Getaltheorie

een introductie

Inleiding

Getaltheorie is een van de oudste deelgebieden 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. De Duitse wiskundige Gauss beschreef de getaltheorie als 'de koningin van de wiskunde', en terecht! Het wonderbaarlijke aan getaltheorie is dat ze niet, of slechts zelden, 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. Maar voor het oplossen van dit soort raadsels is er natuurlijk eerst wat kennis nodig, en wie weet kan je na het lezen van deze uitgebreide introductie wel het bewijs een van die hersenkrakers op jouw naam zetten.

Hoofdstuk 1. Deelbaarheid

Deelbaarheid is misschien wel het meest essentiële begrip binnen de getaltheorie. Het is een manier om meer informatie te creëren over een getal. Deelbaarheid laat ons toe om de diepere betekenis van getallen te vinden, en te ontdekken welke merkwaardige eigenschappen een getal kan hebben.

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. Per definitie is a deelbaar door b als en slechts als er een derde geheel getal k bestaat zodat $a = kb$. We zeggen "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 $a \nmid b$. Als een getal een veelvoud is van 2 noemen we dat getal "even". In het andere geval noemen we het getal "oneven". Zo is 2 bijvoorbeeld even, en is 23 oneven.

Gevolgen.

1. Een gevolg is dat 0 deelbaar is door elk geheel getal. Immers, voor elk geheel getal a bestaat er een getal k zodat $0 = ka$, namelijk $k = 0$. 0 is dus een even getal, want het is deelbaar door 2.
2. Als a en b positief zijn met $a \neq 0$ en $b \mid a$, dan geldt dat $b \leq a$. Want $a = kb$, en omdat a en b positief zijn is k ook positief. Nu geldt dat $b = \frac{a}{k} \leq a$.
3. Als a en b positief zijn zodat $b \mid a$ en $a \mid b$, dan geldt $a = b$. Want uit het tweede gevolg weten we dat $b \leq a$ en dat $a \leq b$, dus moet noodzakelijk $a = b$.
4. Als twee positieve getallen a en b dezelfde delers hebben, dan zijn ze gelijk. Want a is een deler van zichzelf, dus omdat $a \mid a$ geldt dan $a \mid b$. Om een analoge reden geldt dat $b \mid a$. Uit het derde gevolg weten we dan dat $a = b$.

Voorbeeld. Stel dat $a \mid b$ en $b \mid c$. Toon aan dat $a \mid c$.
Oplossing. 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 $y = kx$.

1.2. Lineaire combinatie

Als x en y gehele getallen zijn, noemen we $ax + by$ een lineaire combinatie van a en b.

Voorbeeld 1. Bewijs dat als $d \mid a$ en $d \mid b$, dan $d \mid ax + by$ voor alle gehele getallen x en y.
Oplossing. 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.

1.3. Rest en quotiënt

Voor alle gehele getallen a en b met $b > 0$ bestaat er juist één koppel gehele getallen (q, r) waarvoor $a = q \cdot b + r$ en $0 \leq r < b$. q noemen we dan het quotiënt en r de rest van a bij deling door b. Voor de rest zeggen we ook wel "a modulo b is r" en noteren we

$a \bmod b = r$. De voorwaarde $0 \le r < b$ is hier van kapitaal belang, en mag je nooit vergeten 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 $0 \le 1 < 6$. 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 een oneven getal heeft pariteit 1.

Oefening. Bewijs dat het quotiënt en de rest bij deling van a door b uniek zijn, met $b > 0$. Veronderstel dat er twee 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 of gelijk aan 0 en kleiner dan b kunnen zijn. Bijgevolg zijn rest en quotiënt uniek.

Oefening. Bepaal rest en quotiënt bij deling van
A. 6 door 10.
B. -100 door 7.

We veronderstelden tot nu toe dat de deler positief moet zijn. Dat is echter niet steeds het geval. Ook voor een negatieve deler definiëren we de rest en het quotiënt, maar dan op een licht andere manier. Voor gehele getallen a en b met $b < 0$ definiëren we de rest r en quotiënt q als de gehele getallen waarvoor $a = q \cdot b + r$, en $0 \le r < -b$. (Merk op dat $-b$ een positief getal is.) Ook hier geldt dat de rest en het quotiënt uniek zijn.

Oefening. Bewijs dat het quotiënt en de rest bij deling van a door b uniek zijn, met $b < 0$.

Oefening. Bepaal rest en quotiënt bij deling van
A. 5 door -8.
B. -50 door -9.

We kunnen de definitie nu veralgemenen. Voor alle gehele getallen a en b zijn de rest r en het quotiënt q de gehele getallen waarvoor $a = q \cdot b + r$ en $0 \le r < |b|$. Want als $b > 0$ dan is $|b|$ gewoon gelijk aan b en als $b < 0$ is $|b|$ gelijk aan $-b$.
Tot nu toe namen we aan 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, zo goed als alles wat hierna volgt steunt erop dat er een rest en een quotiënt bestaat.

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

Oefening. Toon aan dat er voor getallen a en b met $b < 0$ een rest en een quotiënt bestaan.

1.4. Grootste gemene deler

Twee gehele getallen hebben altijd gemeenschappelijke delers. Zo hebben 6 en 10 precies 4 gemeenschappelijke delers, namelijk $-2,-1,1,2$. 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 $\text{ggd}(a,b)=d$. 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. De grootste gemene deler van een willekeurig aantal gehele getallen definiëren we analoog als het grootste geheel getal dat een deler is van elk van die getallen. Bijvoorbeeld: $\text{ggd}(15,-12,3)=3$. Merk op dat de grootste gemene deler altijd een positief getal is.
Als $\text{ggd}(a,b)=1$ dan noemen we a en b "onderling ondeelbaar", "copriem" of "relatief priem". Als $a_1,a_2,\cdots,a_n$ gehele getallen zijn zodat $\text{ggd}(a_i,a_j)=1$ voor alle $i\neq j$, dan noemen we $a_1,a_2,\cdots,a_n$ "paarsgewijs relatief priem". Dit betekent niet hetzelfde als $\text{ggd}(a_1,\ldots,a_n)=1$. 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.

Voorbeeld 3. 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 $\text{ggd}(a,b)$ als en slechts als d een deler is van $\text{ggd}(a,b-na)$.
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 de eigenschap van een lineaire combinatie.)
De getallen $\text{ggd}(a,b)$ en $\text{ggd}(a,b-na)$ hebben dezelfde delers en zijn dus gelijk, want dit was één van de gevolgen van de definitie van deelbaarheid.
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.

1.5. Stelling van Bézout

Als a en b gehele getallen zijn is $\text{ggd}(a,b)$ te schrijven als lineaire combinatie van a en b. (Ook hier gaan we ervan uit dat a en b niet beide nul 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.)

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

Gevolgen.
1. Als $c \mid a$ en $c \mid b$, dan $c \mid \text{ggd}(a,b)$. Want c deelt elke lineaire combinatie van a en b, dus c deelt ook $\text{ggd}(a,b)$.
2. $\text{ggd}(a,b)$ de kleinst mogelijke strikt positieve lineaire combinatie is van a en b. Want $\text{ggd}(a,b)$ deelt a en b, dus $\text{ggd}(a,b)$ deelt elke lineaire combinatie $ax+by$ van a en b. Bijgevolg geldt dat als $ax+by>0$, dan $\text{ggd}(a,b) \leq ax+by$. (Dit is het tweede gevolg van de definitie van deelbaarheid.)
3. Elk veelvoud van $\text{ggd}(a,b)$ kan geschreven worden als lineaire combinatie van a en b. 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 4. Stel dat $\text{ggd}(a,b)=1$ en $a \mid bc$. Bewijs dat $a \mid c$.
Oplossing.
Omdat $\text{ggd}(a,b)=1$ bestaan er x en y zodat $ax+by=1$. 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 $c = \ldots \cdot a$. 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.

Oefening. 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.

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

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

Oefening. De stelling van Bézout kan worden veralgemeend naar meerdere getallen. Ook dan is de stelling geldig: als a_1, a_2, ..., a_n gehele getallen zijn, dan kan $\text{ggd}(a_1,a_2,\cdots,a_n)$ geschreven worden als lineaire combinatie van $a_1,a_2,\cdots,a_n$. Bewijs deze veralgemening.

1.6. 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 3. 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 3 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 dat $\text{ggd}(459,342) = \text{ggd}(117,342) = \text{ggd}(117,108) = \text{ggd}(9,108) = \text{ggd}(9,0) = 9$.

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.

We hebben een manier om de grootste gemene deler van twee getallen te schrijven als lineaire combinatie. 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.
Opmerking.
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.

Oefening. 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.

1.7. Lineaire diophantische vergelijking
Een diophantische vergelijking is een vergelijking in één of meerdere variabelen waarbij we zoeken naar gehele oplossingen voor die variabelen. Een lineaire diophantische vergelijking is een vergelijking van de vorm $ax + by = c$, waarbij a, b en c gehele getallen zijn en we oplossingen in gehele getallen zoeken voor x en y.

Oefening. Vind alle mogelijke oplossingen van de diophantische vergelijking $ax + by = c$.
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 rekenschema van Euclides bepalen we dan getallen x_0 en y_0 zodat $ax_0 + by_0 = c$. 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.

Gevolgen.
1. De grootste gemene deler d van twee getallen a en b kan op oneindig veel manieren worden geschreven als lineaire combinatie van a en b. Want de waarde van k mocht elk geheel getal zijn.
2. We kunnen de grootste gemene deler d van twee strikt positieve getallen a en b schrijven als $ax + by$ met $x > 0$ en $y < 0$, of met $x < 0$ en $y > 0$. Want 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 $y > 0$. De voorwaarde dat a en b strikt positief zijn is hier dus nodig. Want als $b \leq 0$ en $a > 0$, dan zou het verhogen van k ervoor zorgen dat x kleiner wordt of gelijk blijft, terwijl y ook kleiner wordt.
Merk dus op dat we zo'n lineaire combinatie dus wel kunnen vinden als a en b beide strikt negatief zijn.

Voorbeeld. 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: $12x - 5y = 3$.
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	2		
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.
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.

Oefening. Bepaal alle oplossingen voor x en y van de vergelijking $50x - 28y = -16$.

1.8. Kleinste gemene veelvoud

Twee gehele getallen hebben gemeenschappelijke veelvouden. Zo zijn bijvoorbeeld ab en $3ab$ gemeenschappelijke veelvouden van a en b. 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, want anders zou het kleinste gemene veelvoud steeds 0 zijn, want 0 is een veelvoud van elk geheel getal.
Het kleinste gemene veelvoud van een willekeurig aantal gehele getallen definiëren we analoog als het kleinste natuurlijk getal, groter dan 0, dat een veelvoud is van elk van die getallen. Bijvoorbeeld: $\text{kgv}(12,5,-6)=60$.

Voorbeeld. Stel dat $a \mid c$ en $b \mid c$. Bewijs dat $\text{kgv}(a,b) \mid c$.
Oplossing.
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 $r=0$, dus $k \mid c$.
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 eigenlijk maar enkele opties:
1. Uit de gegevens leidt je af dat $x=ky$ voor een zeker geheel getal k.
2. Je toont aan dat als een getal een deler is van y, dan ook een deler is van x.
3. 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 waarschijnlijk nog alternatieve methodes, maar hiermee heb je toch al drie relevante. In het algemeen moet je heel vaak gebruik maken van lineaire combinaties.

1.9. Priemgetallen

Een priemgetal p is een positief geheel getal dat precies 2 positieve delers heeft. Bijgevolg zijn deze delers 1 en p. We zeggen ook wel "p is priem". De kleinste tien priemgetallen zijn $2,3,5,7,11,13,17,19,23,29$. Als een getal groter is dan 1 en geen priemgetal is, dan noemen we dat getal "samengesteld". Als een priemgetal p een deler is van een getal n, dan zeggen we ook wel "p is een priemdeler van n".

Voorbeeld. 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 de $\text{ggd}(p,q)=1$ 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 $\text{ggd}(p,q)=1$.

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

1.10. Hoofdstelling van de rekenkunde

Elk natuurlijk getal n groter dan 1 is op een unieke manier te schrijven als het product van priemgetallen, $p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ waarbij $p_1, p_2, \ldots, p_r$ priemgetallen zijn met $p_1 < p_2 < \cdots < p_r$ en $a_1, a_2, \ldots, a_r$ natuurlijke getallen groter dan 0. Dit product noemen we de priemontbinding of priemfactorisatie van n. Bijvoorbeeld, de priemontbinding van 48 is $2^4 \cdot 3$. Als we de symbolen uit de definitie gebruiken, hebben we dus $r = 2$, $p_1 = 2$, $p_2 = 3$, $a_1 = 4$ en $a_2 = 1$. Gewoonlijk schrijven we de priemgetallen dus van klein naar groot in de priemontbinding.
Vaak wordt deze stelling als 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.

Oefening. 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 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.

Oefening. 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 $p_1 \le p_2 \le \cdots \le p_r$ en $q_1 \le q_2 \le \cdots \le q_s$.
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.

Gevolgen.
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 $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ en $y = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$, dan geldt $\text{ggd}(x, y) = p_1^{\min(a_1, b_1)} \cdot p_2^{\min(a_2, b_2)} \cdots p_r^{\min(a_r, b_r)}$.
Want 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 niet bij zowel x en y minstens k kan zijn.
2. Het kleinste gemeen 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 $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ en $y = p_1^{b_1} \cdot p_2^{b_2} \cdots p_r^{b_r}$, dan geldt $\text{kgv}(x, y) = p_1^{\max(a_1, b_1)} \cdot p_2^{\max(a_2, b_2)} \cdots p_r^{\max(a_r, b_r)}$.

Want 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 $p_i^{b_i}$.

Oefening. Bewijs dat er oneindig veel priemgetallen bestaan.
Veronderstel dat er slechts een eindig aantal priemgetallen bestaat. Noem die priemgetallen $p_1, p_2, \cdots, p_n$. Beschouw nu het getal $x = 1 + p_1 p_2 \cdots p_n$.
A. Toon aan dat x geen priemgetal is.
B. Toon aan dat x niet deelbaar is 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.

Oefening. 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}.

Oefening. Toon aan dat $\text{ggd}(a,b) \cdot \text{kgv}(a,b) = ab$ voor alle natuurlijke getallen a en b.

Oefening. Toon aan dat $\text{ggd}(a^n, b^n) = (\text{ggd}(a,b))^n$ voor elk natuurlijk getal n.

Oefening. 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.

Voorbeeld. Toon aan dat $\text{ggd}(\text{kgv}(a,b), \text{kgv}(a,c)) = \text{kgv}(a, \text{ggd}(b,c))$ voor postitieve getallen a, b, c.
Oplossing.
We beschouwen eerst slechts één priemgetal p. Stel dat p in de priemontbinding van a tot de macht x voorkomt, bij b tot de macht y en bij c tot de macht 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 $y \le z$, want de gelijkheid is symmetrisch in y en z. Het rechterlid is dan gelijk aan $\max(x,y)$.
We bekijken nu het linkerlid. Omdat $y \le z$, 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 $y \le z$ dus ook dit is onmogelijk.

Bijgevolg is $\max(x,y) \le \max(x,z)$, 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.

Oefening. Toon aan dat $\text{kgv}(\text{ggd}(a,b),\text{ggd}(a,c)) = \text{ggd}(a,\text{kgv}(b,c))$ voor postitieve getallen a,b,c.

1.11. Aantal delers van een natuurlijk getal

Als $n>1$ 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 $(a_1+1)(a_2+1)\cdots(a_r+1)$.

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

Oefening. Bepaal het aantal gehele delers van
A. 120.
B. 1000.
C. 2^{12}.
D. 10^{10}.

Oefening. Welke natuurlijke getallen hebben precies 101 positieve delers?

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

1.12. Som van de delers van een natuurlijk getal.

Als $n>1$ is 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 $\frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \cdots \frac{p_r^{a_r+1}-1}{p_r-1}$ of dus
$(1+p_1+p_1^2+\cdots+p_1^{a_1})(1+p_2+p_2^2+\cdots+p_2^{a_2})\cdots(1+p_r+p_r^2+\cdots+p_r^{a_r})$.

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

Oefening. Bepaal de som van de positieve delers van
A. 120.
B. 1000.
C. 2^{12}.
D. 10^{10}.

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

Oefening. 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.

1.13. Indicator

De indicator of totiënt van een natuurlijk getal $n>1$ is het aantal natuurlijke getallen groter dan 0 en kleiner dan of gelijk aan n die relatief priem zijn met n. We noteren $\varphi(n)$, waar φ de Euler totiënt functie of phi functie is.
Als $n>1$ en $n=p_1^{a_1}\cdot p_2^{a_2}\cdots p_r^{a_r}$, dan is $\varphi(n)=(p_1-1)p_1^{a_1-1}\cdot(p_2-1)p_2^{a_2-1}\cdots(p_r-1)p_r^{a_r-1}$.

Oefening. Toon de formule voor $\varphi(n)$ aan.
Stel p is een priemdeler van n.
A. Wat is de kans dat een natuurlijk getal groter dan 0 en kleiner of gelijk aan n niet deelbaar is door p?
Stel $p_1^{a_1}\cdot p_2^{a_2}\cdots p_r^{a_r}$ is de priemontbinding van n.
B. Wat is de kans dat een natuurlijk getal groter dan 0 en kleiner of gelijk aan n deelbaar is door geen enkele priemdeler van n?
C. Bepaal het aantal natuurlijke getallen groter dan 0 en kleiner of gelijk aan n die relatief priem zijn met n.

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

Oefening. Bepaal alle natuurlijke getallen n zodat $\varphi(n)=8$.

Oefening. Bepaal alle natuurlijke getallen n zodat $\varphi(\varphi(\varphi(n)))$ een priemgetal is.

1.14. Oplostechnieken

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

1.14.1. 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 hem in de getaltheorie allemaal om delers. Voorbeelden van ontbindingen zijn $a^2-b^2=(a-b)(a+b)$, $a^3-b^3=(a-b)(a^2+ab+b^2)$ 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.

Oefening. Ontbind in factoren.
A. $ab-b-b+1$
B. $3a+4b-2ab-6$
C. $b+a^2+ab+b^2+a^3+a^2b$
D. a^4+4b^4
E. $a^3+b^3+c^3-3abc$
F. $x^{10}+x^5+1$

Oefening. Vind alle natuurlijke getallen n en priemgetallen p zodat $p+1=n^2$.

Oefening. Vind alle gehele getallen a en b zodat $ab=a+b$.

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

Oefening. Zij p een priemgetal. Vind alle natuurlijke getallen a en b zodat $pa+pb=ab$.

Oefening. Vind alle priemgetallen p en natuurlijke getallen n zodat $8^p+27^p=p^n$.

Oefening. Een priemgetal van de vorm 2^n-1 noemen we een Mersennepriemgetal. Stel dat 2^n-1 een priemgetal is. Toon aan dat n een priemgetal is.

Oefening. Een priemgetal van de vorm 2^n+1 noemen we een Fermatpriemgetal. Stel dat 2^n+1 een priemgetal is. Toon aan dat n een macht van 2 is.

Oefening. Vind alle natuurlijke getallen n en priemgetallen p en q zodat $p^2+q^2=n^2$.

1.14.2. Ongelijkheden

Ongelijkheden kunnen voorkomen op verschillende manieren. Een eerste toepassing is het uitsluiten van deelbaarheid. Als a en b positieve getallen zijn, groter dan 0, en $a \mid b$, dan geldt dat $a \le b$. Dus als je twee getallen $x, y > 0$ hebt zodanig dat $x > y$, is het onmogelijk dat $x \mid y$.

Voorbeeld. Vind alle natuurlijke getallen n zodat 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 $n \ge 1$. Dan is $5^n+1 > 5^n > 4^n = 2^{2n} \ge 2^{n+1}$. 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 $5^n+1 > 5^n > 4^n = 2^{2n} \ge 2^{n+1}$ gebruikt. Er zijn natuurlijk nog andere mogelijkheden. Je had het bijvoorbeeld ook kunnen bewijzen met $5^{n+1}+1 > 5^n = 5 \cdot 5^{n-1} > 4 \cdot 5^{n-1} \ge 4 \cdot 2^{n-1} = 2^{n+1}$. 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 nagaan zodat je meer kan doen met de ongelijkheid. Bijvoorbeeld, $5^n > 4^n$ is niet waar voor $n=0$, maar wel voor $n \ge 1$. We zijn dus eerst het geval $n=0$ nagegaan zodat we $n \ge 1$ 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.

Oefening. Vind alle natuurlijke getallen n zodat $2^n+1 \mid 2n+1$.

Oefening. Vind alle natuurlijke getallen n 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. Vind alle natuurlijke getallen a, b en c zodat $a!+b!=c!$.
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 $a \le b$, 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 $c!=a!+b!>b!$ is c groter dan b. Dan is $c! \ge (b+1)! = (b+1)\cdot b! > (1+1)\cdot b! \ge a!+b!$, 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.

Oefening. Vind alle natuurlijke getallen n zodat $n+1=2^n$.

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

Oefening. Vind alle natuurlijke getallen a, b en c zodat $a^a+b^b=c^c$.

Oefening. (JBaMO 2010 vraag 2) Vind alle natuurlijke getallen $n \ge 1$ zodat $n\cdot 2^{n+1}+1$ 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 n bestaat zodat $a^2 < n^2 < (a+1)^2$. Om een analoge reden geldt dat als $a^2 < n^2 < (a+2)^2$, dan $n=a+1$.
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. Vind alle gehele getallen n zodat 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.

Oefening. Vind alle gehele getallen x,y zodat $\frac{x}{y-1}=\frac{y+1}{x+1}$.

Oefening. (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.

1.14.3. Het 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. 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.

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 $3x^2=b^2$.

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

Dus x en y geven ook een oplossing. Maar a was de kleinste waarde die een oplossing gaf, en $x=\frac{a}{3}$ wat kleiner is dan a, aangezien $a>0$. 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 $a,b>1$. 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. 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.

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

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

1.14.4. Vieta jumping

Vieta jumping is een techniek die specifiek is voor een bepaald soort problemen in de getaltheorie. De techniek is ontstaan naar aanleiding van een IMO-vraag uit 1988. De jury had deze vraag eerst niet willen aannemen omdat ze die te moeilijk vonden, maar uiteindelijk hebben ze de vraag toch geaccepteerd. Slechts elf deelnemers slaagden erin de vraag op te lossen. Omdat de techniek zo zelden nodig is zullen we deze vraag ook gebruiken om Vieta jumping te illustreren.

Voorbeeld. (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.

Oplossing.

We bekijken eerst de gevallen $a=0$ en $a=1$. Als $a=0$, dan is $\frac{a^2+b^2}{ab+1}=b^2$, een volkomen kwadraat. Als $a=1$, dan moet $b+1 \mid b^2+1$, dus $b+1 \mid (b^2+1)-(b+1)^2+2(b+1)=2$, dus $b=1$ of $b=0$. In beide gevallen geldt dat de verhouding een volkomen kwadraat is. We kunnen analoog dezelfde redenering maken voor $b=0$ en $b=1$. We veronderstellen nu dus dat $a,b>1$.

Om te beginnen noemen we die breuk $\frac{a^2+b^2}{ab+1}=k$. Voor een vaste waarde van k noemen we S_k de verzameling van alle koppels positieve getallen (a,b) die voldoen aan de vergelijking $\frac{a^2+b^2}{ab+1}=k$. Merk op dat $(a,b)\in S_k$ als en slechts $(b,a)\in S_k$.

We beschouwen dit nu als een kwadratische vergelijking in a: $a^2-kba+b^2-k=0$. De som van de oplossingen voor a van deze vergelijking is kb, en het product is b^2-k. De tweede oplossing, verschillend van a is dan $c=kb-a=\frac{b^2-k}{a}$. Vervolgens tonen we aan dat $c\geq 0$.

Uit $bc+1=\frac{c^2+b^2}{k}\geq 0$ volgt dat $bc+1\geq 0$, dus $c\geq \frac{-1}{b}\geq \frac{-1}{2}$. Omdat $c=kb-a$ een geheel getal is, geldt dat $c\geq 0$.

Dus als $(a,b)\in S_k$, dan $(kb-a,b)\in S_k$. Wegens symmetrie in a en b geldt ook dat als $(a,b)\in S_k$, dan $(a,ka-b)\in S_k$.

Stel dat x de kleinste strikt positieve waarde is waarvoor er een b bestaat zodat $\frac{x^2+b^2}{xb+1}=k$, en y de kleinste strikt positieve waarde van b die hieraan voldoet. Dan geldt dat $x \le y$, want anders zou $y<x$ en dan was x niet de kleinst mogelijke waarde.
Als $x=y$, dan geldt $x^2+1 \mid 2x^2$, dus $x^2+1 \mid 2(x^2+1)-2x^2=2$, wat alleen kan voor $x=1$. Maar in dat geval is k een volkomen kwadraat en zijn we dus klaar. Stel dus $x<y$.

Als $kx-y>0$, dan geldt $(x,kx-y)\in S_k$. Maar $kx-y=\frac{x^2-k}{y}<\frac{x^2}{y}<\frac{x^2}{x}=x<y$. Maar dan was y niet de kleinst mogelijke waarde die bij x hoort.

Omdat we $kx-y\ge 0$ hadden, moet dus $kx-y=0$. Dus $\frac{x^2-k}{y}=0$, zodat $k=x^2$. Bijgevolg is k een volkomen kwadraat.
Opmerking.
Als je dit volledig hebt begrepen ben je al ver geraakt. Deze vraag wordt vaak gezien als de moeilijkste IMO-vraag die er ooit is geweest. Maar laten we even duidelijk maken wat Vieta jumping eigenlijk is. De naam Vieta jumping is genoemd naar de Franse wiskundige François Viète. Hij stelde formules op voor de coëfficiënten van veeltermen in functie van de nulpunten van de veelterm, waaronder die voor de som en het product bij een kwadratische vergelijking. Het grootste deel van de oplossing steunt op deze formules voor de som en het product, en de gelijkheid $kb-a=\frac{b^2-k}{a}$. De techniek bestond er vooral uit om uit één oplossing (a,b) andere oplossingen te creëren: (b,a), $(kb-a,a)$, $(b,ka-b)$, $(a,ka-b)$ en $(ka-b,b)$. 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 a en b 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.

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

<u>Oefeningen</u>
Oefening. (VWO 2013 ronde 2 vraag 17) Als je $10!$ deelt door $9!-1$ krijg je als rest
A. 0 B. 1 C. 8 D. 9 E. 10

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

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

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

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

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

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

Oefening. Vind alle priemgetallen p, q en r zodat $p \mid q - r$ en $p \mid q + r$.

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

Oefening. (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.

Oefening. (JWO 2009 finale vraag 2) Zoek het kleinste natuurlijk getal n zodat $2003 \cdot 2005 \cdot 2007 \cdot 2009 + n$ een volkomen kwadraat is.

Oefening. (JWO 2007 finale vraag 3) Wat is het kleinste getal $\overline{xyz}$ bestaande uit 3 verschillende cijfers x, y en z elk verschillend van 0 zodat 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?

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

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

Oefening. (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.

Oefening. (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.

Oefening (BrMO 2003 ronde 1 vraag 1). Stel $34! = 95232799cd960414084761860964350ab000000$. Bepaal de cijfers a, b, c en d.

Oefening. (IrMO 2007 dag 1 vraag 1) Vind alle koppels priemgetallen (p,q) zodat $p \mid q + 6$ en $q \mid p + 7$.

Oefening. (JWO 2013 finale vraag 1) Bepaal het natuurlijk getal n zodanig dat $\left(\frac{2013}{1} - 1\right) \cdot \left(\frac{2013}{3} - 1\right) \cdot \left(\frac{2013}{5} - 1\right) \cdots \left(\frac{2013}{1005} - 1\right) = 4^n$.

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

Oefening. (NWO 2007 vraag 4) Voor hoeveel natuurlijke getallen n met $1 \le n \le 100$ geldt dat n^n een volkomen kwadraat is?

Oefening. (JWO 2004 finale vraag 4) Vind alle koppels natuurlijke getallen (a,b) zodat $\frac{1}{a}+\frac{1}{b}=\frac{1}{2004}$.

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

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

Oefening. Vind alle natuurlijke getallen $n>1$ waarvoor $\varphi(n) \mid n$.

Oefening. (USAMO 1972 vraag 1) Toon aan dat voor natuurlijke getallen a, b en c geldt dat $\text{ggd}(a,b,c)^2 \cdot \text{kgv}(a,b) \cdot \text{kgv}(b,c) \cdot \text{kgv}(c,a) = \text{kgv}(a,b,c)^2 \cdot \text{ggd}(a,b) \cdot \text{ggd}(b,c) \cdot \text{ggd}(c,a)$.

Oefening. Stel $n>1$. Toon aan dat het aantal koppels natuurlijke getallen (x,y) dat voldoet aan $\text{kgv}(x,y)=n$ gelijk is aan $\tau(n^2)$.

Oefening. Vind alle natuurlijke getallen $n>1$ waarvoor $\varphi(\varphi(n)) \mid n$.

Oefening. Toon aan dat voor natuurlijke getallen p,k met p priem geldt dat $\text{ggd}(\sigma(p^k), \sigma(p^{2k}))=1$.

Oefening. (Polen MO 2013 finale vraag 1) Vind alle gehele getallen x,y zodat $x^4+y=x^3+y^2$.

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

Oefening. (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.

Oefening. Een volmaakt getal is een natuurlijk getal dat gelijk is aan de som van zijn positieve delers, zichzelf niet inbegrepen. Vind de algemene vorm van een even volmaakt getal.
Stel n is volmaakt en even. Dus $n=2^m x$ met $m>0$ en x oneven.
A. Toon aan dat $\sigma(n)=(2^{m+1}-1)\cdot\sigma(x)$.

Omdat n volmaakt is, is $\sigma(n) = 2n$. Stel nu $y = \sigma(x) - x$.
B. Toon aan dat $y \mid x$.
C. Toon aan dat $1 \le y \le x$.
D. Toon aan dat $y = x$ niet kan.
E. Toon aan dat $1 < y < x$ niet kan.
F. Toon aan dat x een priemgetal is en dat $x = 2^{m+1} - 1$.
De algemene vorm van een even volmaakt getal is dus $n = 2^m(2^{m+1} - 1)$ met $2^{m+1} - 1$ een Mersennepriemgetal.

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

Oefening. (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 $d \mid (x+y)^7 - x^7 - y^7$.
A. Is 29 mooi?
B. Is 2006 mooi?
C. Bewijs dat er oneindig veel mooie getallen zijn.

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

Oefening. (IMOSL 2002 vraag 10) Zij $n \ge 2$ 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.

Oefening. (USAMO 1998 vraag 5) Bewijs dat voor ieder natuurlijk getal $n \ge 2$, er een verzameling S van n gehele getallen bestaat zodat $(a-b)^2 \mid ab$ voor iedere verschillende $a, b \in S$.

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

Hoofdstuk 2. Modulair rekenen

2.1. Congruentie en restklasse

Bij het modulair rekenen of modulo rekenen voeren we een nieuw begrip in, congruentie. Als twee gehele getallen a en b dezelfde rest hebben bij deling door c, dan zeggen we "a is congruent met b modulo c" en we noteren $a \equiv b \pmod{c}$. Bijvoorbeeld: $5 \equiv 17 \pmod{3}$, $8 \equiv 12 \pmod{4}$. Als een getal a deelbaar is door c kunnen we dus noteren $a \equiv 0 \pmod{c}$.
Een restklasse modulo een geheel getal c met $c \neq 0$ is een verzameling van alle gehele getallen die bij deling door c dezelfde rest hebben, of dus congruent zijn modulo c.
Bijgevolg zijn er c restklassen modulo c.

Voorbeeld 1. Bewijs dat $a \equiv b \pmod{c}$ als en slechts als $a - b \equiv 0 \pmod{c}$.
Oplossing.
We bewijzen de eigenschap in twee delen.
Deel 1: als $a \equiv b \pmod{c}$ dan $a - b \equiv 0 \pmod{c}$.
Stel $a = q_1 c + r_1$ en $b = q_2 c + r_2$ met $0 \leq r_1, r_2 < c$. Omdat $a \equiv b \pmod{c}$ weten we dat $r_1 = r_2$.
Dan is $a - b = q_1 c - q_2 c = (q_1 - q_2)c$. Dus $a - b \equiv 0 \pmod{c}$.
Deel 2: als $a - b \equiv 0 \pmod{c}$ dan $a \equiv b \pmod{c}$.
Omdat $a - b \equiv 0 \pmod{c}$ is $a - b = kc$. Stel $a = qc + r$. Dan is $b = a - kc = (q - k)c + r$. b heeft dus dezelfde rest als a, dus $a \equiv b \pmod{c}$.
Opmerking.
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".

Oefening. Bewijs de volgende eigenschappen van congruenties.
A. Bewijs dat $a \equiv b \pmod{c}$ als en slechts als $a + d \equiv b + d \pmod{c}$ voor elk geheel getal d.
B. Stel dat $a \equiv b \pmod{c}$ en $d \equiv e \pmod{c}$. Toon aan dat $a + d \equiv b + e \pmod{c}$.
C. Stel dat $a \equiv b \pmod{c}$. Toon aan dat $na \equiv nb \pmod{c}$ voor elk geheel getal n.
D. Stel dat $a \equiv b \pmod{c}$ en $d \equiv e \pmod{c}$. Toon aan dat $ad \equiv be \pmod{c}$.
E. Stel dat $a \equiv b \pmod{c}$. Toon aan dat $a^n \equiv b^n \pmod{c}$ voor elk natuurlijk getal $n > 0$.

Oefening. Toon telkens aan met een voorbeeld dat het omgekeerde van de eigenschappen in B, C, D en E niet steeds waar is.

Voorbeeld. 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 $8^9 \bmod 7$. Er geldt dat $8 \equiv 1 \pmod{7}$, dus wegens eigenschap E geldt $8^9 \equiv 1^9 \pmod{7}$, dus $8^9 \equiv 1 \pmod{7}$. (Als we de letters uit de eigenschap gebruiken is hier dus $a = 8$, $b = 1$, $c = 7$ en $n = 9$.)
Uit eigenschap C volgt nu $25 \cdot 8^9 \equiv 4 \cdot 1 \pmod{7}$. (Met de letters uit de eigenschap: $a = 25$, $b = 4$, $c = 7$, $d = 8^9$ en $e = 1$.) De uiteindelijke rest zal dus 4 zijn.

Oefening. 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.

Oefening. Bereken de rest van 2013^{2014} bij deling door
A. 7
B. -8
C. -9
D. 10
en zeg ook hier steeds welke eigenschappen je gebruikt.

Oefening. Bepaal het kleinste natuurlijk getal n zodat $\dfrac{9^{20}+n}{41}$ een natuurlijk getal is.

Voorbeeld. Bereken $4^{12} \bmod 12$.
Oplossing.
We bekijken eerst $4^2 \bmod 12$, wat gelijk is aan 4. Er geldt dus dat $4^2 \equiv 4 \pmod{12}$. Dus ook $4^3 = 4^2 \cdot 4 \equiv 4 \cdot 4 = 4^2 \equiv 4 \pmod{12}$. Dit kunnen we analoog uitbreiden voor grotere exponenten, en we kunnen dus besluiten dat $4^n \equiv 4 \pmod{12}$ voor elk natuurlijk getal $n > 0$. Dus ook $4^{12} \equiv 4 \pmod{12}$.
Opmerking.
Als we streng zijn hadden we $4^n \equiv 4 \pmod{12}$ moeten bewijzen via inductie, maar omdat het hier zo vanzelfsprekend is lieten we dat even weg. Hou dus wel in gedachten dat het 'analoog uitbreiden' een vorm van inductie is, en dat je in principe bij zo'n werkwijze moet vermelden dat je het met inductie kan bewijzen.
Met dit voorbeeld heb je nog een extra techniek om modulair te rekenen. Er zijn natuurlijk nog heel wat andere manieren, maar van zodra je wat inzicht hebt verkregen in het modulo rekenen zal je die vanzelf ontdekken.

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

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

Oefening. Stel $a \neq b$. Bewijs dat voor $n > 0$ geldt dat $a^n - b^n$ deelbaar is door $a - b$, en dat voor oneven getallen n geldt dat $a^n + b^n$ deelbaar is door $a + b$. Doe dit zonder gebruik te maken van de ontbinding achteraan in de appendix, die je ondertussen ongetwijfeld kent.

Oefening. Stel $d \neq 0$. Toon aan dat $a \equiv b \pmod{c}$ als en slechts als $ad \equiv bd \pmod{cd}$.

Oefening. Bewijs dat als p een priemgetal is en $a \equiv b \pmod{p}$, dan geldt dat $a^{p^n} \equiv b^{p^n} \pmod{p^{n+1}}$ voor elk natuurlijk getal n.

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

2.2. Inverse

Een getal x noemen we een inverse van a modulo b als en slechts als $ax \equiv 1 \pmod{b}$. 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 8 modulo 13.

Oefening. Bewijs dat a een inverse heeft modulo b als en slechts als $\text{ggd}(a,b) = 1$.
A. Stel dat $\text{ggd}(a,b) = 1$. Toon aan dat a een inverse heeft modulo b.
B. Stel dat a een inverse heeft modulo b. Toon aan dat $\text{ggd}(a,b) = 1$.

Oefening. Bewijs dat alle inversen van a modulo b onderling congruent zijn modulo b.

Voorbeeld. Vind alle natuurlijke getallen n met $0 \leq n < 17$ zodat $6n \equiv 8 \pmod{17}$.
Oplossing.
6 heeft een inverse modulo 17, bijvoorbeeld 3. Wegens eigenschap C van congruenties geldt dat $3 \cdot 6n \equiv 3 \cdot 8 \pmod{17}$, dus $n \equiv 24 \pmod{17}$. Dan moet $n = 24 \mod 17 = 7$.

Oefening. Stel dat $\text{ggd}(a,b) = 1$ en $b > 0$. Bewijs dat er voor elk geheel getal c precies één getal x met $0 \leq x < b$ bestaat waarvoor $ax \equiv c \pmod{b}$.

Voorbeeld. Vind alle natuurlijke getallen n met $0 \leq n < 12$ zodat $9n \equiv 6 \pmod{12}$.
Oplossing.
Er geldt dat $3n \equiv 2 \pmod{4}$ als en slechts als $9n \equiv 6 \pmod{12}$, want $3n = 4k + 2$ als en slechts als $9n = 12k + 6$.
We zoeken nu een inverse van 3 modulo 4, bijvoorbeeld 3. Dan geldt $3 \cdot 3n \equiv 2 \cdot 3 \pmod{4}$, of dus $n \equiv 2 \pmod{4}$.
Omdat $0 \leq n < 12$ zijn de oplossingen dus $2, 6, 10$.
Opmerking.
Om de congruentie te vereenvoudigen gingen we over op verborgen modulo rekenen. Hier merk je dus dat je, soms, niet of moeilijk verder geraakt als je bij de nieuwe notatie blijft. Nu konden we met het verborgen modulo rekenen meer informatie verkrijgen.

Oefening. Stel dat $\text{ggd}(a,b) = d$ met $b > 0$ en dat $d \mid c$. Vind het aantal gehele getallen x met $0 \leq x < b$ waarvoor $ax \equiv c \pmod{b}$.

2.3. Chinese reststelling

De Chinese reststelling zegt dat als $m_1, m_2, \ldots, m_n$ gehele getallen zijn die paarsgewijs relatief priem zijn, en $a_1, a_2, \ldots, a_n$ zijn willekeurige gehele getallen, dan bestaan er oneindig veel getallen x zodat $x \equiv a_i \pmod{m_i}$ voor elke i. De 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 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 $10 \equiv 2 \pmod{(-8)}$.

Oefening. Bewijs de Chinese reststelling.

Stel $y = m_1 m_2 \cdots m_n$.

A. Toon aan dat voor elke i er getallen p_i en q_i bestaan zodat $p_i m_i + \dfrac{q_i y}{m_i} = 1$.

Stel nu $r_i = \dfrac{q_i y}{m_i}$.

B. Toon aan dat $r_i \equiv 1 \pmod{m_i}$ en dat $r_i \equiv 0 \pmod{m_j}$ als $i \neq j$.

C. Toon aan dat $x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$ voldoet aan de voorwaarde.

D. Toon aan dat er oneindig veel oplossingen zijn voor x.

Vervolgens bewijzen we dat alle oplossingen voor x congruent zijn modulo y. Zij x_1 en x_2 twee oplossingen.

E. Toon aan dat $m_i \mid x_1 - x_2$ voor elke i.

F. Toon aan dat $x_1 \equiv x_2 \pmod{y}$.

Oefening. Toon aan dat er voor elk natuurlijk getal $n > 0$ een getal m bestaat zodat $n+1 \mid m$ en $n \mid m+1$.

Oefening. Vind alle gehele getallen x zodat $5x \equiv 3 \pmod{7}$ en $6x \equiv 8 \pmod{10}$.

Oefening. 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.

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: 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 $x \equiv a_i \pmod{m_i}$ een oplossing als en slechts als

$a_i \equiv a_j \pmod{\text{ggd}(m_i, m_j)}$ voor alle $i \neq j$. Als het stelsel een oplossing heeft, dan heeft het oneindig veel oplossingen die bovendien congruent zijn modulo $\text{kgv}(m_1, m_2, \ldots, m_n)$.

Oefening. 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. Maar eerst en vooral niet het randgeval vergeten controleren:
A. Toon aan dat de stelling geldt voor $n = 1$.
B. Stel dat $x \equiv a_i \pmod{m_i}$ voor elke i. Toon aan dat $a_i \equiv a_j \pmod{\text{ggd}(m_i, m_j)}$ voor alle $i \neq j$.
Hiermee is het eerste deel reeds voltooid. Vervolgens bewijzen we dat er minstens één oplossing bestaat indien voor alle $i \neq j$ geldt dat $a_i \equiv a_j \pmod{\text{ggd}(m_i, m_j)}$. We bewijzen dit via volledige inductie op n.
Basisstap. We tonen de stelling aan voor $n = 2$.
C. Toon aan dat er gehele getallen q_1, q_2, r, s, t bestaan zodat $a_1 = q_1 s m_1 + q_1 t m_2 + r$ en $a_2 = q_2 s m_1 + q_2 t m_2 + r$.
D. Toon aan dat alle getallen x met $x \equiv q_1 t m_2 + q_2 s m_1 + r \pmod{m_1 m_2}$ voldoen.
Er zijn dus oneindig veel oplossingen.
E. Toon aan dat elke twee oplossingen steeds 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 m congruenties, met $m \leq n$. Beschouw nu zo'n stelsel van $n+1$ 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 $a_i = b_i$ en $m_i = p_i$ voor alle i met $1 \leq i < n$. We willen de inductiehypothese nogmaals toepassen, maar deze keer op het stelsel congruenties $x \equiv b_i \pmod{p_i}$. Daarvoor moeten we er eerst zeker van zijn dat aan de voorwaarde $b_i \equiv b_j \pmod{\text{ggd}(p_i, p_j)}$ is voldaan.
F. Toon aan dat $b_i \equiv b_j \pmod{\text{ggd}(p_i, p_j)}$ geldt voor alle $i \neq j$ met $i, j < n$.
Het wordt dus een probleem wanneer $j = n$. Nu bewijzen we nog voor alle $i < n$ dat $b_i \equiv b_n \pmod{\text{ggd}(p_i, p_n)}$. We bekijken daarvoor een vaste waarde van i.
G. Toon aan dat $b_n \equiv a_n \pmod{\text{ggd}(p_i, m_n)}$ en $b_n \equiv a_{n+1} \pmod{\text{ggd}(p_i, m_{n+1})}$.
H. Toon aan dat $b_n \equiv b_i \pmod{\text{ggd}(p_i, m_n)}$ en $b_n \equiv b_i \pmod{\text{ggd}(p_i, m_{n+1})}$.
I. Toon aan dat $b_n \equiv b_i \pmod{\text{kgv}(\text{ggd}(p_i, m_n), \text{ggd}(p_i, m_{n+1}))}$.
Wie zich nog de oefening uit hoofdstuk 1, bovenaan pagina 13 herinnert, heeft misschien opgemerkt dat $\text{kgv}(\text{ggd}(p_i, m_n), \text{ggd}(p_i, m_{n+1})) = \text{ggd}(p_i, \text{kgv}(m_n, m_{n+1})) = \text{ggd}(p_i, p_n)$.

Bijgevolg geldt dat $b_n \equiv b_i \pmod{\text{ggd}(p_i, p_n)}$. Hierdoor kunnen we de inductiehypothese toepassen, en weten we dat het stelsel oneindig veel oplossingen heeft, die bovendien congruent zijn modulo $\text{kgv}(p_1, \ldots, p_n)$. We zijn bijna klaar:

J. 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.

Oefening. (BSMC 2008 vraag 4) Bewijs dat er voor elk natuurlijk getal k oneindig veel natuurlijke getallen n bestaan zodat $\frac{n - \tau(n^r)}{r}$ een geheel getal is, voor elke $r \in \{1, 2, \cdots, k\}$.

2.4. Kwadraatrest

Stel a en b zijn gehele getallen met $b \neq 0$. We zeggen dat a een kwadraatrest is modulo b als en slechts als er een geheel getal x bestaat zodat $x^2 \equiv a \pmod{b}$. Een niet-kwadraatrest modulo b is een getal dat geen kwadraatrest is modulo b. Bijvoorbeeld, 23 is een kwadraatrest modulo 7 want $3^2 = 9 \equiv 23 \pmod{7}$.

Een kwadraatrestklasse is een verzameling van alle gehele getallen a waarvoor a^2 bij deling door c dezelfde rest geeft.

Voorbeeld. Toon aan dat 2 geen kwadraatrest is modulo 3.

We bekijken eerst wat alle mogelijke kwadraatrestklassen zijn modulo 3. Als $a \equiv b \pmod{3}$, dan geldt $a^2 \equiv b^2 \pmod{3}$. Voor elk geheel getal a bestaat er een getal b met $0 \leq b < 3$ waarvoor $a \equiv b \pmod{3}$, namelijk de rest van a bij deling door 3.

Het volstaat dus om de resten van 0^2, 1^2 en 2^2 te berekenen, want elk ander geheel getal heeft een kwadraat dat congruent is met één van deze kwadraten.

We zien dat deze resten steeds 0 of 1 zijn. Het is dus onmogelijk dat 2 een kwadraatrest is modulo 3.

Oefening. Toon aan dat 0 en 1 de enige kwadraatrestklassen vormen modulo 4.

Oefening. Toon aan dat het aantal kwadraatresten r modulo een oneven priemgetal p en met met $0 \leq r < p$, gelijk is aan $\frac{p+1}{2}$.

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

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

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

Oefening. Vind alle kwadraatrestklassen modulo 5.

Oefening. Vind de mogelijke resten van een derdemacht modulo 7.

Oefening. Toon aan dat n^2+1 nooit deelbaar is door 3.

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

Voorbeeld. Vind alle gehele getallen m en n zodat $n^2+1=4m\cdot(m+1)$.
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 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.

Voorbeeld. Vind alle gehele getallen x en y waarvoor $2x^2+1=5y^2+2$.
Oplossing.
We beschouwen de vergelijking modulo 5. We bekijken eerst wat de mogelijke kwadraatrestklassen zijn modulo 5: $0^2\equiv 0$, $1^2\equiv 1$, $2^2\equiv 1$, $3^2\equiv -1$, $4^2\equiv 1$. Meer resten hoeven we niet te berekenen. De mogelijke resten zijn dus 0, 1 en -1.
Dus $2x^2+1$ kan modulo 5 enkel congruent zijn met $2\cdot 0+1=1$, $2\cdot 1+1=3$ en $2\cdot(-1)+1=1$. Het linkerlid is echter congruent met 2 modulo 5. Dat betekent dat er geen oplossingen zijn.

Oefening. Vind alle natuurlijke getallen n en priemgetallen p en q zodat $p^2+q^2=2^n$.

Oefening. Vind alle gehele getallen a en n met $n\geq 0$ zodat $a\cdot(a+2)=3^n-2$.

2.5. 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".

Oefening. Vind alle primitieve Pythagorese drietallen.
A. Toon aan dat a en b niet tegelijk oneven kunnen zijn.
Veronderstel nu dat b even is. We kunnen veronderstellen omdat de gelijkheid symmetrisch is in a en b. Maar we moeten er achteraf dan wel rekening mee houden dat ook a 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.

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

2.6. Kleine stelling van Fermat

Als p een priemgetal is en a is een geheel getal dat geen veelvoud is van p, dan is $a^{p-1} \equiv 1 \pmod{p}$. De voorwaarde dat $p \nmid a$ is hier belangrijk en mag je zeker niet vergeten bij de oefeningen.

Oefening. Ga na dat de stelling klopt voor $p = 13$ en $a = 2$.

Oefening. Bewijs de stelling van Fermat.
Beschouw de getallen $x_1 = a, x_2 = 2a, \ldots, x_{p-1} = (p-1)a$.

A. Toon aan dat $x_i \equiv x_j \pmod{p}$ onmogelijk is als $i \neq j$.

Beschouw nu de resten van de getallen x_i 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 $y = x_1 \cdot x_2 \cdots x_{p-1}$. Toon aan dat $y \equiv (p-1)! \pmod{p}$.

D. Toon aan dat p geen deler is van $(p-1)!$.

E. Gebruik vragen C en D en toon aan dat $a^{p-1} \equiv 1 \pmod{p}$.

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

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

Oefening. Stel p is een priemgetal. Vind alle natuurlijke getallen a, kleiner dan p zodat $p \mid 1 + a + a^2 + \cdots + a^{p-1}$.

Oefening. Vind alle priemgetallen p en natuurlijke getallen a en b zodat $2^p + a^{p-1} = p^b$.

Oefening. (BrMO 1 2007 vraag 1) Vind vier priemgetallen $p < 100$ die delers zijn van $3^{32} - 2^{32}$.

2.7. Orde

Stel a en b zijn gehele getallen. Het kleinste natuurlijk getal met $n > 0$ waarvoor $a^n \equiv 1 \pmod{b}$ noemen we de orde van a modulo b. Merk op dat de voorwaarde $n > 0$ noodzakelijk is, anders zou de orde steeds 0 zijn. De orde van a modulo b wordt gewoonlijk

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

Oefening. Bewijs dat als a een orde heeft modulo b, dan $\text{ggd}(a,b)=1$.
A. Bewijs dat als a een orde heeft modulo b, dan $\text{ggd}(a,b)=1$.
Nu bewijzen we nog de omgekeerde eigenschap. Stel dus dat $\text{ggd}(a,b)=1$.
A. Toon aan dat er natuurlijke getallen k en l bestaan met $k>l$ zodat $a^k \equiv a^l \pmod{b}$.
B. Toon aan dat er een natuurlijk getal n bestaat met $n>0$ zodat $a^n \equiv 1 \pmod{b}$.
Bijgevolg bestaat er ook een kleinst mogelijke waarde voor n en heeft a een orde modulo b.

Oefening. Stel dat n de orde is van a modulo b, en dat m een natuurlijk getal is zodat $a^m \equiv 1 \pmod{b}$. Bewijs dat $n \mid m$.

Oefening. Zij a,b,p,q gehele getallen met $p,q>0$ en zij n de orde van a modulo b. Toon aan dat $a^p \equiv a^q \pmod{b}$ als en slechts als $p \equiv q \pmod{n}$.

2.8. Stelling van Euler
De stelling van Euler zegt dat als a en n gehele getallen zijn met $\text{ggd}(a,n)=1$ en $n>1$, dan is $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Oefening. 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 $a^{\varphi(p^{k+1})} = \left(a^{\varphi(p^k)}\right)^p$.
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 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

2.9. Stelling van Wilson
Als p een priemgetal is, dan geldt $(p-1)! \equiv -1 \pmod{p}$.

Oefening. Bewijs de stelling van Wilson.
Het is eenvoudig te controleren dat de stelling geldt voor $p=2$. Veronderstel nu dat $p>2$.
A. Vind eerst alle gehele getallen a met $0 \le a < p$ zodat $a^2 \equiv 1 \pmod{p}$.
B. Toon aan dat voor elk geheel getal a met $0 \le a < p$ dat niet voldoet aan vraag A er een ander geheel getal b met $0 \le b < p$ bestaat zodat $ab \equiv 1 \pmod{p}$, en dat zo'n getal b niet voor verschillende getallen a wordt 'gebruikt'.
C. Toon aan dat $(p-1)! \equiv -1 \pmod{p}$.

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

Oefening. Stel p is een oneven priemgetal en k is een natuurlijk getal met $k \le p$. Toon aan dat $(k-1)!(p-k)! \equiv (-1)^k \pmod{p}$.

Oefening. Bereken $1! \cdot 2! \cdot 3! \cdots 10! \mod 11$.

Oefening. Stel dat p een oneven priemgetal is zodat $\left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$. Toon aan dat $p \equiv 3 \pmod 4$.

2.10. Lifting The Exponent Lemma

Het "Lifting The Exponent Lemma" is eigenlijk een verzameling van Lemma's. Het wordt afgekort als LTE. Om te beginnen voeren we enkele notaties in. Stel p is een priemgetal en $n > 0$ een natuurlijk getal. Met $v_p(n)$ bedoelen we de grootste exponent a zodat $p^a \mid n$. We noteren ook $p^a \parallel n$. Bijvoorbeeld: $v_3(63) = 2$, $v_5(1000) = 3$.

Oefening. Toon aan dat $v_p(mn) = v_p(m) + v_p(n)$.

Lemma 1.

Als p geen deler is van n, x of y en $p \mid x-y$ dan geldt $v_p(x^n - y^n) = v_p(x-y)$.

Oefening. Bewijs Lemma 1.

Lemma 2. Het eigenlijke LTE.

Als $p > 2$ een priemgetal is zodat p geen deler is van x of y en $p \mid x-y$, en $n > 0$ een natuurlijk getal, dan geldt $v_p(x^n - y^n) = v_p(x-y) + v_p(n)$.

Oefening. Bewijs Lemma 2.

We bewijzen dit via inductie op $v_p(n)$.

Basisstap. We tonen het aan als $v_p(n) = 1$. Stel dus $n = pb$ zodat p geen deler is van b.

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

B. Toon aan dat $p \mid \sum_{i=0}^{p-1} x^i y^{n-i-1}$.

Vervolgens tonen we aan dat p^2 geen deler is van $\sum_{i=0}^{p-1} x^i y^{n-i-1}$. Stel daarvoor $y = x + kp$.

C. Toon aan dat $x^i y^{n-i-1} \equiv x^{p-1} + ikpx^{p-2} \pmod{p^2}$.

C. Toon aan dat p^2 geen deler is van $\sum_{i=0}^{p-1} x^i y^{n-i-1}$.

D. Toon aan dat $v_p(x^n - y^n) = v_p(x-y) + 1$.

Inductiestap. Veronderstel dat het lemma geldt voor $v_p(n) = a$ met $a > 0$. We tonen het lemma nu aan voor $v_p(n) = a+1$. Stel dus $n = p^{a+1}b$ zodat p geen deler is van b.

E. Toon aan dat $v_p(x^n - y^n) = v_p(x^{p^{a+1}} - y^{p^{a+1}})$.

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

G. Toon aan dat $v_p(x^n - y^n) = v_p(x-y) + v_p(n)$.

Lemma 2 is nu bewezen via inductie.

Lemma 3. LTE voor het geval $p = 2$.

Als x en y oneven zijn zodat $4 \mid x - y$, dan geldt $v_2(x^n - y^n) = v_2(x-y) + v_2(n)$.

Oefening. Bewijs lemma 3.

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

A. Toon aan dat $v_2(x^n - y^n) = v_2(x^{2^a} - y^{2^a})$.

B. Toon aan dat $x^{2^a} - y^{2^a} = (x-y)\prod_{k=0}^{a-1}(x^{2^k} + y^{2^k})$.

C. Toon aan dat $x^{2^k} + y^{2^k} \equiv 2 \pmod 4$ voor $k \geq 0$.

D. Toon aan dat $v_2(x^n - y^n) = v_2(x-y) + v_2(n)$.

Lemma 3 is nu bewezen.

Lemma 4.

Als x en y oneven zijn en n even, dan geldt $v_2(x^n - y^n) = v_2(x+y) + v_2(x-y) + v_2(n) - 1$.

Oefening. Bewijs lemma 4.

We bewijzen dit via inductie op $v_2(n)$.

Basisstap. Veronderstel dat $v_2(n) = 1$.

A. Toon aan dat $v_2(x^n - y^n) = v_2(x^2 - y^2)$.

B. Toon aan dat $v_2(x^n - y^n) = v_2(x+y) + v_2(x-y) + v_2(n) - 1$.

Inductiestap. Veronderstel dat het geldt voor $v_2(n) = a$ met $a > 0$. We tonen het lemma nu aan voor $v_2(n) = a+1$. Stel dus $n = 2^{a+1}b$ met b oneven.

C. Toon aan dat $v_2(x^n - y^n) = v_2(x^{2^{a+1}} - y^{2^{a+1}})$.

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

E. Toon aan dat $v_2(x^n - y^n) = v_2(x^2 - y^2) + a$.

F. Toon aan dat $v_2(x^n - y^n) = v_2(x+y) + v_2(x-y) + v_2(n) - 1$.

Lemma 4 is nu bewezen via inductie.

Oefening. Stel a, b en n zijn gehele getallen met $a \neq b$, $\gcd(a,b) = 1$ en $n > 0$. Toon aan dat $\gcd\left(a-b, \frac{a^n - b^n}{a-b}\right) \mid n$.

Oefening. (EMC 2012 vraag 1) Vind alle natuurlijke getallen $a, b, n > 0$ en priemgetallen p waarvoor geldt dat $a^{2013} + b^{2013} = p^n$.

Oefening. (BxMO 2010 vraag 4) Bepaal alle viertallen (a, b, p, n) van natuurlijke getallen groter dan 0 zodat p een priemgetal is en $a^3 + b^3 = p^n$.

Oefening. (Frankrijk 2012 dag 1 vraag 3) Vind alle viertallen (p, a, b, c) met p priem en $a, b, c > 0$ gehele getallen zodat geldt dat $a^p + b^p = p^c$.

Oefeningen

Oefening. 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.

Oefening. (CanMO 1973 vraag 3) Bewijs dat als p en $p+2$ priemgetallen zijn groter dan 3, dat 6 een deler is van $p+1$.

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

Oefening. 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?

Oefening. (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?

Oefening. Twee priemgetallen p en q met $q = p+2$ noemen we een priemtweeling.
A. Vind vier priemtweelingen.
Drie priemgetallen p, q en r met $r = q+2 = p+4$ noemen we een priemdrieling.
B. Vind alle priemdrielingen.

Oefening. (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 5 keer zoveel Vlamingen als Brusselaars de hand had gegeven. Thomas antwoordde met "Ik heb precies 3 keer zoveel Walen als Brusselaars een hand geschud". Uit welk gewest komt Nathalie en uit welk gewest komt Thomas?

Oefening. (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.

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

Oefening. (Polen MO 1998 ronde 1 vraag 1) Bewijs dat er onder de getallen $50^n + (50n+1)^{50}$, met n een natuurlijke getal, oneindig veel samengestelde getallen zijn.

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

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

Oefening. Bewijs dat voor natuurlijke getallen n geldt dat $7 \mid n^3 + 3^n$ als en slechts als $7 \mid n^3 \cdot 3^n + 1$.

Oefening. Bepaal alle natuurlijke getallen n zodat $2^n \mid 3^n - 1$.

Oefening. Zij a, b, d, n natuurlijke getallen zodat 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.

Oefening. (VWO 1992 finale vraag 1) Bepaal voor elk natuurlijk getal n het grootste natuurlijk getal k zodat $2^k \mid 3^n + 1$.

Oefening. Stel dat $\text{ggd}(m,n) = 1$. Toon aan dat $n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{mn}$.

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

Oefening. (CanMO 1971 vraag 6) Toon aan dat voor alle gehele getallen n, $n^2 + 2n + 12$ geen veelvoud is van 121.

Oefening. (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 $n = 2006$?

Oefening. (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?

Oefening. (VWO 2001 finale vraag 1) Toon aan dat voor elk natuurlijk getal $n > 1$ geldt dat $(n-1)^2 \mid n^{n-1} - 1$.

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

Oefening. Zij $p \geq 5$ een priemgetal. Bewijs dat $7^p - 6^p - 1$ deelbaar is door 43.

Oefening. (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.

Oefening. (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.

Oefening. Bepaal alle natuurlijke getallen x, y en z zodat $3^x + 4^y = 5^z$.

Oefening. Zij $P(n)$ een niet-constante veelterm met gehele coëfficiënten. Bewijs dat er oneindig veel natuurlijke getallen n bestaan waarvoor $|P(n)|$ geen priemgetal is.

Oefening. Bepaal de drie laatste cijfers van het getal $2003^{2002^{2001}}$.

Oefening. Zij p een priemgetal. Vind alle natuurlijke getallen n met de eigenschap dat er geen geheel getal x bestaat zodat $x^n - 1$ deelbaar is door p maar niet door p^2.

Oefening. (USAMO 1986 vraag 3) Bepaal het kleinste natuurlijk getal n zodat het rekenkundig gemiddelde van de getallen $1^2, 2^2, \cdots, n^2$ zelf een kwadraat is.

Oefening. 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.

Oefening. (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?

Oefening. (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.

Oefening. (IMO 1999 dag 2 vraag 1) Bepaal alle paren natuurlijke getallen n en priemgetallen p waarvoor $n < 2p$ en $n^{p-1} \mid (p-1)^n + 1$.

Oefening. (IMOSL 1991 vraag 18) Vind de hoogste waarde van k zodat 1991^k een deler is van $1990^{1991^{1992}} + 1992^{1991^{1990}}$.

Hoofdstuk 3. Kwadraatresten

Legendre symbool

Het Legendre symbool of kwadratisch karakter is een functie die als resultaat geeft of een geheel getal a een kwadraatrest is modulo een priemgetal p. We schrijven $\left(\frac{a}{p}\right)$.

Per definitie is $\left(\frac{a}{p}\right)=0$ als $p \mid a$, $\left(\frac{a}{p}\right)=1$ als a een kwadraatrest is modulo p maar geen veelvoud is van p, en $\left(\frac{a}{p}\right)=-1$ als a geen kwadraatrest is modulo p.

Oefening. Toon aan dat $\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\cdots+\left(\frac{p}{p}\right)=0$.

Criterium van Euler

Het criterium van Euler zegt dat $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

Oefening. Bewijs het criterium van Euler.
A. Bewijs het criterium in het geval dat $p \mid a$.
B. Bewijs het criterium in het geval dat a een kwadraatrest is modulo p.
Veronderstel nu dat a geen kwadraatrest is modulo p. Toon aan dat voor elk getal x met $0 \le x < p$ er een y met $0 \le y < p$ bestaat zodat $xy \equiv a \pmod{p}$.
C. 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.

Oefening. Toon aan dat $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=\left(\frac{ab}{p}\right)$.

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

Oefening. Toon aan dat er oneindig veel priemgetallen van de vorm $4k+1$ bestaan.

Oefening. Stel dat p een priemgetal is en $\gcd(ab, p)=1$. Bewijs dat als p een deler is van a^2+b^2, dan $p \equiv 1 \pmod{4}$.

Primitieve wortel

Als $n>0$ een natuurlijk getal is, dan is a een primitieve wortel modulo n als en slechts als de orde van a modulo n gelijk is aan $\varphi(n)$.

Oefening. Toon aan dat als a een primitieve wortel is modulo met $n > 2$, dan $a^{\frac{\varphi(n)}{2}} \equiv -1 \pmod{n}$.

Kleinste absolute rest

Een lichte variatie op de gewoonlijke rest is de zogenaamde kleinste absolute rest. Bij deling van a door b is de kleinste absolute rest het geheel getal r waarvoor er een geheel getal q bestaat zodat $a = qb + r$, en r in het interval $\left]\frac{-|b|}{2}, \frac{|b|}{2}\right]$ ligt. 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. Je vraagt je misschien af waarom dit nog niet eerder aan bod kwam, aangezien dit helemaal geen moeilijke theorie is. De bedoeling was echter om geen verwarring te zaaien, en dit soort rest komt toch ook maar zelden van pas.

Oefening. Bepaal de kleinste absolute rest bij deling van

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

Lemma van Gauss

Stel p is een oneven priemgetal en a een geheel getal dat niet deelbaar is door p. Beschouw de getallen $a, 2a, \cdots, \frac{p-1}{2}a$ en hun resten bij deling door p. Deze resten zijn allemaal verschillend. Stel n is het aantal resten die groter zijn dan $\frac{p}{2}$.

Het lemma van Gauss zegt dat $\left(\frac{a}{p}\right) = (-1)^n$.

Oefening. 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. Voor een geheel getal x met rest r bij deling door p geldt dus dat $d(x) = r$ als $0 \le r \le \frac{p-1}{2}$ en $d(x) = p - r$ als $\frac{p+1}{2} \le r \le p-1$. Stel n is het aantal resten van de getallen $a, 2a, \cdots, \frac{p-1}{2}a$ bij deling door p, die groter zijn dan $\frac{p}{2}$.

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 $1 \le v, w \le \frac{p-1}{2}$ alleen kan als $v = w$.

C. Toon aan dat de getallen $d(a), d(2a), \cdots, d\left(\frac{p-1}{2}a\right)$ gelijk zijn aan de getallen

$1, 2, \cdots, \frac{p-1}{2}$, in een willekeurige volgorde.

D. Toon aan dat $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$.

Het lemma van Gauss volgt nu uit het criterium van Euler.

Oefening. Bewijs dat $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

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 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Oefening. Bewijs dat 2 een kwadraatrest is modulo een priemgetal p als en slechts als $p \equiv 1 \pmod{8}$, $p \equiv -1 \pmod{8}$ of $p = 2$.

Oefening. Zij $n \ge 3$ oneven en zij p een priemdeler van $2^n - 1$. Bewijs dat $p \equiv \pm 1 \pmod{8}$.

<u>Lemma van Eisenstein</u>

Het lemma van Eisenstein geeft een alternatieve notatie voor het Legendre symbool. Het lemma zegt dat als p een oneven priemgetal is dat geen deler is van een oneven geheel getal a, dan geldt $\left(\frac{a}{p}\right) = (-1)^{\alpha(a,p)}$ met $\alpha(a,p) = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$.

Oefening. Bewijs het lemma van Eisenstein.

Zij U de verzameling gehele getallen $\left\{a, 2a, \cdots, \frac{p-1}{2}a\right\}$ en stel $u_i = ia$. We definiëren V als de verzameling van de resten van de getallen uit U bij deling door p. Noem r_i de rest van u_i bij deling door p. V bevat m getallen $b_1, b_2, \cdots, b_m$ die kleiner zijn dan $\frac{p}{2}$ en n getallen $c_1, c_2, \cdots, c_n$ die groter zijn dan $\frac{p}{2}$.

A. Toon aan dat $m+n=\frac{p-1}{2}$.

B. Toon aan dat $u_i = p\cdot\left\lfloor \frac{ia}{p} \right\rfloor + r_i$.

Noem t de som van de getallen in U, x de som van de getallen b_i en y de som van de getallen c_i.

C. Toon aan dat $t = p\cdot\alpha(a,p)+x+y$.

Zij W de verzameling van de getallen $b_1, b_2, \cdots, b_m$ en $p-c_1, p-c_2, \cdots, p-c_n$.

D. Toon aan dat de getallen in W gelijk zijn aan de getallen $1, 2, \cdots, \frac{p-1}{2}$.

Noem w de som van de getallen in W.

E. Toon aan dat $w = x+pn-y$.

F. Toon aan dat $t-w = p\cdot\alpha(a,p)-2y-pn$.

G. Toon aan dat $n \equiv \alpha(a,p) \pmod 2$.

H. Toon aan dat $\left(\frac{a}{p}\right) = (-1)^{\alpha(a,p)}$.

Oefening. Zij p een oneven priemgetal en a een even geheel getal, niet deelbaar door p.

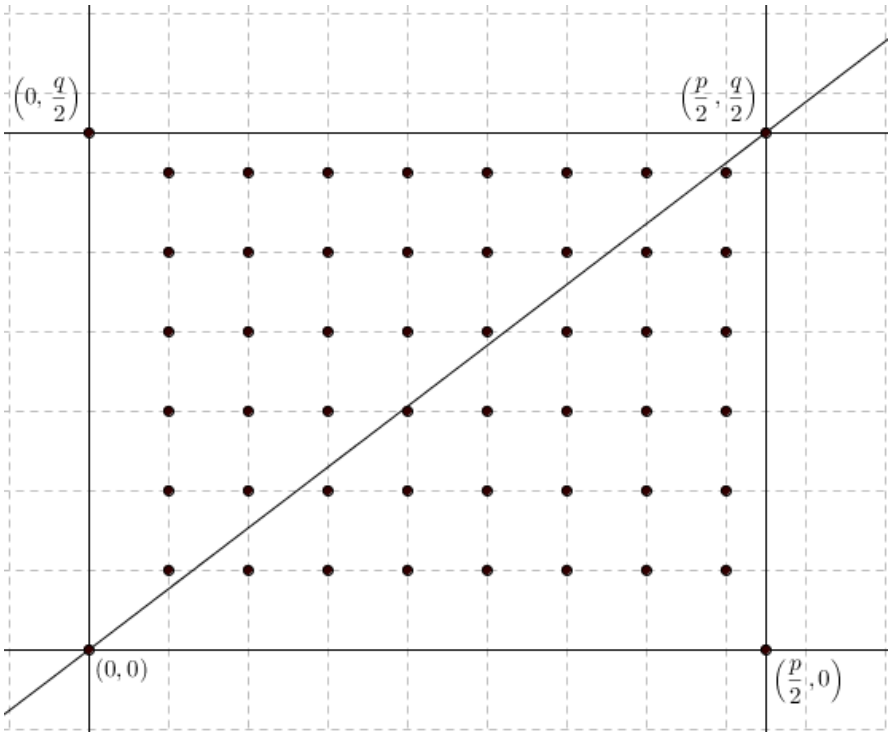
Bewijs dat $\left(\frac{2a}{p}\right) = (-1)^{\alpha(a,p)}$.

<u>Wet van de kwadratische reciprociteit</u>

Voor oneven priemgetallen p en q geldt dat $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Oefening. 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 constructie in een orthonormaal assenstelsel zoals op de figuur.



A. Toon aan dat er geen roosterpunten op de schuine rechte 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. Toon aan dat $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$.

Oefening. Stel dat p en q verschillende priemgetallen zijn zodat $4 \mid p-q$. Bewijs dat q een kwadraatrest is modulo p als en slechts als p een kwadraatrest is modulo q.

Oefeningen

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

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

Oefening. Vind het grootste natuurlijk getal a zodat $a \mid p^{2010}-q^{2010}$ voor alle priemgetallen p en q zodat p minstens 2010 cijfers en q minstens 1020 cijfers heeft.

Hoofdstuk 4. Sommen van kwadraten

Van een natuurlijk getal n zeggen we dat het de som is van twee kwadraten als het kan worden geschreven in de vorm a^2+b^2, met a en b natuurlijke getallen. Bijvoorbeeld, 13 en 4 zijn de som van twee kwadraten, want $13=2^2+3^2$ en $4=0^2+2^2$. Analoog hebben we sommen van drie kwadraten, enzovoort. Merk op dat ook 0 de som is van twee kwadraten. In dit hoofdstuk zullen we bestuderen wanneer een getal kan geschreven worden als de som van twee of meer kwadraten, en op hoeveel manieren zoiets mogelijk is.

4.1. Stelling van 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. Dit volgt uit de identiteit van Brahmagupta-Fibonacci, namelijk $(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$.

Gevolg.
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 $n_1n_2\cdots n_m$ worden geschreven als de som van twee kwadraten. Want met de identiteit van Brahmagupta-Fibonacci kunnen we n_{m-1} en n_m vervangen door één getal dat de som is van twee kwadraten, zodat er nog slechts $m-1$ getallen overblijven. Zo kunnen we steeds het aantal verkleinen, tot er nog maar één getal staat, dat de som is van twee kwadraten. (Eigenlijk passen we hier dus inductie toe, hoewel we het zo niet omschrijven: we vallen terug op een kleiner aantal, $m-1$, en kunnen daaruit besluiten dat het ook waar is voor m.

Oefening. Toon aan dat je $(a^2+b^2)(c^2+d^2)$ op nog een andere manier kan schrijven als de som van twee kwadraten.

Oefening. Stel dat n een natuurijk getal is zodat $2n$ de som is van twee kwadraten. Bewijs dat ook n de som is van twee kwadraten.

Oefening. (VWO 2005 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.

4.2. Stelling: product van twee sommen van kwadraten

Als een natuurijk getal op twee manieren te schrijven is als de som van twee kwadraten, dan is dat getal ook het product van twee sommen van twee kwadraten.

Oefening. Bewijs de bovenstaande stelling.
Stel n is een natuurlijk getal zodat $n=a^2+b^2=c^2+d^2$ met $a,b,c,d>0$.

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.

Oefening. Toon aan dat een priemgetal op hoogstens één manier kan worden geschreven als de som van twee kwadraten.

4.3. Kerststelling van Fermat

Een oneven priemgetal p kan worden geschreven als de som van twee kwadraten als en slechts als $p \equiv 1 \pmod 4$.

Oefening. Bewijs de kerststelling van Fermat.

We noemen ons priemgetal voor de verandering eens n.

A. Toon aan dat een priemgetal $n \equiv 3 \pmod 4$ niet kan worden geschreven als de som van twee kwadraten.

Stel nu $n \equiv 1 \pmod 4$

B. Toon aan dat er een getal v met $0 \le v < n$ bestaat zodat $n \mid v^2 + 1$.

Bijgevolg is $v^2 + 1 = kn$.

C. Toon aan dat $0 < k < n$.

Vervolgens zullen we bewijzen dat, als er getallen a en b bestaan zodat $a^2 + b^2 = xn$ voor een bepaald natuurlijk getal x met $0 < x < n$, er dan een natuurlijk getal y bestaat zodat $0 < y < x$, en waarvoor de vergelijking $a^2 + b^2 = yn$ ook oplossingen heeft voor gehele getallen a en b. Immers, dan kunnen we de waarde van y gebruiken om een nog kleiner getal te vinden, tot we uiteindelijk bij 1 uitkomen. En dan geldt $a^2 + b^2 = n$. Veronderstel nu dus dat $a^2 + b^2 = xn$. 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 $x^2 yn$ als de som van twee kwadraten $p^2 + q^2$.

F. Toon aan dat p en q beide deelbaar zijn door x.

Bijgevolg is $\left(\frac{p}{x}\right)^2 + \left(\frac{q}{x}\right)^2 = yn$, en hebben we een oplossing voor een kleinere waarde y.

Oefening. In het bewijs vond je een kleinere waarde dan x. Maar voor $x = 1$ is dat onmogelijk! Waar in het bewijs veronderstelde je dus dat $x > 1$?

3.4. Tweekwadratenstelling

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 de factor 3 wel met een even exponent voor, en inderdaad: $45 = 3^2 + 6^2$.

Oefening. Bewijs de tweekwadratenstelling.
We bewijzen eerst dat alle priemfactoren van de vorm $4k+3$ tot een even macht moeten voorkomen.
Stel $n = x^2 + y^2$ en $p = 4k+3$ is een priemgetal zodat $p \mid n$.

A. Toon aan dat $x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \cdot y^{p-1} \pmod{p}$.

B. Toon aan dat $p \mid x$, $p \mid y$ en dat p tot een even macht voorkomt in de priemontbinding van n.

Hiermee is het eerste deel bewezen. Nu bewijzen we nog dat elk getal n dat hieraan voldoet kan geschreven worden als de som van twee kwadraten.

C. Bewijs dat 2^a, p^b en q^{2c} elk de som zijn van twee kwadraten als $p \equiv 1 \pmod 4$ en $q \equiv 3 \pmod 4$.

D. Bewijs dat n de som is van twee kwadraten.

Oefening. Gebruik de identiteit van Brahmagupta-Fibonacci om p^2 en p^3 op twee verschillende manieren te schrijven als de som van twee kwadraten. (Twee manieren noemen we hier verschillend als de kwadraten niet gewoon omgewisseld zijn, of als een getal van teken verandert.)

Oefening. Vind alle priemgetallen p waarvoor er natuurlijke getallen a, b, n bestaan zodat $a^2 + b^2 = p^3$ en $a - b = n^3$.

Oefening. (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.

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

Oefening. Zij q een priemgetal van de vorm $4k+3$. Toon aan dat de vergelijking $x^2 + y^2 = q^{2k}$ voor elk natuurlijk getal k precies vier oplossingen heeft in gehele getallen.

Als n een natuurlijk getal is waarvan $p_1, p_2, \ldots, p_r$ de priemdelers van de vorm $4k+1$ zijn met bijbehorende exponenten $a_1, a_2, \ldots, a_r$, zodanig dat n kan geschreven worden als de som van twee kwadraten, dan zijn er precies $4 \cdot \prod_{i=1}^{r} (a_i + 1)$ oplossingen in gehele getallen x, y voor de vergelijking $x^2 + y^2 = n$. Het bewijs hiervoor is te complex en wordt hier niet vermeld.

Vier-kwadratenstelling van Lagrange

De vier-kwadratenstelling staat ook bekend als het vermoeden van Bachet. Dit vermoeden werd in 1770 bewezen door Langrange. De stelling zegt dat elk natuurlijk getal kan worden geschreven als de som van vier kwadraten. Bijvoorbeeld, $12 = 0^2 + 1^2 + 2^2 + 3^2$ en $28 = 1^2 + 1^2 + 1^2 + 5^2 = 2^2 + 2^2 + 2^2 + 4^2$. Zoals je ziet kan dit dus soms op meer manieren. Het bewijs steunt voornamelijk op de identiteit $(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = (aA + bB + cC + dD)^2 + (aB - bA + cD - dC)^2 + (aC - bD - cA + dB)^2 + (aD - dA + bC - cB)^2$, ook wel bekend als de vier-kwadratenidentiteit van Euler. Omdat je die waarschijnlijk niet onmiddellijk zelf had bedacht krijg je die identiteit cadeau.

Oefening. Toon aan dat je $(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2)$ nog op drie andere manieren kan schrijven als de som van twee kwadraten.

Oefening. Stel dat n een natuurijk getal is zodat $2n$ de som is van vier kwadraten. Bewijs dat ook n de som is van vier kwadraten.

Oefening. Bewijs de vierkwadratenstelling.

A. Toon aan dat het volstaat om te bewijzen dat elk priemgetal de som is van vier kwadraten.

B. Bewijs dat 2, en de priemgetallen van de vorm $4k+1$ de som zijn van vier kwadraten.

Stel $n = 4k + 3$ is een priemgetal. We zullen dezelfde techniek gebruiken als in het bewijs van de kerststelling.

C. Toon aan dat er getallen v en w met $0 \le v, w < n$ bestaan zodat $n \mid v^2 + w^2 + 1$.

Bijgevolg is $v^2 + w^2 + 1 = kn$.

D. Toon aan dat $0 < k < n$.

Merk op dat $kn = v^2 + w^2 + 1^2 + 0^2$, de som van vier kwadraten. Veronderstel nu dat er getallen a, b, c, d, x bestaan zodat $a^2 + b^2 + c^2 + d^2 = xn$ en $0 < x < n$. We zoeken een y met $0 < y < x$ waarvoor dit ook geldt, zodat we uiteindelijk $y = 1$ bekomen. Noem e, f, g, h de kleinste absolute resten van respectievelijk a, b, c, d bij deling door x.

E. Toon aan dat $e^2 + f^2 + g^2 + h^2 = yx$ en dat $0 < y < x$ geldt als x oneven is.

F. Schrijf $x^2 yn$ als de som van vier kwadraten $p^2 + q^2 + r^2 + s^2$, en toon aan p, q, r, s alle vier deelbaar zijn door x.

Bijgevolg is ook yn de som van vier kwadraten.

Stel nu dat x even is. We kunnen nu niet met zekerheid zeggen dat $0 < y < x$ voor $e^2 + f^2 + g^2 + h^2 = yx$, immers, het ongelukkige geval $e = f = g = h = \frac{x}{2}$ speelt ons parten.

Uit de vorige oefening weten we echter dat ook $\frac{xn}{2}$ de som van vier volkomen kwadraten is.

Stellen we nu $y = \frac{x}{2}$, dan hebben we $0 < y < x$ en is yn de som van vier kwadraten. Dus ook in het geval $n = 4k + 3$ hebben geldt de stelling. Hiermee is die dus bewezen.

Som van drie kwadraten

Legendre verbeterde de vier-kwadratenstelling door te stellen dat een natuurlijk getal kan worden geschreven als de som van drie kwadraten als en slechts als het niet van de vorm $4^k \cdot (8m + 7)$ is, met k en m natuurlijke getallen. Zijn bewijs was echter onvolledig en werd later voltooid door Gauss.

Oefening. 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.

Oefeningen

Oefening. (VWO 2003 finale vraag 4) In het vlak beschouwt men het rooster van alle punten met gehele coördinaatgetallen. Indien met een getal r goed kiest gaat de cirkel met middelpunt $(0,0)$ en met straal r door een aantal roosterpunten. (bv. 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.

Appendix

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.

Sommatieteken en multiplicatieteken

Een sommatieteken is een verkorte schrijfwijze van een som. Als f een functie is en a en b gehele getallen met $b \geq a$, noteren we $f(a) + f(a+1) + \cdots + f(b-1) + f(b)$ verkort als $\sum_{k=a}^{b} f(k)$. Hierbij is 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. Als ondergrens of bovengrens kan ook oneindig worden genomen.

Bijvoorbeeld: $\sum_{i=-\infty}^{-5} \frac{2}{i^2}$.

Wanneer de som leeg is, dan is de som 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.

Eigenschappen.

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 commutativiteit blijft behouden. We kunnen de som $\sum_{k=a}^{b} \big(f(k) + g(k)\big)$ schrijven als $\sum_{k=a}^{b} f(k) + \sum_{k=a}^{b} g(k)$.
4. Een ander gevolg van de commutativiteit 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 $\sum_{k=1}^{n} k = \frac{n \cdot (n+1)}{2}$ en $\sum_{k=1}^{n} k^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$.

Een multiplicatieteken doet hetzelfde voor een product. $f(a)\cdot f(a+1)\cdots f(b-1)\cdot f(b)$ noteren we als $\prod_{n=a}^{b} f(n)$. Als het product leeg is, dan is het gelijk aan 1.

Faculteit

De faculteit van een natuurlijk getal n met $n>0$ is het product van alle natuurlijke getallen groter dan 0 en kleiner of gelijk aan n. We zeggen "n faculteit" en we noteren $n!=\prod_{k=1}^{n} k$.

Bijvoorbeeld: $2!=2$, $4!=24$, $5!=120$. Per afspraak is $0!=1$.

Binomiaalcoëfficiënt

De binomiaalcoëfficiënt $\binom{a}{b}$, met a en b natuurlijke getallen en $0\le a\le b$ is een natuurlijk getal gelijk aan $\frac{a!}{b!\cdot(a-b)!}$. Bijvoorbeeld: $\binom{3}{2}=3$, $\binom{7}{5}=15$, $\binom{1}{0}=1$.

Binomium van Newton

Het binomium van newton is een algemene uitwerking van $(a+b)^n$ met n een natuurlijk getal: $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}\cdot a^k\cdot b^{n-k}$. Bijvoorbeeld: $(a+b)^4=a^4+4a^3b+6a^2b^2+4ab^3+b^4$ en $(a-1)^5=a^5-5a^4+10a^3-10a^2+5a-1$.

Ontbindingen

Voor $n>0$ een natuurlijk getal en $a,b\neq 0$ reële getallen is $a^n-b^n=(a-b)\cdot\sum_{k=0}^{n-1}a^k b^{n-k-1}$.

Bijvoorbeeld: $a^3-2^3=(a-2)(a^2+2a+4)$.

Lijst van competities

BaMO: Bay Area Mathematical Olympiad
BrMO: British Mathematical Olympiad
BSMC: Balkan Student Mathematical Competition
BxMO: Benelux Mathematical Olympiad
CanMO: Canadian Mathematical Olympiad
EGMO: European Girls' Mathematical Olympiad
EMC: European Mathematical Cup
IMC: International Mathematics Competition for University Students
IMO: International Mathematical Olympiad
IMOSL: International Mathematical Olympiad Shortlist
IrMO: Irish Mathematical Olympiad
JBMO: Junior Balkan Mathematical Olympiad
JEMC: Junior European Mathematical Cup
JWO: Junior Wiskunde Olympiade
NWO: Nederlandse Wiskunde Olympiade
PUMA: Pure Mathematics
Putnam: William Lowell Putnam Competition
RMM: Romanian Master in Mathematics
USAMO: United States of America Mathematical Olympiad
VWO: Vlaamse Wiskunde Olympiade
WINA