Een derde-macht kan niet geschreven worden als een som
van twee derde-machten, of, een vierde-macht als een som
van twee vierde-machten, of, in het algemeen een macht
groter dan twee als som van twee dezelfde machten.
Ik heb een prachtig bewijs van deze stelling maar de kantlijn
is te klein om het te bevatten.

Pierre de Fermat

(geschreven ±1637 in de marge van de uitgave van
Bachet van een boek van Diophantus).

De laatste stelling van Fermat

Docent: Prof. Dr F. Oort

Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. One goes into the first room, and it's dark, completely dark. One stumbles around bumping into the furniture, and gradually, you learn where each piece of furniture is, and finally, after six months or so, you find the light switch.

(**Andrew Wiles** in de BBC documentaire)

Syllabus van een HOVO cursus
Leiden, maandag 11^{15}-13 uur,
26-I, en 2, 9, 16, 23 - II - 2015

De laatste stelling van Fermat

Inhoudsopgave

Inleiding

Zo vaak zeggen mijn vrienden en kennissen dat ze graag wat meer over wiskunde willen weten en horen. Maar hoe kan ik dat doen op een bevattelijke manier zonder de waarheid geweld aan te doen? Al werkend aan deze cursus merk ik dat er inderdaad veel is wat op een begrijpelijk niveau de fascinerende schoonheid van wiskunde kan laten zien.

"Wat me trof in al mijn gesprekken met hen was de buitengewone nauwkeurigheid waarmee ze zich uitdrukten ... de precieze opbouw van het antwoord ... dat wiskundigen domweg een hekel hebben aan het doen van een onware uitspraak ... " Zie [S] pagina 12.

Iets uitleggen wil ik doen op een wiskundig juiste manier. Zo vaak wordt er in onze wereld populariserend geschreven en gesproken (daar heb ik niets op tegen). Maar de grens wordt overschreden als we daarbij onware uitspraken doen. En dit gehoor zal dat ongetwijfeld als storend ervaren.

De schoonheid van wiskunde bestaat eigenlijk uit twee totaal verschillende componenten.

Een ervan is die ongebreidelde stroom van nieuwe gedachten, vergezichten in een abstracte wereld, het plotseling eenvoudig worden van een probleem dat eerst onoplosbaar en erg moeilijk leek. Over de intuïtie van de wiskundige die hieraan ten grondslag ligt zal ik in de cursus af en toe komen te spreken. Juist dit aspect is zo prachtig beschreven in het boek [S] van Singh.

Een ander aspect is het feit dat je al die vergezichten, die prachtige gedachten kunt vatten in precieze beschrijvingen, kunt bewijzen in sluitende gedachtengangen. – Ik hoop en verwacht van alle deelnemers dat ze hiermee aan de slag gaan: niet alleen passief luisteren, maar ook vragen stellen, en vooral elke week tenminste één bewijs zelfstandig en volledig uitschrijven en vraagstukken maken die laten zien dat U deze stof actief kunt hanteren. Zo krijgt U voeling met deze wondere wereld, zo ziet U hoe een beetje nadenken inzicht kan geven.

Deze beide aspecten komen juist zo mooi naar voren in de overeenkomsten, maar vooral ook in de verschillen tussen het boek [S] van Singh enerzijds, en de wat drogere, maar meer precieze tekst van deze syllabus anderzijds.

" Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

In de cursus volgen we het spoor dat de "Laatste Stelling van Fermat" getrokken heeft in de geschiedenis. In 1637 schreef Pierre de Fermat dat hij een wonderlijk bewijs had gevonden van de volgende stelling:

$$n \in \mathbb{Z}_{\geq 3}, \quad x, y, z \in \mathbb{Z}, \quad x^n + y^n = z^n \quad \Longrightarrow \quad xyz = 0.$$

We zullen dit aangeven met FLT (Fermat's Last Theorem). Het werd de "laatste stelling" genoemd, omdat Fermat uitspraken deed, die alle werden opgelost/bewezen/tegengesproken, op deze ene na.

Fermat schreef zijn bewijs echter niet op. We weten nog steeds niet hoe hij deze stelling dacht te bewijzen. We kunnen wel daarover speculeren, ik zal daar iets over vertellen.

Door ongelooflijk veel wiskundigen is hieraan gewerkt. Veel theorie werd ontwikkeld om dit probleem, wat zo eenvoudig lijkt, op te lossen. Pas aan het eind van de 20-set eeuw werd inderdaad bewezen dat deze stelling juist is. Zich baserend op veel voorkennis, en na vele jaren intensief werk gelukte dit aan Andrew Wiles, zie [76].

Overigens ik heb in deze inleiding alvast een oefening ingebouwd. Hierboven vind U de uitspraak van het vermoeden / de stelling in moderne wiskundige notatie. Er staat:

$$n \in \mathbb{Z}_{\geq 3}, \quad x, y, z \in \mathbb{Z}, \quad x^n + y^n = z^n \quad \Longrightarrow \quad xyz = 0;$$

in meer gebruikelijke bewoording:

> "*zij n een geheel getal dat minstens 3 is, laat x en y en z gehele getallen zijn, die een oplossing geven van de vergelijking $X^n + Y^n = Z^n$; dan is of $x = 0$ of $y = 0$ of $z = 0$.*"

In plaats van deze laatste, wat onoverzichtelijke bewering verkies ik de moderne, kortere beschrijving. Ik hoop dat U al gauw went aan deze wiskundige stenografie die het leven zo gemakkelijk maakt.

We hadden ook de formulering kunnen kiezen die Fermat zelf gaf, zoals die hierboven en in vertaling op de omslag van deze syllabus staat.

Aan het eind van de cursus zullen we met elkaar die prachtige BBC productie zien die voorafging aan en de grondslag was voor het boek [S]. Ik heb verschillende keren met studenten deze documentaire bekeken. En elke keer is het een ervaring die me diep raakt. Ik hoop dat U dit ook zo zult ervaren. Een aspect van die documentaire is de open en lucide manier waarop wiskundigen over hun vak praten, die open bevlogenheid, en de diepe eerbied die we als wiskundigen hebben voor ons vak en voor elkaar.

In deze cursus zal ik een aantal (klassiek) bekende stellingen laten zien, met daarbij bewijzen (dat is het hart van de wiskunde):
- Pythagoreïsche drietallen (oplossingen van $X^2 + Y^2 = Z^2$, met x, y, z gehele getallen).
- Welke gehele getallen zijn te schrijven als som van twee kwadraten?
- Een inleiding op begrippen die naar voren komen in de documentaire.
- Een aantal gemakkelijke en ook wat moeilijkere vraagstukken; ga er vooral mee aan de slag.
- Ook zal ik proberen iets weer te geven van de denkwereld van grote wiskundigen zoals Fermat en Euler.

Een afspraak die ik met U in het gehoor maak: als ergens mijn uitleg ook maar even niet duidelijk is, laat dat dan weten; ik begin dan overnieuw, en we gaan na waar ik te weinig details gaf. Ook zal het even wennen zijn voor U om deze wiskundige notatie te gebruiken, ook daarbij vragen stellen zou ik zeggen.

Met [S] verwijs ik naar [65].
Voor wiskundige notatie zie § 13. Lees deze paragraaf geregeld.
Voor variabelen kiest ik vaak hoofdletters, en voor waarden daarvan kleine letters;
toelichting: in plaats van "los op $X^2 = 1$" schrijf ik liever: "vind x met $x^2 = 1$" (ik zal toelichting geven waarom).
Een ster geeft aan dat het betreffende onderdeel meer kennis verondersteld dan ik in deze cursus kan uitleggen, zoals b.v. § 6 Euler: $\mathrm{FLT}_3{}^*$.

1 Pythagoreïsche drietallen: $\mathbf{FLT}_2$

We zullen zien dat in de *laatste stelling van Fermat* de exponent wordt verondersteld $n \geq 3$ te zijn. In deze paragraaf laten we zien (zoals Euclides al wist) dat er voor de vergelijking

$$X^2 + Y^2 = Z^2$$

oneindig veel oplossingen zijn in positieve gehele getallen. Het is heel eenvoudig te bewijzen dat er oneindig veel oplossingen zijn:

(1.1) Vraagstuk. Merk op dat voor elke positief geheel getal B het verschil $(B+1)^2 - B^2$ oneven is. Ga na dag we zo alle positieve oneven getallen krijgen. Ga na dat er voor elk oneven positief geheel getal A er een B is met

$$A^2 + B^2 = (B+1)^2.$$

Conclusie: het aantal oplossingen van $X^2 + Y^2 = Z^2$ in gehele getallen is oneindig. Zie (16.1)

Zijn we nu tevreden? Nee, helemaal niet. Een wiskundige vraagt dan naar alle oplossingen. We zien direct dat we met het vorige vraagstuk niet alle oplossingen krijgen (maak een voorbeeld). We gaan naar een meer systematische aanpak.

(1.2) Definitie: *Een drietal positieve gehele getallen*

$$x, y, z \in \mathbb{Z}_{>0}$$

heet een **Pythagoreïsche drietal**, afgekort PD, *als*

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

We zeggen dat een PD (x, y, z) **primitief** *is*, afgekort pPD, *als de grootste gemene deler van x en y gelijk is aan 1.* We schrijven $\text{ggd}(x, y)$ voor de grootste gemene deler van x en y. Zie § 9 voor meer informatie.

(1.3) Opmerking. Als $x^2 + y^2 = z^2$ dan zijn equivalent:
$\text{ggd}(x, y) = 1$ en
$\text{ggd}(y, z) = 1$ en ook
$\text{ggd}(z, x) = 1$
(ga na). We zullen dit voortaan gebruiken zonder verdere vermelding.

Het volgende vraagtuk is heel eenvoudig, en het geeft precies de goede informatie.

(1.4) Vraagstuk. Voor en even geheel getal y is y^2 deelbaar door 4. Voor een oneven geheel getal x is

$$x^2 \equiv 1 \pmod 4;$$

hier staat: bij deling door 4 van x^2 is de rest gelijk aan 1; zie § 13. Zie (16.2).

Onderstel dat (x, y, z) een pPD is; dan geldt:

óf x is even en y is oneven *óf x is oneven en y is even.*

(1.5) Stelling (Euclides, ± 300 vóór Christus, zie Boek X, Propositie 28a, en Euler): *Als* (x, y, z) *een* pPD *is, met* y *even* (en dus x even) *dan bestaan er* $m, n \in \mathbb{Z}_{>0}$ *met* $m > n$, *en* $\text{ggd}(m, n) = 1$, *en* $m + n$ *oneven, zodanig dat*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Omgekeerd bepaalt een tweetal getallen $m > n > 0$ *met* m *en* n *onderling ondeelbaar, en niet allebei oneven (eenduidig) een* pPD.

(1.6) Hier zijn een paar voorbeelden:

n	m	x	y	z
1	2	3	4	5
1	4	15	8	17
2	3	5	12	13
1	6	35	12	37
2	5	21	20	29
3	4	7	24	25
1	8	63	16	65
2	7	45	28	53
4	5	9	40	41
1	10	99	20	101
2	9	77	36	85
3	8	55	48	73
4	7	33	56	65
5	6	11	60	61
1	12	143	24	145
2	11	117	44	125
3	10	91	60	109
4	9	65	72	97
5	8	39	80	89
6	7	13	84	85
etc.	etc.	etc.	etc.	etc.

Vraag. Wat valt er op? wat voor eigenschapen hebben getallen z die in een pPD (x, y, z) optreden?

(1.7) Gevolg. *Als* (x, y, z) *een* PD *is, dan bestaan er*

$$e \in \mathbb{Z}_{\geq 1} \quad \textit{en} \quad m, n \in \mathbb{Z}_{>0}$$

met $m > n$, *en* $\text{ggd}(m, n) = 1$, *en* $m + n$ *oneven zodanig dat*

$$\{e(m^2 - n^2), e(2mn)\} = \{x, y\} \quad \textit{en} \quad e(m^2 + n^2) = z.$$

Waarschuwing. Voor gehele getallen $m > n > 0$ is $(m^2 - n^2, 2mn, m^2 + n^2)$ een PD, maar niet elk PD is op deze manier te schrijven; geef een voorbeeld waar dit niet kan.

(1.8) Vraagstuk. Bewijs: voor een geheel getal b geldt:

$$b \text{ is deelbaar door } 3 \iff b^2 \text{ is deelbaar door } 3;$$

$$b \text{ is niet deelbaar door } 3 \iff b^2 \equiv 1 \pmod 3.$$

Neem aan dat (x, y, z) een pPD is; dan is $x - y$ niet deelbaar door 3. Zie (16.3).

(1.9) Vraagstuk.

I know an old man in Tralee
Whose age is his wife's age plus three.
Now he rightly declares,
That the sum of their squares
Is a square; so how old could he be?

Wat is de leeftijd van die man? (Geef tenminste één oplossing. Facultatief: ook nog bewijzen dat er maar één oplossing mogelijk is binnen de grenzen gegeven door het gegeven "an old man".) Zie(16.4).

(1.10) Opmerking.* *De vergelijking $y^2 + (y+1)^2 = z^2$ heeft oneindig veel oplossingen in positieve gehele getallen. De oplossingen met $y = 3$, en $y = 20$ zijn de enige met $y < 119$.* We geven alle oplossingen van deze vergelijking.

Omdat $(y, y+1, z)$ een pPD is, zij er m, n met eigenschappen als in (1.5) met

$$m^2 - n^2 - 2mn = \pm 1; \quad \text{schrijf } \; m - n =: t, \quad \text{dan is } \; t^2 - 2n^2 = \pm 1.$$

Bewering. *Alle oplossingen met $t > 0$ en $n > 0$ van deze vergelijking worden gegeven door*

$$(1 - \sqrt{2})^i = t_i - n_i\sqrt{2}, \quad i \geq 1.$$

Dit wordt bewezen door alle eenheden van de ring $\mathbb{Z}[\sqrt{2}]$ te bepalen; die zijn alle van de vorm $(\pm 1 \pm \sqrt{2})^i$ (we bewijzen dat hier niet). Als we dit aannemen dan zien we dat alle oplossingen gegeven worden door:

i	t	n	m	$m^2 - n^2$	$2mn$
1	1	1	2	3	4
2	3	2	5	21	20
3	7	5	12	119	120
4	17	12	29	697	696
5	41	29	70	4059	4060
6	99	70	169	23661	23660
7	239	169	408	137903	137904
etc.	etc.	etc.	etc.	etc.	etc.

Hoe deze rij verder gaat (kunnen we eenvoudig berekenen en) ziet U b.v. op
`https://oeis.org/` door het begin van deze rij getallen $1, 1, 2, 3, 5, 7, 12, 17$ in te typen, of door de rij $1, 2, 5, 12$ te proberen.

De vergelijking $t^2 - 2n^2 = \pm 1$ komt later terug (als de Pell vergelijking), zie (12.1).

2 Bewijzen van de classificatie van PDen

In deze § bewijzen we de Stelling (1.5). We geven drie verschillende bewijzen, vooral om aan te tonen dat een probleem in de wiskunde vaak pas begrepen wordt door toepassing van methoden uit heel verschillende vakgebieden. Juist die manier van aankijken tegen wiskundige begrippen, van heel verschillende invalshoeken, heeft inzicht gegeven.

(2.1) Eerst een paar voor de hand liggende opmerkingen. We zien dat

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 - 2m^2n^2 + n^2 + 4m^2n^2 = (m^2 + n^2)^2.$$

Bovendien, als m en n voldoen aan de eigenschapen in de stelling, dan krijgen we zo een primitief PD: Omdat $m + n$ oneven is, volgt dat $m^2 - n^2$ oneven is; dus is 2 geen gemeenschappelijke factor; als $p > 2$ een priemdeler is van $2mn$, dan is óf p en deler van m en niet van n of omgekeerd; in dat geval is p niet een deler van $m^2 - n^2$.
Conclusie. De eigenschappen van m en n in de stelling garanderen dat we zo een pPD krijgen.

We hebben ook gezien dat voor een pPD (x, y, z) óf x oneven en y even óf x even en y oneven; we nemen aan dat x oneven is (zo niet, dan verwisselen we x en y).

(2.2)

Eerste bewijs van (1.5): *elementaire getaltheorie.*

In dit bewijs gebruiken we het feit dat elk positief geheel getal ontbonden kan worden in priemfactoren, dat die ontbinding eenduidig is (op volgorde van de factoren na), en we gebruiken eigenschapen van de grootste gemene deler. Voor details zie § 9.

Stel $x^2 + y^2 = z^2$ met x oneven. Dan geldt

$$(\frac{y}{2})^2 \quad = \quad \frac{z+x}{2} \cdot \frac{z-x}{2}.$$

Uit de gegevens volgt dat $y/2, \quad (z+x)/2, \quad (z-x)/2 \in \mathbb{Z}_{>0}$. Ga na dat ook

$$\text{ggd}(\frac{z+x}{2} \ , \ \frac{z-x}{2}) = 1.$$

Als p een priemgetal is dat $y/2$ deelt en $u \in \mathbb{Z}_{>0}$ zo dat p^u deelt $b/2$ en p^{u+1} deelt niet $b/2$ is p een deler van $(z+x)/2$ óf van $(z-x)/2$ (en niet van allebei); in het eerste geval is p^{2u} precies de macht van p die $(z+x)/2$ deelt. We concluderen: zowel $(z+x)/2$ als $(z-x)/2$ is een kwadraat van een positief geheel getal. We schrijven

$$m^2 := \frac{z+x}{2} \quad \text{en} \quad n^2 := \frac{z-x}{2}.$$

Ga na dat $\text{ggd}(m, n) = 1$, en dat $m + n$ oneven is. Conclusie:

$$\{(a, b, c) \mid \text{pPD}, \quad 2|b\} \stackrel{\sim}{\longleftrightarrow} \{(m, n) \mid 0 < n < m, \quad \text{ggd}(m, n) = 1, \quad m + n \ \text{ oneven}\}.$$

Dit is het eerste bewijs van Stelling (1.5).

(2.3)

Tweede bewijs van (1.5): *meetkunde.*

Ook hier gebruiken we het feit dat elk positief geheel getal ontbonden kan worden in priemfactoren, dat die ontbinding eenduidig is (op volgorde van de factoren na).

Zij (x, y, z) een PD (niet noodzakelijk primitief); we schrijven

$$u := \frac{x}{z}, \quad \text{en} \quad v := \frac{y}{z},$$

en we zien dat geldt

$$u^2 + v^2 = 1;$$

met ander woorden, het "punt" (u, v) ligt op de cirkel C gegeven door deze vergelijking. We vragen ons omgekeerd af, welke punten op deze cirkel hebben coördinaten in $\mathbb{Q}$? De meetkunde laat ons zien hoe we dat kunnen beslissen. Neem een punt of de cirkel, we kiezen $R := (-1, 0)$, en laat het een punt $S_t := (0, t)$ lopen over de V-as. (Later zullen we bovendien veronderstellen dat $0 < t < 1$.) Verbind de punten R en S_t; dat geeft een lijn met de vergelijking

$$L_t : \quad V = t(U + 1)$$

(ga na); snijdt deze lijn L_t met de cirkel C; dat geeft twee snijpunten (allicht), en wel:

$$L_t \bigcap C \quad = \quad \{R, P_t\} \quad \text{met} \quad P_t = (u = \frac{1 - t^2}{1 + t^2}, \quad v = \frac{2t}{1 + t^2})$$

(ga na). Omgekeerd kunnen uit een punt $P \in C$ met $P \neq R$ de verbindingslijn L bepalen, en we krijgen: als $P = (u, v)$, met $u^2 + v^2 = 1$, dan is

$$t = \frac{v}{u + 1}, \quad P = P_t.$$

We zien

$$t \in \mathbb{Q} \quad \Longleftrightarrow \quad P_t \in (\mathbb{Q} \times \mathbb{Q}) \cap C.$$

Bovendien zien we: $0 < t < 1 \Longleftrightarrow P_t \in \mathbb{Q}_{>0} \times \mathbb{Q}_{>0}$ (ga na; kun je dat "meetkundig inzien"?). We schrijven deze transformaties uit:

$$(x, y, z) \quad \mapsto \quad (u = \frac{x}{z}, \quad v = \frac{y}{z}) \quad \mapsto \quad t := \frac{u}{v + 1} = \frac{y}{x + z},$$

en

$$0 < t = \frac{N}{M} \mapsto (u = \frac{1 - t^2}{1 + t^2}, \quad v = \frac{2t}{1 + t^2}) \quad \mapsto (x = M^2 - N^2, y = 2MN, z = M^2 + N^2).$$

We zien dat

$$\{t \in \mathbb{Q} \mid 0 < t < 1\} \overset{\sim}{\longleftrightarrow} \{P = (u, v) \in C \mid x, y \in \mathbb{Q}_{>0}\}$$

(ga na).

We gebruiken deze formules om het bewijs af te maken. Als $(u, v) \in C$ dan ook $(v, u) \in C$. Als (x, y, z) een PD is, dan geldt ook $y^2 + x^2 = z^2$. Deze dubbelzinnigheid, en het mechanisme om uit $(u, v) \in C(\mathbb{Q})$ een pPD te construeren analyseren we teneinde het bewijs af te maken.

Waarschuwing. De breuk $t = 1/3$ geeft $(x = 8, y = 6, z = 10)$; we zien dat $t = N/M$ met $\text{ggd}(M, N) = 1$ niet garandeert dat $(x = M^2 - N^2, y = 2MN, z = M^2 + N^2)$ een pPD is. Als we $(x = 8, y = 6, z = 10)$ vereenvoudigen tot $(4, 3, 5)$ dan krijgen we een pPD, maar met $x = 4$ even. Nemen we echter $0 < t = n/m < 1$ met $\text{ggd}(m, n) = 1$ en $m+n$ oneven dan is het bijbehorende PD $(x = m^2 - m^2, y = 2mn, z = m^2 + n^2)$. We zien hoe we uit de meetkunde weer terugkeren tot de getaltheorie:

Onder de correspondentie

$$t = \frac{u}{v+1} = \frac{y}{x+z} \quad \text{krijgen we} \quad t' := \frac{1-t}{1+t} = \frac{v}{u+1} = \frac{x}{y+z}$$

(ga na); merk op: $t \mapsto t'$ correspondeert precies met het verwisselen van x en y, met het verwisselen van u en v. Als $0 < t = N/M < 1$ met $\text{ggd}(M, N) = 1$ en $M + N$ even (dus M en N oneven) dan heeft $t' = (1 - t)(1 + t) = (M - N)/(M + N) = n/m$ met $\text{ggd}(m, n) = 1$ de eigenschap dat $0 < t' < 1$ en $m + n$ is oneven. In deze situatie is $M + N$ oneven dan en slechts dan als $m + n$ even is (ga na). We zien: bij gegeven $t \in \mathbb{Q}$ met $0 < t < 1$ geeft P_t een pPD met x oneven óf $t' := (1 - t)/(1 + t)$ heeft deze eigenschap.

QED Stelling (1.5)

(2.4)

Derde bewijs van (1.5): *algebraïsche getaltheorie.*

(2.5) Vraagstuk. (We beginnen met een heel eenvoudig vraagstuk.) *Bewijs dat voor een* pPD (x, y, z) *het getal* z *niet deelbaar is door* 3 (was dit al opgevallen in de tabel (1.6) ?). (Wat is de bijzondere eigenschap van het priemgetal 3 die dit impliceert?) Zie (16.5).

(2.6) In dit bewijs maken we gebruik van de volgende feiten (precieze informatie vinden we in § 10).
We bestuderen $\mathbb{Z}[i]$ met $i := \sqrt{-1}$; dit heet *de ring van gehele getallen van Gauss*:

$$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

De eenheden van de ring zijn $\{\pm 1, \pm i\}$ (een eenheid is een element waarvan de inverse ook in die ring ligt).
In deze ring is de ontbinding in priemfactoren eenduidig op eenheden en volgorde na.
De priemfactoren in $\mathbb{Z}[i]$ zijn:

(2) het element $1 + i$ is een priemelement; merk op dat

$$2 = -i \cdot (1 + i)^2; \quad \text{merk op dat} \quad 1 - i = -i \cdot (1 + i);$$

(3) elk priemgetal $p \in \mathbb{Z}$ met $p \equiv 3 \pmod 4$ is een priemelement in $\mathbb{Z}[i]$;

(1) elk priemgetal $p \in \mathbb{Z}$ met $p \equiv 1 \pmod 4$ is niet een priemelement in $\mathbb{Z}[i]$; voor een dergelijke p zijn er gehele getallen $b > a > 0$ met

$$a^2 + b^2 = p; \quad p = (a + bi)(a - bi) \quad (3.1);$$

we merken op dat bij gegeven p het paar (a, b) met de conditie als boven uniek is; de elementen $a + bi$, en $a - bi$ in het geval (1) zijn (verschillende) priemelementen van $\mathbb{Z}[i]$.

Merk nog op: *als α een priemelement is in $\mathbb{Z}[i]$ dan is er precies één priemgetal p waar α een deler van is.*
Bewijs: als $\alpha = a + bi$ met $a = 0$ of $b = 0$ dan is dit duidelijk (en in dit geval is $p =\mid a \mid$ of $p =\mid b \mid$ en $p \equiv 3 \pmod 4$). Als $a = \pm 1$ en $b = \pm 1$ dan is α een deler van $p = 2$.Als In alle andere vervallen beschouw $(a - bi)(a + bi) = a^2 + b^2 =: P \in \mathbb{Z}$. Dit getal P heeft geen priemdelers van de vorm $\equiv 3 \pmod 4$, ook $P \neq 2$. Dan heeft P meer dan twee onderling verschillende priemdelers in $\mathbb{Z}[i]$, een tegenspraak.

Met behulp van deze resultaten over $\mathbb{Z}[i]$ geven we een bewijs van Stelling (1.5). Laat (x, y, z) een pPD zijn. We zien:

$$x^2 + y^2 = (x + yi) \times (x - yi) = z^2.$$

We merken nog op dat alle priemdelers van z van de vorm $\equiv 1 \pmod 4$ zijn; bewijs: we weten dat z oneven is, dus $p = 2$ is niet een deler van z. Als $q \equiv 3 \pmod 4$ een deler zou zijn van z, dan weten we dat q een priemelement is in $\mathbb{Z}[i]$, concluderen dat q of $(x + yi)$ of $(x - yi)$; we zien dat q een deler is van $\text{ggd}(x, y)$, tegenspraak,

Stap 1. *Een priemelement $\alpha = x + yi$ dat wel $a + bi$ deelt, deelt niet $a - bi$.*

Stel α deelt zowel $x + yi$ als $x - yi$. Dan deelt het ook $x + yi + x - yi = 2x$ en ook $x + yi - (x - yi) = 2bi$. Zij p hét priemgetal dat deelbaar is door α (er is precies één zo'n priemgetal voor elk priemelement α). Dan deelt p het gehele getal $2a$ en ook het gehele getal $2b$. Omdat $\text{ggd}(a, b) = 1$ impliceert dit $p = 2$. Als $1 + i$ een deler is van $a + bi$ dan zou volgen dat $2 = N(1 + i)$ een deler is van $N(a + bi) = a^2 + b^2 = c^2$; hieruit zou volgen dat 2 een deler is van c, en dat is een tegenspraak met het feit dat a even is en $\text{ggd}(c, a) = 1$. Dit bewijst Stap 1.

Stap 2. *En bestaan $m \in \mathbb{Z}_{>0}$ en $n \in \mathbb{Z}_{>0}$ zodanig dat $a + bi = (m + ni)^2$ en $m > n$.*

Merk op dat voor elk priemelement α dat $a + bi$ deelt er een getal $t \in \mathbb{Z}$ is met: $\alpha^{2t} \mid a + bi$ en α^{2t+1} deelt niet $a + bi$. Inderdaad, een dergelijke α deelt c en niet $a - bi$ dus is de maximale macht van α die $a + bi$ deelt ook de maximale macht die c^2 deelt, dus even. Uit de eenduidige factorontbinding in $\mathbb{Z}[i]$ volgt dat $a + bi =$ (eenheid) $\times$ (kwadraat); schrijf $a + bi = e(m + ni)^2$ met e een eenheid en $m > 0$ ($m = 0$ zou een tegenspraak geven, als m negatief is, dan vermenigvuldigen we met -1 en nemen -1 op in e):

$$a + bi \quad = \quad e \times (m + ni)^2 = e\cdot((m^2 + n^2) + (2mn)i).$$

We zien dat $e \neq -1$. Als we zouden hebben dat $e = +i$ of $e = -i$ dan krijgen we $a + bi = 2mnie + (m^2 + n^2)e$, met als conclusie dat $a = 2mnei$; tegenspraak met het feit dat a oneven is. We zien $e = 1$.

Stap 3: Einde van het bewijs.

We zien dat $a = m^2 - n^2 > 0$; dus is $m > n > 1$; verder is $b = 2mn$. Uit $\text{ggd}(a, b) = 1$ volgt $\text{ggd}(m, n) = 1$. Uit het feit dat a even is volgt dat m en n niet beiden oneven zijn; ook m en n niet beiden even kan niet vanwege $\text{ggd}(m, n) = 1$; dus volgt dat $m + n$ oneven is. QED(1.5)

Opmerking. We zien dat voor een pPD (x, y, z) het getal z een product is van priemgetallen van de vorm $\equiv 1 \pmod 4$ (was dat al opgevallen?).

(2.7) Vraagstuk. Zij $p \in \mathbb{Z}$ een priemgetal met $p \equiv 1 \pmod 4$. Bewijs dat er gehele getallen $B > 0$, $A > 0$ bestaan met

$$p^2 = A^2 + B^2.$$

Bewijs dat er x, y bestaan zodanig dat (x, y, p^2) een PD is. Zie (16.6)

(2.8) Opmerking. Een geheel getal $z \geq 5$ komt voor in een pPD (x, y, z) dan en slechts dan als in de factorontbinding van z er geen enkele priemfactor p optreedt met $p \equiv 3 \pmod 4$ (bewijs dit als vraagstuk). Het vorige vraagstuk is hier en bijzonder geval van.
Voorbeeld. We proberen een pPD te maken met $z = 65$. Schrijf:

$$65 = (2+i)(2-i)(3+2i)(3-2i) = \{(2+i)(3+2i)\}\cdot\{(2-i)(3-2i)\} = (4+7i)\cdot(4-7i),$$

en

$$65 = (2+i)(2-i)(3+2i)(3-2i) = \{(2+i)(3-2i)\}\cdot\{(2-i)(3+2i)\} = (8+i)\cdot(8-i).$$

We zien:

$$4^2 + 7^2 = 65 = 8^2 + 1^2.$$

Laat zien dat dit de enige mogelijkheden zijn.

Het combineren van factoren in de ontbinding van z in $\mathbb{Z}[i]$ geeft zo alle oplossingen. We komen hier nog uitvoerig op terug. Zie (4.8).

3 Sommen van kwadraten

We bestuderen de vraag *welke gehele getallen kunnen optreden als de som van twee kwadraten.* Fermat gaf in 1640 de bewering (maar hij publiceerde niet een bewijs) dat

een oneven priemgetal p geschreven kan worden als de som van twee kwadraten dan en slechts dan als $p \equiv 1 \pmod 4$, zie (3.1).

Euler gaf een bewijs in 1747/1749. Daarna werden nog veel andere bewijzen gegeven. Zie bij voorbeeld de tekst van Gauss hierover, [26], Art 182. Meer informatie is te vinden op:

`http://en.wikipedia.org/wiki/Proofs_of_Fermat's_theorem_on_sums_of_two_squares`

In deze paragraaf geven we een elementair bewijs (Liouville, Heath-Brown, Zagier). In § 4 en in § 10 geven we andere bewijzen.

Wat is het verband met de vorige beschouwingen? Als (x, y, z) een pPD is, dan kunnen we schrijven $z = m^2 + n^2$. Omgekeerd, als $z = m^2 + n^2$ dan is $(m^2 - n^2, 2mn, m^2 + n^2)$ een PD.

We beginnen hier met dit onderwerp, en zullen in § 4 en § 10 de beschouwingen verder afmaken.

We allerlei elementaire observaties maken, maar we beginnen met een centraal resultaat:

(3.1) Stelling (Fermat 1640, Euler 1747/1749). Voor elk priemgetal p met $p \equiv 1 \pmod 4$ bestaan er $a, b \in \mathbb{Z}$ met

$$a^2 + b^2 = p.$$

Opmerking. Allicht laat het geval $p = 2$ ook een dergelijke schrijfwijze toe: $2 = 1^2 + 1^2$. We zullen later zien dat het geval $p \equiv 3 \pmod 4$ niet een dergelijke schrijfwijze toelaat, zie (4.2).

We zullen vier bewijzen geven, (3.2), (4.5), (10.4), (10.5). Het derde bewijs vinden we in § 4 (en daarin gebruiken we iets diepere kennis van de algebra). In deze § geven we een (ondoorzichtig ?) elementair bewijs.

Deze stelling werd aangekondigd door Fermat, maar we weten niet of en welk bewijs hij had. Euler schreef op 12 April 1749 aan Goldbach: *" Nunmehr have ich endlich einen bündigen Beweis gefunden, dass ein jeglicher numerus primus vond dieser Form $4n + 1$ eine summa duor. quadr. sind ...."*, en in die brief geeft hij een bewijs; zie
`https://math.dartmouth.edu/~euler/correspondence/letters/OO0852.pdf`

(3.2) Bewijs van (3.1), zie [34] (Heath-Brown) en [78] (Zagier) (geïnspireerd door methoden van Liouville). Beschouw de verzameling

$$S = \{(x, y, z) \in (\mathbb{Z}_{>0})^3 \mid x^2 + 4yz = p\}.$$

We merken op dat deze verzameling niet leeg is: omdat

$$p \equiv 1 \pmod 4 \quad \text{is} \quad (x = 1, y = 1, z = (p-1)/4) \in S.$$

Merk op: als $x = y - z$ dan is

$$x^2 + 4yz = (y - z)^2 + 4yz = (y + z)^2.$$

Conclusie: als $x^2 + 4yz$ niet een kwadraat is, dan is $x \neq y - z$.
Merk op: als $x = 2y$ dan is $x^2 + 4yz = (4y)\cdot(y + z)$ niet een priemgetal.
Conclusie: voor $(x, y, z) \in S$ geldt $x \neq 2y$

Definieer $\sigma : S \to S$ door middel van:

$$\sigma(x, y, z) = (x + 2z, z, y - x - z) \quad \text{als} \quad x < y - z,$$

$$= (2y - x, y, x - y + z) \quad \text{als} \quad y - z < x < 2y,$$

$$= (x - 2y, x - y + z, y) \quad \text{als} \quad x > 2y.$$

Claim. *Hier zijn alle mogelijkheden beschreven,*

$\sigma^2 = \mathrm{id}_S$ (tweemaal σ achter elkaar toepassen geeft de identiteit) (ga na) (een afbeelding met een dergelijke eigenschap heet een involutie) en

σ heeft precies één denkpunt, m.a.w. $\sigma(x, y, z) = (x, y, z)$ komt precies één keer voor.

Bewijs van deze claim. Ga na (we laten hier details aan de lezer over):

(1) $x \neq y - z$, en $x \neq 2y$; hier gebruiken we dat p een priemgetal is, zoals we eerder lieten zien. Definieer:

$$S \supset S_1 := \{(x, y, z) \in S \mid x < y - z\},$$

$$S \supset S_2 := \{(x, y, z) \in S \mid y - z < x < 2y\},$$

$$S \supset S_3 := \{(x,y,z) \in S \mid x > 2y\}.$$

We zien dat $S = S_1 \cup S_2 \cup S_3$.
(2) $\sigma(S_1) \subset S_3$, en $\sigma(S_3) \subset S_1$ en $\sigma(S_2) \subset S_2$.
(3) $\sigma^2 = \mathrm{id}_S$. (We zien $\sigma(S_1) = S_3$ en $\sigma(S_2) = S_2$.)
(4) $\sigma(x,y,z) = (x,y,z) \Longleftrightarrow (x,y,z) = (x = 1, y = 1, z = (p-1)/4)$.
Hiermede is de claim bewezen.

We geven een voorbeeld van de verificatie, in dit geval van een onderdeel van (2). Onderstel $(x,y,z) \in S_1$; dan is inderdaad $\sigma(x,y,z) \in S$:

$$(x+2z)^2 + 4z(y-x-z) = x^2 + 4xz + 4z^2 + 4zy - 4zx - 4z^2 = p;$$

bovendien:

$$x < y - z \quad \Longleftrightarrow \quad x + 2z > 2z; \quad \text{dus} \quad \sigma(x,y,z) \in S_3.$$

De andere verificaties zijn even eenvoudig.

Conclusie. Het aantal elementen in S is *oneven*. Inderdaad: er is precies één dekpunt en alle andere elementen komen in paren voor, onderling verwisseld door de involutie σ.
Definitie: een afbeelding $\iota : V \to V$ heet een *involutie* als ι niet de identiteit is, d.w.z. er is een $v \in V$ met $\iota(v) \neq v$, en ι^2 is wel de identieke afbeelding, d.w.z. $\iota(\iota(v)) = v$ voor alle $v \in V$.

Beschouw $\tau : S \to S$ gegeven door $\tau(x,y,z) = (x,z,y)$. We zien dat $\tau^2 = \mathrm{id}_S$. Omdat $\#(S)$ oneven is, heeft τ tenminste één dekpunt (een eenvoudig en doeltreffend argument; begrijpt U dit detail?). Voor een dekpunt van τ geldt $y = z$ en

$$x^2 + (2y)^2 = p.$$

QED(3.1)

(3.3) Opmerking/Vraagstuk. (Om gevoel voor de complicaties in het bewijs, reken een voorbeeld door. We zien hoe een abstract bewijs nodig is; voor grote p wordt het expliciet doorrekenen van dit soort voorbeelden een heel werk, maar het abstracte bewijs is "eenvoudig".) *Neem $p = 37$, bepaal S, en bepaal de werkingen van σ en van τ hierop.* Zie (16.7).

(3.4) Opmerking/Vraagstuk. (Om gevoel voor de complicaties in het bewijs te begrijpen is het soms goed om ook een voorbeeld door te rekenen waar het bewijs niet opgaat.)
Neem $N = 65$ en probeer S en σ en τ te definiëren zoals hierboven. Zijn die goed gedefinieerd? Wat zijn dekpunten van σ en van τ? Zie (16.8).

Probeer meer gevoel voor de situatie te krijgen door andere gevallen door te rekenen, bij voorbeeld $x^2 + 4yz = 21$ (met $\#(S) = 4$ heeft τ een dekpunt ?); doe ook $N = 77$, etc.

Conclusie. Ik zie niet in hoe je met methoden van het bewijs hierboven een volledig overzicht kunt krijgen en bewijst welke gehele getallen wel of niet te schrijven zijn als een som van kwadraten, en op hoeveel manieren.

Voor een verdere bespreking van deze methoden zie b.v.
`http://www.math.tugraz.at/~elsholtz/WWW/papers/papers30nathanson-new-address3.pdf`

4 Priemgetallen modulo 4

In deze paragraaf gaan we verder in op het resultaat van Fermat, zie (3.1). We gebruiken resultaten uit § 9 en uit § 10. Voor notaties en symbolen zie ook § 11.

(4.1) We verdelen de verzameling van alle priemgetallen in drie deelverzamelingen:
$\{p = 2\}$;
$\{p \mid p \equiv 1 \pmod 4\}$; deze zullen we hier van Type 1 noemen;
$\{p \mid p \equiv 3 \pmod 4\}$; deze zullen we hier van Type 3 noemen.
(Deze terminologie is niet standaard, maar ik gebruik deze hier om resultaten snel weer te geven). Het is duidelijk dat we zo alle priemgetallen hebben: ga na. Deze indeling zal ook in § 10 een grote rol spelen.

(4.2) Vraagstuk. Als er gehele getallen a en b zijn met $a^2 + b^2 = p$, een priemgetal, dan is p niet van Type 3. Zie (16.9).

(4.3) Vraagstuk. (1) Bewijs dat er voor elk priemgetal p van Type 3 er niet gehele getallen A en k bestaan met bestaan zodanig dat$A^2 + 1 = k \times p$.
(2) Bewijs dat er voor elk priemgetal p van Type 1 met $5 \leq p \leq 97$ er gehele getallen A en k zijn met

$$A^2 + 1 = k \times p.$$

Zie (16.10).

Commentaar. Dit vraagstuk is voor mensen die graag veel rekenen. Veel inzicht krijgen we er wellicht niet mee. Kunnen we voor een willekeurig priemgetal p gehele getallen A en k met deze eigenschap vinden? Het lijkt alsof de rekenpartij aangeeft dat zoiets wel mogelijk zou moeten zijn. Voor elk priemgetal is en eindige hoeveelheid werk nodig om dit te beslissen (probeer voor A alle getallen tussen 1 en p). De rekenpartij lijkt weinig inzicht te geven hoe we zoiets in het algemeen zouden kunnen bewijzen.

(4.4) Om dit algemener te doen kunnen we hebben een hulpmiddel gebruiken, zie § 11:

Voor elk priemgetal p is de multiplicatieve groep $\mathbb{F}_p^*$ cyclisch (zie (11.27));

hieruit volgt dat

voor elk priemgetal van Type 1 *is er een* $\alpha \in \mathbb{F}_p^*$ *is met* $\alpha^2 = -1$.

Inderdaad: als $\mathbb{F}_p^*$ voortgebracht wordt door β, en $\alpha := \beta^{(p-1)/4}$ (hier gebruiken we dat $p - 1$ deelbaar is door 4). Dan is $\alpha \neq 1$ en $\alpha^2 = 1$; dus is $\alpha^2 = -1$. Zie § 11, in het bijzonder (11.27). Het bestaan van een dergelijke α wordt wel het Euler criterium of een lemma van Gauss genoemd.

(4.5) Stelling (Fermat, Euler), zie (3.1). *Voor elk priemgetal van* Type 1 *bestaan er* $A, B \in \mathbb{Z}$ *met*

$$a^2 + b^2 = p.$$

Opmerking, nogmaals. Voor $p = 2$ bestaat er ook een dergelijke schrijfwijze: $2 = 1^2 + 1^2$. Voor elk priemgetal q met $q \equiv 3 \pmod 4$ bestaat een dergelijke schrijfwijze niet, zie (4.2).

Opmerking: Grace' lattice point proof. De essentie van het bewijs dat we gaan geven kan als volgt worden samengevat (zie ook [32], 20.4(2)). Neem $a \in \mathbb{Z}$ met de eigenschap $a^2 \equiv -1 \pmod p$. Beschouw

$$\Lambda := \{(x, y) \mid x, y \in \mathbb{Z}, \quad y \equiv ax \pmod p\}.$$

Merk op dat $(x, y) \in \Lambda$ impliceert dat $x^2 + y^2$ deelbaar is door p. Beschouw de verzameling

$$\Lambda \subset (\mathbb{Z} \times \mathbb{Z}) \subset (\mathbb{R} \times \mathbb{R});$$

merk op: $\Lambda \subset (\mathbb{Z} \times \mathbb{Z})$ is een ondergroep; dit is een voorbeeld van het wiskundige begrip "een rooster" in $(\mathbb{R} \times \mathbb{R})$. Het bewijs laat zien dat er een kortste vector ongelijk aan nul bestaat; daarvan wordt bewezen dat die bovendien de gewenste eigenschap heeft. In het bewijs kiezen we A en B met $\mid A \mid < \sqrt{p}$ en $\mid B \mid < \sqrt{p} + 1$, en we laten zien hoe daarmee het bewijs afgemaakt kan worden. Het is instructief om dit rooster te tekenen voor een eenvoudig geval; zie b.v.
`http://www.math.tugraz.at/~elsholtz/WWW/papers/papers30nathanson-new-address3.pdf`

Bewijs. Kies $a \in \mathbb{Z}$, met $0 < a < p$ zodat $a \bmod p =: \alpha \in \mathbb{F}_p^*$ met $\alpha^2 = -1$ (een dergelijke α bestaat omdat $p \equiv 1 \pmod 4$, zie hierboven, en dus bestaat a; zie (11.27)). Zij t het grootste gehele getal $t < \sqrt{p}$. Wiskundigen schrijven dit getal wel als $[\sqrt{p}]$ waar $[U]$ het grootste gehele getal is met $[U] \leq U$, zie Hoofdstuk 13. Beschouw de getallen $a_i \in \mathbb{Z}$ met $0 \leq a_i \leq p - 1$ en kies

$$a_i \equiv i \cdot a \pmod p, \quad 0 \leq i \leq t, \quad 0 \leq a_i \leq p - 1.$$

Beschouw alle verschillen $\mid a_i - a_j \mid$. Dan zijn er indices I en J met

$$\mid a_I - a_J \mid < \frac{p-1}{t}$$

(want, de a_i geordend in klimmende volgorde geven t verschillen tussen opvolgende termen, en de som van die verschillen is hooguit $p - 1$). Merk op:

$$\frac{p-1}{t} < \frac{p-1}{\sqrt{p}-1} = \sqrt{p} + 1.$$

Schrijf $A = I - J$; merk op $0 < \mid A \mid \leq t$. Omdat $\mid a_I - a_J \mid < \sqrt{p}+1$ en $Aa \equiv a_I - a_J \pmod p$ is er een getal B met

$$B \equiv Aa \pmod p, \quad \text{en} \quad -t - 1 \leq B \leq t + 1.$$

We zien:

$$A^2 + B^2 \equiv A^2(1 + a^2) \pmod p; \quad \text{dus} \quad A^2 + B^2 \equiv 0 \pmod p.$$

Omdat $p \geq 5$ en daarom $2p + 2\sqrt{p} + 1 < 3p$ is

$$A^2 + B^2 < (\sqrt{p})^2 + (\sqrt{p} + 1)^2 = 2p + 2\sqrt{p} + 1 < 3p;$$

dus

$$A^2 + B^2 = p \quad \text{óf} \quad A^2 + B^2 = 2p.$$

Als $A^2 + B^2 = p$ dan zijn we klaar. Als $A^2 + B^2 = 2p$ dan zijn A en B beide oneven (want in dat geval weten we dat $A^2 + B^2 \equiv 2 \pmod 4$); dan zijn $(A \pm B)/2$ beide geheel,

$$(\frac{A+B}{2})^2 + (\frac{A-B}{2})^2 = \frac{A^2+B^2}{2} = p,$$

en ook in dit geval schrijven we p als som van twee kwadraten. QED

(4.6) Een ander bewijs loopt als volgt (dit is in wezen het eerste bewijs in de geschiedenis: het bewijs van Euler door middel van "oneindige afdaling"). Begin met $p \equiv 1 \pmod 4$. Neem alle drietallen van positieve gehele getallen $\{a, b, k\}$ met $a^2 + b^2 = kp$. Er is tenminste één zo'n drietal: met $a^2 \equiv -1 \pmod 4$. Neem een drietal waarvoor de k minimaal is. We zien dat de minimale k minder dan $p/4$ is (waarom ?). Een elementair bewijs laat dan zien dat de minimale k gelijk is aan 1; zie [32], 20.4.

(4.7) Opmerking. (1) Voor en priemgetal p van Type 1 is er precies één schrijfwijze $a^2 + b^2 = p$ met gehele getallen met $0 < a < b$. Dit kunnen we bewijzen met resultaten uit § 10.
(2) Laat zien dat het getal 65 op twee essentieel verschillende manieren als som van twee kwadraten van positieve gehele getallen te schrijven is.
(3) Hoe rekenen we uit op hoeveel manieren een geheel getal N als som van kwadraten te schrijven is?

Definieer getal $\mathrm{sk}(N)$:

$$\mathrm{sk}(N) = \#\left(\{(a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 = N\}\right)$$

Pas op, nu zien we $(1, 2)$ en $(-2, 1)$ etc. als schrijfwijzen van 5 die we nu allemaal apart tellen; ga na: $\mathrm{sk}(5) = 8$. Algemener: voor een priemgetal p van Type 1 is $\mathrm{sk}(p) = 8$ (we kunnen de a en b verwisselen, en elk apart van een plus-teken of een min-teken voorzien). Hier is het recept om voor elke $N > 0$ het getal $\mathrm{sk}(N)$ te berekenen als we de priem-factorizatie van N kennen.

(4.8) Propositie. *Veronderstel dat*

$$N = 2^a \times p_1^{n_1} \times \cdots \times p_s^{n_s} \times q_1^{m_1} \times \cdots \times q_t^{m_t}, \quad a \geq 0, \quad s \geq 0, \quad t \geq 0, \quad n_i, m_j \in \mathbb{Z}_{>0}$$

met priemgetallen

$$p_i \equiv 1 \pmod 4, \quad q_j \equiv 3 \pmod 4.$$

Het getal N is te schijven als som van kwadraten (van gehele getallen) dan en slechts dan als alle exponenten $m_1, \cdots, m_t$ even zijn. Als dat het geval is, en $s = 0$ dan is $\mathrm{sk}(N) = 4$ en voor $s > 0$ is

$$\mathrm{sk}(N) = \mathrm{sk}\left(p_1^{n_1} \times \cdots \times p_s^{n_s}\right) = 4 \times (n_1 + 1) \times \cdots \times (n_s + 1).$$

Opgave. Geef een bewijs. Aanwijzing: gebruik methoden uit § 10.

(4.9) Opmerking. Zijn er "meer" priemgetallen van Type 1 dan van Type 3 of "evenveel", wat kunnen we hier over zeggen? Probeer maar eens die aantallen te tellen onder een kleine grens. B.v. hoeveel zijn er van beide met $p < 100$? Zin om verder te rekenen? Geeft dit inzicht? Een fascinerend onderwerp, de "Chebyshev bias," zie (9.21). In § 9 zien we dat er oneindig veel priemgetallen van Type 1 en van Type 3 zijn.

5 Fermat: FLT_4

Al heel lang geleden bewees Pierre de Fermat dat de uitspraak FLT_4 juist is. We leggen zijn bewijs uit. Hierbij maken we gebruik van PDen, zoals in § 1 en van een methode die wel genoemd wordt "de oneindige afdaling"; zie [73], pp. 75-79 voor dit begrip.

(5.1) Stelling (Fermat). *Als $a, b, d \in \mathbb{Z}$ dan geldt:*

$$a^4 + b^4 = d^2 \quad \Longrightarrow \quad abd = 0.$$

Met andere woorden: de vergelijking $X^4 + Y^4 = T^2$ heeft *geen oplossing in positieve gehele getallen.*

(5.2) Gevolg (Fermat).

FLT_4 *is juist.*

Inderdaad volgt (5.2) direct uit Stelling (5.1). QED(5.2)

Bewijs van (5.1) (zoals Fermat dat al deed). (In dit bewijs gebruiken we de classificatie van Pythagoreïsche drietallen.) Stel er is wel een oplossing van $X^4 + Y^4 = T^2$ in positieve gehele getallen (en we gaan een tegenspraak afleiden).

We nemen onder de verzameling van al zulke oplossingen een oplossing (a, b, d) met minimale $d > 0$ (het begin van "de afdaling"). Dan is het drietal (a^2, b^2, d) een oplossing van $U^2 + V^2 = T^2$, m.a.w. het is een PD. Omdat we d minimaal verondersteld hebben, zien we dat $\mathrm{ggd}(a, b) = 1$; conclusie: bovendien is (a^2, b^2, d) een pPD. Na eventueel a en b te verwisselen kunnen we schrijven

$$a^2 = m^2 - n^2, \quad b^2 = 2mn, \quad d = m^2 + n^2$$

voor geschikte m en n met bovendien $\mathrm{ggd}(m, n) = 1$. Omdat a oneven is volgt $a^2 \equiv 1 \pmod 4$ en daarom is m oneven en n even. Uit

$$m^2 = a^2 + n^2 \text{ volgt } a = s^2 - t^2, \quad n = 2st, \quad m = s^2 + t^2$$

voor geschikte positieve gehele getallen s en t met $\mathrm{ggd}(s, t) = 1$. Uit

$$n \text{ is even, en uit } b^2 = 2mn, \quad \mathrm{ggd}(m, n)$$

volgt dat m en $n/2$ kwadraten zijn. Omdat ook $\mathrm{ggd}(s, t) = 1$ en $n = 2st$ volgt dat s en t kwadraten zijn: er zijn positieve gehele getallen u, v en w met

$$s = u^2, \quad t = v^2, \quad m = w^2.$$

Uit $m = s^2 + t^2$ volgt

$$w^2 = u^4 + v^4;$$

we zien hoe we uit een drietal (a, b, d) een nieuw drietal (u, v, w) maken. Omdat

$$0 < w \leq w^2 = m < m^2 + n^2 = d$$

zien we dat een drietal (u, v, w) verkregen hebben, een oplossing van $X^4 + Y^4 = T^2$ (het einde van "de afdaling"), maar met $w < d$; dit is een tegenspraak met de aanname dat de oplossing (a, b, d) met *minimale* d gekozen was. QED(5.1)

6 Euler: $\mathbf{FLT}_3{}^*$

Het Fermat probleem voor de exponent 3 heeft een interessante en lange geschiedenis. Euler was de eerste die het resultaat claimde en een bewijs publiceerde (1753, 1760, 1770). Een zorgvuldige analyse van zijn bewijs liet zien dat er een lacune in zat. Maar ook zien we dat methoden die Euler gebruikte en publiceerde voldoende zijn om het bewijs compleet te maken. Later hebben vele wiskundigen dit probleem nogmaals bestudeerd; allerlei bewijzen zijn gepubliceerd (Kausler 1802, Legendre 1830, etc.). Voor het bewijs, en voor verwijzingen zie:
`http://en.wikipedia.org/wiki/Proof_of_Fermat's_Last_Theorem_for_specific_exponents`

In het bewijs wordt gebruikt dat in de ring $\mathbb{Z}[\omega]$, met $\omega := (-1+\sqrt{-3})/2$, de factorontbinding eenduidig is (op eenheden en volgorde van de factoren na); deze ring wordt wel de ring van gehele getallen van Eisenstein genoemd. Verder volgde Euler de methode van "oneindige afdaling" reeds door Fermat voor het geval $n = 4$ gebruikt. We bespreken dit bewijs hier niet.

7 Iets over topologie, elliptische krommen en een donut*

In de documentaire komt geregeld een "donut" in het beeld: een ring-figuur. Wat heeft dat met getaltheorie, met het bewijs van FLT te maken? In deze paragraaf geef ik en paar beschouwingen (maar, helaas, kan ik niet volledig en mogelijk ook niet helemaal begrijpelijk zijn). Hier sluit ik aan bij "Grand Unified Mathematics", Hoofdstuk 8 in [S].

In de wiskunde zien we vaak een doorbraak als een probleem in het ene deel van de wiskunde in verband gebracht kan worden iets uit een heel ander deel. Het probleem van Fermat gaat over het oplossen van een vergelijking met gehele getallen. Dat is een onderwerp uit de *(elementaire) getaltheorie*. Maar methoden daaruit hebben niet een oplossing gebracht. Het bewijs dat nu gegeven is (veel werk van grote wiskundigen en Andrew Wiles heeft het afgemaakt) maakt gebruik van *algebraïsche meetkunde*, van *analyse*, en van *topologie*.

In de meetkunde kunnen structuren op heel verschillende manieren beschrijven. Elk van die methoden heeft eigenschappen toegesneden op wat je ermee wilt doen.

Algebraïsche meetkunde. We kunnen figuren beschrijven door middel van algebraïsche vergelijkingen. We zagen in (2.3) de vergelijking van een cirkel; het feit dat een lijn daarmee precies twee of precies één snijpunt heeft gaf een fraai bewijs van de classificatie van PDen. We zullen nog meer, geavanceerde, meetkunde van die vorm tegenkomen.

Analyse. Veel verschijnselen in de natuur en in de wiskunde laten zich niet vangen in de beschrijving met algebraïsche middelen. De vergelijking $\sin(\varphi) = 1/2$ heeft oneindig veel oplossingen; dit is niet een algebraïsche vergelijking. Ook is het vaak zo dat objecten uit de algebraïsche meetkunde een parametrizatie toelaten met analytische middelen. Dat is vaak erg mooi, maar het helpt niet direct bij het oplossen van problemen uit de getaltheorie. Als we bij voorbeeld weten dat $\sin(\varphi)$ een rationaal getal is, dan kunnen we bar weinig zeggen over het al of niet rationaal zijn van φ. Dergelijke vragen (transcendentie van π en nog veel meer) zijn fascinerend, maar hielpen ons niet verder bij het Fermat probleem.

Waarom geeft FLT_2 wel oplossingen (alle PDen), en waarom geeft FLT_n voor $n > 2$ geen oplossingen in positieve gehele getallen? Een deel van de verklaring wordt gegeven door een tak van wiskunde die meetkundige eigenschappen van de kromme gegeven door de vergelijking $X^n + Y^n = Z^n$ bestudeerd. Daarmee bedoelen we dat we alle oplossingen met complexe getallen bestuderen (we verlaten even de getaltheorie) en kijken of we de meetkunde van een dergelijke verzameling kunnen begrijpen.

Topologie. Dat is een vorm van beschouwen van meetkundige structuren waar begrippen als lengte, hoeken, recht of krom, geen rol spelen. Om gevoel hiervoor te krijgen, bestudeer het probleem van de bruggen in Königsberg in [S], Hoofdstuk 3. De vraag of je een wandeling kunt maken waarbij je elke brug precies één keer gebruikt heeft er weinig te maken hoe lang die bruggen zijn, of ze recht of krom zijn, welke hoeken de maken met de oevers; deze beschouwingen van Euler worden gezien als het begin van de "rubber-meetkunde", de topologie. Op college zal ik voorbeelden geven, en verdere beschouwingen.

De topologie van de oplos-verzameling (in $\mathbb{C}$) van $X^n + Y^n = Z^n$ met $n > 2$ blijkt wezenlijk anders te zijn dan de topologie van de oplos-verzameling (in $\mathbb{C}$) van $X^2 + Y^2 = Z^2$. We weten nu dat dergelijke meetkundige eigenschappen een beslissende invloed hebben op het gedrag van getaltheoretische oplossingen (wat een prachtige wiskunde). Een oplossing van FLT leek al meer waarschijnlijk toen Faltings in 1983 een diepe stelling bewees waaruit o.a. volgt dat het aantal primitieve oplossingen van $X^n + Y^n = Z^n$ voor en gegeven $n > 3$ eindig is (de meetkunde impliceert eigenschapen in de getaltheorie).

In de volgende paragraaf zal ik iets zeggen over een idee van Frey, waarna het bewijs van FLT, en in het bijzonder de link naar een vermoeden in het grensgebied van analyse en algebraïsche meetkunde, het STW vermoeden, gelegd werd.

Barry Mazur: *You may never have heard of elliptic curves, but they're extremely important. They're not ellipses. They're cubic curves whose solution have a shape that looks like a doughnut.* (Tekst uit de documentaire.)

Ad hoc definitie. Een elliptische kromme E over $\mathbb{Q}$ is een kromme gegeven door een vergelijking

$$Y^2 = X^3 + aX^2 + bX + c$$

met $a, b, c \in \mathbb{Z}$ en zo dat $X^3 + aX^2 + bX + c = 0$ geen meervoudige oplossingen heeft in $\mathbb{C}$ (?? misschien lijkt dit een vreemde benadering, maar met veel theorie kun je dit beter onderbouwen). Wat we ervaren hebben als wiskundigen is dat de aritmetische eigenschappen

van E veel informatie kunnen geven over allerlei verschillende problemen. Met "de topologie van E" bedoelen we: bestudeer

$$E(\mathbb{C}) = \{(x, y) \mid x, y \in \mathbb{C}, \quad y^2 = x^3 + ax^2 + bx + c\} \cup \{\infty\}.$$

Dat extra punt ∞ ligt op elke verticale lijn. Om U te overtuigen dat dit zinvol is: laat zien dat elke lijn gegeven door een vergelijking $uX + vY + w$ met $u, v, w \in \mathbb{Z}$ deze kromme in precies 3 punten snijdt (als multipliciteiten geteld worden in geval van raken). - Essentie van wat volgt: we kunnen een elliptische kromme b.v. over $\mathbb{Q}$ geven, dan de meetkundige eigenschapen van $E(\mathbb{C})$ bestuderen, en daarna de (diepe) aritmetische eigenschappen over $\mathbb{Q}$ proberen te begrijpen.

Parametrizaties.* Soms kunnen we getaltheoretische problemen oplossen door een parametrizatie te geven; we zagen een mooi voorbeeld in (2.3). Welke krommen zijn te prarmatrizeren? Dat hangt af van de meetkunde op die kromme maar ook van wat we willen.

- Elke kegelsnede met een punt erop is te parametrizeren met rationale functies (en dat is precies het bewijs in (2.3): neem de waaier van lijnen door dat punt).
- Krommen van "hoger geslacht" zijn te parametrizeren met transcendente functies; langs die weg krijgen we geen informatie over de arithmetiek. Dit is in wezen het criterium dat FLT_1 en FLT_2 wel oneindig veel oplossingen toelaten, maar $\mathrm{FLT}_{>2}$ slechts eindig veel primitieve oplossingen toelaten $\mathbb{Z}$ (maar het is wel een diepe stelling van Faltings, 1983): het geslacht van de kromme gegeven door FLT_n is gelijk aan $n(n-1)/2$, eenvoudige meetkunde.
- Een cruciaal detail in het bewijs van FLT is het STW vermoeden, dat in wezen zegt dat *elke elliptische kromme over $\mathbb{Q}$ een parametrizatie met rationale functies toelaat vanaf een goed gekozen "modulaire kromme"* (die we heel goed kennen). Toen dat eenmaal begrepen was, en het verband gelegd tussen FLT en STW (door Frey, Serre en Ribet) kon Wiles beginnen met zijn onderzoek, dat was de doorbraak.

Op het college zal ik een bewijs geven van:

$$\textit{de topologische ruime } E(\mathbb{C}) \textit{ is dezelfde als } T;$$

hierin staat "dezelfde" voor topologische equivalentie. De ruimte T is de torus. Die kunt U maken, visualiseren door een rechthoek te nemen, overstaande zijden in dezelfde richting aan elkaar lijmen (er ontstaat aan cilinder), en daarna de andere overstaande zijden eveneens in dezelfde richting aan elkaar lijmen. (nee, de afmeting van die rechthoek doet er niet toe, en een beetje ongelijk lijmen mag ook, etc.).

Essentie van deze beschouwingen: in de volgende paragraaf laten we zien hoe een hypothetische oplossing van een Fermat vergelijking aanleiding geeft tot een elliptische kromme; dat is een "donut", topologisch begrepen, maar de aritmetische eigenschappen zijn moeilijk te begrijpen; de documentaire verwijst naar dit hulpmiddel door een torus in beeld te brengen. Het bewijs van Wiles laat zien dat die hypothetische elliptische kromme niet bestaat.

Ik ben me ervan bewust dat deze paragraaf veel materiaal bevat dat ik niet kan uitleggen op dit niveau. Wel hoop ik dat U een indruk krijgt van de geavanceerde wiskunde die in het bewijs gaat.

8 Een paar opmerkingen over het bewijs van FLT*

Om het uiteindelijke bewijs van Wiles van FLT te begrijpen is veel moeilijke wiskunde nodig. Maar we kunnen hier wel een paar opmerkingen maken over de logische opbouw van het bewijs. We laten zien waarom directe generalisaties van de bewijzen die we lieten zien voor PDen niet werken voor FLT.

De volgende pogingen hebben niet geleid tot een bewijs:

(8.1) Een bewijs met elementaire middelen? Kunnen we (2.2) generaliseren tot een elementaire benadering die een bewijs geeft? Het lijkt *erg onwaarschijnlijk* dat er ooit zo een bewijs gevonden wordt. Vriendelijk verzoek aan iedereen die wel denkt een dergelijk elementair bewijs gevonden te hebben: controleer het helemaal zelf en stuur het niet aan mij op. Verderop speculeren we wat Fermat dacht dat een bewijs zou geven. Zie ook (9.9).

(8.2) Een bewijs met abstracte algebra? We komen hier uitvoerig op terug. We denken dat Fermat deze weg volgde, maar daarin iets over het hoofd zag. Die fout is in ieder geval vele malen daarna gemaakt, b.v. door G. Lamé in 1847, zie
`http://fermatslasttheorem.blogspot.nl/2006/01/lams-proposed-proof.html`
en zie [14], 4.1. In de 19-de eeuw werd de algebraïsche getaltheorie ontwikkeld. Een generalisatie van (2.4) werkt voor sommige exponenten. Met name Kummer gaf een grote bijdrage, en hij bewees FLT in een groot aantal gevallen; zie [14], Ch. 4, Ch. 5. Echter deze methode (analoog aan (2.4)) bewijst niet FLT_n voor alle gevallen $n > 2$.

(8.3) Zijn grote berekeningen, het gebruik van sterke computers, nuttig voor dit probleem ? Zodra rekenmachines ingeschakeld konden worden heeft men geprobeerd om langs die weg uitsluitsel te vinden omtrent FLT. Als zo een tegenvoorbeeld gevonden zo zijn, dan was het probleem (negatief) opgelost. Dat is niet gebeurd (en zal ook niet gebeuren, zoals we nu weten). Om zulke berekeningen goed uit te kunnen voeren zijn wel slimme methodes ontworpen, en men is "een heel eind" gekomen; het was bij voorbeeld bekend (in 1993) dat voor een exponent $2 < n < 4 \times 10^6$ de uitspraak FLT_n juist is; het was in 1985 ook bekend dat FLT_p juist is voor oneindig veel priemgetallen p; voor een overzicht zie
`http://link.springer.com/article/10.1007/s00407-007-0018-2#page-1`
Zijn we door deze berekeningen zoveel verder gekomen? We kenden geen grens waarboven FLT waar zou zijn. Daarom leek het zoekproces via computers onbegrensd.

(8.4) Meetkundige methoden?* In (2.3) zagen we hoe een "parametrizatie" van de cirkel gegeven door de vergelijking $(x/z)^2 + (y/z)^2 = 1$ inzicht gaf en een fraaie oplossing geeft voor het bepalen van als pPD. Werkt een dergelijke benadering ook voor $(x/z)^n + (y/z)^n = 1$ met $n \geq 3$? Deze meetkundige benadering loop vast: die algebraïsche kromme is niet te parametrizeren met rationale functies, wel met "transcendente functies", maar die geven geen informatie over getaltheorie (meer uitleg op het college). Ook deze generalisatie loopt spaak.

(8.5) Triomf: een bewijs met abstracte middelen (met "pure thought"). Het bewijs begint met eerst de speciale gevallen $n = 3$ (Euler) en $n = 4$ (Fermat) apart te doen. Verder worden in het bewijs van Wiles geen aparte gevallen meer bestudeerd.
Eenvoudige observatie: *voor een getal $n \geq 3$ geldt (tenminste) een van de volgende gevallen:*
n is deelbaar door 3;
n is deelbaar door 4;
n is deelbaar door een priemgetal p met $p \geq 5$.
Conclusie. *Als weten dat* FLT_p *waar is voor elk priemgetal $p \geq 5$ dan geldt* FLT_n *voor elke $n \geq 3$.*
Bewijs. We weten dat een getal n een ontbinding in priemfactoren toelaat. Als $n \geq 3$ en n is niet deelbaar door 4, dan is

ófwel n even, en $n/2$ is oneven en $n/2 \geq 3$; in dit geval is n deelbaar door 3 of deelbaar door een priemgetal p met $p \geq 5$;

ófwel n oneven; in dit geval is n deelbaar door 3 of deelbaar door een priemgetal p met $p \geq 5$. Hiermede zijn alle gevallen nagegaan.

Merk op: als $n = dm$ met $d \in \mathbb{Z}_{\geq 1}$ en FLT_m is juist, dan volgt FLT_{dm}; inderdaad een oplossing van

$$(X^d)^m + (Y^d)^m = (Z^d)^m$$

in positieve gehele getallen zou een oplossing geven van $A^m + B^m = C^m$. QED
Conclusie. *Het is voldoende om* FLT_p *te bewijzen voor elk priemgetal p met $p \geq 5$.*

(8.6)* Lang was het probleem FLT een geïsoleerd probleem. We begrepen niet welke methoden gebruikt konden worden om toegang te krijgen. We zagen dat regelrechte generalisaties van methoden die die werkten voor PDen niet werken voor FLT met $n \geq 3$.

Dat werd anders toen het probleem in verband gebracht werd met een heel andere tak van de wiskunde. Eerdere pogingen (Hurwitz? verwijzing zoeken) van onder andere Yves Hellegouarch werden toen (1971-1975) niet begrepen. Voor verwijzingen zie
`http://www.math.unicaen.fr/~nitaj/hellegouarch.html`

Pas recent werd een relatie met heel andere problemen gezien. De grote doorbraak kwam door een benadering voor gesteld door Günther Frey in 1985. Neem een priemgetal $p \geq 5$ en veronderstel dat er wel een oplossing (a, b, c) van de Fermat vergelijking

$$A^p + B^p = C^p$$

in positieve gehele getallen a, b, c zou bestaan. We proberen te laten zien dat het bestaan van tenminste één oplossing van die vorm voor een gegeven p tot een tegenspraak leidt (en dan zijn we klaar). Om tot die tegenspraak te komen beschouwt Frey de vergelijking

$$E = E_{a,b} : \quad Y^2 = X(X - a^p)(X + b^p)$$

(pas op, een drukfout in [S]). Die vergelijking definieert een "elliptische kromme" en, zoals Frey dat formuleert, en we waren het allemaal met hem eens, heeft die kromme zulke vreemde *arithmetische* eigenschappen, dat het onwaarschijnlijk lijkt dat die kromme zou kunnen bestaan. Na werk van Serre en van Ribet was het verband definitief gelegd met een heel andere tak van de wiskunde. We zouden dit kunnen bewijzen als we een "goede parametizatie" van $E_{a,b}$ zouden kennen; weliswaar kan dat niet met rationale functies, maar misschien wel met behulp van "modulaire functies"; het is niet zo moeilijk om in te zien dat dan het probleem opgelost zou zijn.

Maar dat was een bekend open probleem. Reeds gelanceerd door Y. Taniyama in 1955 (in een vorm die niet helmaal precies was); het vermoeden werd in precieze vorm geformuleerde door André Weil in 1967, zie [72] en bewezen door G. Shimura in een bijzonder geval in 1971, zie [64], 7.5; dat geval is hier niet van toepassing, maar het geeft wel een motivatie om aan het algemene geval te beginnen. Dit wordt wel het Shimura-Taniyama vermoeden genoemd. Ik geef de voorkeur aan de juistere benaming *het Shimura-Taniyama-Weil vermoeden*, afgekort STW.

Deze ontwikkelingen, de suggestie van Frey, en werk van Serre en Ribet lieten zien:

$$\text{STW} \implies \text{FLT}_p \text{ voor alle priemgetallen } p \geq 5.$$

Voor een mooie samenvatting, waarvoor wel geavanceerde wiskunde kennis nodig is, zie
`http://math.berkeley.edu/~ribet/Articles/toulousela.pdf`

Dit was het startpunt van de zoektocht die Andrew Wiles begon. Nu is FLT niet meer een geïsoleerd probleem, maar een gevolg van een vermoeden, dat zich afspeelt in een tak van de wiskunde waar we al heel veel weten, waar Wiles kon beginnen met het ontwikkelen van een bewijs.

9 Appendix: De ring van gehele getallen

De paragrafen §§ 9, 11 en 10 geven een paar van de basis-technieken in elementaire algebra. Deze paragrafen bevatten onvoldoende bewijzen. Als u alle resultaten wilt begrijpen inclusief de bewijzen, dan kunt u literatuur over algebra en over elementaire getaltheorie raadplegen; we noemen: [71], [70], [5], [39], [40], [32], [7], [38], [68], [40], [20]

In deze paragraaf bespreken we een paar eigenschappen van de ring $\mathbb{Z}$, en van het rekenen "modulo n", m.a..w. rekenen in $\mathbb{Z}/n$. (In § 11 geven we een formele definitie van de begrippen "groep", "ring", "lichaam").

(9.1) Definitie. We zeggen dat $d \in \mathbb{Z}$ een *deler* is van $a \in \mathbb{Z}$ als er bestaat een $d' \in \mathbb{Z}$ zodanig dat $d \cdot d' = a$. We noteren dit als $d \mid a$; als c niet een deler is van a dan noteren we dit als $c \not\mid a$.

Een getal $p \in \mathbb{Z}$ heet een *priemgetal* als $p \in \mathbb{Z}_{>1}$ en als elke $1 < i < p$ niet een deler is van p. M.a.w. de enige positieve delers van p zijn 1 en p.

(9.2) Opmerkingen. Er zijn oneindig veel priemgetallen (zoals Euclides al heel lang geleden bewees). Probeer een bewijs te vinden.

Euler, bij voorbeeld, beschouwde 1 ook als een priemgetal; daar is niets op tegen, maar formuleringen worden eenvoudiger als we eisen dat dit niet als priemgetal gezien wordt, zoals nu gebruikelijk is.

Een van de moeilijke problemen in computer-technologie: gegeven een (heel groot) getal, ga na of het een priemgetal is, en zo nee, vind een factorizatie in priemfactoren. In theorie geen probleem (het is wel een priemgetal of je kunt het factoriseren), maar in de praktijk bar lastig.

Belangrijke eigenschap, veel gebruikt in bewijzen:

(9.3) Stelling. *Beschouw $n \in \mathbb{Z}_{>1}$;*

(1) *n kan ontbonden worden als een product van priemgetallen;*

(2) *die ontbinding in priem factoren is uniek op de volgorde na.* Hiermee bedoelen we: *als*

$$n = p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t,$$

waar alle p_i en alle ℓ_j priemgetallen zijn, dan is $s = t$ en na eventueel omnummeren geldt $p_1 = \ell_1, \quad \cdots \quad , p_s = \ell_s$.

We ontwikkelen een methode om dit te bewijzen.

(9.4) Lemma (deling met rest). *Laat gegeven zijn gehele getallen $n, d \in \mathbb{Z}$ met $d > 0$. Dan bestaan er $q, r \in \mathbb{Z}$ zodanig dat:*

$$n = q{\cdot}d + r \quad \textit{met} \quad 0 \leq r < d.$$

Bewijs. Voor elke $j \in \mathbb{Z}$ beschouw

$$I_j = \{jd, jd+1, \cdots jd+d-1\} = \{m \in \mathbb{Z} \mid jd \leq m < (j+1)d\}.$$

Duidelijk: als $j \neq k$ dan is $I_j \cap I_k = \emptyset$ en

$$\mathbb{Z} = \cdots \cup I_{-1} \cup I_0 \cup I_1 \cup I_2 \cup \cdots \ .$$

Hieruit volgt dat er voor elke $n \in \mathbb{Z}$ er precies één $q \in \mathbb{Z}$ is met $n \in I_q$. Dit is equivalent met $n = q{\cdot}d + r$ met $0 \leq r < d$. QED

(9.5) De grootste gemene deler. Voor $a \in \mathbb{Z}$ definiëren we $\mid a \mid$, de absolute waarde van a als volgt: als $a \geq 0$ dan is $\mid a \mid = a$; als $a \leq 0$ dan is $\mid a \mid = -a$.

Zij gegeven $a,\ b \in \mathbb{Z}$, waar tenminsten één van beide niet gelijk is aan 0. We definiëren de grootste gemene deler d van a en b als volgt: beschouw

$$\{\delta \quad \mid \quad 0 \leq \delta \leq \mid a \mid, \quad 0 \leq \delta \leq \mid b \mid, \quad \delta \text{ deelt } a, \quad \delta \text{ deelt } b\};$$

merk op dat deze verzameling niet leeg is (het bevat het getal 1). Bovendien is deze verzameling eindig. Het grootste getal in deze verzameling noteren we als $\mathrm{ggd}(a, b)$, de *grootste gemene deler* $d = \mathrm{ggd}(a, b)$ van a en b. Merk op: voor $a = 0$ geldt $\mathrm{ggd}(0, b) = \mid b \mid$; er geldt $\mathrm{ggd}(a, b) > 0$. Als $\mathrm{ggd}(a, b) = 1$, dan zeggen we dat a en b *onderling ondeelbaar* zijn.

(9.6) Lemma. *Zij gegeven $a,\ b \in \mathbb{Z}$. Schrijf $d := \mathrm{ggd}(a, b)$. Er bestaan $x, y \in \mathbb{Z}$ zodanig dat*

$$xa + yb = d.$$

Bewijs. Als $a = 0$ of $b = 0$, dan is de uitspraak waar (ga na). Neem aan dat $\mid a \mid \geq \mid b \mid$ (zo niet, verwissel dan a en b). Als $\mid b \mid = d$ dan voldoet $x = 0$ en $y = \pm 1$. Neem aan dat $\mid b \mid > d$.

Beschouw alle paren gehele getallen (α, β) zodanig dat $\mid \alpha \mid \geq \mid \beta \mid > 0$ en $\mathrm{ggd}(\alpha, \beta) = d$. We nemen aan (inductie hypothese) dat de uitspraak van het lemma waar is voor alle paren (α, β) als boven met $\mid b \mid > \mid \beta \mid \geq d$. Uit (9.4) volgt dat er bestaat:

$$a = q{\cdot}b + r \quad \text{met} \quad 0 \leq r < \mid b \mid .$$

Ga na: $\mathrm{ggd}(a, b) = \mathrm{ggd}(b, r)$. De inductie hypothese zegt dat we kunnen kiezen $x', y' \in \mathbb{Z}$ met

$$x'{\cdot}b + y'{\cdot}r = d; \quad \text{dus} \quad y'{\cdot}a - q{\cdot}b + x'{\cdot}b = d.$$

Voor $x := y'$ en $y := -q + x'$ krijgen we de gevraagde uitspraak. QED

(9.7) Het algoritme van Euclides in $\mathbb{Z}$. Hier is een meer inzichtelijke vorm van het bewijs van het bovenstaande lemma. Begin met $a_1 = a \geq b = a_2 > 0$ en schrijf $a_1 = q_1 a_2 + a_3$, met $0 \leq a_3 < a_2$. Ga inductief verder

$$a_i = q_i a_{i+1} + a_{i+2}, \quad 0 \leq a_{i+2} < a_{i+1}.$$

Merk op dat $d = \text{ggd}(a_1, a_2) = \ldots = \text{ggd}(a_{i+1}, a_{i+2}) = \cdots$. De rij $a_2 > a_3 > \cdots \geq 0$ is strict dalend en we stoppen als $a_s > 0$ en $a_{s+1} = 0$. "Het algoritme stopt":

$$\cdots, a_{s-2} = q_{s-1} a_{s-1} + a_s, \qquad a_{s-1} = q_{s-1} a_s + 0.$$

Dan volgt $d = \text{ggd}(a_{s-1}, a_s) = a_s$. we passen nu inductie van s naar 2. We zien dat $1 \cdot a_{s-1} - q_{s-1} \cdot a_s = d$. Als

$$\xi \cdot a_{i+1} + \eta \cdot a_{i+2} = d$$

dan volgt

$$d = \xi \cdot a_{i+1} + \eta \cdot (a_i - \eta q_i a_{i+1}) = \eta \cdot a_i + (\xi - \eta q_i) a_{i+1}.$$

Inductie bewijst dat $d = \text{ggd}(a_1, a_2)$ geschreven kan worden als $d = xa_1 + ya_2$ met $x, y \in \mathbb{Z}$.

Een voorbeeld/toepassing. Zij $a = p$ een priemgetal en beschouw $b \in \mathbb{Z}$. Als p een deler is van b dan geldt $\text{ggd}(p, b) = p$. Als p niet een deler is van b dan geldt $\text{ggd}(p, b) = 1$ en er bestaan $x, y \in \mathbb{Z}$ met $xp + yb = 1$.

Bewijs van (9.3)**(1)**. Als n een priemgetal is dan is factorizatie mogelijk (met één priemfactor). Onderstel dat $n > 1$ niet een priemgetal is, en dat factorizatie mogelijk is voor alle m met $1 < m < n$. Omdat n niet een priemgetal is, zijn er echte delers, d.w.z. we kunnen schrijven $a = b \cdot b'$ met $1 < b$ en $1 < b'$. Voor b en voor b' is priemfactorizatie mogelijk (de inductie hypothese). Dus volgt factorizatie voor n. Dit bewijst het bestaan van priem factorizatie voor alle $n \in \mathbb{Z}_{>1}$. Nu nog de eenduidigheid.
(2) Neem aan dat $p_1 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_t$ met $1 \leq s \leq t$ (anders links en rechts verwisselen). Neem als inductie-hypothese aan dat *eenduidigheid bewezen is voor factorizaties van getallen waar ontbinding als een product van i priemgetallen met $1 \leq i < s$ mogelijk is.* Die inductie hypothese is juist als $i = 1$ (in dat geval is n een priemgetal). Schrijf $p = p_1$.
Bewering. Er is een index $1 \leq j \leq t$ zodanig dat $p = \ell_j$.
Bewijs. Als dit niet het geval zou zijn, dan zijn er x_i, y_i met $x_i p + y_i \ell_i = 1$ voor alle $1 \leq i \leq t$. Dan zou gelden

$$p \cdot (p_2 \times \cdots \times p_s)(y_1 \times \cdots \times y_t) = (1 - x_1 p) \times \cdots \times (1 - x_t p).$$

Dit kunnen we herschrijven als

$$p \cdot A = 1 + p \cdot B, \qquad A, B \in \mathbb{Z}; \qquad (A - B) \cdot p = 1.$$

Deze tegenspraak bewijs de bewering.

We zien dat

$$p_2 \times \cdots \times p_s = \ell_1 \times \cdots \times \ell_{j-1} \times \ell_{j+1} \cdots \times \times \ell_t.$$

Uit de inductie-hypothese volgt dat hier eenduidigheid op volgorde na geldt. Dit bewijst ook die eenduidigheid voor $p_1 \cdots p_s = \ell_1 \cdots \ell_t$. Dit bewijst **(2)**. QED(9.3)

(9.8) Waarom zoveel aandacht geven aan iets dat eigenlijk zo vanzelf spreekt?

Er zijn ringen waar het analogon van (9.3) niet juist is. We kunnen natuurlijk flauwe voorbeelden nemen zoals een ring $\mathbb{Q}[a,b,c]$ met $ab = 2 = bc$. Maar hier is een serieuzer voorbeeld.

Voorbeeld. Zij $R = \mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5}\}$. In die ring geldt:

$$2{\cdot}3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Eenvoudig is in te zien dat voor elk van de factoren in beide producten geldt dat $\pm$ die factor en ± 1 de enige delers zijn (m.a.w. die factoren zijn elk niet verder te ontbinden). De eenduidigheid faalt.

Voorbeeld. Anderzijds, zij $R = \mathbb{Z}[\sqrt{-1}]$, de "ring van gehele getallen van Gauss". Met de afbeelding $N : R \to \mathbb{Z}$, met $N(a + b\sqrt{-1}) := a^2 + b^2$, de "norm afbeelding, kunnen we het analogon van (9.6) in deze ring afleiden, en unieke factorizatie in deze ring geldt: op eenheden na, $\pm 1, \pm\sqrt{-1}$, en op volgorde na. Het is niet zo moeilijk om in te zien dat de priem elementen, op eenheden na, in deze ringen alle getallen zijn van de vorm: of $1 + i$ of p, of een rationaal priemgetal $p \equiv 3 \pmod 4$, of $a + b\sqrt{-1}$ waar $N(a + b\sqrt{-1})$ een priemgetal is met $\equiv 1 \pmod 4$. Zie verder § 10.

(9.9) Een speculatie. Wat was het "wonderlijke bewijs" dat Fermat had van zijn stelling (vermoeden) FLT?

Schrijf ζ_p voor een complex getal met $\zeta_p \neq 1$ en $(\zeta_p)^p = 1$. Schrijf $\mathbb{Z}[\zeta_p]$ voor de kleinste deelring van $\mathbb{C}$ die $\mathbb{Z}$ en die ζ_p bevat. Het is niet zo moeilijk om in te zien dat *als* eenduidigheid van van factorizatie (op eenheden en op volgorde na) zou gelden in $\mathbb{Z}[\zeta_p]$, en $p > 2$ is een priemgetal, dan volgt FLT_p. Ik speculeer dat Fermat dit wist (een dergelijk bewijs lag geheel binnen zijn mogelijkheden), en dat Fermat veronderstelde (?!) dat eenduidigheid van factorizatie in $\mathbb{Z}[\zeta_p]$ geldt voor alle priemgetallen p; dit is niet waar; deze "fout" is later in de geschiedenis vaker voorgekomen, ook op een serieus wetenschappelijk niveau (Lamé), en pas na de waarschuwing van Kummer weten we dat het bewijs van FLT zo echt niet gaat. Wel werden allerlei gevallen van FLT zo bewezen met een uitgebreide bestudering van factorizaties in $\mathbb{Z}[\zeta_p]$. Een prachtig stuk wiskunde.
Zie bv.: `https://cs.uwaterloo.ca/~alopez-o/math-faq/mathtext/node9.html`

(9.10) Wanneer werkt dit idee wel? Kummer bewees dat als er in de ring $\mathbb{Z}[\zeta_p]$ unieke factorizate heerst, dan is FLT_p juist; hier is ζ_p een complex getal met $(\zeta_p)^p = 1$ en $\zeta_p \neq 1$. Dat is juist voor bij voorbeeld $p < 23$, maar onjuist voor $p = 23$; zie [14], Chapter 5 voor deze theorie en nog veel meer. Zie
`http://en.wikipedia.org/wiki/List_of_number_fields_with_class_number_one`

In de rest van de paragraaf noemen we een paar aspecten over rekenen modulo n. Dit is een mooie, effectieve methode die eigenlijk heel eenvoudig is. Bovendien werkt iedereen er al mee: we weten best dat een afspraak om 20 : 00 uur plaats vindt om 8 : 00 's avonds, rekenen modulo 12.

(9.11) Rekenen modulo n. Gegeven is een getal $n \in \mathbb{Z}_{>1}$. Beschouw de symbolen

$$\mathbb{Z}/n := \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}.$$

In deze verzameling definiëren we optellen, aftrekken en vermenigvuldigen. We schrijven $\overline{m} = \overline{m - in}$ voor elke $i \in \mathbb{Z}$, en we bestuderen de afbeelding

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n, \quad m \mapsto \overline{m}.$$

Met andere woorden: voor $m \in \mathbb{Z}$ schrijven we $m = dn + r$ met $0 \leq r = r(m) < n$ (delen door n met rest) en we beelden $m \in \mathbb{Z}$ af op $\overline{r(m)} = \overline{r}$. We schrijven $\overline{a} + \overline{b} = \overline{a+b}$ ("optellen modulo n"), en analoog voor $\overline{ab}$ en $\overline{a-b}$.

We kunnen ook zeggen (in terminologie die later ontwikkeld zal worden): $\mathbb{Z}/n$ is een ring, en de natuurlijke afbeelding $\mathbb{Z} \to \mathbb{Z}/n$ is een ring-homomorfisme.
Als we willen benadrukken dat we modulo n werken schrijven we $\overline{m} = m \bmod n$.
Maak goed onderscheid tussen enerzijds $(m \bmod n) \in \mathbb{Z}/n$ (de residu klasse van m modulo n) en anderzijds $a \equiv b \pmod{n}$ (en dat wil zeggen dat $a - b$ deelbaar is door n.

(9.12) In veel gevallen is rekenen modulo n en mooi hulpmiddel. Een getal dat $\equiv 2 \pmod 3$ is niet een kwadraat (waarom niet ?). Ga na.

Een voorbeeld. Heeft de vergelijking $T^2 = 47440033367001212$ een oplossing in $\mathbb{Z}$? [Reken modulo 3.]
Een andere methode: op welke decimaal cijfers eindigen kwadraten in $\mathbb{Z}$? [D.w.z. reken modulo 10.]

Een kwadraat in $\mathbb{Z}$, uitgeschreven in het 10-tallig stelsel eindigt op een van de cijfers: $0, 1, 4, 5, 6, 9$. Geef een bewijs.

Verder zien we: *voor elk priemgetal p heeft elke $0 \neq \overline{a} \in \mathbb{Z}/p$ een inverse.*
Probeer dit te bewijzen. In technische termen: $\mathbb{Z}/n$ is een lichaam dan en slechts dan als $n > 1$ een priemgetal is.

We zullen vaak de volgende stelling gebruiken:

(9.13) Stelling (de Chinese rest-stelling). *Voor $m, n \in \mathbb{Z}$ met $\gcd(m, n) = 1$ is de natuurlijke afbeelding*

$$\mathbb{Z}/(mn) \quad \xrightarrow{\sim} \quad \mathbb{Z}/m \times \mathbb{Z}/n$$

een isomorfisme (een bijectieve afbeelding die $+$ en $\times$ en $-$ behoudt).

(9.14) Voor een getal $n \in \mathbb{Z}_{>0}$ geschreven in het 10-tallig stelstel $n = a_1 a_2 \cdots a_m$ schrijven we $s(n)$ voor de som van die cijfers, d.a..z

$$s(n) = \sum_{i=1}^{i=m} a_i.$$

Merk op dat in dit geval $s(n) \leq 9m$. We zien dat er voor elke n een j is met $0 < s^j(N) < 10$.
Opgave. Bewijs:

als $s^j(n) = 3, 6, 9$ dan is n deelbaar door 3;
als $s^j(n) = 9$ dan is n deelbaar door 9.
Zie (16.11).

(9.15) Voor een getal $n \in \mathbb{Z}$ geschreven in het 10-tallig stelstel $n = a_1 a_2 \cdots a_m$ schrijven we $a(n)$ voor de alternerende som van de decimale cijfers van n:

$$a(n) = \pm(a_1 - a_2 + a_3 - a_4 + \cdots) = \frac{\mid n \mid}{n} \sum_{i=1}^{i=m} (-1)^{i-1} a_i.$$

Opgave. Bewijs:
(n is deelbaar door 11) $\iff$ $a(n) = 0$.
Zie (16.12).

(9.16) Opmerking.* Vaak kunnen we aantonen dat een vergelijking geen oplossingen heeft door te reduceren modulo een geheel getal $n > 1$, en dan eerst te bewijzen dat er modulo n geen oplossing is. In sommige gevallen geeft dit toegang tot het probleem.

We kunnen proberen het proces om te draaien: zoek een oplossing van de vergelijking modulo m voor elke $m > 0$, en los de vergelijking ook op over $\mathbb{R}$; we spreken van het *Hasse principe* als het bestaan van een oplossing in elk van die gevallen impliceert dat de oorspronkelijke vergelijking een oplossing heeft. Echter Selmer gaf de vergelijking

$$3X^3 + 4Y^3 + 5Z^3 = 0; \quad \text{zijn er oplossingen met} \quad x, y, x \in \mathbb{Z}, \quad xyz \neq 0?$$

Selmer bewees daarover: de vergelijking heeft voor elke $n \in \mathbb{Z}_{>1}$ een oplossing in $(\mathbb{Z}/n)^3 - \{0,0,0\}$, en er is een oplossing in $\mathbb{R}^3 - \{0,0,0\}$, maar er is geen oplossing in $\mathbb{Z}^3 - \{0,0,0\}$. Zie [61]. Dat was een doorbraak, en nieuwe methoden werden ontwikkeld om verder te komen.

(9.17) Priemgetallen modulo 4. We gaan zien dat eenvoudig te bewijzen is:
(9.17)(3). *Er zijn oneindig veel priemgetallen* $p \equiv 3 \pmod 4$.
Bewijs (variatie op een bewijs van Euclides). We weten dat $7 \equiv 3 \pmod 4$ (begin: er is er tenminste één). Als we een niet-lege verzameling $\{P_1, \cdots, P_n\}$ hebben met alle $P_i \equiv 3 \pmod 4$, dan construeren we een (nieuw) priemgetal Q met $Q \equiv 3 \pmod 4$ en $Q \notin \{P_1, \cdots, P_n\}$ (via een variant op het bewijs van Euclides): kies

$$M := (P_1 \times \cdots \times P_n)^2 + 2.$$

We zien dat $M > 1$ en $M \equiv 3 \pmod 4$. Daarom hebben niet alle priemdelers van M de eigenschap $\equiv 1 \pmod 4$; dus is er een priemdeler Q van M met $Q \equiv 3 \pmod 4$. QED

Iets moeilijker is:
(9.17)(1). *Er zijn oneindig veel priemgetallen* $p \equiv 1 \pmod 4$; zie (9.19).

(9.18) Propositie* (sommen van kwadraten) *Zij* $A, B \in \mathbb{Z}_{>0}$ *en zij* p *een priemgetal dat wel* $A^2 + B^2$ *deelt maar niet* A *deelt* (en dus ook niet B deelt). *Dan geldt*

$$p \not\equiv 3 \pmod 4.$$

De * geeft aan dat het bewijs niet helemaal elementair is (we gebruiken het begrip groep en een paar eigenschappen uit de groepentheorie). (Een ander bewijs gebruikt resultaten uit § 10.)

Bewijs. Als $p = 2$ dan geldt $p \not\equiv 3 \pmod 4$. Neem aan dat p oneven is.

Schrijf

$$a = \overline{A} =: A \bmod p, \quad b = \overline{B} =: B \bmod p, \quad c = b^{-1} \in \mathbb{F}_p := \mathbb{Z}/p.$$

Uit $p \mid A^2 + B^2$ volgt $a^2 + b^2 = 0 \in \mathbb{F}_p$. Dus $(ca)^2 + 1 = 0 \in \mathbb{F}_p$. We zien dat

$$-1 = (ca)^2 \quad \text{een kwadraat is in } \mathbb{F}_p;$$

bovendien is dit kwadraat ongelijk aan nul. Beschouw $(\mathbb{F}_p)^* := \mathbb{F}_p - \{0\}$. Dit is een (multiplicatieve) groep. Deze groep bevat een element van orde 4, want $(ca)^2 = -1 \neq 1$ en $(ca)^4 = 1$. Uit de stelling van Lagrange, zie (11.7), volgt dat 4 een deler is van $\#((\mathbb{F}_p)^*) = p - 1$. QED

Nu een bewijs van (9.17)(1).

(9.19) Gevolg =(9.17)(1). *Er zijn oneindig veel priemgetallen p met $p \equiv 1 \pmod 4$.*
Bewijs. Veronderstel dat $P_1, \cdots, P_t$ oneven priemgetallen zijn, met $t > 0$. We bewijzen dat er een priemgetal P bestaat met

$$P \equiv 1 \pmod 4 \quad \text{en} \quad P \notin \{P_1, \cdots, P_t\};$$

als dit bewezen is dan volgt de uitspraak van het gevolg.

Neem

$$M := (P_1 \times \cdots \times P_t)^2 + 4.$$

Merk op dat M oneven is. We zien uit (9.18) dat elk priemgetal P dat M deelt de eigenschap $P \equiv 1 \pmod 4$ heeft. Als $P \in \{P_1, \cdots, P_t\}$ zou gelden, dan is

$$P \text{ een deler van } M - (P_1 \times \cdots \times P_t)^2 = 4,$$

en dat is een tegenspraak; dus geldt $P \notin \{P_1, \cdots, P_t\}$; zo construeren we een nieuw priemgetal met $P \equiv 1 \pmod 4$. QED

(9.20) Opmerking. Hier is een andere poging om te bewijzen dat er oneindig veel priemgetallen van de vorm $p \equiv 1 \pmod 4$ bestaan. Voor $A \in \mathbb{Z}$ beschouw $A^2 + 1$. Als $A > 0$ dan is een priemfactor van $A^2 + 1$ óf $p = 2$ of van de vorm $p \equiv 1 \pmod 4$ (ga na). Als we alle mogelijke A nemen dan krijgen we oneindig veel van zulke priemfactoren. Krijgen we hiermee een bewijs dat er oneindig veel priemgetallen van de vorm $p \equiv 1 \pmod 4$ bestaan?

Hoopgevend: voor elk priemgetal p met $p \equiv 1 \pmod 4$ is er een A zo dat p een deler is van $A^2 + 1$ (m.a.w. we krijgen ze allemaal).
Echter: voor elk priemgetal p met $p \equiv 1 \pmod 4$ zijn er oneindig veel gehele getallen A zo dat p een deler is van $A^2 + 1$ (want als $p \mid A^2 + 1$ dan is ook $p \mid (A + p)^2 + 1$, etc.). Dit "bewijs"geeft niet de gewenste conclusie.

We stellen de vraag (Chebyshev, 1835) of priemgetallen $\equiv 1 \pmod 4$ al of niet vaker voorkomen dan priemgetallen $\equiv 3 \pmod 4$. Deze vraag heeft geleid tot een stroom van interessante observaties en nieuwe onderzoekingen. We lichten een tipje van de sluier op.

(9.21) De "Chebyshev bias." Schrijf $\pi_{4,1}(x)$ voor het aantal priemgetallen $p \equiv 1 \pmod 4$ met $p \leq x$; analoog $\pi_{4,3}(x)$ voor het aantal priemgetallen $p \equiv 3 \pmod 4$ met $p \leq x$. Voor kleine x kunnen proberen die beide getallen te berekenen; welk getal lijkt steeds groter? Wat bewezen kan worden (niet heel eenvoudig):

$$\lim_{x\to\infty} \frac{\pi_{4,1}(x)}{\pi_{4,3}(x)} = 1;$$

dit is een bijzonder geval van een veel algemenere stelling "Chebotarev's density theorem" (buiten het bestek van ons college) , zie
`http://en.wikipedia.org/wiki/Chebotarev%27s_density_theorem`

(9.22) In een brief in 1835 schrijft Chebyshev aan Fuss dat het lijkt alsof $\pi_{4,3}(x) > \pi_{4,1}(x)$ voor elke x (en dat was ons wellicht al opgevallen, als we een aantal gevallen hadden doorgerekend). Dit heet nu de "Chebyshev's bias" ("bias": vooroordeel). Het bleek een pracht idee, dat weliswaar niet juist bleek, maar dat toch fascinerende wiskunde opleverde. Zie
`http://arxiv.org/pdf/1210.6946v1.pdf`

Littlewood bewees in 1914:

$$\pi_{4,3}(x) - \pi_{4,1}(x) \textit{ wisselt oneindig vaak van teken } x \to \infty.$$

Zie [44]. Nauwkeurige resultaten staan in [59]. In het prachtige artikel [28] over dit mooie onderwerp zien we dat Chebyshev "bijna gelijk had": voor "veel" waarden van x is $\pi_{4,3}(x) > \pi_{4,1}(x)$.

We zien een voorbeeld dat een "eenvoudige vraag", nieuwsgierigheid, kan leiden tot bespiegelingen en diepe resultaten (zoals zo vaak in de wiskunde). Ook zien we dat berekeningen, zelfs bij een groot wiskundige als Chebyshev, tot verkeerde verwachtingen kan leiden.

(9.23) Priemgetallen modulo 3. We gaan zien dat eenvoudig te bewijzen is:
(9.23)(2). *Er zijn oneindig veel priemgetallen* $p \equiv 2 \pmod 3$.
Geef zelf een bewijs. Hint: $(P_1 \times \cdots \times P_t)^2 + 2$.

Iets moeilijker is:
(9.23)(1)*. *Er zijn oneindig veel priemgetallen* $p \equiv 1 \pmod 3$.
We geven een schets van een bewijs; daarbij gebruiken we methoden die niet helemaal elementair zijn.

Feit.*

$$\begin{array}{c} \textit{voor } p \equiv 1 \pmod 3 \textit{ is } -3 \bmod p \in \mathbb{Z}/p \textit{ wel een kwadraat.} \\ \textit{voor } p \equiv 2 \pmod 3 \textit{ is } -3 \bmod p \in \mathbb{Z}/p \textit{ niet een kwadraat.} \end{array}$$

We geven niet een bewijs. Maak voorbeelden om te zien of dit werkt in die gevallen. (Een bewijs volgt uit de zogenaamde kwadratische reciprociteitswet, die we niet behandelen.)

Gevolg. *Zij* $B \in 2\mathbb{Z}_{>0}$ *een even positief geheel getal dat niet deelbaar is door* 3.

$$p \textit{ is priem en } p \mid B^2 + 3 \quad \Longrightarrow \quad p \equiv 1 \pmod 3$$

en p is oneven.
Inderdaad, omdat B even is, is B^2+3 oneven, en dus is $p \neq 2$. Omdat B niet deelbaar is door 3 volgt dat $p \neq 3$. Uit $p \mid B^2+3$ volgt dat $-3 \bmod p \in \mathbb{Z}/p$ een kwadraat is; hieruit volgt $p \equiv 1 \pmod 3$. QED

Bewijs van (9.23)(1). We zien dat $7 \equiv 1 \pmod 3$. Laat $\{P_1, \cdots, P_t\}$ een niet-lege verzameling priemgetallen zijn met $P_i \equiv 1 \pmod 3$ voor alle i. Schrijf

$$B := 2 \times P_1 \times \cdots \times P_t \quad \text{en} \quad M := B^2 + 3.$$

Een priemdeler Q van M is oneven, niet deelbaar door 3 en $Q \equiv 2 \pmod 3$ zoals we zien uit het bovenstaande gevolg. Ook zien we $Q \notin \{P_1, \cdots, P_t\}$. QED

(9.24) Opgave. Vind $a \in \mathbb{Z}$ met $a^2 \equiv -3 \pmod{37}$. Zie (16.13).

(9.25) Opgave. Voor welk(e) priemgetal(len) geldt:

$$15^2 \equiv -3 \pmod p \ ?$$

Zie (16.14).

(9.26) Een voorbeeld van het rekenen modulo n. We laten zien dat 641 een deler is van F_5 (voor het eerst gesignaleerd dor Euler). We zien:

$$641 = 640 + 1 = 5{\cdot}2^7 + 1 = 625 + 16 = 5^4 + 2^4.$$

Dit geeft

$$5{\cdot}2^7 \equiv -1 \pmod{641}, \text{ dus } 5^4{\cdot}2^{4\times 7} \equiv +1 \pmod{641};$$

daarom

$$-2^4{\cdot}2^{28} \equiv 5^4{\cdot}2^2 8 \equiv +1 \pmod{641}; \text{ dus } F_5 \equiv 0 \pmod{641}.$$

QED

10 Appendix: De ring van gehele getallen van Gauss

(10.1) We bespreken een ring die eigenschappen heeft die heel veel lijkt op die van de ring $\mathbb{Z}$. We geven een toepassing van de factorontbinding in deze ring. In deze § zal de notatie i niet gebruikt worden als index, maar als $i = \sqrt{-1}$. We schrijven:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\};\ \text{de ring van gehele getallen van Gauss.}$$

In deze verzameling is optellen, aftrekken, 0 en 1 gedefinieerd. Verder gebruiken we $i^2 = -1$ om de vermenigvuldiging te krijgen. We gebruiken het woord "priemgetal" voor een element $p \in \mathbb{Z}$ dat in die ring een priemgetal is. In de ring $\mathbb{Z}[i]$ zijn de elementen $1, i, -1, -i$ eenheden (elementen die een inverse in $\mathbb{Z}[i]$ hebben). We gebruiken in deze § het woord *priemelement* voor een element $\alpha \in \mathbb{Z}[i]$ dat niet een eenheid is, niet 0 is en niet een ontbinding toelaat $\alpha = zt$ waar z en t geen eenheden zijn.
Voorbeelden; $2 = 2 + 0{\cdot}i$ is niet een priemelement, want $2 = (1+i)(1-i) = i(1-i)^2$.
We zullen zien dat het priemgetal 3 wel een priemelement (in $\mathbb{Z}[i]$) is (ga na).
Merk op dat $5 = (2+i)(2-i)$. We zien dat 5 wel een priemgetal is (in $\mathbb{Z}$), maar niet een priemelement (in $\mathbb{Z}[i]$).
Probeer zelf na te gaan welke priemgetallen wel en welke niet een priemelement zijn.

(10.2) Stelling. *In de ring $\mathbb{Z}[i]$ geldt eenduidigheid van ontbinding in priemelementen, op volgorde, en op eenheden na.*
Bewijs*. Geef

$$N : \mathbb{Z}[i] \to \mathbb{Z} \text{ door } N(a+bi) := a^2 + b^2$$

(wel de "norm-afbeelding" genoemd, vandaar de letter N). Laat zien dat

$$N(\beta{\cdot}\gamma) = N(\beta){\cdot}N(\gamma).$$

Conclusie. *De verzameling van eenheden in $\mathbb{Z}[i]$ is* $\{\pm 1, \pm i\}$ (een eenheid is een element ε zodanig dat er een element ε' bestaat met $\varepsilon{\cdot}\varepsilon' = 1 = \varepsilon'{\cdot}\varepsilon$). Bewijs: als $\varepsilon{\cdot}\varepsilon' = 1$ dan is

$$N(\varepsilon){\cdot}N(\varepsilon') = 1;$$

we zien dat ± 1 en $\pm i$ de enige mogelijkheden zijn in $\mathbb{Z}[I]$.
Claim. *Voor elementen $\beta, \delta \in \mathbb{Z}[i]$ met $\delta \neq 0$ zijn er $\gamma \in \mathbb{Z}[i]$ en $\rho \in \mathbb{Z}[i]$ met*

$$\beta = \gamma{\cdot}\delta + \rho \text{ met} N(\rho) < N(\delta)$$

("deling met rest"; deze eigenschap heet de Euclidische eigenschap van de ring). Een bewijs volgt door in te zien dat cirkels met straal 1 om de punten van $\mathbb{Z}[i]$ in $\mathbb{R} \times \mathbb{R}$ het hele vlak overdekken; pas dit toe op β/γ.

Algemene theorie: in een commutatieve ring R met een afbeelding $N \to \mathbb{Z}$ waar de Euclidische eigenschap geldt geldt uniciteit van factorontbinding in irreducibele elementen (op volgorde en eenheden na). QED

(10.3) Stelling (Fermat, Euler), zie (3.1). *Elk priemgetal p met $p \equiv 1 \pmod 4$ kan geschreven worden als*

$$p = a^2 + b^2, \quad a, b \in \mathbb{Z}_{>0}.$$

Opmerking. Die schrijfwijze is uniek op verwisselen van a en b na (geef zelf een bewijs).

(10.4) Bewijs van (10.3) (Dedekind, 1894). Stap 1. *Er is een getal $d \in \mathbb{Z}$ met $d^2 \equiv -1 \pmod 4$.*

Inderdaad, $(\mathbb{Z}/p)^*$ is een multiplicatieve, cyclische groep van orde $p-1$, en 4 is een deler van $p-1$; dus is er een element $(d \bmod 4) \in (\mathbb{Z}/p)^*$ van precies orde 4.
(Expliciet: zij $p = 4r+1$; laat zien dat $d := (2r)! = 1 \times 2 \times \cdots \times (2r-1) \times (2r)$ de eigenschap $d^2 \equiv -1 \pmod 4$ heeft; geef een bewijs. Zie (11.27).)

Stap 2. *Neem d als in* Stap 1. *Dan is p een deler is van d^2+1.* Dat volgt uit $d^2 + 1 \equiv -1 \pmod 4$. *Daarom is p niet een priemelement van $\mathbb{Z}[i]$.* Inderdaad,

$$p \quad \text{een deler is van} \quad d^2 + 1 = (d+i)(d-i),$$

maar p is niet deler van $(d \pm i)$, want $p{\cdot}(u+vi) = d \pm i$ zou impliceren dat $pv = \pm 1$.

Stap 3. *Voor een priemdeler $a+bi$ van p geldt $a^2+b^2 = p$.* Inderdaad

$$N(a+bi) = a^2 + b^2 \neq 1 \quad \text{want} \quad a+bi \quad \text{is niet een eenheid,}$$

en omdat $a + bi$ een deler is van p zien we

$$N(a + bi) \text{ deelt } N(p) = p^2, \quad \text{maar } N(a^2 + b^2) \neq N(p),$$

want p is niet een priemelement in $\mathbb{Z}[i]$. Dus $N(a + bi) = p$, dus

$$a^2 + b^2 = p.$$

QED

(10.5) Hier is een ander bewijs van (3.1)*. We maken gebruik van Stelling (10.2), en schetsen een bewijs dat gebruik maakt van meer geavanceerde methoden. Neem de ring $\mathbb{Z}[i]$, een priemgetal p met $p \equiv 1 \pmod 4$ en een element $\alpha \in \mathbb{F}_p = \mathbb{Z}/p$ met $\alpha^2 = -1 \in \mathbb{F}_p$ (voor een verwijzing, en een argument, zie boven). Geef een ringhomomorfisme

$$\varphi : \mathbb{Z}[i] \longrightarrow \mathbb{F}_p \text{ door } i = \sqrt{-1} \mapsto \alpha.$$

Beschouw

$$I = \{\rho \mid \rho \in \mathbb{Z}[i], \quad \varphi(\rho) = 0\}.$$

Omdat unieke factorizatie in $\mathbb{Z}[i]$ geldt is er een element $\tau \in I$ zodanig dat elk element van I een veelvoud is van τ. Het is eenvoudig om in te zien dat voor $\tau = a + bi$ er geldt $a^2 + b^2 = p$. QED

(10.6) Stelling. *De priemelementen (op eenheden na) in $\mathbb{Z}[i]$ zijn:*

(2) $1 + i$*;*

(3) *elk priemgetal $p \in \mathbb{Z}$ met $p \equiv 3 \pmod 4$;*

(1) *elk element $a + bi$ zo dat $a^2 + b^2 = p$ een priemgetal is, met $p \equiv 1 \pmod 4$.*

Een bewijs is niet zo moeilijk (raadpleeg de literatuur of geef zelf een bewijs). Gebruik vooral de afbeelding $a + bi \mapsto N(a + bi) = a^2 + b^2$.

(10.7) Nog een **bewijs** van (10.3). In dit bewijs gebruiken we (10.2). Inductie aanname: de uitspraak is reeds bewezen voor alle $q < p$ met $q \equiv 1 \pmod 4$. We nemen $d \in \mathbb{Z}$ met $1 < d < p/2$ en $d^2 \equiv -1 \pmod p$. We kiezen $y = 1$ en $x = d$. Dan geldt $x^2 + y^2 \equiv 0 \pmod p$; schrijf $x^2 + y^2 = ep$. Als een priemgetal $r \equiv 3 \pmod 4$ een deler zou zijn van e dan is r een deler van x en van y; dit bewijzen we als volgt: uit (10.6) volgt dat r een priemelement in $\mathbb{Z}[i]$ is; we zien dat r een deler is van $(x + iy)(x - iy)$; dus is r een deler van tenminste een van deze factoren; uit $r(a + ib) = x \pm iy$ volgt dat r en deler is van x en een deler van y (delers in $\mathbb{Z}$). Uit deze tegenspraak volgt dat een priemgetal s dat e deelt of gelijk is aan 2 of $s \equiv 1 \pmod 4$. We geven een definitie van $e_+, e_- \in \mathbb{Z}[i]$.
Voor een priemgetal s dat e niet deelt schrijven we $e_+(s) = 1 = e_-(s)$.
Als 2^t een deler is van e en 2^{t+1} is niet een deler is van e dan schrijven we

$$e_+(2) = (1 - i)^t = e_-(2).$$

Als s^t een deler is van e en s^{t+1} is niet een deler is van e met $s \equiv 1 \pmod 4$ en $t > 0$, dan

weten we dat $s < p$; volgens de inductie aanname kunnen we kiezen $u + vi$ een deler van $d + i$, dan is $u - vi$ een deler van $d - i$, en $u^2 + v^2 = s$; we schrijven

$$e_+(s) = (u + vi)^t, \quad e_-(s) = (u - vi)^t.$$

We nemen $e_+ = \prod_s \ e_+(s)$ en $e_- = \prod_s \ e_-(s)$. We zien:

$$N(e_+) = e = N(e_-), \quad \text{en} \quad a' + b'i := di + 1/e_+; \quad a :=\mid a' \mid, \quad b =\mid b' \mid$$

geeft $a^2 + b^2 = N(a + bi) = N(d + i)/Ne_+) = p$. Conclusie:

$$0 < a < p/2, \quad 0 < b < p/2, \quad a^2 + b^2 = p.$$

QED

(10.8) Een voorbeeld. Neem $p = 29$. Dan is $d = 12$, want $12^2 = 144 = 5{\cdot}29 - 1$. Hier is $e = 5 = (2 + i)(2 - i)$. Er geldt

$$12 + i = (2 + i)(5 - 2i); \quad a = 2, \quad b = 5 \text{ geeft } 2^2 + 5^2 = 29.$$

Nog een voorbeeld: $p = 89$, $d = 34$. Dan is $d^2 + 1 = 1757 = 13 \times 89$; $N(d + i) = ep$ met $e = 13$. Wat zijn a en b in dit geval?

(10.9) Opgave. Neem $p = 41$, vind d met $1 < d < p/2$ en $d^2 \equiv -1 \pmod{41}$. Vind all paren (x, y) met $0 < x < p/2$, en $0 < y < p/2$, en $x^2 + y^2$ deelbaar door p; voor elk van die paren schrijf $x^2 + y^2 = e(x, y) \times p$; welke $e(x, y)$ komen voor? Zie (16.15).

11 Appendix: Groepen, ringen en lichamen

Ter herinnering. Deze § geeft een samenvatting van een paar feiten die we gebruiken, maar dit is niet een volledig dictaat over deze theorie. Voor verwijzingen zie het begin van § 9. De essentie van deze begrippen kwam veelvuldig voor in de wiskunde. Van een goede formalisering en van een abstract definiëren van deze begrippen kwam de theorie pas in de periode, ruwweg, 1890 - 1930 in focus (maar nog na 1960 hoorde ik een wiskundige vragen: “is dit een concrete of een abstracte groep?”)

We zullen de begrippen “groep”, “ring” en “lichaam” veelvuldig tegenkomen. Dit zijn abstract algebraïsche begrippen. Deze stroomlijnen argumenten, en maken vaak ingewikkelde situaties transparant. Het formaliseren van deze begrippen heeft in de wiskunde een enorme ontwikkeling gebracht.

(11.1) We beginnen met een paar voorbeelden, en zullen daarna dan de abstracte definitie geven.

(11.1)**(1)** In de verzameling $\mathbb{Z} = \{\cdots, -1, 0, 1, 2, \cdots\}$ van de gehele getallen kunen we:

optellen; voor $a, b \in \mathbb{Z}$ is $a + b \in \mathbb{Z}$ gedefinieerd; bovendien geldt (associatieve wet): $a + (b + c) = (a + b) + c$, m.a.w. de volgorde van optellen doet er niet toe;

er is een element $0 \in \mathbb{Z}$ waarvoor geldt $a + 0 = a = 0 + a$ voor alle $a \in \mathbb{Z}$;

tegengestelde: voor elke $a \in \mathbb{Z}$ is er een $-a \in \mathbb{Z}$ met $a + (-a) = 0 = (-a) + a$.

(11.1)**(2)** Het vorige voorbeeld beschrijft een oneindige groep. Hier is een voorbeeld van een eindige groep. Beschouw de verzameling

$$\mathbb{Z}/5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$$

bestaande uit 5 elementen. Hierin kunnen we optellen "modulo 5"; bij voorbeeld $\overline{3} + \overline{4} = \overline{2}$. Met deze optelling krijgen we dezelfde eigenschappen als boven (associativiteit, nul-element, tegengestelde). Zie (9.11).

(11.1)**(3)** In de vorige voorbeelden werd de "operatie" in de groep additief geschreven. maar soms is een multiplicatieve schrijfwijze meer voor de hand liggend. Beschouw de verzameling

$$(\mathbb{Z}/5)^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}.$$

Hierin kunen we "vermenigvuldigen modulo 5. We krijgen analoge eigenschappen als boven (associativiteit, een-element, inverse). Bijvoorbeeld $\overline{2} \times \overline{3} = \overline{1}$, en we schrijven $\overline{3}^{-1} = \overline{2}$.

(11.1)**(4)** In alle voorgaande voorbeelden was de groeps-wet commutatief; dat wil zeggen $a + b = b + a$, respectievelijk $a \times b = b \times a$. Maar we kunnen ook voor beelden beschouwen waar de groeps-wet niet commutatief is. Beschouw de verzameling S_3 van all permutaties van 3 symbolen; laten we die symbolen $1, 2, 3$ noemen. Een permutatie is een handeling die deze symbolen op een (mogelijk andere) manier opschrijft. We kunnen een permutatie definiëren als een bijectieve afbeelding $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$.

Bij voorbeeld schrijven we $\sigma(12)$ voor de permutatie die 1 en 2 verwisselt en 3 op zijn plaats laat. We schrijven $(12)1 = 2$, $(21)2 = 1$ en $(12)3 = 3$ (we zien de permutatie als een soort "functie-symbool", opererend van links). Idem voor de permutatie (13). De groeps-wet is achter elkaar uitvoeren van de permutaties. We zien:

$$(12)(13)1 = 3, (12)(13)2 = 1, (12)(13)3 = 2,$$

en

$$(13)(12)1 = 2, (13)(12)2 = 3, (13)(12)3 = 1.$$

Uitleg van de berekening $(12)(13)1 = 3$. We zien dat eerst (13) werkt, en onder die werking gaat 1 in 3 over. Dan krijgen we: $(12)(13)1 = (12)3 = 3$. Ga alle andere identiteiten hierboven op deze manier na. We kunnen inzien dat met deze groeps-wet en met één-element de identieke permutatie (alles blijft op zijn plaats) aan de regels voldaan is. Echter

$$(12)(13) \neq (13)(12);$$

inderdaad, we zien dat deze twee permutaties verschillend zijn. Deze groepen van permutaties hebben heel veel toepassingen.

(11.1)**(5)** Beschouw twee symbolen a en b. Zij G de verzameling van alle woorden in de letters a en b waarin de combinatie aa en bb niet voorkomen. Het lege woord noteren we als e. We maken een groeps-wet in G, genoteerd als $*$, door woorden achter elkaar te zetten, maar zodra aa voorkomt schrappen we dat, zodra bb voorkomt schrappen we dat. Dit geeft b.v. $a * a = e$,

$b * b = e$, $aba * ab = a$, etc. Ga associativiteit na. Voor elk element is er een inverse, bv. de inverse van *ababab* is *bababa*, want

$$(ababab) * (bababa) = (ababa) * (ababa) = (abab) * (baba) =$$

$$= (aba) * (aba) = (ab) * (ba) = (a) * (a) = e.$$

We krijgen weer een verzameling met een groeps-wet. Die groepswet is niet-commutatief: $ba \neq ab$. Deze groep is niet-commutatief en niet eindig. Overigens: zulke groepen zullen in onze cursus niet voorkomen, maakt U zich geen zorgen hierover.

Als we zo door deze voorbeelden heen werken, dan voelen we aan dat een begrip dat deze situaties systematiseert de verwarring die we bij deze steeds ingewikkelder voorbeelden zien kan

(11.2) Definitie. Een groep is een viertal $(G, *, e, i)$ bestaand uit: een niet-lege verzameling G een "groeps-wet" die aan elke $x, y \in G$ een element $x * y \in G$ toevoegt, een element $e \in G$, en een afbeelding $i : G \to G$, zodat voldaan is aan:
(ass) voor alle $x, y, z \in G$ geldt $x * (y * z) = (x * y) * z$;
(eenh) voor elke $x \in G$ geldt $x * e = e * x$;
(inv) voor elke $x \in G$ is er een $i(x) \in G$ met $i(x) * x = e = x * i(x)$.

Met deze abstracte definitie in de hand, ga de voorbeelden hierboven nog een keer na.

We spreken vaak van "de groep G" als we bedoelen een viertal $(G, *, e, i)$ waar de andere symbolen een duidelijke betekenis hebben.We spreken b.v. van de groep $\mathbb{Z}$ van de gehele getallen, en laten de symbolen $+$, $e = 0$ en $a \mapsto i(a)$ weg.

We gebruiken de additieve schrijfwijze niet voor een niet-commutatieve groep. Maar verder worden zowel additieve schrijfwijze als de multiplicatieve schrijfwijze voor eenzelfde object gebruikt (en dat is juist de kracht van deze theorie).

We zegen dat een groep G *abels* is als de groeps-wet commutatief is. (Hier eren we de grote Noorse wiskundige Niels Henrik Abel.)

(11.3) Definitie. We zeggen dat twee groepen G en H *isomorf* zijn als er een bijectieve afbeelding $\varphi : G \to H$ met $\varphi(e_G) = e_H$, en $\varphi(x * y) = \varphi(x) * \varphi(y)$.

Voor een groep G en een deelverzameling $M \subset G$ zeggen we dat M een *ondergroep* is van G als M het eenheidselement van G bevat, voor elke $x \in M$ ligt ook x^{-1} in M en voor alle $x, y \in M$ ligt ook $x * y$ in M. In dit geval is M, met de geïnduceerde structuur een groep.

(11.4) Een voorbeeld. We laten zien dat $\mathbb{Z}/4$ en $(\mathbb{Z}/5)^*$ isomorf zijn (is dat niet verwarrend .. ?). Schijf

$$\mathbb{Z}/4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}, \quad (\mathbb{Z}/5)^* = \{\tilde{1}, \tilde{2}, \tilde{3}, \tilde{4}\};$$

in de eerste groep: optellen modulo 4; in de tweede groep: vermenigvuldigen modulo 5. Geef φ door:

$$\varphi(\overline{1}) = \tilde{2}, \quad \varphi(\overline{2}) = \tilde{2}^2 = \tilde{4}, \quad \varphi(\overline{3}) = \tilde{2}^3 = \tilde{3}, \quad \varphi(\overline{0}) = \tilde{1}.$$

Ga na dat dit een isomorfisme geeft. Is er nog een ander isomorfisme tussen deze twee groepen?

(11.5) Definitie. Zij G een groep (multiplicatief geschreven). We zeggen dat G *cyclisch* is als er een element $g \in G$ is (een "voortbrenger") zodat dat voor elke $x \in G$ er een $i \in \mathbb{Z}$ is met $x = g^i$ (additieve schrijfwijze: $x = ig$).
Voorbeeld. De additieve groep $\mathbb{Z}$ is cyclisch. Voor elke $n \in \mathbb{Z}$ is $\mathbb{Z}/n$ cyclisch. Ga na: de groep $(\mathbb{Z}/8)^*$ is niet cyclisch. De groep $(\mathbb{Z}/17)^*$ is cyclisch (vind een voortbrenger; let op: multiplicatieve schrijfwijze).

(11.6) Zij G een groep, multiplicatief geschreven, en $x \in G$. We zeggen dat n de *orde* is van x, notatie $\text{orde}(x) = n$ als $n \in \mathbb{Z}_{>0}$, en $x^n = 1$ en voor $1 \leq i < n$ geldt $x^i \neq e$. M.a.w. de orde is de kleinste exponent j nodig om $x^j = e$ te krijgen. Als er een dergelijke exponent niet bestaat dan schrijven we $\text{orde}(x) = \infty$.
Opmerking. Als $x \in G$ en de orde van x is oneindig dan is de ondergroep $\{\cdots, x^{-2}, x^{-1}, e, x, \cdots, x^i, \cdots\}$ isomorf met $\mathbb{Z}$ (additief geschreven). Als $x \in G$ en de orde van x is gelijk aan $n \in \mathbb{Z}_{>0}$ dan is $\{e, x^1, \cdots, x^{n-1}\}$ een ondergroep en die is isomorf met $\mathbb{Z}/n$.
Opmerking. Als G een groep is, dan geven we met $\#(G)$ het aantal elementen in G aan (oneindig of eindig). Dit wordt de orde van G genoemd. Raak niet in verwarring door "de orde van een groep" en "de orde van een element in een groep".

(11.7) Stelling (Lagrange). *Zij G een eindige groep en zij $x \in G$. Dan is*

$$\textit{de orde } \text{orde}(x) \textit{ van } x \textit{ een deler van } \#G, \textit{ de orde van } G.$$

Voor een bewijs: geef het zelf, of raadpleeg de literatuur.

(11.8) Lemma. *Zij G een eindige* abelse *groep.*
(1) *Voor $x, y \in G$ is* $\text{orde}(xy)$ *een deler van* $\text{kgv}(\text{orde}(x), \text{orde}(y))$.
(2) *Voor $x, y \in G$ met* $\text{ggd}(\text{orde}(x), \text{orde}(y)) = 1$ *geldt* $\text{orde}(xy) = \textit{orde}(x) \times \text{orde}(y)$.
(3) *Schrijf m voor het grootste getal dat voorkomt als orde van een element in G:*

$$m := \max_{x \in G} \text{orde}(x).$$

(Dit getal wordt wel de exponent van de abelse groep G genoemd.) *Dan geldt: voor elke $y \in G$ is* $\text{orde}(y)$ *een deler van m.*
Opmerking. Alle onderdelen van dit lemma zijn onjuist voor sommige niet-abelse groepen. Bij voorbeeld in de groep S_3 van permutaties van 3 symbolen zijn de ordes van elementen 1, 2 en 3. We zien dat 2 niet een deler is van het maximum van deze getallen. Het product xy met $\text{orde}(x) = 2$ en $\text{orde}(y) = 3$ heeft $\text{orde}(xy) = 2$.
Zie ook (11.9).

Geef zelf een bewijs van (11.8)(1) en van (11.8)(2).
Bewijs van (11.8)(3). Onderstel $\text{orde}(z) = m$, waar m de exponent is van de eindige abelse groep G, en zij $x \in G$, met $\text{orde}(x) = a$. Als a niet een deler van m zou zijn, dan is er een priemgetal p, en $i, j \in \mathbb{Z}_{\geq 0}$ waar p^i een deler is van m, en p^{i+1} niet een deler van m en p^j een deler van a en $j > i$. Dan heeft $u := z^{p^i}$ orde gelijk aan m/p^i en merk op dat p niet een deler is van m/p^i. Beschouw ook $v := x^{a/p^j}$; we zien dat $\text{orde}(v) = p^j$. Uit (2) volgt dat

$$\text{orde}(u \cdot v) = \frac{m}{p^i} \times p^j = m \times p^{j-i} > m.$$

Dit is een tegenspraak met het feit dat m de grootste orde is die voorkomt in G. We concluderen dat voor elke $x \in G$ de orde van dat element een deler is van m. QED

Voor een eindige (niet noodzakelijk commutatieve) groep G definiëren we de exponent van G het kleinste positieve getal $m \in \mathbb{Z}_{>0}$ zodanig dat voor elke $x \in G$ er geldt $x^m = e$.

(11.9) Opgave. Beschouw de volgende lineaire afbeeldingen $S, U : \mathbb{R}^2 \to \mathbb{R}^2$ gegeven door

$$S(1,0) = (0,1), \quad S(0,1) = (-1,0), \qquad U(1,0) = (0,-1), \quad U(0,1) = (1,-1).$$

Beschouw de groep van lineaire afbeeldingen voortgebracht door S en U onder compositie van afbeeldingen (achter elkaar uitvoeren van afbeeldingen, vermenigvuldigen van matrices). Bewijs:

$$S^2 = -1, \quad \text{orde}(S) = 4, \quad U^3 = 1, \quad \text{orde}(U) = 3, \quad \text{orde}(SU) = \infty.$$

(We zien dat (11.8)(3) onjuist is als we de eis "G is abels" laten vallen.)

(11.10) Torsie. Voor een abelse groep A en een getal $n \in \mathbb{Z}_{>0}$ schrijven we

$$A[n] := \{x \in A \mid x^n = e\}.$$

Voor een abelse groep A schrijven we

$$\text{Tors}(A) := \{x \mid \text{orde}(x) < \infty\}.$$

(11.11) Lemma. (1) *Voor een abelse groep A geldt dat* $\text{Tors}(A) \subset A$ *een ondergroep is.*
(2) *Voor een abelse groep A en $n \in \mathbb{Z}_{>0}$ is $A[n] \subset A$ een ondergroep.*

(11.12) Opmerking/Opgave. In beide conclusies van het lemma is het gegeven "A is abels" nodig; geef tegenvoorbeelden in niet-commutatieve gevallen.

(11.13) Definitie. Een *ring* is een verzameling R met operaties $+, -, \times$ en elementen $0, 1 \in \mathbb{Z}$ zodanig dat:
$\{R, 0, +, -\}$ is een commutatief (additief geschreven) groep,
$\times$ is een operatie $R \times R \to R$ met $((x \times y) \times z) = (x \times (y \times z))$ voor alle $x, y, z \in R$,
voor alle $x \in R$ geldt $1 \times x = x = x \times 1$, en
$x \times (y + z) = x \times y + y \times z$ en $(x + y) \times z = x \times z + y \times z$ voor alle $x, y, z \in R$.
Opmerking. Vaak wordt in plaats van $x \times y$ geschreven xy.
De ring heet *commutatief* als $xy = yx$ voor alle $x, y \in R$.
Ga na dat $\mathbb{Z}$ een (commutatieve) ring is.

Opmerkingen. We laten toe dat de vermenigvuldiging niet commutatief is.
Voorbeeld. De verzameling van 2×2 matrices met elementen in $\mathbb{Z}$ is een niet-commutatieve ring (ga na).
We laten toe dat $-1 = +1$. Bij voorbeeld $\mathbb{Z}/2$ is een ring waarin dit geldt.
We laten toe dat $1 = 0$. Als dat het geval is dan is $R = \{0\}$ (ga na).
We zullen de ringen $\mathbb{Z}$, $\mathbb{Z}/n$, $\mathbb{Z}[\sqrt{-1}]$ veelvuldig tegenkomen.

(11.14) Definitie. Een *delingsring* is een ring waarin elk element ongelijk aan nul een inverse heeft en waarin $0 \neq 1$.
We zullen dergelijke ringen niet tegenkomen.
Een voorbeeld. $R = \mathbb{Z}\cdot 1 \times \mathbb{Z}\cdot i \times \mathbb{Z}\cdot j \times \mathbb{Z}\cdot k$ met $i^2 = -1 = j^2 = k^2$ en $ij = k, \quad jk = i, \quad ki = j, \quad ik = -j, \quad ji = -k, \quad kj = -1$ (is het duidelijk hoe $+, -, \times, 0, 1$ in deze ring eruit zien? (Elementen van deze ring worden quaternionen genoemd, of Hamilton quaternionen).
Een delingsring wordt ook wel een "scheef lichaam" genoemd; deze verkeerde terminologie is verlaten, omdat een scheef lichaam geen lichaam hoeft te zijn, grammaticaal een vreemde constructie.

(11.15) Definitie. Een *lichaam* is een commutatieve ring waarin elk element ongelijk aan nul een inverse heeft en waarin $1 \neq 0$.
Voorbeelden. We kennen $K = \mathbb{Q}, \quad \mathbb{R}, \quad \mathbb{C}$.
Opgave! Zij p een priemgetal. Bewijs dat $\mathbb{Z}/p$ een lichaam is.
Opgave! Zij $n \in \mathbb{Z}$, niet een priemgetal. Bewijs dat $\mathbb{Z}/n$ niet een lichaam is.
Zie (11.21).
Er zijn nog veel meer voorbeelden.
Belangrijke opmerking. Zij K een lichaam en schrijf $K^* := K - \{0\}$. De vermenigvuldiging in K maakt K^* tot een (multiplicatief geschreven) groep. Geef een bewijs.

Het kan voorkomen dat een lichaam eindig is. De voorbeelden $\mathbb{Z}/p$ voor een priemgetal p kennen we. Eindige lichamen zijn volledig geclassificeerd. Ze spelen een grote rol (ook in het dagelijkse leven, b.v. in de cryptografie), maar vooral ook in de wiskunde.

(11.16) Stelling ("de kleine stelling van Fermat"). *Voor een priemgetal p en $a \in \mathbb{Z}$ geldt:*

$$a^p - a \equiv 0 \pmod{p}.$$

We geven twee bewijzen. Allereerst:
Opgave. *Voor een priemgetal p en $i \in \mathbb{Z}$ met $0 < i < p$ is de binomiaal coëfficient $\binom{p}{i}$ deelbaar door p.*
Opmerking. Voor $m \in \mathbb{Z}_{>0}$ schrijven we $m! = 1 \times \cdots \times m$ en $0! = 1$.
Voor $n \in \mathbb{Z}_{>0}$ en $0 \leq i \leq n$ wordt gedefinieerd:

$$\binom{n}{i} = \frac{n!}{i! \times (n-i)!}.$$

We weten dat

$$(X+Y)^n = \sum_{i=0}^{i=n} \binom{n}{i} X^{n-i} Y^i,$$

het "binomium van Newton".
`http://nl.wikipedia.org/wiki/Binomiaalco%C3%ABffici%C3%ABnt`

(11.16)(1) **Eerste bewijs van** (11.16). Voor $a = 0$ is de uitspraak juist. Nu verder met inductie: neem aan dat voor $a \geq 0$ de stelling juist is;

$$(a+1)^p - (a+1) = a^p - a + \sum_{i=1}^{i=p-1} \binom{p}{i} a^i.$$

Uit de inductie-aanname en uit de voorgaande opgave volgt

$$(a+1)^p - (a+1) \equiv 0 \pmod{p},$$

en deze inductie-stap geeft een bewijs van de stelling. QED

(11.16)(2) **Tweede bewijs.** De stelling is juist voor elke a die deelbaar is door p; neem aan dat a niet deelbaar is door p. Dan is $a \bmod p \in (\mathbb{Z}/p)^*$. Uit de stelling van Lagrange, zie (11.7) volgt

$$(a \bmod p)^{p-1} = a \bmod p$$

in de eindige groep $(\mathbb{Z}/p)^*$ die $p-1$ elementen heeft. We zien dat $a^{p-1}-1$ deelbaar is door p (als a niet deelbaar is door p). Voor alle $a \in \mathbb{Z}$ geldt dat $a(a^{p-1}-1)$ deelbaar is door p. QED

(11.17) Opgave. Neem de verzameling van alle priemgetallen die een Mersenne getal delen. Beschrijf deze verzameling. Zie (16.20). [Een Mersenne getal is een getal van de vorm $2^n - 1$ met $n \in \mathbb{Z}_{>1}$.]

(11.18) Zij R een commutatieve ring. Een polynoom met coëfficiënten in R is een uitdrukking $G = \sum a_i T^i$. Deze verzameling wordt aangegeven met $R[T]$. De optelling is coëfficiëntsgewijs, en de vermenigvuldiging gebruikt $T^i T^j = T^{i+j}$ en de vermenigvuldiging in R.

Voor een polynoom $G = \sum a_i T^i$ schrijven we G' voor de afgeleide, gegeven door $G' := \sum i a_i T^{i-1}$.

Dit is een zuiver formele definitie; dut heeft niets met "limieten" te maken. Maar voor een polynoom-functie $G : \mathbb{R} \to \mathbb{R}$ kunnen we de (formele) afgeleide gebruiken, en de afgeleide zoals in de reële analyse, en de resultaten zijn dezelfde; vandaar.
Ga na: als R een ring is, en $G \in R[T]$ en $a \in R$ zo dat $(T-a)^2$ een deler is van G, dan is $G(a) = 0$ en $G'(a) = 0$.

(11.19) Lemma. *Zij R een ring zonder nuldelers, en $G \in R[T]$ een polynoom. Het aantal nulpunten van G in R hooguit gelijk aan de graad van G.*
Opmerking. Als bovendien gegeven is dat voor elke $a \in R$ met $G(a) = 0$ er geldt $G'(a) \neq 0$ en alle nulpunten van G liggen in K dan is het aantal nulpunten van G in R precies gelijk aan de graad van G.
Geef zelf een bewijs van het lemma en van de opmerking.

(11.20) Een voorbeeld. *We laten zien dat het gegeven "R heeft geen nuldelers" in dit lemma nodig is.* Zij $R = \mathbb{Z}/91$. Merk op: $91 = 7 \times 13$. Zij $G = T^3 - 1 \in R[T]$. We zien dat $G' = 3T^2$. Bewijs: $3 \bmod 91 \in R$ is een eenheid (hint: wat is $((-30)\times 3) \pmod{91}$?). Bewijs: als $b \in R$ met $G'(b) = 0$ dan is $b = 0$ (en dus hebben G en G' niet een gemeenschappelijk nulpunt in R want $G(0) \neq 0$). Laat zien dat het aantal nulpunten van G in R groter is dan 3 (de graad van G).

(11.21) Eindige lichamen. Voor elke $n \in \mathbb{Z}_{>1}$ schrijven we

$$\mathbb{Z}/n = \{a \bmod n \mid 0 \leq a < n\}.$$

Dit is een ring.
Stelling. *$\mathbb{Z}/n$ is een lichaam dan en slechts dan als $n = p$, een priemgetal.*
Bewijs. Als $ab = n$ met $1 < a < n$ en $1 < b < n$ dan geldt

$$(a \pmod n) \times (b \pmod n) = n \pmod n = 0, \text{ en } a \pmod n \neq 0, \quad b \pmod n \neq 0.$$

Als $R = \mathbb{Z}/n$ een lichaam zou zijn, en $a \pmod n \neq 0$ dan is er een $x \in R$ met $x \times a \pmod n = 1$. Er zou komen

$$x \times a \pmod n \times b \pmod n = 1 \times b \pmod n = \times b \pmod n \neq 0,$$

en

$$x \times (a \pmod n \times b \pmod n) = x \times 0 = 0,$$

een tegenspraak (we bewijzen en gebruiken: een lichaam heeft geen nuldelers).

Anderzijds veronderstel dat $0 < a < n = p$, waar p een priemgetal is. Dan geldt $\text{ggd}(a, p) = 1$. Dus zijn er $y, z \in \mathbb{Z}$ met $ya + zp = 1$, zie (9.6). Dan geldt $(y \pmod p) \times (a \pmod p) = 1$. Conclusie: elk element $0 \neq \overline{a} \in \mathbb{Z}/p$ heeft een inverse. Dit laat zien dat $\mathbb{Z}/p$ een lichaam is.

(11.22) Dit geeft voorbeelden, $\mathbb{Z}/p$ van een eindig lichaam. Er zijn nog veel meer eindige lichamen, geclassificeerd, een mooie theorie, we gaan er niet verder op in.

Een eigenschap. Als K een eindig lichaam is, dan is er een priemgetal p en inclusie van lichamen $\mathbb{Z}/p \hookrightarrow K$, en $\#(K)$ is een veelvoud van p.
Bewijs: beschouw $1, 1+1, 1+1+1, \cdots$ in K; de kleinste $k > 0$ waarvoor $k \cdot 1 = 0$ in K is een priemgetal (gebruik dat K geen nuldelers heeft); in dat geval is $\mathbb{Z}/p$ als additieve groep een ondergroep van K; uit de stelling van Lagrange volgt dat p een deler is van $\#(K)$.
Opmerking: er geldt zelfs dat er een priemgetal p en een $n \in \mathbb{Z}_{>0}$ is met $\#(K) = p^n$.
Zie literatuur, of zie:
`http://en.wikipedia.org/wiki/Finite_field`

(11.23) Zij R een commutatieve ring. We zeggen dat $a \in R$ een *eenheid* is in R als er een $b \in R$ is met $ab = 1$ (d.w.z. als a een inverse heeft in R. We schrijven R^* voor de verzameling van de eenheden in R.
Laat zien dat R^* een (multiplicatief geschreven) groep is.

Voor $n \in \mathbb{Z}_{>0}$ geldt:

$$(\mathbb{Z}/n)^* = \{a \bmod n \mid 0 < a < n, \quad \text{ggd}(a, n) = 1\};$$

bewijs dit.

(11.24) Opgave. Bepaal de structuur van de groep $(\mathbb{Z}/n)^*$ voor alle $n \in \{5, 6, 8, 9, 10, 13\}$.

(11.25) Definitie/opmerking/opgave. (1) Voor $n \in \mathbb{Z}_{>0}$ definiëren we

$$\varphi(n) = \#((\mathbb{Z}/n)^*);$$

de afbeelding $\varphi : \mathbb{Z}_{>0} \to \mathbb{Z}$ wordt de Euler-φ-functie genoemd.
(2) Ga na: $\varphi(p) = p - 1$, en ook: $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p - 1)$.
(3) Ga na: als $a, b \in \mathbb{Z}_{>0}$ en $\text{ggd}(a, b) = 1$ dan geldt $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.
(4) Bereken $\varphi(144)$, en $\varphi(2343)$.

(11.26) Stelling (Wilson). *Voor elk priemgetal q geldt:*

$$\prod_{1\le i\le q-1} i \equiv -1 \pmod{q}.$$

Notatie: $\prod$ staat voor het product, met grenzen zoals aangegeven. In dit geval:

$$\prod_{1\le i\le q-1} i \;=\; (q-1)! \;=\; 1\times 2\times\cdots\times(q-1).$$

Bewijs. Voor $q=2$ is dit duidelijk. Voor oneven q zien we dat

$$\{1,2,\cdots,q-1\} = \{1\}\cup\{2,\cdots,q-2\}\cup\{q-1\}.$$

Voor $2\le i\le p-2$ is $i^2\not\equiv 1 \pmod{q}$ en dan is er een unieke j met $2\le j\le p-2$ en $ij\equiv +1 \pmod{q}$ en daarvoor geldt dat $i\neq j$; inderdaad: in $\mathbb{F}_p^*$ geldt $1^{-1}=1$, en $(-1)^{-1}=1$ en alle andere elementen met hun inverse komen in paren voor.

We zien

$$\prod_{2\le i\le q-2} i \equiv +1 \pmod{q}$$

en gebruikmakend van

$$\prod_{1\le i\le q-1} i = 1\times(\prod_{2\le i\le q-2} i)\times(q-1)$$

volgt de conclusie. QED

(11.27) Stelling. *Voor een priemgetal met $p\equiv 1 \pmod 4$ is er een $\alpha\in\mathbb{F}_p$ met $\alpha^2 = -1\in\mathbb{F}_p$.*

Eerste bewijs. Schrijf $p=4r+1$. We gebruiken de stelling van Wilson.

Claim.

$$(\prod_{1\le i\le 2r} i)^2 \equiv -1 \pmod{p}.$$

Merk op:

$$1\le i\le 2r,\quad j=p-i \quad\Longrightarrow\quad p-1\ge j\ge 2r+1.$$

Hieruit volgt

$$(\prod_{1\le i\le 2r} i) \equiv (\prod_{p-1\ge j\ge 2r+1} j) \pmod{p}.$$

Conclusie

$$\alpha := ((\prod_{1\le i\le 2r} i) \bmod p) = ((\prod_{p-1\ge j\ge 2r+1} j) \bmod p)$$

heeft de eigenschap $\alpha^2=-1\in\mathbb{F}_p^*$.

Voor een tweede bewijs ontwikkelen we iets meer techniek.

(11.28) Stelling. *Zij K een eindig lichaam. De (multiplicatieve) groep K^* is cyclisch.*
Opmerking. We bewijzen de stelling, maar het bewijs geeft niet aan hoe je een voortbrenger construeert.
Bewijs. Zij $N = \#(K^*)$; als $\#(K) = q$ dan is $N = q - 1$ (want alle elementen ongelijk aan nul in K hebben een inverse in K, liggen daarom in K^*).

Beschouw de (multiplicatief geschreven) groep K^*. We schrijven m voor het maximum van de ordes van elementen van deze groep. We hebben gezien dat orde(x) een deler is van m voor alle $x \in K^*$, zie (11.8).3. Hieruit volgt dat elke $x \in K^*$ een nulpunt is van het polynoom $f = T^m - 1$. Uit (11.19) volgt dat het aantal nulpunten van f hooguit m is. Maar het aantal nulpunten is gelijk aan $\#(K^*) = N = q - 1$. Conclusie: $m = N$. We zien dat er in K^* een element van orde $q - 1$ is. Daaruit volgt dat K^* cyclisch is. QED

Notatie. We schrijven wel $\mathbb{F}_p$ voor het lichaam met p elementen; we zien dat de $(\mathbb{F}_p, +) = (\mathbb{Z}/p, +)$.

(11.29) Tweede bewijs van (11.27). Als $\beta \in \mathbb{F}_p^*$ een voortbrenger is, dan geldt,

$$\beta^{4r} = +1, \quad \alpha := \beta^r, \quad \alpha^2 = -1$$

want $\alpha^4 = +1$, dus $\alpha^2 = \pm 1$, maar $\alpha^2 \neq +1$. QED

Voorbeeld. Laat zien dat zowel (23 mod 53) als (30 mod 53) de gevraagde eigenschap hebben in $(\mathbb{F}_{53})^*$.

(11.30) Uitgewerkt voorbeeld van Stelling (11.28). Neem $p = 11$. We bepalen de structuur van de groep $(\mathbb{F}_{11})^*$; we weten al dat die groep cyclisch is (d.w.z. de groep wordt voortgebracht door één element). In dit voorbeeld zien we dat.

We weten $\#((\mathbb{F}_{11})^*) = 10$; de delers 2 en 5 van 10 geven $2^2 \not\equiv 1 \pmod{11}$ en $2^5 \not\equiv 1 \pmod{11}$; conclusie: 2 mod 11 brengt $(\mathbb{F}_{11})^*$ voort,

$$j \longmapsto 2^j \bmod 11 \quad \text{geeft} \quad (\mathbb{Z}/10, +) \quad \xrightarrow{\sim} \quad ((\mathbb{F}_{11})^*, \times).$$

j	$2^j \bmod 11$	orde
0	1	1
1	2	10
2	4	5
3	8	10
4	5	5
5	10	2
6	9	5
7	7	10
8	3	5
9	6	10

Let op, in $(\mathbb{Z}/10, +)$ gebruiken we de optelling modulo 10 als groeps-wet, in $((\mathbb{F}_{11})^*, \times)$ gebruiken we de vermenigvuldiging modulo 11 als groepswet; de afbeelding stuurt

$$(j \bmod 10) + (k \bmod 10) \text{ naar } (2^j \bmod 11) \times (2^k \bmod 11).$$

We zien dat er precies 4 elementen zijn die als voortbrenger kunnen optreden van $(\mathbb{F}_{11})^*$. Dat konden we ook al concluderen, haast zonder rekenen: dat aantal is het aantal elementen dat $\mathbb{Z}/10$ voortbrengt, en dat aantal is gelijk aan $\varphi(10) = \varphi(2)\cdot\varphi(5) = 4$. Het bepalen van de orde van een k mod 11 geeft wat rekenwerk, maar bepalen van de orde van een j mod 10 is eenvoudig.

(11.31) Vraagstuk. (1) Bewijs dat $(\mathbb{Z}/64)^* \cong (\mathbb{Z}/2) \times (\mathbb{Z}/16)$.
(2) Bewijs dat $(\mathbb{Z}/121)^*$ een cyclische groep is (van orde $\varphi(121) = 110$). Zie (16.16)
[Hier is $\varphi(-)$ de Euler-phi-functie, gegeven door $\varphi(- = n) = \#((\mathbb{Z}/n)^*)$, zie (11.25).]

(11.32) Voorbeelden/vraagstukken. (1) Ga na dat 3 mod 17 een voortbrenger is van $(\mathbb{Z}/17)^*$.
(2) Bepaal de orde van $(k \bmod 41) \in (\mathbb{Z}/41)^*$ voor alle $k \in \{2, 3, 4, 5, 6\}$.
Voorbeeld van een berekening. We zien $2^5 = 32$, en dus is $2^{10} \equiv -1 \pmod{41}$; ook is $2^4 \not\equiv -1 \pmod{41}$; conclusie orde$(2 \bmod 41) = 20$ voor $(2 \bmod 41) \in (\mathbb{F}_{41})^*$). Merk op $3^4 = 81$ en bereken de orde van 3 mod 41.
(3) Bepaal de verzameling van alle elementen die kunnen optreden als een voortbrenger van $(\mathbb{Z}/41)^*$. Zie (16.17).

(11.33) Opmerking. Voor $n \in \mathbb{Z}_{>0}$ waarvan we de factorizatie weten is de structuur van $(\mathbb{Z}/n)^*$ gemakkelijk te bepalen door middel van:
voor $n > 1$ is $(\mathbb{Z}/2^n)^* \equiv (\mathbb{Z}/2) \times (\mathbb{Z}/2^{n-2})$, en
voor $n > 0$ en een priemgetal $p \neq 2$ is $(\mathbb{Z}/p^n)^*$ cyclisch (van orde $p^n - p^{n-1}$).
Gebruik de Chinese reststelling, zie (9.13).

(11.34) Een analogie. Zij K een lichaam. De ring $K[T]$ van polynomen in één variabele met coëfficienten in K heeft eigenschappen die lijken op eigenschappen van $\mathbb{Z}$; bij voorbeeld geldt unieke factorizatie in beide ringen. We proberen in deze ringen stellingen te formuleren. Soms zien we dat analoge beweringen in beide ringen waar zijn. Ook kunnen we proberen voor een vermoeden in de ene ring een analoge uitspraak in de andere ring te beschouwen. Een dergelijke analogie kan een leidraad zijn in welke richting we moeten zoeken. We geven drie voorbeelden, waar de stelling / het vermoeden in $\mathbb{Z}$ moeilijk is, maar de analoge uitspraak in $K[T]$ gemakkelijk te bewijzen is.

(11.34)(1) Het ABC-vermoeden in $\mathbb{Z}$ en in $R = K[T]$.
Veronderstel dat $\mathbb{Q} \subset K$ (anders gezegd: we nemen aan dat K karakteristiek nul heeft). Voor een polynoom $f \in K[T]$ schrijven we $\mathrm{Rad}(f)$ voor het radicaal (ook wel genoemd de conductor) van F: het product van alle irreducibele factoren van f.
Stelling (Mason). *Laat $A, B, C \in K[T]$ met*

$$A + B = C, \quad \mathrm{ggd}(A, B) = 1.$$

Dan geldt

$$\max\{\mathrm{graad}(A).\mathrm{graad}(B), \mathrm{graad}(C)\} \leq \mathrm{graad}(\mathrm{Rad}(ABC)) - 1.$$

Dit zegt dat het aantal priemfactoren van ABC niet te klein kan zijn, in analogie met het ABC vermoeden in $\mathbb{Z}$.

Zie `http://www.fen.bilkent.edu.tr/~franz/ag05/ag-02.pdf`
Het bewijs van deze stelling is niet moeilijk.

(11.34)(2) Het FLT-vermoeden in $\mathbb{Z}$ en in $k[T]$.
Zij $k = \mathbb{C}$ (of, algemener, een lichaam dat algebraïsch gesloten is met $\mathbb{Q} \subset k$).
Stelling (FLT in $k[T]$). *Zij $n \in \mathbb{Z}_{\geq 3}$. Neem $F, G, H \in k[T]$ met*

$$F^n + G^n = H^n \quad \text{ggd}(F, G) = 1.$$

Dan geldt $F, G, H \in k$.
Probeer deze stelling af te leiden uit de vorige stelling.
Zie `http://www.fen.bilkent.edu.tr/~franz/ag05/ag-02.pdf`

(11.34)(3). De PNT in $\mathbb{Z}$ en een analogon in $R = K[T]$. [PNT = Prime Number Theorem.]
Laat K een eindig lichaam zijn met q elementen, Schrijf K_n voor het lichaam (dat K bevat) met q^n elementen. Het is bekend at een dergelijk lichaam bestaan en uniek is op isomorfie na. We zeggen dat een polynoom $f \in K[T]$ monisch is als de coëfficient van de hoogste graads term gelijk aan 1 is. Het aantal monische, irreducibele elementen van graad i in $K_n[T]$ noemen we N_i.
Stelling.

$$N_i \quad \sim \quad \frac{q^i}{i}, \quad i \to \infty.$$

Onder de substitutie $x = q^i$ is de rechterhand gelijk aan $i/^q\log(i)$, en we zien een analogie.
Zie: *Analogue for irreducible polynomials over a finite field* in
`http://en.wikipedia.org/wiki/Prime_number_theorem`
Niet besproken: de Riemann hypothese in het algemeen, en in functielichamen over eindige lichamen.

12 Appendix: Fermat

Over Pierre de Fermat (1601 - 1665) is veel geschreven, wat een schitterend onderwerp. Fermat was jurist, en "amateur"-wiskundige. Een van de grootste in ons vak. Lees bij voorbeeld
`http://nl.wikipedia.org/wiki/Pierre_de_Fermat`
Een leven vol met prachtige wiskunde en bizarre voorvallen (b.v.: In 1653 werd hij getroffen door de pest en werd hij bij vergissing dood verklaard, maar hij zou nog een twaalftal jaren leven).

(12.1) Fermat en de Pell vergelijking. Laat ik slechts één van de anecdotes over Fermat hier weergeven (het is er maar een van de vele...). Literatuur o.a.: [73], II.XIII, pp. 92-99. Zie ook [14], 1.9. Fermat had een uitgebreide correspondentie over wiskundige onderwerpen. Daarin daagde hij vaak anderen uit om berekeningen te doen, waarvan we denken dat hij die zelf al gedaan had. Een geliefd probleem was het oplossen van de vergelijking

$$X^2 - NY^2 = 1,$$

waar $N > 0$ een geheel getal is dat niet een kwadraat is. Heeft die vergelijking een oplossing voor elke N? Voor sommige N zijn oplossingen eenvoudig te vinden, soms lijkt het wel of

berekeningen suggereren dat er geen oplossing bestaat (?).
Bij voorbeeld, $N = 11, x = 10, y = 3$, en $10^2 - 11 \cdot 3^2 = 1$,
$N = 12, x = 7, y = 2$ en $7^2 - 12 \cdot 2^2 = 1$,
en kunnen we ook een oplossing vinden voor $N = 13$? (Een van de favoriete voorbeelden van Euler in zijn algebra boek.)

Evenzo $N = 60, x = 31, y = 4$ en $31^2 - 60 \cdot 4^2 = 961 - 60 \cdot 16 = 1$,
en kunnen we ook een oplossing vinden voor $N = 61$?

Fermat vroeg oplossingen voor de gevallen $N = 61$ en $N = 109$ in zijn brief aan Frenicle in 1657, waarin hij schreef dat hij wat kleine getallen had gekozen "pour ne vous donner trop de peine". De kleinste oplossing voor $N = 61$ is $x = 1766319049$ en voor $N = 109$ is de kleinste $x = 158070671986249$ ("pour ne vous donner trop de peine" ?) , terwijl soms een andere "kleine" N een kleine oplossing kan toelaten, b.v. $N = 110, x = 21, y = 2$. We denken dat Fermat wist hoe hij zulke oplossingen kon vinden, en dat hij vele berekend had voor hij precies wist dat moeilijke kleine gevallen juist $N = 61$ en $N = 109$ zijn. In ieder geval is er een tekst van Fermat waarin hij zegt dat de Pell vergelijking oplossingen heeft voor niet-kwadraat N, zie [14], 1.9, in het bijzonder pp. 25/26. Later heeft Legendre laten zien hoe de theorie van de kettingbreuken bewijst dat er voor elke niet-kwadraat $N > 1$ er een oplossing is, en hoe je een dergelijk oplossing eenvoudig en snel kunt berekenen. Brouncker, Wallis en Fermat kenden waarschijnlijk deze methode, maar het is niet duidelijk of ze ook een bewijs zoals bij Legendre hadden.

Deze vergelijking heet de *Pell vergelijking* (omdat Euler deze terminologie in zijn algebra boek voorstelde), maar nu weten we dat dit niet de juiste terminologie is. De titel van deze paragraaf is onjuist: toen Fermat leefde werd deze vergelijking niet zo genoemd, en Pell heeft weinig met deze vergelijking te maken gehad. In veel oudere wiskunde-culturen werd deze vergelijking al bestudeerd. Een fascinerend onderwerp. Zie [43]; zie
`http://en.wikipedia.org/wiki/Pell's_equation`

De vergelijking $X^2 - NY^2 = -1$ heeft voor sommige N wel en voor andere N niet een oplossing (in positieve, gehele getallen). Dit is begrepen, maar beslissen voor welke N deze vergelijking wel een oplossing heeft is niet zo gemakkelijk. Een algemeen criterium is niet eenvoudig, maar we kunnen wel voor elke N door middel van kettingbreuk-berekening beslissen of er wel een dergelijke oplossing bestaat. Online kunnen we voor een gegeven ("kleine") N dit laten beslissen, zie:
`http://www.numbertheory.org/php/hardy_williams.html`
In [1], in 3.4 op pagina 143 vinden we een tabel van de 21 waarden van niet-kwadraten met $N \leq 101$ waarvoor de negatieve Pell vergelijking wel een oplossing heeft:
$2, 5, 10, 13, 17, 26, 29, 37, 41, 50, 53, 58, 61, 65, 73, 74, 82, 85, 89, 97, 101$.

13 Enkele notaties en symbolen

Wiskundigen gebruiken sommige notaties, symbolen. Die zijn bedoeld als stenografie. Ze geven een snelle en precieze manier om informatie compact weer te geven. Ik zal me in deze cursus van een paar aspecten van wiskundige notatie bedienen. Het stroomlijnt tekst en uitleg en het maakt wiskundige beweringen vaak nauwkeuriger.

Hieronder leg ik een paar aspecten van wiskundige notatie uit. Maar ik geef niet een college

logica of verzamelingen-leer.

(13.1) Het esti-symbool. *We schrijven: $x \in V$; uit de notatie volgt dat V een verzameling is, dat x een element is, en dat het element x in de verzameling V zit.*
Bij voorbeeld, x is de persoon Anne Frank, V is de verzameling van mensen die in de 20ste eeuw geboren zijn; we zien dat $x \in V$ een uitspraak is die waar is, en die we kunnen lezen als: "Anne Frank is in de 20ste eeuw geboren".

We gebruiken het symbool $\notin$ om aan te geven dat het element links ervan niet bevat is in de verzameling rechts daarvan. Zij y de persoon Johann Sebastian Bach. De uitspraak $y \in V$ is niet waar, en $y \notin V$ is wel waar.

(13.2) Inclusie. We gebruiken het symbool $\subset$ om aan te geven dat er links daarvan een verzameling staat, die bevat is in de verzameling die er rechts van staat. Bij voorbeeld laat W de verzameling van vrouwelijke Nederlanders zijn geboren in de 20ste eeuw. De uitspraak $W \subset V$, met V als hierboven, is een ware uitspraak.
Pas op. De uitspraak $x \subset V$ is grammaticaal onjuist: het element x wat links staat is niet een verzameling.
We zullen $V \supset W$ schrijven als we $W \subset V$ bedoelen.

(13.3) We geven met $\{\cdots\}$ een verzameling aan, waar tussen te haken gepreciseerd wordt welke elementen beschouwd worden.
Voorbeeld: $\{x\} \subset V$ is een uitspraak equivalent met $x \in V$;
$\{2, 5\} \subset \{1, 2, 3, 4, 5, 6\}$ is een uitspraak die juist is.

(13.4) Gehele getallen. Met $\{z \mid \cdots\}$ geven we aan de verzameling van alle elementen z die voldoen aan de restricties rechts van $|$.
Voorbeeld: met $\{n \mid n$ is een geheel getal$\}$ geven we aan de verzameling van alle gehele getallen. Die verzameling zullen we noteren als $\mathbb{Z}$;
$\frac{2}{7} \notin \mathbb{Z}$ en $0 \in \mathbb{Z}$ zijn juist, en $\{-3, 5, 18\} \subset \mathbb{Z}$ is juist.

(13.5) Rationale getallen. De verzameling van *breuken van gehele getallen* geven we aan met $\mathbb{Q}$. Een dergelijk getal wordt een *rationaal* getal genoemd. Merk op dat bij voorbeeld de regel $2/7 = (3{\cdot}2)/(3{\cdot}7)$ geldt. Merk op dat $\mathbb{Z} \subset \mathbb{Q}$; inderdaad een geheel getal $n \in \mathbb{Z}$ kan ook gezien worden als breuk $n/1 \in \mathbb{Q}$. (Verzoek: spreek niet van rationele getallen.)

(13.6) Reële getallen*. We kunnen nog en algemener getal begrip invoeren (we geven een definitie die niet helemaal compleet is). Dit kunnen we doen door de verzameling van alle decimale breuken te beschouwen, waar we oneindig veel decimalen achter de komma toelaten (met nog een afspraak, die bijvoorbeeld zegt dat $1.9999\cdots = 2$). Een dergelijk getal wordt *een reëel getal genoemd*. De verzameling van reële getallen wordt aangegeven met $\mathbb{R}$.

We schrijven $\mathbb{C}$ voor de verzameling van complexe getallen: alle getallen van de vorm $a + b\sqrt{-1}$ met $a, b \in \mathbb{R}$. Merk op $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Waarom een * bij deze passage? Een wiskundig sluitende definitie van reële getallen is niet zo eenvoudig te geven; het duurde in de geschiedenis dan ook lang voordat een dergelijke goede definitie gevonden werd: Cantor gaf in 1871 een sluitende definitie (ook Cauchy en Dedekind gaven sluitende constructies). Maar daarvoor konden we (en ook nu kunnen we)

goed werken met een ad hoc benadering. De terminologie "reëel" is afkomstig van Descartes (om deze getallen te onderscheiden van complexe getallen). Voor meer uitleg en verwijzingen, zie

`http://en.wikipedia.org/wiki/Real_number`

Voor en reëel getal U schrijven we $[U]$ voor het groote gehele getal met $[U] \leq U$.
Bij voorbeeld $[\sqrt{2}] = 1$ (want $1^2 \leq 2 < 2^2$);
$[7] = 7$, $[-\sqrt{2}] = -2$, etc.

(13.7) *Er zijn reële getallen die niet rationaal zijn.*
Bewering. $\sqrt{2} \notin \mathbb{Q}$.
Bewijs. (Bewijs uit het ongerijmde.) Veronderstel dat er gehele getallen $m, n \in \mathbb{Z}$ zijn zodanig dat $\sqrt{2} = m/n$. Kwadrateren geeft: $m^2 = 2{\cdot}n^2$. We weten dat ontbinden van gehele getallen in priemfactoren uniek is. Het aantal factoren 2 in n^2 is *even*. We zouden concluderen dat het aantal factoren 2 in $2{\cdot}n^2 = m^2$ *oneven* zou zijn. Deze tegenspraak bewijst de bewering. QED

Opmerking. In de oude Griekse wiskunde was dit een schok: dat er getallen bestaan die niet rationaal zijn. Gehele getallen en quotiënten daarvan werden gezien als bouwstenen. Dat er ook andere getallen bestaan werd eerst niet vermoed, en later in de Griekse wiskunde als vreemd ervaren.

(13.8) Opmerking. Getallen die beschreven kunnen worden als oplossing van een polynoom-vergelijking worden *algebraïsche getallen* genoemd. Gebruikmakend van het begrip *aftelbaarheid*, zie (13.9), kan worden aangetoond dat de verzameling van algebraïsche getallen *aftelbaar* is. Omdat het diagonaal-principe van Cantor aantoont dat $\mathbb{R}$ niet aftelbaar is, zie (13.10), concluderen we: *er zijn reële getallen die niet algebraïsch zijn.* Dit bewijs construeert niet zulke getallen. Het is doorgaans niet zo gemakkelijk constructief het bestaan van zulke getallen aan te tonen.
Voorbeeld. Het getal π is *niet een rationaal getal*, d.w.z. $\pi \notin \mathbb{Q}$ (Lambert 1761; Legendre 1794; Hermite 1873). Pas veel later werd bewezen dat π niet een algebraïsch getal is (Lindemann 1882). Dit resultaat loste een eeuwen-oud probleem op, de kwadratuur van de cirkel: *het is niet mogelijk met passer en liniaal een vierkant te construeren waarvan de oppervlakte gelijk is aan die van een gegeven cirkel.*

(13.9) Aftelbaar. We zeggen dat een verzameling V *aftelbaar oneindig* is als alle elementen daarvan genummerd kunnen worden met behulp van de positieve gehele getallen $1, 2, 3, \cdots$. Anders gezegd: als er een bijectieve afbeelding $\mathbb{Z}_{>0} \to V$ bestaat.

Voorbeeld/Opgave: $\mathbb{Q}$ is aftelbaar oneindig.
Aanwijzing. Laat zien dat het voldoende is om dit te bewijzen voor alle $a/b \in \mathbb{Q}$ met $0 \leq a/b < 1$; zet al die getallen in een (aftelbare) lijst, bij voorbeeld als volgt: $0, 1/2, 1/3, 2/3, 1/4, 3/4, 1/5, 2/5, \cdots$.]

Cantor bewees dat $\mathbb{R}$ niet aftelbaar is, zie (13.10). Hier is dat principe zoals dat door Cantor ontwikkeld werd. Bij voorbeeld zie
`http://en.wikipedia.org/wiki/Cantor's-diagonal-argument`

(13.10) Stelling (Cantor). *De verzameling* $\mathbb{R}$ *is overaftelbaar.*
Dit wil zeggen: als $\alpha_1, \alpha_2, \alpha_3, \ldots$ een rij reële getallen is, dan bestaat er een $\beta \notin \mathbb{R}$.
Bewijs. Het is al voldoende om te bewijzen dat de verzameling $\{\gamma \in \mathbb{R} \mid 0 \leq \gamma < 1\}$ overaftelbaar is. Veronderstel een dergelijk rij als boven is gegeven met bovendien $0 \leq \alpha_i < 1$ voor alle i. Van elk van deze getallen schrijven we de decimale ontwikkeling uit:

$$\alpha_1 = 0,\ a_{1,1}\ a_{1,2}\ a_{1,3}\ a_{1,4} \cdots,$$

$$\alpha_2 = 0,\ a_{2,1}\ a_{2,2}\ a_{2,3}\ a_{2,4}\ \cdots,$$

$$\alpha_3 = 0,\ a_{3,1}\ a_{3,2}\ a_{3,3}\ a_{3,4}\ \cdots,$$

etc.. We construeren positieve gehele getallen $b_1, b_2, \cdots \in \{0, 1\}$ zo dat $b_1 \neq a_{1,1}, \quad b_2 \neq a_{2,2}, \cdots b_i \neq a_{i,i}$ voor alle i, b.v. door: als $a_{i,i} > 0$ dan kiezen we $b_i = 0$ en als $a_{i,i} = 0$ dan kiezen we $b_i = 1$. (Dit heet het "Diagonalverfahren".) Schrijf

$$\beta := 0,\ b_1\ b_2\ b_3 \cdots.$$

Omdat $b_i \neq a_{i,i}$ volgt $\beta \neq \alpha_i$ voor elke i; dus komt β niet in bovenstaande lijst voor. We hebben bewezen dat $\mathbb{R}$ overaftelbaar is. QED

(13.11) We geven met $\Rightarrow$ een logische implicatie aan. Bij voorbeeld $x = 1 \Rightarrow x > 0$ is grammaticaal juist en bovendien een ware uitspraak.

Met $\Longleftrightarrow$ geven we een equivalentie van beweringen aan. Met $\wedge$ geven "en" aan en met $\vee$ het zwakke "of". Voorbeeld: $x^2 = 1 \Rightarrow (x \leq +1) \vee (x \geq -1)$ is een ware uitspraak.

Het symbool $\cap$ wordt gebruikt voor de doorsnede van verzamelingen (de verzameling van gemeenschappelijke elementen), en met $\cup$ geven we de vereniging aan (de verzameling van elementen die in een van beide ligt, of in allebei).
Voorbeelden: $\{x \mid x \in \mathbb{Z}, \quad x \geq 0\} \cap \{x \mid x \in \mathbb{Z}, \quad x \leq 0\} = \{0\}$,
$\{x \mid x \in \mathbb{Z}, \quad x \geq 0\} \cup \{x \mid x \in \mathbb{Z}, \quad x \leq 7\} = \mathbb{Z}$.

(13.12) Met $f : V \to W$ geven we aan dat V en W verzamelingen zijn, en dat f een afbeelding is van V naar W; dat betekent dat f aan elk element van V een element van W toevoegt. Als onder deze afbeelding v afgebeeld wordt op w dan schrijven we $v \mapsto w$ (de pijl $\mapsto$ noemen we een toevoeging);

$$v \mapsto w \quad \Longleftrightarrow \quad \{v\} \to \{w\}.$$

Bij voorbeeld $f : \mathbb{R} \to \mathbb{R}$ gedefiniëerd door $f(x) = x^2$. Dit kan ook weergegeven worden door $x \mapsto x^2$. Let op, de notatie $x \to V$, waar x een element is, is grammaticaal onjuist (aan beiden kanten van $\to$ moet een verzameling staan); de notatie $\{x\} \to V$ is grammaticaal wel juist.

We zeggen dat f injectief is als voor alle $v, v' \in V$ geldt $v \neq v' \Rightarrow f(v) \neq f(v')$; schrijfwijze: $f : V \hookrightarrow W$.

We zeggen dat $f : V \to W$ surjectief als elk element in W het beeld is van een element in V; notatie $f : V \twoheadrightarrow W$.

Ga na: $f : \mathbb{R} \to \mathbb{R}$ gedefiniëerd door $f(x) = x^2$ is niet injectief, en is niet surjectief.

(13.13) $\exists$: er bestaat/er bestaan; $\forall$: voor alle.

Met $x := 3$ bedoelen we: "we definiëren x als gelijk te zijn aan 3". Bij het symbool := staat links een nog niet gedefiniëerd begrip, en rechts ervan iets wat we al kennen.

Met $a \equiv b \pmod{c}$, spreek uit "a is equivalent met b modulo c", bedoelen we: het verschil $a - b$ is deelbaar door c.
Voorbeeld: $1 \equiv 7 \pmod{3}$ is een juiste uitspraak. Ook $2 \not\equiv 7 \pmod{3}$ is juist.
De volgende uitspraak is juist: $(a \equiv 0 \pmod{2}) \iff (a \text{ is even})$.

Voor een eindige verzameling V schrijven we $\#(V)$ voor het aantal elementen van die verzameling.

Veronderstel dat $a_1, \cdots, a_n$ getallen zijn. Som en product daarvan worden genoteerd als

$$\sum_{1 \le i \le n} a_i := a_1 + \cdots + a_n, \qquad \prod_{1 \le i \le n} a_i := a_1 \times \cdots \times a_n.$$

Verklaring van een terminologie. We spreken van een *diophantische vergelijking* als we beschouwen een (of meer) polynoom (polynomen), waarvan de coëfficienten geheel zijn, en waarvan we geïnteresseerd zijn in oplossingen in de gehele getallen. Eigenlijk moeten we spreken van een diophantisch probleem.

Samenvatting
$x \in V$ het element x is bevat in de verzameling V; $y \notin V$;
$W \subset V$ deelverzameling; $V \cap W$ doorsnede; $V \cup W$ vereniging;
$\{z \mid \cdots\}$ verzameling van elementen die aan de voorwaarde(n) $\cdots$ voldoen;
$\mathbb{Z}$ verzameling van gehele getallen, $\mathbb{Q}$ van rationale getallen,
$\mathbb{R}$ van reële getallen, $\mathbb{C}$ van complexe getallen;
$f : V \to W$ afbeelding tussen verzamelingen; $\hookrightarrow$ injectief; $\twoheadrightarrow$ surjectief;
$\mapsto$ toevoeging; $\implies$ logische implicatie; $\iff$ logische equivalentie;
:= links wordt gedefiniëerd door middel van wat er rechts staat;
$a \equiv b \pmod{c}$ "a is equivalent met b modulo c" [c deelt $a - b$].

14 Het 15-spel

In Hoofdstuk 4 van [S] geeft Singh een gedeeltelijke beschrijving van een schuifspel bedacht (?) door Sam Loyd. In deze § geven we meer details.
Opmerking. Een schijnbaar eenvoudig situatie heeft soms zoveel mogelijkheden dat zelfs al het eenvoudig uitproberen veel tijd kost. Zulke combinatorische puzzels lijken onschuldig, maar zijn vaak zonder abstracte theorie moeilijk te begrijpen. Veel crypto-systemen zijn van dezelfde eenvoud. Maar dat wil nog niet zeggen dat ze in korte tijd zijn op te lossen.

Om het te begrijpen: als je een telefoon-boek hebt, dan zoek je bij een naam vrij snel een nummer; omgekeerd, als je een nummer hebt dan kun je de bijbehorende naam vinden door het hele boek door te werken (het is een eindig probleem ... !) tot je dat nummer tegenkomt, maar dat zou wel eens heel lang kunnen duren. Dit eenvoudige principe gebruiken we allemaal dagelijks.

Het 15-spel is een eindig probleem, door álle mogelijkheden na te gaan krijgt je tenslotte wel een oplossing, als die er is, maar hoe lang zou je dan bezig zijn? En als er geen oplossing is, hoe zie je dat door "gewoon" te proberen? Zie ook (9.2).

(14.1) Men zegt dat de puzzel-expert Sam Loyd (soms gespeld als Sam Lloyd, of Samuel Loyd, 1841-1911) in 1878 een puzzel maakte die bestaat uit een rechthoekige doos van afmeting 4×4 met daarin 15 blokjes genummerd van 1 tot en met 15. We kunnen blokjes horizontaal of verticaal schuiven naar het lege vakje. Uitgaande van een beginsituatie is de opgave door schuiven de **standaard-situatie** te bereiken:

1	**2**	**3**	**4**
5	**6**	**7**	**8**
9	**10**	**11**	**12**
13	**14**	**15**	**L**

De beginsituatie die Loyd als uitdaging gaf bestond uit: alle blokjes $1, \cdots, 13$ op hun plaats, en dan daarna 15 en 14 (verkeerd om). Het lijkt een eenvoudig opgave. Een beetje schuiven, en dan de uitgeloofde prijs van \$ 1000 incasseren. Loyd schrijft daarover in "Sam Loyd's Cyclopaedia of 5000 Puzzles, Tricks and Conundrums",

`http://www.mathpuzzle.com/loyd/`

gepubliceerd in 1914 door zijn zoon (die ook Sam Loyd heette):

"*Older inhabitants of Puzzleland will remember how in the seventies I drove the entire world crazy with a little box of movable blocks which became known as the "14-15 Puzzle". The fifteen blocks were arranged in the square box in rectangular order, but with the 14 and 15 reversed. The puzzle consisted of moving the blocks about, one at a time, to bring them back to the present position in every respect except that the error in the 14 and 15 was corrected.*

A prize of \$1000, offered for the first correct solution to the problem, has never been claimed, although there are thousands of persons who say they have performed the required feat.

People became infatuated with the puzzle and ludicrous tales are told of shopkeepers who neglected to open their stores; of a distinguished clergyman who stood under a street lamp all through a wintry night trying to recall the way he had performed the feat. The mysterious feature of the puzzle is that none seem able to remember the sequence of moves whereby they feel sure they have succeeded in solving the puzzle. Pilots are said to have wrecked their ships, and engineers rush their trains past stations. A famous Baltimore editor tells how he went for his noon lunch and was discovered by frantic staff long past midnight pushing little pieces of pie around on a plate! Farmers are known to have deserted their ploughs ... "

Opmerking. Het is mogelijk dat Loyd deze puzzel overnam van een eerdere bron, zie: Jerry Slocum and Dic Sonneveld - "The 15 Puzzle"(ISBN 1-890980-15-3): "Sam Loyd heeft de 15 puzzel niet uitgevonden en heeft ook niets te maken met het populariseren van deze puzzel.

De puzzel-gekte die ontstond rond de 15 Puzzle begon in januari 1880 in Amerika en in april in Europa. De gekte eindigde in juli 1880 en Sam Loyds eerste artikel over de 15 puzzel werd pas 16 jaar later gepubliceerd, in januari 1896. Loyd beweerde voor het eerst in 1891 dat hij de puzzel heeft uitgevonden, en hij hield deze leugen vol tot aan zijn dood 20 jaar later. De echte uitvinder was Noyes Chapman, een postbeambte uit New York, die al een patent aanvroeg in maart 1880."
Zie `http://bd.thrijswijk.nl/15puzzle/15puzznl.htm`

(14.2) Is de puzzel wel zo eenvoudig? Een paar blokjes in een doosje. Met wat schuiven kun je toch alle situaties analyseren?
Opgave. Onderstel dat iemand elke seconde één situatie van het 15 spel realiseert, 12 uur per dag, 365 dagen per jaar. Hoeveel jaar zou die persoon dan bezig zijn? (Hint: $16! = 1 \times 2 \times \cdots \times 16 = 20922789888000$.)

Het blijkt dat "even proberen" niet zo eenvoudig is. Het zal ook blijken dat de duivelse opgave die Sam Loyd voorstelde geen oplossing heeft. In plaats van "domweg proberen" gaan we nadenken.

(14.3) De constructie van een invariant. Zij S een situatie, d.w.z. een rijtje getallen waar $1, \cdots, 16$ precies een keer in voorkomen. We definiëren $v(S)$ als het aantal paren in S dat verkeerd om staat: het aantal paren getallen (x, y) zodanig dan x in S eerder voorkomt dan y, maar $1 \leq y < x \leq 16$; we geven met $s(S)$ aan het aantal stappen dat $L = 16$ afstaat van de linker-onderhoek. We definiëren $d(S) := v(S) + s(S$. Verder,

$$\text{als } d(S) \text{ even is dan schrijven we } p(S) = +,$$

$$\text{als } d(S) \text{ oneven is dan schrijven we } p(S) = -;$$

d voor *defect*, en p voor *pariteit*.

Merk op: voor de standaard-situatie S geldt $v(S) = 0$ en $s(S) = 0$ en $p(S) = +$.

(14.4) Een voorbeeld.

L	**14**	**11**	**8**
15	**1**	**5**	**6**
4	**7**	**2**	**3**
12	**10**	**9**	**13**

We zien hier de situatie:

$$L = 16, 14, 11, 8, \quad 15, 1, 5, 6, \quad 4, 7, 2, 3, \quad 12, 10, 9, 13.$$

We geven aan hoeveel cijfers na x kleiner zijn dan x:

$$L = 16\ (15),\ \ 14\ (13),\ \ 11\ (10),\ \ 8\ (7),\ \ \ 15\ (11),\ \ 1\ (0),\ \ 5\ (3),\ \ 6\ (3),$$

$$4\ (2),\ \ 7\ (2),\ \ 2\ (0),\ \ 3\ (0),\ \ \ 12\ (2),\ \ 10\ (1),\ \ 9\ (0),\ \ 13\ (0).$$

We concluderen dat er 69 paren verkeerd om staan: $v(S) = 69$. Het aantal stappen van L tot de linker-onderhoek is $s(S) = 6$. Conclusie: $d(S) = 69 + 6$, en $p(S) = -$.

(14.5) Stelling. *Als we een begin-situatie S hebben met $p(S) = -$, dan is deze niet door schuiven in de standaard-situatie over te voeren.* (Deze puzzel is in de helft van de gevallen niet op te lossen.)

Conclusie. We zien dat deze situatie zoals beschreven in (14.4) door schuiven niet goed te krijgen is (niet over te voeren is in de standaard-situatie).
Gevolg. De opgave gesteld door Sam Loyd, de begin-situatie $1, \cdots, 12, 13, 15, 14, L$, is niet door schuiven tot de standaard-situatie te herleiden: *de puzzel is onoplosbaar.*

Prachtig toch: in plaats van dom en lang proberen, bewijzen we in een paar regels dat de "14-15-puzzel" van Sam Loyd (met de 14 en 15 verwisseld) niet oplosbaar is. Nadenken loont de moeite.

Bewijs van Stelling (14.5). We nemen een situatie S: een rijtje getallen waar $1, \cdots, 16$, waar $L = 16$, elk precies een keer in voorkomen. We schrijven S' voor de situatie die we krijgen door precies één keer te schuiven. We bewijzen:

$$p(S) \quad = \quad p(S').$$

Horizontaal schuiven. Als we één keer horizontaal schuiven van verandert $v(S)$ met precies één. Inderdaad, als we een blokje naar links schuiven, dan gaat $\cdots, L, x, \cdots$ over in $\cdots, x, L, \cdots$ en alle paren ongelijk aan (L, x) blijven in dezelfde stand staan; we zien dat $v(S) - 1 = v(S')$; verder verder verandert $s(S)$ met precies één. We zien dat $d(S) - d(S') \in \{-2, 0, 2\}$. Dus $p(S) \quad = \quad p(S')$ als S' verkregen wordt uit S door precies één keer horizontaal naar links schuiven. Omdat één keer horizontaal naar rechts schuiven $S \mapsto S'$ de omkering is van één keer horizontaal naar links schuiven $S' \mapsto S$, volgt ook voor die handeling $p(S) \quad = \quad p(S')$
Verticaal schuiven. Veronderstel dat we een blokje naar boven schuiven. Dan is S gelijk aan $S = S_1 \cup \{x, y, z, t, L\} \cup S_2$ en $S' = S_1 \cup \{L, y, z, t, x\} \cup S_2$. Bewering: $v(S) - v(S')$ is *oneven*; inderdaad, de paren (x, y), (y, L), en (x, z), (z, L) en (x, t), (t, L) veranderen allemaal en het het paar (x, L) gaat over in (L, x); dit bewijst het gevraagde. Omdat ook $s(S) - s(S')$ oneven is concluderen we $p(S) \quad = \quad p(S')$. Omdat de handeling een blokje naar onderen schuiven de omgekeerde handeling is, volgt ook in die situatie dat $p(S) \quad = \quad p(S')$.

Een eindig aantal keren schuiven is niets anders dan een eindig aantal keren één keer schuiven. We zien dat onder een eindig aantal keren schuiven $p(S)$ niet verandert. Als we beginnen met $p(S) = -$ dan kunnen we niet schuiven tot we in de standaard situatie met $p(\text{standaard}) = +$ komen. Dit bewijst de stelling. QED

(14.6) Vraagstuk. Bewijs: *als $p(S) = +$, dan is deze situatie door schuiven wel over te voeren in de standaard-situatie.*

(14.7) Conclusie. Van alle begin-situaties is precies de helft onoplosbaar, en de andere helft oplosbaar.

(14.8) Een voorbeeld bij het bewijs.

•	•	•	•
•	**L**	**7**	**8**
9	**6**	•	•
•	•	•	•

Noem deze situatie S en schuif het blokje 6 naar boven; noem die nieuwe situatie S'. Ga na: $d(S') - d(S) = 7 - 1 = 6$.

(14.9) Vraagstuk. We krijgen het spel, maar nu met letters op de blokjes. Hieronder een begin-situatie. Kunnen we zo schuiven dat de spelling correct wordt? Zie (16.18).

D	**E**	**N**	**K**
O	**F**	**S**	**C**
H	**U**	**I**	**F**
W	**T**	**A**	

15 Nog een paar vraagstukken

(15.1) Vraagstuk. Mijn rekenmachine geeft $\sqrt{3339590081146975295} = 1827454536$. Is dat antwoord goed? Zie (16.19).

Nadenken is vaak beter dan het gebruik van een rekenmachine.

(15.2) Vraagstuk. (1) Gegeven zijn 5 punten in $\mathbb{R}^2$, waarvan er geen drie op één rechte liggen. Bewijs dat er 4 van deze punten gekozen kunnen worden zodanig dat de vierhoek met deze punten als hoekpunten convex is.
(2) Ga na hoeveel convexe 4-hoeken er zo gekozen kunnen worden (afhankelijk van de ligging van die punten).
Zie (16.20).

(15.3) Opmerking: het "Happy End Problem" (Ester Klein, 1933). We kunnen ons afvragen hoeveel punten $f(n) = N$ we minimaal nodig hebben (geen drie op een rechte) om zeker te weten dat er een convexe n-hoek geconstrueerd kan worden uit deze punten. We zien direct dat $f(3) = 3$, en uit de vorige opgave zien we dat $f(4) = 5$.
Eenvoudig vraagstuk. Bewijs dat $f(5) > 6$ (m.a.w. construeer een 6-tal punten waaruit geen enkel 5-tal een convexe vijfhoek geeft).
Moeilijk vraagstuk. Bewijs dat $f(5) = 9$.
Voor een verdere discussie, zie:

`http://en.wikipedia.org/wiki/Happy_Ending_problem`
`http://mathworld.wolfram.com/HappyEndProblem.html`
`http://neeldhara.com/ramblings/notes/cgt-01`
`http://planetmath.org/happyendingproblem`
`http://pythagoras.nu/pyth/pdf/artikel_50285_20-24.pdf`

(15.4) De definitie van een graaf; Ramsey theorie. Een *graaf* bestaat uit hoekpunten en zijden. Elke zijde is een lijnstuk, en de twee uiteinden zijn gehecht aan een hoekpunt; het is toegestaan dat er een "lus" (Engels:"loop") is, dat wil zeggen een zijde waar begin- en eindpunt gelijk zijn; het is toegestaan dat er meerdere zijden tussen twee hoekpunten zijn. Grafen worden vaak gebruikt om combinatorische problemen inzichtelijk te maken. We zien een graaf als een abstract concept; soms kun je een graaf visualiseren als een ruimtelijke figuur; niet elke graaf is in te bedden in een vlak. Vaak worden eindige grafen bestudeerd (het aantal hoekpunten en het aantal zijden is eindig).

Een *eindige volledige graaf*, notatie K_n bestaat uit n hoekpunten, en de zijden zijn precies alle verbindingen tussen alle paren van twee verschillende hoekpunten.
De volledige 3-graaf: een driehoek.
De volledige 4-graaf: een tetraëder.

In Ramsey theorie wordt bestudeerd welke disjuncte complete deel-grafen voorkomen in een volledige graaf.
Zie § 33 van [24]. Zie `http://en.wikipedia.org/wiki/Ramsey_theory`

(15.5) Opmerking. We kunnen eenvoudig inzien dat niet elke graaf in het vlak $\mathbb{R}^2$ ingebed kan worden zonder dat zijden elkaar kruisen. Heel eenvoudigste voorbeeld:
Neem een graaf bestaande uit de hoekpunten G, W, E, A, B, C in $\mathbb{R}^2$. We proberen van elk van G, W, E een leiding te leggen naar elk van de huizen A, B, C zonder dat leidingen elkaar kruisen. Opgave: dat is niet mogelijk. (Dit is de volledige graaf K_3.)

(15.6) Vraagstuk $R(3,3)$**.** We nemen een volledige n-graaf, en kleuren elke zijde óf rood (R) óf blauw (B), en we vragen ons af of er in deze K_n een volledige rode K_3 (een rode driehoek) of een volledige blauwe K_3 (een blauwe driehoek) geforceerd voorkomt.
(a) Laat zien dat in een K_5 (een volledige 5-graaf) de zijden zo te kleuren zijn dat er geen rode en ook geen blauwe driehoek in voorkomt.
(b) Laat zien dat voor elke $n \geq 6$ er in een volledige n-graaf met rode en blauwe zijden er tenminste één rode of tenminste één blauwe driehoek voorkomt.
Opmerking. Het resultaat hier gevraagd wordt genoteerd als: $R(3,3) = 6$, waarmee we willen zeggen dat als we twee kleuren gebruiken (het aantal cijfers in $R(\cdots)$), dat we driehoeken zoeken (de getallen 3 en 3), en dat de minimale n die tenminste een dergelijke driehoek forceert

gelijk is aan $n = 6$ in dit geval.
Zie (16.21).

(15.7) Vraagstuk $R(3,4) = 9$**. (a)** Geef een volledige 8-graaf, waarvan de zijden of rood of blauw zijn, zodanig dat er geen rode driehoek, en geen blauw tetraëder voorkomt in deze K_8.
(b) Bewijs dat in een K_9 waarvan de zijden rood of blauw zijn er of een rode driehoek of een blauw tetraëder voorkomt.
(Kortom: $R(3,4) = 9$.)
Zie (16.22)

(15.8) Opmerking. Er gelden de volgende resultaten: $R(3;5) = 14$, $R(3;6) = 18$, $R(3;7) = 23$, $R(3;8) = 28, R(3;9) = 36$. (Probeer hier maar iets van te bewijzen.) Voor nog veel meer resultaten, zie
`http://en.wikipedia.org/wiki/Ramsey%27s_theorem`
`http://mathworld.wolfram.com/RamseyNumber.html`

(15.9) Een Ramsey-spel. Hier is een voorstel voor een spel, een variatie op "Boter, Kaas en Eieren":
twee spelers nemen een vel papier en tekenen daarop daarop 6 punten; de ene speler heeft een rood potlood, de ander een blauw; besloten wordt wie er begint; om beurten wordt een "zet gedaan", en die bestaat uit het trekken van een (mogelijk gebogen) lijnstuk tussen twee van die punten die niet reeds verbonden zijn; dat lijnstuk gaat niet door een van de andere vier punten; dat lijnstuk mag wel andere lijnstukken, die reeds getrokken zijn, snijden; het is duidelijk dat na hoogstens 15 zetten alle mogelijke zijden getekend zijn; winnaar is diegene die het eerste een driehoek van de eigen kleur maakt.
Opmerkingen.

- Omdat $R(3,3) = 6$ eindigt het spel met een winnaar.
- In plaats van 6 punten kunnen we ook met meer punten beginnen, en het spel verloopt precies zo.

(15.10) Een vraagstuk over het Ramsey-spel. Bewijs dat de speler die begint in het het Ramsey $3-3-$spel, zie (15.9), winst kan forceren. Zie (16.23).

(15.11) Nog een Ramsey-spel. Idem als boven, eveneens met twee spelers, maar nu beginnen we met ≥ 18 punten, en winnaar is diegene die het eerst een tetraëder van de eigen kleur afmaakt; het spel eindigt omdat $R(4,4) = 18$ (Greenwood en Gleason, 1955).

(15.12) Vraagstuk $R(3,3,3) = 17$.
(< 17) Bewijs dat de volledige K_{16} een kleuring van de zijden met drie kleuren toelaat, zodat er geen monochrome driehoeken zijn.
(≥ 18) Bewijs dat in de volledige K_{17} elke kleuring van de zijden met drie kleuren er een monochrome driehoek is.
Zie `http://en.wikipedia.org/wiki/Ramsey's_theorem`voor bewijzen.

(15.13) Een Ramsey $3-3-3$−spel. (Dit lijkt wel leuk, maar ook niet erg practisch uitvoerbaar.) Drie spelers zetten 17 punten op een vel papier; zij kunnen de zijden drie verschillende kleuren geven. Verder zijn de spelregels als in (15.9). Winnaar is diegene die het eerst een monochrome driehoek volmaakt.

Waarschijnlijk moeten we nog de volgende spelregel opnemen. Elke speler die aan zet is, en die niet een monochrome driehoek kan maken is verplicht eventuele mogelijkheden van andere spelers om direct te winnen (twee zijden van één kleur, en de derde zijde is nog open) eerst te blokkeren door een van die driehoek(en) af te maken.

Ik weet niet welk van de spelers in dit spel winst kan forceren.

(15.14) Vraagstuk. Deze opgave komt uit [25], Ch.6, Problem 6.4. We hebben 27 blokken van afmeting $1 \times 2 \times 4$. Kunnen we die stapelen tot een kubus met afmeting $6 \times 6 \times 6$? Zie (16.24).

(15.15) Vraagstuk. Zij $n \in \mathbb{Z}_{>0}$. Bewijs dat er een $a \in \mathbb{Z}_{>0}$ bestaat zodanig dat er in de rekenkundige rij

$$\{a, a+n, a+2n, \cdots\} = \{a+in \mid i \in \mathbb{Z}_{>0}\}$$

er oneindige veel priemgetallen zijn. Zie (16.25)

(15.16) Een diepe stelling van Dirichlet.* Een stelling van Dirichlet zegt: voor alle $a, n \in \mathbb{Z}_{>0}$ met $\gcd(a,n) = 1$ is er in de rekenkundige rij

$$\{a, a+n, a+2n, \cdots\} = \{a+in \mid i \in \mathbb{Z}_{>0}\}$$

oneindig veel priemgetallen. Die stelling is niet eenvoudig te bewijzen. Curieus: de opgave (15.15) (waarvan de uitspraak wezenlijk zwakker is dan die van de stelling van Dirichlet, is dat duidelijk?) is heel eenvoudig en elementair te bewijzen, en wel zonder gebruik te maken van deze stelling van Dirichlet.

(15.17) Vraagstuk (M. Kontsevic & D. Zagier). Voor $\alpha, \beta \in \mathbb{R}$ construeren we een rij getallen $\{x_i \mid i \in \mathbb{Z}_{>0}\}$ door:

$$x_1 = \alpha, \quad x_2 = \beta, \quad x_3 = \mid x_2 \mid -x_1, \quad \cdots, \quad x_{i+2} = \mid x_{i+1} \mid -x_i, \cdots.$$

(Een symmetrische manier om deze voorwaarde te geven: $\forall i, \quad x_{i-1} + x_{i+1} = \mid x_i \mid$, en we kunnen net zo goed de rij $\{x_i \mid i \in \mathbb{Z}\}$ beschouwen.)
Bewijs dat er bestaat een $N \in \mathbb{Z}_{>0}$ (onafhankelijk van α en β), zodanig dat

$$\forall \alpha, \quad \beta, \quad i > 0 \quad \text{geldt:} \quad x_i = x_{i+N}.$$

Met andere woorden: *die rij is periodiek*, en de periode hangt niet af van de keuze van α en β.
(Er is geen oplossing te vinden in deze syllabus, maar in de cursus hoop ik een oplossing bespreken. Graag hoor ik hoe iemand er aan begint, en wat voor bewijs er uit komt.) Opmerking: voor $\alpha = 0 = \beta$ komt er $x_i = 0$ voor alle i; voor elke keus $(\alpha, \beta) \neq (0,0)$ blijkt de minimale periode niet af te hangen van de keuze van (α, β).
In het artikel [52] staan oplossingen van dit vraagstuk.

16 Oplossingen van een aantal vraagstukken

(16.1) Oplossing van (1.1). We zien $(B+1)^2-B^2 = 2B+1$; alle oneven positieve getallen komen zo voor. Voor elke oneven

$$A = 2r+1 \quad \text{kiezen we} A^2 = 2B+1: \quad B = 2r^2+2r.$$

Dan is

$$A^2 = (2r+1)^2 = 4r^2+4r+1 = 2B+1; \quad \text{dus} \quad A^2+B^2 = (B+1)^2.$$

Voorbeelden:

$$r = 1: \quad A = 3, \quad B = 4, \quad 3^2+4^2 = (4+1)^2;$$
$$r = 2: \quad A = 5, \quad B = 12, \quad 5^2+12^2 = (12+1)^2,$$

etc.

(16.2) Oplossing van (1.4). Inderdaad, $y^2 = (2r)^2 = 4\times r^2$ en $x^2 = (2s+1)^2 = 4(s^2+s)+1$.

Omdat (x,y,z) een pPD is, zijn niet x en y allebei even. We laten nu zien dat allebei oneven ook niet mogelijk is: als x en y allebei oneven dan is

$$x^2+y^2 \equiv 2 \pmod 4;$$

in dat geval is x^2+y^2 niet het kwadraat van een geheel getal (zoals we hierboven zagen).

(16.3) Oplossing van (1.8). Als 3 voorkomt in de priemfactorontbinding van b^2 dan is dat ook zo voor b en omgekeerd.

Als $b^2 \equiv 1 \pmod 3$ dan is b niet deelbaar door 3; als b niet deelbaar is door 3, dan is

$$b \equiv \pm 1 \pmod 3, \quad \text{dus} \quad b^2 \equiv (\pm 1)^2 \pmod 3.$$

Neem aan dat (x,y,z) een pPD is en dat 3 wel een deler is van $x-y$; dan is 3 niet een deler van x en ook niet van y, want (x,y,z) is een pPD. Dan is

$$x^2+y^2 \equiv 2 \pmod 3,$$

een tegenspraak met $x^2+y^2 = z^2$.

(16.4) Oplossing van (1.9) Uit het vorige vraagstuk weten we dat de leeftijd a van de man, en de leeftijd b van de vrouw niet deel uitmaken van een pPD. Dus zijn die beide leeftijden deelbaar door 3; bovendien is het verschil tussen $a/3$ en $b/3$ gelijk aan 1; dus maken $a/3$ en $b/3$ deel uit van een pPD en $(b/3)+1 = (a/3)$. Omdat bovendien die leeftijden liggen tussen 40 en 110 zien we dat $a = 3\times 21$ en $b = 3\times 20$ een mogelijkheid is.

Om te bewijzen dat er maar één oplossing mogelijk is kunnen we door rekenen alle gevallen nagaan. We weten dat $y^2+(y+1)2 = z^2$ met $17 < y < 35$ (wat de leeftijd van die "oude man" ligt ergens tussen 54 en 108). We weten dat $y = m^2-n^2$ en $y+1 = 2mn$ of omgekeerd. Het is eenvoudig die gevallen door te rekenen. Voor $m+n \le 13$: zie (1.6). Gebruik makend van $17 \le 2mn \le 36$ blijven over de gevallen $(m,1)$ met $12 \le m \le 26$ (en die vallen af) en het geval $(13,2)$ (die ook afvalt). Een ondoorzichtige rekenpartij. Zie (1.10) voor een veel beter argument.

(16.5) Oplossing van (2.5). (Met iets meer techniek laten we zien dat elk priemgetal $p \equiv 3 \pmod 4$ niet een deler is van z in een pPD.) Als 3 een deler is van z, dan is 3 niet een deler van x en niet een deler van y; dan komt er

$$x^2 + y^2 \equiv 2 \pmod 3,$$

een tegenspraak. (Deze bewijsmethode kunnen we niet gebruiken voor andere priemgetallen).

(16.6) Oplossing van (2.7). We weten dat er bestaan gehele getallen $b > a > 0$ bestaan met $a^2 + b^2 = p$. Schrijf:

$$p^2 = \{(b+ai)(b+bai)\}\cdot\{(b-ai)(b-ai)\}m = \{(b^2-a^2)+2abi\}\cdot\{(b^2-a^2)+2abi\} = (b^2-a^2)^2+(2ab)^2.$$

(Voor p^2 behandelen we $b^2 - a^2$ als "m" en $2ab$ als "n".) Voor $x := (b^2 - a^2)^2 - (2ab)^2$ en $y := (b^2 - a^2)^2 \times (2ab)^2$ komt er inderdaad

$$x^2 + y^2 = (p^2)^2.$$

Inderdaad, check:

$$(p^2)^2 = ((b^2 - a^2)^2 - (2ab)^2)^2 + ((b^2 - a^2)^2 \times (2ab)^2)^2 = (b^2 + a^2)^2.$$

Bovendien zijn $b + a$ en $b - a$ en a en b niet deelbaar door p; daarom is dit een pPD.
Voorbeelden.
$a^2 + b^2 = p$, $A = b^2 - a^2$, $B = 2ab$, $\pm x = (b^2 - a^2)^2 - (2ab)^2$, $\pm y = (b^2 - a^2)^2 \times (2ab)^2$:

p	a	b	A	B	x	y	$x^2 + y^2 = (p^2)^2$
5	1	2	3	4	7	24	$7^2 + 24^2 = (5^2)^2$
13	2	3	5	12	119	120	$119^2 + 120^2 = 28561 = (13^2)^2$
17	1	4	15	8	161	240	$161^2 + 240^2 = 83521 = (17^2)^2$
29	2	5	21	20	41	840	$41^2 + 840^2 = 707281 = (29^2)^2$
37	1	6	35	12	1081	840	$1081^2 + 840^2 = 1874161 = (37^2)^2$
41	4	5	9	40	1519	720	$1519^2 + 720^2 = 2825761 = (41^2)^2$
etc.	etc.	etc.	etc.	etc.	etc.	etc.	etc.

(16.7) Oplossing van (3.3). We zien dat $x \in \{1, 3, 5\}$;
$(1, 1, 9)$ is een denkpunt van σ, en die involutie verwisselt de volgende paren:
$(1, 9, 1)$ en $(3, 1, 7)$; $(1, 3, 3)$ en $(5, 3, 1)$; $(3, 7, 1)$ en $(5, 1, 3)$;
het dekpunt van τ is $(1, 3, 3)$, corresponderend met $37 = 1^2 + 4 \times 3 \times 3 = 1^2 + 6^2$
(en het is duidelijk hoe τ andere elementen van S verwisselt).

(16.8) Oplossing van (3.4). Inderdaad kunnen we S geven als

$$S = \{(x, y, z) \in (\mathbb{Z}_{>0})^3 \mid x^2 + 4yz = 65\}.$$

We zien dat mogelijkheden voor x zijn: 1, 3, 5, 7. In het bijzonder is x oneven (want $65-4yz$ is oneven). Dus is $x = 2y$ niet mogelijk. We gebruiken nu al vast dat $65 = 1+64 = 25+49$ de enige manieren zijn om 65 als som van kwadraten te schrijven (eenvoudig na te gaan). Als we een drietal zouden hebben met $x = y-z$ dan is $x^2+4yz = y^2+z^2 = 65$; maar $x^2+4\times1\times8 = 65$ en $x^2 + 4 \times 5 \times 7 = 65$ zijn niet oplosbaar; we concluderen $x \neq y - z$ in alle gevallen, en σ *is*

goed gedefinieerd. Eenvoudig na te gaan: $\#(S) = 5+4+4+3 = 16$; inderdaad, als $x = 1$ dan is $yz = 16$ en dat geeft de mogelijkheden $(y, z) = (16, 1), \quad (8, 2), \quad (4, 4), \quad (2, 8), \quad (1, 16)$, de gevallen $x = 3, \quad 5, \quad 7$ gaan analoog:

$$x = 3, \quad yz = 56/4 = 14, \quad (14, 1), (7, 2), (2, 7), (1, 14),$$

$$x = 5, \quad yz = 40/4 = 10, \quad (10, 1), (5, 2), (2, 5), (1, 10),$$

$$x = 7, \quad yz = 16/4 = 4, \quad (4, 1), (2, 2), (1, 4).$$

We zien dat $\#(S)$ even is, τ is goed gedefinieerd, en τ heeft een even aantal dekpunten. Ik zie hier geen abstract argument om te laten zien dat τ tenminste één dekpunt heeft. Na rekenen (zie hierboven) zien we dat τ twee dekpunten heeft.

(16.9) Oplossing van (4.2). We merken op dat $x^2 \equiv 0, 1 \pmod 4$ voor elk geheel getal x: als x even is, dan is x^2 deelbaar door 4; als $x = 2n+1$ of $x = 2n+3$ dan is $x^2 \equiv 1 \pmod 4$. Dus is $a^2 + b^2 \equiv 0, \quad 1, \quad 2 \pmod 4$; dus $a^2 + b^2 \not\equiv 3 \pmod 4$.

(16.10) Oplossing van (4.3). (1) Het eerste deel van het vraagstuk volgt uit (4.2).
(2) Merk op dat als $A^2 + 1 = k \times p$ dan is ook $(p - A)^2 + 1 = (p - 2A + k) \times p$. We geven de waarden van p en A en k met $A^2 + 1 = k \times p$:

p	A	k
5	2	1
	3	2
13	5	2
	8	5
17	4	1
	13	2
29	12	5
	17	10
37	6	1
	31	26
41	9	2
	32	25
53	23	10
	30	17
61	11	2
	50	41
73	27	10
	46	29
89	34	13
	55	34
97	22	5
	75	58

(16.11) Oplossing van (9.14). Merk op dat voor elke $t \in \mathbb{Z}_{>0}$ geldt dat $10^t \equiv 1 \pmod 9$. Dus geldt dat $n \equiv s(n) \pmod 9$. Herhaal dit proces: $n \equiv s^j(n) \pmod 9$ voor alle n en alle j. Hieruit volgt het criterium.

(16.12) Oplossing van (9.15). Omdat $10 \equiv -1 \pmod{11}$ geldt $n \equiv a(n) \pmod{11}$. Herhaald toepassen hiervan geeft het resultaat.

(16.13) Oplossing van (9.24) We zien: $16^2 = 256 = -3 + 7 \times 37$. We kopmen b.v. op[deze oplossing door: $\mathbb{F}_{37}^*$ wordt voortgebracht door $\tau := 2 \bmod 37$, en $\tau^8 = 34 \bmod 37$, dus $(2^4)^2 \equiv 34 \pmod{37}$. Omdat $-16 \equiv +21 \pmod{37}$ geldt: $21^2 \equiv -3 \pmod{37}$.

(16.14) Een oplossing van (9.25). Uit

$$15^2 + 3 = 225 + 3 = 228 = 4 \times 3 \times 19$$

volgt dat alleen 2, 3 en 19 deze eigenschap hebben.

(16.15) Oplossing van (10.9). Er zijn $(41-1)/10$ van zulke paren (op verwisselen van x en y na): $(1,9), e = 2$, $(2,18), e = 8$, $(3,14), e = 5$, $(4,5), e = 1$, $(6,13), e = 5$, $(7,19), e = 10$, $(8,10), e = 4$, $(11,17), e = 10$, $(12,15), e = 9$, $(16,20), e = 16$. (Merk op: $e = 1$ komt precies éénmaal voor; de priemdelers van e zijn 3, dan en slechts dan als x en y allebei deelbaar door 3, en verder zijn 2 en 5 delers van de andere e; kunnen we dit verklaren?)

(16.16) Oplossing van (11.31)(1). Ga na: $3^8 \equiv 33 \pmod{64}$ en $3^{16} \equiv 1 \pmod{64}$. Laat zien dat de natuurlijke afbeelding

$$< 63 \bmod 64 > \times < 3 \bmod 64 > \xrightarrow{\sim} (\mathbb{Z}/64)^*$$

een isomorfisme is.
Oplossing van (11.31)(2). Ga na: $3^{10} = 19049 = 488 \times 121 + 1$ en $(1+11)^{11} \equiv 1 \pmod{121}$. Concludeer dat de orde van 33 mod 131 gelijk is aan 10×11.

(16.17) Oplossing van (11.32)(3). We zien dat $\text{orde}(k \bmod 41) < 40$ voor alle $k \in \{2,3,4,5\}$ en $\text{orde}(6 \bmod 41) = 40$. Dus is 6 mod 41 een voortbrenger, en

$$(\mathbb{Z}/40, +) \xrightarrow{\sim} ((\mathbb{F}_{41})^*, \times) \quad j \longmapsto 6^j \bmod 41$$

geeft een isomorfisme. Voor alle j met $1 \leq j < 40$ en $\text{ggd}(j, 40) = 1$ is daarom $6^j \bmod 41$ een voortbrenger. Dit geeft $\varphi(40) = \varphi(5) \cdot \varphi(8) = 4 \cdot 4 = 16$ elementen die als voortbrenger van $(\mathbb{F}_{41})^*$ kunnen optreden:

$$\{1 \leq j < 40 \mid \text{ggd}(j, 40)\} \cong \{6^j \bmod 41 \mid j = 1, \ \ 3, \ \ 7, \ \ 9, \cdots, 37, \ \ 39\}.$$

Voorbeelden van die beelden $(6^j \bmod 41) \in (\mathbb{F}_{41})^*$:

$$j = 1: \quad 6; \quad j = 3: \quad 6^3 \equiv 11 \pmod{41};$$

$$j = 7: \quad d^7 \equiv 29 \pmod{41}; \quad \cdots \quad ; j = 39: \quad d^{39} \equiv 8 \pmod{41};$$

zo kunnen alle elementen die een voortbrenger zijn van $(\mathbb{Z}/41)^*$ berekend worden.
Zie [7], tabel op pag. 357 voor een voortbrenger van $(\mathbb{F}_p)^*$ voor $p < 1000$.

(16.18) Oplossing van (14.9). Als de twee letters F in de beginsituatie als verschillend aangemerkt worden, dan is deze puzzel niet door schuiven op te lossen, want de situatie is oneven. Maar als de twee letters F als dezelfde gezien worden, dan kunnen we de puzzel oplossen door de eerste F, die op plek 6 staat, later op plek 12 te zetten, en de tweede F, die op plek 12 staat, later op plek 6 te zetten. Deze verwisseling maakt de situatie even, en de puzzel is dan op te lossen. (Zouden we dit ooit vinden als we de abstracte structuur niet kennen?)

(16.19) **Oplossing van** (15.1). Nee, dit getal is niet een kwadraat want dit getal is wel door 5 maar niet door 25 deelbaar. Of:

$$115655394429732562 9695 \equiv 2 \pmod{11}.$$

De kwadraten modulo 11 zijn $0, 1, 3, 4, 5, 9$. Dit is daarom niet een kwadraat.

(16.20) **Oplossing van** (11.17). Het is duidelijk dat 2 niet een deler is van een getal van de vorm $M_n = 2^n - 1$.
Bewering. Elk priemgetal $p > 2$ is wel deler van een Mersenne getal.
Bewijs. Uit de stelling van Lagrange, (11.7), volgt

$$(2 \bmod p)^{p-1} = (1 \bmod p) \in (\mathbb{Z}/p)^*, \quad p > 2.$$

We zien dat een priemgetal $p > 2$ een deler is van M_{p-1}.

subsection**Oplossing van** (15.2). Eerst een constructie. We schrijven $V^c \subset \mathbb{R}^2$ voor de kleinste convexe verzameling die een verzameling $V \subset \mathbb{R}^2$ bevat; die bestaat: neem de verzameling $\Gamma(V)$ van alle convexe verzamelingen die V bevat; merk op $\Gamma(V) \neq \emptyset$ (want $\mathbb{R}^2 \in \Gamma(V)$); de doorsnede

$$V^c := \cap_{C \in \Gamma(V)} \ C$$

is convex (ga na), en voldoet aan de eisen. De verzameling V^c wordt het *convexe omhulsel* van V genoemd,

Beschrijf V^c voor een eindige verzameling V.
(1) Zij V^c het convexe omhulsel van $V := \{P_1, \cdots, P_5\}$. We zien dat er 3 mogelijkheden zijn:
(d) V^c is een driehoek, en er zijn twee inwendige punten in V^c;
(vier) V^c is een convexe vierhoek, en er is 1 inwendig punt;
(vijf) V^c is een convexe vijfhoek.

(1) + (2) In het geval (vijf) geeft elk 4-tal van deze punten een convexe vierhoek; in dit geval is het aantal convexe vierhoeken dat zo geconstrueerd kan worden gelijk aan 5.

In het geval (vier) zien we al één convexe vierhoek, zeg P_1, P_2, P_3, P_4; trek diagonalen in die vierhoek; als $Q = P_5$ gelegen is in de driehoek gevormd door P_1 en $[P_2, P_3]$, dan is $[P_2, P_3, P_4, P_5]$ convex: elke diagonaal geeft een extra convexe vierhoek; in dit geval is het totale aantal convexe vierhoeken gelijk aan 3.

In het geval (d) hebben we een driehoek, zeg $[P_1, P_2, P_3]$, met twee inwendige punten. De lijn door P_4 en P_5 heeft twee punten aan de ene kant, en één punt, zeg P_3, aan de andere kant; dan is $[P_1, P_2, P_4, P_5]$ de enige convexe vierhoek die in dit geval geconstrueerd kan worden.

(16.21) Een oplossing van (15.6) **(a)** Neem $P_1, \cdots, P_5$, en geef de zijden $< P_1P_2 >, \cdots, < P_4P_5 >, < P_5P_1 >$ een rode kleur, en alle ander zijden in deze complete 5-graaf een blauwe kleur. Het is duidelijk dat er geen rode driehoek voorkomt. Twee blauwe zijden die een hoekpunt gemeen hebben de andere hoekpunten verbonden door een rode zijde (ga na). Dit bewijst onderdeel (a).
(b) Neem een van de hoekpunten van een K_6 met rode en/of blauw gekleurde zijden; noem dat hoekpunt Q. In Q komen 5 gekleurde zijden aan, en tenminste 3 daarvan hebben dezelfde kleur. Veronderstel dat $< QP_1 >, < QP_2 >, < QP_3 >$ rood zijn; als tenminste een van de zijden $< P_1P_2 >, < P_2P_3 >, < P_3P_1 >$ rood is, dan is er een rode driehoek; als geen van deze zijden rood is, dan zijn ze alle drie blauw, en er is een blauwe driehoek.

(16.22) Oplossing van (15.7) **(a)** Maak een dergelijk voorbeeld, of zie bv.
`http://andrescaicedo.files.wordpress.com/2006/12/bsugrad2011.pdf`
(b) we onderscheiden een aantal gevallen:
(1) *Er is een hoekpunt Q in K_9 waar tenminste 4 rode zijden aangehecht zijn*; laat de andere uiteinden van die rode zijden P_1, P_2, P_3, P_4 zijn. Als een van de verbindingszijden $< P_iP_j >$ met $1 \leq i < j \leq 4$ rood is, dan komt er een rode driehoek. Als geen van die verbindingszijden rood is dan komt er een blauw tetraëder.
2) *Alle hoekpunten hebben precies 3 rode zijden aangehecht.* Dat kan niet: dan zouden er precies 9×3 uiteinden van een rode zijde zijn, maar dat aantal is even.
3) *Veronderstel dat* (1) *en* (2) *niet waar zijn.* Dan is er een hoekpunt T waar hooguit 2 rode zijden aangehecht zijn, dus minstens 6 blauwe zijden: $< TP_i >$ met $1 \leq i \leq 6$ zijn blauw. In de K_6 opgespannen door deze 6 punten geldt $R(3,3) = 6$, m.a.w. daarin is er of een rode driehoek (en we zijn klaar), of er is een blauwe driehoek, die samen met R een blauw tetraëder geeft. Einde bewijs.

(16.23) Een oplossing van (15.10). Zeg dat R begint en B de andere speler is. We nummeren de hoekpunten naar aanleiding van de eerste zetten (de nummering doet er niet toe, het is meer een notatie om ons bewijs op te schrijven). Er zijn twee mogelijkheden:
(I) De zet $B1$ heeft een hoekpunt met de zet $R1$ gemeen.
(II) De zet $B1$ heeft niet een hoekpunt met de zet $R1$ gemeen.
Notatie: Ri is de i-de zet van R, etc. We schrijven K voor keus, en F voor een geforceerde zet.

(I) $R1 =< 12 >$, $K:$ $B1 =< 23 >$,
$K:$ $R2 =< 14 >$, $F:$ $B2 =< 24 >$,
$F:$ $R3 =< 34 >$, $F:$ $B3 =< 13 >$,
$K:$ $R4 =< 15 >$, en B heeft geen verweer tegen de dreigingen $< 25 >$ en $< 45 >$.

(I) $R1 =< 12 >$, $K:$ $B1 =< 34 >$,
$K:$ $R2 =< 14 >$, $F:$ $B2 =< 24 >$,
$F:$ $R3 =< 23 >$, $F:$ $B3 =< 13 >$,
$K:$ $R4 =< 15 >$, en B heeft geen verweer tegen de dreigingen $< 25 >$ en $< 45 >$.

(16.24) Oplossing van (15.14). Het antwoord is: nee, uit deze 27 blokken van afmeting $1 \times 2 \times 4$ kunnen we niet een $6 \times 6 \times 6$ kubus maken.
Bewijs (uit [25]). We nemen een $6 \times 6 \times 6$ kubus K in gedachten en geven elke van de 6^3

deel-blokken van afmeting $1 \times 1 \times 1$ de kleur Z of W. Dat doen we als volgt. Verdeel de kubus K in $3 \times 3 \times 3$ kleinere kubussen k_i, elk van afmeting $2 \times 2 \times 2$. Alle $1 \times 1 \times 1$ blokje in een dergelijke deel-kubus k_i krijgen dezelfde kleur; bovendien kiezen we die kleuren zo dat aangrenzende k_i-kubussen verschillend van kleur zijn. Bv.:

Z		Z			Z			Z		Z
	Z		&	Z		Z	&		Z	
Z		Z			Z			Z		Z

Hier staat links de bovenste laag van 9 k_i's, midden de middelste laag, en rechts de onderste laag. We zien dat 14 k_i's de ene en 13 de andere kleur hebben. De kleuren zijn ongelijk verdeeld over de 27×8 blokjes van afmeting $1 \times 1 \times 1$.

Nu denken we ons in dat de 27 blokken gestapeld zouden kunnen worden tot een kubus K. We zien (ga na) dat van elk $1 \times 2 \times 4$ blok k_i dan precies 4 van de $1 \times 1 \times 1$ deel-blokken de ene en 4 de ander kleur krijgen. De kleuren zouden gelijk verdeeld zijn over de 27×8 blokjes van afmeting $1 \times 1 \times 1$; tegenspraak.

(16.25) Oplossing van (15.15). Beschouw alle $x \in \mathbb{Z}$ met $0 < x < n$, en beschouw alle

$$x \bmod n \in \mathbb{Z}/n.$$

Zij $\mathcal{P}$ de verzameling van alle priemgetallen en kijk naar de afbeelding

$$\mathcal{P} \longrightarrow \mathbb{Z}/n \qquad p \mapsto p \bmod n.$$

Merk op dat veelvouden van n niet een priemgetal zijn; we zien dat de oneindige verzameling $\mathcal{P}$ maar eindig veel beelden heeft in $\mathbb{Z}/n - \{0\}$. Voor tenminste één $x = a$ komen er oneindig veel priemgetallen terecht op $p \bmod n = a \bmod n$. Dit is de gevraagde a. (Merk op dat we niet bewijzen, wat wel waar is, dat élke a met $\text{ggd}(a, n) = 1$ gekozen kan worden.)

17 Vergelijking met [S]

Voor deze cursus gebruiken we als lesmateriaal het boek [S] en deze syllabus. Ik geef aan waarom we beide vormen van lesmateriaal kiezen, en ik geef wat overeenkomsten en verschillen.

Lees vooral de beschouwingen van Singh over de manier waarop wiskundigen tegen hun vak aankijken. Hij heeft daarvan prachtige beschrijvingen, vind ik. Ook staan er allerlei passages in over details die ook in de documentaire voorkomen, prettig om te lezen, en nog eens te overdenken.

Uit het voorwoord van John Lynch: *".. mathematicians simply hate to make a false statement .... formal statements have to be absolute."* De valkuil bij het begrijpelijk schrijven op een populaire manier over een moeilijk onderwerp geeft juist vaak aanleiding tot (licht) onjuiste mededelingen. Daarom zult U misschien de stof in het boek pakkend vinden, maar soms het materiaal in deze syllabus wat te saai? Dat is in beide gevallen met opzet zo. Ik geef een paar voorbeelden waar ik het met de formulering van Singh het niet wiskundig eens ben.

p.11 "Counting numbers are sometimes called *whole numbers*, and together with fractions (ratios between whole numbers) are technically referred to as *rational numbers*." In deze terminologie is $\frac{-1}{2}$ niet een rationaal getal.

Overigens, er is en verwarring over "whole number" en over het begrip "natuurlijk getal" in de zin dat de ene auteur wel en de andere auteur niet het getal 0 er ook onder rekent. Ik begrijp uit het boek van Singh dat hij bedoelt: "whole number" = "geheel getal groter dan nul".

p.84 In de bespreking van Euler en het probleem van de bruggen in Königsberg: "... a point should be connected to an even number of lines." (Te kort door de bocht; onjuist; geef tegenvoorbeelden.)

p. 198 De uitleg van de verbodsregels die in acht moeten genomen worden bij een Penrose betegeling zijn onvoldoende. Zonder die verbodsregels kun je een kite en een dart aaneenleggen tot een parallellogram, en met die figuur kun je het vlak betegelen met schuifsymmetrie (maar je krijgt niet een Penrose betegeling). Het stoort mij als er een vage (onvolledige) definitie gegeven wordt van een wiskundig begrip, zonder precisering of goede verwijzing; dat is heel eenvoudig voor dit geval, zie bijvoorbeeld

`http://en.wikipedia.org/wiki/Penrose_tiling`

of [23], of een van de vele prachtige andere artikelen over dit onderwerp

p.219 " ... there are 15 possible permutations given the three names involved." (??)

p. 216 De Frey kromme wordt gegeven door

$$+Y^2 = X(X + A^N)(X - B^N) \text{ of } Y^2 = X^3 + (A^N - B^N)X^2 - A^N B^N X.$$

Drukfouten in [S].

Op pag. 218 wordt Gerhard Frey onrecht aangedaan. In [18] zien we dat de logica perfect in orde is. Zie ook de tekst van Sarnak and of van Ribet in de documentaire.

Bij voorbeeld geeft Ribet een precieze beschrijving: "The Fermat-Taniyama connection grew out of a 1985 Oberwolfach lecture by G. Frey, who pointed out that a non-trivial solution to a $a^p + b^p = c^p$ (with p an odd prime) permits one to write down a semistable elliptic curve which does not appear to satisfy Taniyama's conjecture. Frey's curve is the elliptic curve E given by the deceptively simple cubic equation $y^2 = x(x - a^p)(x + b^p)$ (It might be necessary to effect a preliminary adjustment of (a, b, c) before writing down the curve.) In a manuscript which he distributed in Oberwolfach, Frey outlined an incomplete proof that his curve was not modular, i.e., that one has the implication "Taniyama $\Rightarrow$ Fermat." He expected that his proof would be completed by experts in the theory of modular curves." Zie
`http://math.berkeley.edu/~ribet/Articles/notices.pdf`

pp. 339/340 Bedoelt Singh dat alleen maar "dot diagrams" worden beschouwd met eindig veel lijnen en hoekpunten? (Zonder dat gegeven werkt het bewijs niet.) Ook kan ik een toegelaten "dot diagram" maken met één hoekpunt en nul lijnen (een wiskundige is precies in zulke gegevens).

Overigens, de zinsnede "Generations of mathematicians failed to find a proof of the .... dot conjecture." komt mij vreemd voor. Dit is een trivialiteit. Zie

`http://www.math.niu.edu/~rusin/known-math/00_incoming/dots`

`http://sci.tech-archive.net/Archive/sci.math/2007-02/msg03632.html` zegt: "I'm not sure it was ever a conjecture. It was given by Sylvester as a "Question for solution."A

proof was given by Gallai, and then other proofs appeared, ...Gallai's proof of Sylvester appeared in the American Mathematical Monthly, a journal for undergraduates, and took 2 pages. " (Waarom heeft Singh dit niet beter onderzocht ?)

18 Een aantal wiskundigen

http://en.wikipedia.org/wiki/Timeline_of_mathematics#1s_millennium_BC
http://nl.wikipedia.org/wiki/Lijst_van_wiskundigen
http://www-history.mcs.st-and.ac.uk/history/BiogIndex.html

Pythagoras (Pythagoras van Samos),
geboren tussen 580 en 572 vChr. - gestorven tussen 500 vCHr. en 490 vChr.

Aristoteles (Griekenland, 384 v. Chr. - 322 v. Chr.)

Euclides van Alexandrië (Ptolemaïsch Egypte, circa 365 v. Chr. - 275 v. Chr.)

Archimedes, (Archimedes van Syracuse), (Syracuse, 287 v. Chr. - 212 v. Chr.)

Diophantus, Diophantus van Alexandrië,
(Ptolemaisch Egypte, geboren tussen 200 and 214 - gestorven tussen 284 en 298)

Diophantus van Alexandria (Ptolemaisch Egypte, circa 298 v. Chr. - 214 v. Chr.)

Abu Ja'far Muhammad ibn Musa Al-Khwarizmi (Irak, geboren $\pm$ 780 - gestorven $\pm$850)

Abu Jafar Muhammad ibn al-Hasan Al-Khazin (Iran, $\pm$ 900 - $\pm$ 971)

Abu Mahmud Hamid ibn al-Khidr Al-Khujandi (Perzië, $\pm$ 940 - 1000)

Abu Ali al-Husain ibn Abdallah ibn Sina (Avicenna) (Uzbekistan, 980 - 1037)

Leonardo di Pisa, Leonardo Pisano Fibonacci, of gewoon Fibonacci,
(Italië, geboren tussen 1170 en 1180 - gestorven 1250)

Nicolaus Copernicus (Polen, 1473 - 1543)

Simon Stevin (Nederland, 1548 - 1620)

Johannes Kepler (Duitsland, 1571 - 1630)

Marin Mersenne (Frankrijk, 1588 - 1648)

René Descartes (Frankrijk, 1596 - 1650)

Claude Gaspar Bachet de Mziriac (Frankrijk, 1581 - 1638)

Pierre de Fermat (Frankrijk, 1601 - 1665)

Christiaan Huygens (Nederland, 1629 - 1695)

Isaac Newton (Groot-Brittannië, 1643 - 1727)

Gottfried Wilhelm von Leibniz (Duisland, 1646 - 1716)

Daniel Bernoulli (Zwitserland, 1700 - 1782),
Jakob Bernoulli (Zwitserland, 1654 - 1705),
Johann Bernoulli (Zwitserland, 1667 - 1748),
Nikolaus I Bernoulli (Zwitserland, 1687 - 1759)

Christian Goldbach (Duitsland, 1690 - 1764)

Leonhard Euler (Zwitserland, Rusland, 1707 - 1783)
Joseph-Louis Lagrange (Frankrijk, 1736 - 1813)

Adrien-Marie Legendre (Frankrijk, 1752 - 1833)

Marie-Sophie Germain (Frankrijk, 1776 - 1831) (‘‘Monsieur LeBlanc’’)
‘‘In describing the honourable mission I charged him with, M. Pernety informed me that he made my name known to you. This leads me to confess that I am not as completely unknown to you as you might believe, but that fearing the ridicule attached to a female scientist, I have previously taken the name of M. LeBlanc in communicating to you those notes that, no doubt, do not deserve the indulgence with which you have responded. Letter to Gauss (1807)’’ Zie ook [S] pag. 129.

Carl Friedrich Gauss (Duitsland, 1777 - 1855)

Jean Victor Poncelet (Frankrijk, 1788 - 1867)

Augustin Louis Cauchy (Frankrijk, 1789 - 1857)

Niels Henrik Abel (Noorwegen, 1801 - 1829)

Johann Peter Gustav Lejeune Dirichlet (Duitsland, 1805 - 1859)

Ernst Eduard Kummer (Duitsland, 1810 - 1893)

Karl Weierstrass (Duitsland, 1815 - 1897)

Evariste Galois (Frankrijk, 1811 - 1832)

Pafnuty Lvovich Chebyshev (Rusland, 1821 - 1894)

Bernhard Riemann (Duitsland, 1826 - 1866)

Max Noether (Duitsland, 1844 - 1921)

Georg Ferdinand Cantor (Duitsland, 1845 - 1918)

Felix Klein (Duitsland, 1849 - 1925)

Sofia Vasilyevna Kovalevskaya (Rusland, 1850 - 1891)

Johann Peter Gustav Lejeune Dirichlet (Duitsland, 1805 - 1859)

Hendrik Lorentz (Nederland, 1853 - 1928)

Thomas Joannes Stieltjes Jr (1856 -1884)

Henri Poincaré (Frankrijk, 1854 - 1912)

Thomas Jan Stieltjes (Nederland, 1856 - 1894)

David Hilbert (Duitsland, 1862 - 1943)

Jacques Salomon Hadamard (Frankrijk, 1865 - 1963)

Charles-Jean de La Vallée Poussin (België, 1866 - 1962)

Henri Lon Lebesgue (Frankrijk, 1875 - 1941)

Godfrey Harold Hardy (Groot-Brittannië, 1877 - 1947)

Luitzen Egbertus Jan Brouwer (Nederland, 1881 - 1966)

Emmy Noether (Duitsland, 1882 -1935)

Hermann Weyl (Duitsland, USA, 1885 -1955)

Srinivasa Aiyangar Ramanujan (India, Groot-Brittannië, 1887 - 1920)

Dirk Jan Struik (Nederland, USA, 1894 - 2000)

Maurits Cornelius Escher (Nederlands kunstenaar 1898 - 1972)

Oscar Zariski (Wit-Rusland, USA, 1899 - 1986)

Bartel Leendert van der Waerden (Nederland, 1903 - 1996)

Hans Freudenthal (Duitsland, Nederland 1905 - 1990)

André Weil (Frankrijk, 1906 - 1998)

Edward Maitland Wright (Groot-Brittannië, 1906 - 2005)

Alan Mathison Turing (Groot-Brittannië, 1912 - 1954)

Paul Erdös (Polen, 1913 - 1996)

Richard Phillips Feynman (USA 1918 - 1988)

Kurt Gödel (Duitsland, 1906 - 1978)

John Torrence Tate (USA, 1925)

Jean-Pierre Serre (Frankrijk, 1926)

Yutaka Taniyama (Japan, 1927 - 1958)

Henry Peter Francis Swinnerton-Dyer (Groot-Brittannië, 1927)

Alexander (Alexandre) Grothendieck (Duitsland, Frankrijk, 1928 - 2014)

Goro Shimura (Japan, 1930)

Roger Penrose (Groot-Brittannië, 1931)

Bryan John Birch (Groot-Brittannië, 1931)

Robert Phelan Langlands (Canada, USA, 1936)

Barry Charles Mazur (USA, 1937)

David Bryant Mumford (Groot-Brittannië, USA, 1937)

Gerhard Frey (Duitsland, 1944)

Pierre Deligne (België, 1944; werkt nu aan het IAS, Princeton U.S.A.)

Kenneth Alan (Ken) Ribet (USA, 1948)

Don Zagier (U.S.A., Duitsland, 1951)

Yoichi Miyaoka (Japan)

Victor Kolyvagin (Rusland)

Matthias Flach (Duitsland, Groot-Brittannië, USA)

Andrew Wiles (Groot-Brittannië, 1953)

Gerd Faltings (Duitsland, 1954)

Joseph H. Silverman (USA, 1955)

Richard Taylor (Groot-Brittannië, USA, 1962)

19 Appendix: de tekst die in de BBC documentaire wordt gesproken

Hier is de tekst zoals die op in de documentaire te horen is.
de tekst staat op internet:

http://www.pbs.org/wgbh/nova/transcripts/2414proof.html

‘‘The Proof’’
PBS Airdate: October 28, 1997 Go to the companion Web site
ANNOUNCER: Tonight, on NOVA. He conquered the impossible.
ANDREW WILES: Suddenly, totally unexpectedly, I had this incredible revelation.
PETER SARNAK: I was flabbergasted, excited, disturbed.
ANNOUNCER: How did this man solve an enigma that mystified the greatest minds for centuries?
ANDREW WILES: I believed I solved Fermat’s Last Theorem.
ANNOUNCER: The Proof.
Major funding for NOVA is provided by the Park Foundation, dedicated to education and quality television...by the Corporation for Public Broadcasting, and viewers like you.
ANDREW WILES: Perhaps I could best describe my experience of doing mathematics in terms of entering a dark mansion. One goes into the first room, and it’s dark, completely dark. One stumbles around bumping into the furniture, and gradually, you learn where each piece of furniture is, and finally, after six months or so, you find the light switch. You turn it on,

and suddenly, it's all illuminated. You can see exactly where you were. At the beginning of September, I was sitting here at this desk, when suddenly, totally unexpectedly, I had this incredible revelation. It was the most - the most important moment of my working life. Nothing I ever do again will. . . I'm sorry.

STACY KEACH (NARRATOR): For seven years, Princeton professor Andrew Wiles worked in complete secrecy, struggling to solve the world's greatest mathematical problem. This obsession, which began when he was a child, would later bring him both fame and regret.

ANDREW WILES: So, I came to this. I was a ten-year-old, and one day I happened to be looking in my local public library, and I found a book on math and it told a bit about the history of this problem, that someone had resolved this problem 300 years ago, but no one had ever seen the proof. No one knew if there was a proof. And people ever since had looked for the proof. And here was a problem that I, a ten-year-old, could understand, that none of the great mathematicians in the past had been able to resolve. And from that moment, of course, I just tried to solve it myself. It was such a challenge, such a beautiful problem. This problem was Fermat's last theorem.

JOHN CONWAY: Pierre de Fermat was, by profession, a lawyer. He was Councilor to the Parliament of Toulouse in France. But, of course, that's not what he's really remembered for. What he's really remembered for is his mathematics.

STACY KEACH (NARRATOR): Pierre de Fermat was a 17th-century French mathematician who made some of the greatest breakthroughs in the history of numbers. His inspiration came from studying the Arithmetica, an Ancient Greek text.

JOHN CONWAY: Fermat owned a copy of this book, which is a book about numbers with lots of problems, which presumably, Fermat had to solve. He studied it; he wrote notes in the margins.

STACY KEACH (NARRATOR): Fermat's original notes were lost, but they can still be read in a book published by his son. It was one of these notes that was Fermat's greatest legacy.

JOHN CONWAY: And this is the fantastic observation of master Pierre de Fermat which caused all the trouble. ''Cubum autem in duos cubos.''

STACY KEACH (NARRATOR): This tiny note is the world's hardest mathematical problem. It's been unsolved for centuries, yet it begins with an equation so simple that children know it by heart.

CHILDREN: The square of the hypotenuse is equal to the sum of the squares of the other two sides.

JOHN CONWAY: Yeah. Well, that's Pythagoras's theorem, isn't it? That's what we all did at school. So, Pythagoras's theorem, the clever thing about it is that it tells us when three numbers are the sides of a right-angle triangle. That happens just when X squared plus Y squared equals Z squared.

ANDREW WILES: X squared plus Y squared equals Z squared. And you can ask, ''Well, what are the whole number solutions of this equation?'' You quickly find there's a solution 3 squared plus 4 squared equals 5 squared. Another one is 5 squared plus 12 squared is 13 squared. And you go on looking, and

you find more and more. So then, a natural question is, the question Fermat raised: Supposing you change from squares. Supposing you replace the 2 by 3, by 4, by 5, by 6, by any whole number n, and Fermat said simply that you'll never find any solutions. However far you look, you'll never find a solution.

STACY KEACH (NARRATOR): If n is greater than 2, you will never find numbers that fit this equation. That's what Fermat said. What's more, he said he could prove it. But instead, he scribbled a most enigmatic note.

JOHN CONWAY: Written in Latin, he says he has a truly wonderful proof, ''Demonstrationem mirabilem,'' of this fact. And then, the last words are, ''Hanc marginis exigiutas non caperet.'' ''This margin is too small to contain it.''

STACY KEACH (NARRATOR): So Fermat said he had a proof, but he never said what it was.

JOHN CONWAY: Fermat made lots of marginal notes. People took them as challenges, and over the centuries, every single one of them has been disposed of, and the last one to be disposed of is this one. That's why it's called the last theorem.

STACY KEACH (NARRATOR): Rediscovering Fermat's proof became the ultimate challenge, a challenge which would baffle mathematicians for the next 300 years.

JOHN CONWAY: Gauss, the greatest mathematician in the world. . .

BARRY MAZUR: Oh, yes. Galois. . .

JOHN COATES: Kummer, of course.

KEN RIBET: Well, in the 18th century, Euler didn't prove it.

JOHN CONWAY: Well, you know there's only been the one woman, really.

KEN RIBET: Sophie Germain.

BARRY MAZUR: Oh, there are millions. There are lots of people.

PETER SARNAK: But, nobody had any idea where to start.

ANDREW WILES: Well, mathematicians just love a challenge, and this problem, this particular problem, just looked so simple. It just looked as if it had to have a solution. And of course, it's very special because Fermat said he had a solution.

JOHN CONWAY: This thing has been there like a beacon in front of us. I mean, if you give up, you just get the feeling you've given up. It's like Everest; it won't go away. It still stays there. And so, one person can give up, but another person is still just trying to get a little bit further.

STACY KEACH (NARRATOR): The task was to prove that no numbers, other than 2, fit the equation. But when computers came along, couldn't they check each number one by one and show that none of them worked?

JOHN CONWAY: Well, how many numbers are there to be dealt with? You've got to do it for infinitely many numbers. So, after you've done it for one, how much closer have you got? Well, there's still infinitely many left. After you've done it for a thousand numbers, how many, how much closer have you got? Well, there's still infinitely many left. After you've done it for a million, well, there's still infinitely many left. In fact, you haven't done very many, have you?

STACY KEACH (NARRATOR): A computer can never check every number. Instead, what's needed is a mathematical proof.

PETER SARNAK: A mathematician is not happy until the proof is complete and considered complete by the standards of mathematics.

NICK KATZ: In mathematics, there's the concept of proving something, of knowing it with absolute certainty.

PETER SARNAK: Which - Well, it's called ''rigorous proof.''

KEN RIBET: Well, a rigorous proof is a series of arguments. . .

PETER SARNAK: . . .based on logical deductions. . .

KEN RIBET: Which just build one upon another. . .

PETER SARNAK: . . .step by step. . .

KEN RIBET: . . .until you get to. . .

PETER SARNAK: . . .a complete proof.

NICK KATZ: That's what mathematics is about.

STACY KEACH (NARRATOR): A proof provides a logical demonstration of why no numbers fit the equation without having to check every number. After centuries of failing to come up with such a proof, mathematicians began to abandon Fermat. In the '70s, Fermat was no longer in fashion. At the same time, Andrew Wiles was just beginning his career as a mathematician. He went to Cambridge University as a research student under the supervision of Professor John Coates.

JOHN COATES: I've been very fortunate to have Andrew as a student, and even as a research student, he was a wonderful person to work with. He had very deep ideas then, and it was always clear he was a mathematician who would do great things.

STACY KEACH (NARRATOR): But not with Fermat. Everyone thought Fermat's last theorem was impossible, so Professor Coates encouraged Andrew to forget his childhood dream and work on more mainstream math.

ANDREW WILES: The problem with working on Fermat is that you could spend years getting nothing. It's fine to work on any problem so long as it generates mathematics. Almost the definition of a good mathematical problem is the mathematics it generates, rather than the problem itself.

JOHN CONWAY: You know, not all mathematical problems are useless. Fermat's one really is useless, I think, in a certain sense. It's got no practical value whatsoever.

PETER SARNAK: If it's true, it doesn't imply anything profound, that any of us know. It doesn't lead to anything that's useful, that any of us know. It, by itself, is sort of on the outskirts. It's not what you would consider a mainstream, important, central question in modern mathematics.

ANDREW WILES: And that point, I really put aside Fermat. It's not that I forgot about it; it was always there. I always remembered it, but I realized the only techniques we had to tackle it had been around for 130 years, and it didn't seem they were really getting to the root of the problem. So, when I went to Cambridge, my advisor, John Coates, was working on Iwasawa theory and elliptic curves, and I started working with him.

STACY KEACH (NARRATOR): For Andrew's advisor, and a host of other mathematicians, elliptic curves were the ''in'' thing to study.

BARRY MAZUR: You may never have heard of elliptic curves, but they're extremely important.

JOHN CONWAY: OK. So, what's an elliptic curve?

BARRY MAZUR: Elliptic curves. They're not ellipses. They're cubic curves whose solution have a shape that looks like a doughnut.

PETER SARNAK: They look so simple, yet the complexity, especially arithmetic complexity, is immense.

STACY KEACH (NARRATOR): Every point on the doughnut is the solution to an equation. Andrew Wiles now studied these elliptic equations and set aside his dream. What he didn't realize was that on the other side of the world, elliptic curves and Fermat's last theorem were becoming inextricably linked.

GORO SHIMURA: I entered the University of Tokyo in 1949, and that was four years after the War, but almost all professors were tired and the lectures were not inspiring.

STACY KEACH (NARRATOR): Goro Shimura and his fellow students had to rely on each other for inspiration. In particular, he formed a remarkable partnership with a young man by the name of Utaka Taniyama.

GORO SHIMURA: That was when I became very close to Taniyama. Taniyama was not a very careful person as a mathematician. He made a lot of mistakes, but he made mistakes in a good direction, and so eventually, he got right answers, and I tried to imitate him, but I found out that it is very difficult to make good mistakes.

STACY KEACH (NARRATOR): Together, Taniyama and Shimura worked on the complex mathematics of modular functions.

NICK KATZ: I really can't explain what a modular function is in one sentence. I can try and give you a few sentences to explain. I really can't do it in one sentence.

PETER SARNAK: Oh, it's impossible.

ANDREW WILES: There's a saying attributed to Eichler that there are five fundamental operations of arithmetic: addition, subtraction, multiplication, division, and modular forms.

BARRY MAZUR: Modular forms are functions on the complex plane that are inordinately symmetric. They satisfy so many internal symmetries that their mere existence seem like accidents. But they do exist.

STACY KEACH (NARRATOR): This image is merely a shadow of a modular form. To see one properly, your TV screen would have to be stretched into something called hyperbolic space. Bizarre modular forms seem to have nothing whatsoever to do with the humdrum world of elliptic curves. But what Taniyama and Shimura suggested shocked everyone.

GORO SHIMURA: In 1955, there was an international symposium, and Taniyama posed two or three problems.

STACY KEACH (NARRATOR): The problems posed by Taniyama led to the extraordinary claim that every elliptic curve was really a modular form in disguise. It became knows as the Taniyama-Shimura conjecture.

JOHN CONWAY: What the Taniyama-Shimura conjecture says, it says that every rational elliptic curve is modular, and that's so hard to explain.

BARRY MAZUR: So, let me explain. Over here, you have the elliptic world,

the elliptic curves, these doughnuts. And over here, you have the modular world, modular forms with their many, many symmetries. The Shimura-Taniyama conjecture makes a bridge between these two worlds. These worlds live on different planets. It's a bridge. It's more than a bridge; it's really a dictionary, a dictionary where questions, intuitions, insights, theorems in the one world get translated to questions, intuitions in the other world.

KEN RIBET: I think that when Shimura and Taniyama first started talking about the relationship between elliptic curves and modular forms, people were very incredulous. I wasn't studying mathematics yet. By the time I was a graduate student in 1969 or 1970, people were coming to believe the conjecture.

STACY KEACH (NARRATOR): In fact, Taniyama-Shimura became a foundation for other theories which all came to depend on it. But Taniyama-Shimura was only a conjecture, an unproven idea, and until it could be proven, all the mathematics which relied on it were under threat.

ANDREW WILES: We built more and more conjectures stretched further and further into the future, but they would all be completely ridiculous if Taniyama-Shimura was not true.

STACY KEACH (NARRATOR): Proving the conjecture became crucial, but tragically, the man whose idea inspired it didn't live to see the enormous impact of his work. In 1958, Taniyama committed suicide.

GORO SHIMURA: I was very much puzzled. Puzzlement may be the best word. Of course, I was sad thatSee, it was so sudden, and I was unable to make sense out of this. Some people suggested he lost confidence in himself. That may be so, but I think it was more complex. I don't really know. Confidence in himself, but not mathematically.

STACY KEACH (NARRATOR): Taniyama-Shimura went on to become one of the great unproven conjectures, a foundation for many important mathematical ideas. But what did it have to do with Fermat's last theorem?

ANDREW WILES: At that time, no one had any idea that Taniyama-Shimura could have anything to do with Fermat. Of course, in the '80s, that all changed completely.

STACY KEACH (NARRATOR): But what was the bridge between the two ideas? Taniyama-Shimura says, ''Every elliptic curve is modular'', and Fermat says, ''No numbers fit this equation.'' What was the connection?

KEN RIBET: Well, on the face of it, the Shimura-Taniyama conjecture, which is about elliptic curves, and Fermat's last theorem have nothing to do with each other, because there's no connection between Fermat and elliptic curves. But in 1985, Gerhard Frey had this amazing idea.

STACY KEACH (NARRATOR): Frey, a German mathematician, considered the unthinkable. What would happen if Fermat was wrong and there was a solution to this equation after all?

PETER SARNAK: Frey showed how starting with a fictitious solution to Fermat's last equation - if, indeed, such a horrible beast existed - he could make an elliptic curve with some very weird properties.

KEN RIBET: That elliptic curve seems to be not modular. But Shimura-Taniyama says that every elliptic curve is modular.

STACY KEACH (NARRATOR): So, if there is a solution to this equation, it creates such a weird elliptic curve it defies Taniyama-Shimura.

KEN RIBET: So, in other words, if Fermat is false, so is Shimura-Taniyama. Or, said differently, if Shimura-Taniyama is correct, so is Fermat's last theorem.

STACY KEACH (NARRATOR): Fermat and Taniyama-Shimura were now linked, apart from just one thing.

KEN RIBET: The problem is that Frey didn't really prove that his elliptic curve was not modular. He gave a plausibility argument, which he hoped could be filled in by experts, and then the experts started working on it.

STACY KEACH (NARRATOR): In theory, you could prove Fermat by proving Taniyama, but only if Frey was right. Frey's idea became known as the epsilon conjecture, and everyone tried to check it. One year later, in San Francisco, there was a breakthrough.

KEN RIBET: I saw Barry Mazur on the campus, and I said, ''Let's go for a cup of coffee.'' And we sat down for cappuccinos at this cafe, and I looked at Barry and I said, ''You know, I'm trying to generalize what I've done so that we can prove the full strength of Serre's epsilon conjecture.'' And Barry looked at me and said, ''But you've done it already. All you have to do is add on some extra gamma zero of m structure and run through your argument, and it still works, and that gives everything you need.'' And this had never occurred to me, as simple as it sounds. I looked at Barry, I looked at my cappucino, I looked back at Barry, and I said, ''My God. You're absolutely right.''

BARRY MAZUR: Ken's idea was brilliant.

KEN RIBET: And I was completely enthralled. I just sort of wandered back to my apartment in a cloud, and I sat down and I ran through my argument, and it worked. It really worked. And at the conference, I started telling a few people that I'd done this, and soon, large groups of people knew, and they were running up to me, and they said, ''Is it true that you've proved the epsilon conjecture?'' And I had to think for a minute, and all of a sudden, I said, ''Yes. I have.''

ANDREW WILES: I was at a friend's house sipping iced tea early in the evening, and he just mentioned casually in the middle of a conversation, ''By the way, did you hear that Ken has proved the epsilon conjecture?'' And I was just electrified. I knew that moment the course of my life was changing, because this meant that to prove Fermat's last theorem, I just had to prove Taniyama-Shimura conjecture. From that moment, that was what I was working on. I just knew I would go home and work on the Taniyama-Shimura conjecture.

STACY KEACH (NARRATOR): Andrew abandoned all his other research. He cut himself off from the rest of the world, and for the next seven years, he concentrated solely on his childhood passion.

ANDREW WILES: I never use a computer. I sometimes might scribble. I do doodles. I start trying to find patterns, really, so I'm doing calculations which try to explain some little piece of mathematics, and I'm trying to fit it in with some previous broad conceptual understanding of some branch of mathematics. Sometimes, that'll involve going and looking up in a book to

see how it's done there. Sometimes, it's a question of modifying things a bit, sometimes, doing a little extra calculation. And sometimes, you realize that nothing that's ever been done before is any use at all, and you just have to find something completely new. And it's a mystery where it comes from.

JOHN COATES: I must confess, I did not think that the Shimura-Taniyama conjecture was accessible to proof at present. I thought I probably wouldn't see a proof in my lifetime.

KEN RIBET: I was one of the vast majority of people who believed that the Shimura-Taniyama conjecture was just completely inaccessible, and I didn't bother to prove iteven think about trying to prove it. Andrew Wiles is probably one of the few people on earth who had the audacity to dream that you could actually go and prove this conjecture.

ANDREW WILES: In this case, certainly the first several years, I had no fear of competition. I simply didn't think I or anyone else had any real idea how to do it. But I realized after a while that talking to people casually about Fermat was impossible, because it just generates too much interest, and you can't really focus yourself for years unless you have this kind of undivided concentration, which too many spectators would have destroyed.

STACY KEACH (NARRATOR): Andrew decided that he would work in secrecy and isolation.

PETER SARNAK: I often wondered, myself, what he was working on.

NICK KATZ: Didn't have an inkling.

JOHN CONWAY: No, I suspected nothing.

KEN RIBET: This is probably the only case I know where someone worked for such a long time without divulging what he was doing, without talking about the progress he had made. It's just unprecedented.

STACY KEACH (NARRATOR): Andrew was embarking on one of the most complex calculations in history. For the first two years, he did nothing but immerse himself in the problem, trying to find a strategy which might work.

ANDREW WILES: So, it was now known that Taniyama-Shimura implied Fermat's last theorem. What does Taniyama-Shimura say? It says that all elliptic curves should be modular. Well, this was an old problem, been around for twenty years, and lots of people had tried to solve it.

KEN RIBET: Now, one way of looking at it is that you have all elliptic curves, and then you have the modular elliptic curves, and you want to prove that there are the same number of each. Now, of course, you're talking about infinite sets, so you can't just count them, per se, but you can divide them into packets, and you can try to count each packet and see how things go. And this proves to be a very attractive idea for about thirty seconds, but you can't really get much further than that. And the big question on the subject was how you could possibly count, and in effect, Wiles introduced the correct technique.

STACY KEACH (NARRATOR): Andrew Wiles hoped to solve the problem of counting elliptic curves by converting them into something called Galois representations. Although no less complex than elliptic curves, they were

easier to count. So, it was Galois representations, not elliptic curves, that Andrew would now compare with modular forms.

ANDREW WILES: Now, you might ask, and it's an obvious question, why can't you do this with elliptic curves and modular forms? Why couldn't you count elliptic curves, count modular forms, show they're the same number? Well, the answer is, people tried and they never found a way of counting them, and this was why this is they key breakthrough, that I had found the way to count not the original problem, but the modified problem. I'd found a way to count modular forms and Galois representations.

STACY KEACH (NARRATOR): This was only the first step, and already, it had taken three years of Andrew's life.

ANDREW WILES: My wife's only known me while I've been working on Fermat. I told her a few days after we got married. I decided that I really only had time for my problem and my family, and when I was concentrating very hard, and I found that with young children, that's the best possible way to relax. When you're talking to young children, they simply aren't interested in Fermat, at least at this age. They want to hear a children's story, and they're not going to let you do anything else. So, I'd found this wonderful counting mechanism, and I started thinking about this concrete problem in terms of Iwasawa theory. Iwasawa theory was the subject I'd studied as a graduate student, and, in fact, with my advisor, John Coates, I'd used it to analyze elliptic curves.

STACY KEACH (NARRATOR): Iwasawa theory, Andrew hoped, would be the key to completing his counting strategy.

ANDREW WILES: Now, I tried to use Iwasawa theory in this context, but I ran into trouble. I seemed to be up against a wall. I just didn't seem to be able to get past it. Well, sometimes when I can't see what to do next, I often come here by the lake. Walking has a very good effect in that you're in this state of concentration, but at the same time, you're relaxing; you're allowing the subconscious to work on you.

STACY KEACH (NARRATOR): Andrew struggled for months using Iwasawa theory in an effort to create something called a Class Number Formula. Without this critical formula, he would have nowhere left to go.

ANDREW WILES: So, at the end of the summer of '91, I was at a conference, and John Coates told me about a wonderful new paper of Matthias Flach, a student of his, in which he had tackled the class number formula, in fact, exactly the class number formula I needed. So, Flach, using ideas Kolyvagin, had made a very significant first step in actually producing the class number formula. So, at that point, I thought, 'This is just what I need. This is tailor-made for the problem.' I put aside the completely the old approach I'd been trying, and I devoted myself day and night to extending his result.

STACY KEACH (NARRATOR): Andrew was almost there, but this breakthrough was risky and complicated. After six years of secrecy, he needed to confide in someone.

NICK KATZ: January of 1993, Andrew came up to me one day at tea, asked me if I could come up to his office; there was something he wanted to talk to me about. I had no idea what this could be. I went up to his

office. He closed the door. He said he thought he would be able to prove Taniyama-Shimura. I was just amazed. This was fantastic.

ANDREW WILES: It involved a kind of mathematics that Nick Katz is an expert in.

NICK KATZ: I think another reason he asked me was that he was sure I would not tell other people, I would keep my mouth shut. Which I did.

JOHN CONWAY: Andrew Wiles and Nick Katz had been spending rather a lot of time huddled over a coffee table at the far end of the common room working on some problem or other. We never knew what it was.

STACY KEACH (NARRATOR): To avoid any more suspicion, Andrew decided to check his proof by disguising it in a series of lectures at Princeton, which Nick Katz could attend.

ANDREW WILES: Well, I explained at the beginning of the course that Flach had written this beautiful paper and I wanted to try to extend it to prove the full class number formula. The only thing I didn't explain was that proving the class number formula was most of the way to Fermat's last theorem.

NICK KATZ: So, this course was announced. It said ''Calculations on Elliptic Curves,'' which could mean anything. It didn't mention Fermat, it didn't mention Taniyama-Shimura. There was no way in the world anyone could have guessed that it was about that, if you didn't already know. None of the graduate students knew, and in a few weeks, they just drifted off, because it's impossible to follow stuff if you don't know what it's for, pretty much. It's pretty hard even if you do know what it's for. But after a few weeks, I was the only guy in the audience.

STACY KEACH (NARRATOR): The lectures revealed no errors, and still, none of his colleagues suspected why Andrew was being so secretive.

PETER SARNAK: Maybe he's run out of ideas. That's why he's quiet. You never know why they're quiet.

STACY KEACH (NARRATOR): The proof was still missing a vital ingredient, but Andrew now felt confident. It was time to tell one more person.

ANDREW WILES: So, I called up Peter and asked him if I could come 'round and talk to him about something.

PETER SARNAK: I got a phone call from Andrew saying that he had something very important he wanted to chat to me about. And sure enough, he had some very exciting news.

ANDREW WILES: I said, ''I think you better sit down for this.'' He sat down. I said, ''I think I'm about to prove Fermat's last theorem.''

PETER SARNAK: I was flabbergasted, excited, disturbed. I mean, I remember that night finding it quite difficult to sleep.

ANDREW WILES: But, there was still a problem. Late in the spring of '93, I was in this very awkward position that I thought I'd got most of the curves being modular, so that was nearly enough to be content to have Fermat's last theorem, but there were these few families of elliptic curves that had escaped the net. I was sitting here at my desk in May of '93, still wondering about this problem, and I was casually glancing at a paper of Barry Mazur's, and there was just one sentence which made a reference to actually

what's a 19th century construction, and I just instantly realized that there was a trick that I could use, that I could switch from the families of elliptic curves I'd been using. I'd been studying them using the prime three. I could switch and study them using the prime five. It looked more complicated, but I could switch from these awkward curves that I couldn't prove were modular to a different set of curves, which I'd already proved were modular, and use that information to just go that one last step. And, I just kept working out the details, and time went by, and I forgot to go down to lunch, and it got to about tea-time, and I went down and Nada was very surprised that I'd arrived so late, and then sheI told her that I believed I'd solved Fermat's last theorem. I was convinced that I had Fermat in my hands, and there was a conference in Cambridge organized by my advisor, John Coates. I thought that would be a wonderful place. It's my old hometown, and I'd been a graduate student there. It would be a wonderful place to talk about it if I could get it in good shape.

JOHN COATES: The name of the lectures that he announced was simply ''Elliptic Curves and Modular Forms.'' There was no mention of Fermat's last theorem.

KEN RIBET: Well, I was at this conference on L functions and elliptic curves, and it was kind of a standard conference and all of the people were there. Didn't seem to be anything out of the ordinary, until people started telling me that they'd been hearing weird rumors about Andrew Wiles's proposed series of lectures. I started talking to people and I got more and more precise information. I have no idea how it was spread.

PETER SARNAK: Not from me. Not from me.

JOHN CONWAY: Whenever any piece of mathematical news had been in the air, Peter would say, ''Oh, that's nothing. Wait until you hear the big news. There's something big going to break.''

PETER SARNAK: Maybe some hints, yeah.

ANDREW WILES: People would ask me, leading up to my lectures, what exactly I was going to say. And I said, ''Well, come to my lecture and see.''

KEN RIBET: It's a very charged atmosphere. A lot of the major figures of arithmetical, algebraic geometry were there. Richard Taylor and John Coates. Barry Mazur.

BARRY MAZUR: Well, I'd never seen a lecture series in mathematics like that before. What was unique about those lectures were the glorious ideas, how many new ideas were presented, and the constancy of its dramatic build-up. It was suspenseful until the end.

KEN RIBET: There was this marvelous moment when we were coming close to a proof of Fermat's last theorem. The tension had built up, and there was only one possible punch line.

ANDREW WILES: So, after I'd explained the 3/5 switch on the blackboard, I then just wrote up a statement of Fermat's last theorem, said I'd proved it, said, ''I think I'll stop there.''

JOHN COATES: The next day, what was totally unexpected was that we were deluged by inquiries from newspapers, journalists from all around the world.

ANDREW WILES: It was a wonderful feeling after seven years to have really

solved my problem. I'd finally done it. Only later did it come out that there was a problem at the end.

NICK KATZ: Now, it was time for it to be refereed, which is to say, for people appointed by the journal to go through and make sure that the thing was really correct. So, for two months, July and August, I literally did nothing but go through this manuscript line by line, and what this meant concretely was that essentially every day, sometimes twice a day, I would e-mail Andrew with a question: ''I don't understand what you say on this page, on this line. It seems to be wrong,'' or ''I just don't understand.''

ANDREW WILES: So, Nick was sending me e-mails, and at the end of the summer, he sent one that seemed innocent at first, and I tried to resolve it.

NICK KATZ: It's a little bit complicated, so he sends me a fax, but the fax doesn't seem to answer the question, so I e-mail him back, and I get another fax, which I'm still not satisfied with. And this, in fact, turned into the error that turned out to be a fundamental error, and that we had completely missed when he was lecturing in the spring.

ANDREW WILES: That's where the problem was, in the method of Flach and Kolyvagin that I'd extended. So, once I realized that at the end of September, that there was really a problem with the way I'd made the construction, I spent the fall trying to think what kind of modifications could be made to the construction. There are lots of simple and rather natural modifications that any one of which might work.

PETER SARNAK: And every time he would try and fix it in one corner, it would sort ofSome other difficulty would add up in another corner. It was like he was trying to put a carpet in a room where the carpet had more size than the room, but he could put it in in any corner, and then when he ran to the other corners, it would pop up in this corner. And whether you could not put the carpet in the room was not something that he was able to decide.

ANDREW WILES: So, in September '93, when the proof was running into problems, Nada said to me, ''The only thing I want for my birthday is the correct proof.'' Her birthday is on October 6. I had two or three weeks, and I failed to deliver.

NICK KATZ: I think he externally appeared normal, but at this point, he was keeping a secret from the world, and I think he must have been, in fact, pretty uncomfortable about it.

ANDREW WILES: Towards the end of November, it didn't seem to be working. I sent out an e-mail message announcing that there was a problem with this part of the argument.

JOHN CONWAY: Well, you know, we were behaving a little bit like Kremlinologists. Nobody actually liked to come out and ask him how he's getting on with the proof. So, somebody would say, ''I saw Andrew this morning.'' ''Did he smile?'' ''Well, yes. But he didn't look too happy.''

ANDREW WILES: The first seven years I'd worked on this problem, I loved every minute of it. However hard it had been, there'd been setbacks often, there'd been things that had seemed insurmountable, but it was a kind of private and very personal battle I was engaged in. And then, after there was

a problem with it, doing mathematics in that kind of rather over-exposed way is certainly not my style, and I have no wish to repeat it.

STACY KEACH (NARRATOR): After months of failure, Andrew was about to admit defeat. In desperation, he decided to ask for help, and a former student, Richard Taylor, came to Princeton.

ANDREW WILES: Richard and I spent three months at the beginning of '94 trying to analyze all the possible modifications, and at the end of that period, I was convinced that none of them was really going to give the answer. In September, I decided to go back and look one more time at the original structure of Flach and Kolyvagin to try and pinpoint exactly why it wasn't working, try and formulate it precisely. One can never really do that in mathematics, but I just wanted to set my mind to rest that it really couldn't be made to work. And I was sitting here at this desk. It was a Monday morning, September 19, and I was trying, convincing myself that it didn't work, just seeing exactly what the problem was, when suddenly, totally unexpectedly, I had this incredible revelation. I realized what was holding me up was exactly what would resolve the problem I had had in my Iwasawa theory attempt three years earlier, wasIt was the mostthe most important moment of my working life. It was so indescribably beautiful; it was so simple and so elegant, and I just stared in disbelief for twenty minutes. Then, during the day, I walked around the department. I'd keep coming back to my desk and looking to see if it was still there. It was still there. Almost what seemed to be stopping the method of Flach and Kolyvagin was exactly what would make horizontal Iwasawa theory. My original approach to the problem from three years before would make exactly that work. So, out of the ashes seemed to rise the true answer to the problem. So, the first night, I went back and slept on it. I checked through it again the next morning, and by eleven o'clock, I was satisfied and I went down and told my wife, ''I've got it. I think I've got it. I've found it.' And it was so unexpected, I think she thought I was talking about a children's toy or something and said, ''Got what?'' And I said, ''I've fixed my proof. I've got it.''

JOHN COATES: I think it will always stand as one of the high achievements of number theory.

BARRY MAZUR: It was magnificent.

JOHN CONWAY: It's not every day that you hear the proof of the century.

GORO SHIMURA: Well, my first reaction was, ''I told you so.''

STACY KEACH (NARRATOR): The Taniyama-Shimura conjecture is no longer a conjecture, and as a result, Fermat's last theorem has been proved. But is Andrew's proof the same as Fermat's?

JOHN CONWAY: Fermat's proof was just too big to fit into this margin. Andrew's was 200 pages long. It's not the same proof.

ANDREW WILES: Fermat couldn't possibly have had this proof. It's a 20th century proof. There's no way this could have been done before the 20th century.

JOHN CONWAY: I'm relieved that this result is now settled. But I'm sad in some ways, because Fermat's last theorem has been responsible for so much.

What will we find to take its place?

ANDREW WILES: There's no other problem that will mean the same to me. I had this very rare privilege of being able to pursue in my adult life what had been my childhood dream. I know it's a rare privilege, but if one can do this, if one can really tackle something in adult life that means that much to you, it's more rewarding than anything I could imagine.

BARRY MAZUR: One of the great things about this work is it embraces the ideas of so many mathematicians. I've made a partial list. Klein, Fricke, Hurwitz, Hecke, Dirichlet, Dedekind. . .

KEN RIBET: The proof by Langlands and Tunnell. . .

JOHN COATES: Deligne, Rapoport, Katz. . .

NICK KATZ: Mazur's idea of using the deformation theory of Galois representations. . .

BARRY MAZUR: Igusa, Eichler, Shimura, Taniyama. . .

PETER SARNAK: Frey's reduction. . .

NICK KATZ: The list goes on and on.

BARRY MAZUR: Bloch, Kato, Selmer, Frey, Fermat.

ANNOUNCER: There was another player in the Fermat game. She lived during the French Revolution and pretended to be a man in order to pursue her passion for mathematics. At NOVA's website, meet Sophie Germain at www.pbs.org.

Educators can order this show for $19.95, plus shipping and handling, by calling 1-800-949-8670. And, to learn more about how science can solve the mysteries of our world, ask about our many other NOVA videos.

JOHN CONWAY: It's like effortless; it won't go away. It still stays there.

ANDREW WILES: Well, mathematicians just love a challenge, and this problem, this particular problem, just looked so simple, it just looked as if it had to have a solution.

KEN RIBET: Andrew Wiles is probably one of the few people on earth who had the audacity to dream that you could actually go and prove this conjecture.

Lees ook de beschrijving ''*Who is Andrew Wiles*?'' van Singh:
http://simonsingh.net/books/fermats-last-theorem/who-is-andrew-wiles/

20 Enkele wiskundigen die bijgedragen hebben aan het formuleren en het oplossen van FLT

Uit vorige eeuwen: Pythagoras, Euclides, Diophantus, Pierre de Fermat, Leonhard Euler, Sophie Germain, Johann Peter Gustav Lejeune Dirichlet, Adrien-Marie Legendre, Ernst Eduard Kummer, Henri Léon Lebesgue (en nog meer namen die in de documentarie genoemd worden).

Enkele van de grote wiskundigen van deze eeuw, die bijgedragen hebben aan de oplossing van FLT. Sommigen zien we wel op de BBC-documentaire (we geven dit

aan met **d**), en enkele die we helaas niet zien (we geven dat aan met **n**), in alfabetische volgorde:

n Gerhard Frey (Essen); in 1985 gaf hij het idee waaruit het verband tussen STW en FLT volgt; voor het eerst in de geschiedenis is FLT niet meer een ‘‘geïsoleerd probleem’’. Eerder werk van Hellegouarch gaf ook reeds een indicatie van dit verband, maar dat heeft nooit verder vruchten afgeworpen in die vorm.

d Nicholas Katz (Princeton): hij heeft bij een gedeelte van het wetenschappelijk werk van Wiles als een belangrijk klankbord gefunctioneerd.

d Barry Mazur (Harvard): een veelzijdig wiskundige (van topologie tot getaltheorie), zijn werk over deformaties van Galois-representaties had grote invloed op het werk van Wiles. Allerlei ontwikkelingen zijn verbonden met initiatieven van hem.

d Ken Ribet (Berkeley) bewees dat FLT een gevolg is van STW, technisch een moeilijke en belangrijke stap.

n Jean-Pierre Serre (Parijs), fields medaillist in 1954 (Amsterdam), sindsdien een bron van veel nieuwe ideeën in de moderne wiskunde; veel originele gedachten komen van hem; ook heeft hij een enorme invloed op de manier van denken en publiceren van vele wiskundigen in de laatste 50 jaar. Serre kreeg de Fields medal in 1954 en de Abel prijs in 2003. Serre gaf aan hoe we van TW naar FLT zouden kunnen komen.

n Goro Shimura (Princeton), schreef baanbrekend werk op het gebied van automorfe functies, en van getaltheorie en meetkunde daarmede verbonden.

n Yutaka Taniyama (1927) was een briljant wiskundige; hij pleegde zelfmoord op jonge leeftijd: 17 - XI - 58.

n John Tate (Texas) publiceert niet veel, maar zijn invloed op de moderne wiskunde is groot; zijn idee om arithmetiek en meetkunde te verbinden in één unificerende gedachte, voor een deel door hem zelf uitgewerkt, heeft veel invloed, nog steeds, op de moderne wiskunde; enkele van zijn vermoedens zijn nog niet volledig bewezen; een van de belangrijkste echter in 1966 door Tate in een speciaal geval bewezen werd schitterend bewezen door Faltings in 1983. John Tate kreeg de Abel prijs in 2010.

n Richard Taylor (nu in Princeton); in een laat stadium van het wetenschappelijk werk van Wiles heeft hij een detail helpen oplossen.

n André Weil (Princeton), heeft aan de wieg van de de moderne algebraïsche meetkunde gestaan. Zijn invloed is groot, onder andere toepassingen van de meetkunde in de getaltheorie onder zijn handen uitgegroeid. André Weil overleed op 6-VIII-1998 in Parijs.

d Andrew Wiles (Princeton, nu in Oxford) (geboren 11-IV-1953); als jongensdroom had hij het oplossen van FLT. Zonder dat hij dat zelf realiseerde leerde hij al die technieken die hem later zo goed van pas zouden komen. Toen Frey het idee in 1985 lanceerde dat STW de stelling FLT als gevolg zou kunnen hebben, en Ribet dit even later bewees, begon Wiles aan het onderzoek, dat uiteindelijk leidde tot zijn bewijs van FLT.

Referenties

[1] T. Andreescu, D. Andrica & I. Cucurezeanu - *An introduction to Diophantine equations. A problem-based approach.* Birkhäuser Verlag, New York, 2010.

[2] A. Beiler - *Recreations in the theory of numbers: The queen of mathematics untertains.* Dover Publ., pocket, 1964.

[3] E. Bell - *Men of mathematics.* Simon & Schuster. 1937.

[4] F. Beukers - *Getaltheorie voor beginners.* Epsilon Uitgaven, Utrecht 1999.

[5] F. Beukers - *Elementary number theory.* Collegedictaat WISB321, Utrecht 2012.

[6] F. Beukers, F. Luca & F. Oort - *Power values of divisor sums.* Amer. Math. Monthly **119** (2012), pp. 373-380.

[7] D. Burton - *Elementary number theory.* Allyn & Bacon, 1980.

[8] C. Caldwell - *An amazing prime heuristic.* http://www.utm.edu/staff/caldwell/preprints/Heuristics.pdf

[9] P. Chebyshev - *Mémoire sur les nombres premiers.* J. de Math. Pures Appl. **17** (1852), 366-390. Also in Mémoires présentés à l'Académie Impériale des sciences de St.-Pétersbourg par divers savants **7** (1854), 15--33. Also in Oeuvres 1 (1899), 49-70.

[10] H. Diamond - *Elementary methods in the study of the distribution of prime numbers.* Bulletin Amer. Math. Soc. **7** (1982), 553-589.

[11] L. Dickson - *History of the theory of numbers.* Volume II: Diophantine analysis. Chelsea publ. Cy. New York, 1952.

[12] R. Dijkgraaf -- *Symmetrie,* collegedictaat, een inleiding in de wiskunde; 2001. http://www.science.uva.nl/onderwijs/wns/onderwijsCD/symmetrie/symmetrie.pdf

[13] Apostolos Doxiades - *Oom Petros en het vermoeden van Goldbach.* Oorspronkelijke Griekse titel: *O Theios Petros kai i Eikasia tou Goldbach* (1992). *Uncle Petros and Goldbach's Conjecture: A Novel of Mathematical Obsession.*
zie: http://en.wikipedia.org/wiki/Apostolos-Doxiadis
Lees vooral: http://www.ams.org/notices/200010/rev-jackson.pdf
http://www.authortrek.com/uncle-petros.html

Voor een andere bespreking van dit boek zie:

http://www.math.leidenuniv.nl/~naw/serie5/deel02/mrt2001/pdf/goldbach.pdf

[14] H. Edwards - *Fermat's last theorem. A genetic introduction to algebraic number theory.* Grad. Texts Math. 50, Springer, 1977.

[15] P. Erdös & J. Surányi - *Topics in the Theory of Numbers.* Springer, 2003.

[16] *Leonhard Euler und Christian Goldbach, Briefwechsel, 1729-1764.* Boek met correspondentie van Euler; editors A. Juškevič & E. Winter. Berlin 1965.

[17] G. Frey - *Some aspects of the theory of elliptic curves over number fields.* Expos. Math. 4 (1986), 35-66

[18] G. Frey - *Links between stable elliptic curves and certain Diophantine equations.* Ann. Univ. Sarav. Ser. Math. 1 (1986), 1-40.

[19] G. Frey - *Links between solutions of $A - B = C$ and elliptic curves.* In: Number theory, Ulm 1987 (Ed. H. P. Schlickewei & E. Wirsing). Lect. N. Math. 1380, Springer,1989, pp. 31-62.

[20] A. Fröhlich & M. Taylor - *Algebraic number theory.* Cambridge Std. Advanc. Math. 27, Cambridge Univ. Press, 1991.

[21] Leonardo Pisano Fibonacci - *The book of squares.* An annotated translation into modern English by L. E Sigler. Academic Press, 1987.

[22] M. Gardner - *Mathematical games.* Scientific American, 1977, 101-121.

[23] M. Gardner - *Penrose tiles to trapdoor ciphers.* W. H. Freeman & Cy, New York 1987.

[24] M. Gardner - *The colossal book of mathematics.* W. W. Norton & Co 2001.

[25] M. Gardner - *The colossal book of short puzzles and problems.* W. W. Norton & Co 2005.

[26] C. F. Gauss - *Disquisitiones Arithmeticae.* Geschreven 1798, gepubliceerd in 1801.

[27] C. Gauss, Letter to Encke, 24 Dec. 1849, Werke, vol. 2, Kng. Ges. Wiss., Göttingen, 1863, pp. 444--447.

[28] A. Granville & G. Martin - *Prime number races.* Amer. Math. Monthly **113** (2006), 1-33.

[29] D. Guedj - *Le théorème du perroquet.* Éditions Seuil, 1998. Nederlandse vertaling: *De stelling van de papegaai, roman over de geschiedenis van de wiskunde.* Ambo, 1999,

[30] R. Guy - *Unsolved problems in number theory.* Springer, 3rd Edition 2004.

[31] M. Haddon - *The curious incident of the dog in the night-time.* Jonathan Cape (UK) Doubleday (US), 2003. http://en.wikipedia.org/wiki/The-Curious-Incident-of-the-Dog-in-the-Night-Time

[32] G. Hardy & E. Wright - *An introduction to the theory of numbers.* Oxford, Clarendon Press, first edition 1938, fourth edition, 1975, sixth edition 2008. Onlangs is er een nieuwe druk verschenen, met een appendix over elliptische krommen.

[33] T. Heath - *A history of Greek mathematics.* Oxford, Clarendon Press, 1921.

[34] D. Heath-Brown - *Fermat's two-square theorem.* Invariant (1984), pp. 3-5. Zie ook: http://www.math.tugraz.at/~elsholtz/WWW/papers/papers30nathanson-new-address3.pdf

[35] D. Kehlmann - *Die Vermessung der Welt.* Rowohlt 2005 (ook vertaald in het Engels, in het Nederlands en...). Voor een review zie: http://www.ams.org/notices/200806/tx080600681p.pdf

[36] M. Krízek, F. Luca & L. Somer - *17 Lectures on Fermat numbers from number theory to geometry.* CMS Books in Mathematics Springer, New York 2002.

[37] S. Lang - *Die abc-Vermutung.* El. Math. **48** (1993), 89-99.

[38] S. Lang - *Algebraic number theory.* Grad. Texts Math. 110, Springer, 1986.

[39] S. Lang - *Undergraduate algebra.* Undergr. Text Math., Springer 1987.

[40] S. Lang - *Algebra.* Addison - Wesley Publ. Cy, 1965. Third edition. Addison-Wesley Publ. Cy, 1993.

[41] D. Leavitt - *The Indian clerk.* Bloomsbury, 2007.

[42] A.-M. Legendre - *Essai sur la théorie des nombres.* Duprat, Paris, 1798.

[43] H. W. Lenstra - *Solving the Pell equation.* Notices Amer. Math. Soc. 49 **2002**, 182-192.

[44] J.Littlewood - *Sur la distribution des nombres premiers.* Comptes Rendus, **158** (1914), pp. 1869-1872.

[45] Yuri I. Manin - *Good proofs are proofs that make us wiser.* Interview by Martin Aigner and Vasco A. Schmidt. The Berlin Intelligencer, 1998, pp. 16-19.

[46] B. Mazur - *Number theory as a gadfly.* Amer. Math. Monthly **98** (1991), 593--610.

[47] A. Mingarelli - *Some conjectures in elementary number theory.* http://arxiv.org/abs/1302.5299

[48] D. Musielak - *Sophie's diary: a historical fiction.* AuthorHouse (April 16, 2004).

[49] J. Oesterlé - *Nouvelles approaches du ''théorème'' de Fermat.* Sém. Bourbaki **40** (1987/88), Exp. 694. Astérisque 161-162 (1988), 165-186.

[50] F. Oort - *Priemgetallen.* In: Kaleidoscoop van de wiskunde 1. Editors: F. van der Blij, J. P. Hogendijk, F. Oort. Epsilon Uitgaven, 1990; pp.1-32.

[51] F. Oort - *Congruent numbers in the tenth and in the twentieth century.* In: Vrolijk, Arnoud & Jan P. Hogendijk (eds.), O ye Gentlemen: Arabic Studies on Science and Literary Culture, in Honour of Remke Kruk. Leiden [etc.]: Brill, 2007; pp. 77-97.

[52] F. Oort - *Dynamica en periodieke rijen.* Nw. Archief Wiskunde (5) **13** (2012), 110-111.

[53] F. Oort - *Priemgetallen.* Syllabus van een Kaleidoscoop-voordracht, 11 november 2013.
F. Oort - *Prime numbers.* (Syllabus Academia Sinica en National Taiwan University, 17 December 2012.) Notices of the ICCM **1** Number 2 (2013), 60-78.
Zie http://www.staff.science.uu.nl/~oort0109/

[54] G. Pólya - *Heuristic reasoning in the theory of numbers.* Amer. Math. Monthly **66** (1959), 375-384. http://www.jstor.org/stable/pdfplus/2308748.pdf

[55] K. Ribet - *From the Taniyama-Shimura conjecture to Fermat's last theorem.* Ann. Fac. Sc. Univ. Toulouse **11** (1990), 116-139.

[56] K. Ribet - *Wiles proves Taniyama's conjecture; Fermat's last theorem follows.* Notices A.M.S. 40 (1993), 575-576.

[57] H. Riesel - *Prime numbers and computer methods for factorization.* Progress Math. 57, Birkhäuser, 1985.

[58] K. Rosen - *Elementary number theory and its applications.* Addison Wesley, 2000.

[59] M. Rubinstein & P. Sarnak - *Chebyshev's bias.* Experiment. Math. **3** (1994), 173-197.

[60] W. Scharlau & H. Opolka - *Von Fermat bis Minkowski.* Eine Vorlesung ber Zahlentheorie und ihre Entwicklung. Springer-Verlag, Berlin-New York, 1980.

[61] E. Selmer - *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. Acta Math. **85** (1951), 203-362. Zie b.v. https//www.math.lsu.edu/~verrill/teaching/math7280/selmer-example/selmer-example.pdf

[62] J-P. Serre - *Lecture on the Mordell-Weil theorem.* Asp. Math. E 15, Vieweg, 1989.

[63] D. Shanks - *Solved and unsolved problems in number theory.* Chelsea Publ. Cy., 1978.

[64] G. Shimura - *Introduction to the arithmetic theory of automorphic functions.* Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.

[65] Simon Singh - *Fermat's Last Theorem.* Fourth Estate, 1997.
We citeren dit boek met [S].
Simon Singh - *Het laatste raadsel van Fermat.* Arbeiderspers, 1998.

[66] S. Singh - *The code book, the science of secrecy from ancient Egypt to quantum cryptography.* Fourth Estate, 1999.
S. Singh - *Code, de wedloop tussenmakers en brekers van geheime codes en cijferschrift.* De Arbeiderspers, 1999.
http://www.math.leidenuniv.nl/~naw/serie5/deel01/jun2000/pdf/vermeulen.pdf

[67] S. Singh - *Big bang: the origin of the universe.* Fourth Estate, 2004.
http://www.simonsingh.net/Big-Bang-Reviews.html
S. Singh - *De oerknal.* De Arbeiderspers, 2005.

[68] I. Stewart & D. Tall - *Algebraic number theory.* Second edition. Chapman and Hall Mathematics Series. Chapman & Hall, London, 1987.

[69] *De laatste stelling van Fermat*, Syllabus van lezingen gehouden op 6-XI-1993. WG & Universiteit Utrecht.

[70] Syllabus Algebra, ontwikkeld sinds 1964 in Amsterdam en Leiden, nu online, zie
http://websites.math.leidenuniv.nl/algebra/algebra1.pdf

[71] B. van der Waerden - *Moderne Algebra.* Eerste uitgave in 1931.
Vierde uitgave: Heidelberger Taschenbuch, 2 delen, Springer, 1967.

[72] A. Weil - *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen.* Math. Ann. **168** (1967), 149--156.

[73] A. Weil - *Number theory, an approach through history, from Hammurapi to Legendre.* Birkhäuser 1984.

[74] A. Weil - *Prehistory of the zeta-function.* Sympos. Atle Selberg (1987): Number theory, trace formulas and discrete groups (Editors A. Aubert, E. Bombieri & D. Goldfeld). Acad. Press 1989.

[75] E. Weiss - *Algebraic number theory.* Mc-Graw-Hill Cy, 1963.

[76] A. Wiles - *Modular elliptic curves and Fermat's Last Theorem.* Annals Math. **141** (1995), 443-551.

[77] H. Wilf - *What is an answer?* Amer. Math. Monthly, **89** (1982), 289-292.

[78] D. Zagier - *A one-sentence proof that every prime* $p \equiv 1 \pmod 4$ *is a sum of two squares.* Amer. Math. Monthly **97** (1990), page 144.

[79] D. Zagier - *The first 50 milion prime numbers.*
http://sage.math.washington.edu/edu/2007/simuw07/misc/
zagier-the-first-50-million-prime-numbers.pdf
Published in *The Mathematical Intelligencer*, Vol. **0**, August 1977.

[80] D. Zagier - *Newman's short proof of the prime number theorem.* Amer. Math. Monthly **104** (1997), 705--708.

Frans Oort
Mathematisch Instituut
Pincetonplein 5
3584 CC Utrecht
email: f.oort@uu.nl
http://www.staff.science.uu.nl/~oort0109/