Getaltheorie

Onderzoek naar gehele getallen

W=kunde+

Wim Berkelmans

Handleiding voor de docent

Inleiding

Dit werkboek Getaltheorie geeft een inleiding in het onderzoek naar eigenschappen van gehele getallen.
Het is bestemd voor leerlingen van de onderbouw van het VWO.
Het boek staat vol opdrachten en vraagstukken. Door deze opdrachten te maken ontdekken leerlingen elementaire onderdelen van de getaltheorie.
De meeste opdrachten zijn opgezet in de vorm van een onderzoek. Door dit onderzoek uit te voeren ontdekken leerlingen allerlei verrassende eigenschappen van gehele getallen.
In dit boek maken de leerlingen ook kennis met algebraïsche bewijzen.

Hierna volgen antwoorden en uitwerkingen van de opgaven en onderzoeksopdrachten.

Deelbaarheid

quotiënt resultaat van deling
rest wat overblijft na deling

a = qb + r
q: quotiënt
r: rest

deler
5 is een deler van 25
veelvoud
25 is een veelvoud van 5
deelbaar
25 is deelbaar door 5

a|b a is een deler van b

a|b als er een q is zodat a = qb.

Opgave 1

37 = 5x7 + 2
41 = 5x7 + 6
49 = 7x7

Opgave 2

Als de rest die je overhoudt groter of gelijk aan de deler is, dan kun je deze rest nog verder delen, zodat je weer een kleinere rest overhoudt. Dit gaat door totdat je een rest hebt die kleiner is dan de deler.

Opgave 3

a a = 14 en b = 5, q = 2 en r = 4, 14 = 2x5 + 4.
b b = 0, je kunt niet door 0 delen. In de formule krijg je a = r.
c b > a, q = 0 en r = a.

Opgave 4

a 7|154, want 154 = 12 x 7.
b 11|12320, want 12320 = 112 x 11. Je kunt dit snel zien door de cijfers op de even posities te vergelijken met de cijfers op de oneven posities: 1 + 3 + 0 = 2 + 2.

Onderzoek: stelling over deelbaarheid

a d = 7, a = 49 en b = 70 en d|a en d|b.
d|a+b, want 119 = 17 x 7, dus 7|119.

b Het quotiënt als we a+b door d delen is m+n en de rest is dus 0.

Opgave 5

Stelling 2

Bedenk dat d|a betekent dat er een geheel getal n is zo dat a = n x d.
Voor alle gehele getallen a, b, c, d, e en q geldt:
1. a|0, want 0 = 0 x a.
2. 1|a, want a = a x 1.
3. a|a, want a = 1 x a.

4. Als d en a positief zijn en $d|a$ dan $d \leq a$, want er is een n zo dat $a = n \times d$ en omdat a en d positief zijn is $n > 0$. Als $n = 1$ dan $a = d$. Als $n > 1$ dan $a = d + (n - 1)\, d$. Omdat $(n - 1)\, d > 0$ is dan $a > d$.
5. Als $a|b$ en $b|a$ dan $a = b$.
   Immers, als $a|b$ dan is er een n zo dat $a = n \times b$.
   En als $b|a$ dan is er een m zo dat $b = m \times a$.
   Maar dan: $a = n \times b = n \times (m \times a) = (n \times m) \times a$.
   Dan moet $n \times m = 1$, dus $n = m = 1$.
   Dus $a = b$.
6. Als $d|a$ en $d|b$ dan $d|a+b$ en $d|a–b$.
   Als $d|a$ dan is er een n zo dat $a = n \times d$.
   Als $d|b$ dan is er een m zo dat $b = m \times d$.
   Dan $a + b = (n \times m) \times d$, dus $d|a+b$.
   En zo is ook $d|a–b$.
7. Als $d|a$ dan $d|ab$.
   Als $d|a$ dan is er een n zo dat $a = n \times d$.
   Neem nu $m = n \times b$, dan is $m \times d = (n \times b) \times d = a \times b$.
   Dus $d|ab$.
8. Als $d|a$ dan $db|ab$.
   Als $d|a$ dan is er een n zo dat $a = n \times d$.
   Dan is $a \times b = n \times d \times b$, dus $db|ab$.
9. Als $d|a$ en $d|b$ dan $d|ca+eb$.
   Als $d|a$ dan is er een n zo dat $a = n \times d$.
   Dus $ca = c \times n \times d$.
   Als $d|b$ dan is er een m zo dat $b = m \times d$.
   Dus $eb = e \times m \times d$.
   Dus $ca + eb = (cn + em) \times d$.
   Dus $d|ca+eb$.
10. Als $d|a$ en $a|b$ dan $d|b$.
    Als $d|a$ dan is er een n zo dat $a = n \times d$.
    Als $a|b$ dan is er een m zo dat $b = m \times a$.
    Dus $b = m \times a = m \times (n \times d)$.
    Dus $d|b$.
11. Als $d|a$ met quotiënt q dan $q|a$.
    Als $d|a$ met quotiënt q dan is $a = q \times d = d \times q$.
    Dus $q|a$.

Grootste gemene deler

grootste gemene deler
GGD

kleinste gemene veelvoud
KGV

Onderzoek: gemeenschappelijke delers

a De delers van 12 en 20 zijn: 1, 2 en 4.

b ggd(12,30) = 6.

c De GGD is het getal waarmee je teller en noemer van de breuk deelt om de breuk te vereenvoudigen.

d Elk tweetal getallen heeft een gemeenschappelijke deler, namelijk 1.
Dus hebben ze ook een GGD.

Onderzoek: gemeenschappelijke veelvouden

Twee getallen hebben ook *veelvouden* gemeenschappelijk.

a 60, 120, etc.

b Nee

c 60

d We gebruiken het KGV als noemer om de breuken op te tellen. We zetten daarbij elke breuk eerst om naar een breuk met de KGV als noemer.

e Als kgv(a,b) = c dan is er een n en m zodat c = n x a en c = m x b, dus a|c en b|c. (c is een veelvoud van a dus a|c).

Onderzoek: verband tussen GGD en KGV

Er is een verband tussen de GGD en het KGV.
Laten we eerst eens enkele voorbeelden bekijken.

a ggd(4,6) = 2 en kgv(4,6) = 12.
ggd(4,6) x kgv(4,6) = 24 en 4 x 6 = 24.

b ggd(12,15) = 3 en kgv(12,15) = 60.
ggd(12,15) x kgv(12,15) = 180 en 12 x 15 = 180.

c ggd(5,12) = 1 en kgv(5,12) = 60.
ggd(5,12) x kgv(5,12) = 60 en 5 x 12 = 60.

d ggd(a,b) x kgv(a,b) = a x b.

e Nee
ggd(6,12,15) = 3 en kgv(6,12,15) = 60 en 6 x 12 x 15 = 1080.

Opgave 1

ggd(12,24) = 12.
kgv(12,24) = 12 x 24 / ggd(12,24) = 24.
Als ggd(a,b) = 1, dan is kgv(a,b) = a x b.

Priemgetallen

priemgetal
echte deler
relatief priem

Onderzoek: het aantal delers van een getal

b De delers van het getal 2 zijn 1 en 2.

c De delers van 3 zijn 1 en 3, de delers van 4 zijn 1, 2 en 4.

Opgave 1

a De echte delers van 12 zijn 2, 3, 4 en 6.

b De enige echte deler van 49 is 7.

Opgave 2

Als p een priemgetal is, dan heeft p maar twee delers, namelijk 1 en p. 1 is ook een deler van a. De ggd(a,p) is een deler van p, dus is ggd(a,p) = 1 of ggd(a,p) = p.
ggd(a,p) = p als p|a.

Onderzoek: hoe werkt de zeef van Eratosthenes?

d Nee

e Tot en met 7.

f 97

g 25

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

zeef van Eratosthenes

Stelling 1

In het bewijs van *Stelling 1* wordt gebruik gemaakt van een bewijs uit het ongerijmde. Deze bewijstechniek kan mondeling toegelicht worden.

Ontbinden in factoren

Onderzoek: ontbinden in priemfactoren

a 30 = 2 x 3 x 5. In vier factoren kan niet.

b Priemgetallen kun je niet ontbinden in factoren.

c Een product van twee priemgetallen kun je maar op één manier ontbinden in factoren, of een product van meer priemgetallen.

d Priemgetallen hebben geen echte delers.

e $210 = 10 \times 21 = 2 \times 5 \times 3 \times 7$.

f Nee
g $120 = 2 \times 2 \times 2 \times 3 \times 5$
$345 = 3 \times 5 \times 23$
$512 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$
$1000 = 10 \times 10 \times 10$.

Onderzoek: Eerste stelling van Euclides

Laten we weer eens naar het getal 210 kijken. Dit kun je ontbinden als $210 = 10 \times 21$.

a $210 = 2 \times 3 \times 5 \times 7$.

b Ja, $10 = 2 \times 5$ en $21 = 3 \times 7$.

c $525 = 25 \times 21$.
5 is een deler van 525 en ook van 25.

Euclides

Onderzoek: Hilbert getallen

a 1, 5, 9, 13, 17, 21, 25, 29, 33 en 37.

b $9 \times 21 = 189$. Dit is weer een Hilbert getal.
Neem twee Hilbert getallen: a en b.
$a = 4n + 1$ en $b = 4m + 1$.
Dan is $a \times b = 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1$.
Dit is weer een Hilbert getal.

c 5, 9, 13, 17, 21, 29, etc.

d 21, 33, etc.

e $441 = 9 \times 49 = 21 \times 21$
$693 = 9 \times 77 = 21 \times 99$
$1089 = 9 \times 121 = 33 \times 33$.

Bijzondere getallen

Onderzoek: meerlingen

a (3,5), (17,19), (29,31), (41,43), (59,61).

aliquote deel

getal	delers	aantal	som	a.d.
1	1	1	1	0
2	1,2	2	3	1
3	1,3	2	4	1
4	1,2,4	3	7	3
5	1,5	2	6	1
6	1,2,3,6	4	12	6
7	1,7	2	8	1
8	1,2,4,8	4	15	7
9	1,3,9	3	13	4
10	1,2,5,10	4	18	8
11	1,11	2	12	1
12	1,2,3,4,6,12	6	28	16
13	1,13	2	14	1
14	1,2,7,14	4	24	10
15	1,3,5,15	4	24	9
16	1,2,4,8,16	5	31	15
17	1,17	2	18	1
18	1,2,3,6,18	5	30	12
19	1,19	2	20	1
20	1,2,4,5,20	5	32	12
21	1,3,7,21	4	32	11
22	1,2,11,22	4	36	14
23	1,23	2	24	1
24	1,2,3,4,6, 8,12,24	8	60	36
25	1,5,25	3	31	6
26	1,2,13,26	4	42	16
27	1,3,9,27	4	40	13
28	1,2,4,7,14,28	6	56	28

perfect getal
multiperfect getal

b (5,7,11), (7,11,13), (11,13,17), (13,17,19), (17,19,23), (37,41,43), (41,43,47), (67,71,73), (97,101,103), (101,103,107).

c (3,5,7)

d Als er nog een tweede priemdrieling is waarbij het verschil tussen het hoogste en het laagste getal vier is, zou één van die drie getallen deelbaar zijn door 3, dus niet priem.

e (3,5,7,11), (5,7,11,13), (11,13,17,19), (101,103,107,109), (191,193,197,199), (821,823,827,829), (1481,1483,1487,1489), (1871,1873,1877,1879), (2081,2083,2087,2089), (3251,3253,3257,3259), (3461,3463,3467,3469).

Onderzoek: delers

a Zie tabel.

b Zie tabel.

c Zie tabel.

d Zie tabel.

e Twee.

f De som van de delers is bij een priemgetal 1 meer dan het priemgetal zelf.

Onderzoek: perfecte getallen

a Ja.

b 6 en 28.

c De delers van 120 zijn 1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 60 en 120. De som is 360. Dus 120 is een multiperfect getal. Het aliquote deel van 120 is 240. Dus 120 is geen perfect getal.

d Een perfect getal is gelijk aan zijn aliquote deel. Als je daar het getal zelf bij optelt krijg je de som. Deze som is twee keer het getal zelf. Dus is het getal een deler van deze som en dus een multiperfect getal. Dus is een perfect getal ook een multiperfect getal.

e De delers van 220 zijn 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110 en 220. Het aliquote deel is dus 284.
De delers van 284 zijn 1, 2, 4, 71, 142 en 284. Het aliquote deel is dus 220.

Dus 220 en 284 zijn bevriende getallen.

Onderzoek: aliquote rij

a De aliquote rij van het getal 15 is 15,9,4,3,1,0.

b 16,15,9,4,3,1,0
20,12,16,15,9,4,3,1,0
36,55,17,1,0

c 138, 150, 222, 234, 312, 528, 960, 2088, 3762, 5598, 6570, 10746, 13254, 13830, 19434, 20886, 21606, 25098, 26742, 26754, 40446, 63234, 77406, 110754, 171486, 253458, 295740, 647748, 1077612, 1467588, 1956812, 2109796, 1889486, 953914, 668966, 353578, 176792, 254128, 308832, 502104, 753216, 1240176, 2422288, 2697920, 3727264, 3655076, 2760844, 2100740, 2310856, 2455544, 3212776, 3751064, 3282196, 2723020, 3035684, 2299240, 2988440, 5297320, 8325080, 11222920, 15359480, 19199440, 28875608, 25266172, 19406148, 26552604, 40541052, 54202884, 72270540, 147793668, 228408732, 348957876, 508132204, 404465636, 303708376, 290504024, 312058216, 294959384, 290622016, 286081174, 151737434, 75868720, 108199856, 101437396, 76247552, 76099654, 42387146, 21679318, 12752594, 7278382, 3660794, 1855066, 927536, 932464, 1013592, 1546008, 2425752, 5084088, 8436192, 13709064, 20563656, 33082104, 57142536, 99483384, 245978376, 487384824, 745600776, 1118401224, 1677601896, 2538372504, 4119772776, 8030724504, 14097017496, 21148436904, 40381357656, 60572036544, 100039354704, 179931895322, 94685963278, 51399021218, 28358080762, 18046051430, 17396081338, 8698040672, 8426226964, 6319670230, 5422685354, 3217383766, 1739126474, 996366646, 636221402, 318217798, 195756362, 101900794, 54202694, 49799866, 24930374, 17971642, 11130830, 8904682, 4913018, 3126502, 1574810, 1473382, 736694, 541162, 312470, 249994, 127286, 69898, 34952, 34708, 26038, 13994, 7000, 11720, 14740, 19532, 16588, 18692, 14026, 7016, 6154, 3674, 2374, 1190, 1402, 704, 820, 944, 916, 694, 350, 394, 200, 265, 59, 1, 0

Onderzoek: hoe vind je perfecte getallen?

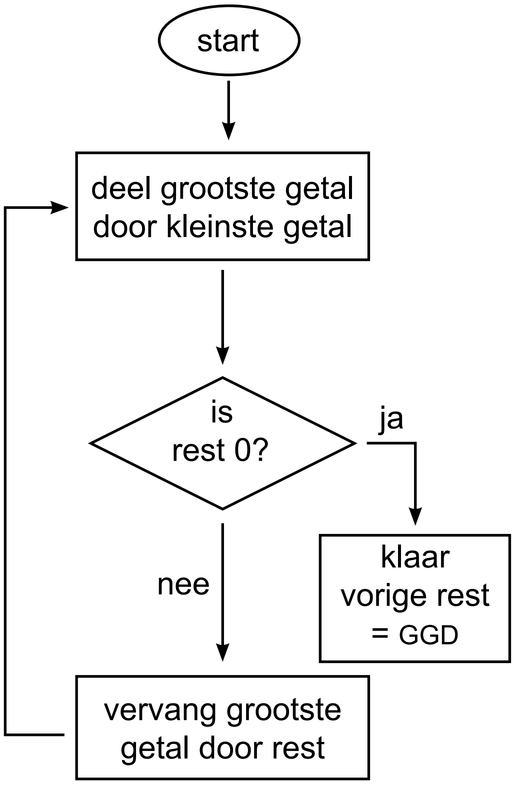
a 1, 1 + 2 = 3

b 3 x 2 = 6

c 6 is het eerste perfecte getal.

d 1 + 2 + 4 = 7 en 7 x 4 = 28 en 28 is een perfect getal.
1 + 2 + 4 + 8 = 15 en 15 is geen priemgetal.
1 + 2 + 4 + 8 + 16 = 31 en 31 x 16 = 496 en 496 is een perfect getal.

Algoritme van Euclides



1 + 2 + 4 + 8 + 16 + 32 + 64 = 127 en 127 x 64 = 8128 en 8128 is een perfect getal.

Onderzoek: Euclides-getal

a $E_1 = 3$, $E_2 = 7$, $E_3 = 31$, $E_4 = 211$, $E_5 = 2311$, $E_6 = 30031$ en $E_7 = 510511$.

b De eerste vijf: 3, 7, 31, 211 en 2311.

Onderzoek: Algoritme van Euclides

a 360 = 2 x 2 x 2 x 3 x 3 x 5

b 84 = 2 x 2 x 3 x 7

c 2, 2 en 3

d 2 x 2 x 3 = 12

e 360 = 30 x 12 en 84 = 7 x 12 en 7 en 30 hebben geen priemfactoren gemeen, dus ggd(360,84) = 12.

f ggd(340569,12056) = 1

g Voer dit algoritme uit met de getallen 360 en 84:
360 = 4 x 84 + 24
84 = 3 x 24 + 12
24 = 2 x 12
Dus ggd(360,84) = 12.

h ggd(360,84) is een deler van 360 en een deler van 84, dus moet het ook een deler zijn van het verschil van 360 en 84 en zo ook van de rest van 360/84. Dus is ggd(360,84) = ggd(84,r_1). Zo kun je doorgaan. Formeel kun je dit met volledige inductie bewijzen.

Opgave 3

340569 = 28 x 12056 + 3001
12056 = 4 x 3001 + 52
3001 = 57 x 52 + 37
52 = 1 x 37 + 15
37 = 2 x 15 + 7
15 = 2 x 7 + 1
Dus ggd(340569,12056) = 1.

4598750834503 = 9317 x 493548576 + 358751911
493548576 = 1 x 358751911 + 134796665
358751911 = 2 x 134796665 + 89158581
134796665 = 1 x 89158581 + 45638084
89158581 = 1 x 45638084 + 43520497

45638084 = 1 x 43520497 + 2117587
43520497 = 20 x 2117587 + 1168757
2117587 = 1 x 1168757 + 948830
1168757 = 1 x 948830 + 219927
948830 = 4 x 219927 + 69122
219927 = 3 x 69122 + 12561
69122 = 5 x 12561 + 6317
12561 = 1 x 6317 + 6244
6317 = 1 x 6244 + 73
6244 = 85 x 73 + 39
73 = 1 x 39 + 34
39 = 1 x 34 + 5
34 = 6 x 5 + 4
5 = 1 x 4 + 1
Dus ggd(493548576,4598750834503) = 1.
Dit blijkt toch nog een hoop werk te zijn.
Beter zou zijn te berekenen: ggd(493548576,4598901054561)
4598901054561 = 9318 x 493548576 + 15423393
493548576 = 32 x 15423393
Dus ggd(493548576,4598901054561) = 15423393.
Dit is in een latere druk aangepast.

Onderzoek: kleinste gemene veelvoud

a 512 = 1 x 360 + 152
360 = 2 x 152 + 56
152 = 2 x 56 + 40
56 = 1 x 40 + 16
40 = 2 x 16 + 8
16 = 2 x 8
Dus ggd(360,512) = 8.

b kgv(360,512) = 360 x 512 / 8 = 23040.

c 360 = 2x2x2 x 3x3 x 5
512 = 2x2x2x2x2x2x2x2x2
ggd(360,512) = 8 = 2x2x2
kgv(360,512) = 23040 = 2x2x2x2x2x2x2x2x2x 3x3 x 5.

d De priemfactoren van de GGD en het KGV zijn precies de priemfactoren van 360 en 512.

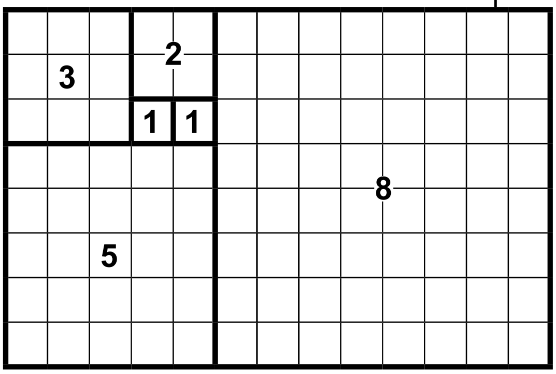
e 60 = 2x2 x 3 x 5
70 = 2 x 5 x 7
ggd(60,70) = 10 = 2 x 5
kgv(60,70) = 420 = 2x2 x 3 x 5 x 7.

f De priemfactoren van de GGD en het KGV zijn precies de priemfactoren van 60 en 70.

g De priemfactoren van de GGD en het KGV van twee getallen zijn precies de priemfactoren van de twee getallen.

h Kies telkens een tweetal getallen en toets de algemene regel.

Fibonacci



rij van Fibonacci

1
1
2
3
5
8
13
21

Opgave 1

2 5 8 11 14 17 20 23 ... telkens 3 erbij optellen.
2 4 6 12 14 28 30 60 62 124 126 ... telkens verdubbelen en dan 2 erbij optellen.
1 4 2 5 3 6 4 7 5 8 6 9 7 ... telkens 3 erbij optellen en dan 2 ervan aftrekken.
1 1 2 3 5 8 13 21 34 55 ... telkens de laatste twee getallen bij elkaar optellen. Dit is de *rij van Fibonacci*.

Onderzoek: rij van Fibonacci

a $f_1 = 1$
$f_2 = 1$
$f_3 = 2$
$f_4 = 3$
$f_5 = 5$
$f_6 = 8$
$f_7 = 13$
$f_8 = 21$
$f_9 = 34$
$f_{10} = 55$
$f_{11} = 89$
$f_{12} = 144$
$f_{13} = 233$
$f_{14} = 377$
$f_{15} = 610$

Algemeen kunnen we dan zeggen: f_n = het n^{de} getal in de rij.
Je kunt dan een algemene formule opschrijven om de getallen in de rij te berekenen: $f_{n+2} = f_{n+1} + ...$

b $f_{n+2} = f_{n+1} + f_n$.

c $ggd(f_3,f_4) = ggd(2,3) = 1$ en
$ggd(f_7,f_8) = ggd(13,21) = 1$.

d $ggd(f_n,f_{n+1}) = 1$

e Als twee opeenvolgende Fibonacci-getallen, f_n en f_{n+1} een echte deler hebben, dan is die deler ook deler van het daaropvolgende Fibonacci-getal f_{n+2}, want $f_{n+2} = f_{n+1} + f_n$.

f Als $ggd(a,b) = 1$ dan $ggd(a,a+b) = 1$ en $ggd(b,a+b) = 1$. Want als a en $a+b$ een gemeenschappelijke echte deler hebben, dan is dat ook een deler van b.

g $ggd(f_2,f_3) = 1$.

$ggd(f_3,f_4) = 1$, enzovoort. Wiskundig correct doe je dit met volledige inductie.

h Bereken:

$gdd(f_3,f_6) = 2$	$ggd(3,6) = 3$	$f_{ggd(3,6)} = f_3 = 2$
$gdd(f_5,f_{15}) = 5$	$ggd(5,15) = 5$	$f_{ggd(5,15)} = f_5 = 5$
$gdd(f_4,f_{12}) = 3$	$ggd(4,12) = 4$	$f_{ggd(4,12)} = f_4 = 3$
$gdd(f_6,f_9) = 2$	$ggd(6,9) = 3$	$f_{ggd(6,9)} = f_3 = 2$

i $ggd(f_m,f_n) = f_{ggd(m,n)}$

Opgave 2: huizen bouwen

a Bij drie huizen zijn er drie mogelijkheden:
vrijstaand - vrijstaand - vrijstaand
vrijstaand - twee onder één kap
twee onder één kap - vrijstaand.

b Bij vier huizen zijn er vijf mogelijkheden:
vrijstaand - vrijstaand - vrijstaand - vrijstaand
vrijstaand - vrijstaand - twee onder één kap
vrijstaand - twee onder één kap - vrijstaand
twee onder één kap - vrijstaand - vrijstaand
twee onder één kap - twee onder één kap.
Bij vijf huizen zijn er acht mogelijkheden en bij zes huizen dertien.

c Telkens als er een huis bij komt, kun je dat als vrijstaand huis vooraan toevoegen aan de combinaties die als laatste had, of je voegt een twee onder één kap toe vooraan bij de combinaties die je de keer daarvoor had. Dan heb je alle mogelijkheden, want een combinatie begint ofwel met een vrijstaand huis plus alle mogelijke combinaties van de laatste keer, ofwel het begint met een twee onder één kap met alle mogelijke combinaties van de één na laatste keer.

Opgave 3

Voorbeelden zijn: bloemen, zaadjes van een zonnebloem, dennenappel, broccoli, romanesco bloemkool.

woord	lengte	a's	b's
a	1	1	0
ab	2	1	1
aba	3	2	1
abaab	5	3	2
abaababa	8	5	3
abaababaabaab	13	8	5
abaababaabaababaababa	21	13	8

Onderzoek: Fibonacci-woorden

c Er komen in de woorden wel eens twee a's achter elkaar voor, maar geen twee b's.

d Nee

e Een b ontstaat door een a te vervangen door ab. Om twee b's te krijgen moet je twee a's vervangen, maar dan krijg je abab, dus ook dan heb je geen twee b's na elkaar.

f Nee

g Een a krijg uit de vervanging van a door ab en uit de vervanging van b door a. Om aaa te krijgen moeten de eerste twee a's komen uit de vervanging van b door a (want als ze voortkomen uit de vervanging van een a moet er een b achter staan). Maar je hebt nooit twee b's achter elkaar dus kun je ook geen twee a's achter elkaar krijgen die voortkomen uit de vervanging van twee b's.

h Bijvoorbeeld dood, pap, mam, sas, negen, redder, radar, meetsysteem, parterretrap.

j Alleen aa, ab en ba komen voor in een Fibonacci-woord. Dus drie verschillende woorddelen van lengte twee.

k Er komen vier verschillende woorddelen van lengte drie voor: aba, aab, bab en baa.

l Er komen vijf verschillende woorddelen van lengte vier voor: aaba, abaa, baab, abab en baba.

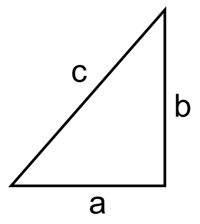
Laatste Stelling van Fermat

Onderzoek: Pythagoreïsche drietallen

a $3^2 + 4^2 = 5^2$
$5^2 + 12^2 = 13^2$
$7^2 + 24^2 = 25^2$
$8^2 + 15^2 = 17^2$
$9^2 + 40^2 = 41^2$
$11^2 + 60^2 = 61^2$
$12^2 + 35^2 = 37^2$

Stelling van Pythagoras

$a^2 + b^2 = c^2$



b Vermenigvuldig elk van de drie getallen met hetzelfde gehele getal.

c $1^2 = 1$
$2^2 = 4$
$3^2 = 9$
$4^2 = 16$
$5^2 = 25$
$6^2 = 36$
$7^2 = 49$
$8^2 = 64$
$9^2 = 81$
$10^2 = 100$

d 1 4 9 16 25 36 49 64 81 100
3 5 7 9 11 13 15 17 19

1 4 9 16 25 ...
3 5 7 9 ...

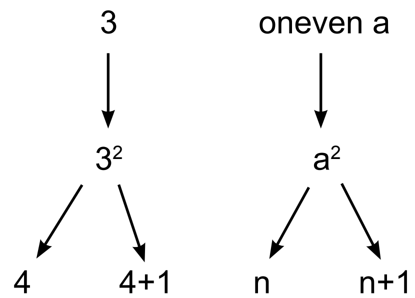
e De verschillen zijn de oneven getallen.

f $(n+1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n + 1 = (n+1) + n$.

g Uit het voorgaande blijkt dat het verschil van de kwadraten van twee opvolgende getallen altijd de som is van deze twee getallen. Dat is dus altijd een even plus een oneven getal. En dat is altijd oneven.

h $5^2 = 25$ is oneven.
Het kwadraat van een oneven getal is oneven.

i 25 staat niet in het rijtje verschillen hierboven, maar als je nog even doorgaat kom je 25 wel tegen. $13^2 - 12^2 = 13 + 12 = 25$. Op deze manier kom je elk oneven getal een keer tegen.



j 5^2 is het verschil tussen 13^2 en 12^2.

k Het Pythagoreïsch drietal is dus (5,12,13).

l Bij $a = 9$ is $n = 40$ en $n+1 = 41$.
$\text{ggd}(a,n,n+1) = 1$.

natuurlijk getal

m Voor een willekeurige n is $ggd(n,n+1) = 1$.
En dus is $ggd(a,n,n+1) = 1$.
Dus het drietal $a,n,n+1$ is altijd een primitief Pythagoreïsch drietal.

o $a = 9 - 4 = 5$
$c = 9 + 4 = 13$.

p $c^2 - a^2 = 13^2 - 5^2 = 169 - 25 = 144 = 12^2 = b^2$,
dus $a^2 + b^2 = c^2$.

q Neem bijvoorbeeld $p = 4$ en $q = 7$.
Dan $a = q^2 - p^2 = 49 - 16 = 33$ en $c = q^2 + p^2 = 49 + 16 = 65$.
Dan $c^2 - a^2 = (q^2 + p^2)^2 - (q^2 - p^2)^2 = 4p^2q^2 = 3136$.
$b = 2pq = 56$.

r
1. Neem twee getallen p en q met $q > p$.
2. Neem $a = q^2 - p^2$
   Neem $b = 2pq$
   Neem $c = q^2 + p^2$
3. Controleer het resultaat.

s $a = q^2 - p^2 = 8^2 - 5^2 = 64 - 25 = 39$
$b = 2pq = 80$
$c = q^2 + p^2 = 64 + 25 = 89$
$a^2 + b^2 = 1521 + 6400 = 7921 = 89^2$.

t $a = q^2 - p^2 = 3^2 - 1^2 = 9 - 1 = 8$
$b = 2pq = 6$
$c = q^2 + p^2 = 9 + 1 = 10$
$a^2 + b^2 = 64 + 36 = 100 = 10^2$.
(6,8,10) is geen primitief Pythagoreïsch drietal.

u Als $q^2 - 1$ een priemgetal is, dan is $a = q^2 - 1$ dus een priemgetal. a is dan een oneven getal. $c - a = q^2 + 1 - (q^2 - 1) = 2$, dus c is ook oneven. En omdat $b = 2q$ even is moet dus $ggd(a,b,c) = 1$.

Andrew Wiles

Pierre de Fermat

Modulo-rekenen

Onderzoek: klokrekenen

a 3 + 10 = 13, dus de klok geeft 1 uur aan.

b Bij 19:00 uur geeft de klok 7 uur aan.
10 + 35 = 45 uur. De klok geeft dan 9 uur aan.

c 7, 19 en 31 leveren allemaal 7 uur op.

d a = 12 x n + b, waarbij n een positief geheel getal is.

e b is de rest bij deling van a door 12.

Opgave 1

Reduceer:
1. 120 = 0 (mod 3)
2. 3001 = 1 (mod 3)
3. 1290 = 10 (mod 16)

Onderzoek: restklasse

$$15 \longrightarrow 3 \pmod{12}$$

a b = 0 in a ≡ b (mod 12) als a een veelvoud van 12 is.

b Bij a ≡ 4 (mod 12) is a een veelvoud van 12 plus 4.

c Er zijn oneindig veel verschillende oplossingen voor a.

d Er zijn 4 verschillende restklassen (mod 4) en 100 restklassen (mod 100).

$$a \equiv b \pmod{12}$$
$$a \equiv b \pmod{m}$$

Onderzoek: modulo-rekenen

a Dan is het 11 uur.

b 9 (mod 12) + 18 (mod 12) ≡ 27 (mod 12) ≡ 3 (mod 12)
7 (mod 5) + 51 (mod 5) ≡ 58 (mod 5) ≡ 3 (mod 5)
347 (mod 7) + 988 (mod 7) ≡ 1335 (mod 7) ≡ 5 (mod 7) of
347 (mod 7) + 988 (mod 7) ≡ 4 (mod 7) + 1 (mod 7) ≡ 5 (mod 7).

c Bereken (de gereduceerde vorm van):
5435 (mod 3) + 98204 (mod 3) ≡ 2 (mod 3) + 2 (mod 3) ≡
1 (mod 3).
92345 (mod 7) + 30940 (mod 7) ≡ 1 (mod 7) + 0 (mod 7) ≡
1 (mod 7).

d $11 \times 12 \pmod 5 \equiv 132 \pmod 5 \equiv 2 \pmod 5$.
$11 \pmod 5 \equiv 1 \pmod 5$ en $12 \pmod 5 \equiv 2 \pmod 5$ dus het resultaat is hetzelfde.

e Als $a \equiv b \pmod m$ en $c \equiv d \pmod m$ dan is
$a + c \equiv b + d \pmod m$, want $a = b + n_1 \times m$ en $c = d + n_2 \times m$, dus
$a + c = b + d + n_1 \times m + n_2 \times m = b + d + (n_1 + n_2) \times m$.

f Als $a \equiv b \pmod m$ en $c \equiv d \pmod m$ dan is
$ac \equiv bd \pmod m$, want $a = b + n_1m$ en $c = d + n_2m$, dus
$ac = bd + bn_2m + dn_1m + n_1n_2m^2 = bd + (bn_2 + dn_1 + n_1n_2m)m$.

g Ja, zoals hierboven.

h $34 \times 36 \pmod 5 \equiv 4 \pmod 5 \times 1 \pmod 5 \equiv 4 \pmod 5$
$34^2 \times 34^2 \pmod 5 \equiv 1 \pmod 5 \times 1 \pmod 5 \equiv 1 \pmod 5$
$34^2 \times 36^2 \pmod 5 \equiv 1 \pmod 5 \times 1 \pmod 5 \equiv 1 \pmod 5$
$539 \times 662 \pmod{10} \equiv 9 \pmod{10} \times 2 \pmod{10} \equiv 8 \pmod{10}$
$3333 \times 3334 \pmod 3 \equiv 0 \pmod 3 \times 1 \pmod 3 \equiv 0 \pmod 3$
$3334 \times 3335 \pmod 3 \equiv 1 \pmod 3 \times 2 \pmod 3 \equiv 2 \pmod 3$
$7 \times 13 \times 58 \times 836 \times 123456789 \pmod{13} \equiv 0 \pmod{13}$, want 13 is een van de factoren.
$17^{21} \pmod{17} \equiv 0 \pmod{17}$.

i Als n even is dan is
$n^2 \pmod 4 \equiv (2m)^2 \pmod 4 \equiv 4m^2 \pmod 4 \equiv 0 \pmod 4$.
Als n oneven is dan is
$n^2 \pmod 4 \equiv (2m + 1)^2 \pmod 4 \equiv 4m^2 + 4m + 1 \pmod 4 \equiv$
$1 \pmod 4$.

Onderzoek: grote machten

a $2^2 \pmod{13} \equiv 4 \pmod{13}$
$2^4 \pmod{13} \equiv 4 \times 4 \pmod{13} \equiv 3 \pmod{13}$
$2^8 \pmod{13} \equiv 3 \times 3 \pmod{13} \equiv 9 \pmod{13}$
$2^{16} \pmod{13} \equiv 9 \times 9 \pmod{13} \equiv 3 \pmod{13}$
$2^{32} \pmod{13} \equiv 3 \times 3 \pmod{13} \equiv 9 \pmod{13}$.

b $49 = 32 + 16 + 1 = 2^5 + 2^4 + 2^0$.
$2^{49} \pmod{13} \equiv 2^{32}2^{16}2^1 \pmod{13} \equiv 9 \times 3 \times 2 \pmod{13} \equiv$
$54 \pmod{13} \equiv 2 \pmod{13}$.

c $52 = 32 + 16 + 4$
$2^2 \pmod 7 \equiv 4 \pmod 7$
$2^4 \pmod 7 \equiv 4 \times 4 \pmod 7 \equiv 2 \pmod 7$
$2^8 \pmod 7 \equiv 2 \times 2 \pmod 7 \equiv 4 \pmod 7$
$2^{16} \pmod 7 \equiv 4 \times 4 \pmod 7 \equiv 2 \pmod 7$
$2^{32} \pmod 7 \equiv 2 \times 2 \pmod 7 \equiv 4 \pmod 7$
$3^{52} \pmod 7 \equiv 2^{32}2^{16}2^4 \pmod 7 \equiv 4 \times 2 \times 2 \pmod 7 \equiv$
$16 \pmod 7 \equiv 2 \pmod 7$.

Onderzoek: modulaire inverse

a De inverse van 3 (mod 7) is 5 (mod 7) want
3 (mod 7) x 5 (mod 7) ≡ 1 (mod 7).

b De inverse van 5 (mod 7) is weer 3 (mod 7).

c Nee, je kunt niet bij elk getal een (modulaire) inverse vinden.
Bijvoorbeeld 2 (mod 6) x a (mod 6) zit in een even restklasse.
Dus kan 1 (mod 6) nooit in deze restklasse zitten.

Je kunt bewijzen dat een getal a (mod m) een inverse heeft dan en slechts dan als ggd(a,m) = 1.

d 15 (mod 17) heeft een inverse, want ggd(15,17) = 1.
15 (mod 17) x 8 (mod 17) ≡ 1 (mod 17),
dus 8 (mod 17) is de inverse van 15 (mod 17).

e 15 (mod 21) heeft geen inverse, want ggd(15,21) = 3.

RSA

F E R M A T

↓ omzetten in cijfers

06 05

↓ vercijferen

06 10

↓ ontcijferen

06 05

↓

F E

publieke sleutel = (s,m) = (11,35)

$y = x^{s} \pmod m$

$x = 6$ ↓ $s = 11$, $m = 35$

$y = 6^{11} \pmod{35}$

Onderzoek: RSA

a

F	E	R	M	A	T
06	05	18	13	01	20

b $m = 5 \times 7 = 35$

c $n = (5 - 1) \times (7 - 1) = 4 \times 6 = 24$

d Neem bijvoorbeeld $s = 11$.

e $6^2 \pmod{35} = 1 \pmod{35}$ dus $y = 6^{11} \pmod{35} = 6$. Dus $y = 06$.
En het volgende getal: $5^{11} \pmod{35} = 10$

F	E	R	M	A	T
06	05	18	13	01	20
06	10	02	27	01	20

f $r = 11$, want $s \times 11 = 11 \times 11 = 121 = 1 \pmod{24}$.
Dus de geheime sleutel is 11 en 35. Hier is toevallig $r = s$, maar dit is doorgaans niet het geval.

g

06	10	02	27	01	20
06	05	18	13	01	20
F	E	R	M	A	T

Opgave 1

R	S	A		I	S		S	L	I	M		B	E	D	A	C	H	T
18	19	01	27	09	19	27	19	12	09	13	27	02	05	04	01	03	08	20

publieke sleutel: s =
m =
geheime sleutel: r =
m =