligned}$$

zodat

$$\begin{aligned}
\left| \bigcup_{k=1}^{m+1} A_k \right| &= |A_{m+1}| + \sum_{k=1}^m (-1)^{k+1} \alpha_{k,m} - \sum_{k=1}^m (-1)^{k+1} \beta_{k,m} \\
&= |A_{m+1}| + \alpha_{1,m} + \sum_{k=1}^m \left( (-1)^{k+2} \alpha_{k+1,m} - (-1)^{k+1} \beta_{k,m} \right) \\
&= \alpha_{1,m+1} + \sum_{k=1}^m (-1)^{k+2} \alpha_{k+1,m+1} \\
&= \sum_{k=1}^{m+1} (-1)^{k+1} \alpha_{k,m+1}.
\end{aligned}$$

□

Merk op dat er nergens in het bewijs gebruik werd gemaakt van het binomium van Newton.

### B.3 Ongelijkheden

#### Stelling B.5. Machtsgemiddelde

Als  $a_1, \dots, a_n \geq 0$  reële getallen zijn en  $p, q \in \mathbb{R}_0$  met  $p < q$ , is

$$\left( \frac{a_1^p + \dots + a_n^p}{n} \right)^{\frac{1}{p}} \leq \left( \frac{a_1^q + \dots + a_n^q}{n} \right)^{\frac{1}{q}}$$

waarbij gelijkheid enkel optreedt als  $a_1 = a_2 = \dots = a_n$ .

**Stelling B.6.**

Als  $a_1, \dots, a_n \geq 0$  reële getallen zijn geldt dat

$$\lim_{p \rightarrow 0} \left( \frac{a_1^p + \dots + a_n^p}{n} \right)^{\frac{1}{p}} = \sqrt[p]{a_1 \cdots a_n}.$$

Voor  $p < 0$  is

$$\left( \frac{a_1^p + \dots + a_n^p}{n} \right)^{\frac{1}{p}} \leq \sqrt[p]{a_1 \cdots a_n}$$

met gelijkheid als en slechts als  $a_1 = a_2 = \dots = a_n$ . De omgekeerde ongelijkheid geldt als  $p > 0$ .

In het bijzonder hebben we:

**Stelling B.7. HM-GM-AM-QM**

Als  $a_1, \dots, a_n \geq 0$  reële getallen zijn, is

$$\frac{n}{\frac{1}{a_1} + \dots + \frac{1}{a_n}} \leq \sqrt[n]{a_1 \cdots a_n} \leq \frac{a_1 + \dots + a_n}{n} \leq \sqrt{\frac{a_1^2 + \dots + a_n^2}{n}}$$

waarbij gelijkheid enkel optreedt als  $a_1 = a_2 = \dots = a_n$ .

**Stelling B.8. Ongelijkheid van Cauchy-Schwarz**

Als  $x_1, \dots, x_n$  en  $y_1, \dots, y_n$  reële getallen zijn, is

$$(x_1 y_1 + \dots + x_n y_n)^2 \leq (x_1^2 + \dots + x_n^2)(y_1^2 + \dots + y_n^2)$$

met gelijkheid als en slechts als er  $c, d \in \mathbb{R}$  bestaan waarvoor  $cx_k = dy_k$  voor alle  $k$ .

**B.4 Lineaire recursies****Definitie B.9. Lineaire homogene recursie**

Indien een complexe rij  $(a_n)_{n \in \mathbb{N}}$  recursief gedefinieerd is door

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \dots + c_k a_{n-k} \quad (n \geq k)$$

met  $c_1, \dots, c_k$  complexe constanten en met  $a_0, \dots, a_{k-1}$  gegeven, dan noemen we dit een *lineaire homogene recursie*.

**Definitie B.10.** Karakteristieke veelterm

De karakteristieke veelterm van de recursie  $a_n = c_1 a_{n-1} + \dots + c_k a_{n-k}$  is de veelterm

$$\chi(x) = x^k - c_1 x^{k-1} - \dots - c_{k-1} x - c_k.$$

**Stelling B.11.**

Gegeven een recursiebetrekking  $a_n = c_1 a_{n-1} + \dots + c_k a_{n-k}$  met karakteristieke veelterm  $\chi$ . Als  $\lambda_1, \dots, \lambda_r$  de wortels zijn van  $\chi$  met multipliciteit  $m_1, \dots, m_r$ , dan worden  $k$  oplossingen van de homogene lineaire recursie gegeven door

$$\lambda_1^n, n\lambda_1^n, \dots, n^{m_1-1}\lambda_1^n, \dots, \lambda_r^n, n\lambda_r^n, \dots, n^{m_r-1}\lambda_r^n,$$

Elke oplossing van de recursie is een lineaire combinatie van deze oplossingen.

We geven als voorbeeld de rij van Fibonacci.

**Definitie B.12.** Rij van Fibonacci

De rij van Fibonacci definiëren we met  $F_0 = 0$ ,  $F_1 = 1$  en  $F_n = F_{n-1} + F_{n-2}$  als  $n \geq 2$ .

**Stelling B.13.**

De rij van Fibonacci heeft als expliciete oplossing

$$F_n = \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \sqrt{5}}.$$

*Bewijs.*

De karakteristieke veelterm is  $x^2 - x - 1$ . De wortels zijn  $\lambda_1 = \frac{1+\sqrt{5}}{2}$  en  $\lambda_2 = \frac{1-\sqrt{5}}{2}$ . De expliciete formule voor  $F_n$  is dus van de vorm

$$c\lambda_1^n + d\lambda_2^n.$$

We vinden  $c$  en  $d$  door invullen van  $n = 0, 1$  en te eisen dat  $F_0 = 0$  en  $F_1 = 1$ . Enig rekenwerk levert  $c = \frac{1}{\sqrt{5}}$  en  $d = \frac{-1}{\sqrt{5}}$ . Hieruit volgt de formule.  $\square$

**B.5 Varia**

**Stelling B.14.** Lagrange-interpolatie

Gegeven complexe getallen  $x_1, \dots, x_n$  en  $y_1, \dots, y_n$  zo dat de  $x_k$  allemaal verschillend zijn, dan is de veelterm

$$L(x) = \sum_{k=1}^n y_k \prod_{\substack{l=1 \\ l \neq k}}^n \frac{x - x_l}{x_k - x_l}$$

de unieke veelterm van graad  $n - 1$  waarvoor  $L(x_1) = y_1, \dots, L(x_n) = y_n$ .

## C

## Complexe getallen

*Life is complex. It has real and imaginary parts.*

(Rich Rosen)

**Definitie C.1.** Complex getal

Een *complex getal* wordt formeel gedefinieerd als een koppel reële getallen  $(x, y)$ . We noteren  $\mathbb{C}$  voor de verzameling van complexe getallen. Het complex getal  $(x, y)$  noteert men ook met  $x + yi$ .

**Definitie C.2.** Reël en imaginair deel

Het *reël deel* en *imaginair deel* van een complex getal definiëren we met

$$\Re(x + yi) = x \quad \text{en} \quad \Im(x + yi) = y.$$

Dit laat ons toe gelijkheid te definiëren voor complexe getallen.

**Definitie C.3.** Gelijkheid van complexe getallen

Twee complexe getallen zijn gelijk als hun reël en imaginair deel gelijk zijn.

**Definitie C.4.**

We definiëren de som en het product van twee complexe getallen  $z_1 = x_1 + y_1i$  en  $z_2 = x_2 + y_2i$  als

$$z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i \quad \text{en} \quad z_1 \cdot z_2 = (x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)i.$$

Informeel gezegd erven complexe getallen de optelling en vermenigvuldiging uit  $\mathbb{R}$  over, als men daar de rekenregel  $i^2 = -1$  aan toevoegt. We zullen vanaf nu een reël getal  $x$  identificeren met het complex getal  $x + 0i$ .

**Stelling C.5.** Polaire gedaante van complexe getallen

Voor een complex getal  $z = x + yi \neq 0$  bestaat er een unieke  $r \in \mathbb{R}^+$  en een unieke  $\theta \in [0, 2\pi[$  waarvoor

$$z = r(\cos \theta + i \sin \theta).$$

$r$  noemt men de *modulus* en  $\theta$  de *poolhoek* of het *argument*. De modulus noteren we met  $r = |z|$ , het argument met  $\arg z$ .

**Gevolg C.6.**

Er geldt dat  $|x + yi| = \sqrt{x^2 + y^2}$ .

Voor reële getallen is de modulus dus gewoon de absolute waarde.

**Gevolg C.7.**

Twee complexe getallen zijn gelijk als en slechts als hun moduli gelijk zijn en, indien de modulus niet 0 is, hun poolhoeken gelijk zijn.

**Stelling C.8.**

Als  $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$  en  $z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$  is

$$z_1 z_2 = r_1 r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)),$$

en als  $z_2 \neq 0$  is bovendien

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} (\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)).$$

**Definitie C.9.**

Voor een complex getal  $x + yi$  definieert men

$$e^{x+yi} = e^x (\cos y + i \sin y)$$

waarbij  $e$  het getal van Euler is.

Bijvoorbeeld,  $e^{\pi i} = -1$ .

**Gevolg C.10. Formule van De Moivre**

Er geldt voor  $n \in \mathbb{N}$  en  $y \in \mathbb{R}$  dat

$$(e^{yi})^n = e^{nyi}$$

of dus

$$(\cos y + i \sin y)^n = \cos ny + i \sin ny.$$

**Stelling C.11.**

Als  $z = e^{a+bi}$  niet 0 is en  $n \in \mathbb{N}^+$  dan heeft de vergelijking  $x^n = z$  precies  $n$  oplossingen. Alle oplossingen zijn van de vorm

$$e^{\frac{a}{n} + \frac{1}{n}(b+k2\pi)i}$$

met  $k \in \{0, \dots, n-1\}$ .



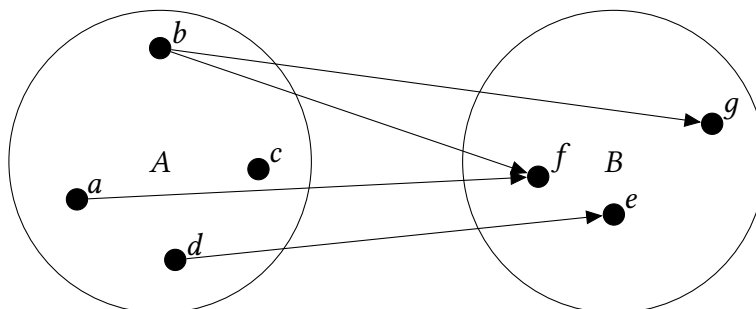
## D.1 Binaire relaties

Intuïtief is een relatie een ‘object’ gedefinieerd over vaste verzamelingen en het ‘verbindt’ elementen uit die verzamelingen. Een strenge definitie gaat als volgt:

**Definitie D.1.** Relatie

Een binaire relatie  $R$  is een tuple  $R = (G, A, B)$  waarbij  $A$  en  $B$  verzamelingen zijn en  $G \subseteq A \times B$ .  $G$  noemen we de grafiek,  $A$  en  $B$  de domeinen. Als  $(a, b) \in G$  zeggen we dat “ $a$  in relatie staat tot  $b$ ” en we noteren  $aRb$ . Indien  $A = B$  zeggen we ook “ $R$  is een binaire relatie op  $A$ ”.

Vaak identificeert men  $R$  met  $G$ . We zullen voortaan het woord ‘binair’ weglaten en kortweg van een relatie spreken. Een relatie wordt typisch afgebeeld met een pijlenvoorstelling. We tekenen een pijl van  $a$  naar  $b$  als  $aRb$ .

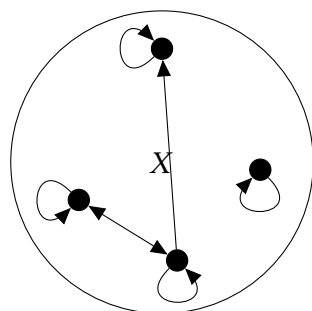


$A = \{a, b, c, d\}$  en  $B = \{e, f, g\}$  zijn hier de domeinen, en  $G = \{(a, f), (b, g), (b, f), (d, e)\}$  is de grafiek.

**Definitie D.2.** Reflexieve relatie

Een relatie  $R$  gedefinieerd op  $X$  is *reflexief* als  $\forall x \in X : xRx$ .

Bijvoorbeeld,  $\geq$ ,  $\leq$ ,  $=$  zijn reflexieve relaties op  $\mathbb{R}$  en  $|$  is een reflexieve relatie op  $\mathbb{Z}$ . De pijlenvoorstelling van een reflexieve relatie kan er bijvoorbeeld als volgt uitzien:

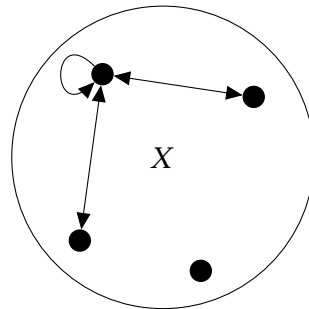


Het enige dat van belang is, is dat elk element een pijl heeft die naar zichzelf terugkeert.

**Definitie D.3.** Symmetrische relatie

Een relatie  $R$  op  $X$  is *symmetrisch* als  $\forall x, y \in X : xRy \Leftrightarrow yRx$ .

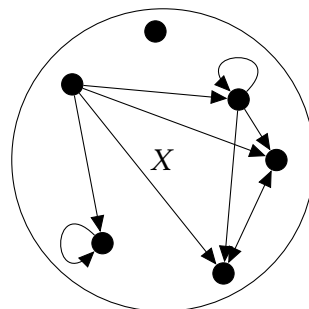
De oorsprong van het woord ‘symmetrisch’ spreekt voor zich. Een voorbeeld is  $aRb \Leftrightarrow |a - b| < 5$  (gedefinieerd op bijvoorbeeld  $\mathbb{R}$ ). In de voorstelling is een pijl tussen verschillende elementen ofwel afwezig, ofwel wijst hij in beide richtingen:



**Definitie D.4.** Transitieve relatie

Een relatie  $R$  op  $X$  is *transitief* als  $\forall x, y, z \in X : xRy \wedge yRz \Rightarrow xRz$ .

Typische transitieve relaties zijn  $\geq$  en  $\leq$  op  $\mathbb{R}$ , of  $|$  op  $\mathbb{Z}$ . Een voorbeeld van een mogelijke pijlenvoorstelling:

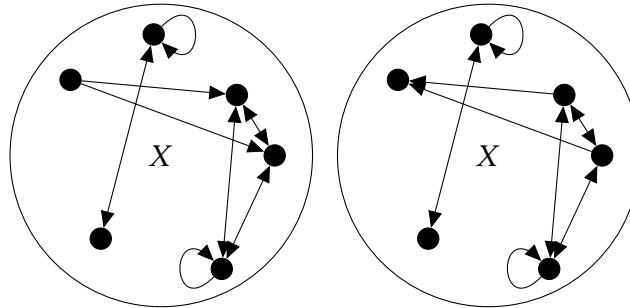


In deze context kan het interessant zijn om ook de Euclidische relaties te vermelden, maar voor de opbouw tot de stelling van Lagrange zijn ze geenszins van belang.

**Definitie D.5.** Euclidische relatie

Een relatie  $R$  op  $X$  is *rechts-Euclidisch* als  $\forall x, y, z \in X : xRy \wedge xRz \Rightarrow yRz$ .  $R$  is *links-Euclidisch* als  $\forall x, y, z \in X : yRx \wedge zRx \Rightarrow yRz$ .

Mogelijke pijlenvoorstellingen van een rechts- en links-euclidische relatie zijn respectievelijk:



Merk op dat we, door bij een rechts-Euclidische relatie de pijlen om te draaien, een links-Euclidische relatie bekomen.

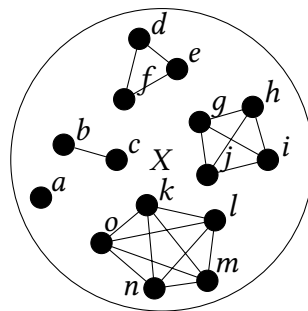
**Opgave D.6.** Bewijs dat een relatie  $R$  op  $X$  zowel links- als rechts-Euclidisch is als en slechts als  $R$  symmetrisch en transitief is.

**D.1.1** Equivalentierelaties

**Definitie D.7.** Equivalentierelatie

Een relatie  $R$  op  $X$  is een *equivalentierelatie* als  $R$  reflexief, symmetrisch en transitief is.

Een mogelijke pijlenvoorstelling:



Hierbij moeten alle lijnen wel een dubbele pijl hebben, en om de tekening overzichtelijk te houden hebben we de pijlen van de elementen naar zichzelf weggelaten.

Opmerkelijk in dit voorbeeld is dat de elementen gegroepeerd zijn, en dat binnen zo'n groepje alle elementen in relatie staan tot elkaar. Toeval?

**Definitie D.8.** Equivalentieklasse

Als  $x \in X$  en  $R$  is een relatie op  $X$ , dan noemen we de verzameling  $[x]_R = \{y \in X : yRx\}$  de *equivalentieklasse van  $x$  onder  $R$* .

Vaak zullen we gewoon  $[x]$  schrijven in plaats van  $[x]_R$  als het duidelijk is wat we bedoelen. In het voorbeeld hierboven is bijvoorbeeld  $[i] = \{g, h, i, j\}$  en  $[a] = \{a\}$ .

**Lemma D.9.**

Zij  $R$  een equivalentierelatie op  $X$ . Dan gelden:

1.  $x \in [x]$ .
2. Als  $xRy$ , dan is  $[x] = [y]$ .
3. Voor alle  $x, y, z \in X$  geldt dat als  $x \in [y]$  en  $x \in [z]$ , dan  $[y] = [z]$ . Anders gezegd, elk element zit in precies één equivalentieklasse.
4. Als  $x, y, z \in X$  en  $x, y \in [z]$ , dan is  $xRy$ .

*Bewijs.*

Als oefening. □

Een equivalentierelatie geeft aanleiding tot een zogenaamde *quotiëntverzameling*.

**Definitie D.10.** Quotiëntverzameling

Als  $R$  een equivalentierelatie is op  $X$ , dan noemen we  $X/R = \{[x] : x \in X\}$  de *quotiëntverzameling van  $X$  onder  $R$* .

**Lemma D.11.**

Zij  $R$  een equivalentierelatie op  $X$ . Dan is  $X/R$  een partitie van  $X$ .

*Bewijs.*

Als oefening. □

Dit is precies het patroon dat we voorspeld hadden: een equivalentierelatie op  $X$  deelt de elementen van  $X$  op in groepjes, equivalentieklassen, op zo'n manier dat de equivalentieklassen een partitie vormen van  $X$ . Uit het laatste puntje van het vorige lemma weten we dat binnen zo'n groepje alle elementen met elkaar in relatie staan.

Een interessant tussenresultaat, maar niet van belang voor de stelling van Langrange is het volgende.

**Stelling D.12.** Hoofdstelling van equivalentierelaties

Zij  $X$  een niet-lege verzameling. Dan is de afbeelding die  $R$  afbeeldt op  $X/R$  een bijectie van de equivalentierelaties op  $X$  naar de partities van  $X$ .

In het bijzonder weten we hieruit dat als  $X$  eindig is, het aantal equivalentierelaties gelijk is aan het aantal partities.

**Opgave D.13.** (Hoofdstelling van equivalentierelaties) Definieer voor elke partitie  $P$  de relatie  $R_P$  op  $X$  met  $xR_P y \Leftrightarrow \exists K \in P : x, y \in K$ .

- A. Toon aan dat, voor elke partitie  $P$ ,  $R_P$  een equivalentierelatie is op  $X$ .
- B. Bewijs dat als  $x \in K \in P$ , dan  $K = [x]_{R_P}$ .
- C. Toon aan dat  $P = X/R_P$ .

Bijgevolg is de afbeelding  $R \mapsto X/R$  surjectief.

- D. Bewijs dat ze ook injectief is.

Bijgevolg is ze bijectief.

## D.2 Groepen

## D.3 Nevenklassen

**Definitie D.14.** Nevenklasse

Zij  $G$  een groep,  $H \leq G$  en  $g \in G$ , dan noemen we  $gH = \{gh : h \in H\}$  een *linkse nevenklasse van  $H$  in  $G$* . Analoog noemen we  $Hg = \{hg : h \in H\}$  een *rechtse nevenklasse van  $H$  in  $G$* .

**Notatie D.15.**

De verzameling van alle linkernevenklassen van een deelgroep  $H$  van  $G$  noteren we als  $G/H$ . Analoog noteren we  $G \setminus H = \{Hg : g \in G\}$ .

**Opgave D.16.** Bewijs dat voor een deelgroep van een abelse groep de linkse en rechtse nevenklassen gelijk zijn.

## D.4 De stelling van Lagrange

**Stelling D.17.** Stelling van Lagrange voor eindige groepen

Zij  $G$  een eindige groep en  $H \leq G$ . Dan is  $\frac{|G|}{|H|} = |G/H| = |G \setminus H|$ . In het bijzonder is  $|H|$  een deler van  $|G|$ .

**Opgave D.18.** (Stelling van Lagrange) Definieer de relatie  $R$  op  $G$  met  $aRb \Leftrightarrow \exists h \in H : a = bh$ .

A. Toon aan dat  $R$  een equivalentierelatie is.

B. Toon aan dat voor elke  $g \in G$ ,  $gH$  de equivalentieklasse is van  $g$  in  $G$  onder  $R$ .

Bijgevolg is  $G/R = G/H$ . Noem  $H_1, \dots, H_n$  de nevenklassen van  $H$ .

C. Bewijs dat  $\sum_{k=1}^n |H_k| = |G|$ .

D. Bewijs dat  $|H_k| = |H|$  voor  $k = 1, \dots, n$ .

Bijgevolg is  $|G| = n \cdot |H|$ . Een analoge redenering voor rechtse nevenklassen leert dat het aantal rechtse nevenklassen ook gelijk is aan  $\frac{|G|}{|H|}$ .

**Definitie D.19.** Index

Als  $G$  een eindige groep is en  $H \leq G$  noteren we  $[G : H] = \frac{|G|}{|H|}$  en noemen dit de *index van  $H$  in  $G$* .

# Hints

## Inleiding

**Hint 0.17.** **Blz. 13**  
 $\lceil x \rceil = - \lfloor -x \rfloor$

**Hint 0.19.** **Blz. 13**  
Voor  $z \in \mathbb{Z}$  is  $\lfloor x + z \rfloor = \lfloor x \rfloor + z$ . Sta vooral niet te lang stil bij wat ongeloofwaardig is.

## 1. Deelbaarheid

**Hint 1.15.** **Blz. 18**  
 $|b| = |-|b|$

**Hint 1.33.** **Blz. 23**  
Dit kan volledig analoog als de gewone stelling van Bézout.

**Hint 1.47.** **Blz. 27**  
 $10 \cdot (9! - 1) = 10! - 10$ .

**Hint 1.52.** **Blz. 27**  
Zoek gepaste lineaire combinaties van  $a + b$  en  $a - b$ .

**Hint 1.56.** **Blz. 27**  
Toon aan dat de twee getallen delers van elkaar zijn.

## 2. Priemgetallen

**Hint 2.20.** **Blz. 32**  
Werk analoog aan het bewijs van het vorige lemma.

**Hint 2.46.** **Blz. 36**  
 $\varphi(n)$  is even voor  $n > 2$ .

**Hint 2.52.** **Blz. 37**  
Kies  $a \in \mathbb{N}$  zo dat je de vergelijking  $a = n^2 + p$  handig kan herschrijven.

**Hint 2.55.** **Blz. 37**  
Schrijf  $a$  en  $b$  met hun priemontbinding.

**Hint 2.59.** **Blz. 37**

$\frac{p(n)}{n}$  is steeds van de vorm  $\frac{1}{2^a}$ . Tel voor elke  $a$  hoeveel keer  $\frac{1}{2^a}$  voorkomt.

**Hint 2.61.** **Blz. 38**

De kleinste deler is 1, de op-een-na kleinste is een priemgetal. Maak gevalsonderscheid voor de volgende twee delers.

**Hint 2.64.** **Blz. 38**

Telescoop.

**Hint 2.65.** **Blz. 38**

Bepaal het aantal koppels m.b.v. de priemontbinding van  $n$ . Je zou er dan  $\tau(n^2)$  in moeten herkennen.

**Hint 2.66.** **Blz. 38**

Vind geschikte lineaire combinaties.

**Hint 2.67.** **Blz. 38**

Let op het aantal factoren 2.

**Hint 2.68.** **Blz. 38**

Let op het aantal factoren 2.

### 3. Talstelsels

**Hint 3.11.** **Blz. 42**

A. Maak gebruik van de representatie uit de vorige stelling.

B. Beschouw de eerste index waarop de representaties verschillen. Toon aan dat de representatie met de grootste waarde op die index strikt groter is dan de andere.

### 4. Ad-hocmethodes voor diophantische vergelijkingen

**Hint 4.2.** **Blz. 44**

$$a^2 - 1$$

**Hint 4.3.** **Blz. 44**

$$ab - a - b + 1$$

**Hint 4.5.** **Blz. 45**

$$a^n - b^n$$

**Hint 4.7.** **Blz. 45**

$$a^n + b^n$$

**Hint 4.29.** **Blz. 49**



Ontbind.

**Hint 4.30.**

**Blz. 49**

Ontbind.

**Hint 4.31.**

**Blz. 49**

Er zijn meerdere manieren om de vergelijking  $p^2 + 7pq + q^2 = n^2$  in de vorm  $a^2 - b^2 = \dots$  te schrijven. Probeer op de plaats van de puntjes zo weinig mogelijk (priem)factoren te krijgen.

**Hint 4.32.**

**Blz. 49**

Ontbind.

**Hint 4.35.**

**Blz. 49**

$d_i \geq i$ .

**Hint 4.36.**

**Blz. 49**

Vervolledig de kwadraten.

**Hint 4.41.**

**Blz. 49**

Toon aan dat  $4 \mid n$ .

## 5. Dirichlet-convolutie

**Hint 5.35.**

**Blz. 58**

A.  $d \in S_n \Leftrightarrow n/d \in S_n$  is duidelijk een voldoende voorwaarde. Kies  $f$  en  $g$  zo dat blijkt dat ze ook nodig is.

B. Toon eerst aan dat het neutraal element noodzakelijk  $\varepsilon$  is.

C. We willen

$$(f *_S (g *_S h))(n) = \sum_{d \in S_n} \sum_{e \in S_{n/d}} f(d)g(e)h(n/de) = \sum_{d \in S_n} \sum_{e \in S_d} f(e)g(d/e)h(n/d) = ((f *_S g) *_S h)(n)$$

Kies  $f, g, h$  goed om aan te tonen dat dit equivalent is met

$$\{(d, e) : d \in S_n, e \in S_{n/d}\} = \{(e, d/e) : d \in S_n, e \in S_d\}.$$

Besluit. (Zie de antwoorden voor alternatieve formuleringen van het resultaat.)

**Hint 5.46.**

**Blz. 60**

Beide leden zijn multiplicatief.

## 6. Intermezzo: low-budget ggd calculus

**Hint 6.3.** **Blz. 62**

Als  $d$  en  $e$  ggd's zijn, geldt  $d \mid e$  en  $e \mid d$ ...

**Hint 6.21.** **Blz. 66**

Werk de haakjes uit zoals eerder; gebruik eventueel inductie.

**Hint 6.23.** **Blz. 67**

De meest elegante methode is waarschijnlijk via inductie op  $m + n$ ...

## 7. Modulorekenen

**Hint 7.12.** **Blz. 70**

Modulo 9 is  $10 \equiv 1$ .

**Hint 7.13.** **Blz. 70**

Modulo  $a - b$  is  $a \equiv b$ .

**Hint 7.35.** **Blz. 75**

$\text{ggd}(n, n + 1) = 1$

**Hint 7.67.** **Blz. 82**

Werk modulo 9 en 11.

**Hint 7.68.** **Blz. 82**

Let vooral op deelbaarheid door 3 en 11.

**Hint 7.77.** **Blz. 82**

Telescoop.

**Hint 7.90.** **Blz. 83**

Werk modulo 19.

## 8. Exponentiële congruenties I

**Hint 8.19.** **Blz. 87**

Elke term is 0 of 1 modulo 11.

**Hint 8.24.** **Blz. 87**

Gebruik inductie en het binomium van Newton.

## 9. Kwadraatresten

## 10. Polynoomcongruenties

**Hint 10.9.** **Blz. 101**  
Werk analoog aan de bewijzen voor de eigenschappen van gewone congruenties.

**Hint 10.14.** **Blz. 102**

A.

B.  $f$  heeft al zeker  $p - 1$  nulpunten...

C.  $x = 0$  (of equivalent, maar gemakkelijker te zien:  $x = p$ )

## 11. Exponentiële congruenties II

**Hint 11.2.** **Blz. 103**  
Binomium van Newton

**Hint 11.26.** **Blz. 107**  
LTE

**Hint 11.35.** **Blz. 109**  
Zij  $w$  een primitieve wortel. Gebruik dat elke primitieve wortel van de vorm  $w^k$  is met  $\text{ggd}(k, p - 1) = 1$ .

**Hint 11.65.** **Blz. 115**  
Beschouw priemdelers van  $\Phi_n(x)$  voor een goed gekozen  $x$ .

**Hint 11.71.** **Blz. 116**  
Werk analoog aan Opgave 11.63.

**Hint 11.78.** **Blz. 117**  
Vergelijk met de overeenkomstige eigenschappen voor cyclotomische veeltermen.

**Hint 11.79.** **Blz. 117**  
Gebruik de formule  $z_k = \prod_{d|k} \Psi_d$ .

**Hint 11.83.** **Blz. 119**  
Kies voor  $p$  een priemdelers van  $a^n - 1$ , die geen deler is van  $a - 1$ . (Waarom bestaat zo'n  $p$ ?)

**Hint 11.84.** **Blz. 119**  
Kies een priemgetal  $p_1$  met  $\text{ord}_{p_1}(2) = n$ ,  $p_2$  met  $\text{ord}_{p_2}(p_1) = n, \dots$

**Hint 11.89.** **Blz. 120**  
Toon m.b.v. LTE aan dat uit  $\text{ord}_{p^2}(2) > \text{ord}_p(2)$  zou volgen dat  $\text{ord}_{p^2}(2) = p \text{ord}_p(2)$ .

## 12. Binomiaalcongruenties

**Hint 12.4.** **Blz. 122**

Vertrek van de formule van Legendre en schrijf  $n = (n_k \dots n_0)_p$ .

**Hint 12.10.** **Blz. 123**

Maak onderscheid naar gelang  $q$  priem is.

## 13. Kwadratische vergelijkingen

**Hint 13.53.** **Blz. 140**

Zoek het niet te ver, bekijk het eens modulo een of ander getal.

**Hint 13.72.** **Blz. 142**

Houd wat begrenzings bij tijdens het bewijs van het bestaan van oplossingen, te beginnen bij Dirichlet's benaderingsstelling. Deze bovengrens is heel onnauwkeurig.

## 14. Rationale en irrationale getallen

**Hint 14.9.** **Blz. 145**

Kies  $k$  zo groot dat  $\frac{a_{n+1}}{a_1 a_2 \dots a_n} > M$  voor alle  $n > k$ . Kies vervolgens een gepaste waarde voor  $M$ .

## 15. Veeltermen

### 16. Toepassingen

**Hint 16.7.** **Blz. 152**

Bewijs het volgende sterkere resultaat:  $n \in [0, g(a, b)]$  kan voorgesteld worden a.s.a.  $g(a, b) + 1 - n$  niet kan voorgesteld worden.

**Hint 16.10.** **Blz. 152**

Toon aan dat  $\sigma(n^2)$  steeds oneven is.

**Hint 16.15.** **Blz. 153**

A.  $2^{k+1}m = (2^{k+1} - 1)\sigma(m)$

B.  $\sigma(m) = 2^{k+1}x$

C.  $\sigma(m) = m + x$ , dus de enige delers van  $m$  zijn  $m$  en  $x$ .

**Hint 16.17.** **Blz. 153**

A.  $\sigma(n) = 2n \equiv 2 \pmod{4}$ .

B.  $\sigma(p_1^{a_1}) = 1 + p_1 + \dots + p_1^{a_1}$ . Maak onderscheid naar gelang  $a_1$  even of oneven is.

C.  $\sigma(p_k^{a_k}) = 1 + p_k + \dots + p_k^{a_k} \equiv a_k + 1 \pmod{2}$

D.  $\sigma(p_1^{a_1}) = 1 + p_1 + \dots + p_1^{a_1} \equiv a_1 + 1 \pmod{4}$

**Hint 16.19.**

**Blz. 154**

105 = 3 · 5 · 7. Het Euler-priemgetal kan niet 3 of 7 zijn. Bepaal nu een ondergrens voor de overvloedigheidsindex.

**Hint 16.20.**

**Blz. 154**

825 = 3 · 5<sup>2</sup> · 11. Maak onderscheid naar gelang de hoogste exponent van 3.

**Hint 16.21.**

**Blz. 154**

Probeer extra priemfactoren toe te voegen in de veronderstelling dat 3 of 7 tot een niet-zo-hoge exponent voorkomen.

**Hint 16.23.**

**Blz. 154**

Neem in de sommatie  $\sigma(n)$  de termen  $d$  en  $\frac{n}{d}$  samen.

**Hint 16.26.**

**Blz. 154**

In het geval dat  $3 \mid n$ , maak onderscheid tussen  $v_3(n) = 2$  en  $v_3(n) > 2$ .

**Hint 16.48.**

**Blz. 159**

De magische constante is  $\frac{n^3-n}{2}$ , dus het volstaat dat elke diagonaal in de Latijnse vierkanten sommeert tot  $\frac{n^2-n}{2}$ .

**Hint 16.49.**

**Blz. 159**

Elk getal in  $[0, n[$  komt in de som precies 1 keer voor.

**Hint 16.51.**

**Blz. 160**

Elk getal in  $[0, n[$  dat congruent is met  $b$  modulo  $d$  komt in de som precies  $d$  keer voor.

**Hint 16.62.**

**Blz. 163**

$$y \left\lfloor \frac{x}{y} \right\rfloor = x - (x \bmod y)$$

## 17. Algoritmen

### Opgaven deel I

**Hint I.11.**

**Blz. 166**

Inductie.

**Hint I.12.**

**Blz. 166**

Merkwaardige producten.

**Hint I.13.**

**Blz. 166**

Schrijf alles als product van faculteiten en machten van 2.

**Hint I.24.** **Blz. 167**  
Inductie.

**Hint I.28.** **Blz. 167**  
Werk modulo 9.

**Hint I.41.** **Blz. 168**  
Herschrijf het product met faculteiten.

**Hint I.42.** **Blz. 168**  
 $2^{15} - 2^3 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$ . Denk aan Fermat.

**Hint I.44.** **Blz. 168**  
Voor  $-1 < x < 1$  is  $-x > \ln(1 - x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$ .

**Hint I.45.** **Blz. 169**  
Welke van  $p, q, r$  kunnen/moeten 2 zijn?

**Hint I.47.** **Blz. 169**  
Observeer dat  $x$  geheel moet zijn. Schat de kwadraten af (neem een veelterm van even graad!).

**Hint I.48.** **Blz. 169**  
Werk modulo 8.

**Hint I.52.** **Blz. 169**

A. Het volstaat om aan te tonen dat  $3^{m_1} \equiv \pm 3^{m_2}$  impliceert dat  $m_1 = m_2$ .

B. Noem  $w(n)$  het aantal kwadraten modulo  $2^n$ . Stel de recursie  $w(n) = 2^{n-3} + w(n-2)$  op.

**Hint I.55.** **Blz. 169**  
Zo'n rij is in elk geval periodiek modulo eenderwelk geheel getal.

**Hint I.70.** **Blz. 170**  
Toon aan dat beide getallen delers van elkaar zijn.

**Hint I.109.** **Blz. 173**  
Modulo 43 is  $7^2 \equiv 6$  en  $6^2 \equiv -7$

## 18. Modulorekenen revisited

**Hint 18.15.** **Blz. 181**  
Noem  $m$  het kleinste strikt positief element uit de deelring.

**Hint 18.60.** **Blz. 190**  
Zij  $a$  een element verschillend van  $e$ . Wat zijn de mogelijkheden voor  $\text{ord}(a)$ ?

**19. Ringuitbreidingen van  $\mathbb{Z}$**

**20. De  $p$ -adische getallen**

**Opgaven deel II**

**21. Zonder naam**

**22. Befaamde vermoedens**

**Opgaven deel III**

**A. Notaties**

**B. Nuttige stellingen**

**C. Complexe getallen**

**D. Verzamelingen**

# Antwoorden

## Inleiding

### 1. Deelbaarheid

**Antwoord 1.15.** **Blz. 18**  
Aangezien  $|b| = |-|b|$  kunnen we  $(-q, r)$  nemen, met  $(q, r)$  quotiënt en rest bij deling door  $-b$  (die positief is). We konden ook het bewijs voor het geval  $b > 0$  nabootsen.

### 2. Priemgetallen

**Antwoord 2.14.** **Blz. 31**  
Ja.

**Antwoord 2.31.** **Blz. 33**

A. 11

B. 11

C. 16

D. 12

E. 27

**Antwoord 2.34.** **Blz. 34**  
 $p^{100}$  met  $p$  priem.

**Antwoord 2.36.** **Blz. 34**

A. 63

B. 728

C. 72

D. 168

E.  $7 \cdot 13 \cdot 31$

**Antwoord 2.42.** **Blz. 35**

A.  $2^4$



- B.  $2 \cdot 3^4$
- C.  $(p-1)(q-1)$
- D.  $p(p-1)(q-1)$
- E.  $(p-1)(q-1)(r-1)$
- F.  $(p-1)p^{m-1}(q-1)q^{n-1}$

**Antwoord 2.53.**

**Blz. 37**

- A. Volledig analoog als voor de gewone priemontbinding, per inductie
- B.  $2n$  met  $n$  oneven
- C.  $60 = 2 \cdot 30 = 6 \cdot 10$ , of  $36 = 2 \cdot 18 = 6 \cdot 6$ .
- D. Nee, bijvoorbeeld  $a = 6$  en  $b = 2$
- E. Nee:  $30 \mid 6 \cdot 10$  of  $18 \mid 6 \cdot 6$ , maar  $6$  en  $10$  zijn zelf priem!

### 3. Talstelsels

**Antwoord 3.1.**

**Blz. 39**

Niks!  $2_{10} = 10_2$ ,  $3_{10} = 10_3$ ,  $4_{10} = 10_4$ , ...,  $5516_{10} = 10_{5516}$ : elk getal wordt in zijn eigen basis geschreven als  $10!$

### 4. Ad-hocmethodes voor diophantische vergelijkingen

**Antwoord 4.41.**

**Blz. 49**

$\emptyset$ .

### 5. Dirichlet-convolutie

**Antwoord 5.35.**

**Blz. 58**

- A.  $d \in S_n \Leftrightarrow n/d \in S_n$  is duidelijk voldoende. Stel dat  $d \in S_n$ . Kies  $f(d) = 1$  en  $0$  anders, en  $g(n/d) = 1$  en  $0$  anders. Dan is  $(f *_S g)(n) = 1$ . Uit  $(g *_S f)(n) = 1$  blijkt dat  $n/d \in S_n$ .
- B. Zij  $e$  een neutraal element. Uit  $e * \varepsilon = \varepsilon$  blijkt achtereenvolgens  $S_1 = \{1\}$ ,  $e(1) = 1$ ,  $e(2) = 0$ ,  $e(3) = 0$ , ... Dus  $e = \varepsilon$ . Het is duidelijk dat  $\varepsilon$  (tweezijdig) neutraal element is a.s.a.  $\{1, n\} \subset S_n$ .

C. Er zijn verschillende manieren om dit te formuleren. De eerste:

$$\begin{cases} d \in S_n \\ e \in S_{n/d} \end{cases} \Leftrightarrow \begin{cases} de \in S_n \\ d \in S_{de} \end{cases}$$

De tweede:

$$\begin{cases} e \in S_n \\ d/e \in S_{n/e} \end{cases} \Leftrightarrow \begin{cases} d \in S_n \\ e \in S_d \end{cases}$$

Of nog:

(T) Transitiviteit:  $d \in S_n \implies S_d \subset S_n$

(P) Compatibiliteit met producten:  $d \in S_n$  en  $e \in S_{ne} \implies de \in S_{ne}$

(Q) Compatibiliteit met quotiënten:  $d \in S_n$  en  $e \in S_d \implies d/e \in S_{n/e}$

(S) Substitutie:  $d \in S_{df}$  en  $e \in S_f \implies d \in S_{de}$

Merk op: als  $*_S$  commutatief is, volgt (P) uit (T): dan is  $n/d \in S_n$  en  $n \in S_{ne}$ , dus  $\frac{ne}{de} = n/d \in S_{ne}$ , en volgt (S) uit (Q):  $f \in S_{df}$  en  $f/e \in S_f$ , dus  $f/(f/e) \in S_{df/(f/e)}$ .

D. Volgt triviaal uit de voorwaarden voor associativiteit. Merk op dat hetzelfde niet geldt voor commutativiteit en neutraal element.

- E.
- Niet commutatief:  $1^k \mid n$  maar  $(n/1)^k \nmid n$ .
  - Geen neutraal element:  $n \notin S_n$  voor  $n > 1$
  - Niet associatief: (T) en (Q) gelden, maar (P) faalt voor bvb.  $d = e$  en  $n = d^k$ . Ook (S) faalt, voor bvb.  $f = d^{k-1}$ ,  $e = 1$ .

Interessant is dat  $*_S$  wél multiplicativiteit bewaart (zie Opgave 5.36).

**Antwoord 5.38.**

**Blz. 59**

Multiplicatief a.s.a.  $a, b \in V \Leftrightarrow ab \in V$  voor  $\text{ggd}(a, b) = 1$ , of nog: a.s.a.  $V$  primitief is (met de terminologie uit Opgave 5.36) en gesloten onder vermenigvuldigen van coprieme elementen. Totaal multiplicatief a.s.a.  $V$  gesloten is onder vermenigvuldigen en delers.

**Antwoord 5.39.**

**Blz. 59**

Zijn  $f, g$  en  $1_V$  multiplicatief, dan is  $f *_S g = (f \cdot 1_V) *_S g$  multiplicatief omdat  $f \cdot 1_V$  dat is.

**Antwoord 5.42.**

**Blz. 60**

$$\underbrace{1 * \dots * 1}_k$$

**Antwoord 5.45.**

**Blz. 60**

$\mu^2$  en  $\lambda$

## 6. Intermezzo: low-budget ggd calculus

Antwoord 6.19.

Blz. 66

A.  $ac + ad + bc + bd$

B.  $ad + ae + bd + be + cd + ce$

C.  $a^2 + ab + ab + b^2 = a^2 + ab + b^2$

D.  $a^3 + a^2b + ab^2 + b^3$

(De laatste twee zijn nog verder te vereenvoudigen met freshman's dream.)

## 7. Modulo rekenen

Antwoord 7.35.

Blz. 75

$m = n^2 - 1$  werkt

Antwoord 7.57.

Blz. 80

Bijvoorbeeld  $(3, 0, 3)$ :  $x^2 + y^2 = 3$  heeft geen gehele oplossingen.

Antwoord 7.80.

Blz. 83

$\frac{n}{\text{ggd}(n, k+1)}$

Antwoord 7.90.

Blz. 83

Nee

## 8. Exponentiële congruenties I

Antwoord 8.14.

Blz. 86

A. Nee.

B. Ja.

## 9. Kwadraatresten

### 10. Polynoomcongruenties

### 11. Exponentiële congruenties II

### 12. Binomiaalcongruenties

### 13. Kwadratische vergelijkingen

Antwoord 13.48.

Blz. 138

Gaan we analogoos tewerk als daarnet door  $z$  te kiezen met  $\sqrt{\frac{a}{z_0}} \leq z < \sqrt{az_0}$ , dan kunnen we  $2\sqrt{d}|y|$  afschatten door

$$2\sqrt{d}|y| \leq \max_{\sqrt{\frac{a}{z_0}} \leq t < \sqrt{az_0}} \left| t - \frac{a}{t} \right|.$$

De functie  $f(t) = \left| t - \frac{a}{t} \right|$  is opnieuw dalend voor  $0 < t < \sqrt{a}$  en stijgend voor  $t > \sqrt{a}$ . Het gevraagde volgt nu wegens  $f\left(\sqrt{\frac{a}{z_0}}\right) = f(\sqrt{az_0}) = \frac{z_0-1}{\sqrt{z_0}}\sqrt{a}$ .

## 14. Rationale en irrationale getallen

**Antwoord 14.13.** **Blz. 146**

Bijvoorbeeld  $a_n = 2^{2^n} + 1$

**Antwoord 14.23.** **Blz. 148**

Nee.

## 15. Veeltermen

### 16. Toepassingen

**Antwoord 16.42.** **Blz. 158**

$a_{rk} = n \cdot ((r+k) \bmod n) + (r+2k) \bmod n + 1$  (Dit kan niet zomaar verder vereenvoudigd worden.)

**Antwoord 16.46.** **Blz. 159**

Bijvoorbeeld  $a_{rk} = (2r+k) \bmod n$  en  $b_{rk} = (r+2k) \bmod n$ . Indien  $3 \mid n$  is het onmogelijk dat  $\text{ggd}(p-q, n) = \text{ggd}(p+q, n) = \text{ggd}(p, n) = \text{ggd}(q, n) = 1$ .

**Antwoord 16.62.** **Blz. 163**

$b + \frac{an-a-n+d}{2} - (b \bmod d)$  waarbij  $d = \text{ggd}(a, n)$ .

## 17. Algoritmen

### Opgaven deel I

**Antwoord I.24.** **Blz. 167**

$$\frac{n+1}{2}$$

**Antwoord I.26.** **Blz. 167**

Ja.

**Antwoord I.28.** **Blz. 167**

4

**Antwoord I.34.** **Blz. 168**

**Antwoord I.43.** **Blz. 168**  
Enkel voor  $3^3 + 4^3 + 5^3 = 6^3$ .

**Antwoord I.45.** **Blz. 169**  
(2, 59, 2) en (11, 2, 23)

**Antwoord I.47.** **Blz. 169**  
3

**Antwoord I.59.** **Blz. 169**  
2 en 3.

**Antwoord I.71.** **Blz. 170**  
30

**Antwoord I.72.** **Blz. 170**  
 $p^2$

**Antwoord I.74.** **Blz. 170**  
Vals.

**Antwoord I.86.** **Blz. 172**  
Ja.

## 18. Modulo rekenen revisited

**Antwoord 18.15.** **Blz. 181**  
 $m\mathbb{Z}$  met  $m \in \mathbb{N}$ .

**Antwoord 18.60.** **Blz. 190**  
 $C_4$  en  $(\mathbb{Z}/8\mathbb{Z})^\times$

## 19. Ringuitbreidingen van $\mathbb{Z}$

### 20. De $p$ -adische getallen

#### Opgaven deel II

**Antwoord II.1.** **Blz. 195**  
(3, 6, 2), (4, 4, 2), (4, 6, 3), (6, 6, 4), (6, 10, 5) en omwisselen van  $a$  en  $b$ .

**21. Zonder naam**

**22. Befaamde vermoedens**

**Opgaven deel III**

**A. Notaties**

**B. Nuttige stellingen**

**C. Complexe getallen**

**D. Verzamelingen**

# Referenties

- [1] H. de Blank en J. Steenstra. *Sommen van Kwadraten*. Amsterdam, 2012.
- [2] G. D. Brikhoff en H. S. Vandiver. *On the Integral Divisors of  $a^n - b^n$* . <http://www.jstor.org/stable/info/2007263>. 1904.
- [3] S. Cambie. *Pell-like-equations*. 2014.
- [4] D. Đjukić. *Pell's Equation*. <http://www-bcf.usc.edu/~lototsky/PiMuEp/Pell-IMO.pdf>. 2007.
- [5] Y. Ge. *Elementary Properties of Cyclotomic Polynomials*. [http://www.yimin-ge.com/doc/cyclotomic\\_polynomials.pdf](http://www.yimin-ge.com/doc/cyclotomic_polynomials.pdf). 2008.
- [6] F. Q. Gouvêa. *p-adic Numbers. An Introduction*. Second. Springer, 1997.
- [7] A. Heinis en H. Brandsma. *Getallen*. Doe-boek voor 12-16 jarigen. Amsterdam, 1998.
- [8] A. J. Hildebrand. *Introduction to Analytic Number Theory*. <http://www.math.uiuc.edu/~hildebr/ant/>. Lecture Notes from an introductory graduate course on Analytic Number Theory. 2005.
- [9] IMOmath. *Pell's equations*. <http://imomath.com/index.php?options=615>.
- [10] L. Thompson. *Zsigmondy's Theorem*. [www.artofproblemsolving.com/Forum/download/file.php?id=25872](http://www.artofproblemsolving.com/Forum/download/file.php?id=25872). 2009.

# Lijst van symbolen

## Symbolen

$\dagger$	66
$\varepsilon$	50
$\equiv$	68
$\bar{x}_b$	39
$a^{-1}$	71
$(\dots)_b$	39
$(a, b)$	61
$\binom{a}{b}$	205
$\binom{a}{p}$	90
$*$	50
$A \times B$	191
$R^\times$	183
$x\#$	197
$G/H$	220
$G \setminus H$	220
$[G : H]$	221
$[a]_n$	177
$[x]_R$	219
$[x]$	11
$\lfloor x \rfloor$	12
$\{x\}$	12
$n!$	205
$\Phi$	111
$\prod$	205
$\sum$	203
$\mu$	53, 147
$p^k \parallel n$	31
$\alpha(a, p)$	94
$\varepsilon$	50
$\varphi$	35
$\nu_p(n)$	31
$\sigma$	34
$\tau$	34

## 0-9

$1$	50
$1_V$	59
$1_{\text{sq}}$	59

## A

$\arg$	214
--------	-----

## C

$C_\infty$	190
$C_n$	190

## G

$\text{ggd}$	19
--------------	----

## I

$\text{id}$	50
$\Im m$	214
$\text{ind}$	109
$\text{inf}$	10

## K

$\text{kgv}$	20
--------------	----

## M

$(\text{mod } n)$	68
$a \text{ mod } b$	18

## N

$N(z)$	134
$\mathbb{N}$	9
$\mathbb{N}^+$	9

## O

$O_b(a)$	84
$\text{ord}$	110, 186
$\text{ord}_b(a)$	84

## Q

$\mathbb{Q}$	10
--------------	----

## R

$\mathbb{R}$	10
$\text{rad}$	58, 116
$\Re e$	214

## S

$\text{sup}$	10
--------------	----

## Z

$\mathbb{Z}$	9
$\mathbb{Z}[\sqrt{d}]$	133
$\mathbb{Z}/n\mathbb{Z}$	177
$(\mathbb{Z}/n\mathbb{Z})^\times$	183



# Index

<b>A</b>	
Abel	
abelse groep	185
additieve functie	36
additieve notatie	185
algebraïsch	147
argument	214
aritmatische functie	33
<b>B</b>	
Bézout	
stelling	21, 23
Bachet	
vermoeden	131
basis	39
basis (indexrekenen)	109
begrensde verzameling	10
Bertrand, postulaat	32
binomiaalcoëfficiënt	205
Borozdin	199
bovengrens	10
Brahmagupta-Fibonacci	
identiteit	128
stelling	128
Brocard	
probleem	38
Brun	200
<b>C</b>	
Cauchy-Swcharz	
ongelijkheid	211
Cayley	
Cayley-tabel	189
ceilfunctie	11
Chinese reststelling	75
comaximaal	192
complementair	157
complex getal	214
congruentie	68
kwadratisch	96, 97
lineaire congruentie	74
convolutie, Dirichlet	
convolutieproduct	50
copriem	20
copriem (ideaal)	192
<b>D</b>	
De Moivre	
formule	215
De Polignac	200
deelbaar	16
deelbaarheidsrij	162
sterk	162
deelgroep	186
deelring	181
deeltal	16
deler	16
grootste gemene	19
descente finie	129
descente infinie	47
Diophantische vergelijking	25
kwadratisch	125
lineair	25
direct product	
van groepen	191
van ringen	191
voor groepen	190
Dirichlet	
benaderingsstelling	144
convolutie-eenheid	50
Dirichlet-inverse	51
<b>E</b>	
eenheidswortel	109
primitief	110
Eisenstein	
criterium	149
lemma	94
entierfunctie	12
equivalentieklasse	219
equivalentierelatie	218
hoofdstelling	220
Euclides	
algoritme van Euclides	23
reken-schema van Euclides	23
Euclidisch	218



inversie .....	54	Pythagoras	
Möbius-inversieformule .....	55	drietal .....	79
machtsgemiddelde .....	210	<b>Q</b>	
$n$ -demachtsrest .....	78	quotiënt .....	18
magisch vierkant .....	155	quotiënttring .....	182
magische constante .....	155	quotiëntverzameling .....	219
modulus (complex getal) .....	214	<b>R</b>	
modulus (congruentie) .....	68	radicaal .....	58, 116
multiplicatieve functie .....	36	rationaal getal .....	10, 33
multiplicatieve notatie .....	185	reëel deel .....	214
<b>N</b>		reëel getal .....	10
natuurlijk getal .....	9	recursie	
nevenklasse .....	220	lineair .....	211
Newton		reflexief .....	216
binomium .....	207	relatie	
norm .....	134	binair .....	216
nulpunt .....	100	equivalentierelatie .....	218
<b>O</b>		Euclidisch .....	218
ondergrens .....	10	links-Euclidisch .....	218
oneven getal .....	16	rechts-Euclidisch .....	218
ongelijkheid .....	45, 210	reflexief .....	216
machtsgemiddelde .....	210	symmetrisch .....	217
ontbinding .....	44	transitief .....	217
orde .....	84	relatief priem .....	20
orde (eenheidswortel) .....	110	paarsgewijs .....	20
orde (groep) .....	186	rest .....	18
ordelemma .....	85, 188	restklasse .....	68
<b>P</b>		ring .....	180
pariteit .....	18	commutatief .....	180
Pell-typevergelijking .....	127	ringautomorfisme .....	189
Pell-vergelijking .....	127	ringisomorfisme .....	189
perfect getal .....	152	ringmorfisme .....	189
poolhoek .....	214	root flipping .....	47
priemdeler .....	28	<b>S</b>	
priemfactorisatie .....	29	samengesteld getal .....	28
priemgetal .....	28	sommatieteken .....	203
Euler .....	154	sterke deelbaarheidsrij .....	162
Fermat .....	45	Stifel-Pascal	
Mersenne .....	45, 153	formule .....	206
Thabit .....	175	supremum .....	10
Wieferich .....	86, 120, 175	supremumprincipe .....	10
Wolstenholme .....	123	symmetrisch .....	217
priemontbinding .....	29	<b>T</b>	
primitief (eenheidswortel) .....	110	talstelsel .....	39, 40
primitieve wortel .....	106	binair .....	39
primoriaal .....	197		

decimaal .....	39
hexadecimaal .....	39
toegevoegde (complex getal) .....	134
totiënt .....	35
Touchard	
stelling .....	154
transcendent .....	147
transitief .....	217
trapfunctie .....	12
twee-kwadratenstelling .....	130

## V

valuatie .....	31
veelterm	
cyclotomische veelterm .....	111
karakteristiek (recursie) .....	212
monische veelterm .....	100
nulveelterm .....	101
veeltermcongruentie .....	101
veelvoud .....	16
vier-kwadratenstelling .....	131
Vieta	
jumping .....	47
Vinogradov .....	199
voortbrenger .....	186

## W

welordeningsprincipe .....	9
Wilson	
stelling .....	80, 102, 108

## Z

zaagtandfunctie .....	12
Zhang .....	200