

# Schakelcursus Wiskunde 2006

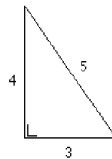
## Deel 1: wat getaltheorie.

### 1 Inleiding.

In de Informatica, en wel in het bijzonder in de complexiteitstheorie en in de telecommunicatie (bv. encryptie), wordt veelvuldig gebruik gemaakt van methoden uit de getaltheorie.

We zullen hier in kort bestek een aantal nuttige elementaire stellingen bespreken. Aanname is, dat je (op papier) kunt optellen, aftrekken, vermenigvuldigen en delen en weet dat getallen op een unieke manier zijn te ontbinden in *priemgetallen*.

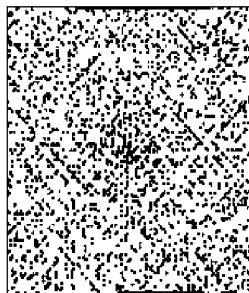
Getaltheorie is een meer dan 2500 jaar oud onderwerp uit de wiskunde met vele gemakkelijk formuleerbare, maar soms moeilijk op te lossen vragen zoals: hoeveel priemgetallen zijn er? Zijn er méér rechthoekige driehoeken met gehele zijden dan de hier getekende?



Moeilijker: kun je elk getal schrijven als som van 9 derdemachten?

Het vak is daarom zowel eerbiedwaardig als - voor vele mensen - leuk en fascinerend. En, zoals gezegd: van nut binnen de computerwetenschap.

De onderwerpen uit onderstaande stof komen uit sommige van mijn colleges. Als voorkennis veronderstel ik minstens dat je kunt vermenigvuldigen en delen en weet wat een "ontbinding in priemgetallen" is.



De priemgetallen, getekend op een spiraal. Vele ervan komen te liggen op rechte lijnen.

## Notaties

$\mathbb{N} = \{1, 2, 3, \dots\}$	$\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$	<i>Natuurlijke getallen</i>
$\mathbb{Z} = \{\dots -3, -2, 0, 1, 2, 3, \dots\}$		<i>Gehele getallen</i>
$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\}$	Breuken	<i>Rationale getallen</i>
$\mathbb{R}$ oneindige decimale breuken als 3, 1415...		<i>Reële getallen</i>
$\mathbb{N}_0^2 = \{(i, j) \mid i \text{ en } j \text{ uit } \mathbb{N}_0\}$		<i>Roostergetallen</i>

## 2 "Modulo"rekenen.

Deze belangrijke techniek komt steeds weer terug: in security, complexiteitstheorie maar ook bijvoorbeeld bij algorithmen met veeltermen.

We werken nu steeds met *gehele* getallen, dus  $\{\dots -2, -1, 0, 1, 2, \dots\}$ . De verzameling van de gehele getallen noemen we  $\mathbb{Z}$ .

$a|b$  wil zeggen  $a$  deelt  $b$ , dus  $b$  is van de vorm  $a \cdot c$ . Zo geldt  $3|6$ ,  $5|5$ ,  $7|0$ , maar **niet**  $0|7$  en **niet**  $5|12$ .

Laat eerst  $n = 12$ . Elk getal is deelbaar met rest door 12;  $38 = 3 \cdot 12 + 2$ ;  $11 = 0 \cdot 12 + 11$ ;  $-53 = (-5) \cdot 12 + 7$ ;  $72 = 6 \cdot 12 + 0$ . We zorgen steeds dat de rest in het bereik  $\{0, 1, 2, \dots, 11\}$  ligt. Op de klok kun je alle uren reduceren tussen 0 en 11 uur, zo noem je  $22u30$  ook  $10u30$  ('s avonds).

Als  $a = 12 \cdot v + r$  met  $r$  de rest, dan noemen we  $r$  ook:  $a \bmod 12$ . Dus  $38 \bmod 12 = 2$ ,  $11 \bmod 12 = 11$ ,  $-53 \bmod 12 = 7$ ,  $72 \bmod 12 = 0$ .

Als  $a \bmod 12 = b \bmod 12$  dan schrijven we ook  $a = b \bmod 12$ . Dit is hetzelfde als  $a - b$  is deelbaar door 12; oftewel  $12|(a-b)$ .

Er gelden de regeltjes: als  $a = b \bmod 12$  en  $c = d \bmod 12$  dan  $a \pm c = b \pm d \bmod 12$  en  $ac = bd \bmod 12$ . Hierdoor treden er altijd *dezelfde uitkomsten mod 12* op, of je nu rekent met bepaalde getallen  $\{a, b, c, \dots\}$  of met getallen die een 12-voud verschoven zijn, vb.  $\{a+36, b-12, c+1296, \dots\}$ . In de wiskunde kun je dit elegant formuleren door verzamelingen van de vorm  $\underline{a} = \{a + 12v \mid v \text{ geheel}\}$  te beschouwen. Dit heet de *restklasse mod 12* van  $a$ .

Hoeveel mogelijke restklassen zijn er? Net zoveel als er mogelijke resten zijn; dus je hebt 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11. Je kunt rekenen met restklassen via het volgende recept:  $\underline{a} \cdot \underline{b}$  bereken je door in  $\underline{a}$  een getal  $x$  te pakken en in  $\underline{b}$  een getal  $y$  en  $z = xy \bmod 12$  te bepalen; dan is  $\underline{a} \cdot \underline{b} = \underline{z}$ . Volgens bovenstaande rekenregeltjes hangt de uitkomst namelijk niet af van welke  $x$  en  $y$  je kiest! Net zo bij de optelling.

Wiskundigen maken vaak nieuwe getallen als verzamelingen; zo kun je de breuk  $t/n$  ook zien als verzameling  $\{(a, b) \mid a \text{ en } b \text{ geheel en } a \cdot n = b \cdot t\}$ . Dit is de manier om de rationale getallen op te bouwen vanuit de gehele getallen!

Gewoonlijk laten we de onderstreping van de restklassen weer weg, als er geen verwarring dreigt.

Je kunt nu dus rekenen met de getallen 0 t/m 11 door steeds elke uitkomst door zijn rest  $\text{mod } 12$  te vervangen (“reduceren mod 12”). Je kunt optellen en vermenigvuldigen, maar niet delen! Uit  $a.m = b.m \text{ mod } 12$  volgt niet  $a = b \text{ mod } 12$ ; zo is bv.  $2.3 = 6.3 \text{ mod } 12$ .

## 2.1 Een toepassing.

Dat er getallen zijn in  $\mathbb{R}$  die niet in  $\mathbb{Q}$  zitten weet men al 2500 jaar (sinds Pythagoras). Een voorbeeld is  $\sqrt{2}$ : die zit in  $\mathbb{R}$  maar niet in  $\mathbb{Q}$ .

**Bewijs:** Laat  $\frac{a}{b}$  een breuk zijn met  $\text{ggd}(a, b) = 1$  en  $\frac{a^2}{b^2} = 2$ . Dan  $a^2 = 2b^2$  dus  $a = 0 \text{ mod } 2$ . Stel  $a = 2a_0$ . Dan  $4a_0^2 = 2b^2$  dus  $2a_0^2 = b^2$ . Maar dan net zo  $b = 2b_0$ ; dus  $\text{ggd}(a, b)$  is minstens 2: tegenspraak.

De Grieken konden dezelfde ”mod” redenering toepassen t/m  $\sqrt{17}$ ; natuurlijk werkt hij algemeen.

$\sqrt{2}$  is de oplossing van een veeltermvergelijking met coëfficiënten uit  $\mathbb{Z}$ ; te weten van

$$X^2 - 2 = 0$$

Een getal dat voldoet aan een veeltermvergelijking over  $\mathbb{Z}$  heet **algebraïsch**.

Een diep resultaat dat pas in 1881 is bewezen door Lindemann luidt:

- Het getal  $\pi (= 3, 141592 \dots)$  is **niet** algebraïsch!  
Je kunt het informeel ook zó zeggen:
- Alle uitdrukkingen zoals  $3\pi^5 - 41\pi^4 + 7\pi - 81$  verschillen!  
(Waarom is dat hetzelfde? Denk hierover na!)

Je ziet, dat de indeling in  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$  en  $\mathbb{R}$  nog wel wat valt te verfijnen!

### Opgaven.

1. Je kunt het bovenstaande natuurlijk doen voor alle  $n \neq 0$ , niet alleen voor  $n = 12$ . Hoeveel restklassen zijn er dan?

2. a. Laat zien dat als  $n$  een priemgetal is, uit  $a.m = b.m \text{ mod } n$  volgt  $a = b \text{ mod } n$  (tenzij  $m = 0 \text{ mod } n$ ). Doe het evt. eerst voor  $n = 7$ .  
b. Stel  $d$  is de ggd van  $m$  en  $n$ . Laat nu ook zien dat uit  $a.m = b.m \text{ mod } n$  volgt  $a = b \text{ mod } n/d$ .

3. De “negenproef”. Vroeger controleerden boekhouders lange optel-/vermenigvuldigings-berekeningen wel als volgt: neem van elk voorkomend getal de som der cijfers (sdc) (als die boven de 10 ligt, doe je het nog eens, enz. tot je onder de 10 zit).

Doe de berekening na met deze sdc's (je mag tussendoor steeds wanneer je zin hebt de uitkomsten vervangen door de sdc). De uitkomst moet gelijk zijn aan de som der cijfers van het oorspronkelijke resultaat; als dat niet zo is dan zit er ergens een fout in de berekening.

**Voorbeeld:**  $86 + 57 = 143$ .

86 heeft als sdc  $8 + 6 = 14$  en die:  $1 + 4 = 5$ . 57 heeft als sdc 3;  $3 + 5 = 8$ . De sdc van 143 is eveneens 8.

- a. Ga zelf na hoe dit werkt bij de berekening 15.17.
- b. Als de negenproef klopt, is de oorspronkelijke berekening dan altijd juist?
- c. Het geheim: ga na dat de sdc van  $n$  gelijk is aan  $n \bmod 9$ . Doe dat door  $n$  10-talig op te schrijven, dus zeg als  $a + b.10 + c.100 + \dots$

4. Het is nu 10 uur. Hoe laat is het over 87 uur?

5. Beschouw een functie van de getallen  $\{0, 1, \dots, n-1\} \bmod n$ ; b.v.  $f(a) = a^2 \bmod n$ . Maak een rijtje:  $a_1 = a$ ;  $a_2 = f(a)$ ,  $\dots$ ,  $a_{i+1} = f(a_i)$  (alle  $i$ ). Bewijs dat  $a_1, a_2, \dots$  *periodiek* is: vanaf zeker punt geldt  $a_i = a_{i+p}$  ( $p$  de vaste periode)! Voorbeeld:  $f(a) = 2a \bmod 7$ ; rijtje (vanaf  $a = 2$ ): 2, 4, 1, 2, 4, 1,  $\dots$ ; periode 3. *Hint*: laatjesprincipe!

6. Stop de paren  $\langle t_i \bmod n, t_{i+1} \bmod n \rangle$  in laatjes en bewijs dat  $t_i \bmod n$  periodiek is. Hier zijn de getallen  $t_i$  aantallen konijntjes uit het probleem van Fibonacci:  $t_1 = 1$ ,  $t_2 = 1$ ,  $t_{i+2} = t_{i+1} + t_i$  ( $i \geq 1$ ).

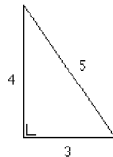
- Wanneer is het aantal konijntjes  $t_i$  deelbaar door 13?
- (Moeilijk): kun je een formule verzinnen voor  $t_i \bmod 11$ ?

7. Als een getal een 8 voud  $+7$  is, dan is het géén som van 3 kwadraten! (Reken  $\bmod 8$ ).

8. Marian verwacht 6 gasten. Ze verdeelt de pinda's over 6 schaaltes; dit komt uit. Dan hoort ze dat er nog een extra gast komt; ze herverdeelt over 7 schaaltes en houdt 2 pinda's over. Hoeveel pinda's had ze?

9. Kan een kwadraat eindigen op 79?

10. Als  $x^2 + y^2 = z^2$  (bv.  $3^2 + 4^2 = 5^2$ )



dan is  $x$  of  $y$  door 3 deelbaar, en  $x, y$  of  $z$  door 5.

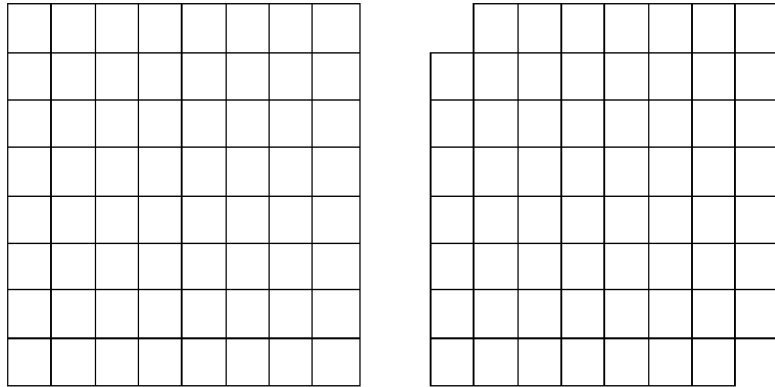
11. Fermat dacht dat  $w^{2^n} + 1$  altijd priem was. Dit klopt voor  $n = 0, 1, 2, 3, 4$  maar Euler vond  $2^{2^5} + 1 = 641.6700417$ . In feite zijn er niet meer van deze

Fermat-se priemgetallen bekend: misschien is  $2^{2^{20}} + 1$  er een (van 315653 cijfers ...). Verifieer dat  $2^{2^5} + 1$  door 641 deelbaar is!

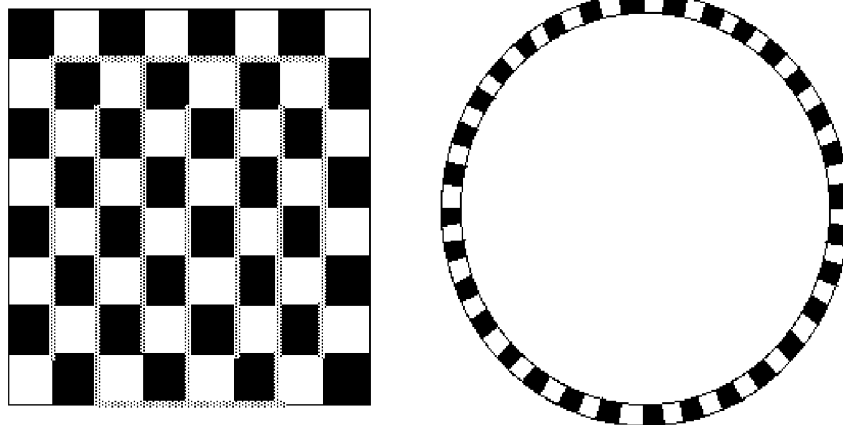
12.  $11\ 111\ 111\ 111\ 111\ 111\ 111\ 111 = \frac{10^{23}-1}{9}$  is priem! Laat zien dat zo'n ééntjes-priemgetal een priem aantal ééntjes bezit!

## 2.2 Als oefening en ter illustratie: legpuzzelproblemen.

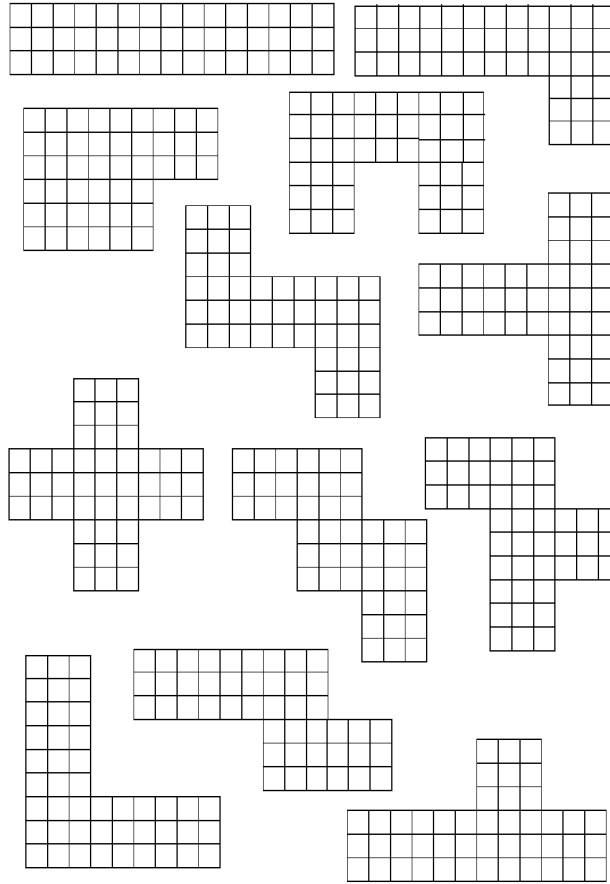
**Opgave:** je kunt natuurlijk een  $8 \times 8$  schaakbord opvullen met  $1 \times 2$  en  $2 \times 1$  dominostenen. Kun je het ook nog als je twee tegenoverliggende hoekpunten weglaat?



**Stelling van Gomory:** als je van een  $8 \times 8$  bord twee velden weglaat, dan kun je de figuur met domino's volleggen precies dan als de verdwenen velden zwart en wit waren!



**Opgave:** Precies één van de volgende borden is niet overdekbaar met paardensprongen. Welk?



Om iets meer te kunnen zeggen over dit soort puzzels is er een methode bedacht door een zekere meneer Kelly. Om voldoende ruimte te hebben verdelen we het hele vlak maar in vierkantjes, die we coördinaten  $(i, j)$  geven met  $i$  en  $j$  geheel:

		(2,2)	
(1,0)			
(0,0)	(0,1)	(0,2)	

Inplaats van de hokjes zwart of wit te kleuren geven we elk hokje een aparte "kleur": hokje  $(i, j)$  krijgt kleur  $x^i y^j$  met  $x$  en  $y$  twee onbekenden (n.b.  $x^0 =$

$y^0 = 1$ ).

Bovenstaande rechthoek heeft dan "somkleur"  $(1+x+x^2+x^3) + (y+xy+x^2y+x^3y) + (y^2+xy^2+x^2y^2+x^3y^2) = (1+x+x^2+x^3) \cdot (1+y+y^2) = \frac{x^4-1}{x-1} \cdot \frac{y^3-1}{y-1}$ . Net zo heeft een  $a$  bij  $b$  rechthoek  $V$  met linksonder de oorsprong  $(0,0)$  somkleur:

$$KL(V) = \frac{x^b - 1}{x - 1} \cdot \frac{y^a - 1}{y - 1}.$$

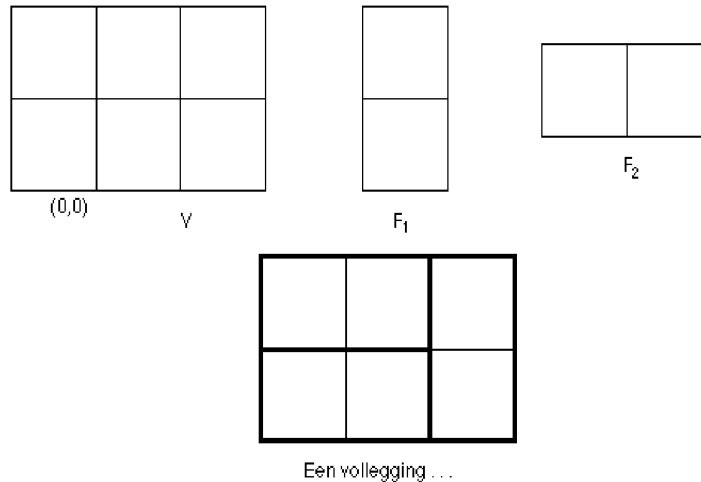
De somkleur van een rechthoek met linksonder  $(i, j)$  is uiteraard  $x^i \cdot y^j$  keer zo groot.

We gaan nu proberen een rechthoek  $V$  vol te leggen met dominostenen van grootte 1 bij  $d$ . Deze kunnen liggen of rechtopstaan. De liggende steen  $F_1$  heeft zoals we zagen somkleur  $(x^d-1)/(x-1)$ ; de staande  $F_2$  somkleur  $(y^d-1)/(y-1)$ .

Stel, we leggen  $V$  vol met domino's;  $F_1$  met zijn linkerkant op  $(a_1, b_1), (a_2, b_2), \dots$  en  $F_2$  met zijn onderkant op  $(c_1, d_1), (c_2, d_2), \dots$  dan geldt voor de somkleur:

$$KL(V) = (x^{a_1}y^{b_1} + \dots) \cdot KL(F_1) + (x^{c_1}y^{d_1} + \dots) \cdot KL(F_2);$$

noem dat  $f_1(x, y) \cdot KL(F_1) + f_2(x, y) \cdot KL(F_2)$ . Voorbeeld:

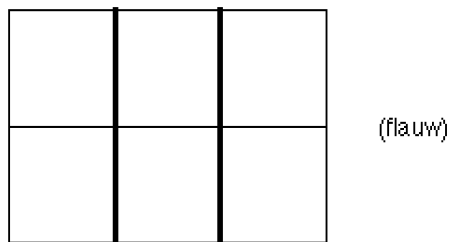


Bij deze vollegging is  $KL(V) = (1+y)KL(F_1) + (x^2)KL(F_2)$ .

Met behulp van deze vergelijkingen kunnen we nu volleggingen bestuderen. Zo kun je onmiddellijk inzien dat het verminkte bord van Gomory niet vol te leggen valt!

**Opgave:** zie dit in!

Een *flauwe vulling* van  $V$  is er een met alle steentjes evenwijdig. Dan deelt  $d$  dus de zijde  $a$  of de zijde  $b$



Als  $d$  een priemgetal is volgt direct: als  $V$  vulbaar is dan is  $V$  flauw vulbaar. Maar bv. voor  $d = 6$  is dat helemaal niet duidelijk: je zou misschien een  $8$  bij  $15$  rechthoek kunnen volleggen. De verrassende stelling (van de Bruijn) zegt nu: *dat kan niet!* Concreter:

**Stelling.** Als  $V$  vollegbaar is, dan ook flauw vollegbaar! (En natuurlijk omgekeerd.)

We zullen dit nu, via *mod rekenen* inzien voor een eenvoudig geval (het algemene is niet veel moeilijker te bewijzen, maar vergeet het gebruik van zgn. *complexe getallen*).

### Puzzel-voorbeeld

Neem eens een  $16 \times 21$  bord. De oppervlakte is deelbaar door  $6$ , dus zou je het wellicht met  $1 \times 6$  (en  $6 \times 1$ ) dominostenen kunnen overdekken.

Volgens de stelling van de Bruijn komt dit puzzeltje echter niet uit: want duidelijk is dat er geen flauwe vulling bestaat! (Een kartonnen uitvoering is een aardig verjaarscadeautje ....)

Laten we in dit geval even nagaan dat de stelling klopt. De volleg-voorwaarde voor een  $a \times b$  rechthoek met  $1 \times 6$  en  $6 \times 1$  domino's is:

$$\frac{x^a - 1}{x - 1} \cdot \frac{y^b - 1}{y - 1} = f(x, y) \cdot \frac{x^6 - 1}{x - 1} + g(x, y) \cdot \frac{y^6 - 1}{y - 1}.$$

We kiezen nu  $x = y = 3$ , dus:

$$\frac{3^a - 1}{3 - 1} \cdot \frac{3^b - 1}{3 - 1} = n \cdot \frac{3^6 - 1}{3 - 1} + m \cdot \frac{3^6 - 1}{3 - 1} \text{ met } n = f(3, 3), m = g(3, 3) \text{ geheel,}$$

oftewel:

$$(3^a - 1)(3^b - 1) = (3^6 - 1) \cdot k \text{ met } k \text{ geheel.}$$

Neem dit nu *mod 7*. Dan is  $3^6 - 1 = 9^3 - 1 = 2^3 - 1 = 7 = 0 \text{ mod } 7$  dus  $7$  is een deler van  $3^a - 1$  of van  $3^b - 1$ .

Wanneer deelt  $7$  een getal  $3^k - 1$ ? We maken een tabelletje:

$k$	0	1	2	3	4	5	6	7	8	9	10	11	12	...
$3^k \text{ mod } 7$	1	3	2	6	4	5	1	3	2	6	4	5	1	...
$3^k - 1 \text{ mod } 7$	0	2	1	5	3	4	0	2	1	5	3	4	0	...

Blijkbaar is dat alleen zo voor  $k = 0, 6, 12, \dots$  dus  $k = 0 \pmod 6$ . Maar dan volgt uit  $3^a - 1 = 0 \pmod 7$  dat  $a = 0 \pmod 6$ ; of uit  $3^b - 1 = \pmod 7$  dat  $b = 0 \pmod 6$ .

$a$  en  $b$  waren de zijden van de rechthoek; minstens één ervan is dus deelbaar door 6: de rechthoek is flauw vulbaar!

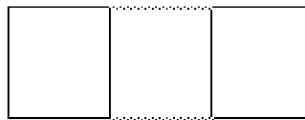
En uw geacht familielid is waarschijnlijk volgend jaar nog bezig, zijn  $16 \times 21$  bord vol te leggen ....

**Opgave.** De volgende puzzels zijn onmogelijk:

1. Een  $6 \times 6 \times 6$ -kubus opvullen met  $1 \times 2 \times 4$ -blokjes. (Hint: verdeel in  $2 \times 2 \times 2$  kubusjes.)

2. Een  $25 \times 25$  "dambord" volleggen met  $2 \times 2$  en  $3 \times 3$  stenen (kleur de rijen om-en-om zwart en wit).

3. Een rechthoek is desd. vollegbaar met "gap-o-mino's"



als één der zijden lengte deelbaar door 4 heeft! (Hint: reken mod 4.)

### 3 Een kleinigheid over getalstelsels.

Gewoonlijk schrijf je een getal 10-tallig: 7893 wil zeggen  $700 + 800 + 90 + 3 = 7 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10 + 3$ .

Dit kun je i.p.v. met 10 ook doen met een ander "grondtal", bv.  $1 \cdot 3^8 + 1 \cdot 3^6 + 2 \cdot 3^5 + 1 \cdot 3^4 + 1 \cdot 3^3 + 1 \cdot 3^2 + 0 \cdot 3 + 0 \cdot 3^0 = 7893$  d.w.z. in het *drietallig stelsel* schrijf je 7893 als: 11211100. De voorkomende cijfers hierin zijn 0,1 en 2 (net zoals je in het 10-tallig stelsel 0 t/m 9 gebruikt).

Het *unaire systeem* wordt soms voor theoretische doeleinden gebruikt; verder is het knap waardeloos. 23 schrijf je daarin als 11111 11111 11111 11111 111.

Het *tweetailig stelsel* of *binair* notatie wordt gebruikt in computers. Voorbeeld:

$$53 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 \cdot 1 \text{ dus, binair: } 110101.$$

De nullen en eentjes hierin heten de *bits* van 53.

Als  $2^{k-1} \leq n \leq 2^k - 1$  dan telt  $n$   $k$  bits.  $k$  is dus

$$\lceil \log_2 n \rceil + 1,$$

voor wie het precies wil weten ( $\lceil \dots \rceil$  wil zeggen: naar beneden afronden).

Ook *teksten* worden (via de zgn ASCII codering) weergegeven als rijen bits.

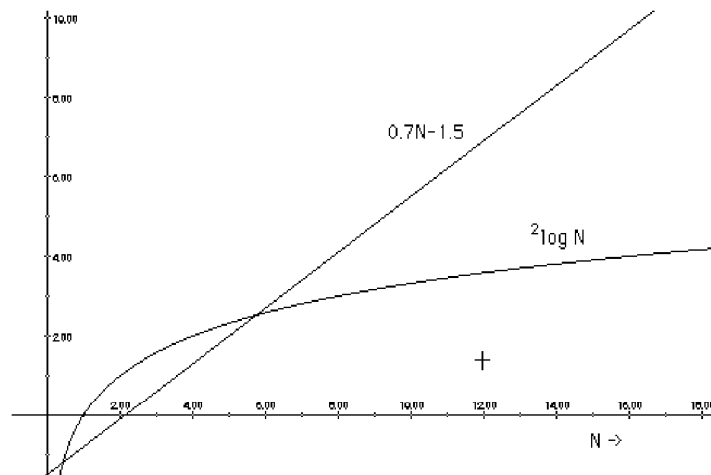
**Nog enige feiten:**

1. Het geval  $N$  telt ongeveer  ${}^2\log N$  bits in het tweetallig stelsel (exact: entier  $({}^2\log N) + 1$ )

**Voorbeeld:**  $1605 = 11001000101$ , binair geschreven.

2.  ${}^2\log N$  is een functie die voor grote  $N$  veel kleiner is dan functies van de vorm  $A \cdot N + B$ .

**Voorbeeld:**



**3.1 Toepassing: “Indiaas” machtsverheffen.**

Stel je wilt een getal tot een grote macht verheffen; zeg  $3^{153}$ . Dit soort problemen komt tegenwoordig heel vaak voor in de zgn. cryptografie; dat is de manier waarop banken hun gegevens coderen om ze veilig over te sturen.

Als je het doet volgens de methode  $3 \times 3 = 9$ ,  $3 \times 9 = 27$ ,  $3 \times 27 = 81$  etc. dan kost het je 152 vermenigvuldigoperaties (ga dat na!).

Met behulp van het tweetallig stelsel kan het echter in véél minder!

De exponent 153 ziet er, tweetallig, uit als 10011001. We gaan nu “bitjes knabbelen”:

$$3^{10011001} = 3 \cdot 3^{10011000} = 3 \cdot 3^{1001100} \cdot 3^{1001100}$$

(2 vermenigvuldigingen; rechter ééntje van de exponent verdwijnt)

$$3^{1001100} = 3^{100110} \cdot 3^{100110}$$

(1 vermenigvuldiging; rechter nulletje verdwijnt) etc.

We komen zo uit op slechts 10 vermenigvuldigingen! Deze truc was 2000 jaar geleden in India al bekend.

Merk op dat we hebben “geabstraheerd” van het langer worden van de gebruikte getallen; ook dat kan extra tijd vergen.

**Opgaven.**

1. Ga na hoe het bovenstaande vermenigvuldigschema voor  $3^{153}$  eruit ziet als je de exponenten gewoon tientallig schrijft. Eenvoudig, niet?
2. Hoe verhouden zich de lengten (als strings) van de tientallige representatie en de binaire representatie van  $n$ ?

## 4 Kettingbreuken!

Bij het maken van tandwielsystemen (bv. klokken) sta je vaak voor het probleem, ingewikkelde verhoudingen over te brengen door een stelsel tandwielen. Laten we eens kijken naar een *planetarium*, een astronomisch uurwerk dat de bewegingen van de planeten om de zon weergeeft. Beroemde planetaria zijn ontworpen door Christiaan Huygens en Eise Eisinga.

Zoals ongetwijfeld iedereen uit z'n hoofd weet, verhouden de omlooptijden van Mars en van de Aarde zich als  $\frac{686,980}{365,256} = \frac{171745}{91314} = 1,8808178373524$ . Niemand zal het in z'n hoofd halen, om tandwielen te gaan vijlen met 171745 en 91314 tandjes!

Wat je wilt hebben, zijn twee kleinere tandwielen van grootte  $a$  en  $b$  zodat  $\frac{a}{b}$  een zeer goede benadering is van  $\frac{171745}{91314}$ . De manier waarop men dit aanpakt staat bekend als de

**kettingbreukontwikkeling.**

Voor de eenvoud een kleiner voorbeeld. Als we de breuk  $\frac{689}{610}$  hebben, dan kun je die vereenvoudigen als:  $\frac{13.53}{13.47} = \frac{53}{47}$ . Dit komt omdat teller en noemer de ggd 13 hebben. Maar wat te doen bij bv.  $\frac{689}{610}$ ? Welnu:

$$\begin{aligned} \text{Schrijf: } \frac{689}{610} &= 1 + \frac{79}{610} = 1 + \frac{1}{\frac{610}{79}} = 1 + \frac{1}{7 + \frac{57}{79}} = 1 + \frac{1}{7 + \frac{1}{1 + \frac{22}{57}}} = \dots = 1 + \frac{1}{7 + \frac{1}{1 + \frac{22}{57}}} = \\ &\dots = 1 + \frac{1}{7 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{4}}}}}}} \end{aligned}$$

Om redenen die te maken hebben met het zenuwstelsel van de drukker, schrijft men dit meestal als  $[1, 7, 1, 2, 1, 1, 2, 4] \dots$

Deze *kettingbreuk* nu kun je gebruiken om  $\frac{689}{610}$  te benaderen door hem op diverse plaatsen af te kappen: bv.:  $1; 1 + \frac{1}{7} = \frac{8}{7} + \frac{1}{7 + \frac{1}{1}} = \frac{9}{8}; 1 + \frac{1}{7 + \frac{1}{1 + \frac{1}{2}}} = \frac{26}{23}$  enzovoorts.

Dit leidt tot een tabelletje.

$i$	$i^e$ benaderingsbreuk	
0	1	$\approx 1,000$
1	8/7	
2	9/8	
3	26/23	$\approx 1,130$
4	35/31	
5	61/54	$\approx 1,1296$
6	157/139	
7	689/610	$\approx 1,129508$

Zoals je ziet, is 61/54 een hele schappelijke benadering; in een planetarium heb je dan twee tandwielen die  $10\times$  zo klein zijn!

Men kan aantonen dat dit soort benaderingen *optimaal* zijn (“beste benaderingen”) als je een grens stelt aan het aantal tandjes (d.w.z. aan teller en noemer).

Als je op bovenstaande wijze te werk gaat met de breuk  $\frac{3141592653}{100000000}$  dan vind je de bekende benaderingen voor  $\pi$ :  $\frac{22}{7}$  en  $\frac{355}{113}$  (goed in 6 decimalen!).

#### 4.1 Het algoritme van Euclides.

Bovenstaande kettingbreukontwikkeling wordt vaak iets anders opgeschreven als:

$$\begin{aligned}
 689 &= 1 \cdot 610 + 79 \\
 610 &= 7 \cdot 79 + 57 \\
 79 &= 1 \cdot 57 + 22 \\
 57 &= 2 \cdot 22 + 13 \\
 22 &= 1 \cdot 13 + 9 \\
 13 &= 1 \cdot 9 + 4 \\
 9 &= 2 \cdot 4 + 1 \\
 4 &= 4 \cdot 1 + 0
 \end{aligned}$$

Denk erover na waarom dit op hetzelfde neerkomt. Je kunt dit voor elk tweetal positieve gehele getallen doen. De algemene vorm is een rij delingen met rest:

$$\begin{aligned}
 a &= a_0 b + r_1 & 0 \leq r_1 < b \\
 b &= a_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\
 r_1 &= a_2 r_2 + r_3 & 0 \leq r_3 < r_2 \\
 \dots & & \dots & \\
 r_{n-2} &= a_{n-1} r_{n-1} + r_n \\
 r_{n-1} &= a_n r_n + 0
 \end{aligned}$$

Merk nu op: als  $d$  de *ggd* is van  $a$  en  $b$ , dan zit  $d$  in elke  $r_i$  dus uiteindelijk in  $r_n$ . Omgekeerd zit  $r_n$  als factor in  $r_{n-1}$ ,  $r_{n-2}$  en uiteindelijk in  $b$  en  $a$ . Dus,  $r_n = d = \text{ggd}(a, b)$ . Bovenstaand rekenschema heet het

#### Algoritme van Euclides

om de  $ggd$  te bepalen en het was tweeduizend jaar lang "het" (enige) algoritme. In het college T2 (Inl. Complexiteitstheorie) zullen we dit algoritme nader analyseren.

## 4.2 Inverteren mod $n$ .

We beschouwen opnieuw de getallen  $mod\ n$ :  $\{1, 2, \dots, n-1\}$ . We zagen eerder dat we binnen dit kleine domein kunnen optellen, aftrekken en vermenigvuldigen, maar dat delen niet altijd ging. Wat zou je moeten verstaan onder  $\frac{1}{3} mod\ 17$  (ook wel genoteerd als  $3^{-1} mod\ 17$ )?

Net als in het veel grotere domein van de reële getallen is dat de oplossing  $x$  van de vergelijking  $3x = 1$  - hier dus geschreven:  $3x = 1 mod\ 17$ . Teruggrijpend op de gehele getallen komt dit neer op het vinden van twee getallen  $x$  en  $y$  met  $3x = 1 - 17y$ , oftewel  $3x + 17y = 1$ . Merk op dat  $ggd(3, 17) = 1$ ; als deze  $ggd$  groter was dan kon dit nooit! Bv,  $3x + 6y = 1$  kan niet; en 3 heeft dus zeker geen inverse  $mod\ 6$ .

Het algoritme van Euclides is uitermate geschikt voor het inverteren!

**Stelling** Laten  $a$  en  $b \in \mathbb{Z}$ , beide ongelijk 0; en zij  $d = ggd(a, b)$ . De vergelijking  $ax + by = d$  heeft altijd een oplossing  $(x, y)$ , en  $a$  heeft een inverse  $a^{-1} mod\ n$  (nl.  $x$ ) d.e.s.d. als  $d = 1$ .

**Bewijs:** Dit gaat middels het

*Uitgebreide algoritme van Euclides ("Extended Euclid(es)"):*

Hierin houd je bij twee getallen  $x_i$  en  $y_i$  zodanig dat  $r_i = x_i a + y_i b$ . Zo is (zie in het algemene schema hierboven)  $x_1 = 1, y_1 = -a_0$  (Vraag: wat zijn  $x_2$  en  $y_2$ ? Vul in  $r_1 = x_1 a + y_1 b$  in de tweede regel!) Uiteindelijk vinden we  $d = r_n = x_n a + y_n b$ ; we hebben de  $ggd$  van  $a$  en  $b$  geschreven als  $d = x_n a + y_n b$ . Is  $d = 1$  dan volgt nog:  $x_n a = 1 mod\ b$ :  $a$  is inverteerbaar  $mod\ b$  en de inverse  $x_n$  is te vinden via Extended Euclides.

## 4.3 Het verband met kettingbreuken (facultatief).

Kettingbreuken hebben enkele wonderlijke eigenschappen en spelen een belangrijke rol in de getaltheorie. Laten we eerst eens de zaken iets algemener opschrijven. Stel  $X$  is een reëel getal dat je in een kettingbreuk wilt ontwikkelen. Dat gaat zó:

$$X = a_0 + \frac{1}{X_1} \quad \text{met} \quad a_0 = \lfloor X \rfloor,$$

het grootste gehele getal  $\leq X$ . Het restje (dat  $< 1$  is!) stellen we  $\frac{1}{X_1}$  met  $X_1$  dus  $> 1$ , en daarmee gaan we net zo verder:  $X_1 = a_1 + \frac{1}{X_2}$  met  $a_1 = \lfloor X_1 \rfloor$ . Zo vind je  $X = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots}}}$ .

De benaderingsbreuken noemen we  $\frac{P_i}{Q_i}$ . Dus

$$\frac{P_0}{Q_0} = \frac{a_0}{1}; \quad \frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}; \quad \frac{P_2}{Q_2} = \frac{a_0 + a_2 + a_0 a_1 a_2}{a_1 a_2 + 1}$$

enz. (zie dit in!). Met een *sprongbewijs* (volledige inductie) kun je nagaan dat

$$P_n = a_n P_{n-1} + P_{n-2}$$

$$Q_n = a_n Q_{n-1} + Q_{n-2}$$

en je mag  $n$  vanaf 0 laten lopen als je nog definieert:

$$P_{-2} = 0 \quad P_{-1} = 1$$

$$Q_{-2} = 1 \quad Q_{-1} = 0.$$

Een wonderlijke eigenschap van benaderingsbreuken is:

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^{n+1} \quad (n \geq -1)$$

Immers:  $P_n Q_{n-1} - Q_n P_{n-1} = (a_n P_{n-1} + P_{n-2}) Q_{n-1} - (a_n Q_{n-1} + Q_{n-2}) P_{n-1} = -(P_{n-1} Q_{n-2} - Q_{n-1} P_{n-2})$  (enz ...!)

Hieruit kun je een aantal dingen aflezen.

1.  $\left| \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} \right| = \frac{1}{Q_n Q_{n-1}}$  dus  $\frac{P_n}{Q_n}$  en  $\frac{P_{n-1}}{Q_{n-1}}$  liggen “erg dicht” bij elkaar!
2.  $P_n$  en  $Q_n$  hebben  $\text{ggd} = 1$ , immers de  $\text{ggd}$  deelt  $(-1)^{n+1}$ !

Hoe bepaal je de  $\text{ggd}$  van  $a$  en  $b$  ( $a > b$ ) met kettingbreuken? Merk eerst op dat de kettingbreuk van  $\frac{a}{b}$  *stopt*: immers schrijf  $a = bv + r$ ,  $0 \leq r < b$  (stel  $r \neq 0$ ) dan  $\frac{a}{b} = v + \frac{r}{b} = v + \frac{1}{\frac{b}{r}}$  dus  $a_0 = v$  en je gaat voort met een breuk  $\frac{b}{r}$  waarvan de noemer  $< b$  is. Dit “dalen der noemers” moet stoppen!

$$\text{Dus } \frac{a}{b} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}$$

We mogen aannemen dat  $a_n > 1$  is, want  $\frac{\ddots}{a_{n-1} + \frac{1}{\ddots}} = \frac{\ddots}{a_{n-1} + 1}$ . Dan is  $\frac{P_n}{Q_n} = \frac{a}{b}$

dus  $\begin{cases} a = dP_n \\ b = dQ_n \end{cases}$  met  $d = \text{ggd}(a, b)$ , want  $P_n$  en  $Q_n$  hebben  $\text{ggd} = 1$ !

Maar dan is  $P_n Q_{n-1} - Q_n P_{n-1} = \frac{a}{d} Q_{n-1} - \frac{b}{d} P_{n-1} = (-1)^{n+1}$  zodat

$$d = a \cdot (-1)^{n+1} Q_{n-1} - b \cdot (-1)^{n+1} P_{n-1}$$

De truc is dus: kap de kettingbreuk van  $\frac{a}{b}$  af op de *voorlaatste* plaats. Je vindt tevens een oplossing van de vergelijking

$$ax + by = d$$

in gehele getallen! In feite komt e.e.a. weer neer op "Extended Euclides". Over het oplossen van vergelijkingen in gehele getallen (zgn. "Diophantische vergelijkingen") zijn vele boeken vol te schrijven.

### Opgaven.

1. *Ter info:* Met kettingbreuken kun je ook de *vergelijking van Pell* oplossen:

$$x^2 - Dy^2 = 1.$$

De kettingbreuk van  $\sqrt{D}$  is nl. altijd periodiek, en je vindt oplossingen  $x = P_i$ ,  $y = Q_i$  (*einde info*).

*Eigenlijke opgave:* bewijs  $\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, 1, 1, 1, 4, \dots]$  en vind (een) oplossing(en) van  $x^2 - 7y^2 = 1$ . Als je dit ook kunt voor  $x^2 - 919y^2 = 1$  ben je knap; de kleinste oplossingen hebben meer dan 60 cijfers!

2. Vind de *ggd* van 48 en 63 en los op  $48x + 63y = \text{ggd}(48, 63)$ .

3. Laat  $a^2 - 7b^2 = c^2 - 7d^2 = 1$ . Schrijf  $(a + b\sqrt{7})(c + d\sqrt{7}) = e + f\sqrt{7}$ . *Bewijs:*  $e^2 - 7f^2 = 1$ .

## 5 Priemgetallen.

We behandelen hier enkele belangrijke stellingen, van nut in, bijvoorbeeld, security en de theorie van error correcting codes. Ook is dit hoofdstukje een verdere oefening in het modulorekenen.

- Priemgetallen zijn de natuurlijke getallen  $p > 1$  zonder delers  $\neq 1, p$ .
- Elk geheel getal is eenduidig ontbindbaar in priemgetallen.
- Er zijn er oneindig veel (Euclides)! Want als er maar  $k$  waren (zeg  $p_1 = 2$ ,  $p_2 = 3$ ,  $p_3, \dots, p_k$ ) dan heeft  $p_1 p_2 \dots p_k + 1$  een grotere priemdeeler; tegenspraak!
- Snel een lijst maken van de eerste priemgetallen: de zeef van Eratosthenes. Schrap uit  $\mathbb{N}$  alle 2-vouden  $> 2$  en omcirkel 2; dan alle 3-vouden  $> 3$  en omcirkel 3 etc. (pak steeds het eerste, nog niet geschrapte of omcirkelde getal  $k$ ; omcirkel het en schrap alle  $k$ -vouden  $> k$ ). Over blijven de omcirkelde priemgetallen:

1 (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) ...

Er zijn nog steeds mensen bezig dit te versnellen (op de computer)!

### Interessante eigenschappen

1. Hoeveel priemgetallen  $< N$  zijn er? Antwoord: ongeveer  $\frac{N}{\epsilon \log N}$ . Dit is de beroemde *priemgetalstelling*. Over de grootte van de afwijking van deze schatting bestaan nog allerlei onbewezen vermoedens. In de praktijk gebruikt men dit resultaat bij het zoeken naar zeer grote priemgetallen t.b.v. de cryptografie.

2. Beschouw eens  $\{1, 2, \dots, p-1\}$ , de getallen  $\text{mod } p$  behalve 0. Pak een  $a \text{ mod } p$ ,  $a \neq 0$ . Bewering:

$$\{a.1, a.2, \dots, a.(p-1)\} = \{1, 2, \dots, p-1\} \pmod{p}.$$

Immers: de linkerverzameling zit in de rechter en heeft gelijke grootte, want uit  $ax = ay \text{ mod } p$  volgt  $a(x-y) = 0 \text{ mod } p$  dus  $p$  deelt  $a$  (onjuist) of  $p$  deelt  $x-y$ ;  $x = y \text{ mod } p$ .

Dan is ook  $(a.1) \cdot (a.2) \cdot \dots \cdot (a.(p-1)) = 1 \cdot 2 \cdot \dots \cdot p-1 \text{ mod } p$  dus  $a^{p-1}(p-1)! = (p-1)!$ ;  $a^{p-1} = 1 \text{ mod } p$ .

$$\text{Als } a \neq 0 \text{ mod } p \text{ dan } a^{p-1} = 1 \text{ mod } p$$

Dit heet de *Kleine Stelling van Fermat* (de "Grote" is onlangs ook bewezen!) Zo is  $7^{18} - 1$  deelbaar door 19.

Een gevolg is: de vergelijking

$$ax = 1 \text{ mod } p$$

is altijd oplosbaar: neem maar  $x = a^{p-2}$  (dit is ook weer een mooie eigenschap van priemgetallen; zo is  $3x = 1 \text{ mod } 6$  *niet* oplosbaar!)

**3. Opgave.** Noem  $a^{-1}$  de oplossing van  $ax = 1 \text{ mod } p$ . Wanneer is  $a^{-1} = a$ ? Schrap in  $1 \cdot 2 \cdot 3 \cdot \dots \cdot p-1 \text{ mod } p$  paren  $a$  en  $a^{-1}$  weg en bewijs aldus de

**Stelling van Wilson:**

$$(p-1)! + 1 \text{ is deelbaar door } p \text{ als } p \text{ priem.}$$

Ga ook na dat dit nooit zo is als  $p$  niet priem is! We hebben zo dus een criterium om uit te maken of  $n$  een priemgetal is: kijk of  $\frac{(n-1)!+1}{n}$  geheel is. Dit kost echter wel veel rekenwerk!

4. Vermoeden van Goldbach: elk even getal  $\geq 4$  is de som van 2 priemgetallen. Onbewezen! (Opm. Vinogradov bewees in 1937: elk groot, oneven getal is som van 3 priemgetallen!)

5. Tweelingpriemgetalvermoeden: er zijn oneindig veel paren priemgetallen  $p$ ,  $p+2$  (zoals 17 en 19, of 59 en 61). Onbewezen!

6. Wanneer is de *binom*  $\binom{p}{a}$  door  $p$  deelbaar? Als  $a \neq 0 \pmod p$  dan altijd, want  $\binom{p}{a} = \frac{p!}{a!(p-a)!}$ . Gevolg:  $(x + y)^p = x^p + y^p \pmod p$  - handig!

7. Er zijn willekeurig grote “gaten” in  $\mathbb{N}$  zonder priemgetallen erin .....

8. Als  $p$  een *4voud* + 1 is, dan is  $p$  te schrijven als  $a^2 + b^2$ .

**Opgave.** Als  $p$  een *4voud* + 3 is, dan niet! Waarom?

9.  $223092870n + 2236133941$  is priem voor  $n = 0, 1, \dots, 15$ .

10 Elk getal  $n \in \mathbb{N}$  is te schrijven als

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

(voor een bewijs - m.b.v. priemgetallen - zie de Appendix).

11.  $n^2 + n + 41$  is priem voor  $n = -40 \text{ t/m } +39$ .

12. De getallen  $\{1, 2, 3, \dots, p-1\} \pmod p$  zijn te schrijven als  $\{1, a, a^2, \dots, a^{p-2}\} \pmod p$  voor zekere  $a$ . Deze heet een *voortbrenger*. Voorbeeld:  $a = 3 \pmod{31}$ . Niet elke  $a$  doet 't; bv.  $2^5 = 1 \pmod{31}$ .

Deze voortbrengers zijn van groot belang in de cryptografie (geheimschriften en codes; veilig betalen). Helaas is er nog geen *bewezen juiste* en *snelle* manier om ze te vinden (bij grote  $p$ ).

**Opgave.** Ontbind  $100!$  in priemfactoren!

### Toepassing in de cryptografie:

Een truc om samen een geheime sleutel af te spreken over een *onveilige* communicatielijn!

Tabelletje:

$x =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$3^x \text{ mod } 31$	1	3	9	27	19	26	16	17	20	29	25	13	8	24	10	30

16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
28	22	4	12	5	15	14	11	2	6	18	23	7	21	1

$A$ (lice) en  $B$ (ob) willen communiceren.  $A$  kiest een *geheim getal*, 14, en  $B$  ook: 25.

*Openbaar*, d.w.z. publiekelijk toegankelijk zijn:  $3^{14} \text{ mod } 31 = 10$  en  $3^{25} \text{ mod } 31 = 6$ .

$A$  zoekt op  $B$ 's openbare getal, 6, en berekent  $S = 6^{14} \text{ mod } 31$ .

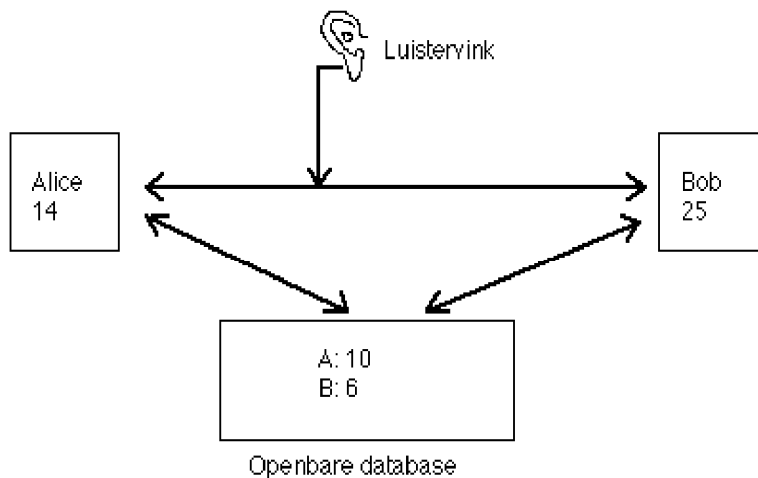
$B$  zoekt op  $A$ 's openbare getal, 10, en berekent  $S' = 10^{25} \text{ mod } 31$ .

Nu is  $S = S'$ . Want  $6^{14} = (3^{25})^{14}$  en  $10^{25} = (3^{14})^{25} \text{ mod } 31$ .  $S$  is de geheime, gemeenschappelijke sleutel!

De veiligheid berust op het feit, dat weliswaar  $3 \rightarrow 3^x$  snel is uit te rekenen (bv. op z'n "Indiaas"), maar voor het oplossen van  $3^x = a$  zijn geen snelle (algemene) algorithmen bekend!

Ga zelf na, dat over de lijn alleen veilige informatie wordt gestuurd!

In de praktijk werkt men natuurlijk niet met 31, maar met priemgetallen van wel een paar honderd bits! ( $\approx 2^{200}$ ). Hoe die te vinden, is weer een ander chapter...



## 5.1 Perfecte getallen (facultatief).

Een *perfect getal* is gelijk aan de som van zijn delers (behalve de grootste deler, nl. zichzelf). Voorbeeld:  $6 = 1 + 2 + 3$ ;  $28 = 1 + 2 + 4 + 7 + 14$ .

Andere perfecte getallen zijn 496, 8128, 137438691328. Tot en met 8128 waren ze al in de oudheid bekend (Nicomachus, Iamblichus). Tot op heden is niet bekend of er *oneindig veel* perfecte getallen zijn, en of er *oneven* perfecte getallen bestaan.

*Euler* bewees dat alle even perfecte getallen er uit zien als  $2^{n-1}(2^n - 1)$  waar  $2^n - 1$  priem is (een zgn. Mersenne-priemgetal). Het vinden van Mersenne priemgetallen is een grote sport op de computer, omdat men snelle methoden kent om na te gaan of  $2^n - 1$  wel priem is. Noem  $M_n = 2^n - 1$ . Als  $M_n$  priem is, dan moet  $n$  priem zijn (waarom?) Het grootst bekende perfecte getal in 1985 was  $2^{216090}M_{216091}$ .

We zullen eens nagaan waarom  $2^{n-1}M_n$  perfect is als  $M_n$  priem is.

### Twee stellingen over delers

Laat  $d(n)$  het aantal delers van  $n$  zijn; bv.  $d(6) = 4$  (4 delers: 1, 2, 3 en 6) en  $d(p) = 2$  als  $p$  priem is. Laat  $\sigma(n)$  de som der delers van  $n$  zijn, dus bv.  $\sigma(n) = 2n$  als  $n$  perfect is.

$d(n)$  heeft een mooie eigenschap. Laten  $m$  en  $n$  onderling ondeelbaar zijn:  $\text{ggd}(m, n) = 1$ . Bewering:  $d(mn) = d(m)d(n)$ . Dit is flauw: elke deler van  $mn$  valt uniek uiteen in een “ $m$ -stuk” en een “ $n$ -stuk”!

Nu is, voor  $p$  priem,  $d(p^i) = i + 1$  want  $p^i$  heeft delers  $1, p, p^2, \dots, p^i$ . Dus:

**Stelling.** Laat  $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$  (priemgetalontbinding). Dan is  $d(n) = (i_1 + 1)(i_2 + 1) \dots (i_k + 1)$ .

Ook  $\sigma(n)$  voldoet aan bovenstaande mooie eigenschap:

$$\underbrace{(d_1 + d_2 + \dots)}_{\text{delers van } m} \underbrace{(e_1 + e_2 + \dots)}_{\text{delers van } n} = \dots + \underbrace{d_i e_j + \dots}_{\text{delers van } mn}$$

Maar  $\sigma(p^i) = 1 + p + p^2 + \dots + p^i = \frac{p^{i+1} - 1}{p - 1}$ . Dus:

**Stelling.**  $\sigma(n) = \frac{(p_1^{i_1+1} - 1)(p_2^{i_2+1} - 1) \dots (p_k^{i_k+1} - 1)}{(p_1 - 1)(p_2 - 1) \dots (p_k - 1)}$  ( $n$  als boven).

Van  $2^{n-1}M_n$  is dus de som der delers

$$\sigma(2^{n-1}M_n) = \frac{2^n - 1}{2 - 1} \cdot \frac{M_n^2 - 1}{M_n - 1} = (2^n - 1)(M_n + 1) = 2^n(2^n - 1) = 2 \cdot 2^{n-1}M_n$$

dus de som der delers  $< 2^{n-1}M_n$  is  $2^{n-1}M_n$ :  $2^{n-1}M_n$  is perfect!

Met iets meer moeite (raadpleeg een boekje over getaltheorie!) kun je inzien dat dit de enige even perfecte getallen zijn.

Nauw verwant hieraan zijn *bevriende getallen*: ze hebben elkaars delersom (zichzelf weer niet meegeteld). Zo is  $220 = 2^2 \times 5 \times 11$ , som = 284 en  $284 = 2^2 \times 71$ , som = 220.

**Opgave.** Als  $n > 1$ ,  $a = 3 \cdot 2^n - 1$ ,  $b = 3 \cdot 2^{n-1} - 1$ ,  $c = 9 \cdot 2^{2n-1} - 1$  en  $a$ ,  $b$  en  $c$  zijn priem dan zijn  $2^n ab$  en  $2^n c$  bevriend.

## 6 Gemengd moois - om door te lezen...

Voor (veel) meer zie bv. *David Wells, "The Penguin Dictionary of Curious and Interesting Numbers"* (Penguin pocket, ISBN 01400.80295).

- Probleem van Brocard: Wanneer is  $n! + 1$  een kwadraat?  $n = 4, 5, 7$  ( $7! + 1 = 5041 = 71^2$ ). Of er meer zijn: onbekend!
- Zijn er gehele (evt. negatieve)  $x, y$  en  $z$  met  $x^3 + y^3 + z^3 = 31$ ?
- Is er een *snelle* methode om een deler ( $\neq 1, n$ ) van  $n$  te vinden?
- Er bestaat een reëel getal  $\alpha$  met de eigenschap:  $[7^{2^n} \alpha] - 7^{2^{n-1}} [7^{2^{n-1}} \alpha]$  is het  $n^e$  priemgetal! ( $[ \ ] =$  naar beneden afronden.)
- Als  $n$  oneven is dan is  $n$  op precies  $8d(n)$  manieren te schrijven als som van 4 kwadraten.
- $1^3 + 6^3 + 8^3 = 9^3$ . Euler vermoedde 2 eeuwen terug dat een  $k^e$  macht niet te schrijven is als som van (minstens 2 doch) minder dan  $k$   $k^e$  machten. Dit leek plausibel tot Landau en Parker in 1966 (pas!) kwamen met:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5 \dots$$

- Het aantal *partities* van  $n$  (bv.  $4 = 4 = 1+3 = 2+2 = 1+1+2 = 1+1+1+1$ ; 5 partities) is voor grote  $n \sim \frac{1}{4n\sqrt{3}} e^{\pi\sqrt{\frac{2n}{3}}}$  ( $\sim$  betekent: de verhouding komt voor grote  $n$  steeds dichterbij 1 te liggen).
- $x^n + y^n = z^n$  heeft geen oplossing in  $\mathbb{Z}$  met  $n > 3$  en  $xyz \neq 0$  (Wiles, 1993). Het bewijs is te lang voor dit blaadje.

## 7 Appendix: de stelling van Lagrange

(facultatief: alleen voor de doordouwers).

Een van de mooiste stellingen uit de getaltheorie is de volgende:

**Stelling** (Lagrange): *Elk positief geheel getal is de som van 4 kwadraten.*

Het bewijs kun je met het geleerde in deze cursus helemaal begrijpen. Hier komt het, in vier stappen.

**Bewijs:**

**I. Een hulpstelling:**  $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = (ax + by + cz + dt)^2 + (-bx + ay + dz - ct)^2 + (-cx - dy + az + bt)^2 + (-dx + cy - bz + at)^2$ . Dit kun je narekenen; deze uitdrukking heeft te maken met de zogenaamde "quaternionen".

Gevolg: we hoeven de vierkwadratenstelling nu alleen nog voor priemgetallen  $p$  te bewijzen! Het geval  $p = 2$  is flauw. Vanaf nu is  $p$  priem en oneven.

**II.** Zij dus  $p$  priem  $\neq 2$ . We bewijzen eerst dat er een getal  $m$  is,  $1 \leq m < p$ , en getallen  $x, y, z, t$  zó, dat  $x^2 + y^2 + z^2 + t^2 = pm$ .

Vooraf merken we op dat uit  $x^2 = y^2 \pmod p$  volgt:  $x = y$  of  $x = -y \pmod p$ . Immers,  $(x + y)(x - y) = 0 \pmod p$  dus  $p|(x + y)$  of  $p|(x - y)$ .

Gevolg:  $K = \{0^2, 1^2, 2^2, \dots, (\frac{p-1}{2})^2\}$  is precies de verzameling kwadraten  $\pmod p$ ; dat zijn er dus  $\frac{p+1}{2}$  stuks.

Stel verder:  $K^* = \{-k - 1 \pmod p \mid k \in K\}$ . Ook  $|K^*| = \frac{p+1}{2}$ . Omdat  $K$  en  $K^* \subseteq \{0, 1, \dots, p-1\}$  geldt  $K \cap K^* \neq \emptyset$  want anders hadden ze samen  $p + 1$  elementen. Gevolg: er zijn  $a, x$ , en  $y \pmod p$  met

$$a = x^2 \pmod p \text{ en } a = -y^2 - 1 \pmod p.$$

Maar dan is

$$x^2 + y^2 + 1 = 0 \pmod p ; \text{ zeg } x^2 + y^2 + 1 = pm.$$

Dus is er een  $m > 0$  met:  $x^2 + y^2 + z^2 + t^2 = pm$  heeft een oplossing met  $z = 1, t = 0$ . Omdat je  $x$  en  $y \leq \frac{p-1}{2}$  kunt nemen, is  $mp < ((\frac{p-1}{2})^2 + (\frac{p-1}{2})^2 + 1)$  waaruit je gemakkelijk narekent dat  $m < p$  (ja zelfs,  $m \leq \frac{p+1}{2}$ ).

**III.** Beschouw vanaf nu de *kleinst mogelijke*  $m > 0$  met, voor zekere  $x, y, z$  en  $t$ :  $x^2 + y^2 + z^2 + t^2 = pm$ . Uit stap **II** volgt dat die  $m$  er moet zijn. Zoals we zagen is  $m < p$ . Ons doel is, aan te tonen dat in feite  $m = 1$ .

**Stel m is even.**

**Geval 1:**  $x$  en  $y$  en  $z$  en  $t$  zijn allemaal even. Dan kun je schrijven:  $m = 4m'$  en  $(\frac{x}{2})^2 + (\frac{y}{2})^2 + (\frac{z}{2})^2 + (\frac{t}{2})^2 = \frac{1}{4} \cdot 4m'p = m'p$ . Dat kan niet ( $m' \neq 0$ ; maar  $m$  was de kleinst mogelijke).

**Geval 2:** onder  $x, y, z, t$  zitten **oneven** getallen. Dan zijn dat er 2 of 4 (anders zou  $m$  oneven zijn). Na eventueel hernoemen van  $x, y, z$  en  $t$  kunnen we daarom aannemen dat  $x = y \pmod 2$  én  $z = t \pmod 2$ . Dan zijn  $x + y$  en  $z + t$  dus beide even. Maar dan kun je schrijven:

$$(\frac{x+y}{2})^2 + (\frac{x-y}{2})^2 + (\frac{z+t}{2})^2 + (\frac{z-t}{2})^2 = \frac{1}{2}(x^2 + y^2 + z^2 + t^2) = \frac{1}{2}mp.$$

Dit kan opnieuw niet wegens de minimaliteit van  $m$ .

**IV. Dus  $m$  is oneven.** We willen, naar we ons herinneren, in  $x^2 + y^2 + z^2 + t^2 = mp$  graag  $m = 1$  hebben. Stel echter,  $m$  is groter dan 1.

Deel met rest:  $x = mx' + x''$  met  $-\frac{m}{2} < x'' < \frac{m}{2}$  ( $\frac{m}{2}$  is  $> 0$ ;  $x''$  gelijk aan  $\pm \frac{m}{2}$  kan niet want  $m$  is oneven). Net zo:  $y = my' + y''$ ;  $z = mz' + z''$ ;  $t = mt' + t''$ . Dan is

$$x''^2 + y''^2 + z''^2 + t''^2 = (x - mx')^2 + (y - my')^2 + (z - mz')^2 + (t - mt')^2 = x^2 + y^2 + z^2 + t^2 \pmod{m} = 0 \pmod{m}.$$

Ook is  $x''^2 + y''^2 + z''^2 + t''^2 < 4 \cdot (\frac{m}{2})^2 = m^2$ , dus  $x''^2 + y''^2 + z''^2 + t''^2 = \nu m$  met  $\nu m < m^2$ ; oftewel  $\nu < m$ .

Merk ook op dat  $\nu \neq 0$  omdat anders  $x'' = y'' = z'' = t'' = 0$  zou zijn, dus  $x = y = z = t = 0 \pmod{m}$ . Dat zou impliceren dat  $x^2 + y^2 + z^2 + t^2 = 0 \pmod{m^2}$ ;  $pm = 0 \pmod{m^2}$ ;  $m|p$ . Maar  $m$  was  $< p$  en tevens, naar we hier aannamen,  $> 1$ .

We hebben  $(x^2 + y^2 + z^2 + t^2)(x''^2 + y''^2 + z''^2 + t''^2) = mp \cdot \nu m = \nu m^2 p$ .

Maar - zie onderdeel I - dit is opnieuw te schrijven als som van vier kwadraten  $(xx'' + yy'' + zz'' + tt'')^2 + (\dots)^2 + (\dots)^2 + (\dots)^2 \stackrel{(zeg)}{=} X^2 + Y^2 + Z^2 + T^2$ .

Daarin is:

$X = xx'' + yy'' + zz'' + tt'' = x^2 + y^2 + z^2 + t^2 \pmod{m} = 0 \pmod{m}$ ; zeg  $X = mX_0$  en net zo:  $Y = -yx'' + xy'' + tz'' - zt'' = -yx + xy + tz - zt = 0 \pmod{m}$  en idem voor  $Z$  en  $T$ . Dus  $X^2 + Y^2 + Z^2 + T^2 = m^2 X_0^2 + m^2 Y_0^2 + m^2 Z_0^2 + m^2 T_0^2 = \nu m^2 p$ ;

$$X_0^2 + Y_0^2 + Z_0^2 + T_0^2 = \nu p \text{ met } \nu < m.$$

Maar  $\nu$  was  $> 0$  en  $m$  was minimaal. Dat kan niet; en deze tegenspraak vloeit voort uit de aanname dat  $m > 1$  is. Dus  $m$  moet 1 zijn, en  $mp = p$  is de som van 4 kwadraten.

**Opmerking:** bovenstaand verhaal III kun je ook zien als een *effectieve* methode om de gewenste vier kwadraten te bepalen! (programmaatje...?)

\*\*\*\*\*