Getaltheorie

Hoofdstuk 1. Deelbaarheid

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 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: $b \mid a$.
Als een getal een veelvoud is van 2 noemen we dat getal "even". In het andere geval noemen we het getal "oneven".

Gevolgen.
1. 0 is deelbaar door elk geheel getal. Immers, voor elk geheel getal a bestaat er een getal k zodat $0 = ka$, namelijk $k = 0$.
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 $a > 0$ is $k > 0$, zodat $b = \frac{a}{k} \leq a$.
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 $a \leq b$, dus $a = b$.
4. Als twee positieve getallen a en b dezelfde delers hebben, dan zijn ze gelijk. Want omdat $a \mid a$ geldt dan $a \mid b$. Analoog geldt dat $b \mid a$. Uit het derde gevolg weten we dan dat $a = b$.

Oefening. Stel dat $a \mid b$ en $b \mid c$. Toon aan dat $a \mid c$.

Oefening. Bepaal alle gehele delers van 10, 17, 24, 31 en 50.

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.

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".
De rest van een getal a bij deling door 2 noemen we ook "de pariteit van a".

Oefening. Bewijs dat het quotiënt en de rest bij deling van a door b uniek zijn.
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 dan 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.
C. -5 door 8.
D. -50 door -9.

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

Grootste gemene deler

Twee getallen hebben gemeenschappelijke delers. 1 is bijvoorbeeld een deler van elk getal. 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 a en b. We noteren $\text{ggd}(a,b)=d$. Bijvoorbeeld: $\text{ggd}(6,10)=2$, $\text{ggd}(0,5)=5$, $\text{ggd}(-12,-16)=4$.
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: $\text{ggd}(15,-12,3)=3$.
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".

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

Stelling van Bézout

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

Oefening. Bewijs de stelling van Bézout.
Noem V de verzameling van alle lineaire combinaties van a en b.
A. Toon aan dat V een 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|d, en dat $c\leq d$.
Bijgevolg is d de grootste gemene deler van a en b, en is d 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 $\text{ggd}(a,b)\le ax+by$.

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 $a\mid c$.

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

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

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

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

Oefening. Bewijs de volgende veralgemening van de stelling van Bézout. 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 $a_1,a_2,\cdots,a_n$.

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

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

<u>Algoritme van Euclides</u>
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 $\text{ggd}(a,b)=\text{ggd}(a,r)$.
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. Dat noteren we boven de deler. Dan berekenen we het product van het quotiënt met de deler, en dat noteren we onder het deeltal.

	1				
459	342				
342					

Dan trekken we het bekomen product af van het deeltal en hebben we 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 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.

<u>Lineaire diophantische vergelijking</u>
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 $y=y_0-\frac{ka}{d}$.

Voorbeeld. Bepaal alle oplossingen voor x en y van de vergelijking $24x-10y=6$.
Oplossing.
We schrijven eerst $\text{ggd}(24,-10)$, of dus $\text{ggd}(24,10)$, als lineaire combinatie van 24 en 10 via het rekenschema van Euclides.

	2	2	2		
24	10	4	2	0	
20	8	4			

We vinden $\text{ggd}(24,10)=2=1\cdot 10-2\cdot 4=1\cdot 10-2\cdot(1\cdot 24-2\cdot 10)=-2\cdot 24+5\cdot 10$, of dus $2=-2\cdot 24-5\cdot(-10)$.
Om 6 te schrijven als lineaire combinatie vinden we dan $6=3\cdot 2=-6\cdot 24-15\cdot(-10)$.
We hebben dus dat $x_0=-6$ en $y_0=-15$.
De algemene oplossing is dan $x=x_0+\frac{k\cdot(-10)}{2}=-6-5k$ en $y=y_0-\frac{k\cdot 24}{2}=-15-12k$,
met k een willekeurig geheel getal.

Oefening. Bepaal alle oplossingen voor x en y van de vergelijking $25x-14y=-8$.

<u>Kleinste gemene veelvoud</u>
Het kleinste gemene veelvoud k van twee gehele getallen a en b is het kleinste natuurlijk getal, groter dan 0, dat een veelvoud is van a en b. We noteren $\text{kgv}(a,b)=k$. Bijvoorbeeld: $\text{kgv}(8,6)=24$, $\text{kgv}(-2,5)=10$, $\text{kgv}(-10,-18)=90$.
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 $a \mid r$. Analoog geldt 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. Dan moet $r = 0$, dus $k \mid c$.

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".
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 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 $\text{ggd}(p,q) = p$.
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 $0 \le a < p$.

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 $p_1, p_2, \cdots, p_r$ priemgetallen zijn met $p_1 < p_2 < \cdots < p_r$ en $a_1, a_2, \cdots, a_n$ natuurlijke getallen groter dan 0. Dit product noemen we de priemontbinding of priemfactorisatie van n.

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 $n = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_s$.
A. Toon aan dat q_s niet in de rij $p_1, p_2, \cdots, p_r$ 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 $\text{ggd}(x,y) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_r^{\min(a_r,b_r)}$.
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 $\text{kgv}(x,y) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_r^{\max(a_r,b_r)}$.

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. 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, dus het is onmogelijk dat er slechts een eindig aantal priemgetallen bestaat.

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

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 n met $n > 1$ een volkomen kwadraat is als en slechts alle priemfactoren van n tot een even macht voorkomen in de priemontbinding.

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

<u>Aantal delers van een natuurlijk getal</u>
Als n een natuurlijk getal is met priemontbinding $p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$, dan is het aantal positieve delers $\tau(n)$ van n gelijk aan $(a_1+1)(a_2+1)\cdots(a_r+1)$.

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

Oefening. Hoeveel gehele delers heeft 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.

Som van de delers van een natuurlijk getal.

Als n 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 2^{12}.

Oefening. Bepaal de som van de positieve delers van 1000.

Oefening. Zij n 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.

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. Voorbeelden van ontbindingen zijn $a^2-b^2=(a-b)(a+b)$, $a^3-b^3=(a-b)(a^2+ab+b^2)$ en $ab+a+b+1=(a+1)(b+1)$.

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. $a^3+b^3+c^3-3abc$

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. Vind alle natuurlijke getallen n zodat $7^n \mid 9^n-1$.

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 $p^2+q^2=n^2$.

Oefening. Voor welke natuurlijke getallen n is n^4+4^n een priemgetal?

Ongelijkheden

Het kan gebeuren dat een diophantische vergelijking geen oplossingen heeft omdat het ene lid steeds groter is dan het andere. Het volstaat dat van de ongelijkheid bewijzen om aan te tonen dat er geen oplossingen zijn.

Voorbeeld. Vind alle natuurlijke getallen a, b en c zodat $a!+b!=c!$.

Oplossing.

Stel eerst dat $a=b$. Dan is $2a!=c!$. We zien dat $a=0$ en $a=1$ een oplossing geven. Stel nu $a>1$. Omdat $c>a$ en a en c natuurlijke getallen zijn, is $c\geq a+1$. Dan is $c!\geq(a+1)!=(a+1)\cdot a!\geq(2+1)\cdot a!>2a!$. Het is dus onmogelijk dat $2a!=c!$ omdat $c!$ steeds groter is.

Stel nu $a<b$. Als $a,b<2$ krijgen we terug de oplossing $c=2$. Stel dus $1<a<b$.

Omdat $c!=a!+b!>b!$ is c groter dan b. We zien dat $c!\geq(b+1)!=(b+1)\cdot b!>(1+1)b!>a!+b!$, dus is het onmogelijk dat $a!+b!=c!$ omdat $c!$ steeds groter is.

De enige oplossingen zijn dus die met $a,b<2$ en $c=2$.

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 $a^a+b^b=c^c$.

Indicator

De indicator of totiënt van een natuurlijk getal $n>1$ is het aantal natuurlijke getallen groter dan 0 en kleiner of gelijk aan n dat relatief priem is met n. We noteren $\varphi(n)$, waar φ de Euler totiënt functie of phi functie is.

Als $n=p_1^{a_1}\cdot p_2^{a_2}\cdots p_r^{a_r}$, 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 dat relatief priem is 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.

Oefeningen

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

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. (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 $34! = 95232799cd960414084761860964 35ab000000$. 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. (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. Vind alle drietallen (a,b,c,n,p) met p priem zodat $a^2+b^2=c^2$ en $a+b+c=p^n$.

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

Oefening. 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 priemgetal.

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 $n \geq 2$ een natuurlijk getal, met delers $1 = d_1 < d_2 < \cdots < d_k = n$. Bewijs dat $d_1 d_2 + d_2 d_3 + \cdots + d_{k-1} d_k$ altijd kleiner is dan n^2 en bepaal wanneer het een deler is van n^2.

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

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 $a \equiv 0 \pmod{c}$.
Het is belangrijk om te weten dat dit nieuw symbool niets meer is dan een handige 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".
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 $a \equiv b \pmod{c}$.

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.

Oefening. Bereken $10^{10} \mod 3$

Oefening. Bereken $17^9 \mod 7$.

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

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 $a + b$.

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.

Inverse

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

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 $\text{ggd}(a,b) = 1$.

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 de eigenschap uit oefening 5 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 $ax \equiv c \pmod{b}$.

Oefening. Vind alle natuurlijke getallen n met $0 \leq n < 12$ zodat $9n \equiv 6 \pmod{12}$.

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 $ax \equiv c \pmod{b}$.

Chinese reststelling

De Chinese reststelling zegt dat als $m_1, m_2, \cdots, m_n$ gehele getallen zijn die paarsgewijs relatief priem zijn, en $a_1, a_2, \cdots, a_n$ zijn 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 afgekort als CRS.

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 $p_i m_i + \frac{q_i y}{m_i} = 1$.

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

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.

Oefening. 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 $i \neq j$.

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

<u>Kwadraatrest</u>

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 $x^2 \equiv b \pmod{a}$. Een niet-kwadraatrest modulo b is een getal dat geen kwadraatrest is modulo b.

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

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

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

Oefening. Toon aan dat 0 en 1 de enige kwadraatresten zijn modulo 4.

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

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

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

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

Oefening. Vind alle kwadraatresten 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.

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 kwadraatresten 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 $a\cdot(a+2)=3^n-2$.

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 $7\mid n^3\cdot 3^n+1$.

<u>Pythagorees drietal</u>

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.

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 $c=x^2+y^2$.

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.

<u>Kleine stelling van Fermat</u>

Als p een priemgetal is en a is een geheel getal dat geen veelvoud is van p, dan is $a^{p-1}\equiv 1 \pmod{p}$.

Oefening. Bewijs de stelling van Fermat.

Beschouw de getallen $x_1=a$, $x_2=2a$, ..., $x_{p-1}=(p-1)a$.

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

Beschouw nu de resten van x_i modulo p. Wegens het vorige zijn die dus allemaal verschillend.

B. Toon aan dat die resten de getallen 1, 2, ..., $p-1$ 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 $3^{32} - 2^{32}$.

Orde

Stel a en b zijn gehele getallen. Het kleinste natuurlijk getal n met $n > 0$ waarvoor $a^n \equiv 1 \pmod{b}$ noemen we de orde van a modulo b.

Oefening. Bewijs dat als a een orde heeft modulo b, dan $\text{ggd}(a,b) = 1$.

Oefening. Stel dat $\text{ggd}(a,b) = 1$. Bewijs dat a een orde heeft modulo b.

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 en 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 $p \equiv q \pmod{n}$.

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

Stelling van Wilson.

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

Oefening. Bewijs de stelling van Wilson.
De stelling geldt voor $p = 2$. Veronderstel nu dat $p > 2$.
A. Vind 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 1 er een geheel getal b met $0 \le b < p$ bestaat zodat $ab \equiv 1 \pmod{p}$.
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 $1! \cdot 2! \cdot 3! \cdots 10! \bmod 11$.

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

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.

<u>Lemma 3.</u> 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.

<u>Lemma 4.</u>

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 $a \neq b$, $\text{ggd}(a,b) = 1$ en $n > 0$. Toon aan dat $\text{ggd}\left(a-b, \frac{a^n - b^n}{a-b}\right) \mid n$.

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 $a^3 + b^3 = p^n$.

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. 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 $a+1$ de inverse is van $b-1$ 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. (CanMO 1971 vraag 6) Toon aan dat voor alle gehele getallen n, $n^2 + 2n + 12$ geen veelvoud is van 121.

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

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. (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 2) 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. Kwadratische stellingen

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 a een primitieve wortel is modulo met $n > 2$ als en slechts als $a^{\frac{\varphi(n)}{2}} \equiv -1 \pmod{n}$.

Oefening. Toon aan dat 2 een primitieve wortel is modulo 3^n, voor $n \geq 1$.

Oefening. Stel dat a een primitieve wortel is modulo p^m. Bewijs dat a een primitieve wortel is modulo p^n voor alle $n > m$.

Oefening. Vind alle natuurlijke getallen n zodat er een primitieve wortel bestaat modulo n.
Stel $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ en veronderstel dat er een primitieve wortel bestaat modulo n.

A. Toon aan dat de getallen $(p_1 - 1)p_1^{a_1 - 1}, (p_2 - 1)p_2^{a_2 - 1}, \cdots, (p_r - 1)p_r^{a_r - 1}$ paarsgewijs relatief priem zijn.

B. Toon aan dat 2^k, p^k en $2p^k$, met p priem en $k > 0$ de enige mogelijkheden zijn.

Beschouw eerst het geval $n = 2^k$.

C. Toon aan dat 2^k geen primitieve wortel kan hebben als $k > 2$, en dat 2 en 4 een primitieve wortel hebben.

Stel nu $n = p^k$, en a is een niet-kwadraatrest modulo p.

D. Toon aan dat a een primitieve wortel is modulo p^k.

Stel $n = 2p^k$.

E. Toon aan dat er een oneven niet-kwadraatrest a bestaat modulo p.

F. Toon aan dat a een primitieve wortel is modulo $2p^k$.

<u>Lemma van Gauss</u>

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 $d(x)$ voor een geheel getal x met rest r bij deling door p, zodat $d(x) = r$ als $0 \leq r \leq \frac{p-1}{2}$ en $d(x) = p - r$ als $\frac{p+1}{2} \leq r \leq p-1$. 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.

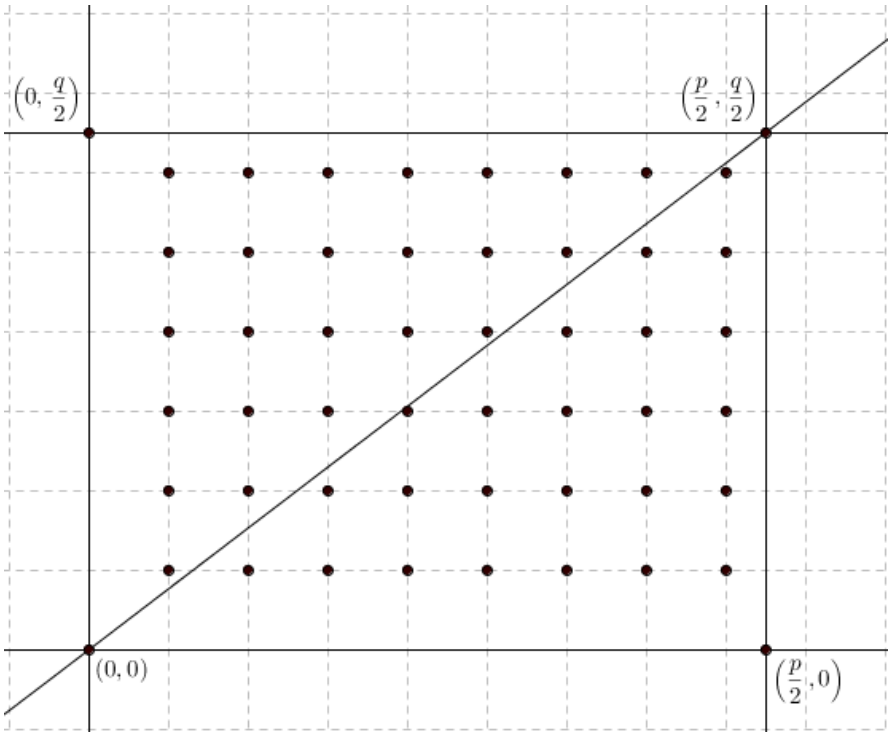
Bewijs dat $\left(\frac{2a}{p}\right) = (-1)^{\alpha(a,p)}$.

<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. 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

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

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. (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.

Stelling

Als een natuurlijk 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.

Kerststelling van Fermat

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

Tweekwadratenstelling

Een getal kan worden geschreven als de som van twee kwadraten als en slechts als alle priemdelers van de vorm $4k+3$ in de priemontbinding van dat getal tot een even macht voorkomen.

Oefening. Bewijs de tweekwadratenstelling.
A. Toon aan dat als een getal kan worden geschreven als de som van twee kwadraten, de priemdelers van de vorm $4k+3$ tot een even macht voorkomen.

Frobeniusgetal

Postulaat van Bertrand
Het postulaat van Bertrand is een vermoeden dat, voor elk natuurlijk getal $n>0$ er een priemgetal p bestaat met $n<p\le 2n$. Dit vermoeden is inmiddels bewezen.

Stelling van Dirichlet

Vermoeden van Catalan

Oefening. (CanMO 1974 vraag 6) Een onuitputbare voorraad van postzegels van 8 cent en van 15 cent zijn voorhanden. Sommige waarden kunnen met deze twee postzegels niet bereikt worden. Wat is het grootste onbereikbare bedrag met deze twee postzegels?

Oefening. (CanMO 1976 vraag 5) Bewijs dat een natuurlijk getal de som is van minimum twee opeenvolgende getallen als en slechts als dat getal geen macht van 2 is.

Oefening. (VWO 1994 vraag 2) Bepaal alle natuurlijke getallen a,b,c met $c\le 94$ zodat $(a+\sqrt{c})^2+(b+\sqrt{c})^2=60+20\sqrt{c}$.

Appendix

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

Een multiplicatieteken doet hetzelfde voor een product. $f(a) \cdot f(a+1) \cdots f(b-1) \cdot f(b)$ noteren we als $\prod_{n=a}^{b} f(n)$.

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 $0 \leq a \leq b$ 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: $(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.

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