Getaltheorie

een introductie

Bart Michels

Inhoudsopgave

Voorwoord

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

Wat is getaltheorie?

De grenzen van een wiskundig vakgebied 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*[1])

[1] `http://math.stackexchange.com/a/216578/43288`

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 t.e.m. de hoofdstelling van de rekenkunde, het deel over oplosstrategieën op het einde van hoofdstuk 1 en vervolgens hoofdstuk 2 t.e.m. het deeltje over kwadraatresten. 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 1 en vervolgens de stelling van Wilson en Fermat in hoofdstuk 2. Daarna zie je maar. Het hoofdstuk over toepassingen is misschien wel eens leuk, en je hoeft er niet veel voor te kennen. 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.

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 een veel diepere theorie. Dit gedeelte heeft namelijk diepe wortels in de verzamelingenleer, en we doen dan ook geen poging om alles axiomatisch op te bouwen.
Daarom hier geen formele definitie van natuurlijke getallen.

Notatie

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

We schrijven ook $\mathbb{N}^\times = \mathbb{N} \setminus \{0\} = \{1, 2, 3, \ldots\}$.[2]

Eigenschap 0.1.1. 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

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

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

Notatie

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.[3]

[2] 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 $\mathbb{N}_0 = \{0, 1, \ldots\}$, anderen $\mathbb{N}_0 = \{1, 2, \ldots\}$. Over de betekenis van $\mathbb{N}^\times$ bestaat nagenoeg geen twijfel.

[3] Men noemt $\mathbb{R}$ om die reden de *Cauchy-completering* van $\mathbb{Q}$.

Notatie

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 0.1.2. 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 0.1.3. 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 0.1.4.

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. □

Stelling 0.1.5.

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 $z \geqslant r$ voor alle $z \in \mathbb{Z}$. Dan zou $\mathbb{Z}$ naar boven begrensd zijn door r, een tegenstrijdigheid. □

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

Stelling 0.1.6. 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 $v - z > v - r \geqslant 0$ 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 $-k$. □

Uit stelling 0.1.5 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

Voor $r \in \mathbb{R}$ noteren we $\lceil r \rceil$ voor het kleinste geheel getal groter of gelijk aan r. Men zegt ook wel 'ceil r' en $\lceil \cdot \rceil$ wordt soms de *ceilfunctie* 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

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*[4], *trapfunctie* of *floorfunctie* genoemd. We zeggen ook "r naar beneden afgerond is $\lfloor r \rfloor$".

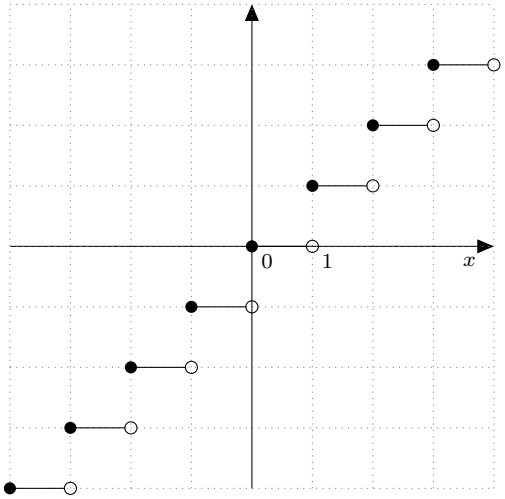
We spreken ook van het 'gedeelte voor de komma' van r, zoals blijkt uit de decimale notatie: $\lfloor 3 \rfloor = 3$, $\lfloor 2.4 \rfloor = 2$ en $\lfloor -1.3 \rfloor = -2$.
Aan de hand van het geheel deel definieert men het *fractioneel deel* van een reëel getal.

[4]Naar het Franse *entier*, wat *geheel* betekent.

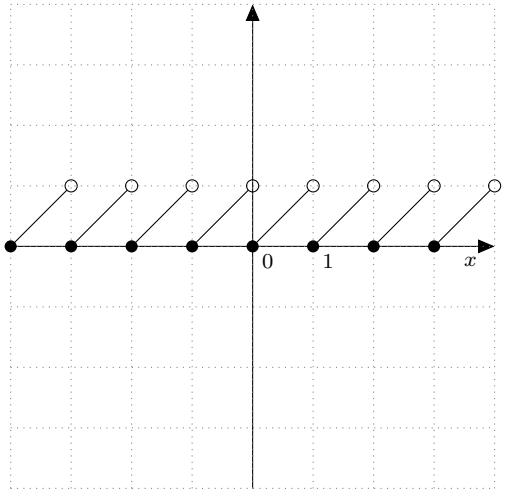
Definitie. Fractioneel deel

Voor $r \in \mathbb{R}$ definiëren we het *fractioneel deel* als $\{r\} = r - \lfloor r \rfloor$.[5] 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

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

Veronderstel nu omgekeerd dat er een geheel getal z is zo dat $z \leqslant x < z + 1$. 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 $z \leqslant \lfloor x \rfloor$ en $z > \lfloor x \rfloor - 1$ leert ons dat $z = \lfloor x \rfloor$. Samenvattend,

Stelling 0.1.7.

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

Met een volledig analoge redenering bewijst men:

Stelling 0.1.8.

Voor elk reëel getal x bestaat er een uniek geheel getal z waarvoor $z - 1 < x \leqslant z$, 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 0.1. Bewijs dat $\lfloor -x \rfloor = -\lceil x \rceil$ voor alle $x \in \mathbb{R}$.

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

Opgave 0.2. Hoe ziet de grafiek van $\lceil \cdot \rceil$ eruit? H

Opgave 0.3. Bewijs dat $\lfloor x \rfloor \lfloor y \rfloor \leqslant \lfloor xy \rfloor$ voor $x, y > 0$.

Opgave 0.4. (VWO 2013 ronde 1 vraag 22) Hoeveel van de volgende gelijkheden gelden voor alle reële getallen $x \geqslant 1$ en $y \geqslant 1$? 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 $n \geqslant 5$". Dit predikaat is vals voor $n = 0, 1, 2, 3, 4$ en waar voor alle andere natuurlijke getallen.

Eigenschap 0.2.1. 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.

We illustreren dit met een voorbeeld. We tonen aan dat $0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$ voor alle $n \in \mathbb{N}$. De uitspraak $P(n)$ is hier "$0 + 1 + 2 + \cdots + n$ 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 $0 + 1 + \cdots + k = \frac{k(k+1)}{2}$. Tellen we hier aan beide

[5] Soms noteert men $\{r\}$ als r mod 1, om redenen die in hoofdstuk 1 duidelijk worden.

kanten $k+1$ bij: $0 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + k + 1$. $P(k+1)$ 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 $n \in \mathbb{N}$.

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 dus $P(n)$ waar voor alle $n \in \mathbb{N}$. □

Als inductiebasis kan men ook $P(k)$ bewijzen voor een zekere $k > 0$. Het inductieprincipe zegt dan dat $P(n)$ waar is voor alle $n \geqslant k$. Over de uitspraken $P(0), P(1), \ldots, P(k-1)$ 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 $n \geqslant z$, dan kan men met het inductieprincipe besluiten dat $P(n)$ voor alle $n \geqslant z$. 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 $n \geqslant z$" vertaald zich als "$Q(n+1)$ volgt uit $Q(n)$ voor alle $n \geqslant 0$".

I
Elementaire getaltheorie

Hoofdstuk 1. Deelbaarheid

1.1 Deler en veelvoud

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. Deler en veelvoud

We zeggen dat a deelbaar is door b als er een derde geheel getal k 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.

Gevolg 1.1.1.

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 $|b| \leqslant |a|$.
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 twee getallen $a, b \in \mathbb{Z}_0$ 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 $k = 0$. 0 is dus een even getal, want het is deelbaar door 2.
2. Als $b \leqslant a$, dan is $a = kb$, en omdat $a \neq 0$ is $|k| \geqslant 1$. Nu geldt dat
$$|b| = \frac{|a|}{|k|} \leqslant \frac{|a|}{1} = |a| \,.$$
3. Uit het tweede gevolg weten we dat $|b| \leqslant |a|$ en dat $|a| \leqslant |b|$, 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 anloge reden geldt dat $b \mid a$. Uit het derde gevolg weten we dat $a = \pm b$.

□

Stelling 1.1.2. Transitiviteit van de deelbaarheid

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 $y = kx$. □

Opgave 1.1. Zij $x, y \in \mathbb{Z}$ zo dat $3 \mid x$ en $3 \mid x + y$. Is dan ook $3 \mid y$?

Opgave 1.2. 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 1.3. Stel dat $a, b \in \mathbb{Z}$ zo dat $91 \mid a$ en $56 \mid b$. Bewijs dat $14 \mid 12a + 3b$.

Definitie. 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 1.1.3.

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. □

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 1.4. 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 $k \leqslant 14$ is $7k \leqslant 98$, wat kleiner is dan 100. Maar als $k \geqslant 15$ is $7k \geqslant 105$, 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.

1.1.1 Rest en quotiënt

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

Definitie. Rest en quotiënt

Zij a en b gehele getallen met $b \neq 0$. Gehele getallen q en r waarvoor $a = bq + r$ en $0 \leqslant r < |b|$ 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 $0 \leqslant r < b$ 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 $0 \leqslant 1 < 6$. 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 1.5. 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 1.1.4. Uniciteit 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 $0 \leqslant q < |b|$.

We bewijzen eerst de uniciteit van rest en quotiënt.

Opgave 1.6. Toon aan dat quotiënt en rest uniek zijn. Veronderstel dat er twee verschillende quotiënten zijn met bijbehorende 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 1.8.5 steunt erop dat er een rest en een quotiënt bestaat.

Voorbeeld 1.7. 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 $q \leqslant \frac{a}{b} < q+1$. Dus $bq \leqslant a < bq+b$ (merk op dat we hier de voorwaarde $b > 0$ gebruiken), wat we kunnen schrijven als $0 \leqslant a - qb < b$. Stellen we nu $r = a - qb$, dan hebben we getallen q en r waarvoor $a = qb + r$ en $0 \leqslant r < b$. Aan de twee voorwaarden is voldaan, dus bestaan er een quotiënt en een rest.

Opgave 1.8. Bewijs zelf dat er ook een rest en een quotiënt bestaan bij deling van a door b met $b < 0$.

Zoals eerder beloofd een praktische voorwaarde voor deelbaarheid.

Eigenschap 1.1.5. 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. □

We hernemen het eerdere voorbeeld.

Voorbeeld 1.9. 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.

1.1.2 Talstelsels

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

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. De inspiratie voor het bedenken van nieuwe symbolen raakt 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 $0, 1, \ldots, 9$ 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 $0, 1, \ldots, b-1$. Als we een natuurlijk getal n voorstellen in basis b als $a_m a_{m-1} \cdots a_0$, waarbij $a_0, \ldots, a_m$ 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. De voorwaarde is wel dat $a_m \neq 0$ als $n \neq 0$. Om duidelijk te maken dat n in basis b staat geschreven, noteert men vaak $(a_m a_{m-1} \cdots a_0)_b$.
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.

Opgave 1.10. Tien heeft de eigenschap dat, wanneer je het schrijft in zijn eigen basis, er een 1 en een 0 staat. Wat maakt tien zo speciaal?

Opgave 1.11. 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 $10 \neq 11$.

Stelling 1.1.6.

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

Opgave 1.12. Bewijs dat de voorstelling in basis b uniek is.

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.

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. 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. 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 $\text{ggd}(a_1, \ldots, a_n)$.

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. Relatief priem

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

De uitspraak "$a_1, a_2, \ldots, a_n$ zijn paarsgewijs relatief priem" betekent niet hetzelfde als $\text{ggd}(a_1, a_2, \ldots, a_n) = 1$. 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.

1.2.1 De stelling van Bézout

Stelling 1.2.1. Stelling van Bézout[6]

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 1.13. Bewijs 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 $c \leqslant d$.

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

Gevolg 1.2.2.

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.

[6] Naar Étienne Bézout. Voor het eerst geformuleerd door de Fransman Bachet in de 17e eeuw

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 $\text{ggd}(a, b) \leqslant ax + by$. (Gevolg 1.1.1.2.)
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 1.14. 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 1.1.3 en Gevolg 1.2.2.2.)
De getallen $\text{ggd}(a, b)$ en $\text{ggd}(a, b - na)$ hebben dezelfde delers en zijn dus gelijk wegens Gevolg 1.1.1.4.
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 1.2.3.

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 $c = \cdots \cdot a$. 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.

Opgave 1.15. 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 1.16. Stel dat $\text{ggd}(a, b) = 1$. Toon aan dat $\text{ggd}(a, c) = \text{ggd}(a, bc)$.

Opgave 1.17. 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 1.2.4. Stelling van Bézout, algemeen geval

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

Opgave 1.18. Bewijs deze veralgemening.

1.2.2 Kleinste gemene veelvoud

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

Definitie. 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. 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 $\text{kgv}(a_1, \ldots, a_n)$.

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

Stelling 1.2.5.

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 $k \mid c$. □

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.

1.2.3 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 1.14. 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 1.14 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.

Gevolg 1.2.6.

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

Dit illustreren we met het bovenstaande voorbeeld. Als we de eerste deling uitvoeren bekomen 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 1.19. 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.

1.2.4 Lineaire Diophantische vergelijkingen

Een Diophantische vergelijking is een heel algemeen begrip.

Definitie. 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

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

en

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

Diophantische vergelijkingen. Vooraleer dat soort mastodonten aan te pakken beginnen we met een iets eenvoudigere vergelijking.

Definitie. Lineaire Diophantische vergelijking

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

Stelling 1.2.7.

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

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

Opgave 1.20. Bewijs deze majestueuze stelling.

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 1.2.8.

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 1.2.8.2. Want als bijvoorbeeld $b \leqslant 0$ 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 1.21. Bepaal alle oplossingen voor x en y 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 1.22. Bepaal alle gehele getallen m en n waarvoor $50m - 28n = -16$.

Opgave 1.23. Bepaal alle oplossingen voor p en q van de vergelijking $-35p + 84q = 65$.

Voor een leuke praktische toepasssing van dit soort vergelijkingen verwijzen we naar sectie 7.1.

1.3 Priemgetallen

Definitie. 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 priemdeler van n".

Definitie. 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 1.24. 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 1.25. Zij p een priemgetal. Toon aan dat $p \mid \binom{p}{a}$ voor elke a met $0 < a < p$.

1.3.1 Hoofdstelling van de rekenkunde

Stelling 1.3.1. 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 $p_1, p_2, \ldots, p_r$ verschillende priemgetallen zijnen $a_1, a_2, \ldots, a_r$ natuurlijke getallen groter dan 0. Deze schrijfwijze is bovendien uniek, op de volgorde van de factoren na.

Definitie. 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 in latere oefeningen zal je merken dat er ook getallenverzamelingen bestaan waar niet elk getal een unieke ontbinding heeft. Het is dus nodig om dit te bewijzen.

Opgave 1.26. 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 1.27. 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 $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$ en $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s$. (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 $p_1, p_2, \ldots, p_r$ 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 $p_1, p_2, \ldots, p_r$ voorkomt.
Aangezien er geen kleinste getal n is zonder unieke priemontbinding, is er dus geen enkel getal zonder unieke priemontbinding.

1.3.2 Gevolgen van de hoofdstelling

Gevolg 1.3.2.

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 waarbij de exponent van p_i in de priemontbinding 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 1.3.3. 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. Dit betekent natuurlijk zo goed als hetzelfde, en zijn bewijs is dan ook precies het bewijs dat we zullen gebruiken:

Opgave 1.28. Bewijs dat er oneindig veel priemgetallen bestaan.

Veronderstel dat er slechts een eindig aantal priemgetallen bestaat. Noem die priemgetallen $p_1, p_2, \ldots, p_n$. 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 1.29. 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 1.3.4.

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

Opgave 1.30. Bewijs de stelling als oefening.

Opgave 1.31. Toon aan dat $\text{kgv}(x^n, y^n) = (\text{kgv}(x,y))^n$ voor elk natuurlijk getal n. Geldt hetzelfde voor de grootste gemene deler?

Opgave 1.32. 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.

Notatie

Als $n \in \mathbb{Z}_0$ en p is een priemgetal noteren we $\nu_p(n)$ voor het aantal priemfactoren p in de priemontbinding van $|n|$.[7] Indien $\nu_p(n) = k$ noteren we ook $p^k \| n$.

Zo is $\nu_2(-1) = 0$, $\nu_5(50) = 2$ en $\nu_7(2) = 0$.

Opgave 1.33. Bewijs dat $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ voor priemgetallen p en $a, b \in \mathbb{Z}_0$.

Lemma 1.3.5.

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 $\nu_p(a) = x$, $\nu_p(b) = y$ en $\nu_p(c) = z$. 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 $y \leqslant z$, want de gelijkheid is symmetrisch in y en z. Het rechterlid is dan gelijk aan $\max(x,y)$.
We bekijken nu het linkerlid. Omdat $y \leqslant z$, 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 $y \leqslant z$ dus ook dit is onmogelijk.
Bijgevolg is $\max(x,y) \leqslant \max(x,z)$, 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. □

[7] De ν is een Griekse letter nu, en geen v. De volledige context wordt in hoofdstuk 10.2 toegelicht.

Lemma 1.3.6.

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 1.34. Bewijs Lemma 1.3.6.

Stelling 1.3.7. Formule van Legendre

Er geldt dat

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

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

Opgave 1.35. Bewijs deze stelling als oefening.

Definitie. Primoriaal

Voor een reëel getal $x \geqslant 2$ 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 $7\# = 2 \cdot 3 \cdot 5 \cdot 7$.

Stelling 1.3.8. 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 Tsjebysjev, werd in 1845 als vermoeden geformuleerd door de Fransman Joseph Betrand. Het werd voor het eerst bewezen in 1850 door Pafnoeti Tsjebysjev, in Hoofdstuk 10.2 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 typische toepassing van het Postulaat van Bertrand is de volgende.

Opgave 1.36. Vind alle natuurlijke getallen n waarvoor $n!$ een kwadraat is.

1.4 Aritmetische functies

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

1.4.1 Aantal delers

Opgave 1.37. Bepaal het aantal positieve delers van A

A. 2^{10}.

B. 3^{10}.

C. $2 \cdot 3 \cdot 5 \cdot 7$.

D. $4 \cdot 3 \cdot 5$.

E. $4 \cdot 9 \cdot 25$.

Stelling 1.4.1.

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 1.38. Toon de formule voor $\tau(n)$ aan.

Opgave 1.39. Welke natuurlijke getallen hebben precies 101 positieve delers? A

Opgave 1.40. Toon aan dat een natuurlijk getal groter dan 0 een oneven aantal delers heeft als en slechts als dat getal een volkomen kwadraat is.

1.4.2 Som van delers

Opgave 1.41. 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 1.4.2.

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 1.42. Toon de formule voor $\sigma(n)$ aan.

Opgave 1.43. Welke natuurlijke getallen hebben 31 als som van hun positieve delers?

Opgave 1.44. 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.

1.4.3 Totiëntfunctie

Definitie. Totiënt

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

Opgave 1.45. 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 $m, n \geqslant 1$.

Analoog aan τ en σ hebben we een expliciete formule voor φ.

Stelling 1.4.3.

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

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

Een intuïtief argument voor deze formule gaat als volgt: als p een priemdeler van n is, is de 'kans' dat een getal in $\mathbb{N}^\times_{\leqslant n}$ 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 1.8.5 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.2.2).
Bewijs.
Noteer voor een priemdeler p van n, A_p als de verzameling van getallen in $\mathbb{N}^\times_{\leqslant n}$ die deelbaar zijn door p. Dus $\varphi(n) = n - \left|\bigcup_{p|n} A_p\right|$. Voor verschillende priemgetallen $p_1, \ldots, p_k$ geldt, aangezien $\text{kgv}(p_1, \ldots, p_k) = p_1 \cdots p_k$, dat $\left|\bigcap_{l=1}^k A_{p_l}\right| = \frac{n}{p_1 \cdots p_k}$. Zij nu $p_1, \ldots, p_k$ de verschillende priemdelers van n. Het inclusie-exclusieprincipe zegt dat

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

wat kan worden ontbonden als

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

□

Opgave 1.46. Toon aan dat $\varphi(n)$ even is voor $n > 2$.

Opgave 1.47. Bepaal alle natuurlijke getallen a zo dat $\varphi(a) = 8$.

Opgave 1.48. Bepaal alle natuurlijke getallen n zo dat $\varphi(\varphi(\varphi(n)))$ een priemgetal is.

Zoals je misschien hebt gemerkt zijn de bewijzen van de formules voor τ, σ en φ heel sterk combinatorisch. Verderop zal de *Dirichlet convolutie* toelaten om minder combinatorische (maar ook minder intuïtieve) bewijzen te geven, die misschien wel nauwkeuriger lijken.

1.4.4 Multiplicatieve functies

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

Definitie. Multiplicativiteit

Een functie $f : \mathbb{N}^\times \to \mathbb{C}$ noemt men *multiplicatief* als $f(ab) = f(a) \cdot f(b)$ voor alle coprieme $a, b \in \mathbb{N}^\times$, en als $f(1) \neq 0$.[8] 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. Additiviteit

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

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

Opgave 1.49. Als f een multiplicatieve functie is, wat zijn dan de mogelijke waarden voor $f(1)$?

Opgave 1.50. 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.

[8] 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 1.4.4.

τ, σ en φ 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 σ en φ. Dat ze niet totaal multiplicatief zijn zien we bijvoorbeeld aan $3 = \tau(4) \neq \tau(2)^2$, $7 = \sigma(4) \neq \sigma(2)^2$ en $2 = \varphi(4) \neq \varphi(2)^2$. □

Definitie

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

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

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

1.5 Rationale en irrationale getallen

De verzamelingen $\mathbb{N}$ en $\mathbb{Z}$ zijn nu al tamelijk uitgepluisd. Het is de beurt aan $\mathbb{Q}$ en $\mathbb{R}$ om hun geheimen prijs te geven.

Eigenschappen[9] 1.5.1.

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

Wie rationaal zegt, zegt irrationaal.

Definitie. 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 1.5.2. Eenduidigheid van rationale getallen

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

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

Opgave 1.51. Bewijs stelling 1.5.2.

Een typische toepassing van deze stelling is:

Opgave 1.52. Zij $n \in \mathbb{N}$ geen volkomen kwadraat. Bewijs dat $\sqrt{n}$ irrationaal is.

Opgave 1.53. Zij p een priemgetal. Bewijs dat voor natuurlijke getallen $n \in \mathbb{N}^\times$ geldt dat $\log_p(n) \in \mathbb{Q}$ als en slechts als n een macht van p is.

1.5.1 Expansies van niet-gehele getallen

De vraag rijst of we elk reëel getal in elk talstelsel kunnen voorstellen, en of die schrijfwijze uniek is. Het antwoord is ja, hoewel het nu minder voor de hand ligt:

Stelling 1.5.3.

1.5.2 Diophantische benadering

Stelling 1.5.4.

Als α 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 α 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 $q \in \mathbb{N}$.[10]

Opgave 1.54. We bewijzen stelling 1.5.4.

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 $0, \{\alpha\}, \ldots, \{n\alpha\}$.

A. Toon aan dat er zeker twee van die getallen in hetzelfde deelinterval van lengte $\frac{1}{n}$ liggen.

B. Toon aan dat er getallen $a \in \mathbb{N}^\times$ 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.

C. Bewijs dat er een $k \in \mathbb{N}^\times$ 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 1.5.5.

Als α irrationaal is, $r \in \mathbb{R}$ en $\varepsilon > 0$, dan bestaan er $q \in \mathbb{N}^\times$ en $p \in \mathbb{Z}$ zo dat $|q\alpha - p - r| < \varepsilon$.

[9]

[10] Men zegt dat de verzameling van fractionele delen $\{q\alpha\}$ *dicht* is in $[0,1]$.

Bewijs.
We kunnen de vorige stelling toepassen op $\{r\}$, zodat er een $q \in \mathbb{N}$ bestaat waarvoor $|\{q\alpha\} - \{r\}| < \varepsilon$. Stellen we $p = \lfloor q\alpha \rfloor - \lfloor r \rfloor$, dan geldt $|q\alpha - p - r| < \varepsilon$. □

Nemen we in het bijzonder $r = 0$, dan vinden we $\frac{p}{q} \in \mathbb{Q}$ waarvoor $\left|\alpha - \frac{p}{q}\right| < \frac{\varepsilon}{q} \leqslant \varepsilon$. 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:

Stelling 1.5.6. Benaderingsstelling van Dirichlet

Zij α een irrationaal getal en $n \in \mathbb{N}^\times$. Dan bestaan er $p \in \mathbb{Z}$ en $q \in \{1, \ldots, n\}$ waarvoor $\left|\alpha - \frac{p}{q}\right| < \frac{1}{(n+1)q}$.

Opgave 1.55. Bewijs Dirichlet's benaderingsstelling.

Gevolg 1.5.7.

Als $\alpha \in \mathbb{R}$ bestaan er oneindig veel koppels $(p, q) \in \mathbb{Z} \times \mathbb{N}^\times$ 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 $k \in \mathbb{N}^\times$. Als α irrationaal is, neem dan $n_1 \in \mathbb{N}^\times$. Wegens de vorige stelling bestaan er $p_1 \in \mathbb{Z}$ en $q_1 \leqslant n_1$ 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. □

1.5.3 Toepassingen van Diophantische benadering

1.6 Dirichlet-convolutie

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. 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 1.6.1.

Het Dirichlet-convolutieproduct is commutatief en associatief, en heeft als neutraal element ϵ.

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

1.6.1 Inverteerbaarheid

Definitie. Dirichlet-inverse

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

Opgave 1.56. Toon aan dat een Dirichlet-inverse, als ze bestaat, uniek is.

Opgave 1.57. 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 1.6.2. Criterium voor inverteerbaarheid

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

Bewijs.
Als f inverteerbaar is, is $f(1) \cdot f^{-1}(1) = (f * f^{-1})(1) = \epsilon(1) = 1$, 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 1.6.3. 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 convoluteren met h^{-1} geeft $(f * h) * h^{-1} = (g * h) * h^{-1}$, dus $f = g$ aangezien $*$ associatief is en ϵ als neutraal element heeft. □

1.6.2 Convoluties en multiplicativiteit

Stelling 1.6.4.

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

Opgave 1.58. Bewijs deze eigenschap van de convolutie.

Let er op dat Stelling 1.6.4 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 1.59. Bewijs dat $\mathbf{1} * \mathbf{1} = \tau$ en $\mathbf{1} * \mathrm{id} = \sigma$.

Stelling 1.6.5.

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 $\gcd(a, b) = 1$ 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 $\gcd(a, b) = 1$. We hebben

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

Aangezien $\gcd(a, b) = 1$ is in het linkerlid $d = xy$ met $x \mid a$ en $y \mid b$, $\gcd(x, y) = 1$. 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 $f(1)^2 g(a)g(b) = g(a)g(b)$. □

Gevolg 1.6.6.

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

Opgave 1.60. Bewijs als oefening.

1.6.3 Möbiusinversie

Definitie. Kwadraatvrij en kwadraatvol

Een natuurlijk getal $n \in \mathbb{N}^\times$ 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. Möbiusfunctie

Voor $n \in \mathbb{N}^\times$ definiëren we de Möbiusfunctie μ 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 1.6.7.

μ is multiplicatief.

Opgave 1.61. Bewijs dat μ inderdaad multiplicatief is.

De volgende convolutie ligt aan de basis van de Möbiusinversie:

Lemma 1.6.8.

Er geldt dat $\mu * \mathbf{1} = \epsilon$.

Bewijs.
Aangezien μ en $\mathbf{1}$ mutiplicatief zijn is ook $\mu * \mathbf{1}$ 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 $n \in \mathbb{N}^\times$. Dan is $\epsilon(p^n) = 0$. Er geldt

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

zodat $(\mu * \mathbf{1})(p^n) = \epsilon(p^n)$. □

Gevolg 1.6.9.

Als $n > 1$ geldt

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

Indien $n = 1$ is deze som 1.

Opgave 1.62. Zij n het product van m verschillende priemgetallen. Pas de formule $\sum_{d|n} \mu(d) = 0$ toe en leid daaruit af dat

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

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

Stelling 1.6.10. Möbius-inversiestelling

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

Bewijs.
Indien $f = \mu * g$ is $\mathbf{1} * f = \mathbf{1} * (\mu * g) = (\mathbf{1} * \mu) * g = \epsilon * g = g$. Omgekeerd, indien $g = \mathbf{1} * f$ is $\mu * g = \mu * (\mathbf{1} * f) = (\mu * \mathbf{1}) * f = \epsilon * f = f$. □

De Möbius-inversiestelling laat zich ook uitdrukken met de zogenaamde Möbius-inversieformule. In feite is dit niets meer dan een herformulering van de inversiestelling:

Gevolg 1.6.11. 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 1.63. 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.

1.6.4 Toepassing: expliciete formules voor aritmetische functies

Een enigszins verrassende convolutie is de volgende:

Stelling 1.6.12.

Er geldt dat $\mathbf{1} * \varphi = \mathrm{id}$, 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 φ opnieuw te bewijzen steunen we niet op die formule.

Bewijs.

We tellen het aantal breuken in $\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}\}$ 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 $\sum_{d|n} \varphi(d)$. □

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 1.5.2.

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

Bewijs.

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

□

Zoals je kan zien hebben we de voorwaarde $\mathrm{ggd}(k,d) = 1$ weggewerkt door een extra sommatie $\sum_{f|\mathrm{ggd}(k,d)} \mu(f) = \epsilon(\mathrm{ggd}(k,d))$. We konden daardoor gewoon sommeren over

alle $k \leqslant d$. 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 $k \leqslant d$ 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 veelvouden zijn van f.

Uit deze convolutie volgt ook de formule voor φ: aangezien $\varphi * \mathbf{1} = \mathrm{id}$ is $\varphi = \mathrm{id} * \mu$, zodat φ multiplicatief is. Voor een priemmacht p^n volgt uit de definitie van φ 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. $\varphi(p^n) = \sum_{d \mid p^n} \mu(d) \cdot \frac{p^n}{d} = p^n - \frac{p^n}{p} + 0 + \cdots + 0 = (p-1)p^{n-1}$.) De algemene formule voor φ volgt nu uit de multiplicativiteit.

De identiteit kent nog een mooi bewijs, op voorwaarde dat we al weten dat φ multiplicatief is. (Dit bewijs past niet in de opbouw die we hierboven gaven omdat het net de multiplicativiteit van φ is die met de laatste stelling bewezen werd.)
Bewijs.
Via inductie. Voor $n = 1$ is het duidelijk, stel nu dat het geldt voor $1, \ldots, n-1$. Zij $p^k \| n$ 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 $\sum_{d \mid n, p^k \mid d} \varphi(d) = \varphi(p^k) \sum_{f \mid m} \varphi(f) = (1 - \frac{1}{p}) \cdot p^k m = (1 - \frac{1}{p})n$. In de tweede som is $d \mid \frac{n}{p}$, dus die som is wegens de inductiehypothese $\frac{n}{p}$. Optellen levert $(1 - \frac{1}{p})n + \frac{n}{p} = n$. □

1.6.5 Möbiusinversie in multiplicatieve vorm

De Möbius-inversieformule kent ook een multiplicatieve variant. Het bewijs ervan kan helaas niet met het convolutieproduct gegeven worden.[11]

Stelling 1.6.13. Möbius-inversieformule, multiplicatieve vorm

Als f, g aritmetische functies zijn waarvoor

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

dan is

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

Opgave 1.64. Bewijs de multiplicatieve vorm van de Möbius-inversieformule.

[11] Een verklaring hiervoor is het gebrek aan commutativiteit van de multiplicatieve variant van het convolutieproduct.

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:[12]

- 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 luidt een extra voorwaarde:

- Elk element heeft een invers element voor de vermenigvuldiging.

Dit garandeert dat een negatieve exponent ten gevolge van μ 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 1.65. Bewijs dat voor elk naturlijk getal $n > 0$

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

Opgave 1.66. Bewijs dat voor elk natuurlijk getal $n > 0$

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

1.6.6 Elimineren van de floorfunctie

Opgave 1.67. Bewijs dat voor $n \geqslant 1$,

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

Opgave 1.68. Bewijs dat voor $n \geqslant 1$,

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

Opgave 1.69. Bewijs dat voor $n \geqslant 1$,

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

Opgave 1.70. Bewijs dat voor $n \geqslant 1$,

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

[12] Onder de eerste vier voorwaarden noemt men die verzameling een *commutatieve ring (met eenheid)*.

1.7 Technieken

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

(*Godfried Bomans*)

In dit onderdeel bespreken we enkele oplosstrategieën die van pas kunnen komen bij het oplossen van Diophantische vergelijkingen of bij specifieke types opgaven. Hierin ligt de basis van het oplossen van meer geavanceerde opgaven.

1.7.1 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 1.71. 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 1.72. Vind alle priemgetallen p zo dat $p + 1$ een volkomen kwadraat is.

Opgave 1.73. Vind alle gehele getallen a en b zo dat $ab = a + b$.

Definitie. Mersennepriemgetal

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

Opgave 1.74. Stel dat $2^n - 1$ een priemgetal is. Toon aan dat n een priemgetal is.

Definitie. Fermat-priemgetal

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

Opgave 1.75. Stel dat $2^m + 1$ een priemgetal is. Toon aan dat m een macht van 2 is.

1.7.2 Ongelijkheden

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

Voorbeeld 1.76. 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 $n \geqslant 1$. Dan is $5^n + 1 > 5^n > 4^n = 2^{2n} \geqslant 2^{n+1}$. 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 $5^n+1 > 5^n > 4^n = 2^{2n} \geqslant 2^{n+1}$ gebruikt. Er zijn natuurlijk nog andere mogelijkheden. Je had het bijvoorbeeld ook kunnen bewijzen met

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

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 $n \geqslant 1$. We zijn dus eerst het geval $n = 0$ nagegaan zodat we $n \geqslant 1$ 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 1.77. Vind alle natuurlijke getallen n waarvoor $2^n + 1 \mid 2n + 1$.

Opgave 1.78. 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 1.79. 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 $a \leqslant b$, 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

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

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 1.80. Vind alle natuurlijke getallen n zo dat $n + 1 = 2^n$.

Opgave 1.81. (CanMO 1983 vraag 1) Vind alle natuurlijke getallen w, x, y, z die voldoen aan $w! = x! + y! + z!$.

Opgave 1.82. Vind alle natuurlijke getallen a, b en c zo dat $a^a + b^b = c^c$.

Opgave 1.83. (JBaMO 2010 vraag 2) Vind alle natuurlijke getallen $n \geqslant 1$ 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 $a \geqslant 0$. 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 1.84. 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 1.85. Vind alle gehele getallen x en y zo dat $\frac{x}{y-1} = \frac{y+1}{x+1}$.

Opgave 1.86. (Q-E-D Competitie juni 2012)

A. Vind alle natuurlijke getallen n waarvoor geldt dat $n^2 + 12n + 20$ een volkomen kwadraat is.

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

1.7.3 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 1.87. 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 ${a_0}^2 = 3{b_0}^2$.
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 1.88. Bewijs dat er geen strikt positieve gehele getallen x en y zijn die voldoen aan $x^2 + 2y^2 = 4xy$.

Opgave 1.89. Vind alle gehele getallen x, y en z zijn die voldoen aan $x^3 + 3y^2 = 9z^2$.

1.7.4 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 1.90. 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 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 $a \leqslant b$, 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 $\frac{a^2+1}{b} \leqslant \frac{b^2+1}{b} = b + \frac{1}{b} < b + 1$. 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 Franois Viète. Hij stelde formules op voor de coëffciënten 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 1.91. Vind alle natuurlijke getallen n waarvoor er $x, y \in \mathbb{N}$ bestaan zo dat

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

1.8 Addendum: low-budget ggd 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 rechstreeks uit volgt[13]. 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 besteaan 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

[13] In algebraïsche termen: elk Euclidisch domein is een UFD.

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

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 $a_1, \ldots, a_n$ enkel bestaat wanneer minstens één van de getallen niet 0 is. We zullen naar deze voorwaarde kortweg referen als "$\text{ggd}(a_1, \ldots, a_n)$ 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.[14] Een oplossing bestaat erin de definitie van de grootste 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 gerbruik 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. 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.
Het antwoord op de tweede vraag is dan weer positief, of toch in zekere zin:

Opgave 1.92. 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 1.93. (Commutativiteit) Bewijs dat $(a, b) = (b, a)$ voor alle $a, b \in \mathbb{Z}$ indien (a, b) bestaat.

Opgave 1.94. 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.

1.8.1 Distributiviteit

Eigenschap 1.8.1. 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 1.8.2.

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 $bc = ka$. Dan is $axc + yka = c$, of dus $(xc + yk)a = c$. Dus $a \mid c$.
Gebruik makend van de distributieve eigenschap kan dit heel wat korter (en zonder gebruik te maken van de stelling van Bézout):

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

□

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

1.8.2 Associativiteit

Eigenschap 1.8.3. 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 1.8.4.

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 1.8.5. 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 1.8.6.

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 $ab \mid c$. □

1.8.3 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 definieren als in

Definitie

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

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

Notatie

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

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 1.96. Indien $a_1, \ldots, a_n \in \mathbb{Z}$ 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 1.97. Probeer in te zien waarom meer algemeen geldt dat we extra ggd-haakjes binnen ggd-haakjes mogen negeren zonder dat het resultaat wijzigt.

Opgave 1.98. Overtuig jezelf ervan dat de distributieve eigenschap ook geldig is voor meedere variabelen, in de vorm:

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

1.8.4 Additieve notatie

Notatie

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

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

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 1.99. 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. $(a \dot{+} b)^3$

1.8.5 Freshman's dream voor ggd's

Lemma 1.8.7.

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

Opgave 1.100. Bewijs als oefening. H

Eigenschap 1.8.8. Freshman's dream voor ggd's

Voor $n \in \mathbb{N}^\times$ 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:

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

Links en rechts delen door (het niet-0 getal) $(a \dotplus b)^n$ levert $(a \dotplus b)^n = a^n \dotplus b^n$. □

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 1.8.4: 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. □

Opgave 1.101. 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 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 $(a^n, b^n) = 1$. □

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 $m \geqslant 0$. 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. □

Opgaven hoofdstuk 1

1.1 Deler en veelvoud

Opgave 1.102. (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 1.103. (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 1.104. (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

1.2 Grootste gemene deler

Opgave 1.105. Stel dat $\text{ggd}(a, b) = 1$. Bewijs dat $\text{ggd}(a + b, a - b) \in \{1, 2\}$. H

Opgave 1.106. Bewijs dat $\text{ggd}(3a, 6a + 1) = 1$.

Opgave 1.107. (IMO 1959 dag 1 vraag 1) Bewijs dat de breuk $\frac{21n+4}{14n+3}$ voor geen enkel natuurlijk getal n vereenvoudigbaar is.

Opgave 1.108. Bewijs dat $\text{ggd}(2n^2 - 1, n + 1) = 1$.

Opgave 1.109. Toon aan dat $\text{kgv}(n, n + 1) = n^2 + n$.

Opgave 1.110. Stel dat $\text{ggd}(a, b) = 1$. Bewijs dat $\text{ggd}(a + b, a^2 - ab + b^2) \in \{1, 3\}$.

Opgave 1.111. Bewijs dat voor natuurlijke getallen x en y geldt dat $17 \mid 2x + 3y$ als en slechts als $17 \mid 9x + 5y$.

Opgave 1.112. (NWO 1982 ronde 2 vraag 4) Stel $n = 9^{753}$. Bepaal $\text{ggd}(n^2 + 2, n^3 + 1)$.

Opgave 1.113. 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

1.3 Priemgetallen

Opgave 1.114. 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 1.115. Vind alle priemgetallen p, q en r zo dat $p \mid q - r$ en $p \mid q + r$.

Opgave 1.116. (CanMO 1978 vraag 2) Vind alle koppels (a, b) van natuurlijke getallen die voldoen aan $2a^2 = 3b^3$. H

Opgave 1.117. (IrMO 2007 dag 1 vraag 1) Vind alle koppels priemgetallen (p, q) zo dat $p \mid q + 6$ en $q \mid p + 7$.

Opgave 1.118. (NWO 2007 vraag 4) Voor hoeveel natuurlijke getallen n waarvoor $1 \leqslant n \leqslant 100$ geldt dat n^n een volkomen kwadraat is?

Opgave 1.119. (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 1.120. 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 1.121. (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 1.122. (BaMO 1989 vraag 1) Vind alle natuurlijke getallen die de som zijn van de kwadraten van hun vier kleinste positieve delers. H

Opgave 1.123. Vind alle $n \in \mathbb{N}$ waarvoor $\frac{n!-1}{2n+7} \in \mathbb{N}$.

Opgave 1.124. Zij $a \in \mathbb{N}$ geen kwadraat. Bewijs dat de vergelijking $n! + a = b^2$ een eindig aantal oplossingen (n, b) heeft.

Vermoeden. ttl = Probleem van Brocard

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

1.4 Aritmetische functies

Opgave 1.125. Toon aan dat het product van de positieve delers van een natuurlijk getal n gelijk is aan $n^{\frac{\tau(n)}{2}}$. H

Opgave 1.126. 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 1.127. 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 1.128. Vind alle natuurlijke getallen $n > 1$ waarvoor $\varphi(n) \mid n$. H

Opgave 1.129. Vind alle natuurlijke getallen $n > 1$ waarvoor $\varphi(\varphi(n)) \mid n$. H

Opgave 1.130. (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.

Opgave 1.131. Bewijs voor $n \geqslant 1$ dat

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

1.5 Rationale en irrationale getallen

1.6 Dirichlet convolutie

Opgave 1.132. Bewijs dat $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$ voor $n \in \mathbb{N}^{\times}$.

Opgave 1.133. Op hoeveel manieren kan een natuurlijk getal geschreven worden als product van

A. 3 natuurlijke getallen?

B. $n \geqslant 1$ natuurlijke getallen?

Schrijf je resultaten als convolutie.

Opgave 1.134. Zij f een totaal multiplicatieve functie en g inverteerbaar. Bewijs dat $(fg)^{-1} = fg^{-1}$.

Opgave 1.135. Bewijs dat voor $n \geqslant 1$,

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

Opgave 1.136. Aan welke bekende functies zijn A

$$\sum_{d^2|n} \mu(d) \qquad \text{en} \qquad \sum_{d^2|n} \mu(\tfrac{n}{d})$$

gelijk?

1.7 Technieken

Ontbinden

Opgave 1.137. (JWO 2010 finale vraag 2) Vind alle gehele getallen a en b waarvoor $\frac{1}{a} - \frac{1}{b} = 6$.

Opgave 1.138. Zij p een priemgetal. Vind alle natuurlijke getallen a en b zo dat $pa + pb = ab$.

Opgave 1.139. Vind alle priemgetallen p en natuurlijke getallen n zo dat $8^p + 27^p = p^n$.

Opgave 1.140. 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 1.141. (JWO 2004 finale vraag 4) Vind alle $a, b \in \mathbb{N}$ zo dat

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

Opgave 1.142. (Q-E-D Competitie augustus 2012) . Voor welke natuurlijke getallen n H is $n^4 + 4^n$ een priemgetal?

Opgave 1.143. (Q-E-D Competitie augustus 2012) . Voor welke natuurlijke getallen n is $2^{2^n-2}+1$ een priemgetal? H

Opgave 1.144. Vind alle priemgetallen p en q zo dat $p^2+7pq+q^2$ een volkomen kwadraat is. H

Opgave 1.145. (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 1.146. Zij $a, b, c, d \in \mathbb{N}^\times$ met $ab = cd$. Bewijs dat $a^2 + b^2 + c^2 + d^2$ geen priemgetal is.

Ongelijkheden

Opgave 1.147. (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.

Opgave 1.148. (IMOSL 2002 vraag 10) Zij $n \geqslant 2$ een natuurlijk getal, met delers $1 = d_1 < d_2 < \cdots < d_k = n$. Bewijs dat $d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$ altijd kleiner is dan n^2 en bepaal wanneer het een deler is van n^2. H

Opgave 1.149. (Polen MO 2013 finale vraag 1) Vind alle gehele getallen x, y zo dat $x^4 + y = x^3 + y^2$. H

Opgave 1.150. (WiNA 2010) Bepaal de priemgetallen p waarvoor zowel $\frac{p+1}{2}$ als $\frac{p^2+1}{2}$ volkomen kwadraten zijn.

Extremenprincipe

Opgave 1.151. Bepaal de gehele oplossingen van $3a^2 + 3b^2 + 19ab = 0$.

Vieta Jumping

Opgave 1.152. (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.

Opgave 1.153. (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 $a = b$.

Hoofdstuk 2. Modulorekenen

2.1 Congruentie

Bij het modulair rekenen of modulorekenen voeren we een nieuw begrip in, congruentie.

Definitie. 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 1.1.5 noteren $a \equiv 0 \pmod{c}$.

Definitie. 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.[15] Vaak is het gewoon een handig woord om beknopt iets uit te drukken.

Stelling 2.1.1. 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 $0 \leqslant r_1, r_2 \leqslant |c|$. 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 $a - b \equiv 0 \pmod{c}$.

[15] In deel 2 bekijken we de restklassen als objecten op zichzelf. Verassend genoeg blijkt deze licht verschillende invalshoek heel wat krachtiger te zijn.

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 $0 \leqslant r \leqslant |c|$. Dan is $b = a - kc = (q - k)c + r$. b heeft dus dezelfde rest als a, dus $a \equiv b \pmod{c}$. □

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 eigenschap 2.1.1.1 toelaat om dit te doen, omdat $a \equiv b$ equivalent is met $a - b \equiv 0$ en dus met $c \mid a - b$.

Opgave 2.1. Bewijs zelf eigenschappen 2 tot en met 5.

Opgave 2.2. Toon telkens aan met een voorbeeld dat het omgekeerde van de eigenschappen 2, 3, 4 en 5 niet steeds waar is.

Voorbeeld 2.3. 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 mod 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 2.4. 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 2.5. 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 2.6. Bepaal het kleinste natuurlijk getal n zo dat $\frac{9^{20}+n}{41}$ een natuurlijk getal is.

Voorbeeld 2.7. Bereken 4^{12} mod 12.

Oplossing.
We bekijken eerst 4^2 mod 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 2.8. Bereken

A. 3^8 mod 6.

B. 9^{20} mod (-36).

C. 5^{32} mod 40.

D. 7^{2000} mod (-42).

Opgave 2.9. Bewijs dat een natuurlijk getal deelbaar is door 9 als en slechts als de som van zijn cijfers deelbaar is door 9. H

Opgave 2.10. Stel $a \neq b$. Bewijs dat voor $n > 0$ geldt dat $a^n - b^n$ deelbaar is door $a - b$, zonder gebruik te maken van de algemene ontbinding van $a^n - b^n$. H

Lemma 2.1.2.

$a \equiv b \pmod{c}$ 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 $ad \equiv bd \pmod{cd}$. □

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

Opgave 2.12. 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 2.13. Bewijs dat er oneindig veel priemgetallen van de vorm $4k + 3$ bestaan.

Opgave 2.14. Bewijs dat er oneindig veel priemgetallen van de vorm $6k + 5$ bestaan.

2.2 Lineaire congruenties

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

2.2.1 Inverteerbaarheid

Definitie. 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

$$ax + by = 1 \tag{2.1}$$

in x en y. De volgende stelling volgt daarom onmiddelijk uit stelling 1.2.7.

Stelling 2.2.1. 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 van 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.

2.2.2 Lineaire congruenties

Lemma 2.2.2. 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 $m \mid d(x - y) \Leftrightarrow dx \equiv dy \pmod{m}$. □

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 $x \equiv y$. □

Voorbeeld 2.15. Vind alle natuurlijke getallen n met $0 \leqslant n < 17$ 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 $n = 24 \bmod 17 = 7$.
We kunnen dus de inverse van a gebruiken, indien die bestaat, om (2.2) op te lossen. Indien men de inverse zomaar kan bedenken is het oplossen van (2.2) dus helemaal niet moeilijk. Lemma 2.2.2 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

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

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

De volgende lemma's volgen onmiddellijk uit de definitie.

Lemma 2.2.3.

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

Lemma 2.2.4.

a en b zijn inverteerbaar als en slechts ab inverteerbaar is. Er geldt dat $(ab)^{-1} \equiv a^{-1}b^{-1}$.

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 2.2.5.

Er geldt dat $a^{-n} \equiv (a^n)^{-1} \pmod{m}$ als $n \in \mathbb{N}$ en $\text{ggd}(a, m) = 1$.

Gevolg 2.2.6.

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. Lineaire congruentie

Een *lineaire congruentie* is een congruentie van de vorm

$$ax \equiv b \pmod{c} \tag{2.2}$$

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 (2.2) 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 2.2.7.

De lineaire congruentie (2.2) 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 (2.2) is equivalent aan het vinden van oplossingen van

$$ax + cy = b. \tag{2.3}$$

Wegens Stelling 1.2.7 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 $k \in \{1, \ldots, d\}$, na reductie modulo c alle verschillende oplossingen geven modulo c. Er zijn precies d zo'n waarden voor k. □

Het zou omslachtig zijn om voor het oplossen van (2.2) steeds (2.3) op te lossen. Dat is in sommige gevallen ook helemaal niet nodig:

Als a geen inverse heeft kan de congruentie via Lemma 2.1.2 gereduceerd worden tot een congruentie waarin dat wel het geval is:

Voorbeeld 2.16. Vind alle natuurlijke getallen n met $0 \leqslant n < 12$ zo dat $9n \equiv 6 \pmod{12}$.

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 $0 \leqslant n < 12$ 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.

2.2.3 Stelsels congruenties: de Chinese reststelling

Net zoals er stelsels van vergelijkingen zijn, zijn er ook stelsels van congruenties. De *Chinsese reststelling* bespreekt de oplossingen van zo'n stelsel.

Stelling 2.2.8. Chinese reststelling

Als $m_1, m_2, \ldots, m_n$ paarsgewijs relatief prieme gehele getallen zijn, en $a_1, a_2, \ldots, a_n$ zijn willekeurige gehele getallen, dan bestaan er oneindig veel getallen x zo dat $x \equiv a_k \pmod{m_k}$ voor elke k. Alle oplossingen voor x zijn bovendien congruent modulo $m_1 m_2 \cdots m_n$.

De stelling wordt gewoonlijk afgekort als CRS.
Even een voorbeeld om dit duidelijk te maken. 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 2.17. Bewijs de 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 $x = r_1a_1 + r_2a_2 + \cdots r_na_n$ 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 2.18. Toon aan dat er voor elk natuurlijk getal $n > 0$ een getal m bestaat zo dat $n + 1 \mid m$ en $n \mid m + 1$. H

Opgave 2.19. Vind alle gehele getallen x zo dat $5x \equiv 3 \pmod{7}$ en $6x \equiv 8 \pmod{10}$.

Opgave 2.20. Toon aan dat er een rij bestaat van 19 opeenvolgende natuurlijke getallen die elk deelbaar zijn door de 17-de macht van een natuurlijk getal.

2.2.4 De Chinese reststelling: veralgemening

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 2.2.9. Chinsese reststelling, algemeen geval

Als $m_1, m_2, \ldots, m_n$ en $a_1, a_2, \ldots, a_n$ 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 $\text{kgv}(m_1, m_2, \ldots, m_n)$.

Opgave 2.21. Bewijs de uitbreiding van de 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 $\text{kgv}(m_1, \ldots, m_n)$, 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 $a_1 = q_1 s m_1 + q_1 t m_2 + r$ en $a_2 = q_2 s m_1 + q_2 t m_2 + r$.

C. Toon aan dat $x = q_1 t m_2 + q_2 s m_1 + t$ voldoet.

D. Toon aan dat er oneindig veel oplossingen 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 $j \leqslant n$. 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 $0 \leqslant k < n$.
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

$$b_n \equiv a_n \pmod{\text{ggd}(p_k, m_n)} \qquad \text{en} \qquad b_{n+1} \equiv a_{n+1} \pmod{\text{ggd}(p_k, m_{n+1})}.$$

G. Toon aan dat

$$b_n \equiv b_k \pmod{\text{ggd}(p_k, m_n)} \qquad \text{en} \qquad b_{n+1} \equiv b_k \pmod{\text{ggd}(p_k, m_{n+1})}.$$

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 1.3.6 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 $\text{kgv}(p_1, p_2, \ldots, p_n)$. We zijn bijna klaar:

I. Toon aan dat de oplossingen congruent zijn modulo $\text{kgv}(m_1, m_2, \ldots, m_{n+1})$.

Ziezo, daarmee is de kous af. Wegens volledige inductie geldt de stelling nu voor elk natuurlijk getal n.

Opgave 2.22. (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 $r \in \{1, 2, \ldots, k\}$.

2.3 Kwadraatresten

Definitie. 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 2.11.3 is daaraan toegewijd.

Lemma 2.3.1.

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 $0 \leqslant b < 3$ 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. □

Opgave 2.23. 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 2.3.2.

Er zijn precies $\frac{p+1}{2}$ kwadraten modulo een oneven priemgetal p.

Opgave 2.24. Bewijs dat dit inderdaad zo is.

A. Toon aan dat het volstaat om het aantal verschillende resten van a^2 met $0 \leqslant a < p$ te bekijken.

B. Wanneer geldt dat $a^2 \equiv b^2$ als $0 \leqslant a, b < p$?

C. Toon nu aan dat het aantal verschillende resten gelijk is aan $\frac{p+1}{2}$.

Opgave 2.25. Vind alle kwadraatresten modulo 5.

Analoog aan kwadraatresten definiëren we n-demachtsresten in het algemeen.

Definitie. 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 2.26. Vind alle derdemachtsresten modulo 7.

Opgave 2.27. Toon aan dat $n^2 + 1$ nooit deelbaar is door 3.

Opgave 2.28. Stel dat $3 \mid a^2 + b^2$. Toon aan dat $9 \mid a^2 + b^2$.

2.3.1 Toepassing: Diophantische vergelijkingen

Voorbeeld 2.29. 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 mogelijke rest is, zoals je zal zien in het volgende voorbeeld.

Voorbeeld 2.30. 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: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 1$, $3^2 \equiv 4$, $4^2 \equiv 1$. 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 2.31. Vind alle natuurlijke getallen n en priemgetallen p, q zo dat $p^2 + q^2 = 2^n$.

Opgave 2.32. Vind alle gehele getallen a en n met $n \geqslant 0$ zo dat $a \cdot (a + 2) = 3^n - 2$.

2.3.2 Pythagorese drietallen

Definitie. 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 2.3.3.

Alle primitieve Pythagorese drietallen zijn van de vorm

$$(2xy, x^2 - y^2, x^2 + y^2) \qquad \text{of} \qquad (x^2 - y^2, 2xy, x^2 + y^2)$$

met $\text{ggd}(x, y) = 1$.

Opgave 2.33. 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 $(2xy, x^2 - y^2, x^2 + y^2)$, of ook $(x^2 - y^2, 2xy, x^2 + y^2)$ omdat we a en b konden omwisselen.

Het is helaas niet zo dat ook elk niet-primitief drietal van die vorm is.

Opgave 2.34. Vind een Pythagorees drietal (a, b, c) met b oneven, dat niet van de vorm $(2xy, x^2 - y^2, x^2 + y^2)$ 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.

2.4 Stelling van Wilson

De stelling van Wilson bewijst vaak zijn nut. Problemen waarin Wilson van pas komt zijn echter vaak eenvoudig herkenbaar.

Stelling 2.4.1. Stelling van Wilson

Als p een priemgetal is, dan geldt

$$(p - 1)! \equiv -1 \pmod{p}.$$

Opgave 2.35. Bewijs de stelling van Wilson.

Het is eenvoudig te controleren dat de stelling geldt voor 2. Veronderstel nu dat $p > 2$.

A. Vind alle gehele getallen a met $0 \leqslant a < p$ zo dat $a^2 \equiv 1 \pmod{p}$.

B. Toon aan dat voor elk geheel getal a met $0 \leqslant a < p$ dat niet voldoet aan $a^2 \equiv 1$, er een ander geheel getal b met $0 \leqslant b < p$ bestaat zo dat $ab \equiv 1 \pmod{b}$, en dat zo'n getal b steeds bij precies één getal a hoort.

C. Toon aan dat $(p-1)! \equiv -1 \pmod{p}$.

Opgave 2.36. Toon aan dat $p! + p$ deelbaar is door p^2 als p een priemgetal is.

Stelling 2.4.2.

Als p een oneven priemgetal is k is een natuurlijk getal met $k \leqslant p$, 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 2.37. Bereken $1! \cdot 2! \cdots 10! \bmod 11$.

Gevolg 2.4.3.

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 2.4.4.

-1 is een kwadraat modulo een priemgetal p als en slechts als $p = 2$ of $p \equiv 1 \pmod{4}$.

Opgave 2.38. Bewijs dat dit inderdaad het geval is.

2.5 Multiplicatieve orde

Definitie. Orde

Als $a, b \in \mathbb{Z}_0$ noemen we de kleinste $n \in \mathbb{N}^\times$ waarvoor $a^n \equiv 1 \pmod{b}$, indien n bestaat, de orde van a modulo b. We noteren $n = \text{ord}_b(a)$.

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 2.5.1.

Er geldt dat a een orde heeft modulo b als en slechts als $\text{ggd}(a, b) = 1$.

Opgave 2.39. Bewijs deze voorwaarde.

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 2.5.2.

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 $3, 3^2, 3^3, \ldots$ dan vinden we de rij $3, 9, 5, 4, 1, 3, 9, 5, 4, 1, \ldots$ De rij is periodiek met periode 5, dus $O_{11}(3) = 5$. 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 2.5.3.

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, $3 \cdot 4 = 12 \equiv 1$.

2.5.1 Eigenschappen van de orde: het ordelemma

Stelling 2.5.4. 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 2.40. Bewijs het ordelemma.

Gevolg 2.5.5.

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 2.2.2 en Gevolg 2.2.6 geldt dat $a^x \equiv a^y$ als en slechts als $a^{x-y} \equiv 1$. Wegens de vorige stelling is dit equivalent met $n \mid x - y$. □

Het volgende lemma zegt iets over de orde van het product van gehele getallen met dezelfde modulus.

Lemma 2.5.6.

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 $kl = x$. □

Lemma 2.5.7.

Zij a, k, n gehele getallen. Dan is $\text{ord}_n(a) = \text{ord}_n(a^k)$ als en slechts als $\text{ggd}(k, \text{ord}_n(a)) = 1$.

Opgave 2.41. Bewijs dit lemma.

We kunnen, onder bepaalde voorwaarden, ordes met verschillende moduli combineren:

Lemma 2.5.8.

Zij a, n, m gehele getallen met $\text{ggd}(m, n) = 1$, $\text{ord}_m(a) = x$ en $\text{ord}_n(a) = y$. Dan geldt $\text{ord}_{mn}(a) = \text{kgv}(x, y)$.

Opgave 2.42. Bewijs bovenstaand lemma.

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 2.43. 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 $a \equiv 1 \pmod{b}$?

2.5.2 De kleine stelling van Fermat

Stelling 2.5.9. Kleine stelling van Fermat

Als p een priemgetal is en $p \nmid a$, dan is

$$a^{p-1} \equiv 1 \pmod{p}.$$

Opgave 2.44. Bewijs de stelling van Fermat.
Beschouw de getallen $x_k = ka$ voor $1 \leqslant k \leqslant p-1$

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 $1, 2, \ldots, p-1$ 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 2.5.10.

Voor elk geheel getal a en elk priemgetal p geldt dat $a^p \equiv a \pmod{p}$.

Opgave 2.45. Bewijs dit gevolg.

Gevolg 2.5.11.

Voor elk priemgetal p geldt dat $\mathrm{ord}_p(a) \mid p-1$.

Bewijs.
Dit volgt meteen uit het ordelemma en de stelling van Fermat □

Opgave 2.46. Toon aan dat $1^{10} + 2^{10} + \cdots + 9999^{10}$ deelbaar is door 11.

Opgave 2.47. Vind alle priemgetallen p en $a, b \in \mathbb{N}$ zo dat $2^p + a^{p-1} = p^b$.

Opgave 2.48. (BrMO 1 2007 vraag 1) Vind vier priemgetallen kleiner dan 100 die delers zijn van $3^{32} - 2^{32}$.

2.5.3 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 samengsestelde getallen een gelijkaardige eigenschap geldt. Daar geeft de stelling van Euler een antwoord op.

Stelling 2.5.12. 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 2.5.13. 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 2.49. Toon deze eigenschap aan. H

Opgave 2.50. Bewijs 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 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Zoals je hebt gemerkt is dit bewijs nogal langdradig en onelegant. Nochtans is het best wel een interessante techniek om de stelling eerst te bewijzen voor priemmachten en pas daarna voor algemene getallen. Zoals je misschien hebt gemerkt kwam de formule voor $\varphi(n)$ om de hoek kijken. We komen nog terug op deze bewijstechniek wanneer we het over primitieve wortels zullen hebben.
Er is, naast dit bewijs, ook een bewijs mogelijk analoog aan dat van de kleine stelling van Fermat.

Opgave 2.51. 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 2.5.14.

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. □

Stelling 2.5.15.

Als $a, b \in \mathbb{Z}$ en $n > 1$ zo dat $\text{ggd}(ab, n) = 1$ en $n \mid a^n - b^n$, dan is $a - b$ deelbaar door de kleinste priemdeler van n.

2.6 Polynoomcongruenties

Definitie

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. Monische veelterm

Een veelterm $f \in \mathbb{C}[x]$ waarvan de hoogstegraadscoëfficiënt 1 is noemt men monisch.

Lemma 2.6.1.

Als $f, g \in \mathbb{Q}[x]$ monisch zijn en $fg \in \mathbb{Z}[x]$, dan zijn $f, g \in \mathbb{Z}[x]$.

Opgave 2.52. We bewijzen lemma 2.6.1.

Stel $f(x) = x^k + a_{k-1}x^{k-1} + \cdots + a_0$ en $g(x) = x^l + b_{l-1}x^{l-1} + \cdots + b_0$. 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 priemdeler 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 $mnfg$ niet deelbaar is door p.

Dit is echter onmogelijk omdat $p \mid mn$ en $fg \in \mathbb{Z}[x]$. Dus $mn = 1$, zodat $f, g \in \mathbb{Z}[x]$.

2.6.1 Begrippen

We breiden de betekenis van enkele begrippen uit tot het modulorekenen.

Definitie. 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. 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. 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 2.6.2. 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 $n \in \mathbb{N}^\times$.

Opgave 2.53. Bewijs deze eigenschappen. H

Definitie. 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.

2.6.2 Factorisatiestellingen

Stelling 2.6.3.

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 $f = a_0 + a_1 x + \cdots + a_k x^k$, dan is

$$f \equiv a_0 - a_0 + a_1(x-n) + \cdots + a_k(x^k - n^k)$$

omdat $a_0 + a_1 n + \cdots + a_k n^k \equiv 0$. Elke veelterm $a_1(x-n), a_2(x^2-n^2), \ldots, a_k(x^k-n^k)$ kan ontbonden worden door een factor $(x-n)$ voorop te zetten. Dus ook hun som f kan ontbonden worden in de vorm $(x-n)\cdot g(x)$. g heeft graad $n-1$ omdat $a_k \not\equiv 0$. □

Stelling 2.6.4.

Als p een priemgetal is heeft een veelterm van graad n modulo p hoogstens n nulpunten modulo p.

Opgave 2.54. Bewijs deze stelling.
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.

A. 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 $a \in \mathbb{Z}$.

B. Toon aan dat f toch geen graad heeft.

De vorige stelling laat een alternatief bewijs voor de stelling van Wilson toe.

Opgave 2.55. Bewijs de stelling van Wilson door gebruik te maken van stelling 2.6.4.
Zij p een priemgetal. Beschouw de veelterm

$$f(x) = (x-1)(x-2)\cdots(x-(p-1)) - x^{p-1} + 1.$$

A. Toon aan dat f hoogstens van graad $p-2$ is modulo p.

B. Toon aan dat f een nulveelterm is modulo p.

C. Vind nu een handige x om uit $f(x) \equiv 0 \pmod{p}$ de stelling van Wilson af te leiden.

Stelling 2.6.5.

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 2.56. Bewijs stelling 2.6.5.
Stel $p-1 = dk$ en $f(x) = 1 + x^d + (x^d)^2 \cdots + (x^d)^{k-1}$.

A. Toon aan dat $x^{p-1} - 1 = (x^d - 1)f(x)$ precies dk nulpunten heeft modulo p.

B. Toon aan dat $x^d - 1$ precies d nulpunten heeft modulo p.

2.7 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. Primitieve wortel

We noemen a een primitieve wortel modulo n als $\text{ord}_n(a) = \varphi(n)$.

Opgave 2.57. 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 $n \geqslant 1$.

2.7.1 Nodige voorwaarde

Stelling 2.7.1. 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 2.58. Stel $n = p_1^{e_1} \cdots p_k^{e_k}$. Bewijs dat er slechts een primitieve wortel kan bestaan modulo n als $\text{ggd}(\varphi(p_1^{e_1}), \ldots, \varphi(p_k^{e_k})) = 1$. Leid hier de vorige stelling uit af.

2.7.2 Existentie

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 2.7.2.

Als p een oneven priemgetal is en q is een priemdeler van p zo dat $q^k \mid p - 1$, dan bestaat er een getal met orde q^k modulo p.

Opgave 2.59. Bewijs zelf eens.

Stelling 2.7.3.

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 $d = q_1^{e_1} \cdots q_k^{e_k}$. Lemma's 2.5.6 en 2.7.2 bieden al wat nodig is om de stelling te bewijzen. □

Gevolg 2.7.4.

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 $1, g, g^2, \ldots, g^{d-1}$ 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 2.5.7 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. □

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 2.7.5.

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 2.60. Bewijs bovenstaand lemma.

Stelling 2.7.6.

Zij w een primitieve wortel modulo een oneven priemgetal p. Dan is w of $w + p$ een primitieve wortel modulo p^k voor alle $k > 0$.

Opgave 2.61. Bewijs deze stelling.

Er rest nog het geval $2p^k$. Ook hier zullen primitieve wortels bestaan.

Opgave 2.62. 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 2.7.7.

Er bestaat een primitieve wortel modulo $2p^k$ met p priem.

2.7.3 Karakterisaties

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 2.7.8.

w is een primitieve wortel is modulo n als en slechts als de resten van $w, w^2, \ldots, w^{\varphi(n)}$ bij deling door n allemaal verschillend zijn.

Bewijs.
Wegens Gevolg 2.5.2 is dit een equivalente formulering van $\text{ord}_n(w) = \varphi(n)$. □

2.7.4 Gevolgen

Gevolg 2.7.9.

Als w een primitieve wortel is zijn de resten van $w, w^2, \ldots, w^{\varphi(n)}$ precies de getallen in $\{1, \ldots, n\}$ die relatief priem zijn met n. Elke andere primitieve wortel moet dus van de vorm w^k zijn.

Stelling 2.7.10.

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 Gevolg 2.5.7 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 2.63. Stel dat er een primitieve wortel bestaat modulo n en zij A de verzameling van natuurlijke getallen in $\{1, \ldots, n\}$ relatief priem met n. Toon aan dat

$$\prod_{a \in A} a \equiv -1 \pmod{n},$$

en bewijs de stelling van Wilson.

Stelling 2.7.11. Product van primitieve wortels

Het product van alle primitieve wortels modulo p is congruent met 1 modulo p.

Opgave 2.64. Bewijs deze eigenschap van primitieve wortels. H

Stelling 2.7.12. Som van primitieve wortels

De som van alle primitieve wortels modulo p is congruent met $\mu(p-1)$ modulo p.

Opgave 2.65. Bewijs deze eigenschap van primitieve wortels.

Opgave 2.66. Zij p een priemgetal. Bewijs dat de som van de vijdemachten van $1, 2, \ldots, p-1$ deelbaar is door p.

Opgave 2.67. Toon aan dat als a een primitieve wortel is modulo n met $n > 2$, dan $n \mid a^{\frac{\varphi(n)}{2}} + 1$.

Opgave 2.68. Bepaal de grootste gemene deler van de getallen van de vorm $n^{13} - n$.

2.7.5 Indexrekenen

Definitie. Index

Zij n een natuurlijk getal met een primitieve wortel w en $a \in \mathbb{Z}$ met $\gcd(a, n) = 1$. Het unieke natuurlijke getal $k \in \{0, \ldots, \varphi(n)-1\}$ waarvoor $w^k \equiv a \pmod{n}$ noemen we de *index* van k modulo n t.o.v de *basis* w.

2.8 Lifting The Exponent

Het Lifting The Exponent Lemma, afgekort LTE, bestaat uit vier lemma's die vaak nuttig blijken op wedstrijden. Het is inmiddels voldoende ingeburgerd om het op wedstrijden te vermelden zonder bewijs.

2.8.1 Het eigenlijke LTE

Het eerste lemma dient vooral ter ondersteuning van de volgende lemma's. Het zal in de praktijk weinig of niet voorkomen, of niet onder die naam vermeld worden vanwege zijn eenvoud.

Lemma 2.8.1.

Als p een priemgetal is, $p \nmid n, x, y$ en $p \mid x - y$, dan geldt

$$\nu_p(x^n - y^n) = \nu_p(x - y).$$

Opgave 2.69. Bewijs dit lemma.

Stelling 2.8.2. 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

$$\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n).$$

Opgave 2.70. Bewijs het hoofdlemma.

We bewijzen dit via inductie op $\nu_p(n)$.

Basisstap. We tonen het aan als $\nu_p(n) = 1$. Stel dus $n = pb$ zo dat $p \nmid b$.

A. Toon aan dat $\nu_p(x^n - y^n) = \nu_p(x^p - y^p)$.

B. Toon aan dat

$$p \mid \sum_{k=0}^{p-1} x^k y^{p-k-1}.$$

Vervolgens tonen we aan dat

$$p^2 \nmid \sum_{k=0}^{p-1} x^k y^{p-k-1}. \tag{2.4}$$

Stel daarvoor $y = x + mp$.

C. Toon aan dat $x^k y^{p-k-1} \equiv x^{p-1} + kmpx^{p-2} \pmod{p^2}$.

D. Toon (2.4) aan.

E. Toon aan dat $\nu_p(x^n - y^n) = \nu_p(x - y) + 1$.

Hiermee is de basisstap voltooid.
Inductiestap. Veronderstel dat het lemma geldt voor $\nu_p(n) = a$ met $a > 0$. We tonen het lemma nu aan voor $\nu_p(n) = a + 1$. Stel dus $n = p^{a+1}b$ zo dat p geen deler is van b.

F. Toon aan dat $\nu_p(x^n - y^n) = \nu_p(x^{p^{a+1}} - y^{p^{a+1}})$.

G. Toon aan dat $\nu_p(x^n - y^n) = \nu_p(x^{p^a} - y^{p^a}) + 1$.

H. Bewijs dat $\nu_p(x^n - y^n) = \nu_p(x - y) + \nu_p(n)$.

Het is nu bewezen via inductie.

Gevolg 2.8.3.

Als n oneven is, p oneven, $p \nmid x, y$ en $p \mid x + y$, dan

$$\nu_p(x^n + y^n) = \nu_p(x + y) + \nu_p(n).$$

2.8.2 Het geval $p = 2$

Stelling 2.8.4. LTE voor het geval $p = 2$

Als x en y oneven zijn zo dat $4 \mid x - y$, dan geldt

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n)$$

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 2.71. Bewijs LTE als $p = 2$.
Stel $n = 2^a b$ met b oneven.

A. Toon aan dat $\nu_2(x^n - y^n) = \nu_2(x^{2^a} - y^{2^a})$.

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 $i \geqslant 0$.

C. Bewijs dat $\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(n)$.

Ook lemma 2.8.4 geldt nu als bewezen.

Gevolg 2.8.5.

Voor oneven $n \in \mathbb{N}$ geldt dat als x en y oneven zijn en $4 \mid x+y$, dan

$$\nu_2(x^n + y^n) = \nu_2(x+y) + \nu_2(n).$$

Het vierde lemma is een variatie op lemma 3. Het behandelt nog steeds het geval $p = 2$, maar de voorwaarden zijn anders.

Stelling 2.8.6. Uitbreiding op het geval $p = 2$

Als x en y oneven zijn en n even, dan

$$\nu_2(x^n - y^n) = \nu_2(x+y) + \nu_2(x-y) + \nu_2(n) - 1.$$

Opgave 2.72. Bewijs het vierde lemma.

Stel $n = 2^a b$ met b oneven.

A. Toon aan dat $\nu_2(x^n - y^n) = \nu_2(x^{2^a} - y^{2^a})$.

B. Toon aan dat $4 \mid x^2 - y^2$.

C. Toon aan dat $\nu_2(x^n - y^n) = \nu_2(x^2 - y^2) + a - 1$.

D. Bewijs dat $\nu_2(x^n - y^n) = \nu_2(x+y) + \nu_2(x-y) + \nu_2(n) - 1$.

Ook het vierde lemma is nu bewezen.

2.8.3 LTE in deelbaarheidsgedaante

LTE kent een handige quasi-equivalente vorm, waarbij verassend genoeg geen congruenties worden gebruikt.

Opgave 2.73. Stel a, b zijn gehele getallen met $a \neq b$ en $\gcd(a,b) = 1$. In Hoodstuk 1 zagen we reeds dat $\gcd(a+b, a-b) \mid 2$ en $\gcd(a^2 + ab + b^2, a-b) \mid 3$. Toon nu algemeen aan dat

$$\gcd\left(\frac{a^n - b^n}{a-b}, a-b\right) \mid n$$

voor $n > 1$.

Opgave 2.74. Zij $a, b \in \mathbb{Z}$ met $a \neq b$ en $n > 1$. Bewijs dat

$$\gcd\left(\frac{a^n - b^n}{a-b}, a-b\right) = \gcd\left(nd^{n-1}, a-b\right)$$

waarbij $d = \gcd(a,b)$.

Stelling 2.8.7. LTE in deelbaarheidsgedaante

2.8.4 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 2.75. (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 2.76. (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 2.77. (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 $a^p + b^p = p^c$.

2.9 Cyclotomische veeltermen

Cyclotomische veeltermen zijn een bijzonder soort veeltermen in $\mathbb{Z}[x]$. Ze hebben heel wat interessante eigenschappen.

2.9.1 Complexe eenheidswortels

Definitie. Eenheidswortel

Een complex getal ζ waarvoor $\zeta^n = 1$ noemen we een n-de eenheidswortel.

De n-de eenheidswortels zijn precies $e^{\frac{2\pi i}{n}}, e^{2\frac{2\pi i}{n}}, \ldots, e^{n\frac{2\pi i}{n}}$.

Definitie. Orde van een eenheidswortel

Als ζ een n-de eenheidswortel is, noemen we de kleinste $k \in \mathbb{N}^\times$ waarvoor $\zeta^k = 1$ de *orde* van ζ. We noteren $\text{ord}(\zeta)$.

De volgende eigenschap komt je vast bekend voor.

Lemma 2.9.1. Ordelemma voor eenheidswortels

Als ζ 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 $0 \leqslant r < x$.
Er volgt dat $\zeta^r = 1$, dus $r = 0$. □

Definitie. Primitieve eenheidswortel

Een n-de eenheidswortel ζ noemen we primitief als $\text{ord}(\zeta) = n$. We noemen ζ een primitieve n-eenheidswortel.

In het bijzonder is $e^{\frac{2\pi i}{n}}$ steeds primitief.

Lemma 2.9.2. Criterium voor primitiviteit

Een n-de eenheidswortel ζ is primitief als en slechts als de verzameling $\{\zeta, \zeta^2, \ldots, \zeta^n\}$ alle n-de eenheidswortels bevat.

Bewijs.
Dit volgt meteen uit Lemma 2.9.1. □

Lemma 2.9.3.

Zij $k \in \mathbb{Z}$ en ζ een primitieve n-eenheidswortel. Dan is ζ^k ook primitief als en slechts als $\text{ggd}(k, n) = 1$.

Opgave 2.78. Bewijs dit lemma.

Gevolg 2.9.4. Aantal primitieve eenheidswortels

Er zijn precies $\varphi(n)$ primitieve n-eenheidswortels.

2.9.2 Algebraïsche eigenschappen

Definitie. 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 2.9.5.

$\Phi_n(x)$ heeft graad $\varphi(n)$.

Bewijs.
Dit volgt uit gevolg 2.9.4. □

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 de volgende stelling.

Stelling 2.9.6.

Er geldt dat

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Bewijs.
Aangezien elke n-de eenheidswortel ζ een unieke orde heeft komt elke factor $(x - \zeta)$ een 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 complexere cyclotomische veeltermen bepalen. Bekijk een priemgetal p. Dan is $\Phi_p(x)\Phi_1(x) = x^p - 1$, dus:

Gevolg 2.9.7.

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 Φ_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 2.9.6 en gevolg 2.9.7 gebruiken om Φ_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 2.79. Zij $p > 2$ priem. Bewijs dat $\Phi_{2p}(x) = \Phi_p(-x)$.

Stelling 2.9.8.

De cyclotomische veelterm Φ_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 2.6.1 dat ook $\Phi_n \in \mathbb{Z}[x]$. □

Gevolg 2.9.9.

Als $a \in \mathbb{Z}$ en $n \in \mathbb{N}$, dan is $\Phi_n(a) \mid a^n - 1$.

Stelling 2.9.10.

Er geldt dat

$$\Phi_n(x) = \prod_{d|k} \left(x^{\frac{n}{d}} - 1\right)^{\mu(d)}$$

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 stellingen 1.6.13 en 2.9.6. □

Opmerking.
We zullen de voorwaarde $x^n \neq 1$ in het vervolg niet steeds vermelden, en gewoon veronderstellen dat hieraan voldaan is.

Gevolg 2.9.11.

Er geldt dat $\Phi_n(x) > 0$ voor alle $x > 1$ en $n \in \mathbb{N}^\times$.

Lemma 2.9.12.

Zij p een priemgetal en $n \in \mathbb{N}^\times$, dan geldt

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{als } p \mid n \\ \frac{\Phi_n(x^p)}{\Phi_n(x)} & \text{als } p \nmid n. \end{cases}$$

Opgave 2.80. Bewijs lemma 2.9.12.

Gevolg 2.9.13.

Als p priem is en $k, n \in \mathbb{N}^\times$ 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 2.9.12. □

2.9.3 Toepassingen in de getaltheorie

Lemma 2.9.14.

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 'saaie' eigenschappen achter de rug. Hoog tijd om de cyclotomische veeltermen met getaltheorie te vermengen.

2.9.3.1 Priemdelers van cyclotomische veeltermen

Lemma 2.9.15.

Zij $a \in \mathbb{Z}$, $n, d \in \mathbb{N}$ zo dat $d \mid n$ en $d < n$. Als p een gemeenschappelijke priemdeler is van $\Phi_n(a)$ en $\Phi_d(a)$, dan geldt $p \mid n$.

Opgave 2.81. Bewijs dit lemma.

Stelling 2.9.16.

Zij $n \in \mathbb{N}$ en $a \in \mathbb{Z}$. Elke priemdeler p van $\Phi_n(a)$ voldoet aan $p \equiv 1 \pmod{n}$ of $p \mid n$.

Opgave 2.82. Bewijs deze stelling.

p is geen deler van a, aangezien $p \mid \Phi_n(a) \mid a^n - 1$ wegens gevolg 2.9.9. Stel $\mathrm{ord}_p(a) = k$.

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 $p \mid n$.

De volgende stelling is hier een heel interessant gevolg van:

Stelling 2.9.17.

Als $n \in \mathbb{N}^\times$ bestaan er oneindig veel priemgetallen van de vorm $kn + 1$.

Opgave 2.83. Bewijs deze stelling.

Het lijkt aannemelijk dat voor natuurlijke getallen a en b met $\mathrm{ggd}(a, b) = 1$ er oneindig veel priemgetallen bestaan die congruent zijn met b modulo a. Dat is wat Dirichlet bewees:

Stelling 2.9.18. Stelling van Dirichlet, kwalitatieve vorm

Als $a, b \in \mathbb{N}^\times$ met $\mathrm{ggd}(a, b) = 1$ zijn er oneindig veel priemgetallen van de vorm $ka + b$.

Het bewijs gebruikt - zover geweten is - complexe analyse en wordt daarom hier voorlopig niet gegeven. In hoofdstuk 10.2 presenteren we een kwantitatieve vorm.

Gevolg 2.9.19.

Zij p en q priemgetallen en $a \in \mathbb{Z}$ zo dat

$$q \mid 1 + a + \cdots + a^{p-1}.$$

Dan is $q = p$ of $q \equiv 1 \pmod{p}$.

Stelling 2.9.20.

Als $n, m \in \mathbb{N}$ en $a \in \mathbb{Z}$ zo dat $\mathrm{ggd}(\Phi_n(a), \Phi_m(a)) > 1$. 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, $l \in \mathbb{N}^\times$.

Opgave 2.84. Bewijs bovenstaande stelling.

Zij p een priemdeler van $\mathrm{ggd}(\Phi_n(a), \Phi_m(a))$. Stel $m = p^s x$ en $n = p^t y$ met $s, t \geqslant 0$ 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 $g = \mathrm{ggd}(x, y)$.

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 priemdeler van $\text{ggd}(\Phi_n(a), \Phi_m(a))$, dus hebben we, indien $\frac{m}{n} \neq 1$, noodzakelijk steeds hetzelfde priemgetal.

Opgave 2.85. (IMOSL 2006) Vind alle gehele oplossingen van de vergelijking

$$\frac{x^7 - 1}{x - 1} = y^5 - 1.$$

2.9.3.2 Verband met primitieve wortels

Ongeveer analoog aan oefening no bewijst men de volgende stelling:

Stelling 2.9.21.

De primitieve wortels modulo p zijn de nulpunten van Φ_{p-1} modulo p.

Opgave 2.86. Bewijs deze stelling.

Het vinden van primitieve wortels is dus equivalent aan het oplossen van de congruentie $\Phi_{p-1}(x) \equiv 0 \pmod{p}$. Helaas blijkt dit het vinden van primitieve wortels niet echt eenvoudiger te maken.

2.9.4 De stelling van Zsigmondy

Stelling 2.9.22. Stelling van Zsigmondy

Zij $a, b \in \mathbb{N}^\times$ 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 $k \in \{1, 2, \ldots, n-1\}$, behalve in de gevallen

1. $2^6 - 1^6$.
2. $n = 2$ en $a + b$ is een macht van 2.

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.

2.9.4.1 Bewijs van Zsigmondy

Definitie. Radicaal

Het radicaal van een natuurlijk getal $n \in \mathbb{N}^\times$ 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 preiemgetal. Het blijkt essentiëel in het bewijs voor de stelling van Zsigmondy.

Lemma 2.9.23.

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 $\mathrm{ord}_p(a) = q$.

Opgave 2.87. Bewijs dit lemma.

Zij nu a, b, n zoals in de stelling. We proberen te bewijzen dat er inderdaad een primitieve priemdeler te vinden is.

Reductie tot cyclotomische veeltermen We proberen de stelling te formuleren aan de hand van cyclotomische veeltermen. Bij het controleren of een priemdeler van $a^n - b^n$ primitief is kunnen we een kleine vereenvoudiging doorvoeren:

Opgave 2.88. Om te controleren of $p \mid a^n - p^n$ 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 2.89. Toon aan dat H

$$\Psi_k = \prod_{d|n} {z_{\frac{k}{d}}}^{\mu(d)} \quad \text{en} \qquad z_k = \prod_{d|k} \Psi_d.$$

Als $z_n = n = p_1^{a_1} \cdots p_r^{a_r}$ waarbij $p_{s_1}, \ldots, p_{s_t}$ 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 2.90. Bewijs dat $P_n \mid \Psi_n$, d.i.: de primitieve priemdelers van z_n zijn (met hun hele multipliciteit) bevat in de factor Ψ_n. H

Stel nu $\Psi_n = \lambda_n P_n$. In wat volgt proberen we λ_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 λ_n
Opgave 2.91.

A. Toon aan dat $\Psi_n \mid \frac{z_n}{z_d}$ voor elke deler $d < n$ van n.

B. Bewijs dat $\mathrm{rad}(\lambda_n) \mid n$.

C. Toon aan dat $\mathrm{ggd}(\lambda_n, P_n) = 1$.

Stel dat p een priemdeler van λ_n is. Stel $n = p^\alpha q$ met $p^\alpha \| n$. 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 priemdeler van λ_n is waarvoor $p \mid \Psi_q$.

E. Bewijs dat p uniek bepaald is als de grootste priemdeler van n.

Stel dus $\lambda_n = p^\beta$.

F. Bewijs dat $\beta = 1$.

Een ondergrens voor P_n

Opgave 2.92. Om te besluiten dat $P_n > 1$ onderscheiden we drie gevallen. resume,,

G. Bewijs dat $P_n > 1$ als $\lambda_n = 1$.

H. Toon aan dat $P_n > 1$ als λ_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 $P_n = 1$. resume,,

I. Bewijs dat $p > 2$.

Stel $n = p^\alpha q$ met $p \nmid q$. resume,,

J. Bewijs dat $p = \Psi_{pq}(a^{p^{\alpha-1}}, b^{p^{\alpha-1}})$ toch groter is dan p.

Dus $\alpha = 1$. resume,,

K. Bewijs dat $p = \frac{\Psi_q(a^p,b^p)}{\Psi_q}$ gelijk is aan 3.

L. Toon aan dat $n = 6$, $a = 2$ en $b = 1$.

2.9.4.2 Zsigmondy voor sommen

De volgende stelling veralgemeent de stelling van Zsigmondy voor sommen:

Gevolg 2.9.24. Stelling van Zsigmondy voor sommen

Zij $a, b \in \mathbb{N}^\times$ met $\gcd(a,b) = 1$ 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 $k \in \{1, 2, \ldots, n-1\}$, behalve in het geval $2^3 + 1^3$.

Opgave 2.93. Bewijs deze veralgemening.

2.9.4.3 Gevolgen

2.9.4.4 Sterkere resultaten

2.10 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.

2.10.1 LTE, Fermat, Euler, Bang, Zsigmondy, en Dirichlet

Herinner je de volgende eigenschap (lemma 2.5.13): als $a \equiv b \pmod{p^k}$, dan is voor alle $n \geqslant 0$ 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 $\nu_p(a^{p^n}-b^{p^n}) = n+\nu_p(a-b)$. Als dus $\nu_p(a-b) \geqslant k$ is wegens LTE zeker $\nu_p(a^{p^n}-b^{p^n}) \geqslant n+k$. 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 $k \geqslant 2$.

Deze eigenschap en LTE zijn voorbeelden van congruenties (of toch een vermomde congruentie wat LTE betreft) waarbij al aan een zekere cogruentie 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 priemmachten: als $p \nmid a$, dan is $a^{(p-1)p^{k-1}} \equiv 1 \pmod{p^k}$. Kiezen we nu $n \geqslant 0$, 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 priemmachten. (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 gespreken, bij vaste $a \in \mathbb{Z}$ aangeeft hoe groot een priemmacht 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 $k \leqslant 2$.) 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 priemmachten weten we dus al tamelijk wat. Een analoge, maar veel moeilijker te beantwoorden vraag is of er, gegeven natuurlijke getallen

a en n, een priemmacht 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 2.94. Zij $a, n \in \mathbb{N}^\times$ en n priem. Toon aan dat er een priemgetal p bestaat zo dat $\text{ord}_p(a) = n$. H

Opgave 2.95. 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 priemmacht 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 2.96. Zij $n \in \mathbb{N}^\times$. Bewijs dat er oneindig veel priemgetallen $p \equiv 1 \pmod{n}$ bestaan.

Merk op dat we dit laatste resultaat ook iets rechstreekser 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.

2.10.2 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 $p \mid a^n - b^n$ onmiddelijk 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. Wieferich-priemgetal[16]

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 2.97. 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:

[16]Naar de Duitse wiskundige Arthur Wieferich (1884-1954)

Lemma 2.10.1.

Toon aan dat een priemgetal p Wieferich is als en slechts als $\text{ord}_p(2) = \text{ord}_{p^2}(2)$.

Opgave 2.98. 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 2.5.8: 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 $\text{ord}_{mn}(a) = \text{kgv}(x, y)$.

2.10.3 Ordes en periodieke expansies

2.11 Binomiaalcongruenties

Over exponentiële congruenties weten we nu toch al tamelijk wat. Een andere klasse van congruenties zijn 'binomiaalcongruenties'.

2.11.1 De stelling van Lucas

Stelling 2.11.1. Stelling van Lucas

Zij $m, n \geqslant 0$ 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

$$\binom{n}{m} \equiv \prod_{j=0}^{k} \binom{n_j}{m_j} \pmod{p}.$$

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

Opgave 2.99. Bewijs dat

$$\nu_p\binom{n}{m} = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor - \sum_{k=1}^{\infty} \left\lfloor \frac{m}{p^k} \right\rfloor - \sum_{k=1}^{\infty} \left\lfloor \frac{n-m}{p^k} \right\rfloor$$

voor $m, n \geqslant 0$.

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 2.11.2. 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 $n \in \mathbb{N}$

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Opgave 2.100. Bewijs zelf eens. H

Dit geeft een alternatieve formule voor $\nu_p\binom{n}{m}$, namelijk

$$\nu_p\binom{n}{m} = \frac{s_p(m) + s_p(n-m) - s_p(n)}{p-1}.$$

Kummer ging nog verder en vereenvoudigde de uitdrukking $\frac{s_p(m)+s_p(n-m)-s_p(n)}{p-1}$:

Stelling 2.11.3. Stelling van Kummer

Zij $m, n \geqslant 0$ 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 $\nu_p\binom{n}{m}$ gelijk aan het aantal indices $j \leqslant k$ waarvoor $n_j < m_j$.

Opgave 2.101. Bewijs de stelling van Kummer.

Stel $r = n - m = (r_k \dots r_0)_p$. Stel $c_j = 0$ als $n_j \geqslant m_j$ en 1 als $n_j < m_j$. Stel ook $c_{-1} = 0$.

A. Bewijs dat $n_j = m_j + r_j + c_{j-1} - pc_j$ voor $0 \leqslant j \leqslant k$.

B. Bewijs dat $s_p(m) + s_p(n-m) + s_p(m) = (p-1)(c_0 + \dots + c_k) + c_k$

C. Besluit Kummer's stelling.

2.11.3 De stelling van Wolstenholme

Stelling 2.11.4. Stelling van Wolstenholme

Zij $p > 3$ een priemgetal. Dan is

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

Definitie. Wolstenholme-priemgetal

Een *Wolstenholme-priemgetal* is een priemgetal $p > 7$ waarvoor

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}.$$

Opgaven hoofdstuk 2

2.1 Congruentie

Opgave 2.102. 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 2.103. (BrMO 2003 ronde 1 vraag 1) Gegeven dat H

$$34! = 95232799cd960414084761860964 35ab000000,$$

bepaal de cijfers a, b, c en d.

Opgave 2.104. (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 2.105. (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 2.106. (CanMO 1980 vraag 1) Als $a679b$ een vijfcijferig getal is dat deelbaar is door 72, bepaal dan a en b.

Opgave 2.107. 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 2.108. (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?

Opgave 2.109. 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 2.110. (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?

Opgave 2.111. (VWO 2010 finale vraag 1) Op hoeveel nullen eindigt $101^{100} - 1$?

Opgave 2.112. Bepaal alle natuurlijke getallen n zo dat $2^n \mid 3^n - 1$.

Opgave 2.113. (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 2.114. Bepaal het laatste cijfer van $4^2 + 4^4 + 4^8 + 4^{16} + \cdots + 4^{2^{101}}$

2.2 Lineaire congruenties

Opgave 2.115. 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 2.116. n waterleliebladen liggen in een vijfer, geranschikt in een cirkel. Een kikker 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? A

2.3 Kwadraatresten

Opgave 2.117. Bewijs dat de vergelijking $x^2+y^2 = 2^k$ precies vier oplossingen in gehele getallen heeft, voor elk natuurlijk getal k.

Opgave 2.118. (JWO 2002 finale vraag 2) Bewijs dat er geen enkel getal bestaande uit meerdere gelijke cijfers na elkaar een kwadraat is.

Opgave 2.119. Vind alle oplossingen in gehele getallen van $x^2 + 4 = y^5$.

Opgave 2.120. Vind alle priemgetallen die geschreven kunnen worden als $a^4+b^4+c^4-3$, waarbij a, b, c zelf priemgetallen zijn.

Opgave 2.121. 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 2.122. (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 2.123. Bepaal alle natuurlijke getallen x, y en z zo dat $3^x + 4^y = 5^z$.

2.4 Stelling van Wilson

Opgave 2.124. Kunnen 18 opeenvolgende gehele getallen in twee gropen worden verdeeld zodanig dat het product van de getallen in elk van de groepen hetzelfde is? H A

2.5 Multiplicatieve orde

Opgave 2.125. (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 2.126. (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 2.127. 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 2.128. (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 2.129. Stel dat $\gcd(m,n) = 1$. Toon aan dat $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$.

Opgave 2.130. Vind alle natuurlijke oplossingen van $2^x + 7 = y^2$.

Opgave 2.131. Bepaal alle natuurlijke getallen a, b zo dat

$$(a+19b)^{18} + (a+b)^{18} + (19a+b)^{18}$$

een volkomen kwadraat is.

Opgave 2.132. 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 2.133. Stel $p > 5$ is een priemgetal. Toon aan dat alle delers van $\frac{6^p-1}{5}$ van de vorm $kp+1$ zijn.

Opgave 2.134. Als $a, b, n > 0$ natuurlijke getallen zijn zo dat $a \neq b$, bewijs dan dat

$$2n \mid \varphi(a^n + b^n).$$

Opgave 2.135. (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 2.136. Bepaal de drie laatste cijfers van het getal $2003^{2002^{2001}}$.

Opgave 2.137. (LIMO 2007) Zij n een natuurlijk getal, p een priemgetal en d een deler van $(n+1)^p - n^p$. Bewijs dat $d \equiv 1 \pmod{p}$.

2.6 Polynoomcongruenties

2.7 Primitieve wortels

Opgave 2.138. Zij p en q oneven priemgetallen met $q = 2p+1$. Bewijs dat -4 een primitieve wortel is modulo q.

2.8 Lifting The Exponent

Opgave 2.139. (IMOSL 1991 vraag 18) Vind de hoogste waarde van k zo dat

$$1991^k \mid 1990^{1991^{1992}} + 1992^{1991^{1990}}.$$

Opgave 2.140. 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.

2.9 Cyclotomische veeltermen

Opgave 2.141. Noteer met Φ_n' de afgeleide van Φ_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 2.142. (IMOSL 2002) Zij $p_1, p_2, \ldots, p_n$ verschillende priemgetallen groter dan 3. Bewijs dat $2^{p_1 \cdots p_n} + 1$ minstens 4^n positieve delers heeft.

2.10 Recapitulatie exponentiële congruenties

2.11 Binomiaalcongruenties

Opgave 2.143. Zij p een priemgetal. Bewijs dat $\binom{2p}{p} \equiv 2 \pmod{p}$.

Opgave 2.144. Zijn n en q natuurlijke getallen met $n \geqslant 5$ en $2 \leqslant q \leqslant n$. Bewijs dat $q-1$ een deler is van $\left\lfloor \frac{(n-1)!}{q} \right\rfloor$. H

2.12 Overige opgaven

Opgave 2.145. (CanMO 1971 vraag 6) Toon aan dat voor alle $n \in \mathbb{Z}$, $n^2 + 2n + 12$ geen veelvoud is van 121.

Opgave 2.146. (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 2.147. (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 2.148. (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 2.149. (USAMO 1979 vraag 1) Vind alle 14-tallen van (niet noodzakelijk verschillende) natuurlijke getallen waarvoor de som van de vierdemachten 1599 is.

Opgave 2.150. Zij $p \geqslant 5$ een priemgetal. Bewijs dat $7^p - 6^p - 1$ deelbaar is door 43.

Opgave 2.151. 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 2.152. (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 2.153. 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 2.154. 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 2.155. (USAMO 1986 vraag 3) Bepaal het kleinste natuurlijk getal $n > 1$ zo dat het rekenkundig gemiddelde van de getallen $1^2, 2^2, \ldots, n^2$ zelf een kwadraat is.

Opgave 2.156. 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 2.157. (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 2.158. 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 2.159. (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.

Hoofdstuk 3. Kwadraatresten

In hoofdstuk 1.8.5 maakte je al kennis met kwadraatresten. Het bleek dat er niet steeds evenveel kwadraatresten als gewone resten zijn.

3.1 Het Legendre-symbool

Definitie. Legendre-symbool

Is $a \in \mathbb{Z}$ en p een oneven priemgetal, dan definiëren we het *Legendre-symbool* of *kwadratisch karakter*[17] 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 3.1.1.

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

$$\left(\frac{a^2}{p}\right) = 1.$$

Opgave 3.1. Bewijs deze eigenschappen van het Legendre-symbool.

Opgave 3.2. Toon aan dat

$$\sum_{k=1}^{p} \left(\frac{k}{p}\right) = 0$$

als p een oneven priemgetal is.

3.1.1 Het criterium van Euler en multiplicativiteit

Stelling 3.1.2. Criterium van Euler

Er geldt dat

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Opgave 3.3. Bewijs het criterium van Euler.

A. Bewijs het criterium in het geval dat $p \mid a$.

[17] In een verder hoofdstuk komt een verantwoording voor het woord *karakter*.

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 3.1.3. 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 $n \in \mathbb{N}^\times$.

Het criterium van Euler laat ons een 'properder' bewijs toe van stelling 2.4.4.

Opgave 3.4. Bewijs dat -1 een kwadraatrest is modulo een priemgetal p als en slechts als $p = 2$ of $p \equiv 1 \pmod{4}$.

Opgave 3.5. 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 3.1.4.

Er bestaan oneindig veel priemgetallen van de vorm $4k + 1$.

Opgave 3.6. Bewijs deze stelling.

3.2 Kwadratische reciprociteit

3.2.1 Kleinste absolute resten: het lemma van Gauss

Definitie. 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 $r \in \left]\frac{-|b|}{2}, \frac{|b|}{2}\right]$.

Bijvoorbeeld, bij deling van 14 door 5 is die rest -1, want -1 ligt in het interval $\left]\frac{-5}{2}, \frac{5}{2}\right]$. 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 3.7. 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 3.2.1. Uniciteit van de kleinste absolute rest

Bij deling van a door b bestaat er een kleinste absolute rest, die bovendien uniek is.

Opgave 3.8. Bewijs deze stelling.

Lemma 3.2.2. Lemma van Gauss

Zij p een oneven priemgetal en $a \in \mathbb{Z}$ met $p \nmid a$. Beschouw de getallen $a, 2a, \ldots, \frac{p-1}{2}a$ en hun kleinste absolute resten modulo p. Zij n het aantal negatieve resten, dan is

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Opgave 3.9. Bewijs het lemma van Gauss.

Stel $y = a \cdot 2a \cdots \frac{p-1}{2}a$. Definieer de functie $d(x)$ als de absolute waarde van de kleinste absolute rest van x bij deling door p.

A. Toon aan dat $y \equiv (-1)^n \cdot d(a) \cdot d(2a) \cdots d\left(\frac{p-1}{2}a\right) \pmod{p}$.

B. Toon aan dat $d(va) = d(wa)$ met $1 \leqslant v, w \leqslant \frac{p-1}{2}$ alleen kan als $v = w$.

C. Toon aan dat de getallen $d(a), d(2a), \ldots, d\left(\frac{p-1}{2}a\right)$ gelijk zijn aan de getallen $1, 2, \ldots, \frac{p-1}{2}$, 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 3.2.3. 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 3.10. Bewijs deze stelling.

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 3.11. 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 momgelijke priemfactoren. Omdat we tot nu toe geen handige techniek hebben om $\left(\frac{q}{p}\right)$, met q priem, te bereken hebben we voorlopig niet veel andere mogelijkheden dan een macht van 2.

Opgave 3.12. 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 3.13. 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 3.14. 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 3.15. 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 3.16. 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 3.17. Zij n oneven en p een priemdeler van $2^n - 1$. Bewijs dat $p \equiv \pm 1 \pmod{8}$.

3.2.2 Eisensteins weg naar kwadratische reciprociteit

Om de wet van de kwadratische reciprociteit te kunnen bewijzen hebben we eerst een bekend lemma nodig.

Lemma 3.2.4. 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 3.18. Bewijs het lemma van Eisenstein.

Stel $u_1 = a, u_2 = 2a, \ldots, u_{\frac{p-1}{2}} = \frac{p-1}{2}a$. Noem r_k rest van u_k bij deling door p. Noem $b_1, b_2, \ldots, b_m$ de resten kleiner dan $\frac{p}{2}$ en $c_1, c_2, \ldots, c_n$ 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 $b_1, b_2, \ldots, b_m$ en $p - c_1, p - c_2, \ldots, p - c_n$.

B. Toon aan dat die getallen gelijk zijn aan $1, 2, \ldots, \frac{p-1}{2}$, 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 3.19. 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 3.2.5. 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 3.20. Bewijs de wet van de 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.

A. Toon aan dat er geen roosterpunten op de diagonaal liggen.

B. Toon aan dat het aantal roosterpunten binnen de onderste driehoek gelijk is aan $\alpha(q,p)$.

C. Toon aan dat het aantal roosterpunten binnen de bovenste driehoek gelijk is aan $\alpha(p,q)$.

D. Toon aan dat $\alpha(p,q)+\alpha(q,p)=\frac{(p-1)(q-1)}{4}$.

E. 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 3.21. 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 3.22. Voor welke priemgetallen heeft de congruentie $x^2\equiv -3 \pmod p$ een oplossing?

Opgave 3.23. 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.

3.2.3 Systematisch bepalen van het Legendre-symbool

De kwadratische reciprociteit laat ons toe om systematisch elk Legendre-symbool te bepalen. Met 'systematisch' bedoelen we zonder elegant nadenken zoals in oefening no. 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 de factoren 2 afsplitsen en daarvan het Legendre-symbool bepalen met stelling 3.2.3. 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 de kwadratische reciprociteit, dan komen er Legendre-symbolen te staan met kleinere priemgetallen. Als we voor elk van de factoren dit proces blijven herhalen bekomen we steeds kleinere priemgetallen tot er alleen priemgetallen 3 staan. Alle Legendre-symbolen met 3 als priemgetal kunnen eenvoudig bepaald worden omdat de 'noemer' steeds ofwel 0, 1 of -1 is modulo 3. Het volstaat dan om het criterium van Euler te gebruiken.

We illustreren deze inzichtsloze methode:

Voorbeeld 3.24. 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.

3.3 Kwadratische congruenties

Analoog aan lineaire congruenties zijn er kwadratische congruenties.

Definitie. Kwadratische congruentie

Een kwadratische congruentie is een congruentie van de vorm

$$ax^2 + bx + c \equiv 0 \pmod{m} \tag{3.1}$$

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 $m \in \mathbb{N}^\times$ omdat de congruentie voor negatieve moduli op precies hetzelfde neerkomt.

Lemma 3.3.1.

Zij $m = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdots {p_r}^{a_r}$, dan is x een oplossing van (3.1) als en slechts als x een oplossing van elk van de congruenties

$$ax^2 + bx + c \equiv 0 \pmod{{p_k}^{a_k}}.$$

Opgave 3.25. Bewijs dit lemma.

Als we de priemontbinding van m kennen is het probleem dus vereenvoudigd tot het vinden van oplossingen modulo machten van priemgetallen.

3.3.1 Priemgetallen als moduli

Lemma 3.3.2.

Als p een oneven priemgetal is en $p \nmid a$ kan de congruentie

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

Herleid worden tot

$$y^2 \equiv d \pmod{p} \tag{3.2}$$

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 (3.2) hangt af van het kwadratisch karakter van d modulo p.

Stelling 3.3.3.

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.

Opgave 3.26. Bewijs de voorgaande stelling.

Het geval waar m een oneven priemgetal is beschouwen we als afgehandeld. We gaan verder met p^k, p oneven.

Stelling 3.3.4.

Stelling 3.3.5.

Als $m = p^k$ en $p \mid a$ is de congruentie 3.1 te herleiden tot een kwadratische congruentie modulo p^{k-1}. Als $p \nmid a$ kan de congruentie herleid worden tot

$$y^2 \equiv d \pmod{p^k}.$$

3.3.2 Priemmachten en het lemma van Hensel

3.4 n-demachtsresten

3.4.1 Recapitulatie exponentiële congruenties

Opgaven hoofdstuk 3

Opgave 3.27. Zij m en n natuurlijke getallen. Bewijs dat $4mn - m - n$ nooit een volkomen kwadraat is.

Opgave 3.28. Zij $p, q \geqslant 5$ priemgetallen zo dat $p = 2q+1$. Bewijs dat -3 een primitieve wortel is modulo p.

Opgave 3.29. Zijn $a, b, c \in \mathbb{N}$ paarsgewijs relatief priem met $c^2 = a^2 - ab + b^2$. Zij p een priemdeler van c. Bewijs dat $p \equiv 1 \pmod 6$.

Opgave 3.30. Zij F_n het n-de Fibonacci-getal. Bewijs dat voor elk priemgetal $p > 7$ geldt dat $F_p \equiv \left(\frac{p}{5}\right) \pmod p$.

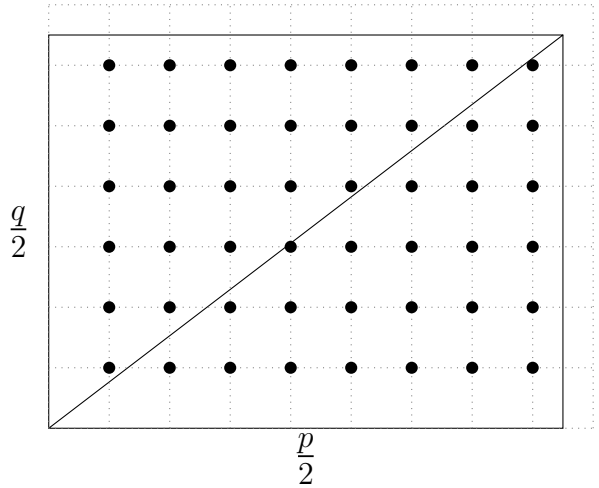
Opgave 3.31. Bewijs dat 16 een vokomen achtste macht is modulo elk priemgetal p.

Opgave 3.32. (Polen MO 2013 vraag 2) Zij a en b gehele getallen zo dat $6a \mid 3 + a + b^2$. Bewijs dat $a < 0$.

Opgave 3.33. Voor welke natuurlijke getallen n bestaat er een natuurlijk getal m zo dat

$$2^n - 1 \mid m^2 + 9\,?$$

Opgave 3.34. (WiNA 2014) Zij $p = 4n + 1$ een priemgetal, bewijs dat $p \mid n^n - 1$.



Hoofdstuk 4. Kwadratische vergelijkingen

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.

4.1 Completing the square

Voorbeeld 4.1. 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 herschijven door te vermenigvuldigen met 4: $4a^2 + 4ab = (2a+b)^2 - b^2$.
Dit herschijven is wat men *completing the square* noemt, vrij vertaald, *vervolledigen van het kwadraat*.

Voorbeeld 4.2. 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: $9x^2 + 6xy + \ldots = \ldots$ 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 bekomen $-5(3x+y)$. 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,

$$(6x + 2y - 5)^2 + 4y^2 + 12y =$$

4.2 Classificatie

Definitie. 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.

4.2.1 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.

4.2.2 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 $(u^2 - kz)(u^2 + kz) = F$. 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 2×2-stelsel in x en y, waaruit de oplossingen moeten volgen.
Ook interessant is wanneer $D > 0$ geen kwadraat is.

Definitie. 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. 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.

4.2.3 Conclusies en praktische strategie

Merk dus op dat we het gedrag van de vergelijking al vanaf het begin kunnen voorspellen, naargelang het teken van $D = b^2 - 4ac$.[18] Als $D < 0$ krijgen we iets met een som van

[18] In een algebraische context wordt $ax^2 + bxy + cy^2 + dx + ey + f$ een (niet-homogene) *binaire kwadratische vorm* genoemd.

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.

4.3 Sommen van kwadraten

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.

4.3.1 Som van twee kwadraten: multiplicativiteit

Stelling 4.3.1. 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, zijnde

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

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 4.3.2.

Als $n_1, n_2, \ldots, n_m$ 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 4.3.3.

Stel dat $\in \mathbb{N}$ zo dat $2n$ de som is van twee kwadraten. Dan is ook n de som van twee kwadraten.

Opgave 4.3. Bewijs dit lemma.

Lemma 4.3.4.

Als een natuurijk 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 4.4. Bewijs het bovenstaand lemma.

Zij n zoals in de opgave en veronderstel $a, b, c, d \geqslant 0$. 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 4.5. Zij p een priemgetal. Bewijs dat de vergelijking $x^2 + y^2 = p$ steeds precies 0 of 4 gehele oplossingen (x, y) heeft.

4.3.2 De twee-kwadratenstelling

Stelling 4.3.5. 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 4.6. Bewijs de 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 $0 \leqslant v < p$ 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 4.3.6. 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 4.7. Bewijs de twee-kwadratenstelling.

Stel eerst dat $n = x^2 + y^2$ en $p = 4k + 3$ is een priemdeler 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 4.8. 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 4.9. 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 4.10. (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 4.11. 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 4.3.7.

Zij n een natuurlijk getal is waarvan $p_1, p_2, \ldots, p_r$ de priemdelers van de vorm $4k+1$ zijn met bijbehorende exponenten $a_1, a_2, \ldots, a_r$. 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.

4.3.3 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 4.3.8. Vier-kwadratenstelling van Langrange[19]

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 identeit. 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 4.3.9.

Zij $n \in \mathbb{N}$ zo dat $2n$ de som van vier kwadraten is. Dan is ook n de som van vier kwadraten.

Opgave 4.12. Bewijs dit lemma.

Opgave 4.13. Bewijs de vier-kwadratenstelling.

Wegens Euler's identiteit volstaat het om aan te tonen dat het geldt voor priemgetallen.

[19] Ook bekend als het vermoeden van Bachet, voor het eerst bewezen door Lagrange in 1770.

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 $\left\lfloor \frac{-p}{2} \right\rfloor < v, w \leqslant \left\lfloor \frac{p}{2} \right\rfloor$ 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.

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 4.3.10.

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 oorprong 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 4.14. 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.

4.3.4 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*)

4.3.4.1 Het probleem van Waring

4.3.4.2 De veelhoeksgetalstelling van Fermat

4.4 De kwadratische vorm $a^2 + nb^2$

4.4.1 Eindige afdaling

Opgave 4.15. 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 4.4.1. 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.

4.4.2 Uniciteit

Opgave 4.16. Zij $p = a^2 + 2b^2$ een priemgetal. Toon aan dat a en b uniek zijn op hun teken na.

4.5 Pell-vergelijkingen

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.

4.5.1 De norm in $\mathbb{Z}[\sqrt{d}]$

Notatie

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 4.5.1.

De som en het product van elementen uit $\mathbb{Z}[\sqrt{d}]$ zitten terug in die verzameling.[20]

Bewijs.
Het bewijs is niet meer dan een rechtstreekse controle:

$$(x_1 + y_1\sqrt{d}) + (x_1 + y_1\sqrt{d}) = (x_1 + x_2) + (y_1 + y_2)\sqrt{d}$$

en

$$(x_1 + y_1\sqrt{d})(x_1 + y_1\sqrt{d}) = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}.$$

[20] Men noemt $\mathbb{Z}[\sqrt{d}]$ *gesloten* onder optelling en vermenigvuldiging.

□

De volgende stelling is een gevolg van het feit dat d geen kwadraat is.

Stelling 4.5.2.

Voor elk getal $z \in \mathbb{Z}[\sqrt{d}]$ bestaan er unieke $x, y \in \mathbb{Z}$ waarvoor $z = x + y\sqrt{d}$.

Opgave 4.17. Bewijs deze stelling.

Dankzij deze unieke notatie zijn de volgende functies goed gedefinieerd.

Definitie. Toegvoeging

Het *toegevoegde* van van $z = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ definiëren we als $x - y\sqrt{d}$. We noteren $\overline{z} = x - y\sqrt{d}$.

Men gaat eenvoudig na dat toevoeging multiplicatief is: voor alle $z_1, z_2 \in \mathbb{Z}[\sqrt{d}]$ geldt dat $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$. 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. Norm

De *norm* van $z \in \mathbb{Z}[\sqrt{d}]$ definiëren we als $N(z) = z \cdot \overline{z}$.

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 4.18. 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 4.19. Stel dat $z \in \mathbb{Z}[\sqrt{d}]$ met $N(z) = 1$. Bewijs dat ook $z^{-1} \in \mathbb{Z}[\sqrt{d}]$ en dat $N(z^{-1}) = 1$.

4.5.2 Bestaan van oplossingen

Het bestaan van oplossingen in het algemeen hebben we te danken aan Lagrange:

Stelling 4.5.3.

Elke Pell-vergelijking $x^2 - dy^2 = 1$ heeft een oplossing.

Opgave 4.20. Bewijs deze stelling.

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 $N(z) = 1$.

4.5.3 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 4.5.4.

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 analoog. Dan bestaat er een unieke $k \in \mathbb{Z}$ waarvoor ${z_0}^k \leqslant z < {z_0}^{k+1}$. Bekijk nu het getal $z_1 = z{z_0}^{-k}$. Dat zit ook in $\mathbb{Z}[\sqrt{d}]$ Er geldt dat $1 \leqslant z_1 < z_0$ 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. □

Voor een element z met norm 1 is $z^{-1} = \overline{z}$. We kunnen de oplossingen dus evengoed schrijven als $z = \pm {z_0}^n$ of $z = \pm \overline{z_0}^n$, 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 $z_1, z_2, \ldots > 1$ 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 4.5.5.

Zij $x, y \in \mathbb{Z}$. Als $x + y\sqrt{d}$ minimaal is, dan zijn $x, y \in \mathbb{N}^\times$.

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 $x > 0$. □

De minimale oplossing moet dus enkel worden gezocht onder de elementen met positieve 'coëfficiënten'.

Gevolg 4.5.6.

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 $x = \frac{z+\overline{z}}{2}$ en $y = \frac{z-\overline{z}}{2\sqrt{d}}$. 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 $n \geqslant 0$ en het plusteken)

$$x = \frac{1}{2}\sum_{k=0}^{n} x_0^{n-k} y_0^k \binom{n}{k} \left(\sqrt{d}^k + \left(-\sqrt{d}\right)^k\right)$$

$$\text{en} \quad y = \frac{1}{2\sqrt{d}}\sum_{k=0}^{n} x_0^{n-k} y_0^k \binom{n}{k} \left(\sqrt{d}^k - \left(-\sqrt{d}\right)^k\right)$$

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 4.21. 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

$$x = \pm\,\frac{(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n}{2} \qquad \text{en} \qquad y = \pm\,\frac{(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n}{2\sqrt{2}}$$

met $n \in \mathbb{Z}$. Bijvoorbeeld $n = 2$ geeft (met het plusteken) $(x, y) = (17, 12)$, $n = 3$ geeft $(99, 70)$.

4.5.4 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 4.22. 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 $x_n > 0$. □
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 $n \geqslant 0$ 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 $n \geqslant 0$ en met het minteken bekomen we dan precies de oplossingen met $x, y < 0$. Verder weten we dat $z_0^{-1} = \overline{z_0}$. Met $n \leqslant 0$ 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 $n \geqslant 0$, 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 4.23. (Baltic Way 1990 vraag 13) Bewijs dat de vergelijking $x^2 - 7y^2 = 1$ oneindig veel oplossingen in natuurlijke getallen heeft.

4.6 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 paragraaf is steeds $a \neq 0, 1$.

4.6.1 Karakterisatie en begrenzingen

We kunnen de algemene oplossing opnieuw karakteriseren als we de 'kleine' oplossingen kennen:

Stelling 4.6.1.

Zij z een oplossing van $N(z) = a$ en z_0 de minimale oplossing van de corresponderende Pell-vergelijking. Zij $z_1, z_2, \ldots$ de elementen in $[1, z_0[$ met norm a. Dan is $z = \pm\, z_m z_0^k$ voor unieke $m \in \mathbb{N}^\times$ en $k \in \mathbb{Z}$.

Bewijs.
Stel dat $z > 0$, het andere geval gaat analoog. Bekijk de unieke $k \in \mathbb{Z}$ waarvoor $z_0^k \leqslant z < z_0^{k+1}$. Dan is $1 \leqslant z z_0^{-k} < z_0$, en bijgevolg $z z_0^{-k} = z_m$ voor zekere m. De uniciteit volgt uit het feit dat $z_1, z_2, \ldots$ in het interval $[1, z_0[$ liggen en dus geen factor z_0^l met $l \geqslant 1$ kunnen verschillen. □

Merk op dat niets zegt over het aantal $z_1, z_2, \ldots$ Misschien zijn het er oneindig veel, of slechts 1. We noemen $z_1, z_2, \ldots$ de minimale oplossingen van de Pell-typevergelijking.

Stelling 4.6.2. 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 $|y| \leqslant \frac{z_0+1}{2\sqrt{d z_0}} \sqrt{|a|}$.

Bewijs.
Idee van het bewijs: voor een oplossing $z = x + y\sqrt{d}$ van $N(z) = a$ geldt dat $2\sqrt{d}\,|y| = |z - \overline{z}| = \left|z - \frac{a}{z}\right| \leqslant |z| + \left|\frac{a}{z}\right|$. $|y|$ 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 $\sqrt{\frac{|a|}{z_0}} \leqslant z_0^m z_1 < \sqrt{|a|\, z_0}$. 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

$$2\sqrt{d}\,|y| \leqslant |z| + \left|\frac{a}{z}\right| \leqslant \max_{\sqrt{\frac{|a|}{z_0}} \leqslant t < \sqrt{|a| z_0}} \left(t + \frac{|a|}{t}\right) = \frac{z_0 + 1}{\sqrt{z_0}} \sqrt{|a|},$$

aangezien $t + \frac{|a|}{t}$ dalend is voor $0 < t < \sqrt{|a|}$ en stijgend voor $t > \sqrt{|a|}$. □

Opmerking.
Deze stelling zegt niet dat elke minimale oplossing een y-waarde heeft met $|y| \leqslant \frac{z_0+1}{2\sqrt{d z_0}} \sqrt{|a|}$. 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 $0 \leqslant y \leqslant \frac{z_0+1}{2\sqrt{d z_0}} \sqrt{|a|}$.

Opgave 4.24. Als $a > 0$ lijkt de ongelijkheid $\left|z - \frac{a}{z}\right| \leqslant |z| + \left|\frac{a}{z}\right|$ 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 $|y| \leqslant \frac{z_0-1}{2\sqrt{d z_0}} \sqrt{a}$.

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[21]

$$y = 12055735790331359447442538767$$

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 4.6.3. Bovengrens voor minimale oplossingen

Elke minimale oplossing van $x^2 - dy^2 = a$ voldoet aan $|y| \leqslant \frac{\max(|a|,z_0)+1}{2\sqrt{d}}$.

Bewijs.
Zij z minimaal. Er geldt $2\sqrt{d}\,|y| = |z - \overline{z}| \leqslant z + \frac{|a|}{z}$. 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 $z_0 \leqslant |a|$ is $z_0 \in [1, |a|]$ en dus $f(z_0) \leqslant f(1) = f(|a|)$, zodat $z_0 + \frac{|a|}{z_0} \leqslant 1 + |a|$. Als $z_0 \geqslant |a|$ is $z_0 + \frac{|a|}{z_0} \leqslant |z|_0 + 1$. Combineren we deze twee gevallen, dan blijkt dat $2\sqrt{d}\,|y| \leqslant \max(|a|\,, z_0) + 1$. □

In het bijzonder leren we hieruit dat er hoogstens een eindig aantal minimale oplossingen is.

4.6.2 Gedrag van minimale oplossingen

We bekijken enkele voorbeelden van Pell-typevergelijkingen die het gedrag van minimale oplossingen illustreren.

Voorbeeld 4.25. 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 minmale oplossingen $z = x + y\sqrt{7}$ bepalen van $N(z) = 2$ waarvoor dus $|y| \leqslant \frac{\max(|a|,z_0)+1}{2\sqrt{d}}$. We hebben $|a| < z_0 < 16$ en $\sqrt{7} > 2$ zodat $|y| < \frac{17}{4}$. Het volstaat dan om te controleren of $-4, \ldots, 4$ 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 $n \geqslant 0$) 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 4.26. 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 $|y| \leqslant \frac{\max(|a|,z_0)+1}{2\sqrt{d}} = 3 + \sqrt{10}$. We bekijken dus $y \in \{-6, \ldots, 6\}$. De mogelijke minimale oplossingen blijken $(\pm\,3, 0)$, $(\pm\,7, \pm\,2)$, en $(\pm\,13, \pm\,4)$. Enkel 3, $7 + 2\sqrt{10}$ en $13 + 4\sqrt{10}$ liggen in het interval $[1, 19 + 6\sqrt{10}]$. Alle

[21] *A First Course in Algebra*, J. Rotman

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 $x^2 - 5y^2 = -4$.

Zoals bij Pell-vergelijkingen kunnen we ook hier soms gemakkelijk beargumenteren dat een vergelijking oneindig veel oplossingen heeft.

Voorbeeld 4.27. 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 $x_n > 0$.□
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 4

Opgave 4.28. Bewijs dat de vergelijking $a^2 - 15b^2 = 3$ geen gehele oplossingen heeft. H

Opgave 4.29. (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 4.30. (VWO 2003 finale vraag 4) In het vlak beschouwt men het rooster van alle punten met gehele cordinaatgetallen. 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 4.31. 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 4.32. (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 4.33. (LIMO 2014 vraag 8)

A. Bepaal alle $(x,y) \in \mathbb{Z}^2$ zodanig dat $|3x^2 - 7xy + 3y^2 - 6| \leqslant 1$.

B. Bepaal alle $(x,y,z) \in \mathbb{Z}^3$ zodanig dat $|x^4 + y^4 + z^4 - 2x^2y^2 - 2x^2z^2 - 2y^2z^2| \leqslant 4$.

Opgave 4.34. (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 4.35. 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 4.36. Vind alle driehoeken waarvan de zijden opeenvolgende natuurlijke getallen zijn en waarvan de oppervlakte ook natuurlijk is.

Opgave 4.37. Zij $A = \{n^2 - 1 \mid n \in \mathbb{N}^\times\}$. Bewijs dat voor elke $a \in A$ oneindig veel koppels (b,c) in A te vinden zijn met $b = ac$.

Opgave 4.38. 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 4.39. Bewijs dat er oneindig veel natuurlijke koppels (x,y) bestaan waarvoor $\frac{x+1}{y} + \frac{y+1}{x} = 4$.

Opgave 4.40. (USAMO 1986 vraag 3) Bepaal het kleinste natuurlijk getal $n > 1$ zo dat het rekenkundig gemiddelde van de getallen $1^2, 2^2, \ldots, n^2$ zelf een kwadraat is.

Opgave 4.41. Bewijs dat $5x^2 + 4$ of $5x^2 - 4$ een kwadraat is als en slechts als x een Fibonaccigetal is.

Opgave 4.42. 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 4.43. 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 4.44. Bewijs dat de vergelijking $x2 - dy^2 = -1$ oplosbaar is als en slechts als $c^2 - dy^2 = -4$ dat is.

Opgave 4.45. 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 4.46. 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 4.47. Toon aan dat een Pell-vergelijking $x^2 - dy^2 = 1$ een oplossing heeft met H

$$0 < |y| < 16^{1024^{a^3}}.$$

Opgave 4.48. Vind alle $n \in \mathbb{N}$ waarvoor $3^n - 2$ een kwadraat is.

Opgave 4.49. Bewijs dat als $\frac{x^2+1}{y^2} + 4$ een kwadraat is, dit gelijk is aan 9.

Opgave 4.50. (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 $|ab - c^2| \leqslant 4$.

Hoofdstuk 5. Diophantische benadering

5.1 Kettingbreuken

5.2 Pellvergelijkingen

5.3 De irrationaliteitsmaat

5.3.1 Thue-Siegel-Roth

5.3.2 Liouville-getallen

Opgaven hoofdstuk 5

Opgave 5.1. Zij (x_n) een rij natuurlijke getallen zo dat $\sin x_n$ strikt daalt en nadert naar 0. Is dan noodzakelijk $\sqrt[n]{\sin x_n} \to 1$? A

Opgave 5.2. Bestaat er een irrationaal getal α waarvoor de verzameling $\{\{2^n\alpha\} \mid n \in \mathbb{N}\}$ niet dicht is in $[0,1]$?

Opgave 5.3. Zij (a_n) een strikt stijgende rij natuurlijke getallen zo dat

$$\lim_{n\to\infty} a_k^{2^{-k}} = \infty.$$

Bewijs dat $\sum_{n=1}^{\infty} \frac{1}{a_n}$ convergeert naar een irrationaal getal.

Opgave 5.4. Zij (a_n) een strikt stijgende rij natuurlijke getallen. Bewijs dat $\sum_{n=1}^{\infty} \frac{2^{a_n}}{a_n!}$ convergeert naar een irrationaal getal.

Opgave 5.5. Zij (a_n) een strikt stijgende rij natuurlijke getallen zo dat

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_1 a_2 \cdots a_n} = \infty.$$

Bewijs dat $\sum_{n=1}^{\infty} \frac{1}{a_n}$ convergeert naar een irrationaal getal.

Hoofdstuk 6. Veeltermen

Definitie. 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. 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 6.0.1. Rationale worteltest

Zij $\frac{p}{q}$ een rationale wortel van $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$, 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 6.0.2. Gehele worteltest

Zij n een gehele wortel van $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. Dan is $n \mid a_0$.

Stelling 6.0.3. Criterium van Eisenstein

Zij $P = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$. Als er een priemgetal p bestaat waarvoor $p \mid a_0, a_1, \ldots, a_{n-1}$ en $p^2 \nmid a_0$, dan is P irreducibel.

Stelling 6.0.4. 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 $\mathbb{Z}$-eenheidsveelterm die geen $\mathbb{Q}$-eenheidsveelterm is (de enige zulke eenheidsveeltermen zijn ± 1).

Opgaven hoofdstuk 6

Opgave 6.1. Bewijs dat $x^n + x + 3$ irreducibel is over $\mathbb{Q}$ voor $n \geqslant 1$.

Hoofdstuk 7. Toepassingen

7.1 Het Frobeniusgetal

Definitie. Frobeniusgetal

Het *Frobeniusgetal* van een eindige verzameling natuurlijke getallen $a_1, \ldots, a_n$ met $\text{ggd}(a_1, \ldots, a_n) = 1$ is het grootste natuurlijk getal dat niet kan worden geschreven als lineaire combinatie van die getallen, waarbij enkel positieve coëfficiënten zijn toegelaten. We noteren $g(a_1, \ldots, a_n)$.

Het is niet vanzelfsprekend dat het Frobeniusgetal steeds bestaat indien aan de voorwaarden voldaan is. Gelukkig is het wel zo:

Stelling 7.1.1.

Als $\text{ggd}(a_1, \ldots, a_n) = 1$ dan bestaat het Frobeniusgetal $g(a_1 \ldots, a_n)$.

Opgave 7.1. Zij $a_1, \ldots, a_n$ natuurlijke getallen met $\text{ggd}(a_1, \ldots, a_n) = 1$. Bewijs dat $g(a_1 \ldots, a_n)$ inderdaad bestaat.

Voor $n = 2$ en $n = 3$ zijn exacte formules bekend voor het Frobeniusgetal, maar de wereld wacht nog steeds op een oplossing voor grotere waarden van n.

Stelling 7.1.2.

Het Frobeniusgetal van twee getallen a en b is gelijk aan $ab - a - b$.

Opgave 7.2. 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 $x, y \geqslant 0$.

Stelling 7.1.3.

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 7.3. Bewijs bovenstaande stelling.

7.2 Perfecte en bevriende getallen

Definitie. 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 griekene 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. Overvloedig en gebrekkig

We noemen een natuurlijk getal $n \in \mathbb{N}^\times$ overvloedig als $\sigma(n) > 2n$ en gebrekkig als $\sigma(n) < 2n$.

Opgave 7.4. Bestaan er perfecte volkomen kwadraten? H

7.2.1 De overvloedigheidsindex

De mate van overvloedigheid vatten we samen in de verhouding $\frac{\sigma(n)}{n}$:

Definitie. 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

$$I(n) = \frac{\sigma(n)}{n} = \prod \frac{p^{a_k+1} - 1}{p^{a_k}(p-1)} = \prod \frac{p - p_k^{-a_k}}{p-1}.$$

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 7.2.1.

Als $a \mid b$ en $a \neq b$ is $I(a) < I(b)$.

Opgave 7.5. Bewijs dat 6 het enige perfecte getal is dat deelbaar is door 6.

7.2.2 Een eerste karakterisatie

Stelling 7.2.2. 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 7.6. 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 Mersenne-priemgetallen. 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 7.2.3. 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 7.7. 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 priemdeler is, we hernummeren 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

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 7.8. Kan een oneven perfect getal deelbaar zijn door 105? H

Opgave 7.9. Kan een oneven perfect getal deelbaar zijn door 825? H

Opgave 7.10. Kan een oneven perfect getal deelbaar zijn door $5313 = 3 \cdot 7 \cdot 11 \cdot 23$? H

7.2.3 Enkele congruenties

Lemma 7.2.4.

Een perfect getal is niet congruent met 2 modulo 3.

Opgave 7.11. Bewijs als oefening. H

Stelling 7.2.5. 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 $n \equiv 9 \pmod{36}$. □

Stelling 7.2.6.

Een oneven perfect getal is congruent met 1 modulo 12, 117 modulo 468 of 81 modulo 324.

Opgave 7.12. Bewijs. H

7.3 Het probleem van Josephus

7.4 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:

$$\begin{array}{cccc} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{array}$$

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 $9 + 15 + 2 + 8$... Gek, niet? Wat dit magisch vierkant extra elegant maakt is dat de voorkomende getallen precies 1 tot en met 16 zijn.

Definitie. Magisch Vierkant

Een *magisch vierkant van orde* $n \in \mathbb{N}^\times$ 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 $1, \ldots, n^2$ of $0, \ldots, n^2 - 1$ 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. 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 $n \in \mathbb{N}^\times$ de getallen $1, \ldots, n^2$ 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 $1, \ldots, n^2$?

Opgave 7.13. Bewijs dat de som van de getallen in een $n \times n$ magisch vierkant steeds deelbaar is door n.

Opgave 7.14. Bewijs dat de magische constante van een magisch vierkant met getallen $1, \ldots, n^2$ enkel $\frac{n^3+n}{2}$ kan zijn.

7.4.1 De Latijnse strategie

We bekijken nog een voorbeeld van een magisch vierkant geconstrueerd door Ramanujan:

$$\begin{array}{cccc} 22 & 12 & 18 & 87 \\ 88 & 17 & 9 & 25 \\ 10 & 24 & 89 & 16 \\ 19 & 86 & 23 & 11 \end{array}$$

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:[22]

$$\begin{array}{cccc} 22 & 12 & 18 & 87 \\ 88 & 17 & 9 & 25 \\ 10 & 24 & 89 & 16 \\ 19 & 86 & 23 & 11 \end{array}$$

Merk op dat in elke kolom, elke rij en elke diagonaal precies één getal van iederee kleur staat. Iets preciezer, we kunnen het magisch vierkant als volgt schrijven als een som van matrices:

[22] Er wordt nagedacht over een kleurenblind-vriendelijker alternatief.

$$\begin{pmatrix} 22 & 12 & 18 & 87 \\ 88 & 17 & 9 & 25 \\ 10 & 24 & 89 & 16 \\ 19 & 86 & 23 & 11 \end{pmatrix} = \begin{pmatrix} 22 & 9 & 16 & 86 \\ 86 & 16 & 9 & 22 \\ 9 & 22 & 86 & 16 \\ 16 & 86 & 22 & 9 \end{pmatrix} + \begin{pmatrix} 0 & 3 & 2 & 1 \\ 2 & 1 & 0 & 3 \\ 1 & 2 & 3 & 0 \\ 3 & 0 & 1 & 2 \end{pmatrix}$$

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 7.15. 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 7.16. 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 7.17. 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. Latijns vierkant

Een latijns vierkant van orde $n \in \mathbb{N}^\times$ 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 $0, \ldots, n-1$ of $1, \ldots, n$, waarbij de voorkeur soms gaat naar $0, \ldots, n-1$. Met deze definitie kunnen we bovenstaande observaties neerschrijven:

Stelling 7.4.1.

Zij $A = (a_{rk})$ en $B = (b_{rk})$ $n \times n$ Latijnse vierkanten met symbolen $0, \ldots, n-1$. 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 $0, \ldots, n^2 - 1$.

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 de het bekomen magisch vierkant de getallen $1, \ldots, 4^2$ en niet $0, \ldots, 4^2 - 1$ 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

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 7.18. 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 7.19. Ga na dat dit inderdaad het geval is.

We bekijken dit nu iets algemener, waarbij we toelaten dat de matrixelementen, meetkundig gezien, rechten met een willekeurige richtingscoëfficiënt vormen:

Stelling 7.4.2.

Zij $n \in \mathbb{N}^\times$ 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 $a_{rk} = (p_1 r + q_1 k + m_1) \bmod n$ en $b_{rk} = (p_2 r + q_2 k + m_2) \bmod n$. Dan geldt:

1. A is Latijns als en slechts als $\text{ggd}(p_1 q_1, n) = 1$, en analoog voor B.
2. Als A en B Latijns zijn geldt: A en B zijn complementair als en slechts als $\text{ggd}(p_1 q_2 - p_2 q_1, n) = 1$.

Opgave 7.20. Bewijs als oefening.

In feite geldt de implicatie "$\text{ggd}(p_1 q_2 - p_2 q_1, n) = 1 \Rightarrow$ 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 $\text{ggd}(p_1 q_1 p_2 q_2, n) = 1$ dat p_1, q_1, p_2, q_2 oneven zijn, zodat $\text{ggd}(p_1 q_2 - p_2 q_1, n) = 1$ onmogelijk is.

Gevolg 7.4.3.

Zij $n \in \mathbb{N}^\times$ oneven. Dan bestaat een magisch vierkant van orde n met getallen $1, \ldots, n^2$.

Opgave 7.21. 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 $1, \ldots, n^2$. We bekijken daarom later nog enkele andere methoden.

7.4.1.1 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 7.22. 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 7.4.4.

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 nevendiagonaal 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 7.23. Bewijs.

Opgave 7.24. 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 7.4.5.

Zij A en B complementaire Latijnse $n \times n$ vierkanten met getallen $0, \ldots, n-1$. Dan is $nA + B$ magisch met goede diagonaalsommen zodra elk van de vier diagonalen ofwel

1. de getallen $0, \ldots, n-1$ bevat
2. enkel het getal $\frac{n-1}{2}$ bevat.

Opgave 7.25. 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 7.26. Zij $n \in \mathbb{N}^\times$ (niet noodzakelijk oneven) en $a, b \in \mathbb{Z}$ met $\gcd(a, n) = 1$. Toon aan dat $\sum_{k=0}^{n-1}(ak+b) \bmod n = \frac{n^2-n}{2}$. H

Iets algemener geldt:

Stelling 7.4.6.

Zij $n \in \mathbb{N}^\times$ (niet noodzakelijk oneven) en $a, b \in \mathbb{Z}$ met $\gcd(a, n) = d$. Dan is

$$\sum_{k=0}^{n-1}(ak+b) \bmod n = \frac{n^2-nd}{2} + n \cdot (b \bmod d).$$

Opgave 7.27. Toon aan. H

In het geval $\gcd(p+q, n) = 3$ 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 $\gcd(p-q, n) = 3$,

$$\sum_{k=0}^{n-1}(pk+q(n-1-k)+m) \bmod n = \frac{n^2-3n}{2} + n\cdot(m \bmod 3)$$

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 $n = 3, 5, 7, 9$:

7.4.1.2 De Siamese methode

Het linkse Latijnse vierkant is zo geconstreerd dat op de hoofddiagonaal telkens alle n verschillende getallen staan, en op de nevendiagonaal steeds het getal $\frac{n-1}{2}$. Het rechtse vierkant is zo geconstrueerd dat op de nevendiagonaal 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):

$$\begin{pmatrix} 7 & 0 & 5 \\ 2 & 4 & 6 \\ 3 & 8 & 1 \end{pmatrix} = 3 \cdot \begin{pmatrix} 2 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 16 & 23 & 0 & 7 & 14 \\ 22 & 4 & 6 & 13 & 15 \\ 3 & 5 & 12 & 19 & 21 \\ 9 & 11 & 18 & 20 & 2 \\ 10 & 17 & 24 & 1 & 8 \end{pmatrix} = 5 \cdot \begin{pmatrix} 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 0 & 2 & 4 \\ 2 & 4 & 1 & 3 & 0 \\ 3 & 0 & 2 & 4 & 1 \\ 4 & 1 & 3 & 0 & 2 \\ 0 & 2 & 4 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 29 & 38 & 47 & 0 & 9 & 18 & 27 \\ 37 & 46 & 6 & 8 & 17 & 26 & 28 \\ 45 & 5 & 7 & 16 & 25 & 34 & 36 \\ 4 & 13 & 15 & 24 & 33 & 35 & 44 \\ 12 & 14 & 23 & 32 & 41 & 43 & 3 \\ 20 & 22 & 31 & 40 & 42 & 2 & 11 \\ 21 & 30 & 39 & 48 & 1 & 10 & 19 \end{pmatrix} = 7 \cdot \begin{pmatrix} 4 & 5 & 6 & 0 & 1 & 2 & 3 \\ 5 & 6 & 0 & 1 & 2 & 3 & 4 \\ 6 & 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 2 & 3 & 4 & 5 & 6 & 0 & 1 \\ 3 & 4 & 5 & 6 & 0 & 1 & 2 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 5 & 0 & 2 & 4 & 6 \\ 2 & 4 & 6 & 1 & 3 & 5 & 0 \\ 3 & 5 & 0 & 2 & 4 & 6 & 1 \\ 4 & 6 & 1 & 3 & 5 & 0 & 2 \\ 5 & 0 & 2 & 4 & 6 & 1 & 3 \\ 6 & 1 & 3 & 5 & 0 & 2 & 4 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 46 & 57 & 68 & 79 & 0 & 11 & 22 & 33 & 44 \\ 56 & 67 & 78 & 8 & 10 & 21 & 32 & 43 & 45 \\ 66 & 77 & 7 & 9 & 20 & 31 & 42 & 53 & 55 \\ 76 & 6 & 17 & 19 & 30 & 41 & 52 & 54 & 65 \\ 5 & 16 & 18 & 29 & 40 & 51 & 62 & 64 & 75 \\ 15 & 26 & 28 & 39 & 50 & 61 & 63 & 74 & 4 \\ 25 & 27 & 38 & 49 & 60 & 71 & 73 & 3 & 14 \\ 35 & 37 & 48 & 59 & 70 & 72 & 2 & 13 & 24 \\ 36 & 47 & 58 & 69 & 80 & 1 & 12 & 23 & 34 \end{pmatrix}$$

$$= 9 \cdot \begin{pmatrix} 5 & 6 & 7 & 8 & 0 & 1 & 2 & 3 & 4 \\ 6 & 7 & 8 & 0 & 1 & 2 & 3 & 4 & 5 \\ 7 & 8 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 8 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 0 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 0 & 1 \\ 3 & 4 & 5 & 6 & 7 & 8 & 0 & 1 & 2 \\ 4 & 5 & 6 & 7 & 8 & 0 & 1 & 2 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 3 & 5 & 7 & 0 & 2 & 4 & 6 & 8 \\ 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 0 \\ 3 & 5 & 7 & 0 & 2 & 4 & 6 & 8 & 1 \\ 4 & 6 & 8 & 1 & 3 & 5 & 7 & 0 & 2 \\ 5 & 7 & 0 & 2 & 4 & 6 & 8 & 1 & 3 \\ 6 & 8 & 1 & 3 & 5 & 7 & 0 & 2 & 4 \\ 7 & 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 \\ 8 & 1 & 3 & 5 & 7 & 0 & 2 & 4 & 6 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 \end{pmatrix}$$

7.4.2 Conway's LUX-methode

7.4.3 Kroneckerproduct

7.5 Lineaire recursies

7.5.1 Periodiciteit

7.6 De rij van Fibonacci

7.6.0.1 De Pisanoperiode

Stelling 7.6.1.

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 7.6.2.

Zij p een priemgetal waarvoor 5 geen kwadraatrest is. Dan is de pisanoperiode modulo p een deler van $p^2 - 1$.

7.6.0.2 Deelbaarheidsrijen

Definitie. Deelbaarheidsrij

Een gehele rij (a_n) noemen we een *deelbaarheidsrij* indien voor alle $m, n > 0$ geldt dat als $m \mid n$, dan $a_m \mid a_n$.

7.6.0.3 Sterke deelbaarheidsrijen

Stelling 7.6.3.

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 $\gcd(a_m, a_n) = a_{\gcd(m,n)}$ voor alle $m, n > 0$.

Definitie. Sterke deelbaarheidsrij

Een gehele rij (a_n) noemen we een *sterke deelbaarheidsrij* indien $\gcd(a_m, a_n) = a_{\gcd(m,n)}$ voor alle $m, n > 0$.

Merk op dat elke sterke deelbaarheidsrij automatisch een deelbaarheidsrij is.

Opgaven hoofdstuk 7

7.1 Het Frobeniusgetal

7.2 Perfecte en bevriende getallen

Opgave 7.28. (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 $p_1 < \ldots < p_k$. Bewijs dat e_1 even is.

Opgave 7.29. (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 7.30. Zij n een even perfect getal. Bewijs dat het product van zijn delers een macht van n is.

Opgave 7.31. Als $n \in \mathbb{N}^\times$ en $\sigma(n) = 2n + 1$, bewijs dat n een oneven kwadraat is.

7.3 Het probleem van Josephus

7.4 Magische vierkanten

Opgave 7.32. Zij $n \in \mathbb{N}^\times$ en $a, b \in \mathbb{Z}$. Bepaal $\sum_{k=0}^{n-1} \left\lfloor \frac{ak+b}{n} \right\rfloor$. H A

7.5 Lineaire recursies

Opgave 7.33. Toon aan dat een lineaire recursie van recursiediepte k na een tijdje periodiek wordt modulo $n \in \mathbb{N}$ met periode hoogstens n^k.

7.6 De rij van Fibonacci

Opgave 7.34. Zij F_n het $n$de Fibonaccigetal. Bewijs dat $F_n^2 - 28$ nooit priem is zodra $n > 5$.

Opgave 7.35. (LIMO 2012) Vind alle koppels (m, n) van natuurlijke getallen waarvoor $F_n = 2^{2^m} + 1$.

Hoofdstuk 8. Algoritmen

8.1 Algoritme van Euclides

8.2 Modulaire machtsverheffing

8.3 Factorisatie

8.3.1 Dixon's algoritme

8.4 Priemgetallen

Stelling 8.4.1.

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 $p = 3$.

8.4.1 Lucas-Lehmer

Stelling 8.4.2.

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 $s_{p-2} \equiv 0 \pmod{2^p - 1}$.

8.4.2 Miller-Rabin

8.5 RSA-encryptie

8.5.1 Diffie-Hellman protocol

8.6 Primitieve wortels

8.7 Sommen van kwadraten

8.8 Pellvergelijkingen

8.8.1 Chakravala methode

De volgende stelling hebben we te danken aan Lagrange:

Stelling 8.8.1.

De Chakravala methode geeft steeds na een eindig aantal stappen een gehele oplossing.

Opgaven hoofdstuk 8

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 beláchelijk) moeilijk.

Opgave I.1. Zij $a, m \in \mathbb{N}^\times$. Bewijs dat er oneindig veel $n \in \mathbb{N}^\times$ bestaan zo dat $m \mid \tau(na^n + 1)$.

Opgave I.2. Zij (a_n) een rij natuurlijke getallen waarvoor $\gcd(a_n, a_m) = \gcd(n, m)$ voor$n \neq m$. Bewijs dat $a_n = n$ voor alle n.

Opgave I.3. Bewijs dat $n+3$ en n^2+3 niet tegelijk derdemachten kunnen zijn als $n \in \mathbb{N}$.

Opgave I.4. Bewijs dat $n+3$ en n^2+3n+3 niet tegelijk derdemachten kunnen zijn als $n \in \mathbb{N}$.

Opgave I.5. 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.6. Vind alle priemgetallen p, q en $m \in \mathbb{N}$ met $1 + 2^m p^2 = q^5$.

Opgave I.7. (USAMO 1998 vraag 5) Bewijs dat voor ieder natuurlijk getal $n \geqslant 2$, 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.8. (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.9. (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.10. Stel dat $a \in \mathbb{N}^\times$ zo dat $2a+1$ en $3a+1$ beide kwadraten zijn. Bewijs dat $5a+3$ niet priem is.

Opgave I.11. Bewijs dat $n!$ op precies één nul minder eindigt als $3^{n!} - 1$, voor $n \geqslant 4$.

Opgave I.12. Zij $f : \mathbb{Z} \to \mathbb{Z}$ een functie die voor elke $q \in \mathbb{N}^\times$ periodiek is met periode (een deler van) q. Is f dan een veelterm?

Opgave I.13. Noteer met p_n het n-de priemgetal. Vind alle n met $p_n + p_{n+1} = 1 + p_{n+2}$.

Opgave I.14. Zij $a, b, c, d \in \mathbb{R}$ met $ad \neq bc$. Bewijs dat er gehele x, y bestaan zo dat

$$|(ax+by)(cx+dy)| \leqslant \frac{1}{2}|ad-bc|.$$

Opgave I.15. Bewijs dat $512^3 + 675^3 + 720^3$ geen priemgetal is.

Opgave I.16. (PEN A67) Zij $A = \{a_1, \ldots, a_n\}$ een deelverzameling van $\mathbb{N}^\times$. Bewijs dat

$$\operatorname{kgv}(A) = \prod_{k=1}^{n} \alpha_k^{(-1)^k}$$

waarbij

$$\alpha_k = \prod_{\substack{S \subseteq \mathbb{N}^\times_{\leqslant n} \\ |S|=k}} \operatorname{ggd}\{a_l \mid l \in S\}.$$

Opgave I.17. Zij $p \equiv 3 \pmod 4$ een priemgetal. Bewijs dat de vergelijking

$$\left|x^2 - py^2\right| = \frac{p-1}{2}$$

een gehele oplossing heeft.

Opgave I.18. (China TST 2014) Zij $k \in \mathbb{N}^\times$. Bewijs dat er een $n \in \mathbb{N}^\times$ is zo dat $k! + (2k)! + \cdots + (nk)!$ een priemdeler groter dan $k!$ heeft.

Opgave I.19. Bewijs dat het Legendre symbool $\left(\frac{\cdots 2 \cdots}{p}\right) = (-1)^{\frac{(p-1)(p+5)}{8}}$.

Opgave I.20. Zij $p > 2$ een priemgetal en $rp + 1 \mid p^p - 1$. Bewijs dat r even is.

Opgave I.21. De getallen $1, 2, \ldots, 2013^2$ worden rij per rij in een 2013×2013 rooster geschreven. Vervolgens kleurt men de getallen in de rijen en kolommen die een kwadraat bevatten. Hoeveel getallen worden niet gekleurd?

Opgave I.22. Zij $n \in \mathbb{N}$ oneven. Bepaal het aantal factoren 2 van $\left\lfloor (1+\sqrt{3})^n \right\rfloor$. H A

Opgave I.23. Noem een priemgetal paars als het van de vorm $\left|3^a - 2^b\right|$ is, en kleurrijk als het van de vorm $\left|3^a \pm 2^b\right|$ is.

A. Vind het kleinste niet-paarse priemgetal.

B. Bewijs dat er oneindig veel niet-kleurrijke priemgetallen bestaan.

Opgave I.24. Zij a, b verschillende reële getallen zo dat $a^n - b^n \in \mathbb{Z}$ voor alle $n \in \mathbb{N}^\times$. A Zijn a en b dan noodzakelijk geheel?

Opgave I.25. 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.26. Het getal 2^{29} heeft precies 9 cijfers. Welk cijfer ontbreekt? H A

Opgave I.27. De functie $f : \mathbb{N} \to \mathbb{Z}$ 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.28. Bepaal alle functies $f : \mathbb{N} \to \mathbb{Z}$ die voldoen aan $m + n \mid f(m) + f(n)$ voor alle $m, n \in \mathbb{N}$.

Opgave I.29. Noteer met F_n het n-de Fibonaccigetal. Bewijs dat $5^k \mid F_{5^k}$ voor $k \in \mathbb{N}$.

Opgave I.30. 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.31. Zij p een priemdeler 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.32. 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.33. 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.34. Bewijs dat de vergelijking $2a^4 + 2a^2b^2 + b^4 = c^2$ geen gehele oplossingen heeft met $a \neq 0$.

Opgave I.35. Vind alle $n, k \in \mathbb{N}$ waarvoor $(n-1)! + 1 = n^k$.

Opgave I.36. Zij $a, b, c \in \mathbb{Z}$ met $c \neq 0$ en $\gcd(a, b, c) = 1$. Bewijs dat er een $n \in \mathbb{N}$ bestaat met $\gcd(an + b, c) = 1$. (Zonder gebruik te maken van de stelling van Dirichlet.)

Opgave I.37. 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.38. Zij $n > 1$ en a, b zo dat $0 < a, b < n$. Bewijs dat $\gcd\left(\binom{n}{a}, \binom{n}{b}\right) > 1$.

Opgave I.39. Als $n \geqslant 1$, bewijs dat H

$$\prod_{k=1}^{n} \left(4 - \frac{2}{k}\right)$$

een even natuurlijk getal is.

Opgave I.40. Bewijs dat $2^{15} - 2^3$ een deler is van $a^{15} - a^3$ voor alle $a \in \mathbb{Z}$. H

Opgave I.41. Wanneer is de som van drie opeenvolgende natuurlijke derdemachten terug een derdemacht? A

Opgave I.42. 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.43. Vind alle triples priemgetallen p, q, r waarvoor $p(p+q) = r + 120$. ✿ H A

Opgave I.44. 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.45. Vind alle $x \in \mathbb{R}$ waarvoor $8x^3 - 20$ en $2x^5 - 2$ vokomen kwadraten zijn. ✿ H A

Opgave I.46. Bewijs dat de vergelijking $x^3 = y^2 + 6$ geen gehele oplossingen heeft. ✿ H

Opgave I.47. Zij $a, b \in \mathbb{Z}$ met $\gcd(a, b) = 1$. Bewijs dat de verzameling $\{ak + b \mid k \in \mathbb{N}\}$ een deelverzameling $\{c_1, \ldots, c_n\}$ van paarsgewijs relatief prieme getallen heeft voor elke $n > 0$. (Zonder gebruik te maken van de stelling van Dirichlet.) ✿

Opgave I.48. Zij $a \in \mathbb{N}^\times$. Bewijs dat de congruentie ✿

$$a^2 + \gcd(a, b)^2 \equiv 0 \pmod{b \cdot \gcd(a, b)}$$

een eindig en even aantal natuurlijke oplossingen voor b heeft.

Opgave I.49. 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.50. Zij $n \geqslant 2$. ✿ H

A. Bewijs dat er voor elke oneven $a \in \mathbb{Z}$ unieke $k \in \{0, 1\}$ en $m \in \{0, \ldots, 2^{n-2} - 1\}$ zijn met $a \equiv (-1)^k \cdot 3^m \pmod{2^n}$.

B. Bewijs dat er $\frac{1}{3}(2^{n-1}+4)$ kwadraten zijn modulo 2^n als n even is en $\frac{1}{3}(2^{n-1}+5)$ als n oneven is (voor $n \geqslant 1$).

Opgave I.51. Als r en s gehele getallen zijn met $11s = 13r$, is $r + s$ dan steeds deelbaar door 8? ✿

Opgave I.52. Vind alle $x, y, z \in \mathbb{N}^\times$ waarvoor $x^2 + y^2 + x + y + 1 = xyz$. ✿

Opgave I.53. Vind alle $n \in \mathbb{N}$ waarvoor $324 + 455^n$ een priemgetal is. ✿ H A

Opgave I.54. Bewijs dat $3^n - 5 \cdot 2^n$ geen priemgetal is voor oneindig veel $n \in \mathbb{N}$. ✿ H

Opgave I.55. Vind alle priemgetallen p, q waarvoor zowel $2p - 1$, $2q - 1$ als $2pq - 1$ kwadraten zijn. ✿

Opgave I.56. 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.57. Zij $k, m, n > 0$ zo dat $k^{m+n} = nm^n$. Bewijs dat $m = k$ en $n = k^k$.

Opgave I.58. Bepaal de natuurlijke getallen x en y als $x^3 - 5x + 10 = 2^y$. A

Opgave I.59. Bewijs dat er oneindig veel natuurlijke getallen n zijn waarvoor $\lfloor 2^n \cdot \sqrt{2} \rfloor$ geen priemgetal is.

Opgave I.60. (China TST 2014) Bewijs dat voor gehele $k, N > 0$,

$$\left(\frac{1}{N} \sum_{n=1}^{N} (\omega(n))^k \right)^{\frac{1}{k}} \leqslant k + \sum_{p^n \leqslant N} \frac{1}{p^n}$$

waarbij de som in het rechterlid loopt over alle priemmachten kleiner of gelijk aan N.

Opgave I.61. Vind de kleinste $n > 0$ zo dat $79n + 1 = 2^a 3^b$ voor zekere $a, b \in \mathbb{N}$.

Opgave I.62. Vind alle priemgetallen p, q waarvoor $p^q + q^p$ een kwadraat is.

Opgave I.63. Zij m en n gehele getallen met $3m^2 + 3 = 4n^2 + n$. Bewijs dat $m - n$ een kwadraat is.

Opgave I.64. Zij $x, y \in \mathbb{Z}_0$ met $\gcd(x(x+1), y) = 1$. Stel dat $\mathrm{ord}_y(x) = 3$, wat is dan $\mathrm{ord}_y(x+1)$?

Opgave I.65. Noteer met $p(n)$ het product van de priemgetallen kleiner dan n. Bepaal alle $n > 3$ waarvoor $p(n) = 2n + 16$.

Opgave I.66. (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.67. 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 $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{N}^\times$. Bewijs dat er oneindig veel priemgetallen in S zijn.

Opgave I.68. Zij $x, y > 0$ gehele getallen met $2xy \mid x^2 + y^2 - x$. Bewijs dat x een kwadraat is.

Opgave I.69. Zij $m, n \in \mathbb{Z}_0$ met $\gcd(m,n) = 1$. Zij $a \in \mathbb{Z}$ met $\gcd(a, mn) = 1$. Bewijs dat H

$$\operatorname{ord}_{mn}(a) = \operatorname{kgv} \operatorname{ord}_m(a), \operatorname{ord}_n(a).$$

Is de voorwaarde $\gcd(m,n) = 1$ noodzakelijk?

Opgave I.70. 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 $a \in \{1, \ldots, p-1\}$?

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 $m, n, q \in \mathbb{N}^\times$,

$$\sum_{m \mid q} \sum_{n \mid q} \frac{\mu(m)\mu(n)}{mn} \gcd(m,n) = \frac{\varphi(q)}{q}.$$

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 $n \in \mathbb{N}^\times$. 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

$$\sum_{r=1}^{\frac{p-1}{2}} r \left(\frac{r}{p}\right) = 0.$$

Opgave I.81. Bepaal het laatste niet-nul cijfer van $\binom{1027}{41}$.

Opgave I.82. Geen van de getallen in de rij $a, a+d, a+2d, \ldots$ is deelbaar door n. Bewijs dat $\gcd(d, n) = 1$.

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 $x, y, n \in \mathbb{N}^\times$ 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

$$q = \frac{1}{n_1} + \cdots + \frac{1}{n_k}$$

met $n_1, \ldots, n_k$ semi-priemmachten?

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 $k \geqslant 3$ 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 $a_1 \in \{1, \ldots, m-1\}$ 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 $\frac{2^{p-1}}{p}$ 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 $a, b \in \mathbb{N}^\times$ 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.

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.104. Zij p een priemgetal en $k \in \mathbb{N}^\times$. Bewijs dat $\frac{p^{2k}-1}{p^2-1}$ geen kwadraat kan zijn.

Opgave I.105. 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.106. Toon aan dat de vergelijking $x^2 - y^{10} + z^5 = 6$ geen gehele oplossingen heeft.

Opgave I.107. Zij p een priemdeler van $2^{2^n} + 1$, en stel dat $p \equiv 1 \pmod{2^{n+3}}$. Is 2 dan een vierdemacht modulo p?

Opgave I.108. Bewijs dat $99^{100} + 100^{101} + 101^{99} + 1$ geen priemgetal is.

Opgave I.109. Voor welke priemgetallen p en natuurlijke getallen m heeft p een oneven orde modulo rad $\left(\frac{p^m-1}{p-1}\right)$?

Opgave I.110. Zij $a, b \in \mathbb{N}^\times$ 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.111. Los $p^a + 1 = 2q^b$ op voor $a, b \geqslant 2$ en oneven priemgetallen p, q.

Opgave I.112. 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.113. Voor welke natuurlijke getallen q is $\sigma(q) - q \mid q - 1$?

Opgave I.114. Vind alle Fibonaccigetallen die de som van twee derdemachten groter dan 0 zijn.

Opgave I.115. Vind alle functies $f : \mathbb{N}^\times \to \mathbb{N}^\times$ 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.116. Bestaan er gehele $a, b > 1$ waarvoor $a^4 \equiv 1 \pmod{b^2}$ en $b^4 \equiv 1 \pmod{a^2}$?

Opgave I.117. Voor welke natuurlijke x zijn er x opeenvolgende gehele getallen waarvan de som een priemgetal is?

Definitie. Thabit-priemgetal

Een *Thabit-priemgetal* is een priemgetal van de vorm $3 \cdot 2^n - 1$.

Opgave I.118. 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.119. Welke veeltermen P voldoen aan $P(n) > 0$ en $\varphi(n) \mid \varphi(P(n))$ voor alle $n \in \mathbb{N}^\times$?

Opgave I.120. Vind alle gehele x, y met $x^3 + 5 = y^5$.

Opgave I.121. Voor welke $n \in \mathbb{N}$ is $n^7 + 7$ een volkomen kwadraat?

Opgave I.122. 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.123. Zijn Wieferich-priemgetallen de enige oplossingen voor $2^{n-1} \equiv 1 \pmod{n^2}$?

Onderzoeksopdrachten

Met deze opgaven is het er nog erger aan toe. Bij de open problemen zijn er al een aantal vermoedens over wat er waar is en wat niet; daar is het bovendien duidelijk wat men wil bewijzen. De bedoeling van dit deel is om een aantal probleemstellingen voor te stellen waarover nog niet veel geweten is. Het is dan ook niet meteen duidelijk wat men zou willen bewijzen, wat plausibel lijkt en wat niet. Dat wil niet zeggen dat deze probleemstellingen onvoorstelbaar moeilijk zijn. Mogelijks zijn ze heel doenbaar maar heeft nog niemand er eens diep over nagedacht. Aan jou dus om de eerste te zijn. Suggesties om deze lijst verder aan te vullen zijn welkom.

Opgave I.124. Wat kan je zeggen over de waarde van 

$$\sum_{d|q^n-1} \mu(\tfrac{q^n-1}{d}) q^{\mathrm{ord}_d(q)}?$$

Beschouw eventueel eerst de gevallen waarbij q priem is of een priemmacht is.

II
Algebra

Hoofdstuk 9. Modulorekenen revisited

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 1.8.5 hebben bewezen, zullen we hier (voor even toch) heel bewust niet gebruiken. De bedoeling is om een volledig zelfstandige opbouw te geven.

9.1 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

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 9.1.1.

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

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.

9.1.1 Bewerkingen in $\mathbb{Z}/m\mathbb{Z}$

We voeren nu formeel twee nieuwe bewerkingen in.

Definitie

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 $V + W = \{v + w \mid v \in V \text{ en } w \in W\}$ noteren (indien die laatste optelling betekenisvol is), analoog voor vermenigvuldiging.

Lemma 9.1.2.

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 9.1.3.

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 9.1.4.

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 1.8.5 een begrip 'congruentie' invoeren, dan hebben we gratis de volgende eigenschappen:

Gevolg 9.1.5.

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 $[ab] = [a] \cdot [b]$. □

9.1.2 Ringen

Wat men in de algebra graag doet is zoiets veralgemenen van $\mathbb{Z}$ naar andere verzamelingen.

Definitie

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

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 9.1.6.

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

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

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 9.1. 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 9.2. Bepaal alle deelringen van $\mathbb{Z}$. H A

9.1.3 Quotiëntringen

We veralgemenen nu de constructie van $\mathbb{Z}/m\mathbb{Z}$ naar algemene ringen.

Definitie

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 9.3. Als $m \in \mathbb{Z}$ is $m\mathbb{Z}$ een ideaal van $\mathbb{Z}$.

Definitie

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 appendix B.5 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 9.1.7.

Congruentie modulo een ideaal I is een equivalentierelatie. De equivalentieklasse van a is $a + I$.

Opgave 9.4. Bewijs deze eigenschap.

Dit verklaart de volgende definities:

Definities

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 of factorring R modulo I*.

Vandaar de notatie $\mathbb{Z}/m\mathbb{Z}$ die we eerder hebben gezien. Analoog als toen bewijst men de volgende eigenschappen:

Lemma 9.1.8.

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 9.5. 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 9.1.9.

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 vermenivuldiging in R/I aan de hand van de bewerkingen met verzamelingen, zonder eerst formeel twee nieuwe bewerkingen in te voeren en nadien te controleren of die goed gedefinieerd zijn.

9.2 De groep $(\mathbb{Z}/m\mathbb{Z})^{-1}$

9.2.1 Inverteeraarheid 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 1.8.5 volgt uit de stelling van Bézout:

Eigenschap 9.2.1.

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

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

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 9.2.2.

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. □

9.2.2 Groepen

De structuur van $R^\times$ is die van wat men een *groep* noemt.

Definitie

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 9.2.3.

Een ring R vormt een groep onder zijn optelling. $R^\times$ vormt een groep onder vermenigvuldiging.

Bewijs.
Voor de optelling volgt dit rechstreeks 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. □

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 9.2.4.

In een groep G geldt:
1. Er is een uniek neutraal element
2. Elk element heeft een unieke inverse.

Opgave 9.6. Bewijs zelf als oefening.

Merk op dat de groepsbewerking niet commutatief hoeft te zijn.

Definitie

Een groep met een commutatieve groepsbewerking is een *abelse groep* of *commutatieve groep*.

Notaties

Vaak zullen we de groepsbewerking 'vermenigvuldiging' noemen, en de bewerking niet altijd noteren. We schrijven dan $a \cdot a = a^2$, $a \cdot a \cdot a \cdot a = a^3$, 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 9.7. Bewijs dat in een groep geldt dat $(ab)^{-1} = b^{-1}a^{-1}$ voor alle a, b.

Opgave 9.8. Bewijs dat in een groep, $(a^{-1})^{-1} = a$ voor alle a.

Notaties

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 9.9. Toon aan dat $a^{-n} = (a^n)^{-1}$.

Opgave 9.10. Toon aan dat $a^m a^n = a^{m+n}$ voor willekeurige $m, n \in \mathbb{Z}$.

Definitie

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.

9.2.3 Orde van een element

In hoofdstuk 1.8.5 hebben we bewezen:

Eigenschap 9.2.5.

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

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 9.2.6.

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 1.8.5:
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. □

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

Zij G een groep en $a \in G$. We stellen $\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, a^0, a, a^2, \ldots\}$ 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

Een groep G is *cyclisch* als $G = \langle a \rangle$ voor een zekere $a \in G$.

Opgave 9.11. Bewijs dat elke cyclische groep abels is.

We hebben:

Gevolg 9.2.7.

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 $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$. Stel dat $k \geqslant 0$. 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 $a^{-k} = a^{-r} = a^{n-r}$. □

9.2.4 Eigenschappen van de orde: het ordelemma

Opgave 9.12. Zij G een groep, $H \leqslant G$ 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 9.2.8.

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 onmiddelijk gevolg is:

Gevolg 9.2.9. Stelling van Euler

Zij $m \in \mathbb{N}^\times$ 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 9.13. Bewijs dat $(\mathbb{Z}/m\mathbb{Z}, +)$ steeds cyclisch is.

Opgave 9.14. 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 9.2.10. 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 $0 \leqslant r < \text{ord}(a)$, dus moet noodzakelijk $r = 0$.□

9.3 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 essentiëel dezelfde structuur hebben, men spreekt van *isomorfe* structuren.

9.3.1 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

Zij G en H groepen. Een afbeelding $f : G \to H$ is een *groepsmorfisme* 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 9.15. ln is een groepsmorfisme van de groep $(\mathbb{R}^+, \cdot)$ naar $(\mathbb{R}, +)$.

Definities

Een *groepsisomorfisme* is een groepsmorfisme 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 noeteren $G \cong H$.

ln is klaarblijkelijk een groepsisomorfisme. Analoge definities gaan op voor ringen:

Definities

Zij $(R, \oplus, \otimes)$ en $(S, \boxplus, \boxtimes)$ ringen. Een afbeelding $f : R \to S$ is een *ringmorfisme* als f een groepsmorfisme 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 9.16. 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 eenveel 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:

$\cdot$	$[2^0]$	$[2^1]$	$[2^2]$	$[2^3]$
$[2^0]$	$[2^0]$	$[2^1]$	$[2^2]$	$[2^3]$
$[2^1]$	$[2^1]$	$[2^2]$	$[2^3]$	$[2^0]$
$[2^2]$	$[2^2]$	$[2^3]$	$[2^0]$	$[2^1]$
$[2^3]$	$[2^3]$	$[2^0]$	$[2^1]$	$[2^2]$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Een Cayley-tabel van een groep is een tabel waarin het resultaat van de groepsbewerking voor elle koppels groepselementen 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. □
We weten al dat $\mathbb{Z}/m\mathbb{Z}$ steeds cyclisch is. Ook $\mathbb{Z}$ is cyclisch, want elk element is te schrijven als $1 + \cdots + 1$ of het tegengestelde daarvan. Het leuke is nu dat het begrip 'isomorfisme' ons toelaat om in zekere zin alle cyclische groepen te kennen.

Stelling 9.3.1.

Een cyclische groep is ofwel isomorf met $(\mathbb{Z}/n\mathbb{Z}, +)$ voor zekere $n \in \mathbb{N}^\times$, 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 $G = \{e, a, a^2, \ldots, a^{n-1}\}$ 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: $f(a^k \cdot a^l) = f(a^{k+l}) = k + l = f(a^k) + f(a^l)$. □

We hernemen het voorgaande voorbeeld. We wisten dat $(\mathbb{Z}/5\mathbb{Z})^\times$ cyclisch is. Aangezien die groep orde 4 heeft, volgt onmiddelijk dat hij isomorf is met $\mathbb{Z}/4\mathbb{Z}$.

Notatie

Voor $n \in \mathbb{N}^\times$ schrijven we C_n voor een niet nader gespecifieerde cyclische groep van orde n, en C_∞ voor een niet nader gespecifieerde 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 9.17. Bepaal op een isomorfisme na alle groepen van orde 4. Met welke bekende groepen zijn ze isomorf? H A

9.3.2 Som en product van structuren

9.3.3 Direct product

Met twee groepen kan men een nieuwe groep construeren als volgt:

Definitie

Zij G en H groepen (niet noodzakelijk met dezelfde bewerking). 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 9.18. Ga na dat het direct product van twee groepen inderdaad een groep is.

Gevolg 9.3.2.

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 9.19. 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
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.

$\cdot$	$[1]$	$[3]$	$[5]$	$[7]$
$[1]$	$[1]$	$[3]$	$[5]$	$[7]$
$[3]$	$[3]$	$[1]$	$[7]$	$[5]$
$[5]$	$[5]$	$[7]$	$[1]$	$[3]$
$[7]$	$[7]$	$[5]$	$[3]$	$[1]$

$+$	$(0,0)$	$(0,1)$	$(1,1)$	$(1,0)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,1)$	$(1,0)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,0)$	$(1,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,0)$	$(0,1)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,1)$	$(0,0)$

Definitie

Voor groepen $G_1, \ldots, G_n$ definiëren we het *direct product* $G_1 \times \cdots \times G_n$ 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

We schrijven $G \times G = G^2$, $G \times G \times G = G^3$, enzovoort.

Definitie

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.

9.4 De chinese reststelling

We proberen de Chinese reststelling te veralgemenen. Om te beginnen hebben we een nieuwe notie van 'relatief priem' nodig.

Definitie

Zij R een commutatieve ring en A, B idealen van R. We noemen A en B *copriem* als $A + B = R$.

9.5 Veeltermringen

9.5.1 Factorisatiestellingen

9.6 Cyclische groepen

Stelling 9.6.1.

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 9.20. Bewijs deze eigenschap.

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 $d = \sum_{c|d} A(d)$ 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 $\varphi(n) \geqslant 1$ is er een element g van orde n. Daar $|\langle g \rangle| = n$ en $\langle g \rangle \leqslant G$ is $\langle g \rangle = G$, dus G is cyclisch.

Gevolg 9.6.2.

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 $g^{\frac{n}{d}}$.

9.7 Het veld $\mathbb{F}_p$

Opgaven hoofdstuk 9

Opgave 9.21. Zij G een groep en A en B cyclische deelgroepen van G. Bewijs dat $A \cap B$ ook cyclisch is.

Opgave 9.22. (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 9.23. (VJO 1993) Bepaal of er een niet-triviaal homomorfisme bestaat van $(\mathbb{Q}, +)$ naar $(\mathbb{Z}, +)$.

Hoofdstuk 10. Ringuitbreidingen van $\mathbb{Z}$

10.1 Case study: de Ramanujan-Nagell vergelijking

10.2 Mordell-vergelijkingen

Opgave 10.1. Bewijs dat $n^3 + 7$ geen volkomen kwadraat kan zijn voor $n \in \mathbb{N}$.

Opgave 10.2. Vind alle natuurlijke oplossingen van $8^x + 17 = y^2$.

Opgaven hoofdstuk 10

Hoofdstuk 11. De p-adische getallen

Opgaven hoofdstuk 11

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

Hoofdstuk 12. 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 *Introduction to Analytic Number Theory*, A.J. Hildebrand. Voor de volledigheid vermelden we wel enkele interessante resultaten die tot dusver zijn bewezen.

12.1 Eveneens 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 priemdeler 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.

Lemma 12.1.1.

Er geldt dat $x\# < 4^x$ voor alle $x > 2$.

Opgave 12.1. Bewijs dit lemma.

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 12.2. We bewijzen het postulaat van Bertrand.
Om te beginnen schatten we de centrale binomiaalcoëfficiënten af naar onder.

A. Toon aan dat

$$\frac{4^n}{2n} \leqslant \binom{2n}{n}$$

voor $n > 0$.

Vervolgens zoeken we een bovengrens voor machten van priemgetallen die de binomiaalcoëfficiënt delen. Noteer voor een priemgetal p en $n \in \mathbb{N}$, $R(p, n) = \nu_p\binom{2n}{n}$.

B. Toon aan dat $p^{R(p,n)} \leqslant 2n$.

C. Toon aan dat $R(p, n) = 0$ als $\frac{2}{3}n < p \leqslant n$.

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 priemdeler p van $\binom{2n}{n}$ voldoet aan $p \leqslant \frac{2}{3}n$.

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 12.1.2. Priemgetalstelling

Er geldt dat $\pi(n) \sim \frac{n}{\log n}$.

Stelling 12.1.3. Stelling van Dirichlet, kwantitatieve vorm

Zij $a, b \in \mathbb{N}^\times$ met $\text{ggd}(a,b) = 1$. Dan is
$$\sum_{\substack{p \leqslant x \\ p \equiv b \pmod a}} \frac{1}{p} = \frac{1}{\varphi(a)} \ln\ln x + O_a(1).$$

In het bijzonder volgt hieruit, zoals eerder vermeld, dat er oneindig veel priemgetallen congruent met b modulo a zijn.

Opgaven hoofdstuk 12

Opgave 12.3. Noteer met p_n het $n$de priemgetal. Bewijs dat $p_n + p_{n+1} > p_{n+2}$ voor $n \geqslant 2$.

Opgave 12.4. Vind alle natuurlijke oplossingen voor $n! = 2^a - 2^b$.

Opgave 12.5. (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 $n \geqslant 2$. Bewijs dat $a_n \to 1$.

Hoofdstuk 13. Befaamde vermoedens

13.1 Sommen van priemgetallen

Vermoeden. Sterk vermoeden van Goldbach

Elk even natuurlijk getal groter dan 2 is te schrijven als de som van twee priemgetallen.

Vermoeden. 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 13.1. Toon aan dat het zwakke vermoeden van Goldbach volgt uit het sterke vermoeden.

Stelling 13.1.1. 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 13.1.2. Borozdin

Het zwakke vermoeden van Goldbach is geldig voor getallen groter dan $3^{3^{15}}$.

Stelling 13.1.3. Helfgott, 2013

Het zwakke vermoeden van Goldbach is waar.

13.2 Priemhiaten

Vermoeden. Tweelingpriemvermoeden

Er zijn oneindig veel koppels priemgetallen p en q met $q = p + 2$.

Vermoeden. 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 13.2.1. Zhang, 2013

Er is een natuurlijk getal $n < 7 \cdot 10^7$ zo dat er oneindig veel priemhiaten gelijk zijn aan n.

Stelling 13.2.2. Polymath Project, 2014

Er is een natuurlijk getal $n \leqslant 246$ zo dat er oneindig veel priemhiaten gelijk zijn aan n.

Stelling 13.2.3. Brun, 1915

$$\sum_p \frac{1}{p}$$

convergeert, waarbij de som loopt over de priemgetallen die lid zijn van een priemtweeling. Meer bepaald is het aantal priemtweelingen kleiner dan n asymptotisch $O(n/\log^2 n)$.

Opgaven hoofdstuk 13

Opgave 13.2. 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

Appendix A. Notaties

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

Als f een functie is en a en b gehele getallen met $a \leqslant b$, 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.1.1.

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 bovegrens 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

$$\sum_{\substack{-10 \leqslant a < 101 \\ a \text{ oneven} \\ a \neq 51}} f(a).$$

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

Als f een functie is en a en b gehele getallen met $a \leqslant b$, 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. Faculteit

De *faculteit* van een natuurlijk getal $n \in \mathbb{N}^\times$ is het product van alle natuurlijke getallen in $\{1, \ldots, n\}$. We noteren

$$n! = \prod_{k=1}^{n} k.$$

We definiëren ook $0! = 1$.

Bijvoorbeeld: $2! = 2$, $4! = 24$, $5! = 120$.

Definitie. Binomiaalcoëfficiënt

De *binomiaalcoëfficiënt*

$$\binom{a}{b}$$

met $a, b \in \mathbb{N}$ en $b \leqslant a$ 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.2.1.

Er is symmetrie:

$$\binom{a}{b} = \binom{a}{a-b}.$$

Eigenschap A.2.2. Formule van Stifel-Pascal

Voor alle $a, b \in \mathbb{N}$ met $b \leqslant a$ is

$$\binom{a}{b} + \binom{a+1}{b} = \binom{a+1}{b+1}.$$

Het bewijs van deze identiteit is niet meer dan een rechstreekse verificatie.

Eigenschap A.2.3.

Als $a, b \in \mathbb{N}$ met $b \leqslant a$ 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 $b \leqslant a$. 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 $s - 2$. □

Appendix B. Nuttige stellingen

B.1 Ontbindingen

Stelling B.1.1. 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.1.2.

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 $A_1, A_2, \ldots, A_n$ eindige verzamelingen. Het inclusie-exclusieprincipe geeft een algemene formule om het aantal elementen in de unie $A_1 \cup A_2 \cup \cdots \cup A_n$ te tellen, in functie van het aantal elementen in de doorsnedes, zoals $A_1 \cap A_2$, $A_2 \cap A_n$, $A_1 \cap A_2 \cap A_3$, $A_2 \cap \cdots \cap A_n$, 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.2.1.

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.2.2. Veralgemeend inclusie-exclusieprincipe

Zij $A_1, \dots A_n$ eindige verzamelingen. Dan is

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{k=1}^{n} (-1)^{k+1} \alpha_k$$

waarbij

$$\alpha_k = \sum_{\substack{S \subseteq \mathbb{N}^{\times}_{\leqslant n} \\ |S|=k}} \left| \bigcap_{l \in S} A_l \right|.$$

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 inductiehypthese leert dat

$$|B_1 \cup B_2 \cup \ldots \cup B_n| = \sum_{k=1}^{n} (-1)^{k+1} \beta_k$$

met

$$\beta_k = \sum_{\substack{S \subseteq \{1,2,\ldots,n\} \\ |S|=k}} \left| \bigcap_{l \in S} B_l \right|.$$

Stel analoog

$$\alpha_k = \sum_{\substack{S \subseteq \{1,2,\ldots,n\} \\ |S|=k}} \left| \bigcap_{l \in S} A_l \right|.$$

Merk op dat $|A_1 \cup A_2 \cup \ldots \cup A_n| = 1 + |B_1 \cup B_2 \cup \ldots \cup B_n|$. 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 $k \leqslant p$ 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.[23] Het is echter veel intuitiever 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 $n = 2, \ldots, n = m$, 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

$$\alpha_{k,n} = \sum_{\substack{S \subseteq \{1,2,\ldots,n\} \\ |S|=k}} \left|\bigcap_{l \in S} A_l\right|$$

en analoog

$$\beta_{k,n} = \sum_{\substack{S \subseteq \{1,2,\ldots,n\} \\ |S|=k}} \left|\bigcap_{l \in S} B_l\right|$$

voor natuurlijke getallen k, n met $k \leqslant n$.

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

$$\left|\bigcup_{k=1}^{m+1} A_k\right| = |A_{m+1}| + \sum_{k=1}^{m} (-1)^{k+1} \alpha_{k,m} - \sum_{k=1}^{m} (-1)^{k+1} \beta_{k,m}.$$

[23] Een voordeel hiervan is dat het zich laat veralgemenen tot willekeurige maten μ, 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

$$
\begin{aligned}
(-1)^{k+2}\alpha_{k+1,m} - (-1)^{k+1}\beta_{k,m} &= (-1)^{k+2}\left(\sum_{\substack{S\subseteq\{1,2,\ldots,m\}\\|S|=k+1}}\left|\bigcap_{l\in S}A_l\right| + \sum_{\substack{S\subseteq\{1,2,\ldots,m\}\\|S|=k}}\left|\bigcap_{l\in S}(A_{m+1}\cap A_l)\right|\right)\\
&= (-1)^{k+2}\left(\sum_{\substack{S\subseteq\{1,2,\ldots,m+1\}\\|S|=k+1\\m+1\notin S}}\left|\bigcap_{l\in S}A_l\right| + \sum_{\substack{S\subseteq\{1,2,\ldots,m+1\}\\|S|=k+1\\m+1\in S}}\left|\bigcap_{l\in S}A_l\right|\right)\\
&= (-1)^{k+2}\sum_{\substack{S\subseteq\{1,2,\ldots,m+1\}\\|S|=k+1}}\left|\bigcap_{l\in S}A_l\right|\\
&= (-1)^{k+2}\alpha_{k+1,m+1}
\end{aligned}
$$

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.3.1. Machtsgemiddelde

Als $a_1, \ldots, a_n \geqslant 0$ reële getallen zijn en $p, q \in \mathbb{R}_0$ met $p < q$, is

$$\left(\frac{a_1^p + \cdots + a_n^p}{n}\right)^{\frac{1}{p}} \leqslant \left(\frac{a_1^q + \cdots + a_n^q}{n}\right)^{\frac{1}{q}}$$

waarbij gelijkheid enkel optreedt als $a_1 = a_2 = \ldots = a_n$.

Stelling B.3.2.

Als $a_1, \ldots, a_n \geqslant 0$ reële getallen zijn geldt dat

$$\lim_{p \to 0} \left(\frac{a_1^p + \cdots + a_n^p}{n} \right)^{\frac{1}{p}} = \sqrt[n]{a_1 \cdots a_n}.$$

Voor $p < 0$ is

$$\left(\frac{a_1^p + \cdots + a_n^p}{n} \right)^{\frac{1}{p}} \leqslant \sqrt[n]{a_1 \cdots a_n}$$

met gelijkheid als en slechts als $a_1 = a_2 = \ldots = a_n$. De omgekeerde ongelijkheid geldt als $p > 0$.

In het bijzonder hebben we:

Stelling B.3.3. HM-GM-AM-QM

Als $a_1, \ldots, a_n \geqslant 0$ reële getallen zijn, is

$$\frac{n}{\frac{1}{a_1} + \cdots + \frac{1}{a_n}} \leqslant \sqrt[n]{a_1 \cdots a_n} \leqslant \frac{a_1 + \cdots + a_n}{n} \leqslant \sqrt{\frac{{a_1}^2 + \cdots + {a_n}^2}{n}}$$

waarbij gelijkheid enkel optreedt als $a_1 = a_2 = \ldots = a_n$.

Stelling B.3.4. Ongelijkheid van Cauchy-Schwarz

Als $x_1, \ldots, x_n$ en $y_1, \ldots, y_n$ reële getallen zijn, is

$$(x_1 y_1 + \cdots + x_n y_n)^2 \leqslant (x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2)$$

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. Lineaire homogene recursie

Indien een complexe rij $(a_n)_{n \in \mathbb{N}}$ recursief gedefinieerd is door

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} \qquad (n \geqslant k)$$

met $c_1, \ldots, c_k$ complexe constanten en met $a_0, \ldots, a_{k-1}$ gegeven, dan noemen we dit een *lineaire homogene recursie*.

Definitie. Karakteristieke veelterm

De *karakteristieke veelterm* van de recursie $a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k}$ is de veelterm

$$\chi(x) = x^k - c_1 x^{k-1} - \cdots - c_{k-1} x - c_k.$$

Stelling B.4.1.

Gegeven een recursiebetrekking $a_n = c_1 a_{n-1} + \ldots + c_k a_{n-k}$ met karakteristieke veelterm χ. Als $\lambda_1, \ldots, \lambda_r$ de wortels zijn van χ met multipliciteit $m_1, \ldots, m_r$, dan worden k oplossingen van de homogene lineaire recursie gegeven door

$$\lambda_1^n, n\lambda_1^n, \ldots, n^{m_1-1}\lambda_1^n, \ldots, \ldots, \lambda_r^n, n\lambda_r^n, \ldots, n^{m_r-1}\lambda_r^n,$$

Elke oplossing van de recursie is een lineaire combinatie van deze oplossingen.

We geven als voorbeeld de rij van Fibonacci.

Definitie. 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 $n \geqslant 2$.

Stelling B.4.2.

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. □

B.5 Varia

Stelling B.5.1. Lagrange-interpolatie

Gegeven complexe getallen $x_1, \ldots, x_n$ en $y_1, \ldots, y_1$ 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 $L(x_1) = y_1, \ldots, L(x_n) = y_n$.

Appendix C. Complexe getallen

Life is complex. It has real and imaginary parts.

(*Rich Rosen*)

Af en toe worden in de cursus complexe getallen gebruikt. Voor wie er nog niet goed mee vertrouwd is geven we hier een beknopt overzicht.

Definitie. 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. Reël en imaginair deel

Het *reëel deel* en *imaginair deel* van een complex getal definiëren we met

$$\mathrm{Re}(x + yi) = x \quad \text{en} \qquad \mathrm{Im}(x + yi) = y.$$

Dit laat ons toe gelijkheid te definiëren voor complexe getallen.

Definitie. Gelijkheid van complexe getallen

Twee complexe getallen zijn gelijk als hun reëel en imaginair deel gelijk zijn.

Definitie

We definiëren de som en het product van twee complexe getallen $z_1 = x_1 + y_1 i$ en $z_2 = x_2 + y_2 i$ als

$$z_1 + z_2 = (x_1 + x_2) + (y_1 + y_2)i \quad \text{en} \quad z_1 \cdot z_2 = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1)i.$$

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 reëel getal x identificeren met het complex getal $x + 0i$.

Stelling C.0.2. 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 θ de *poolhoek* of het *argument*. De modulus noteren we met $r = |z|$, het argument met $\arg z$.

Gevolg C.0.3.

Er geldt dat $|x + yi| = \sqrt{x^2 + y^2}$.

Voor reële getallen is de modulus dus gewoon de absolute waarde.

Gevolg C.0.4.

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.0.5.

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

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.0.6. 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.0.7.

Als $z = e^{a+bi}$ niet 0 is en $n \in \mathbb{N}^\times$ 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 $k \in \{0, \ldots, n-1\}$.

Appendix D. Verzamelingen

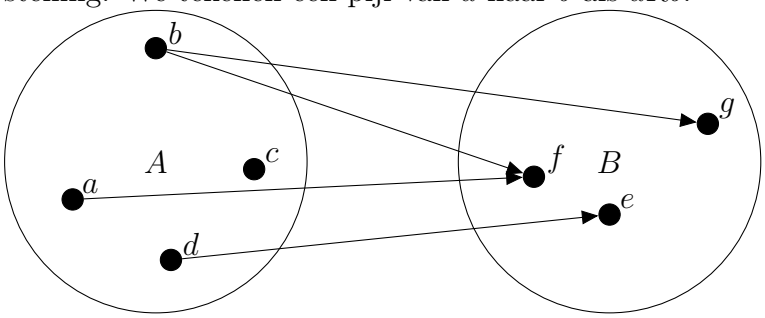
D.1 Binaire relaties

Intuïtief is een relatie een 'object' gedefinieerd over vaste verzamelingen en het 'verbindt' elementen uit die verzamelingen. Een strenge definitie gaat als volgt:

Definitie. Relatie

Een binaire relatie R is een tupel $R = (G, A, B)$ 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.

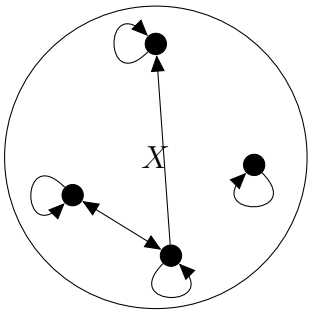


$A = \{a, b, c, d\}$ en $B = \{e, f, g\}$ zijn hier de domeinen, en $G = \{(a, f), (b, g), (b, f), (d, e)\}$ is de grafiek.

Definitie. Reflexieve relatie

Een relatie R gedefinieerd op X is *reflexief* als $\forall x \in X : xRx$.

Bijvoorbeeld, $\geqslant, \leqslant, =$ 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:

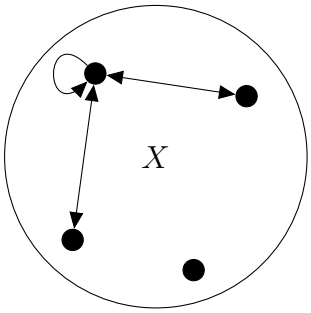


Het enige dat van belang is, is dat elk element een pijl heeft die naar zichzelf terugkeert.

Definitie. Symmetrische relatie

Een relatie R op X is *symmetrisch* als $\forall x, y \in X : xRy \Leftrightarrow yRx$.

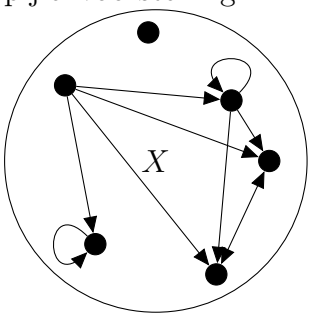
De oorsprong van het woord 'symmetrisch' spreekt voor zich. Een voorbeeld is $aRb \Leftrightarrow |a-b| < 5$ (gedefinieerd op bijvoorbeeld $\mathbb{R}$). In de voorstelling is een pijl tussen verschillende elementen ofwel afwezig, ofwel wijst hij in beide richtingen:



Definitie. 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 $\geqslant$ en $\leqslant$ op $\mathbb{R}$, of $|$ op $\mathbb{Z}$. Een voorbeeld van een mogelijke pijlenvoorstelling:

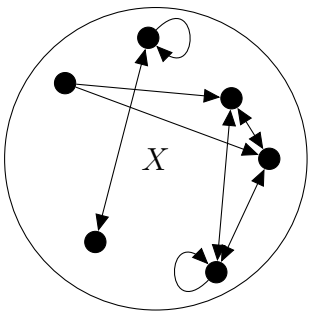


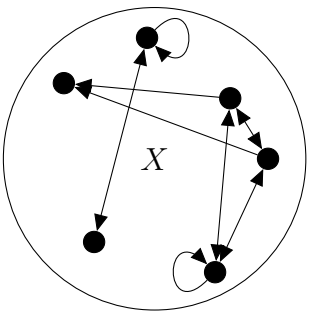
In deze context kan het interessant zijn om ook de Euclidische relaties te vermelden, maar voor de opbouw tot de stelling van Lagrange zijn ze geenszins van belang.

Definitie. 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.

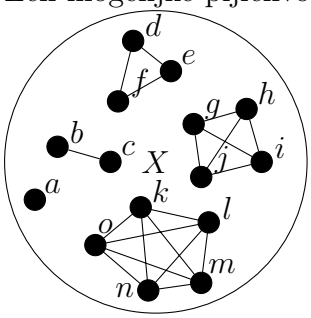
Opgave D.1. Bewijs dat een relatie R op X zowel links- als rechts-Euclidisch is als en slechts als R symmetrisch en transitief is.

D.1.1 Equivalentierelaties

Definitie. 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. We zullen zien dat dit geen toeval is.

Definitie. Equivalentieklasse

Als $x \in X$ en R is een relatie gedefinieerd op X, dan noemen we de verzameling $[x]_R = \{y \in X \mid yRx\}$ 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.1.1.

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.

Opgave D.2. Bewijs deze eigenschappen van equivalentieklassen.

Een equivalentierelatie geeft aanleiding tot een zogenaamde *quotiëntverzameling.*

Definitie. Quotiëntverzameling

Als R een equivalentierelatie is op X, dan noemen we $X/R = \{[x] \mid x \in X\}$ de *quotiënt-verzameling van X onder R.*

Lemma D.1.2.

Zij R een equivalentierelatie op X. Dan is X/R een partitie van X.

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.

Opgave D.3. Bewijs deze eigenschap van quotiëntverzamelingen.

Een interessant tussenresultaat, maar niet van belang voor de stelling van Langrange is het volgende.

Stelling D.1.3. 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.4. Bewijs de hoofdstelling van equivalentierelaties.

Definieer voor elke partitie P de relatie R_P op X met $xR_Py \Leftrightarrow \exists K \in P : x, y \in K$.

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. Nevenklasse

Zij G een groep, $H \leqslant G$ 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

De verzameling van alle linkernevenklassen van een deelgroep H van G noteren we als G/H. Analoog noteren we $G\backslash H = \{Hg \mid g \in G\}$.

Opgave D.5. Bewijs dat voor een deelgroep van een abelse groep de linkse en rechtse nevenklassen gelijk zijn.

D.4 De stelling van Lagrange

Stelling D.4.1. Stelling van Lagrange voor eindige groepen

Zij G een eindige groep en $H \leqslant G$. Dan is $\frac{|G|}{|H|} = |G/H| = |G\backslash H|$. In het bijzonder is $|H|$ een deler van $|G|$.

Opgave D.6. Bewijs de 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 $H_1, \ldots, H_n$ de nevenklassen van H.

C. Bewijs dat $\sum_{k=1}^{n} |H_k| = |G|$.

D. Bewijs dat $|H_k| = |H|$ voor $k = 1, \ldots, n$.

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. Index

Als G een eindige groep is en $H \leqslant G$ noteren we $[G : H] = \frac{|G|}{|H|}$ en noemen dit de *index van H en G*.

Hints

Hint 0.2. **Blz. 13**
$\lceil x \rceil = - \lfloor -x \rfloor$

Hint 0.4. **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.

Hint 1.92. **Blz. 51**
Als d en e ggd's zijn, geldt $d \mid e$ en $e \mid d$...

Hint 1.100. **Blz. 55**
Werk de haakjes uit zoals eerder; gebruik eventueel inductie.

Hint 1.101. **Blz. 56**
De meest elegante methode is waarschijnlijk via inductie op $m + n$...

Hint 1.104. **Blz. 57**
$10 \cdot (9! - 1) = 10! - 10$.

Hint 1.105. **Blz. 57**
Zoek gepaste lineaire combinaties van $a + b$ en $a - b$.

Hint 1.113. **Blz. 57**
Toon aan dat de twee getallen delers van elkaar zijn.

Hint 1.114. **Blz. 57**
Kies $a \in \mathbb{N}$ zo dat je de vergelijking $a = n^2 + p$ handig kan herschrijven.

Hint 1.116. **Blz. 57**
Schrijf a en b met hun priemontbinding.

Hint 1.120. **Blz. 57**
$\frac{p(n)}{n}$ is steeds van de vorm $\frac{1}{2^a}$. Tel voor elke a hoeveel keer $\frac{1}{2^a}$ voorkomt.

Hint 1.122. **Blz. 58**
De kleinste deler is 1, de op-een-na kleinste is een priemgetal. Maak gevalsonderscheid voor de volgende twee delers.

Hint 1.125. **Blz. 58**
Telescoop.

Hint 1.126. **Blz. 58**
Bepaal het aantal koppels m.b.v. de priemontbinding van n. Je zou er dan $\tau(n^2)$ in moeten herkennen.

Hint 1.127. **Blz. 58**
Vind geschikte lineaire combinaties.

Hint 1.128. **Blz. 58**
Let op het aantal factoren 2.

Hint 1.129. **Blz. 58**
Let op het aantal factoren 2.

Hint 1.142. **Blz. 59**
Ontbind.

Hint 1.143. **Blz. 60**
Ontbind.

Hint 1.144. **Blz. 60**
Er zijn meerdere manieren om de vergelijking $p^2 + 7pq + q^2 = n^2$ in de vorm $a^2 - b^2 = \ldots$ te schrijven. Probeer op de plaats van de puntjes zo weinig mogelijk (priem)factoren te krijgen.

Hint 1.145. **Blz. 60**
Ontbind.

Hint 1.148. **Blz. 60**
$d_i \geqslant i$.

Hint 1.149. **Blz. 60**
Vervolledig de kwadraten.

Hint 2.9. **Blz. 63**
Modulo 9 is $10 \equiv 1$.

Hint 2.10. **Blz. 63**
Modulo $a - b$ is $a \equiv b$.

Hint 2.18. **Blz. 68**
$\text{ggd}(n, n+1) = 1$

Hint 2.49. **Blz. 77**
Gebruik inductie en het binomium van Newton.

Hint 2.53. **Blz. 79**
Werk analoog aan de bewijzen voor de eigenschappen van gewone congruenties.

Hint 2.64. **Blz. 83**
Zij w een primitieve wortel. Gebruik dat elke primitieve wortel van de vorm w^k is met $\text{ggd}(k, p-1) = 1$.

Hint 2.89. **Blz. 94**
Vergelijk met de overeenkomstige eigenschappen voor cyclotomische veeltermen.

Hint 2.90. **Blz. 94**
Gebruik de formule $z_k = \prod_{d|k} \Psi_d$.

Hint 2.94. **Blz. 97**
Kies voor p een priemdeler van $a^n - 1$, die geen deler is van $a - 1$. (Waarom bestaat zo'n p?)

Hint 2.95. **Blz. 97**
Kies een priemgetal p_1 met $\mathrm{ord}_{p_1}(2) = n$, p_2 met $\mathrm{ord}_{p_2}(p_1) = n$, ...

Hint 2.98. **Blz. 98**
Toon m.b.v. LTE aan dat uit $\mathrm{ord}_{p^2}(2) > \mathrm{ord}_p(2)$ zou volgen dat $\mathrm{ord}_{p^2}(2) = p\,\mathrm{ord}_p(2)$.

Hint 2.100. **Blz. 99**
Vertrek van de formule van Legendre en schrijf $n = (n_k \dots n_0)_p$.

Hint 2.103. **Blz. 100**
Werk modulo 9 en 11.

Hint 2.104. **Blz. 100**
Let vooral op deelbaarheid door 3 en 11.

Hint 2.113. **Blz. 100**
Telescoop.

Hint 2.124. **Blz. 101**
Werk modulo 19.

Hint 2.144. **Blz. 103**
Maak onderscheid naar gelang q priem is.

Hint 4.28. **Blz. 129**
Zoek het niet te ver, bekijk het eens modulo een of ander getal.

Hint 4.47. **Blz. 131**
Houd wat begrenzingen bij tijdens het bewijs van het bestaan van oplossingen, te beginnen bij Dirichlet's benaderingsstelling. Deze bovengrens is heel onnauwkeurig.

Hint 7.4. **Blz. 135**
Toon aan dat $\sigma(n^2)$ steeds oneven is.

Hint 7.6. **Blz. 136**

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 7.7. **Blz. 136**

A. $\sigma(n) = 2n \equiv 2 \pmod 4$.

B. $\sigma(p_1^{a_1}) = 1 + p_1 + \cdots + p_1^{a_1}$. Maak onderscheid naar gelang a_1 even of oneven is.

C. $\sigma(p_k^{a_k}) = 1 + p_k + \cdots + p_k^{a_k} \equiv a_k + 1 \pmod 2$

D. $\sigma(p_1^{a_1}) = 1 + p_1 + \cdots + p_1^{a_1} \equiv a_1 + 1 \pmod 4$

Hint 7.8. **Blz. 136**
$105 = 3 \cdot 5 \cdot 7$. Het Euler-priemgetal kan niet 3 of 7 zijn. Bepaal nu een ondergrens voor de overvloedigheidsindex.

Hint 7.9. **Blz. 136**
$825 = 3 \cdot 5^2 \cdot 11$. Maak onderscheid naar gelang de hoogste exponent van 3.

Hint 7.10. **Blz. 136**
Probeer extra priemfactoren toe te voegen in de veronderstelling dat 3 of 7 tot een niet-zo-hoge exponent voorkomen.

Hint 7.11. **Blz. 137**
Neem in de sommatie $\sigma(n)$ de termen d en $\frac{n}{d}$ samen.

Hint 7.12. **Blz. 137**
In het geval dat $3 \mid n$, maak onderscheid tussen $\nu_3(n) = 2$ en $\nu_3(n) > 2$.

Hint 7.25. **Blz. 142**
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 7.26. **Blz. 142**
Elk getal in $[0, n[$ komt in de som precies 1 keer voor.

Hint 7.27. **Blz. 142**
Elk getal in $[0, n[$ dat congruent is met b modulo d komt in de som precies d keer voor.

Hint 7.32. **Blz. 145**
$y \left\lfloor \frac{x}{y} \right\rfloor = x - (x \bmod y)$

Hint I.7. **Blz. 148**
Inductie.

Hint I.8. **Blz. 148**
Merkwaardige producten.

Hint I.9. **Blz. 148**
Schrijf alles als product van faculteiten en machten van 2.

Hint I.22. **Blz. 149**
Inductie.

Hint I.26. **Blz. 149**
Werk modulo 9.

Hint I.39. **Blz. 150**
Herschrijf het product met faculteiten.

Hint I.40. **Blz. 150**
$2^{15} - 2^3 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$. Denk aan Fermat.

Hint I.42. **Blz. 151**
Voor $-1 < x < 1$ is $-x > \ln(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}$.

Hint I.43. **Blz. 151**
Welke van p, q, r kunnen/moeten 2 zijn?

Hint I.45. **Blz. 151**
Observeer dat x geheel moet zijn. Schat de kwadraten af (neem een veelterm van even graad!).

Hint I.46. **Blz. 151**
Werk modulo 8.

Hint I.50. **Blz. 151**

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.53. **Blz. 151**
Toon aan dat $4 \mid n$.

Hint I.54. **Blz. 151**
Zo'n rij is in elk geval periodiek modulo eenderwelk geheel getal.

Hint I.69. **Blz. 153**
Toon aan dat beide getallen delers van elkaar zijn.

Hint 9.2. **Blz. 163**
Noem m het kleinste strikt positief element uit de deelring.

Hint 9.17. **Blz. 171**
Zij a een element verschillend van e. Wat zijn de mogelijkheden voor $\text{ord}(a)$?.

Antwoorden

Antwoord 1.37. **Blz. 32**

A. 11

B. 11

C. 16

D. 12

E. 27

Antwoord 1.39. **Blz. 33**
p^{100} met p priem.

Antwoord 1.41. **Blz. 33**

A. 63

B. 728

C. 72

D. 168

E. $7 \cdot 13 \cdot 31$

Antwoord 1.45. **Blz. 34**

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 1.99. **Blz. 55**

A. $ac \dot{+} ad \dot{+} bc \dot{+} bd$

B. $ad \dot{+} ae \dot{+} bd \dot{+} be \dot{+} cd \dot{+} ce$

C. $a^2 \dot{+} ab \dot{+} ab \dot{+} b^2 = a^2 \dot{+} ab \dot{+} b^2$

D. $a^3 \dot{+} a^2b \dot{+} ab^2 \dot{+} b^3$

Antwoord 1.136. **Blz. 59**
μ^2 en λ

Antwoord 2.43. **Blz. 75**

A. Nee.

B. Ja.

Antwoord 2.116. **Blz. 101**
$\frac{n}{\text{ggd}(n,k+1)}$

Antwoord 2.124. **Blz. 101**
Nee

Antwoord 5.1. **Blz. 132**
Nee.

Antwoord 7.21. **Blz. 141**
$a_{rk} = n \cdot ((r+k) \bmod n) + (r+2k) \bmod n + 1$ (Dit kan niet zomaar verder vereenvoudigd worden.)

Antwoord 7.24. **Blz. 141**
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 7.32. **Blz. 145**
$b + \frac{an-a-n+d}{2} - (b \bmod d)$ waarbij $d = \text{ggd}(a,n)$.

Antwoord I.22. **Blz. 149**
$\frac{n+1}{2}$

Antwoord I.24. **Blz. 149**
Ja.

Antwoord I.26. **Blz. 149**
4

Antwoord I.32. **Blz. 150**
60

Antwoord I.41. **Blz. 150**
Enkel voor $3^3 + 4^3 + 5^3 = 6^3$.

Antwoord I.43. **Blz. 151**
$(2, 59, 2)$ en $(11, 2, 23)$

Antwoord I.45. **Blz. 151**
3

Antwoord I.53. **Blz. 151**
$\varnothing$.

Antwoord I.58. **Blz. 152**
2 en 3.

Antwoord I.71. **Blz. 153**
30

Antwoord I.72. **Blz. 153**
p^2

Antwoord I.74. **Blz. 153**
Vals.

Antwoord I.86. **Blz. 154**
Ja.

Antwoord 9.2. **Blz. 163**
$m\mathbb{Z}$ met $m \in \mathbb{N}$.

Antwoord 9.17. **Blz. 171**
C_4 en $(\mathbb{Z}/8\mathbb{Z})^\times, \cdot$

Antwoord II.1. **Blz. 176**
$(3, 6, 2), (4, 4, 2), (4, 6, 3), (6, 6, 4), (6, 10, 5)$ en omwisselen van a en b.

Referenties

Index