Elliptische krommen en hun rol in de wiskunde

Frans Oort

november / december 2011

HOVO-cursus wiskunde Utrecht

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 [82] 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.

Nadenken loont. – Ik denk dat materiaal van deze cursus kan worden uitgelegd aan iedereen die bereid is na te denken, ongeacht de voorkennis.

In deze cursus bespreek ik een prachtige structuur: een *elliptische kromme*. Weliswaar is dat begrip niet heel eenvoudig uit te leggen. Maar we zien dit in veel aspecten van de wiskunde op een vaak onverwachte manier opduiken.

Een elliptische kromme is niet een ellips, en als reële ruimte gezien is het niet een kromme. Maar deze krommen traden op bij het berekenen van "elliptische integralen", vandaar de naam.

"Elke formule in een tekst halveert het aantal geïnteresseerde lezers.
Als dit zo zou zijn dan heeft deze syllabus aan het eind bar weinig lezers over. Maar ik verwacht dat dít gehoor daar anders over denkt. Mooie wiskunde kun je nu eenmaal niet uitleggen zonder logische stappen te beschrijven met wiskundige terminologie, zonder de gedachten te preciseren in compacte formules. In vroegere wiskundige culturen werd soms wiskunde beschreven in lange teksten, die bovendien niet precies genoeg waren. In de moderne wiskunde kunnen we een hoge mate van precisie bereiken door de dingen die we beschrijven in eenvoudige en directe definities te vatten, en vervolgens met duidelijke formules de voortgang van de gedachten gang te ondersteunen. – Ja, dat kan wel eens abstract worden. Daarom is het zo goed als een wiskundige tekst gelardeerd wordt met uitleg, beschrijven van de achtergrond, benoemen van de wiskundige intuïtie, en vooral door het expliciet maken van "dwarsverbanden" (bij voorbeeld een algebraïsche formule meetkundig begrijpen, we zullen daar mooie voorbeelden van zien).

Hier en daar zal ik wat verder gaan dan elementaire voorkennis toestaat. Elk onderdeel waar iets meer voorkennis verondersteld wordt wordt met een * aangegeven. Zulke onderdelen kunt U gerust overslaan. *Al het andere materiaal hoop ik, verwacht ik, is geheel toegankelijk voor iedereen die durft na te denken, die bereid is abstracte gedachten toe te laten.*

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.

Een ander aspect is het feit dat je al die vergezichten, die prachtige gedachten kunt vatten in precieze beschrijvingen, dat je moeilijke conclusies kunt bewijzen door middel van sluitende gedachten gangen. – Ik hoop en verwacht van alle deelnemers dat ze aan de slag gaan: niet

alleen passief luisteren, maar ook vragen stellen, en vooral elke week tenminste één bewijs zelfstandig en volledig uitschrijven. Zo krijgt U voeling met deze wondere wereld, zo ziet U hoe een nadenken inzicht kan geven, hoe de elegantie en schoonheid wonderlijke vergezichten opent.

Een elliptische kromme is zo interessant, en kan zo mooi gebruikt worden, omdat twee verschillende structuren in één object samen komen. Enerzijds zien we het begrijp "groep": een verzameling waarvan de elementen kunnen worden "opgeteld" zie § 7. Dit is een abstractie van een begrip dat we steeds weer tegen komen: alle symmetriën van één object vormen een groep, met "achter elkaar uitvoeren" als groepswet. Maar in de algebra en getal theorie zie we ook steeds die structuur optreden: gehele getallen kun je optellen, zoals we al sinds onze kinder jaren weten, en nog steeds heeft die optelling geheimen, kunnen we fascinerende vragen daarover stellen. Als U met een pinpas geld uit de muur haalt gebruikt U structuren die die door de groepen theorie gegeven worden; zie § 12. Groepen zijn overal om ons heen.

Anderzijds zijn er meetkundige eigenschappen. Om U een eenvoudig, maar zoals zal blijken, een uiterst effectief middel aan te geven: bij een punt op een kromme in het vlak kunnen we de raaklijn tekenen en ons afvragen of er nog meer snijpunten zijn. Een elliptische kromme is een kubische kromme (gegeven door een derde-graads vergelijking), een raaklijn geeft een wel-bepaald derde snijpunt; plotseling krijgen we bij één punt op een kubische kromme een hele reeks nieuwe punten door steeds het proces raaklijn - derde snijpunt te herhalen. De algebraïsche formules die dit proces beschrijven zijn exact maar heel ingewikkeld, terwijl het meetkundig idee prachtig eenvoudig is.

Al deze aspecten worden in een elliptische kromme bij elkaar gebracht: het is een meetkundige structuur, en de punten erop vormen een groep. Dan kunnen we verwachten dat een dergelijke rijke structuur allerlei toepassingen heeft.

We zullen er twee laten zien. Het probleem van de *congruente getallen*, zie § 5, is al vele eeuwen oud. We hebben nog steeds niet een sluitend criterium welke getallen congruent zijn. Lang is dit een probleem geweest waar we niet de achter liggende structuur begrepen. Tot we inzagen dat het samen valt met het vinden van rationale punten op een elliptische kromme. Plotseling kunnen we het probleem op een heel andere manier benaderen. Alle technieken beschikbaar voor elliptische kromme kunnen we gaan toepassen, en tot een helder vermoeden over dit probleem komen (dat nog niet opgelost is).

In 1822 bewees Poncelet zijn sluitingsstelling over punten op en raaklijnen aan twee kegelsneden. De bewijzen de Poncelet vond waren ingenieus maar niet gemakkelijk te begrijpen. We zullen zien in § 6 dat een diepe stelling over elliptische krommen een verder verbluffend eenvoudig bewijs van deze stelling geeft (waar de combinatie van de meetkunde en de optelling op een ellliptische kromme een doorslaggevende rol speelt).

We zullen ook nog even stil staan bij een van de mooiste ontwikkelingen in de moderne wiskunde: *de Laatste Stelling van Fermat.* 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 hebben tot 1995 moeten wachten op een bewijs. In de syllabus zal ik nog aangeven waar naar mijn mening mogelijk dat "wonderlijke bewijs" van Fermat was, zie (4.36). Lang was dit een "geïsoleerd probleem". In 1985 kwam de wiskundige Gerhard Frey met het volgende

idee: beschouw $n \in \mathbb{Z}_{\geq 3}$, waar n een "groot getal is" (voor kleine n was het probleem opgelost, maar uiteindelijk bleek $n = p \geq 5$ voldoende te zijn: alle voorgaande berekeningen werden vervangen door "pure thought"). Veronderstel dat er een oplossing $a, b, c \in \mathbb{Z}$ van de Fermat vergelijking is met $abc \neq 0$ (m.a.w. neem aan dat er een tegenvoorbeeld zou bestaan). Beschouw de elliptische kromme gegeven door $Y^2 = X(X - a^n)(X + b^n)$. We hebben veel ervaring met het werken met zulke kromme, en we krijgen al snel de intuïtie dat een kromme met zulke uitzonderlijk eigenschappen niet kan bestaan; dan kan ook een dergelijke oplossing niet bestaan, en FLT zou bewezen zijn. Dit was een grote doorbraak. Plotseling was het probleem in verband gebracht met een rijke, veel bestudeerde structuur. Tien jaar later was Andrew Wiles in staat (met hulp van Ribet, Serre, Taylor, en met theorie ontwikkeld door vele anderen) te laten zien dat de achter liggende theorie (het vermoeden van Shimura-Taniyama-Weil) juist was, en daarmee werd een probleem na 350 jaar opgelost. Met als centraal hulpmiddel: ellliptische krommen.

Aspecten uit de geschiedenis van de wiskunde kun je op twee wezenlijk verschillende manieren beschrijven. Enerzijds kan men kiezen voor de methode de notatie, het gedachten goed, de gevoelens van de periode die je beschrijft zorgvuldig te beschrijven in de taal en notatie van die tijd; een historicus zal in het algemeen deze weg volgen. Anderzijds kun je het historisch materiaal in moderne notatie en interpretatie weergeven. Hier heb ik voor voor deze tweede methode gekozen.

De §§ 1 – 6 bevatten het basis materiaal voor de cursus. De appendices A – C gaan over technische begrippen die ik nodig zal hebben. Notaties en symbolen die we gebruiken worden uitgelegd in § 14. De §§ 10 – 13 bevatten materiaal dat niet veel met het onderwerp van deze cursus te maken heeft; wellicht vindt U het leuk om die onderwerpen door te nemen. Ook zullen we elke week een of meer vraagstukken / puzzels maken.

1 Elliptische krommen

Deze paragraaf zal onvolledig zijn (de theorie van elliptische krommen is enorm), en ook zullen de beschouwingen lang niet allemaal elementair zijn. Ik probeer dit onderwerp zo direct en elementair mogelijk te brengen. We nemen soms een lichaam K, zonder te specificeren welk. In de praktijk van deze cursus zal meestal $K = \mathbb{C}$ genomen worden, of $K = \mathbb{Q}$ en een heel enkele keer $K = \mathbb{R}$; voor de theorie van lichamen zie de literatuur, of zie § 8.

(1.1) Eerst een paar hulpmiddelen. Voor een veelterm (polynoom) $f = A_0X^n + A_1X^{n-1} + \cdots + A_{n-1}X + A_n$ schrijven we F_X of $(d/dX)f$ voor de formele afgeleide; dit geven we door $(d/dX)BX^i := iBX^{i-1}$, waar B de variabele X niet bevat.

We schrijven $\mathbb{A}^2_K$ voor de affiene ruimte van dimensie twee; soms werken we over K, en dan is $\mathbb{A}^2(K) = K^2$; maar soms willen we punten met coördinaten in $\mathbb{C}$ beschouwen, en we schrijven $\mathbb{A}^2_K(\mathbb{C}) = \mathbb{C}^2$. Beschouw een veelterm in twee variabelen $f \in K[X, Y]$ (denk aan $K = \mathbb{Q}$ en $f = -Y^2 + X^3 + AX + B$). We schrijven $\mathcal{Z}(f) \subset \mathbb{A}^2$ (spreek uit: de nulpuntenverzameling van f) voor:

$$\mathcal{Z}(f) = \{(x, y) \mid f(x, y) = 0\}; \quad \text{voor } \ K \subset L: \quad \mathcal{Z}(f)(L) := \{(x, y) \in L^2 \mid f(x, y) = 0\}.$$

We zeggen dat $P = (x, y) \in \mathcal{Z}(f)$ een *niet-singulier punt* is als

$$f_X(P) \neq 0 \quad \text{en} \quad f_Y(P) \neq 0.$$

(1.2) Een uitleg.* merk op dat we X gebruiken voor een variabele, en x voor een waarde die de variabele kan aannemen. Waarom doen we zo ingewikkeld? We willen graag meetkundige methoden in de getal theorie gebruiken. Als we nemen $f = X^2 + Y^2 + 1$ dan is $\mathcal{Z}(f)(\mathbb{Q}) = \emptyset$ maar $\mathcal{Z}(f)$ bevat veel punten (met coördinaten b.v. in $\mathbb{C}$). We zullen voorbeelden van een eliptische kromme E zien waar $E(\mathbb{Q})$ eindig is, maar $E(\mathbb{C})$ heel groot.

Neem aan dat $P = (0, 0) \in \mathbb{A}^2$ en $f(P) = 0$. Dan kunnen we schrijven

$$f = 0 + aX + bY + (\text{hot})$$

waar "hot" staat voor "hogere orde termen", d.w.z. termen waarvan de totale graad in X en Y minstens twee is. Wat is de conditie "P is niet-singulier op $\mathcal{Z}(f)$ in dit geval? Ga na: dit is equivalent met $a \neq 0$ of $b \neq 0$. Intuïtief: "de kromme is glad in de buurt van P, en de raaklijn en de kromme zien er in de buurt van P precies zo uit".

(1.3) Definitie. We werken over een lichaam $K \subset \mathbb{C}$. We werken in het vlak $\mathbb{A}^2_K$. Om een elliptische kromme te definiëren gebruiken we twee getallen

$$A, B \in K \quad \text{met} \quad 4{\cdot}A^3 + 27{\cdot}B^2 \neq 0.$$

We schrijven

$$E = \mathcal{Z}(-Y^2 + X^3 + AX + B) \cup \{\infty\}.$$

In het bijzonder:

$$E(L) = \{(x, y) \in L^2 \mid y^2 = x^3 + aX + B\} \cup \{\infty\}.$$

Hierbij is ∞ een punt dat we aan $\mathbb{A}^2$ toevoegen. Het is gelegen ("in het oneindige") op elke verticale rechte. De verzameling $E(\mathbb{C})$ zal genoemd worden "*de elliptische kromme gedefiniëerd door* A, B".

(1.4) Een uitleg / opmerkingen.* Waar komt die conditie $4{\cdot}A^3 + 27{\cdot}B^2 \neq 0$ vandaan?
Opgave. Laat zien dat dit equivalent is met "$\mathcal{Z}(-Y^2 + X^3 + AX + B)$ is niet-singulier".

Wat een onbegrijpelijke definities zult U denken, en misschien ook zeggen. Om tot een meer logische definitie te komen zou ik kunnen zeggen: "*een elliptische kromme is een projectieve, niet-singuliere kromme van geslacht één met een vast gekozen punt*". We kunnen bewijzen dat een dergelijke kromme in te bedden is in een projectief vlak. Dat we die inbedding zo kunnen kiezen dat het gekozen punt een buigpunt is, bovendien gelegen in $(0:1:0)$ (het punt gelegen op oneindig waar alle verticale lijnen elkaar ontmoeten); bovendien kunnen we nog een coördinaten transformatie toepassen zodanig dat de vergelijking van de kromme in affiene coördinaten $Y^2 = X^3 + AX + B$ wordt.

Opgave. De vergelijking $y^2 = X^3 - 3X + 2$ definiëert niet een eliptische kromme; waarom niet?

(1.5) Andere normaal vormen. Soms is het gemakkelijker om een vergelijking te gebruiken (om E te definiëren) die iets verschillend is van de vergelijking in (1.3). We zeggen dat twee vergelijkingen over K dezelfde E geven als er een inverteerbare, lineaire transformatie is over K die de ene vergelijking in de andere overvoert.
Voorbeeld. De vergelijking $V^2 + V = U^3 - U$ gaat door de transformatie toe $4U = X,\ \ 8V + 4 = Y$ over in $Y^2 = X^3 - 16X + 16$; zie (3.15).
Voor allerlei normaal vormen zie de appendix van deze §.

(1.6) De raaklijn. Neem $P = (x, y) \in C := \mathcal{Z}(f) \subset \mathbb{A}^2$; neem aan dat dit een niet-singulier punt is van $C = \mathcal{Z}(f)$. We definiëren de raaklijn ℓ aan C in P als:

$$\ell = \mathfrak{t}_{C,P} = \mathcal{Z}(f_X(P)(X - x) + f_Y(P)(Y - y)).$$

Ga na: omdat P niet-singulier is op C is het polynoom $\mathcal{Z}(f_X(P)(X - x) + f_Y(P)(Y - y))$ lineair en ongelijk aan nul; merk op: $P \in \mathfrak{t}_{C,P}$.

(1.7) Een uitleg.* Neem aan dat $P = (0, 0)$ en $f = 0 + aX + bY + (\text{hot})$ met $a \neq 0$ of $b \neq 0$. Dan is $\mathcal{Z}(f_X(P)(X - x) + f_Y(P)(Y - y)) = aX + bY$. We zien dat we precies het lineaire gedeelte van f gebruiken om ℓ te defniëren. Als $P = (x, y)$ dan schrijven we $f = 0 + a(X - x) + b(Y - y) + (\text{hotin}(X - x).(Y - y))$, etc.

(1.8) Snijpuntsmultipliciteit. Dit is een veelzijdig onderwerp. Geheel in de stijl van deze cursus geven we de definitie in een speciaal geval, en verwijzen voor algemenere definities en eigenschappen naar algemenere theorie.

Zij $g \in K[X, Y, Z]$ een homogeen polynoom en schrijf $C := \mathcal{Z}(g)$. Zij $L := \mathcal{Z}(aX + bY + cZ) \subset \mathbb{P}^2_K$ een lijn; we nemen aan $a \neq 0$ of $b \neq 0$ of $c \neq 0$; beschouw $P = [x : y : z] \in C \cap L$. We definiëren $i(C, L; P)$, de *snijpuntsmultipliciteit* van C en L in P als volgt. Onderstel dat $a \neq 0$. Substitueer:

$$g(-(bY + cZ)/a, Y, Z).$$

Als dit polynoom in Y en Z gelijk aan nul is, dan deelt $aX + bY + cZ$ het polynoom g, en we schrijven $i = \infty$. Zo niet, dan is dit poynoom na substitutie niet gelijk aan nul en we schrijven

$$g(-(bY + cZ)/a, Y, Z) = (yZ - zY)^{\alpha}.h(Y, Z)$$

met $h(y,z) \neq 0$ (m.a.w. we splitsen de factor $(yZ - zY)$ af zo vaak als dat kan). Terzijde: we weten dat $\alpha > 0$ (is dit duidelijk ?). We schrijven in dit geval

$$i(C, L; P) \quad := \quad \alpha.$$

Overigens, als $Q \notin C \cap L$, dan schrijven we $i(C, L; Q) = 0$.

(1.9) Opgave. Uitleg raaklijn. Zij $(x, y) = P \in C^0 = \mathcal{Z}(f)$ met notatie als boven, en zij $P \in L = \mathcal{Z}(aX + bY + c)$ met $a \neq 0$ of $b \neq 0$. Bewijs: dan is $i(C, L; P) > 0$ en

$$i(C^0, L; P) = 1 \quad \Longleftrightarrow \quad \left(P \in C^0 \quad \text{is niet-singulier en} \quad L \neq \mathfrak{t}_{C^0,P}\right).$$

M.a.w. de raaklijn is in een niet-singulier punt de enige lijn die met hogere multipliciteit snijdt en in een singulier punt snijden alle lijnen door dat punt met een hogere multipliciteit.

(1.10) Lemma. *Elke rechte lijnm snijdt E in precies drie punten, met getelde multipliciteiten. Als $m \cap E = \{P, Q, S\}$ en $P, Q \in E(L)$, met m en E gedefinieerd over K en $K \subset L$, dan is ook $S \in E(L)$.*

Bewijs. Als die lijn verticaal is, gegeven door $aX + c$, met $a \neq 0$, dan geeft substitutie de vergelijking $y^2 = (-c/a)^3 + A(-c/a) + b$. Die vergelijking heeft precies twee oplossingen, samenvallend als die lijn aan de kromme raakt, of verschillend anders. Bovendien ligt ∞ ook op die lijn. We krijgen 3 snijpunten.

Als die lijn niet verticaal is, dan kan die lijn gegeven worden door $aX + bY + c$ met $b \neq 0$. Substitutie geeft $((-ax - c)/b)^2 = x^3 + Ax + b$. Dat geeft een vergelijking van graad precies 3, en we krijgen drie oplossingen voor x; uit $y = (-ax - c)/b$ volgt de y-coördinaat van een dergelijk punt. We zien dat we drie snijpunten krijgen (geteld met multipliciteit).

De coördinaten van het derde snijpunt kunnen verkregen worden door oplossingen van de vergelijkingen voor $m = \mathcal{Z}(H)$, $E = \mathcal{Z}(f)$; eliminatie van één van de variabelen geeft een kubische vergelijking in de ander (of een kwadratische als $\infty \in m$); daarvan weten dat twee nulpunten gelegen zijn in L, dus het eventuele derde nulpunt ook. QED

(1.11) Een mooi mechanisme: raaklijn – derde snijpunt. Voor gegeven $P, Q \in E(L)$ construeren we de rechte lijn m die P met Q verbindt; als $P \neq Q$ dan ligt die lijn vast; als $P = Q$, dan trekken we de raaklijn $m = \mathfrak{t}_{E,P}$ in $P = Q$ aan E. Het derde snijpunt (gebruik het vorige lemma) noemen we $P * Q$. we hebben gezien dat bij gegeven $P, Q \in E(L)$ het punt $P * Q$ vast ligt. Bovendien geldt: $P * Q \in E(L)$.

We zullen i (5.24) een *"mysterieus mechanisme"* zien: een toepassing van de "raaklijn – derde snijpunt methode" in de getal theorie; een eenvoudig meetkundig principe geeft mysterieuze algebraïsche formules, en het geeft inzicht in een vraag betreffende congruente getallen.

We gaan dat mechanisme $P_0 \in E$, raaklijn, derde snijpunt is P_1, $\cdots$ $P_i \in E$, raaklijn, derde snijpunt is $P_{i+1}, \cdots$ in een aantal gevallen doorrekenen.

(1.12) Opgave. Zij $P = P_0 = (1, 0)$ op de kromme gegeven door $Y^2 + Y = X^3 - X^2$. Bepaal alle P_i. Vergelijk (3.2).

(1.13) Opgave. Zij $P = P_0 = (0, 0)$ op de kromme gegeven door $Y^2 + Y = X^3 - X$. Bepaal een aantal P_i. Maar dan wil je toch wel opgeven na een tijdje ? Vergelijk (3.14).

(1.14) Opgave. Zij $P = P_0 = (3, -8)$ op de kromme gegeven door $Y^2 = X^3 - 43X + 166$. Bepaal alle P_i. (hier de moed niet opgeven.). Vergelijk [79] .

We gaan nu een curieuze handeling verrichten, cruciaal voor alle verder beschouwingen. We kiezen het punt $\infty =: 0$, dat wil zeggen we noemen dat punt het nul-punt op E, en we gaan een *commutative groepswet* op $E(\mathbb{C})$ definiëren.

(1.15) Constructie. Voor gegeven $P, Q \in E(L)$ construeren we de rechte lijn m die P met Q verbindt; als $P \neq Q$ dan ligt die lijn vast; als $P = Q$, dan trekken we de raaklijn $m = \mathfrak{t}_{E,P}$ in P aan E. Het derde snijpunt (gebruik het vorige lemma) noemen we $S = P * Q$. Verbindt $P * Q$ met 0 door de lijn m'; dat wil zeggen trek de verticale lijn door S als $S \neq 0$, als $S = 0$. Noem het derde snijpunt van L' met $E(\mathbb{C})$ het punt $P + Q$; als $S = 0$ schrijven we $P + Q = 0$.

$$m \cap E = \{P, Q, P * Q\} \quad m' \cap E = \{P * Q, 0, P + Q\} : \quad P + Q = (P * Q) * 0.$$

We maken wat opmerkingen. We zien dat $P + Q = Q + P$. Als E gegeven is zoals in (1.3) dan geldt dat voor alle $P = (x, y) \in E$ geldt $-P = (x, -y)$; inderdaad, in dat geval is $S = 0$; dit is de definitie van de inverse voor de optelling. Merk op / bewijs dat voor $P = (x, y)$ geldt: $2P = 0$ dan en slechts dan als $f_Y(P) = 0$; als E gegeven is zoals in (1.3) dan geldt $P \neq 0, 2P = 0 \Rightarrow P = (x, 0)$.

(1.16) Feit. *Voor gegeven $A, B \in K$, met $4{\cdot}A^3 + 27{\cdot}B^2 \neq 0$, en de keuzen $\infty =: 0$ en de operaties $+$ en $-$ als boven is de verzameling $E(K)$ een groep.*
Een bewijs zal ik niet geven. Het staat in elk goed boek over elliptische krommen. Bv. zie [41]. Het bewijs van dit feit is niet moeilijk op een punt na: inderdaad geldt $((P + Q) + R) = (P + (Q + R))$.

Een elliptische krommen combineert twee aspecten: het is een meetkundig object (we kunnen de raaklijn in een punt trekken, en nog veel meer van zulke meetkundige technieken toepassen), en het is een algebraïsch object (de punten vormen een groep), en die twee aspecten zijn met elkaar verbonden (de groepswet volgt uit een meetkundige constructie).
Opmerking.* Dit is een zeldzaamheid. Bewezen kan worden: een projectieve algebraïsche kromme een groepswet toelaat gedefini¨eerd door meetkunde eigenschappen dan en slechts dan als het een elliptische kromme is.

Appendix van deze §: **normaalvomen.**

In de meeste gevallen wordt een elliptische kromme gegeven door een vergelijking. We zullen gebruik maken en verwijzen naar de volgende vergelijking, die vaak *Weierstrass vergelijkingen* worden genoemd.
Zie [41], III.2 en VIII.3; [52], II.2; [79], III.1; [80], I.4; [81], I.3 en p. 43.

In elk van deze gevallen geldt: de vergelijking geeft een niet-singuliere kromme (en dus een elliptische kromme) dan en slechts dan als $\Delta = \Delta(E) \neq 0$.

Elk van de vergelijkingen vermeld in (1.17) – (1.19) wordt een *Weierstrass vergelijking* of een *Weierstrass normaal vorm* genoemd.

(1.17)

$$Y^2 = X^3 + AX + B; \qquad \text{(W1)}$$

$\Delta(E) = 4A^3 + 27B^2$.

(1.18)

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6; \qquad \text{(W2)}$$

$b_2 = a_1^2 + 4a_2$,
$b_4 = 2a_4 + a_1a_3$,
$b_6 = a_3^2 + 4a_6$,
$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$,
en
$\Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$,

(1.19)

$$Y^2 = X^3 + aX^2 + bX + c; \qquad \text{(W3)}$$

$\Delta(E) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$,

(1.20)

$$Y^2 = 4X^3 - g_2X - g_3; \qquad \text{(W4)}$$

$$\Delta(E) = g_2^3 - 27g_3^2.$$

(1.21) (J. Tate)

$$Y^2 + XY = X^3 - \frac{36}{t-1728}X - \frac{1}{t-1728}; \qquad \text{(W5)}$$

$$\Delta(E) = t^2/(t-1728)^3;$$

(! bewijs dit !).

(1.22) De Legendre normaal vorm.

$$Y^2 = X(X-1)(X-\lambda) \qquad \text{(W6)}$$

$$\Delta = \Delta(E) = \lambda^2(1-\lambda)^2; \qquad j(E) = 2^8 \cdot \frac{(1-\lambda+\lambda^2)^3}{\lambda^2(1-\lambda)^2}.$$

(1.23)

$$X^3 + Y^3 + Z^3 = 3\mu XYZ \qquad \text{(W7)}$$

$$j(E) = 3^3 \cdot \frac{\mu^3(\mu^3+8)^3}{(\mu^3-1)^3}.$$

Laat zien dat dit een elliptische kromme is desda $\mu^3 \neq 1$.

2 Elliptische krommen over $\mathbb{C}$

In deze § beschrijven we een klassieke methode: uniformizatie van elliptische krommen over $\mathbb{C}$ met behulp van transcendente functies. We zullen niet veel bewijzen. Het is goed om de uitspraken van deze paragraaf te begrijpen, als motivatie en achtergrond bij het hanteren van elliptische krommen. Methoden uit deze § zijn klassiek, en ook modern te bewijzen. Het blijkt echter dat deze methode niet altijd de juiste informatie geeft in arithmetische situaties.

(2.1) Opmerking. Een elliptische kromme over $\mathbb{C}$ kan gegeven worden door middel van een vergelijking, zie (1.20):

$$Y^2 = 4X^3 - g_2X - g_3; \qquad (W3)$$

met

$$\Delta = \Delta(E) = g_2^3 - 27g_3^2 \neq 0.$$

(2.2) Definitie. Onderstel gegeven $\omega_1, \omega_2 \in \mathbb{C}$ zodanig dat $\{\omega_1, \omega_2\}$ een $\mathbb{R}$-lineair onafhankelijk stelsel is. De groep

$$\mathbb{Z}\cdot\omega_1 \times \mathbb{Z}\cdot\omega_2 =: \Lambda_{\omega_1,\omega_2} = \Lambda \subset \mathbb{C}$$

wordt een *rooster* in $\mathbb{C}$ genoemd.
Equivalente definitie. De additieve groep $\Lambda \subset \mathbb{C}$ bevat een stelsel $\mathbb{R}$-voortbrengers voor de $\mathbb{R}$-vectorruimte $\mathbb{C}$ en $\Lambda \subset \mathbb{C}$ is discreet, d.w.z. er is een $\epsilon \in \mathbb{R}_{>0}$ zodanig dat elke cirkel in $\mathbb{C}$ met straal ϵ hooguit één punt van Λ bevat.

(2.3) Feit / Stelling* (Weierstrass; complexe uniformizatie van een elliptische kromme.)
(1) *Zij E een elliptische kromme over $\mathbb{C}$. Veronderstel dat $Y^2 = 4X^3 - g_2X - g_3$ een vergelijking is die E geeft. Dan is er een rooster $\Lambda = \Lambda_{\omega_1,\omega_2} \subset \mathbb{C}$, en er is een meromorfe functie $\wp$ op $\mathbb{C}$, holomorf op $\mathbb{C}$ buiten Λ, die dubbel-periodiek is:*

$$\wp(z) = \wp(z + a\cdot\omega_1 + b\cdot\omega_2), \qquad \forall a, b \in \mathbb{Z}$$

die voldoet aan de differentiaal vergelijking

$$(\wp')^2 = \wp^3 - g_2\wp - g_3.$$

Hier is $\wp' = (d/dz)(\wp)$. *In dit geval geeft*

$$(\wp, \wp') : \mathbb{C} \longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C})$$

een surjectieve afbeelding, die een groeps-ismorfisme

$$\mathbb{C}/\Lambda \quad \xrightarrow{\sim} \quad E(\mathbb{C})$$

induceert. Hierin wordt elke $z \in \Lambda$ afgebeeld op $\infty = 0 \in E$.
(2) *Omgekeerd geeft elk rooster $\Lambda = \Lambda_{\omega_1,\omega_2} \subset \mathbb{C}$ een Weierstrass dubbel-periodiek functie, die aan een differentiaal vergelijking voldoet, en die vergelijking definieert een elliptische kromme (zoals hierboven).*
(3) Merk op: een $\mathbb{C}$–lineaire afbeelding $\mathbb{C} \to \mathbb{C}$ is niets anders dan het vermenigvuldigen met een complex getal $t \in \mathbb{C}$. *Een afbeelding*

$$\times t : \mathbb{C} \longrightarrow \mathbb{C} \quad \textit{die de eigenschap heeft} \quad t\cdot\Lambda \subset \Lambda$$

induceert een endomorfisme van $E(\mathbb{C})$. Dit geeft een isomorfisme van ringen:

$$\{t \in \mathbb{C} \mid t{\cdot}\Lambda \subset \Lambda\} \xrightarrow{\sim} \mathrm{End}_{\mathbb{C}}(\mathbb{C}/\Lambda) \cong \mathrm{End}(E).$$

Voor expliciete formules zie o.a. [81], pag. 43. Zie ook [41], Ch. VI; [52], Ch. III; [79], Ch. VI.
Een klassieke beschrijving van de Weierstrass $\wp$–functie vinden we in:
E. Whittaker & G. Watson – A course of modern analysis. Cambridge Univ. Press, 1969.
QED

Over deze stelling en over het bewijs ervan is veel te vertellen. Laat ik slechts enkele opmerkingen maken. Het klassiek bewijs van deze stelling maakt gebruik van complexe functie-theorie. Daarin kunnen we het verband tussen enerzijds de getallen g_2 en g_3 en anderzijds de perioden ω_1 en ω_2 expliciet (maar niet eenvoudig) geven. Die formules zijn erg mooi, mar niet altijd practisch.

Hier is een voorbeeld. Als ω_1/ω_2 (imaginair) kwadratisch is over $\mathbb{Q}$ dan is $j(\mathbb{C}/\Lambda)$ een getal dat geheel is over $\mathbb{Z}$. Maar het is niet eenvoudig om dat feit expliciet uit de formules af te leiden.

Een modern bewijs van de stelling maakt gebruik van theorie van complexe Lie groepen; daarin volgt de afbeelding $\mathbb{C} \cong \mathfrak{t}_{E,0} \to E(\mathbb{C})$ als exponentiaal afbeelding; compactheid van $E(\mathbb{C})$ geeft dat de kern van deze afbeelding een rooster is, en daarom voortgebracht over $\mathbb{Z}$ door twee "perioden". Het laatste deel van de stelling past in een algemene theorie, die voor compacte algebraïsche variëteiten een isomorfisme geeft tussen de analytische en de algebraïsche afbeeldingen (een diepe stelling van Chow en van Serre). Beide benaderingen zijn niet elementair.

Deze stelling ligt ten grondslag aan een indrukwekkend apparaat, de benadering van arithmetische problemen via modulaire vormen (geheel buiten het materiaal voor dit project, helaas !).

(2.4) Opgave. Zij $\Lambda_\tau := \mathbb{Z}{\cdot}1 + \mathbb{Z}{\cdot}\tau$ met $\tau \in \mathbb{C}$ en $\mathrm{Im}(\tau) > 0$. Stel dat er een $t \in \mathbb{C}$ is met $t \notin \mathbb{R}$ en $t(\Lambda_{1,\tau}) \subset \Lambda_{1,\tau}$. Bewijs dat in dit geval $L := \mathbb{Q}(\tau) \supset \mathbb{Q}$ een imaginair kwadratische uitbreiding is (m.a.w. τ voldoet aan een kwadratische vergelijking over $\mathbb{Q}$).

(2.5) Opgave. (1). Zij $K \subset \mathbb{C}$ een lichaam. Zij E een elliptische kromme over K. Laat zien dat $\mathrm{End}(E)$ een commutatieve ring is.
(2) Over $\mathbb{C}$. Bewijs dat elke orde in elk imaginair kwadratisch getallen lichaam L kan optreden als een endomorfismen ring van een elliptische kromme over $\mathbb{C}$ (een orde in L: een deelring van de ring van gehelen $\mathcal{O}_L$ die bovendien daarin van eindig index is als additieve groep).

(2.6) Opmerking. We willen graag toepassingen van deze theorie van elliptische krommen over $\mathbb{C}$ maken in de getal theorie (b.v. punten met coördinaten in $\mathbb{Q}$ uitrekenen, of voldoende theorie ontwikkelen over elliptische krommen over $\mathbb{Q}$ om FLT te bewijzen). Het blijkt dat (2.3) niet direct hierbij helpt, en wel om de volgende reden. De functies $\wp$ en $\wp$ zijn "transcendente functies" (net zoals de sinus, de cosinus, de logaritme). Voor een dergelijke functie is het vaak heel moeilijk om een verband te leggen tussen arithmetische eigenschappen van enerzijds z en anderzijds de waarde $h(z)$. Aan dit soort problemen is eeuwen lang gewerkt, en er zijn nog veel vragen onbeantwoord.

Vergelijk (2.3) met de parametrizatie

$$t \longmapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right) \in C := \mathcal{Z}(X^2+Y^2-1) \subset \mathbb{A}^2_{\mathbb{Q}};$$

Zie (4.9). Deze laatste parametrizatie gebruikt rationale functies (breuken van polynomen). We concluderen dat $C(\mathbb{Q})$ een oneindige verzameling is.

Maar uit het feit dat

$$\left(\mathbb{Q}\cdot 1 + \mathbb{Q}\cdot\sqrt{-1}\right) \subset \mathbb{C}$$

een oneindige deelverzameling is volgt niet dat

$$\left(\mathbb{Q}\cdot 1 + \mathbb{Q}\cdot\sqrt{-1}\right)/\Lambda \subset \mathbb{C}/\Lambda \cong E(\mathbb{C})$$

een oneindige verzameling in $E(\mathbb{Q})$ geeft.

Wel is het zo dat (2.3) toegang geeft tot de theorie van "modulaire vormen", en die bevat de sleutel tot veel ontwikkelingen in de klassiek en de moderne wiskunde (waaronder het bewijs van FLT).

3 Torsie punten

In deze paragraaf behandelen we punten van (on)eindige orde op elliptische krommen. We zullen zien:

over $\mathbb{C}$ kunnen we de groep van punten van eindige orde precies aangeven;

over een willekeurig lichaam, maar in het bijzonder over $\mathbb{Q}$, hangt het af van de kromme en het lichaam;

we kunnen in veel gevallen effectief beslissen welke punten eindige orde hebben;

er zijn in het algemeen veel punten van oneindige orde, maar om te beslissen of er voor een gegeven kromme E over $\mathbb{Q}$ punten van niet-eindige orde zijn is een lastig probleem.
We zullen veel voorbeelden zien.

(3.1) Beschouw een abelse groep A. Dat wil zeggen dat A een groep is waar de groepswet commutatief is; zie § 7. We schrijven de groepswet als optelling. We zien dat $a + b = b + a$ voor all $a, b \in A$.

Voor een geheel getal n en $a \in A$ schrijven we na, of $n{\cdot}a$ voor $a{+}\cdots{+}a$ (met n summanden); bij voorbeeld $3a = a + a + a$, en $(-1){\cdot}a = -a$.

Voor een element $a \in A$ zeggen we dat de *orde* van a gelijk is aan n, als $n \in \mathbb{Z}_{>0}$, verder $na = 0$ en voor alle $1 \leq i < n$ geldt $ia \neq 0$; we zeggen dat de orde van a oneindig is als $ia \neq 0$ voor alle $i \in ZZ_{>0}$.

We zeggen dat $a \in A$ een torsie-element is als er een $n \in \mathbb{Z}_{>0}$ is met $na = 0$. Een torsie-element is een element van eindig orde. We schrijven $\mathrm{Tors}(A)$ voor de verzameling van torsie-elementen in A. Voor $n \in \mathbb{Z}_{>0}$ schrijven we

$$A[n] = \{a \mid na = 0\}.$$

Eigenschap. De deelverzamelingen $\mathrm{Tors}(A) \subset A$ en $A[n] \subset A$ zijn ondergroepen.
Bewijs. Als $a, b \in A[n]$ dan geldt $0 = (na) + (nb) = n(a + b)$, omdat A commutatief is, en ook $-a \in A$. Dit bewijst de tweede uitspraak. Omdat $\mathrm{Tors}(A)$ de vereniging is van alle $A[n]$ voor alle $n > 0$ volgt de eerste uitspraak.

Opmerking / waarschuwing. Voor een niet-abelse groep gelden bovenstaande uitspraken in het algemeen niet.

In deze paragraaf bestuderen we punten van eindige en van oneindige orde op elliptische krommen.

(3.2) Voorbeelden / eigenschappen.
(2) Heeft een elliptische kromme punten van orde gelijk aan 2? We zien:

$$2P = 0 \quad \Longleftrightarrow \quad P{*}P = 0;$$

geef een bewijs.

Hoe berekenen we $P{*}P$? We bepalen de raaklijn $\ell = \mathfrak{t}_{E,P}$ en bepalen het derde snijpunt: $\ell \cap E = \{P, P, P{*}P\}$. Het punt $0 \in E$ is gelegen op elke "verticale lijn". Als ℓ gegeven wordt door $\alpha x + \beta y + \gamma = 0$ dan is ℓ verticaal desda $\beta = 0$. Als E gegeven is door $f = 0$ en $P = (x, y)$ dan wordt $\mathfrak{t}_{E,P}$ gegeven door $f_X(P)(X - x) + f_Y(P)(Y - y)$; die lijn is verticaal desda $f_Y(P) = 0$. We hebben bewezen:

Conclusie: *Punten van orde twee zijn alle punten van de doorsnede*

$$E[2] = \mathcal{Z}(f_Y) \cap E \cup \{0\}.$$

Als E gegeven wordt door $Y^2 = X^3 + AX + B$ dan zijn de punten van orde precies twee de punten $(x, 0)$ met $x^3 + Ax + B = 0$.
Conclusie: $E(\mathbb{C})[2] \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$.

(3) Feit:

$$3P = 0 \quad \Longleftrightarrow \quad P \text{ is een buigpunt,}$$

$$P, Q \text{ zijn buigpunten} \Longrightarrow P{*}Q \text{ is een buigpunt.}$$

Geef een bewijs.

(3.3) Feit. *Er zijn 9 buigpunten op een elliptische kromme.* (We komen nog met een uitleg hiervan.)

(3.4) Opgave. Bewijs dat $p \in E$ een buigpunt is dan en slechts dan als $3P = 0$.

(3.5) Opgave. Bewijs dat de lijn door twee verschillende buigpunten op E deze kromme nog in een derde punt snijdt, en dat punt is ook een buigpunt.

We zien de curieuze, mooie configuratie van 9 punten in het vlak (één daarvan is gelegen "in het oneindige": op elke verticale lijn), en elke lijn die twee van deze punten verbindt gaat door nog precies een ander punt hiervan.

Merk op dat we over $\mathbb{C}$ werken. Over andere lichamen is dat anders in het algemeen. Probeer maar eens een dergelijke configuratie te "tekenen"; daarmee bedoelen we in het vlak $\mathbb{R} \times \mathbb{R}$. Dat lukt niet, zoals je al gauw opmerkt. inderdaad:

(3.6) Opgave. Zij $A, B \in \mathbb{R}$ en laat E over $\mathbb{R}$ gegeven zijn door $Y^2 = X^3 + AX + B$. Beschouw $E(\mathbb{R})[3]$, dat wil zeggen beschouw alle punten $P = (x, y) \in \mathbb{R}^2$ op die kromme met $sP = 0$, en het punt 0. Bewijs dat $E(\mathbb{R})[3]$ bestaat uit hooguit 3 elementen (bewezen kan worden dat het uit precies 3 elementen bestaat, en dat $E(\mathbb{R})[3] \cong \mathbb{Z}/3$).

(3.7) Punten van orde 3 op een elliptische kromme kunen als volgt gevonden worden. Zij $E = \mathcal{Z}(f)$. Beschouw het homogene polynoom verkregen uit f door bij alle termen factoren Z erbij te zetten tot de totale graad 3 is. Bij voorbeeld voor $f = -Y^2 + X^3 + AX + B$ krijgen we $g = -Y^2Z + X^3 + AXZ^2 + BZ^3$. Dan vormen we de Hessiaan:

$$\mathrm{Hes}(g) := \det \begin{pmatrix} f_{XX} & f_{XY} & f_{XZ} \\ f_{YX} & f_{YY} & f_{YZ} \\ f_{ZX} & f_{ZY} & f_{ZZ} \end{pmatrix};$$

dit heet *de Hessiaan* van g; we schrijven f_{XY} voor $(d/dY)((d/dX)(g))$, etc. Let wel, dit zijn "formele afgeleiden", in de zin dat $(d/dX)(HX^m) := mHX^{m-1}$, waar H niet de variabele X bevat.

Merk op: als g homogeen is van graad m, dan is $\mathrm{Hes}(g)$ homogeen van graad $3(m-2)$ of $\mathrm{Hes}(f) = 0$. In ons geval heeft de Hessiaan graad 3.

Voor een elliptische kromme E geldt dat de snijpunten van E met zijn Hessiaan precies alle buigpunten zijn.

(3.2)**(5)** *We geven een voorbeeld van een elliptische kromme met een* 5*-torsie punt.* Neem de elliptische kromme gegeven door $Y^2 + Y = X^3 - X^2$. We beginnen met het punt
$P_1 = P = (1, 0)$; we zien $\mathfrak{t}_{E,P} : X + Y + 1 = 0$; dus $P*P = P_2 = (0, -1)$.
We herhalen dit spel, steeds in het volgend punt de raaklijn, trekken, en derde snijpunt bepalen:
$P_2 = (0, -1)$, $\mathfrak{t} : Y + 1 = 0$, $P_2*P_2 = P_3 = (1, -1)$;
$P_3 = (1, -1)$, $\mathfrak{t} : X = Y$, $P_3*P_3 = P_4 = (0, 0)$;
$P_4 = (0, 0)$, $\mathfrak{t} : Y = 0$, $P_4*P_4 = P_1 = (1, 0)$.

We zien dat dit proces het uitgangspunt terug geeft. We leiden af:

$$P_1 = -P_3 = 2{\cdot}P_2 = -4{\cdot}P_1; \quad \text{conclusie: } 5P = 0.$$

We zien dat we een punt van orde 5 hebben. Merk op dat voor elk punt van oneven orde een dergelijk proces het uitgangspunt terug geeft (bewijs ?).

(3.8) Stelling. *Zij E een elliptische kromme over $\mathbb{C}$ en $n \in \mathbb{Z}_{>0}$. Dan geldt:*

$$E(\mathbb{C})[n] \quad \cong \quad (\mathbb{Z}/n)^2.$$

Ik ken geen elementair bewijs van deze stelling. In deze cursus ga ik er niet verder op in.

We kunnen wel een bewijs geven als we Stelling (2.3) aannemen. Uit die stelling volgt dat er een rooster

$$\Lambda = \Lambda_{\omega_1,\omega_2} \subset \mathbb{C}$$

is en een isomorfisme $\mathbb{C}/\Lambda \cong E(\mathbb{C})$. Dus volgt

$$E(\mathbb{C})[n] = \frac{1}{n}\Lambda/\Lambda \cong (\mathbb{Z}/n)^2 :$$

alle punten $z \in \mathbb{C}$ modulo Λ met de eigenschap dat $nz \in \Lambda$.

(3.9) Als we werken over $\mathbb{Q}$ dan is de situatie heel anders, want punten op E met coördinaten in $\mathbb{C}$ hoeven geen coördinaten in $\mathbb{Q}$ te hebben.
Stelling (Nagell en Lutz). *Zij E een elliptische kromme over $\mathbb{Q}$ gegeven door $Y^2 = X^3 + AX + B$ met $A, B \in \mathbb{Z}$. Zij $(x, y) = P \in \mathrm{Tors}(E(\mathbb{Q}))$. Dan geldt:*
$x, y \in \mathbb{Z}$ en
óf $y = 0$ (en P is een punt van orde 2),
óf $y \neq$ en dan geldt dat y^2 een deler is van $D = 4A^3 + 27B^2$.
Ook hiervan ken ik geen elementair bewijs. Voor het resultaat in de stelling is het essentieel dat we werken over $\mathbb{Q}$, en dat de vergelijking voor E is gegeven (merk op dat D afhangt van die vergelijking). De grote kracht van deze stelling is dat hiermee voor elke E over $\mathbb{Q}$ de groep $\mathrm{Tors}(E(\mathbb{Q}))$ effectief bepaald kan worden (effectief: zodra we de vergelijking kennen, weten we hoeveel reken tijd we nodig hebben); dit zien we b.v. in de volgende opgave.

(3.10) Opgave. (Hierin mag (3.9) gebruikt worden.) Bepaal $\mathrm{Tors}(E(\mathbb{Q}))$ waar E gegeven is door $Y^2 = X^3 - X$.

(3.11) Opgave. Laat E over $\mathbb{Q}$ gegeven zijn door $Y^2 = X^3 + 1$. Bepaal $\mathrm{Tors}(E(\mathbb{Q}))$.

(3.12) In [44] vinden we elliptische krommen met een niet-triviale torsie die in families bewegen.

(3.13) B. Mazur bewees een curieuze, prachtige stelling:
Voor een kromme E over $\mathbb{Q}$ geldt:

$$\textit{óf}\quad \mathrm{Tors}(E(\mathbb{Q}) \cong \mathbb{Z}/n \quad n = 1,2,3,9,10,12, \quad \textit{óf}\quad \mathrm{Tors}(E(\mathbb{Q}) \cong \mathbb{Z}/n, \quad 1 \le n \le 4.$$

Zie [49], of zie [41], Th. 1.7. Het bewijs van deze stelling is lastig.

We kunnen de Stelling van Nagell-Lutz, zie (3.9) ook gebruiken om te laten zien dat een punt niet een torsie-punt is.

(3.14) Voorbeeld. We geven E door $Y^2 = X^3 - 16X + 16$. We zien dat $(0,4)$ daar op ligt. We zien ook dat $(0,4)*(0,4) = (4,-4)$. En $(4,-4)*(4,-4) = (8,-20)$. Omdat in dit geval $D = 4{\cdot}(-16)^3 + 27{\cdot}16^2 = -16{\cdot}37$ zien we dat $(8,-20)$ niet een torsie-punt is (want 20^2 deelt niet D). Dus is $(0,4)$ niet een torsie-punt, alhoewel wel geldt dat 4^2 een deler is van D.

Alternatief bewijs: reken ook $8{\times}(0,4)$ uit, en laat zien dat de coördinaten van dat punt niet geheel zijn; daaruit volgt ook dat $(0,4) \notin \mathrm{Tors}(E)$.

(3.15) Opmerking. Geef E_2 door $V^2 + V = U^3 - U$. Pas de transformatie toe $4U = X$, $8V + 4 = Y$. Laat zien dat de vergelijking voor E_2 overgaat in de vergelijking voor E in (3.14), dat het punt $(u = 0, v = 0)$ overgaat in $(0,4)$. Berekeningen met E als in (3.14) kunnen we ook doen met E_2, maar om (3.9) toe te passen moeten we een vergelijking van de goede soort hebben, vandaar de situatie zoals in (3.14).

Dit geeft ook aan hoe we (3.9) toe kunnen passen: eerst transformeren we tot we de formule in de goede vorm hebben, en dan passen we "$y^2 \mid D$" toe.

(3.16) Voorbeeld. Geef E door $Y^2 = X^3 - X + 4$. We zien dat $P = (0,2) \in E(\mathbb{Q})$ en we vragen ons af of dit een torsie-punt is. Omdat $D = 4{\cdot}(-1)^3 + 27{\cdot}4^2$ deelbaar is door y^2 als $y = 2$ kunnen we (3.9) niet direct toepassen: we kunnen zó niet beslissen of P een torsie-punt is. We zoeken een andere methode.

We zien dat $\mathfrak{t}_{E,P}$ gegeven wordt door $-X - 4Y + 8 = 0$. Substitutie van $4Y = -X + 8$ in $-(4Y)^2 + 16(X^3 - X + 4)$ levert $16X^3 - X^2$. We zien dat $-2P = P*P = (1/16, 127/64)$. We concluderen met behulp van (3.9) dat $-2P$ niet eindige orde heeft. Dus heeft P ook niet eindige orde.
In [41], pag.77, Example 2 zien we de volgende berekening:
voor de kromme gegeven door $Y^2 + Y = X^3 - X$ en het punt $P := (0,0)$ krijgen we:
$2P = (1,0)$, $3P = (-1,-1)$, $4P = (2,-3)$, $5P = (1/4, -5/8)$,
$6P = (6,14)$, $7P = (-5/9, 8/27)$, $8P = (21/25, -69/125)$.

(3.17) Opgave. Geef E over $\mathbb{Q}$ door $Y^2 = X^3 + 17$. Laat zien dat $\mathrm{Tors}(E(\mathbb{Q})) = 0$. (Maar we zien wel punten: $(-1,4)$ en $(-2,3)$ liggen op die kromme, en misschien nog wel veel meer? zie (3.19).)

We hebben gezien dat voor punten die niet torsie zijn, veelvouden al heel gauw noemers krijgen in de coördinaten. Dat is inderdaad zo, en dat is precies te beschrijven: we gaan zien dat voor elk niet-torsie-punt een geheel veelvoud niet gehele coördinaten heeft.

(3.18) Stelling (Siegel, 1929). *We geven een elliptische kromme E door $Y^2 = X^3 + AX + B$ met $A, B \in \mathbb{Z}$. Dan is de verzameling van "gehele punten" eindig:*

$$\#\left(\{(x,y) \in \mathbb{Z}^2 \mid y^2 = x^3 + Ax + B\}\right) < \infty.$$

Een bewijs van bovenstaande stelling is lastig, ook in concrete gevallen. Hier is een beroemd voorbeeld dat mooi illustreert hoe grillig getal theorie kan zijn:

(3.19) Voorbeeld. Zij cE gegeven door $Y^2 = X^3 + 17$. Dan bestaat de verzameling van "gehele punten" zoals in bovenstaande stelling uit:

$$\{(-2, \pm 3), (-1, \pm 4), (2, \pm 5), (4, \pm 9), (8, \pm 23), (43, \pm 228), (52, \pm 375), (5234) \pm 378661\}.$$

Opmerkingen. Voor de elliptische kromme E gegeven over $\mathbb{Q}$ door $Y^2 = X^3 + 17$ geldt dat

$$E(\mathbb{Q}) =< (-2, 3), (2, 5) > \cong \mathbb{Z}^2,$$

een torsie-vrije groep van rang 2; zie [79], III.2, Exa. 2.4. Het is lastig om zulke resultaten te bewijzen.

Voor deze vergelijking is $D = 27 \cdot 17^2$. Uit de bovenstaande gegevens volgt dat alleen $(x, y) = (-2, \pm 3) \in E(\mathbb{Z})$ punten zijn is waar y^2 een deler is van D. Dat zijn geen torsiepunten. Dus volgt uit (3.9) dat $\mathrm{Tors}(E(\mathbb{Q})) = 0$.

(3.20) Stelling (Mordell, 1922). *Zij E een elliptische kromme over $\mathbb{Q}$. De groep $E(\mathbb{Q})$ is eindig voortgebracht.* Dat betekent dat er een eindig aantal punten $P_1, \cdots, P_m \in E(\mathbb{Q})$ is, zodanig dat voor elke $P \in E(\mathbb{Q})$ er bestaan $a_i \in \mathbb{Z}$ met $P = \sum_i \ a_i P_i$.
Gevolg. *Voor elke E over $\mathbb{Q}$ is er een $r_E = r \in ZZ_{\geq 0}$ en een isomorfisme*

$$E(\mathbb{Q}) \cong \mathrm{Tors}(E(\mathbb{Q})) \times \mathbb{Z}^r,$$

Het getal r wordt de rang van E genoemd.

(3.21) Opmerking. We hebben gezien dat voor gegeven het berekenen van $\mathrm{Tors}(E(\mathbb{Q}))$ effectief is (als we eenmaal de vergelijking van E weten, dan weten we D, en uit (3.9) zien we welke mogelijkheden er zijn voor de X-coördinaat van een torsiepunt). Echter we kennen geen effectief algoritme om r_E te berekenen.
Open probleem. Beschouw alle E over $\mathbb{Q}$. Is de verzameling $\{r_E\}$ begrensd?

Experimenten en berekeningen hebben al een vrij grote rang laten zien; zie [70]; de literatuur hierover is heel groot.

Het antwoord op deze vraag is niet bekend, en eigenlijk weten we niet wat we verwachten. Soms lijkt het dat we steeds grotere getallen vinden, dan weer geven overwegingen aan dat de rang best eens begrensd zou kunnen zijn. Een intrigerend, moeilijk probleem. Er is veel over geschreven, veel over nagedacht (en eigenlijk weten we niet waar we moeten beginnen). Berekeningen geven krommen met een hoge rang (elke keer gaat die grens weer omhoog; die berekeningen zijn slim en formidabel).

(3.22) We zullen in § 5 voor elke (kwadraatvrije) $N \in \mathbb{Z}_{>0}$ de elliptische kromme E_N gegeven door $Y^2 = X(X^2 - N^2)$ tegenkomen. We zien dat die kromme reeds over $\mathbb{Q}$ de volle 2-torsie heeft:

$$E_N(\mathbb{Q})[2] = \{(0, 0), (0, +n), (0, -n), 0\} \cong (\mathbb{Z}/2)^2 .$$

Het kan bewezen worden dat dit ook alle torsie is van $E_n(\mathbb{Q})$: er geldt $\mathrm{Tors}_N(E(\mathbb{Q})) = (\mathbb{Z}/2)^2$ voor elke kwadraatvrije N; zie [42], I.9, Prop. 17 op pag. 44 voor een bewijs, waar reductie modulo priemgetallen gebruikt wordt. Dit speelt een belangrijke rol bij het probleem van de congruente getallen. Het geval $N = 1$ zagen we al in (3.10).

(3.23) Opgave. (We bewijzen een speciaal geval van (5.14).) Zij p een priemgetal, en geef E_p door $Y^2 = X(X-p)(X+p)$ over $\mathbb{Q}$. Bewijs:

$$\mathrm{Tors}(E_p(\mathbb{Q})) \cong (\mathbb{Z}/2)^2.$$

(Desgewenst kan de stelling van Nagell-Lutz gebruikt worden.)

(3.24) Oplossing van (3.6). Beschouw alle punten in $P \in E(\mathbb{R})[3]$ en alle lijnen ℓ die twee van die punten verbinden. Als er meer dan 3 elementen zijn, dan kunnen we beschouwen alle paren (P, ℓ) met $P \notin \ell$ (een niet-lege verzameling) en daarin een paar dat minimale afstand van P tot ℓ heeft; leidt een tegenspraak af. (eenvoudige Euclidische meetkunde, teken een paatje).

(3.25) Oplossing van (3.11). Voor $A = 0$ en $B = 1$ zien we $D = 27$. Direct duidelijk: $E(\mathbb{Q})[2] = \{(-1, 0), 0\}$ (want $X^3 + 1 = (X-1)(X^2 + X - 1)$ en die tweede factor heeft geen nulpunt in $\mathbb{Q}$). Voor $(x, y) = P \in \mathrm{Tors}(E(\mathbb{Q}))$ met $y \neq 0$ geeft de stelling dat y^2 een deler is van 27; dus $y \in \{-3, -1, 1, 3\}$; dus $y = \pm 1$ en $x = 0$; we zien dat de lijn gegeven door $Y = 1$ de kromme drievoudig snijdt; dus is $(0, \pm 1)$ een buigpunt. Conclusie:

$$\mathrm{Tors}(E(\mathbb{Q})) = (\mathbb{Z}/2) \times (\mathbb{Z}/3) \cong \mathbb{Z}/6.$$

(3.26) Een aanwijzing voor (3.17). Probeer alle y met $y^2 \mid 27 \cdot 17^2$. We vinden $P = (-2, \pm 3)$ als enige punten die een torsie-punt zouden kunnen zijn. Pas verdubbeling toe, tot er een punt komt met niet-gehele coördinaten, of een punt waarvan de y-coördinaat niet voldoet aan (3.9).

4 Pythagoreïsche drietallen

(4.1) Vaak bestuderen we vergelijkingen van de vorm $X^n+Y^n = Z^n$ en oplossingen daarvan in de gehele getallen.

Het vermoeden van Fermat, we komen daar nog op terug, zegt dat zulke oplossingen $(z, y, x) \in \mathbb{Z}^3$ voor $n \geq 3$ alleen maar bestaan met $xyz = 0$ (dat worden wel de "triviale oplossingen" genoemd). We zullen later nog uitvoerig ingaan op de vraag waar die conditie "$n \geq 3$" vandaan komt.

In deze paragraaf houden we ons bezig met het gevel $n = 2$: de classificatie van alle "Pythagoreïsch drietallen". Deze theorie zal uitvoerig gebruikt worden in de paragraaf § 5 over congruente getallen.

We zullen zien dat er dan oneindig veel oplossingen bestaan, en we zullen ze allemaal classificeren. We zullen een dergelijk drietal $(z, y, x) \in \mathbb{Z}^3$, een oplossing van $X^2 + Y^2 = Z^2$, een Pythagoreïsch drietal noemen.

Hier begint eigenlijk de geschiedenis van een mooi onderwerp. Op een oud Babylonisch klei-tablet gedateerd tussen 1800 en 1650 vóór Christus zijn een aantal van dergelijke oplossingen vermeld; zie het klei-tablet Plimpton 322, [59], [30]. Het is aannemelijk dat zulke drietallen en rol speelden in oude beschavingen.

Soms wordt vermeld dat het drietal $(3, 4, 5)$ gebruikt werd om rechte hoeken te construeren bij het bouwen van de Egyptische piramides. Ik ken geen historische of archeologische gegevens om deze veronderstelling te onderbouwen.

Uit de stelling van Pythagoras volgt dat (x, y, z) een dergelijk drietal is, deze getallen kunnen optreden als lengtes van een rechthoekige driehoek; vandaar de naamgeving.

De classificatie van alle Pythagoreïsche driehoeken is een van de oudste stellingen van de wiskunde. Euclides beschreef dit in zijn "Elementen", Boek X, Propositie 28a, ongeveer 23 eeuwen geleden.

(4.2) Definitie: Pythagoreïsche drietallen. Een drietal positieve gehele getallen $(x, y, z) \in (\mathbb{Z}_{>0})^3$ heet een *Pythagoreïsch drietal* als $x^2 + y^2 = z^2$. We zullen dit begrip aangeven met PD.
Primitief PD. We zeggen dat een PD (x, y, z) *primitief* is als $\text{ggd}(x, y) = 1$. Afkorting: pPD.

Merk op: als $\text{ggd}(x, y) = 1$ en $x^2 + y^2 = z^2$ dan volgt ook $\text{ggd}(y, z) = 1$ en $\text{ggd}(z, x) = 1$, ga na!
We schrijven ggd voor de *grootste gemene deler* van een tweetal positieve gehele getallen; zie (9.5) voor een definitie van dit begrip.

Enkele voorbeelden: $(3, 4, 5)$, $(6, 8, 10)$, $(5, 12, 13)$, $(9, 40, 41)$ zijn PDen. Het tweede voorbeeld is niet primitief, de andere wel.

(4.3) Opmerking/Opgave Voor elke $B \in \mathbb{Z}_{\geq 1}$ is $(B + 1) - B^2$ een oneven getal, en alle oneven getallen ≥ 3 komen op deze manier voor: $4 - 1 = 3$, $9 - 4 = 5$, $\cdots$. Merk op dat voor elke $A \in \mathbb{Z}_{\geq 1}$ het kwadraat $(2A + 1)^2$ oneven is. Kies $(B + 1) - B^2 = (2A + 1)^2$. Zie [82], pag. 341.

$\boxed{\text{FLT}_2}$ **Opgave.** Gebruik deze opmerkingen om te bewijzen dat er oneindig veel pPD bestaan. Zie (4.27).

We geven een stelling die alle PDen classificeert. We zullen drie verschillende bewijzen geven van de stelling die deze classificatie geeft.

(4.4) Lemma. *Als (x, y, z) een primitief* PD *is, dan is z oneven, en van x en y is er precies één even, en één oneven.*
Bewijs. Als een geheel getal $u \in \mathbb{Z}$ even is, dan is u^2 deelbaar door 4. Als u oneven is dan geldt $u^2 \equiv 1 \pmod 4$; d.w.z. u^2 kan geschreven worden als $u^2 = q{\cdot}4 + 1$; inderdaad, als $u = 2k + 1$ dan is $u^2 = 4k^2 + 4k + 1 = (k^2 + k){\cdot}4 + 1$.

Als x en y beide even zouden zijn, dan is het drietal niet primitief. Als x en y beide oneven zouden zijn dan geldt $x^2 + y^2 \equiv 2 \pmod 4$; dus is $x^2 + y^2$ niet een kwadraat in dit geval. Blijft over: van x en y is er precies één even, en één oneven; in dat geval is z oneven. QED

Afspraak: Als (x, y, z) een pPD is, dan nemen we aan dat x oneven is en y even (zo niet, dan verwisselen we x en y).

Merk op:

$$(m^2 - n^2)^2 \quad + (2m{\cdot}n)^2 \quad = \quad (m^2 + n^2)^2.$$

Voor elke keuze van $m, n \in \mathbb{Z}$ met $m > n > 0$ krijgen we op deze manier een PD. We laten zien dat dit ze allemaal zijn:

(4.5) Stelling. *Als (x, y, z) een primitief* PD *is met x oneven, dan zijn er getallen $m, n \in \mathbb{Z}_{>0}$ met $m > n$, en $\gcd(m, n) = 1$ en $m + n$ oneven zodat*

$$x = m^2 - n^2, \quad y = 2m{\cdot}n, \quad z = m^2 + n^2.$$

We zien dat de stelling alle primitieve PDen geeft; hieruit kunnen alle Pythagoreïsche drietallen bepaald worden.
Kijk naar deze tabel, bij voorbeeld naar de laatste kolom; is er iets dat opvalt aan deze getallen?
Welke priemgetallen treden op als delers van z?
Komt een waarde voor z meerdere malen voor in deze tabel?

Voor we aan een bewijs beginnen gaan we eerst een fundamenteel hulpmiddel invoeren: de *eenduidigheid van factorizatie* in $\mathbb{Z}$.

Merk op dat als voor gehele getallen $d, e \in \mathbb{Z}$ geldt $d{\cdot}e = 1$ dan is óf $e = +1$ óf $e = -1$. We zullen $+1$ en -1 de eenheden van $\mathbb{Z}$ noemen. We zeggen dat een geheel getal $p > 1$ een priemgetal is als elke getal d met $1 < d < p$ niet een deler is van p. M.a.w. de enige positieve delers van een priemgetal p zijn 1 en p zelf. Als we schrijven $n = \pm p_1 \times \cdots \times p_s$, waar $p_1, \cdots, p_s$ priemgetallen zijn, dan spreken we van een (priem)factorizatie van het gehele getal n.

(4.6) 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.

Voor het ontbinden van gehele getallen in priemfactoren, en de uniciteit van een dergelijke factorizatie, op volgorde van de factoren na, zie (9.3)

Iedereen die denkt dat we wel al te zorgvuldig bezig zijn, wordt aangeraden de voorbeelden (4.14), (4.33), en (4.36) door te nemen. Daar zien we dat eenduidigheid in andere getalsystemen niet hoeft op te gaan. We zien de subtiliteiten die een grote rol speelden in eerdere, goede en foute bewijzen van FLT.

(4.7) Opmerking. *Als* $m, n \in \mathbb{Z}_{>0}$ *met* $m > n$, *en* $\text{ggd}(m, n) = 1$ *en* $m + n$ *oneven dan is* $(m^2 - n^2, 2mn, m^2 + n^2)$ *primitief.*
Bewijs. Uit "$m + n$ is oneven" volgt dat $m^2 - n^2 = (m + n)(m - n)$ oneven is; dus is 2 niet een gemeenschappelijk factor van $m^2 - n^2$ en $2mn$. Stel $p > 2$ is een priemdeler van $m^2 - n^2$ en van $2mn$; dan is het ook een deler van $m^2 + n^2$; dan is het ook een priemdeler van m^2, dus van m, ook een priemdeler van n^2 dus van n, tegenspraak. QED

(4.8) Bewijs I van (4.5)**: Elementaire getaltheorie.**
Zie bv. zie bv. [37], Chapter XIII.
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 $\mathrm{ggd}(m,n) = 1$, en dat $m+n$ oneven is. Conclusie:

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

Dit is het eerste bewijs van de stelling (4.5).

Schrijf alle stappen zorgvuldig uit.

(4.9) Bewijs II van (4.5)**: Meetkunde.**
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.

QEDStelling (4.5)

Opmerking: via de meetkunde zien we direct dat er oneindig veel PD zijn (want er zijn oneindig veel t met $t \in \mathbb{Q}$ en $0 < t < 1$. Het bewijs zou gegeven kunnen worden met de formules hierboven zonder meetkundige motivatie of achtergrond.

Zoals zo vaak: de meetkunde suggereert een prachtig algebraïsch bewijs.

(4.10) Bewijs III van (4.5)**: Algebraïsche getaltheorie.***

We geven een bewijs, waarin we methoden gebruiken die niet helemaal elementair zijn. In dit bewijs gebruiken we enkele begrippen uit de algebra. We merken eerst op dat $a^2 + b^2 = c^2$ in $\mathbb{C}$ gefactoriseerd kan worden als:

$$(a + b{\cdot}\sqrt{-1})(a - b{\cdot}\sqrt{-1}) = c^2.$$

We gaan nu eigenschappen onderzoeken van getallen zoals die aan de linkerkant voorkomen.

(4.11) We zulen het begrip "ring" gebruiken. Een voorbeeld daarvan is $\mathbb{Z}$. In en ring is er een element 0, een element 1, een commutatieve optelling en een vermenigvuldiging (die in alle voorbeelden die we gebruiken ook commutatief zal zijn). Voor deze operaties gelden gebruikelijke axioma's, zoals $(a + b) + c = a + (b + c)$, en $a(b + c) = ab + ac$, en $a + 0 = a$ en $b{\cdot}1 = b$ etc. Merk op dat in het algemeen er niet van elk element een inverse in $\mathbb{Z}$ bestaat. De verzameling $\mathbb{Q}$ van rationale getallen is ook een voorbeeld van een ring; daarin geldt dat elk element ongelijk aan nul een inverse heeft (en een dergelijk systeem heet een lichaam).

(4.12) De gehele getallen van Gauss.* Beschouw:

$$R = \mathbb{Z}[\sqrt{-1}] := \{x + y{\cdot}i \mid x, y \in \mathbb{Z}\},$$

waar het symbool i gebruikt wordt als $i = \sqrt{-1}$. In deze verzameling kunnen we optellen, aftrekken en vermenigvuldigen, waar de regel $i^2 = -1$ gebruikt wordt. Het getal $0 = 0 + 0{\cdot}i$ treedt als "nul" op, en het getal $1 = 1 + 0{\cdot}i$ treedt als "een" op. Met deze operaties is dit een ring, die wel de "*Ring van gehele getallen van Gauss*" genoemd wordt. Deling is niet in alle gevallen mogelijk, b.v. is $i/2$ niet een element van $R = \mathbb{Z}[\sqrt{-1}]$. We bepalen eerst de elementen die wel een inverse hebben in deze ring: de verzameling $\{1, +i, -1, -i\}$ is de verzameling van de "eenheden", d.w.z. de elementen die een inverse hebben. Hoe bewijzen we zoiets? Neem

$$N : R = \mathbb{Z}[\sqrt{-1}] \longrightarrow \mathbb{Z}, \quad N(x + y{\cdot}i) := x^2 + y^2,$$

de "norm-afbeelding". Het is duidelijk dat deze verwisselt met $\times$. Als $u, z \in R$ met $u{\cdot}z = 1$ dan geldt $N(u){\cdot}N(z) = 1$. Ga na:

$$N(z) = 1 \quad \Longleftrightarrow \quad z \in \{1, +i, -1, -i\}.$$

We zeggen dat een element $z \in R$ *irreducibel* is, als z niet een eenheid is, en als $z = u{\cdot}v$ impliceert dat óf u óf v een eenheid is. Enkele voorbeelden: $1 + i$ is irreducibel, alhoewel $1 + i = i{\cdot}(1 - i)$. We zien dat $13 = (2 + 3i)(2 - 3i)$, en concludeer dat $13 \in R$ niet irreducibel in R is. Is $7 \in R$ irreducibel? Is $1 - 5i \in R$ irreducibel?

(4.13) De getallen -3 en $+3$ zijn irreducibel in $\mathbb{Z}$; we hebben de gewoonte aangenomen om alleen positieve irreducibele elementen in $\mathbb{Z}$ priemgetallen te noemen. Merk op dat $1 \in \mathbb{Z}$ niet een priemgetal is, niet irreducibel is (vroeger, ten tijde van Euler deed men dat wel). Een waarschuwing; beschouw $5 \in \mathbb{Z} \subset \mathbb{Z}[\sqrt{-1}] \subset \mathbb{C}$; we zien: 5 is irreducibel in $\mathbb{Z}$, reducibel in $\mathbb{Z}[\sqrt{-1}]$ en een eenheid in $\mathbb{C}$.

We gaan irreducibele elementen in R zoeken. Maar eerst een

(4.14) Waarschuwing. We zijn zo gewend dat "ontbinding in irreducibele factorenëenduidig is op eenheden en volgorde na. In $\mathbb{Z}$ geldt dat op $\pm$ na: $6 = 2{\cdot}3 = (-2){\cdot}(-3)$. In het algemeen geldt die eenduidigheid in een willekeurige ring niet. Hier is een voorbeeld: neem de ring

$$T := \mathbb{Z}[\sqrt{-5}] = \{x + y{\cdot}\alpha \mid x, y \in \mathbb{Z}\},$$

met $\alpha^2 = -5$, bij voorbeeld als deelverzameling van $\mathbb{C}$ beschouwd. Merk op dat in T geldt:

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

Het is gemakkelijk in te zien dat de factoren $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5}) \in T$ irreducibel zijn. Ook zien we dat $+1, -1 \in T$ de eenheden zijn. Hier zien we dat er niet sprake is van eenduidige factor ontbinding in déze ring T.

(4.15) Feit. * *Neem de ring $R = \mathbb{Z}[\sqrt{-1}]$ van gehele getallen van Gauss. In deze ring geldt de eenduidigheid van ontbinding in irreducibele factoren op eenheden na, de eenheden zijn:*

$$\{1, +i, -1, -i\}.$$

De irreducibele elementen van deze ring zijn:

2: *Het element* $1+i \in \mathbb{Z}[i]$ *is een irreducibel element.*
N.B. merk op: $2 = -i \cdot (1+i)^2$.

3 mod 4**:** *Als* $p \in \mathbb{Z}$ *een priemgetal is met* $p \equiv 3 \pmod 4$ *dan is* p *irreducibel in* $\mathbb{Z}[i]$.

1 mod 4**:** *Als* $p \in \mathbb{Z}$ *een priemgetal is met* $p \equiv 1 \pmod 4$ *dan zijn er* $x, y \in \mathbb{Z}$ *met* $x^2+y^2 = p$, *dan is* $(x+yi)(x-yi) = p$, *en* p *is reducibel in* $\mathbb{Z}[i]$.
Als $x, y \in \mathbb{Z}$ *met* $x^2+y^2 = p$, *waar* p *een priemgetal is in* $\mathbb{Z}$ *met* $p > 2$,
dan is met $p \equiv 1 \pmod 4$ *en* $x+yi$ *is irreducibel in* $\mathbb{Z}[i]$.

Het feit dat $\mathbb{Z}[i]$ een ontbindingsring is, is in bijna elk boek over algebra te vinden, zie bv. [68], pag. 297.

(4.16) Als in een ring eenduidigheid van factor ontbinding heerst, dan wordt een irreducibel element ook wel een priem element genoemd. Maar wees voorzichtig, $13 \in \mathbb{Z}$ is een priemgetal, 13 is een irreducibel element van $\mathbb{Z}$, maar is niet een irreducibel element van $R = \mathbb{Z}[\sqrt{-1}]$.

(4.17) Het feit dat een oneven priemgetal p met $p \equiv 1 \pmod 4$ te schrijven is als som van 2 kwadraten (en dan ook reducibel is in $\mathbb{Z}[\sqrt{-1}]$) werd door Fermat bewezen. Euler was de eerste die een bewijs ervan publiceerde. Er zijn allerlei bewijzen van deze stelling, zie bv. [78], Section 47; [10], 12.2; [37], 20.2 en 20.3.

(4.18) Opmerking. Probeer maar eens "statistiek" te bedrijven, neem een grens (bv $n_0 = 200$) en tel het aantal priemgetallen $p < n_0$ die 1 mod 4 zijn, en die 3 mod 4 zijn. Het valt al gauw op dat ruwweg de helft in de eerste en ruwweg de helft in de tweede categorie valt. Inderdaad, dat is een stelling: voor $n_0 \to$ bestaan die fracties, en ze zijn beide gelijk aan 1/2, namelijk

$$lim_{n_0 \to \infty} \ \frac{\#\{p < n_0 \mid p \ \text{ is priem}, \ p \equiv 1 \pmod 4\}}{\#\{p < n_0 \mid p \ \text{ is priem}\}} = \frac{1}{2}.$$

Dit is niet elementair.

(4.19) We nemen aan dat het bovengenoemde feit (4.15) bewezen is, en we geven het derde bewijs van (4.5).
We laten eerst zien:

Als (x, y, z) *een primitief PD is,*
en p *is een priemgetal dat* z *deelt, dan geldt:* $p \equiv 1 \pmod 4$.

We hebben al gezien dat voor een pPD de bijbehorende z oneven is, dus 2 is niet een deler van z. Veronderstel dat $p \equiv 3 \pmod 4$ een deler is van z. In R weten we dat die $p \in R$ irreducibel is, en we hebben de factorizatie

$$(x + y \cdot i)(x - y \cdot i) = z^2.$$

Merk op dat daaruit volgt dat deze p een deler is van $x + y \cdot i$ (en ook van $x - y \cdot i$). Hieruit concluderen we dat p een deler is van x en van y (ga na), tegenspraak met het feit dat (x, y, z) een primitieve PD is. We concluderen dat *alleen priemgetallen met* $p \equiv 1 \pmod 4$ *kunnen optreden als priem delers van* z in en pPD. [Was dat al opgevallen aan de tabel?]

Zij p een priemgetal met $p \equiv 1 \pmod 4$. Dan bestaan er $a, b \in \mathbb{Z}$ zodanig dat

$$(a + b{\cdot}i)(a - b{\cdot}i) = p \quad \text{in} \quad R = \mathbb{Z}[i];$$

dat volgt uit het bovengenoemde feit; deze ontbinding is eenduidig op eenheden in R na, dat betekent dat de getallen x, y eenduidig zijn op teken en op volgorde na. Bij voorbeeld: $i{\cdot}(a + bi) = -b + ai$.

Stel (x, y, z) is een pPD, en laat

$$z = \prod_j \; p_j$$

een ontbinding in priemgetallen in $\mathbb{Z}$ zijn (een priemgetal kan meerdere malen voorkomen), en schrijf

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

Als p een priemgetal is dat z deelt, dan is $p \equiv 1 \pmod 4$, en we kunnen schrijven $p = (a + bi)(a - bi)$; deze beide factoren zijn onderling ondeelbaar in $\mathbb{Z}[i]$, en precies één ervan is een deler van $(x + y{\cdot}i)$ en de andere is een deler van $(x - y{\cdot}i)$. Door het kiezen van de goede tekens en de goede volgorde kunnen we schrijven

$$p_j \quad = \quad (a_j + b_j{\cdot}i)(a_j - b_j{\cdot}i), \quad a_j, b_j \in \mathbb{Z}$$

zo dat:

$$(x + y{\cdot}i) = \prod_j \; (a_j + b_j{\cdot}i)^2,$$

en

$$(x - y{\cdot}i) = \prod_j \; (a_j - b_j{\cdot}i)^2.$$

Uitvermenigvuldigen geeft een keuze voor m en n:

$$\prod_j \; (a_j + b_j{\cdot}i) =: m + n{\cdot}i.$$

Uit

$$(x + y{\cdot}i) = (m + n{\cdot}i)^2 = (m^2 - n^2) + 2mni$$

volgt wat we willen bewijzen. QED(4.5)

(4.20) Omgekeerd kunnen we PDen construeren met behulp van de gehele getallen van Gauss. Kies priemgetallen p_j, met $1 \leq j \leq t$, die alle $p \equiv 1 \pmod 4$ zijn. Schrijf elk van deze als $p_j \quad = \quad (a_j + b_j{\cdot}i)(a_j - b_j{\cdot}i)$, maar kies de tekens zo dat bij gelijke priemgetallen deze tekens gelijk zijn. We definiëren dan x en y met behulp van $(x + y{\cdot}i) = \prod_{j=1}^{t} \; (a_j + b_j{\cdot}i)^2$, en we krijgen een pPD. Op deze manier worden alle primitieve PD geconstrueerd. Hiermede eindigt het derde bewijs van Stelling (4.5).

(4.21) Enkele voorbeelden: Neem $z = 65 = 5 \times 13$. De factorizatie

$$65 = \{(1 - 2i)(2 + 3i)\} \; \times \; \{(1 + 2i)(2 - 3i)\} = (8 + i)(8 - i)$$

geeft $(8 + i)^2 = 63 + 16{\cdot}i$, en dit geeft

$$63^2 + 16^2 = 95^2.$$

De factorizatie

$$65 = \{(1 - 2i)(-2 + 3i)\} \; \times \; \{(1 + 2i)(-2 - 3i)\} = (4 + 7i)(4 - 7i),$$

en dit geeft

$$33^2 + 56^2 = 65^2.$$

(4.22) We zien dat $z = 25 = 5 \times 5$ alleen maar voorkomt als

$$25 = \{(1+2i)^2\} \times \{(1-2i)^2\}$$

en dit geeft

$$7^2 + 24^2 = 25^2.$$

Weliswaar heeft 25 twee priemfactoren, maar het verdelen van de factoren $(1 \pm 2i)$ kan maar op een manier gebeuren willen we een pPD krijgen.

(4.23) Neem $z = 1885 = 5 \times 13 \times 29$. Laat zien dat de factorizatie

$$(1-2i)(2+3i)(5+2i) = -34 + 27i$$

aanleiding geeft tot

$$27^2 + 34^2 = c,$$

de getallen $m = 34$ en $n = 27$ geven

$$427^2 + 1836^2 = 1885^2.$$

Andere verdelingen laten zien dat deze $z = 1885$ meerdere malen optreedt in een pPD, en wel precies vier keer.

(4.24) Voorbeeld. Neem $z = 29^3$. Uit het bewijs weten we dat dit voorkomt in een PD. Hoe vinden we x en y? Merk op dat $29 = 5^2 + 2^2 = (5+2i)(5-2i)$. We berekenen:

$$(5+2i)^3 = 125 + 3{\cdot}25{\cdot}2{\cdot}i + 3.{\cdot}5{\cdot}4i^2 + 8{\cdot}i^3 = 142 + 65i.$$

We zien:

$$65^2 + 142^2 = 29^3; \qquad (x = 142^2 - 65^2 = 15939, \quad y = 2{\cdot}142{\cdot}65 = 18460, \quad 29^3 = 24389)$$

is een PD.

(4.25) Opgave: Zij $z \in \mathbb{Z}$ een product van priemgetallen die alle $\equiv 1 \pmod 4$ zijn. Onderstel dat er t onderling verschillende priemfactoren in z zijn (een priemfactor kan meerdere keren optreden, maar telt in deze telling maar voor één). Dan komt z precies 2^{t-1} keer voor in de lijst van primitieve PDen.

Recreatie: zie [5], Chapter XIV.

(4.26) Opmerking. Waarom geven we verschillende bewijzen? Allereerst is het instructief om te zien dat dit probleem zich niet in een vakje laat duwen: we kunnen het op veel verschillende manieren benaderen. Gauss gaf in zijn leven 8 verschillende bewijzen van één stelling; we zijn in goed gezelschap.

Maar ook: we zouden kunnen proberen FLT elementair te bewijzen. We hebben hier heel verschillende benaderingen van het geval $n = 2$ gezien. Kan een van deze methoden gegeneraliseerd worden naar $n \geq 3$? Dat loopt vast in de eerste twee bewijzen (om heel verschillende redenen). Het derde bewijs was een bron van inspiratie voor goede en foute bewijzen, zie (4.36). Verder: het meetkundige (tweede) bewijs geeft inzicht, waarmee we zullen "verklaren" waarom $\mathrm{FLT}_{n=2}$ wel oplossing heeft, en het aannemelijk is dat $\mathrm{FLT}_{n\geq 3}$ slechts eindig veel primitieve oplossingen heeft (inderdaad, dat volgt uit een diepe stelling van Faltings), zodat er enige kans is dat dit een stelling wordt....en we hebben een "verklaring"gevonden voor de voorwaarde $n \geq 3$.

(4.27) **Oplossing** van Opgave (4.3). Voor elke $A \in \mathbb{Z}_{\geq 1}$ en $B := 2A(A+1)$ geldt

$$(2B+1) + B^2 = (B+1)^2, \quad 2B+1 = (2A+1)^2; \quad \text{dus is } (B, 2A+1, B+1) \quad \text{een PD.}$$

Allicht: $\text{ggd}(B, B+1) = 1$. Dit bewijst het bestaan van oneindig veel pPDen. We zien dat er oneindig veel primitieve oplossingen van $X^2 + Y^2 = Z^2$ bestaan.

Zijn we nu tevreden en kunnen we de rest na (4.3) van de paragraaf overslaan? Nee, een wiskundige probeert een classificatie van álle oplossingen te geven. Zoals we zullen zien, zal ons dat later goed van pas komen.

Opmerking. We zien dat de keuze $m := A+1, \quad n = A$ geeft $x = m^2 - n^2 = 2A+1$, en $y = 2mn = 2A(A+1) = B$, en $m^2 + n^2 = B+1$. Dit geeft deze pPDen een plaats in de classificatie zoals gegeven in Stelling (4.5). We zien dat we lang niet all oplossingen kregen.

we besluiten deze paragraaf met een bespiegeling over het Fermat probleem, of te wel "De Laatste Stelling van Fermat", afgekort door FLT = Fermat's Last Theorem. Dit onderwerp zal maar terzijde besproken worden in de cursus. Maar ik kan me voorstellen dat U deze extra informatie prettig vindt.

We hebben gezien dat de vergelijking $X^2 + Y^2 = Z^2$ veel oplossingen heeft met $(x, y, z) \in \mathbb{Z}^3$.

FLT_n : kies $n \in \mathbb{Z}_{>2}$ dan geldt:

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

Met andere woorden: een oplossing in gehele getallen is alleen maar mogelijk als tenminste één van die getallen gelijk is aan nul ("triviale oplossingen"). Deze stelling werd "bewezen" door Fermat. We hebben 350 jaar naar een bewijs gezocht, er werden veel deel resultaten gevonden. Tenslotte is het Andrew Wiles gelukt een compleet en sluitend bewijs voor het algemene geval te vinden, zie [96] (een fascinerende geschiednis). Hier geven we wat details over de eerste bewijzen van speciale gevallen, en een speculatie wat het bewijs van Fermat geweest zou kunnen zijn.

Hier bewijzen we FLT voor $n = 4$ zoals Fermat dat deed, en we bewijzen FLT voor $n = 3$ zoals Euler dat deed. Voor $n = 4$ gebruiken we de eenduidigheid van factor ontbinding in $\mathbb{Z}$, zie (9.3), en we gebruiken de classificatie en constructie van Pythagoreïsche drietallen, zie (4.5). In beide gevallen gebruiken we een methode die afkomstig is van Fermat: "de oneindige afdaling".

(4.28) **Stelling** (Fermat). *Als $x, y, w \in \mathbb{Z}$ met $x^4 + y^4 = w^2$ dan is $xyw = 0$.*
Bij voorbeeld, zie [41], III.d, of [78], Th. 62 on page 144.

(4.29) **Gevolg** (Fermat). FLT_4 *is juist, dat wil zeggen:*

$$x, y, z \in \mathbb{Z}, \quad x^4 + y^4 = z^4 \quad \Longrightarrow \quad xyz = 0.$$

Bewijs van (4.28). Als er een oplossing (x, y, w) is dan is $(\pm x, \pm y, \pm z)$ ook een oplossing; we kunnen daarom veronderstellen dat $x \geq 0$ en $y \geq 0$ en $w \geq 0$. Onderstel dat er een oplossing bestaat met $x > 0$ en $y > 0$ en $w > 0$ (en we komen tot een tegenspraak; een "bewijs uit het ongerijmde"). We nemen zo'n oplossing waar de w *minimaal* is in de verzameling van dergelijke oplossingen. Dan geldt dat de grootste gemene deler van x en y gelijk aan 1 is.

Bovendien kunnen we veronderstellen dat x oneven is en y even (anders verwisselen we deze twee). Gebruikmakend van (4.5) zien we dat er gehele getallen $m > n > 0$ bestaan zodanig dat:

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

zodanig dat $\text{ggd}(m, n) = 1$, en $m + n$ oneven. We zien dat (x, n, m) een pPD is. Dus bestaan er $a > b > 0$ met $\text{ggd}(a, b)$ zodanig dat

$$x = a^2 - b^2, \quad n = 2ab, \quad m = a^2 + b^2.$$

Dan geldt:

$$\left(\frac{y}{2}\right) \quad = \quad ab(a^2 + b^2);$$

ga na: $\text{ggd}(a, a^2 + b^2) = 1$ en $\text{ggd}(b, a^2 + b^2) = 1$. Uit de eenduidigheid van priemfactor ontbinding, zie (9.3), volgt dat er bestaan $s > 0$ en $t > 0$ en $u > 0$ met $a = s^2$, en $b = t^2$ en $a^2 + b^2 = u^2$. Hieruit volgt

$$s^4 + t^4 = u^2; \quad \text{bovendien:} \quad u \leq a^2 + b^2 = m < w.$$

Uitgaande van de "minimale" (x, y, w) vinden we een nieuwe oplossing (s, t, u) met $0 < u < w$. Dit is een tegenspraak. QED(4.28)
Allicht: (4.28)$\Longrightarrow$(4.29) QED(4.29)

We beginnen met een bewijs van $\text{FLT}_{n=3}$. Het is een mooi bewijs. De reden waarom ik dit geef is dat we vol ontzag beseffen hoe goed Euler was, de eerste die dit bewees, maar ook omdat dit een prelude was in de geschiedenis op veel foute bewijzen, maar ook op een correct bewijs van Kummer, waardoor veel gevallen van FLT_n bewezen konden worden.

Advies. De rest van dit hoofdstuk bevat onderwerpen die technisch wat lastiger zijn. U kunt de rest van dit hoofdstuk in eerste lezing overslaan. We laten zien wat een deel van de historische ontwikkeling geweest is (hoofdzakelijk 19-de eeuw), en we formuleren een *speculatie*, zie (4.36), die volgens mij uitlegt wat Fermat mogelijk als bewijs van FLT dacht te hebben.

(4.30) Factor ontbinding.* We beschouwen nu factor ontbinding in een wat algemenere context. Schrijf $\zeta = \zeta_6$ voor het complexe getal

$$\zeta := (1 + \sqrt{-3})/2. \quad \text{Merk op:} \quad \zeta^2 = \zeta - 1, \quad \zeta^6 = 1.$$

Schrijf

$$\mathcal{O} = \mathbb{Z}[\zeta] = \{z = a + b\zeta \mid a, b \in \mathbb{Z}\},$$

dat wil zeggen, $\mathcal{O}$ is de verzameling van complexe getallen van de vorm $z = a + b(-1 + \sqrt{-3})/2$ met $a, b \in \mathbb{Z}$. Merk op: $0 \in \mathcal{O}$, $\quad 1 \in \mathcal{O}$; als $z_1, z_2 \in \mathcal{O}$ dan $z_1 + z_2 \in \mathcal{O}$ en $z_1 - z_2 \in \mathcal{O}$ en $z_1 z_2 \in \mathcal{O}$. Een verzameling met dergelijke operaties $+$ en $\times$ waar aan de gebruikelijke axioma's is voldaan noemen we een *ring*; de optelling $+$ wordt commutatief verondersteld, d.w.z. $z_1 + z_2 = z_2 + z_1$. Als zoals in dit geval ook de vermenigvuldiging $\times$ commutatief is (zoals hier het geval is), dan spreken we van een *commutatieve ring*.

We noemen $e \in \mathcal{O}$ een *eenheid* als er een $e' \in \mathcal{O}$ bestaat met $ee' = 1$. De verzameling van eenheden van $\mathcal{O}$ noteren we als $\mathcal{O}^*$. Merk op dat het element $\zeta = (+1 + \sqrt{-3})/2$ een eenheid is; inderdaad: $\zeta^3 = -1$, en $\zeta^6 = 1$ (ga na). Merk op dat $\zeta^2 = \zeta - 1$; we zien dat $\omega := -1 + \zeta$ ook een eenheid is. Het helpt om elementen van $\mathcal{O}$ in het complexe vlak te tekenen.

We zeggen dat $z \in \mathcal{O}$ een irreducibel element is als z niet een eenheid is, en als een factortontbinding $z = rs$ impliceert $r \in \mathcal{O}^*$ of $s \in \mathcal{O}^*$.

(4.31) Propositie. *In de ring* $\mathcal{O} = \mathbb{Z}[(+1+\sqrt{-3})/2]$ *zoals hierboven gedefiniëerd geldt:*

$$\mathcal{O}^* = \{1,\ \ \zeta,\ \ \zeta^2,\ \ \zeta^3 = -1,\ \ \zeta^4 = -\zeta,\ \ \zeta^5 = \zeta^2\}.$$

Bewijs. We voeren een afbeelding $N : \mathcal{O} \to \mathbb{Z}$ in gegeven door

$$N(a + b{\cdot}\zeta) = a^2 + ab + b^2.$$

Uitleg van deze formule: dit is de lengte in het kwadraat van dit complexe getal; inderdaad,

$$z = a + b{\cdot}\zeta = (a + \frac{b}{2}) + \frac{b}{2}{\cdot}\sqrt{-3}; \quad N(z) = (a + \frac{b}{2}) + 3{\cdot}(\frac{b}{2})^2 = a^2 + ab + b^2.$$

Als $e \in \mathcal{O}^*$ dan is $N(e) = 1$. We zoeken alle $(a, b) \in \mathbb{Z}^2$ met $a^2 + ab + b^2 = 1$. We zien dat alleen de oplossingen $(a = \pm 1, b = 0)$ en $(a = 0, b = \pm 1)$ en $a = b = \pm 1$ mogelijk zijn (ga na). QED

(4.32) Propositie. * *In de ring* $\mathcal{O} = \mathbb{Z}[(+1+\sqrt{-3})/2]$ *zoals hierboven gedefiniëerd geldt bestaan en eenduidigheid van de priemfactor ontbinding op volgorde en eenheden na.*
We zullen het bewijs niet volledig geven. Maar de uitspraak volgt, zoals we dat in §4 deden, uit:

Het Euclidisch algoritme in $\mathcal{O}$**.** *Als* $z, d \in \mathcal{O} = \mathbb{Z}[(+1+\sqrt{-3})/2]$ *met* $N(d) < N(Z)$ *dan zijn er* $x, r \in \mathcal{O}$ *met*

$$z = x{\cdot}d + r, \quad \text{en} \quad r = 0 \quad \text{of} \quad N(r) < N(d).$$

(Dit is "deling met rest" in $\mathcal{O}$.)
We kunnen inzien dat inderdaad deze eigenschap geldt in deze $\mathcal{O}$. We kunnen inzien dat als het Euclidisch algoritme in $\mathcal{O}$ geldt, dan geldt in $\mathcal{O}$ eenduidigheid van de priemfactor ontbinding op volgorde en eenheden na (precies zoals we dat deden in §4). Deze stappen bewijzen de propositie.

(4.33) We lopen langs de rand van de afgrond. Beschouw de ring

$$R := \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid \ a, b \in \mathbb{Z}\} \quad \subset \quad \mathcal{O}$$

Ook hier weer kunnen we eenheden en irreducibele elementen definiëren. We zien dat $R^* = \{1, -1\}$: het is een deelverzameling van $\mathcal{O}^*$ en dit zijn de enige elementen van $\mathcal{O}^*$ in R. We zien de factorizatie

$$2{\cdot}2 = 4 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

Ga na dat $2,\ 1 + \sqrt{-3},\ 1 - \sqrt{-3}$ irreducibele elementen zijn in R. Concludeer dat de eenduidigheid van priemfactor ontbinding niet geldt in R.

Merk op: $a + b{\cdot}\zeta \in \mathcal{O}$ is een element van R dan en slechts dan als b even is.

(4.34) Lemma. Zij $z \in \mathcal{O} = \mathbb{Z}[\zeta]$. Dan is er een $i \in \mathbb{Z}$ zodanig dat $\zeta^i{\cdot}z \in R = \mathbb{Z}[\sqrt{-3}]$.
Bewijs. Beschouw $z = a + b{\cdot}\zeta \in R$. We onderscheiden drie gevallen:
(0) b is even.
(1) a is oneven en b is oneven.
(2) a is even en b is oneven.

We bewijzen dat in geval (i) er geldt: $\zeta^i \cdot z \in R$. Dit is duidelijk voor $i = 0$.
In geval (1):

$$\zeta \cdot (a + b\cdot\zeta) = a\cdot\zeta + b\cdot(-1 + \zeta) = -b + (a + b)\cdot\zeta \in R.$$

In geval (2):

$$\zeta^2 \cdot (a + b\cdot\zeta) = (-a - b) + a\cdot\zeta \in R.$$

QED

(4.35) Stelling* (Euler). FLT_3 *is juist, dat wil zeggen:*

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

Opmerking. We kunnen ons afvragen of Euler inderdaad een volledig bewijs had.
Bewijs. Neem aan dat er een niet-triviale oplossing bestaat (en we zullen tot een tegenspraak komen). Het is voldoende deze stelling te bewijzen voor het geval dat $\mathrm{ggd}(x, y) = 1$, dat x en y oneven en z even zijn, dat $z > 0$ en dat z minimaal is in de verzameling van alle oplossingen. We onderscheiden twee gevallen:
(I) z is niet deelbaar door 3;
(I) z is deelbaar door 3.

We nemen aan dat x, y, z voldoen aan de condities hierboven, en dat we in geval (I) zijn. We laten zien/construeren:

(I.1) $a := (x + y)/2$, $b := (x - y)/2$, en 4 deelt a, en b is oneven,

$$\frac{a}{4}\cdot(a^2 + 3b^2) = (\frac{z}{2})^3,$$

er bestaan $r, s \in \mathbb{Z}$ met $(a/4) = r^3$ en $(a^2 + 3b^2) = s^3$.

(I.2) Er bestaan $c, d \in \mathbb{Z}$ zodanig dat d is oneven, c is even en:

$$a = c^3 - 9cd^2, \quad b = 3c^2d - 3d^3, \quad \mathrm{ggd}(c, c^2 - 9d^2) = 1, \quad \mathrm{ggd}(c, d) = 1;$$

in het bijzonder $a^2 + 3b^2 = (c + 3d^2)^3$.

(I.3) Er bestaan $e, f, g \in \mathbb{Z}$ zodanig dat $\mathrm{ggd}(f, g) = 1$, met e niet deelbaar door 3 en

$$\frac{c}{4} = e^3, \quad c + 3d = f^3, \quad c - 3d = g^3, \qquad f^3 + g^3 = (2e)^3.$$

Onderstel dat deze stappen bewezen zijn. Een berekening leert dat $\mid 2e \mid < z$. We hebben een "kleinere oplossing'. Deze tegenspraak bewijst de stelling in het geval (I). Nu nog de drie stappen hierboven bewijzen.

Het geval (I.1) berust op eenduidige factor ontbinding in $\mathbb{Z}$; we laten dit als opgave.

Voor het geval (I.2) construeren we $c, d \in \mathbb{Z}$ met $a + b\sqrt{-3} = (c + d\sqrt{-3})^3$. Allereerst:
Claim. *Een ireducibel element $\pi \in \mathcal{O}$ is niet een deler van $a + b\sqrt{-3}$ én van $a - b\sqrt{-3}$.*
Als π we een deler zou zijn van beide factoren, dan is π ook een deler van $a+b\sqrt{-3}+a-b\sqrt{-3} = 2a$, en een deler van $a + b\sqrt{-3} - (a - b\sqrt{-3}) = 2b\sqrt{-3}$. Merk op dat $2 \in \mathcal{O}$ irreducibel is, en 2 is niet een deler van $a + b\sqrt{-3}$; dus $\pi \neq 2$. (Alle beschouwingen op eenheden na in $\mathcal{O}$.) Stel dat $\sqrt{-3}$ een deler zou zijn van $a \in \mathcal{O}$; dan zou 3 een deler zijn van a in $\mathbb{Z}$, tegenspraak. Blijft

over: π is een deler van a en van b; omdat $\text{ggd}(a,b)=1$ bestaan er in $\mathbb{Z}$ elementen A,B met $Aa+Bb=1$. Dan zou π een deler zijn van 1 in $\mathcal{O}$; dus π een eenheid in $\mathcal{O}$, tegenspraak want π is ireducibel. QEDClaim

Merk op dat $a+sb^2=s^3$. We ontbinden $s\in\mathcal{O}$ in priemfactoren in $\mathcal{O}$, gebruik makend van (4.32), en van de Claim hierboven:

$$s=(\pi_1\times\cdots\times\pi_m)\times(\pi_1'\times\cdots\times\pi_m');$$

hierbij hebben we deze factoren zo geordend dat π_i precies die factoren zijn die deler zijn van $a+b\sqrt{-3}$ in $\mathcal{O}$. Gebruik makend van (4.34) vermenigvuldigen we elk van de factoren π_j met een macht van ζ zodanig dat het product in $R=\mathbb{Z}[\sqrt{-3}]$ zit. We concluderen dat we krijgen

$$a+b\sqrt{-3}=(\zeta^M\times(A_1+B_1\sqrt{-3})\times\cdot\times(A_m+B_m\sqrt{-3})^3=\zeta^{3M}\times(A+B\sqrt{-3})^3$$

met $A_j,B_j,A,B\in\mathbb{Z}$. Dan is $\zeta^{3M}=+1$ of $=-1$; schrijf $c=\zeta^{3M}\cdot A$ en $d=\zeta^{3M}\cdot B$. Uit

$$a+b\sqrt{-3}=(c+d\sqrt{-3})^3\quad\text{volgt}\quad a=c^3-9cd^2,\quad b=3c^2d-3d^3.$$

De rest van (I.2) volgt uit een directe beschouwing.

We laten het bewijs van (I.3) als opgave. Hiermede eindig een bewijs van de stelling in geval (I).

Voor het geval (II) zien we dat 3 een deler van a is, en we krijgen

$$\frac{a}{4}\cdot(b^2+3(\frac{a}{3})^2)=9\cdot(\frac{z}{6})^3.$$

Analoog als voorheen construeren we c en d met

$$\frac{a}{3}=3c^2d-3d^3,\quad b=c^3-9cd^2;\quad\text{dus}\quad 8r^3=(2d)(c+d)(c-d).$$

We zien dat de factoren 3-de machten zijn in $\mathbb{Z}$,

$$c+d=e^3,\quad 2d=f^3,\quad c-d=g^3;\quad\text{dus}\quad f^3+g^3=e^3.$$

Hieruit zien we een "kleinere" oplossing, tegenspraak, en dit geeft een bewijs van geval (II). We laten details over aan de lezer als opgave. QED(4.35)

Opmerking. Zie [20], Chapter 2, §2. Zie [37], 13.4. Zie [34], pp 127-131; merk op dat in $R=\mathbb{Z}[\sqrt{-3}]$ geen eenduidige factor ontbinding heerst. Daarom waren we in het bewijs boven iets voorzichtiger dan in dit boek.

(4.36) Een Speculatie. Wat was het "*wonderbaarlijke bewijs*" dat Pierre de Fermat voor ogen had ten hij zijn beroemde aantekening in de kantlijn maakte? Het is onwaarschijnlijk dat Fermat iets wist van de methoden die in het 20-ste eeuwse bewijs van Wiles gebruikt werden. Laat ik echter speculeren.

Neem $n\in\mathbb{Z}_{\geq 2}$. Schrijf ζ_n voor het complexe getal met absolute waarde gelijk aan 1 en argument gelijk aan $2\pi/n$, m.a.w. $\zeta_n:=e^{2\pi\sqrt{-1}}$. Dat getal heeft de eigenschap dat $\zeta_n^n=1$ en $\zeta_n^j\neq 1$ voor alle j met $1\leq j<n$. We schrijven $R_n=\mathbb{Z}[\zeta_n]$ voor de deelverzameling van $\mathbb{C}$ bestaande uit getallen van de vorm

$$z=a_0+a_1\cdot\zeta+\cdots+a_j\cdot\zeta^j+\cdots+a_{n-1}\cdot\zeta^{n-1}.$$

We kunnen gaan rekenen in dit getal-systeem (in die ring). Onderstel dat $n > 2$ *oneven* is; bij voorbeeld $n = p > 2$ is een priemgetal. Het is niet moeilijk om in te zien dat we de volgende pylynoom-gelijkheid hebben:

$$X^n + Y^n \quad = \quad (X+Y)(X+\zeta{\cdot}Y)\cdots(X+\zeta^j{\cdot}Y)(X+\zeta^{n-1}{\cdot}Y).$$

Analoog zoals we het hierboven voor het geval $n = 3$ deden geldt:

Stelling. *Als $R_n = \mathbb{Z}[\zeta_n]$ eenduidige factorizatie heeft, dan geldt FLT_n.*

Dit is een bijzonder geval van een algemenere stelling van Kummer.

Het is mogelijk dat Fermat dacht dat er eenduidige factorizatie heerst in R_n voor elke n en zodoende tot zijn bewering FLT *kwam.*

Deze foute bewijsvoering is tot laat in de 19-de eeuw, vaak door gerenommeerde wiskundigen, als "bewijs"van FLT gegeven tot Kummer afdoende aantoonde wat hier aan schort.

Wel geeft deze redenering enig resultaat:

Zij p een priemgetal met $2 < p < 23$. Dan bezit $R_p = \mathbb{Z}[\zeta_p]$ eenduidige factorizatie;
Conclusie. *Voor deze priemgetallen is* FLT_p *juist.*

Voor andere priemgetallen vond Kummer een prachtig en elegant criterium. Voor elke p kunnen we definiëren een getal $h_p \in \mathbb{Z}_{>0}$, het *klasse-getal van de ring R_p*. Dat getal "meetïn hoeverre R_p verwijderd is van unieke factorizatie; in het bijzonder$h_p = 1$ dan en slechts dan als unieke factorizatie geldt in R_p.

Kummer definiëert:

$$(p \text{ is regulier}) \quad \Longleftrightarrow \quad (p \text{ deelt niet } h_p),$$

en bewijst:

Stelling. (Kummer, 1850). *(p is regulier)* $\quad\Longrightarrow\quad$ *(*FLT_p *is juist).*

Zie [20], Hoofdstukken 4 en 5.

Dit bewijst al veel meer gevallen van FLT. Bij voorbeeld: als $2 \leq p < 100$ en $p \notin \{37, 59, 67\}$ dan is p regulier, en dus geldt FLT_p. Deze theorie van Kummer was een van de eerste krachtige theoretische methoden om FLT aan te pakken in de geschiedenis. Voor meer informatie zie bij voorbeeld:
http://primes.utm.edu/glossary/page.php?sort=Regular

Opmerking. Het aantal niet-reguliere priemgetallen is oneindig; na Kummer bleven er dus nog veel gevallen over. Bovendien is het nog steeds niet bewezen (maar wel vermoed) dat het aantal reguliere priemgetallen oneindig is (de methode van Kummer bewees daarom niet FLT_p voor oneindig veel gevallen).

5 Congruente getallen

We bestuderen een probleem, het vinden van "congruente getallen", dat voor de eerste keer te vinden is in een anoniem Arabisch manuscript geschreven voor 972. In 1225 Fibonacci bestudeerde dit probleem. Verschillende gevallen werden bestuderd door Fermat. Het is mogelijk dat Fermat, gestimuleerd door zijn oplossing van het geval $N = 2$, zijn FLT formuleerde.

Veel onderzoek is verricht. Veel gevallen zijn nu beslist. Maar, dit probleem uit de 10-de eeuw, is in wezen in de 20-eeuw nog steeds onopgelost. We geven hier een uittreksel uit [62].

(5.1) Definitie I. Een positief geheel getal N heet een *congruent getal* als er bestaat een $\delta \in \mathbb{Q}$ zodanig dat

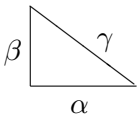
$$\delta^2 - N, \quad \delta^2, \quad \delta^2 + N$$

kwadraten zijn in $\mathbb{Q}$. We zullen schrijven CG = congruent getal, en CGP = het probleem van het vinden van congruente getallen / bepalen of een gegeven getal congruent is.

Opmerking. Deze terminologie, ingevoerd door Fibonacci, lijkt vreemd. Het bedoelt uit te drukken dat de drie getallen een rekenkundige rij vormen. Als de twee opeenvolgende verschillen gelijk zijn dan noemt Fibonacci dit in Latijns *congruum*, vandaar de naamgeving; zie [29], pp. 53/54, page 54, regel 13.

Vanuit algebraïsch standpunt lijkt deze vraag vreemd. Maar een meetkundige beschouwing helpt:

(5.2) Definitie II. Een positief geheel getal N heet een *congruent getal* als er een rechthoekige driehoek bestaat met lengtes van zijden in $\mathbb{Q}$ en met oppervlak gelijk aan N.
Als de lengtes van de zijden $\alpha, \beta, \gamma \in \mathbb{Q}$ zijn, met behulp van de stelling van Pythagoras zien we dan:



$$\alpha \cdot \beta/2 = N,$$
$$\alpha^2 + \beta^2 = \gamma^2;$$
een voorbeeld is: $\alpha = 9/6, \quad \beta = 40/6, \quad \gamma = 41/6, \quad N = 5.$

(5.3) Lemma. *Deze beide definities zijn equivalent.*
Bewijs. Veronderstel $\delta^2 - N = \xi^2$ en $\delta^2 + N = \lambda^2$. Schrijf $\gamma := 2\delta$, en $\alpha := \lambda + \xi$ en $\beta := \lambda - \xi$. Dan is

$$\alpha \cdot \beta = \lambda^2 - \xi^2 = 2N$$

en

$$\alpha^2 + \beta^2 = \lambda^2 + 2\lambda\xi + \xi^2 + \lambda^2 - 2\lambda\xi + \xi^2 = 2\lambda^2 + 2\xi^2 = 4\delta^2 = \gamma^2.$$

We zien dat Definitie I als gevolg heeft Definitie II.

Omgekeerd, onderstel $\alpha, \beta, \gamma \in \mathbb{Q}$ en $N \in \mathbb{Z}$ zoals in Definitie II zijn gegeven. Definieëer $\delta := \gamma/2$. Dan is

$$\delta^2 \pm N = \frac{1}{4}(\gamma^2 \pm 2\alpha\beta) = (\frac{1}{2}(\alpha \pm \beta))^2.$$

Dus voldoen δ and N aan Definitie I. We zien dat de twee definities aan elkaar gelijk zijn. QED

We zien dat $N = 5$ een CG is (volgens Definitie II). De overgang naar Definitie I geeft: kies $\delta = 41/12$. We zien dat

$$\delta^2 - 5 = \frac{1681}{144} - 5 = \frac{961}{144} = (\frac{49}{12})^2 \quad \text{and} \quad \delta^2 + 5 = \frac{1681}{144} + 5 = \frac{2401}{144} = (\frac{31}{12})^2.$$

Dit voorbeeld komt voor in het Arabische manuscript (in totaal geeft dat manuscript 30 congruente getallen), zie [1], zie pp. 256/257, maar ook in en artikel van Abu Jafar Muhammad ibn al-Hasan Al-Khazin, zie [77], page 83, zie [3]. Of het voorbeeld $N = 5$ een congruent getal is werd rond 1220 door Johann Panormitanus di Palermo aan Leonardo di Pisa (Fibonacci) gevraagd, zie [18], page 460. Fibonacci vond dezelfde oplossing als hierboven; dit was voor hem een begin voor zijn boek "Liber Quadratorum" (1225).

(5.4) Voorbeeld/Opgave. Is $N = 13$ een congruent getal? Zie (5.33).

(5.5) Definitie. We zeggen dat $M \in \mathbb{Z}_{>} 0$ "*kwadraatvrij*" is als 1 het grootste kwadraat van een geheel getal is dat M deelt; equivalent: M is niet deelbaar door p^2, voor welk priemgetal p dan ook.

Een kwadraatvrij CG heet een *primitief congruent getal*, afgekort pCG.

Merk op: voor $N \in \mathbb{Z}_{>0}$ en D een positief geheel getal is N een CG dan en slechts dan als D^2N een CG is. Bij voorbeeld, de gevallen $N = 15$, en $D^2N = 60$ en $D^2N = 240$ worden besproken door Al-Khazin, zie [3], page 149.

(5.6) In de "Arithmetica" van Diophantus vinden we in V.9.III.22, zie ook II.9.II.20, een probleem geformuleerd als het van oplossingen van de twee vergelijkingen $s^2 + w = u^2$ en $s^2 - w = v^2$ in 4 variabelen. Diophantus merkt ook het verband op met rechthoekige driehoeken. We zouden dus kunnen zeggen dat het probleem van de congruente getallen, CGP, afkomstig is van Diophantus. De vraag naar oplossingen in de gehele getallen leidt tot het probleem van de congruente getallen.

Echter het lijkt dat in het anonieme Arabische manuscript er voor het eerst een keuze $N = w \in \mathbb{Z}$ bestudeerd wordt en bovendien worden Pythagoreïsche drietallen gebruikt om voorbeelden van CGen te construeren. Daarom ben ik geneigd om te stellen dat het CGP voor de eerste keer in de geschiedenis genoemd wordt in de 10-de eeuwse Arabische wiskunde.

Merk op dat werk van Diophantus reeds bekend was in die tijd in de Arabische wiskunde, bij voorbeeld zie [3], page 136. Maar we weten niet of de auteur van het anonieme manuscript de *Arithmetica* van Diophantus kende ; zie [18], pp. 459/460, en zie [77], pp. 9/10. We weten dat Al-Khazin werk van Diophantus kende, maar in dezelfde vorm als wat we nu tot onze beschikking hebben?

(5.7) Kies $\boxed{N = 1}$. Is dit een congruent getal? Deze vraag werd tenminste 7 eeuwen bestudeerd, en foute bewijzen werden gegeven, zie [18], page 462, [15], page 20. Fibonacci zei dat hij een bewijs had dat dit niet een CG is; we betwijfelen of hij werkelijk een bewijs had. Pas het genie Fermat wist deze vraag te beantwoorden. We zullen zien dat dit probleem een catalysator was in wiskundig onderzoek. Zie (5.29).

We vragen ons af wat de CGen zijn, en hoe we kunnen bepalen of een gegeven getal congruent is. Waarom is het probleem $N = 1$ zo moeilijk? We kennen het verband met de PDen, en die kennen we toch allemaal? Een dergelijk probleem dient zorgvuldig gesteld te worden (zoals altijd in het leven ...). We formuleren drie vragen.

(5.8) Vraag A. *Kunnen we een lijst maken waarin alle* pCGen *staan?*

We zullen zien dat dit niet moeilijk is, en dat die lijst oneindig lang is. Lost dit ons probleem op? Onderstel dat we willen weten of $N = 1$ een CG getal is. We inspecteren de lijst. Na lang zoeken hebben we nog steeds dit getal niet gevonden. Wat zegt dat? Nog niets. En we zullen zien dat voor een relatief klein getal (bv. $N = 157$, $N = 263$) we heel ver moeten gaan in die lijst om inderdaad dat getal te vinden. Voorbeelden staan o.a. op de laatste twee pagina's van deze syllabus.

(5.9) Vraag B. *Is er een effectieve manier om te beslissen of een gegeven getal congruent is?*
Hiermee bedoelen we: is er een formule die voor elk gegeven geheel getal N de hoeveel tijd (of de hoeveel rekenkundige stappen) geeft zodanig dat het beslissen of N een CG getal is gedaan kan worden binnen die tijd?

Notatie. Een paar (δ, N) zoals in Definitie I, of, equivalent, $((\alpha, \beta, \gamma), N)$ zoals in Definitie II heet een "presentatie" van het CG N.

(5.10) Vraag C. *Hoeveel presentaties heeft een* CG ?

Stop. Alvorens verder te lezen, laat de vragen goed tot U doordringen, probeer te begrijpen dat dit inderdaad goede formulering zijn van het CGP, en probeer in te schatten welke vraag een moeilijk/gemakkelijk antwoord heeft.

(5.11) Over methodes in het anonieme Arabische manuscript merkt Woepcke op in [1] on page 252: "C'est en effet la meilleure méthode possible ... les divers moyens particuliers qui permettent dans certains cas de reconnaître immédiatement si un nombre donné est ou n'est pas nombre congruent." We kunnen de vraag stellen wat de "best mogelijk methode" is (het kan best zin dat er later betere gevonden worden). Maar mijn bezwaar richt zich vooral op "reconnaître immédiatement ... ou n'est ...": elk eindig deel van de lijst geeft niet een beslissing of $N = 1$ een CG is; voor oneindig veel getallen is het nu nog steeds niet bekend of ze een CG zijn; zo "onmiddellijk" is die methode dus niet.

We gaan nu de theorie van de PDen gebruiken, zoals beschreven in §4, in het bijzonder in Stelling (4.5). Als $\alpha^2 + \beta^2 = \gamma^2$ een driehoek beschrijft met oppervlak $\alpha\beta/2$ dan is voor elke $\rho > 0$ een driehoek $(\rho\alpha)^2 + (\rho\beta)^2 = (\rho\gamma)^2$, met oppervlak $\rho^2\alpha\beta/2$. Als N een CG is en $D \in \mathbb{Z}_{>0}$ dan is D^2N en omgekeerd. Daarom is het voldoende om alleen maar kwadaraatvrije congruente getallen te beschouwen: pCG.

We maken een lijst van alle PDen (x, y, z); voor elk zo'n drietal kiezen we de grootste $D \in \mathbb{Z}_{>0}$ zodat D^2 een deler is van $xy/2$. Dan is

$$\alpha := x/D, \quad \beta := y/D, \quad \gamma := z/D \quad \text{een presentatie van het pCG} \quad N := \alpha\beta/2 = xy/(2D^2),$$

en elk pCG kan op deze manier gevonden worden.

(5.12) Conclusie (een positief antwoord op vraag **A**). *Er is een (oneindige) lijst waar alle* pCGen *precies éénmaal in voorkomen.*

n	m	x	y	x	D	N	
1	2	3	4	5	1	6	
1	4	15	8	17	2	15	
2	3	5	12	13	1	30	
1	6	35	12	37	1	210	$x = m^2 - n^2$
2	5	21	20	29	1	210	$y = 2mn$
3	4	7	24	25	2	21	$z = m^2 + n^2$
1	8	63	16	65	6	14	
2	7	45	28	53	3	70	
4	5	9	40	41	6	5	
1	10	99	20	101	3	110	$ND^2 = (m^2 - n^2)mn$
2	9	77	36	85	3	154	
3	8	55	48	73	2	330	
4	7	33	56	65	2	231	
5	6	11	60	61	1	330	
1	12	143	24	145	2	429	
2	11	117	44	125	3	286	
3	10	91	60	109	1	2730	
4	9	65	72	97	6	65	
5	8	39	80	89	2	390	
6	7	13	84	85	1	546	
etc.	etc.	etc.	etc.	etc.	etc.	etc.	

We beginnen met n en m in de linker kolommen zodanig dat

$$0 < n < m, \quad \gcd(m, n) = 1, \quad m + n \quad \textit{is oneven.}$$

Kies voor D^2, het grootste kwadraat dat $ab/2 = (m^2 - n^2)\cdot m\cdot n$ deelt. schrijf

$$\alpha = a/D, \quad \beta = b/D, \quad \gamma = c/D \quad \textit{and} \quad N = \alpha\beta/2 = (m^2 - n^2)\cdot m\cdot n/D^2;$$

dit is een pCG.

Merk op dat het CGP voor N vertaald is in het vinden van $m > n$ en D zodat

$$N\cdot D^2 = m\cdot n\cdot(m^2 - n^2).$$

we zullen ook zeggen dat $((m, n), D, N)$ een presentatie is van het pCG N.

We gaan nu een verband leggen tussen congruente getallen en elliptische krommen over $\mathbb{Q}$. Hier is eerst de meetkundige intuïtie. we hebben gezien dat N een congruent getal is als voldaan is aan de vergelijkingen

$$\alpha^2 + \beta^2 = \gamma^2 \quad \alpha^2\cdot\beta^2 = 2N.$$

Zie ook (5.26). Voor een gegeven N kunnen we dit zien als twee vergelijkingen in 3 variabelen. Meetkundig betekent dat de doorsnede van twee kwadratische oppervlakken in de 3-dimensionale ruimte. We weten (onder aanname dat die doorsnede niet-singulier is), dat er zo een ellliptische kromme komt; we kunne proberen die door middel van een vergelijking in het vlak weer te geven. Een oplossing $(\alpha, \beta, gamma) \in \mathbb{Q}^3$ zou dan een rationaal punt geven op die kromme. Daarom is het niet verwonderlijk dat er geldt:

(5.13) **Feit** (zie [42], Prop. 1 op pagina 4, en Prop. 19 op pp. 46/47): *Zij* $N \in \mathbb{Z}_{>0}$. *Beschouw de elliptische kromme* E_N *gedefiniëerd door de vergelijking*

$$E_N : \quad Y^2 = X \cdot (X - N) \cdot (X + N).$$

Dan is N *een congruent getal dan en slecht dan als er bestaan*

$$x, y \in \mathbb{Q} \ \ \textit{met} \ \ y \neq 0 \ \ \textit{en} \ \ (x, y) \in E_N(\mathbb{Q}).$$

Ook geldt:

(5.14) **Feit.** Zij N een kwadraatvrij getal. Over $K = \mathbb{Q}$ geven we E_N door $Y^2 = X(X - N)(X + N)$. Dan geldt:

$$\mathrm{Tors}(E(\mathbb{Q})) = \{\infty, (0,0), (N,0), (-N,0)\} \cong (\mathbb{Z}/2)^2.$$

Een bewijs is te vinden: [42], I.9, Prop.17 op pag. 44. Voor $N = 1$ zie (3.10). Een speciaal geval, N is een priemgetal, bewijzen we in (3.23).

(5.15) Uit de stelling van Mordell, zie [41], pag. 14, Th. 1.5, weten we dat $E_N(\mathbb{Q})$ en abelse groep is die *eindig voortgebracht* is; we kunnen schrijven $E_N(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r$, waar $r \in \mathbb{Z}_{\geq 0}$ en T een eindige abelse groep is (waar r en T afhangen van de keuze van de elliptische kromme). Het blijkt dat in dit geval $\#(T) = 4$: deze eindige groep bestaat uit $\{0, (-N,0), (0,0), (+N,0)\}$. De bovenstaande stelling zegt:

$$N \quad \text{is congruent} \quad \Longleftrightarrow \quad r(E_N) > 0.$$

(5.16) We geven een deel van het bewijs van (5.13). We schrijven $\alpha, \beta, \gamma \in \mathbb{Q}$ voor de lengtes van de zijden van een rechthoekige driehoek met oppervlakte $\alpha \cdot \beta/2 = N$, maar we kiezen de volgorde zo dat $\alpha < \beta < \gamma$ (dus $\alpha = a/D$, of $= b/D$ en $\beta = b/D$ of $= a/D$. De "vertaling"die we gaan gebruiken hebben we reeds gezien:

$$\{(\alpha, \beta, \gamma) \in \mathbb{Q}^3 \mid 0 < \alpha < \beta < \gamma, \ \ \alpha^2 + \beta^2 = \gamma^2\} \stackrel{\sim}{\leftrightarrow}$$

$$\stackrel{\sim}{\leftrightarrow} \{x \in \mathbb{Q} \mid x > 0, \ \ \text{zo dat} \ \ x, x - N, x + N \ \ \text{elk een kwadraat in } \mathbb{Q}_{>0} \text{ is}\},$$

door middel van:

$$(\alpha, \beta, \gamma) \mapsto (x = \frac{\gamma^2}{4}, y = \pm \frac{(\beta^2 - \alpha^2) \cdot \gamma}{8}),$$

en

$$x \mapsto (\alpha = \sqrt{x + N} - \sqrt{x - N}, \ \ \beta = \sqrt{x + N} + \sqrt{x - N}, \ \ \gamma = 2 \cdot \sqrt{x}).$$

Zo zien we: als N en congruent getal is, dan schrijven we

$$y = \pm \sqrt{x^3 - N^2 x},$$

en dan zijn er $x, y \in \mathbb{Q}$ met $y \neq 0$ en $(x, y) \in E_N$. De omkering is niet geheel vanzelfsprekend, we verwijzen naar [42], pp. 46/47.

(5.17) We geven een kleine moeilijkheid in het bewijs aan. Neem $N = 5$. We zien dat

$$P = (x = -4, y = 6) \in E_N(\mathbb{Q}),$$

want substitutie van $x = -4$ in $X^3 - 25{\cdot}X = X(X-5)(X+5)$ geeft $(-4){\cdot}(-4-5){\cdot}(4-+5) = 4{\cdot}9$. Echter dit punt P voldoet niet aan de voorwaarde dat $x - N, x, x + N$ kwadraten zijn.

Maar laten we niet de moed verliezen. Trek de raaklijn in dit punt $P \in E_5$ aan die kromme. Omdat de kromme wordt gegeven door de vergelijking

$$F := -Y^2 + X^3 - 25{\cdot}X = 0$$

wordt de raaklijn in een punt $(x, y) = P \in E_5 = E$ aan die kromme. gegeven door de vergelijking

$$\frac{\partial F}{\partial X}(x){\cdot}(X - x) + \frac{\partial F}{\partial Y}(y){\cdot}(Y - y) = 0.$$

De raaklijn in $P = (x = -4, y = 6) \in E_N(\mathbb{Q})$ wordt gegeven door

$$(48 - 25)(X + 4) - 12(Y - 6) = 0;$$

deze lijn, gegeven door $23X - 12Y + 4{\cdot}41 = 0$, snijdt de kromme E_5 in het punt $P = (x = -4, y = 6)$ twee maal (allicht, zo hebben we deze lijn geconstrueerd), en het snijdt de kromme in het punt

$$(\frac{41^2}{4{\cdot}6^2}, \quad -\frac{(40^2 - 9^2){\cdot}41}{8{\cdot}6^3}) = Q \in E_5(\mathbb{Q})$$

(ga na!). Met behulp van dít punt kunnen we een bijbehorend drietal berekenen, en we krijgen dat

$$\alpha = \frac{9}{6}, \quad \beta = \frac{40}{6}, \quad \gamma = \frac{41}{6}$$

(ga na!). We zien dat $Q = 2P$, en met meer theorie beschikbaar, bewijzen we dat elk punt

$$Q = (x, y) \in E_N(\mathbb{Q})$$

dat verkregen wordt als $Q = 2P$ met $P \in E_N(\mathbb{Q})$ bewijst dat N congruent is; zo verloopt de rest van het bewijs van het bovenstaande feit.

(5.18) We zien een subtiel verschil tussen de meetkunde enerzijds en de getaltheorie anderzijds van dit probleem: neem $M, N \in \mathbb{Z}_{>0}$, dan geldt:

$$E_N \quad \cong_{\mathbb{R}} \quad E_M,$$

maar

$$E_N \quad \cong_{\mathbb{Q}} \quad E_M \quad \Longleftrightarrow \quad \exists d \in \mathbb{Q}_{>0} \ \text{ met } \ M = d^2{\cdot}N.$$

Als E_N gegeven wordt door $Y^2 = X^3 - M^2X$, dan geeft de substitutie $X = d^2{\cdot}\xi, \quad Y = d^3{\cdot}\eta$ een vergelijking die bij deling door d^6 een vergelijking geeft die E_M definiëert.

(5.19) Voorbeeld: We weten dat $N = 5$ een congruent getal is, door middel van $a = 9, b = 40, c = 41, D = 6$. Zoals we reeds zagen geeft de constructie:

$$(\alpha = \frac{9}{6}, \beta = \frac{40}{6}, \gamma = \frac{41}{6}) \mapsto (x = \frac{41^2}{4 \cdot 6^2}, \quad y = \pm\frac{(40^2 - 9^2) \cdot 41}{8 \cdot 6^3}).$$

Inderdaad is $y^2 = x^3 - 5^2 \cdot x$ (ga na). Merk op dat

$$x - 5 = (\frac{31}{12})^2, \quad x = (\frac{41}{12})^2, \quad x + 5 = (\frac{49}{12})^2.$$

Nu os de brug geslagen tussen enerzijds ons probleem en anderzijds de theorie van elliptische krommen. Dit geeft aanlieidng tot het volgende.

(5.20) Vraag B: een vermoeden. Het is verrassend te zien dat een antwoord op vraag **B** nog steeds onbekend is. Dat betekent dat in veel gevallen we ad hoc methodes moeten toepassen om te beslissen of en een gegeven getal N congruent is. Abstracte methodes zijn ontwikkeld, en op die manier zijn sommige gevallen opgelost. Sommige gevallen zijn beslist door middel van zeer snelle rekentechnieken.

In 1983 formuleerde Tunnel een vermoeden dat precies formuleert van welke getallen we *verwachten* dat ze een CG zijn. Het vermoeden is verrassend. Dit is niet iets wat je zou concluderen als je een (lange) lijst maakt van CGen en die consulteert. De wiskunde achter dit vermoeden is diep en is gebaseerd op een van de meest interessante en onopgeloste problemen van de 20-ste eeuw. Hier is het vermoeden van Tunnell

Zij $N \in \mathbb{Z}_{>0}$ kwadraatvrij. Onderstel allereerst dat N *oneven* is. Definiëer

$$L(N) := \#\left(\{(x, y, z) \in \mathbb{Z}^3 \mid N = 2x^2 + y^2 + 32z^2\}\right)$$

en schrijf

$$R(N) := \frac{1}{2}\#\left(\{(x, y, z) \in \mathbb{Z}^3 \mid N = 2x^2 + y^2 + 8z^2\}\right).$$

Voor $N \in \mathbb{Z}_{>0}$ kwadraatvrij en N *even* schrijven we

$$L(N) := \#\left(\{(x, y, z) \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 32z^2\}\right)$$

en

$$R(N) := \frac{1}{2}\#\left(\{(x, y, z) \in \mathbb{Z} \mid \frac{N}{2} = 4x^2 + y^2 + 8z^2\}\right).$$

Zie [42], pag. 221.

Bij gegeven N is het meestal eenvoudig om $L(N)$ en $R(N)$ te berekenen.

(5.21) Stelling (Coates and Wiles). *Zij N een* pCG. *Dan is $L(N) = R(N)$.*

(5.22) Vermoeden (Tunnell). *Zij N een kwadraatvrij positief geheel getal. Als $L(N) = R(N)$ dan* (?) *is N een* pCG.

Een toepassing. Kies $N = 1$. We zien: $L(N) = 2$ en $R(N) = 1$; ja, want in beide gevallen zijn de enige oplossingen $x = 0,\ y = \pm 1,\ z = 0$. De stelling impliceert dat $N = 1$ niet een CG is. Merk op dat deze stelling van Coates and Wiles een bewijs geeft van dit feit, eeuwen eerder reeds op een veel eenvoudiger manier bewezen door Fermat.

Een toepassing. Kies $N = 157$. Laat zien dat $L(N) = 0 = R(N)$. Als het vermoeden juist zou zijn, dan kunnen we concluderen dat $N = 157$ een CG is. Dit is ook juist, zoals een berekening van D. Zagier aantoonde, zie [42], pag. 5.

Merk op dat het criterium zoals Tunnell dat voorstelt inderdaad effectief is. Bij gegeven N hoeven we alleen maar drietallen (x, y, z) te beschouwen met $\mid x \mid < \sqrt{N}/2, \quad \mid y \mid \leq \sqrt{N}$ and $\mid z \mid < \sqrt{N/8}$. Heel weinig berekeningen zijn nodig, and dat aantal kan expliciet begrensd worden in termen van N.
Conclusie. Als het vermoeden van Tunnell juist is, dan heeft Vraag **B** een bevestigend antwoord.

P. Monsky bewees dat voor elk *priemgetal* N met $N \equiv 5 \pmod 8$ of $N \equiv 7 \pmod 8$ een CG is; zie [54]. Dit geeft een bewijs dat gevallen als $N = 13$ en $N = 157$ inderdaad CGen zijn, zonder berekeningen uit te voeren, maar door zuiver denkwerk.

Dit bewijst dat er oneindig veel CGen bestaan: gebruik het bewijs van Monsky, en gebruik de stelling van Dirichlet die zegt dat in de rekenkundige rij $\{5 + 8i \mid i \in \mathbb{Z}_{>0}\}$ er oneindig veel priemgetallen zijn. Is er een elementair bewijs voor het bestaan van oneindig veel pCGen ?

Een van de meest belangrijke vermoedens in de moderne wiskunde is die uitgesproken door Birch en Swinnerton-Dyer, zie [8]. Dit is een van de Clay Mathematics Institute Millenium problems, waarvoor \$ 1,000,000 is uitgeloofd voor een oplossing. Zie
http://www.claymath.org/millennium/
http://planetmath.org/encyclopedia/BirchAndSwinnertonDyerConjecture.html
http://www.claymath.org/millennium/Birch_and_Swinnerton-Dyer_Conjecture/BSD.pdf
Als dat vermoeden waar is, dan volgt het vermoeden van Tunnell, en dus zou een positief antwoord op vraag **B** volgen. Dit is typerend voor de moderne wiskunde. Bij het bestuderen van een vraag, formuleren we een veel algemenere vraag of mogelijk theorie, die de wiskundige structuur achter die vraag formuleert. We zien dat dit vaak tot onverwachte ontwikkelingen leidt.

We gaan Vraag **C** beantwoorden. We beginnen met een voorbeeld, dat een speciaal geval zal zijn van algemenere formules later.

(5.23) We weten dat $3^2 + 4^2 = 5^2$; dus is $(3, 4, 5)$ een PD, en we zien dat $xy/2 = 3{\cdot}4/2 = 6$ een CG is (en we nemen $D = 1$).

Kies $A = 49, B = 1200, C = 1201$. Merk op: $49^2 = 2401$. Dan geldt

$$1201^2 = 1200^2 + 2.1200 + 1 = 1200^2 + 49^2.$$

Kies $E = 70$. Dan is $AB/(2E^2) = 49 \times 1200/(7^2 \times 10^2 \times 2) = 6$. We hebben een nieuwe presentatie van het congruente getal $N = 6$ geproduceerd. Merk op dat $D = 1 < E = 70$.

Hier is nog een voorbeeld. We weten dat $((n = 4, m = 5), D = 2, 5)$ een presentatie is van het congruente getal 5. We zien dat $(V = 720, U = 1681, E = 747348)$,

$$720 \times 1681 \times (1681 - 720) \times (1681 + 720) = 5 \times 747348^2,$$

en we hebben een andere presentatie van $N = 5$. merk op dat $D = 2 < E = 747348$.

(5.24) Een mysterieus mechanisme Dit zijn bijzondere gevallen van de volgende algemene formules.

Veronderstel $m > n$ zijn als in (4.5); kies D zodat $N = m{\cdot}n{\cdot}(m^2 - n^2)/D^2$ een pCG is, dat wil zeggen dat $((m, n), D, N)$ een presentatie is van N:

$$m{\cdot}n{\cdot}(m^2 - n^2) \quad = D^2 \cdot N, \quad xy = 2ND^2.$$

Kies

$$U := z^2 = (m^2 + n^2)^2, \quad V = 2xy = 2(m^2 - n^2)2mn.$$

Dan geldt:

$$U \cdot V \cdot (U - V) \cdot (U + V) = z^2 \cdot 2xy \cdot (y^2 + y^2 - 2xy) \cdot (x^2 + y^2 + 2xy) =$$

$$= 2xy \cdot z^2 \cdot (x - y)^2 \cdot (x + y)^2 =$$

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

Conclusie. Beginnen met een presentatie $((m, n), D, N)$ geven deze formules een nieuwe presentatie van N door middel van

$$U = c^2, \quad V = 2ab, \quad E = |\{2 \cdot z \cdot D \cdot (x - y) \cdot (x + y)\}|.$$

Merk op dat $D < E$.

(5.25) Gevolg (een antwoord op Vraag C). *Voor elk congruent getal is het aantal presentaties oneindig.*
Inderdaad, deze formules construeren uit elke presentatie een nieuwe presentatie met veel grotere getallen $D < E$. Dit proces kan oneindig vaak herhaald worden, en steeds krijgen we nieuwe presentaties. QED

(5.26) * Hoe komt een mens ooit aan een dergelijk idee? De vergelijkingen $\alpha^2 + \beta^2 = \gamma^2$ en $\alpha \cdot \beta = 2N$ kunnen beschouwd worden als twee kwadratische vergelijkingen in drie onbekenden (zeg, over $\mathbb{C}$) de oplos verzameling is een kromme (in $\mathbb{C}^3$), en algemene theorie vertelt je dat dit een "elliptische kromme" is. De formules geven na een coördinaten transformatie deze kromme in de vorm $Y^2 = X^3 - N^2X$ als een vlakke derde graads kromme. Met andere woorden, meetkundig is het bovenstaande "feit" geen verrassing. Inderdaad, dit vinden we al bij Diophantus, waar twee vergelijkingen $s^2 - w = u^2$, $s^2 + w = u^2$ in vier variabelen worden beschouwd. Dit geeft een oppervlak in de 4-dimensionale ruimte. Neem een waarde voor w vast, zoals in het probleem van de CGen. Dat geeft een vlakke snede van dit oppervlak, en de doorsnede is een elliptische kromme.

Opmerking. We moeten wel erg ver in de lijst gaan om weer een nieuwe presentatie te vinden. Daarom was dit verschijnsel ons nog niet opgevallen.

(5.27) Hoe kunnen we deze vreemde formules vinden? We gebruiken §1. Het principe gebaseerd is op een meetkundige interpretatie van het begrip CG. De methode voor het vinden van een dergelijk methode staat eigenlijk al bij Diophantus. Het vinden van de formules hierboven, volledig binnen het bereik van bij voorbeeld Diophantus zien we pas door de meetkundige interpretatie, die pas in de 20-ste eeuw duidelijk werd. We zagen dit in (5.26).

(5.28) We zien soms presentaties van hetzelfde pCG niet verkregen uit elkaar door het bovenstaande mechanisme. Bij voorbeeld $(n, m) = (1, 6)$, $(n, m) = (2, 5)$ with $D = 1$ and $(n, m) = (7, 8)$ with $D = 2$ geven drie verschillende presentaties voor $N = 210$. Een dergelijk verschijnsel kon pas worden verklaard met de theorie van arithmetiek op elliptische krommen.

(5.29) **Theorem** (Pierre de Fermat). $N = 1$ *is niet een congruent getal.*
See [41], Coroll. 4.20.

$\boxed{N = 1}$ Lang was dit een open probleem. Soms werden verkeerde bewijzen geproduceerd, zie [18], pag. 462, [15], pag. 20. Na vele eeuwen kwam Fermat met een bewijs.

Voor de samenhang tussen werk van Diophantus en het CGP zie (5.26)

(5.30) FLT **en** $N = 2$**.**
Pierre de Fermat (1608 – 1665) bewees dat $N = 1$, $N = 2$ en $N = 3$ niet CGen zijn. Uit (4.28) **Stelling** (Fermat). *Als* $x, y, w \in \mathbb{Z}$ *met* $x^4 + y^4 = w^2$ *dan is* $xyw = 0$.
concluderen we:

(5.31) **Gevolg** (Fermat). $N = 2$ *is niet een congruent getal.*
Bewijs. We nemen aan dat $N = 2$ wel een CG is, en komen tot een tegenspraak. Inderdaad, onderstel dat $\delta = c/d \in \mathbb{Q}$ de eigenschap heeft dat $\delta^2 - 2 = (u/d)^2$ and $\delta^2 + 2 = (v/d)^2$. Schrijf $x = uv$, $y = 2cd$ and $t = c^4 + 4d^4$. Omdat

$$u^2 = c^2 - 2d^2, \quad w^2 = c^2 + 2d^2$$

krijgen we

$$x^4 + y^4 = (uv)^4 + (2cd)^4 = ((c^2 - 2d^2)(c^2 + 2d^2))^2 + 16c^4d^4 = (c^4 + 4d^4)^2 = t^2.$$

Dit is in tegenspraak met Stelling (4.28). Dit bewijst het gevolg. QED

Was dit de inspiratie voor Fermat om zijn FLT te formuleren ?

We geven nog wat meer voorbeelden. Soms zijn er eenvoudige methoden om te beslissen of een gegeven getal congruent is. Soms denken we of weten al dat een gegeven getal congruent is, maar is er een enorme reken partij nodig om een presentatie te vinden. In die gevallen ligt het getal vaak veel te ver in de lijst zoals in A om op die manier een presentatie te vinden; dan moet theorie eerst helpen om de berekening te vereenvoudigen.

$\boxed{N = 13}$
Met $m = 325$, en $n = 36$ zien we:

$$m{\cdot}n{\cdot}(m^2 - n^2) = 325{\cdot}36{\cdot}289{\cdot}361 =$$

$$= 13{\cdot}5^2{\cdot}6^2{\cdot}17^2{\cdot}19^2.$$

Conclusie: $N = 13$ is een CG.

We zien dat $\delta = 106921/19380$ de eigenschap heeft dat $\delta^2 - 13 = (80923/19380)^2$ and $\delta^2 + 13 = (127729/19380)^2$. Dat is niet zo eenvoudig te vinden.

$\boxed{N = 23}$
Kies $m = 24336$, en $n = 17689$; dan is $m = 156^2$, $n = 133^2$, $m - n = 6647 = 17^2 \times 23$, en $m + n = 42025 = 205^2$. Dus is 23 een CG.

$\boxed{N = 157}$
Dit "kleine" getal is een CG (voorspeld door Tunnell, bewezen dor Monsky met "zuiver denkwerk", en bewezen door D. Zagier met behulp van een berekening). We zoeken de $\delta = c/d$ zodat $\delta^2 \pm 157$ kwadraten zijn waar d het minst aantal cijfers heeft; dit treedt op met $m = 443624018997429899709925$, and $n = 166136231668185267540804$; zie [42], pag. 5 voor de bijbehorende driehoek.

Dit is een mooi voorbeeld van het "chaotische gedrag" van het getal D in de lijst van CGen; als we te werk gaan zoals in Vraag A, dan krijgen we die lijst, maar het kan voorkomen dat voor een klein getal de bijbehorende D erg groot is. Dit maakt het probleem, in de vorm van Vraag B zo moeilijk. We zullen zien dat $N = 10374$ een kleine presentatie heeft, en $N = 263$ een heel grote.

$\boxed{N = 219}$
Dit is een CG omdat $48 \times 73 \times (73 + 48) \times (73 - 48) = 219 \times (4 \times 5 \times 11)^2$.

Bekijk de rij getallen $3, 11, 19, \cdots, i8 + 3, \cdots, 211$ with $0 \leq i \leq 26$;
dit zijn allemaal kwadraatvrije getallen die niet congruent zijn. Maar $219 = 3 \times 73 = 27 \times 8 + 3$ is een CG, alhoewel 3 en 73 niet CGen zijn. Verder is $N = 171 = 9 \times 29 = 21 \times 8 + 3$ wel een CG.

Bastien bewees dat elk priemgetal van de vorm $i8 + 3$ niet een CG is; zie [4].

Merk op dat $49 \times 48 \times 1 \times 97 = 28^2 \times 291$; dit bewijst dat 291 een CG is; idem voor 299, omdat $36 \times 13 \times 23 \times 49 = 42^2 \times 299$.

We zien het soms onvoorspelbare gedrag van getallen wat betreft het gedrag als wel/niet een CG.

$\boxed{\text{N=263}}$ De keus

$m = 241504696540719988647244439501505 6$

en

$n = 219658997253142085134052135647096 9$

bewijst dat dit een CG is (zoals bewezen door Monsky, voorspeld door Tunnell).

Alle gevallen $1 \leq N \leq 999$, zijn doorgerekend:

http://www.asahi-net.or.jp/ KC2H-MSM/mathland/math10/matb2000.htm

http://www.asahi-net.or.jp/ kc2h-msm/mathland/math10/mail1001.htm

Zie ook [43]. Zie ook de laatste pp. van deze syllabus.

$\boxed{N = 10374}$ Dit is het grootste CG te vinden in het Arabische manuscript [1]. Inderdaad,

kies $n = 3$ and $m = 13$ en we krijgen

$$m{\cdot}n{\cdot}(m+n){\cdot}(m-n) = 13 \times 6 \times 19 \times 17 = 10374.$$

Hier zien we een relatief grote N die een kleine presentatie heeft.

Voor elke N met $N \equiv r \pmod 8$, met $r \in \{5, 6, 7\}$, voorspelt het vermoeden van Tunnell dat dit niet een CG. Maar voor andere congruenties is dit niet zo eenvoudig:

$r = 0$ 8 is niet een CG en 24 is een CG;
$r = 1$ 1 is niet een CG en and 41 is een CG;
$r = 2$ 2 is niet een CG en 34 is een CG;
$r = 3$ 3 is niet een CG en 219 is een CG;
$r = 4$ 4 is niet een CG en 28 is een CG.

(5.32) Een paar verwijzingen. Er is de afgelopen 10 eeuwen enorm veel gepubliceerd over het CGP. We geven slechts een paar verwijzingen.

In het tweede deel van Dickson, zie [18], vinden we in Chapter 16 een overzicht van vroege pogingen om het CGP op te lossen. In [36], Problem D27 vinden we een overzicht van bekende oplossingen, en we vinden daar ook recente verwijzingen. In [77] vinden we het verband tussen de *Arithmetica* van Diophantus en Arabische middeleeuwse wiskunde. In [42] vinden we een overzicht van een paar moderne methodes, in het bijzonder de weg naar het vermoeden van Tunnell, zoals geformuleerd in [92].

Voor overzichten zie ook [2] and [15]. In het bijzonder zie [41] voor een heldere uiteenzetting die nodig zijn voor een moderne benadering.

Voor meer gespecialiseerde moderne benaderingen zie [88], [79], [43], [54].

Voor een benadering op elementair niveau, zie [5].

Het CGP, bekend in de oudheid, veel bestudeerd is na zoveel eeuwen nog steeds onopgelost. Net zoals dat bij FLT het geval was: het is nu niet meer een geïsoleerd probleem: sinds 1983 weten we dat dit probleem opgelost is als we het vermoeden van Birch en Swinnerton-Dyer op juist is.

(5.33) Oplossing. Een oplossing: Met $m = 325$ en $n = 36$ komt er

$$m{\cdot}n{\cdot}(m^2 - n^2) = 325{\cdot}36{\cdot}298{\cdot}361 =$$

$$= 13{\cdot}5^2{\cdot}6^2{\cdot}17^2{\cdot}19^2.$$

Conclusie: $N = 13$ is een congruent getal.

6 Het Poncelet probleem

In deze paragraaf behandelen we een klassiek probleem. Dat werd door V. Poncelet in 1822 opgesteld en opgelost. Er is een mooie geschiedenis aan verbonden. We hebben nu een modern bewijs "in een paar regels" dat gebruik maakt van de theorie van elliptische krommen.

Om het probleem goed te formuleren hebben we eerst wat kennis over de definitie en eigenschappen van "het projectieve vlak" nodig.

(6.1) $\mathbb{P}^2$, het projectieve vlak. We schrijven $\mathbb{A}^2(K) = K^2$, het affiene vlak over een lichaam K (spoedig zullen we $K = \mathbb{C}$ nemen, maar laat ik het eerst wat algemener opzetten). Een eigenschap die niet prettig is: er "ontbreken punten". Evenwijdige lijnen die verschillend zijn snijden elkaar niet. Dat gaan we verhelpen door $\mathbb{A}^2$ uit te breiden.

We construeren $\mathbb{P}^2(K)$, zodanig dat $\mathbb{A}^2 \subset \mathbb{P}^2$ en zodanig dat elke twee lijnen in $\mathbb{P}^2$ wel tenminste een punt gemeen hebben. Schrijf $K^* := K - \{0\}$; dit is een multiplicatieve groep. Voor $\lambda \in K^*$ en $(x, y, z) \in K^3$ schrijven we $\lambda{\cdot}(x, y, z) = (\lambda{\cdot}x, \lambda{\cdot}y, \lambda{\cdot}z)$, en we schrijven $(x, y, z) \sim (\lambda{\cdot}x, \lambda{\cdot}y, \lambda{\cdot}z)$. De equivalentie klassen onder deze relatie zijn of het punt $(0, 0, 0)$ of een lijn in K^3. We schrijven:

$$K^3 - \{0\} \quad \longrightarrow \quad \big(K^3 - \{0\}\big) \,/\, \sim =: \mathbb{P}^2(K); \quad (x, y, z) \bmod \sim =: [x : y : z].$$

Met andere woorden: punten van $\mathbb{P}^2(K)$ zijn van de vorm $[x : y : z]$; hierin is minstens een van de coördinaten ongelijk aan nul, en alleen de verhoudingen tussen die coördinaten spelen een rol.

Voorbeeld. Neem de polynomen $aX + bY + cZ$ en $\alpha X + \beta Y + \gamma Z$ die ongelijk aan nul zijn (niet alle coëficiënten gelijk aan nul), en beschouw de nulpunten $\mathcal{Z}(aX + bY + cZ) = \ell \subset \mathbb{P}^2$, en $\mathcal{Z}(\alpha X + \beta Y + \gamma Z) = m \subset \mathbb{P}^2$. Bewering: $\ell \cap m \neq \emptyset$.
Bewijs. De punten $(x, y, z) \in K^3$ met $ax + by + cz = 0$ vormen een vlak $V \subset K^3$ dat bevat $0 = (0, 0, 0)$ en idem geeft de andere vorm een vlak W. Omdat $0 \in V \cap W$ en omdat $\dim(V) + \dim(W) = 4 > 3$ volgt uit eenvoudige lineaire algebra dat $\dim(V \cap W) > 0$ (die vlakken in K^3 vallen samen, of snijden elkaar in een lijn door 0. Dus is $\ell \cap m \neq \emptyset$.

Voor een polynoom $g \in K[X, Y, Z]$ en een punt $P = [x : y : z]$ is de formulering $g(P)$ niet zinvol in het algemeen. Echter, als g homogeen is (alle termen hebben de zelfde totale graad), dan is de uitspraak $g(P) = 0$ wel zinvol: omdat g homogeen is, zeg van graad m, geldt $g(\lambda{\cdot}x, \lambda{\cdot}y, \lambda{\cdot}z) = \lambda^m g(x, y, z)$ en $g(P) = 0$ desda $g\lambda P) = 0$.

We zien dat $\mathbb{A}^2 \subset \mathbb{P}^2$. Aan $(x, y) \in \mathbb{A}^2$ kunnen we toevoegen $[x : y : 1] \in \mathbb{P}^2$. Omgekeerd, als $[x : y : z] \in \mathbb{P}^2$ met $z \neq 0$ dan kunnen we hier aan toevoegen $(x/z, y/z) \in \mathbb{A}^2$. Zodoende komt er:

$$\mathbb{A}^2 \hookrightarrow \mathbb{P}^2, \quad (x, y) \mapsto [x : y : 1], \quad [x : y : z] \mapsto (x/z, y/z).$$

We zien dat elke lijn in $\mathbb{A}^2$ precies een punt geeft in $\mathbb{P}^2$ "in het oneindige", en elke twee evenwijdige lijnen gaan door datzelfde punt.

Terugblik. Neem $f = -Y^2 + X^3 + AX + B$. We beschouwden de kromme gedefinieerd door dit polynoom, en daar namen we nog een punt 0 bij. Dit kunnen we nu als volgt begrijpen. Schrijf g voor het polynoom dat we uit f verkrijgen door f op de "zuinigste manier" homogeen te maken: in dit geval $g = -Y^2Z + X^3 + AXZ^2 + BZ^3$; laat $E = \mathcal{Z}(g) \subset \mathbb{P}^2$. Dan zien we dat voor

$$\mathbb{A}^2 = \mathbb{P}^2 - \{[x : y : z] \mid z = 0\} \hookrightarrow \mathbb{P}^2, \quad E := \mathcal{Z}(g) \subset \mathbb{P}^2$$

we krijgen

$$\mathbb{A}^2 \supset \mathcal{Z}(f) = \mathbb{A}^2 \cap \mathcal{Z}(g) \subset E \subset \mathbb{P}^2, \quad \{[x:y:z] \mid z=0\} \cap E = \{[0:1:0]\}.$$

Dit verklaart de opzet die we eerder hanteerden.

(6.2) Kegelsneden. Neem homogeen polynoom $g \in K[X,Y,Z]$ van graad twee. Dan heet $\mathcal{Z}(g) \subset \mathbb{P}^2$ een *kegelsnede*. We noemen die kegelsnede *ontaard* als er een singulariteit is.

We beschrijven de classificatie van kegelsneden over $K = \mathbb{C}$.
(1a) Het kan zijn dat we kunnen schrijven $g = (aX + bY + cZ)^2$. In dat geval is $\mathcal{Z}(g)$ een "dubbel tellende lijn".
(1b) Het kan zijn dat we kunnen schrijven $g = h_1[\cdot]h_2$, waar h_1 en gh_2 lineaire vormen zijn met $\mathcal{Z}(h_1) = \ell_1 \neq \ell_2 = \mathcal{Z}(h_2)$. In dit geval bestaat $cZ(g)$ uit twee verschillende lijnen die elkaar snijden.
(2) Als $cZ(g)$ een singulariteit heeft, dan zijn we ineen van de twee bovenstaande gevallen. Als dit niet het geval is, dan spreken we van een niet-ontaarde kegelsnede. Als $\mathcal{Z}(g_1)$ en $\mathcal{Z}(g_2)$ beide niet-ontaard zijn, dan is er een lineaire transformatie van $\mathbb{P}^2$ die de ene in de andere overvoert.

Over een lichaam dat niet algebraïsch gesloten is (bij voorbeeld over $\mathbb{R}$), of over een lichaam van karakteristiek twee is de classificatie ingewikkelder. Het feit dat we over ellips, hyperbool, parabool spreken heeft ermee te maken dat we dan over $\mathbb{R}$ werken, en een inbedding $\mathbb{A}^2 \subset \mathbb{P}^2$ kiezen: de parabool raakt aan "de lijn in oneindig", de ellips (en de cirkel) heeft met die lijn geen reële snijpunten, en de hyperbool heeft met die lijn twee verschillende reële snijpunten.

Voor de rest van deze paragraaf werken we over $K = \mathbb{C}$, het lichaam van de complexe getallen. Het woord kegelsnede zullen we in de rest van deze paragraaf alleen maar gebruiken voor het niet-ontaarde geval.

(6.3) Lemma. *Zij $D \subset \mathbb{P}^2$ een kegelsnede, en $P \in \mathbb{P}^2$ met $P \notin D$. Dan zijn er precies twee (onderling verschillende) lijnen door P die raken aan D.* ("De poollijn van P ten opzichte van$D$ snijdt D in twee verschillende punten.").
Notatie. Voor een polynoom g schrijven we g_X voor $(d/dX)(g)$ (de andere variabelen worden dan als constanten gezien). De afgeleide hier is de "formele afgeleide: $(d/dX)(aX^m) = maX^{m-1}$, waar $a$een constante is die X niet bevat.
Bewijs. Als $P = [a:b:c]$ en $D = \mathcal{Z}(g)$ dan wordt de raaklijn in een punt $Q \in D$ gegeven door $\mathcal{Z}(g_X(Q)X + g_Y(Q)Y + g_Z(Q)Z$ en we zien dat P op die raaklijn ligt als $\mathcal{Z}(g_X(Q)a + g_Y(Q)b + g_Z(Q)c = 0$. Dus geeft $\mathcal{L}_P = \mathcal{Z}(g_X a + g_Y b + g_Z c)$ snijpunten met D die, verbonden met P alle lijnen geven door P die raken aan D; de lijn $\mathcal{L}_P$ wordt wel de poollijn van P ten opzichte van D genoemd. We moeten laten zien dat voor $P \notin D$ die lijn $\mathcal{L}_P$ de kegelsnede D in twee verschillende punten snijdt. We passen een transformatie toe, zodanig dat $D = \mathcal{Z}(X^2 + Y^2 + Z^2)$ en $P = [a:b':c']$; we veronderstellen dat $a \neq 0$ (anders, verwissel coördinaten), en schrijf $P = [-1:b:c]$. Uit

$$g_X a + g_Y b + g_Z c = 0 \quad \text{volgt} \quad X = bY + cZ.$$

Substitutie in $X^2 + Y^2 + Z^2 = 0$ geeft

$$(b^2+1)Y^2 + 2bcYZ + (c^2+1)Z^2 = 0. \quad (*)$$

De discriminant van dit polynoom is

$$(2bc)^2 - 4(b^2+1)(c^2+1) = -4(b^2+c^2+1).$$

Omdat $P \notin D$ volgt $1 + b^2 + c^2 \neq 0$. Dus heeft $(*)$ twee verschillende oplossingen. QED

(6.4) We zullen gebruik maken van het volgende feit. Veronderstel dat $C, D \subset \mathbb{P}^2$ twee kegelsneden zijn die elkaar overal transversaal snijden (dat wil zeggen voor elke $P \in C \cap D$ zijn de raaklijnen $\mathfrak{t}_{C,P}$ en $\mathfrak{t}_{D,P}$ verschillend). Dan geldt

$$\#\,(C \cap D) = 4.$$

Voor een bewijs, zie (6.9).

(6.5) Notatie. De verzameling van raaklijnen aan D geven we aan met $D^\vee$.

(6.6) De Poncelet constructie. Gegeven zijn kegelsneden $C, D \subset \mathbb{P}^2$ die elkaar overal transversaal snijden. We beginnen met $(P_0, \ell_0) = (P, \ell) \in C \times D^\vee$ met $P \in \ell$. Een dergelijk paar noemen we

$$\text{een Poncelet paar:} \quad P \in C, \quad \ell \in D^\vee, \quad P \in \ell.$$

We construeren inductief

$$\text{de Poncelet-rij} \quad (P_0, \ell_0), \quad (P_1, \ell_1), \cdots$$

als volgt. Bij gegeven (P_i, ℓ_i) schrijven we $\ell_i \cap C = \{P_i, P_{i+1}\}$ (het kan zijn dat $\ell^i \in C^\vee \cap D^\vee$, de lijn ℓ_i raakt aan beide kegelsneden, en dan is $P_i = P_{i+1}$). Vervolgens schrijven we $\{\ell_i, \ell_{i+1}\}$ voor de verzameling van alle lijnen door P_{i+1} die raken aan D (het kan zijn dat $P_{i+1} \in C \cap D$, en in dat geval is $\ell_i = \ell_{i+1}$). Dit geeft de inductieve constructie (tweede snijpunt, dan tweede raaklijn, etc.) van de Poncelet-rij gegeven door C en D

(6.7) De sluitingsstelling (Poncelet, 1822). *Gegeven zijn twee* (niet-ontaarde) *kegelsneden $C, D \subset \mathbb{P}^2$ die elkaar overal transversaal snijden. Als er een Poncelet-paar $(P_0, \ell_0) = (P, \ell)$ en een getal $n \in \mathbb{Z}_{>0}$ zijn zodanig dat*

$$(P_0, \ell_0) = (P_n, \ell_n)$$

(de constructie sluit na n stappen)

$$\textit{dan sluit de Poncelet-rij na } \ n \ \textit{ stappen voor elk begin-paar } \ (P_0', \ell_0').$$

.

(6.8) Opmerking / Opgave. Maak een situatie met $C, D \subset \mathbb{P}^2$ als boven, een Poncelet-paar (P_0, L_0) en een $n \in \mathbb{Z}_{>0}$ zodanig dat de Poncelet constructie een Poncelet-rij geeft waarin (P_n, L_n) met $P_0 = P_n$ terwijl er een ander Poncelet-paar (Q_0, M_0) is met $Q_0 \neq Q_n$. Merk op het subtiele verschil in de formulering hier en in 6.

(6.9) Bewijs van $\#(C \cap D) = 4$.
Stap 1. We laten zien dat we een niet-ontaarde kegelsnede C kunnen parametriseren. Kies een punt $R \in C$. Elke lijn ℓ door R snijdt C in nog een punt: $\ell \cap C = \{R, P\}$; het komt voor dat $R = P$, namelijk als ℓ de raaklijn in R is. Omgekeerd geeft elk punt $P \in C$ de lijn die R en P verbindt. Parametrizatie van alle lijnen door R geeft een paramtrizatie van C.
Concreet voorbeeld (dat zagen we al bij Pythagoreïsche driehoeken). Neem de cirkel gegeven door $X^2 + Y^2 = 1$. Zij $R = (-1, 0) \in C$. Voor elke $(0, t)$ op de Y-as komt er een lijn ℓ_t die R en $(0, t)$ verbindt: $t(X + 1) = Y$. Die lijn snijdt C in $P = ((1 - t^2)/(1 + t^2), 2t/(1 + t^t))$. Hier zien we de parametrizatie

$$t \longmapsto [1 - t^2 : 2t : 1 + t^2] \in C$$

Stap 2. We zien dat de coördinaten van een punt op C kwadratische vormen in een variabele t zijn; of: homogene kwadratische vormen $\mathcal{X}(S,T), \mathcal{Y}(S,T), \mathcal{Z}(S,T)$ in de homogene variableen S, T. Substitutie daarvan in de vergelijking g die D definieert geeft $g(\mathcal{X}(S,T), \mathcal{Y}(S,T), \mathcal{Z}(S,T))$. Die vorm is niet identiek nul (want C en D zijn verschillend). Er zijn 4 nulpunten, en die zijn onderling verschillend (want C en D snijden elkaar overal transversaal). We concluderen dat er precies 4 waarden voor $[S : T]$ zijn die de snijpunten $C \cap D$ geven. QED

We beginnen met een bewijs van (6.7). We beschouwen

$$E \subset C \times D^\vee; \quad E := \{(P, \ell) \mid P \in C, \ \ \ell \in D^\vee, \ \ \ P \in \ell\}.$$

We zien de projecties $p : E \to C$ en $q : E \to D$. Merk op dat p twee-op-een is boven alle punten van C die niet in D liggen (in zulke punten zijn er twee raaklijnen aan D te trekken), en boven elk punt van $C \cap D \subset C$ ligt er precies een punt op E. niet nodig, maar mooi voor de symmetrie: we kunnen inzien dat er precies 4 gemeenschappelijke raaklijnen zijn voor C en D, oftewel $\#(C^\vee \cap D^\vee) = 4$, en de projectie q is twee-op-een buiten die punten van $D^\vee$.
Feit. *E is een elliptische kromme (na een keuze van $0 \in E$).* We kunnen die kromme krijgen door de 4 punten in $C \cap D$ in de parametrizatie van C na een transformatie de waarden $\{0, 1, \lambda, \infty\}$ te geven, en dan wordt E gegeven door $Y^2 = X(X - 1)(X - \lambda)$.
Feit. *De Poncelet constructie $(P, \ell) = \tau \mapsto \tau' = (P', \ell')$ is een afbeelding $\varphi : E \to E$, en deze afbeelding wordt geven door:*

$$\exists \alpha \in E : \quad \varphi(\tau) = \tau + \alpha, \ \ \forall \tau \in E.$$

Dit volgt uit een diepe stelling over elliptische krommen.

Als we deze constructie en deze feiten aannemen, dan volgt het bewijs van 6: Uit het feit dat bij gegeven (P_0, ℓ_0) de constructie sluit: $\tau_0 = (P_0, \ell_0) = (P_n, \ell_n)$ volgt

$$\varphi^n(\tau_0) = \tau_0 + n{\cdot}\alpha = \tau_0; \quad \text{dus} \quad n{\cdot}\alpha = 0.$$

Voor elke $\sigma_0 \in E$ volgt $\varphi^n(\sigma_0) = \sigma_0 + n{\cdot}\alpha = \sigma_0$. Dit bewijst (6.7). QED

(6.10) Opmerking / Opgave. Maak een situatie met $C, D \subset \mathbb{P}^2$ als boven, een Poncelet-paar (P_0, L_0) en een $n \in \mathbb{Z}_{>0}$ zodanig dat de Poncelet constructie een Poncelet-rij geeft waarin (P_n, L_n) met $P_0 = P_n$ terwijl er een ander Poncelet-paar (Q_0, M_0) is met $Q_0 \neq Q_n$. Merk op het subtiele verschil in de formulering hier en in 6.

(6.11) Oplossing van (6.8). Kies $P_2 \in C \cap D$, verder L_1 de raaklijn in P_2 aan D, tweede snijpunt met C is P_1, andere raaklijn L_1 aan D door P_1 snijdt nog in $P_0 \in C$. Dan zien we $P_1 = P_3$ en $P_0 = P_4$. Maar dit is niet een sluitings-situatie (waarom niet?).

7 Appendix A: Groepen

We zullen de begrippen "groep", "ring" en "lichaam" veelvuldig tegen komen. 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.

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

(7.1)**(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 $a + (-a) = 0 = (-a) + a$.

(7.1)**(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).

(7.1)**(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 $\overline{3}^{-1} = \overline{2}$.

(7.1)**(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 een-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.

(7.1)**(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

(7.2) 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.

(7.3) 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.

(7.4) 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?

(7.5) Zij G een groep, multiplicatief geschreven, en $x \in G$. We zeggen dat n de orde is van x, notatie $\mathrm{ord}(x) = n$ als $n \in \mathbb{Z}> 0$, en $x^n = 1$ en voor $1 \leq i < n$ geldt $x^n = e$. M.a.w.. de orde is de kleinste exponent j nodig om x^j te krijgen. Als er een dergelijke exponent niet bestaat dan schrijven we $\mathrm{ord}(x) = \infty$.

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

$$\mathrm{Tors}(A) := \{x \mid \mathrm{ord}(x) < \infty\}.$$

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

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

8 Appendix B: Ringen en lichamen

(8.1) Definitie. Een vijftal $(R, +, 0, i, \times)$ wordt een *ring* genoemd als R een (niet-lege) verzameling is, verder $(R, +, 0, i)$ een additief geschreven groep is, en voor elke $x, y \in R$ er gedefinieerd is een $x \times y \in R$ zodanig dat:
(assoc) $x \times (y \times z) = (x \times y\times)z$, voor alle $x, y, z \in R$,
(een) $x \times 1 = x = 1 \times x$ voor alle $x \in R$, en
(distr) $a \times (x + y) = a \times x + a \times y$, $(a + b) \times x = a \times x + b \times x$.

(8.2) Voorbeelden. Voor $R = \mathbb{Z}$ (met de gebruikelijke operaties) gelden deze regels: dit is een ring.

Evenzo voor de verzameling $\mathbb{Q}$ van de rationale getallen. Evenzo voor de verzameling $\mathbb{C}$ van de complexe getallen

Voor elke $n \in \mathbb{Z}\geq 1$ Is de verzameling $\mathbb{Z}/n$ met optellen en vermenigvuldigen modulo n een ring.

Schrijf $i = \sqrt{-1}$ en

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

Met de gebruikelijke operaties in $\mathbb{C}$ beperkt tot $\mathbb{Z}[i]$ is R een ring.

De verzameling $R = \{0\}$ met $0 = 1$ is een ring; dat lijkt flauw, maar het is nuttig om dit voorbeeld ook te beschouwen.

Een element $x \in R$ wordt een *nuldeler* genoemd als $x \neq 0$ en als er een $y \neq 0$ bestaat met $xy = 0$. Laat zien dat de ring $\mathbb{Z}/6$ nuldelers heeft. Wat is de nodig en voldoende voorwaarde in $n \in \mathbb{Z}_{>1}$ opdat de ring $\mathbb{Z}/n$ een nuldeler heeft?

Het classificeren van alle ringen is een moeilijk probleem in die algemeenheid.

In de definitie wordt niet verondersteld dat de operatie $\times$ commutatief is. inderdaad bestaan er niet-commutatieve ringen (de $+$ is wel commutatief in elke ring). maar die zullen we niet verder in onze betrekkingen beschouwen.

Vaak schrijven we xy in plaats van $x \times y$; ook wordt wel de notatie $x{\cdot}y$ gebruikt.

(8.3) Definitie. Een *lichaam* K is een commutatieve ring waarin bovendien $0 \neq 1$, en elke element $x \in K$ met $x \neq 0$ een inverse heeft; deze laatste eigenschap kan ook gegeven worden als: $K^* := K - \{0\}$ is met de operatie $\times$ een groep.

(8.4) Voorbeelden. We kennen al de lichamen $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Zij p een priemgetal en $K := \mathbb{Z}/p$. Dit is een lichaam. Inderdaad, als $x = \overline{m} = m \bmod p$ waar p niet een deler is van n, dan is $\gcd(n, p) = 1$; dus zijn er $a, b \in \mathbb{Z}$ met $ap + bm = 1$; in dat geval geldt

$$\overline{b}{\cdot}\overline{m} = \overline{bm} = \overline{1} = 1 \in K.$$

Dit lichaam wordt wel genoteerd als $\mathbb{F}_p = \mathbb{Z}/p$.

Merk op dat in een lichaam K geldt: als $x, y \in K$, $x \neq 0$ en $y \neq 0$ dan is $xy \neq 0$. We zien dat $\mathbb{Z}/n$ een lichaam is dan en slechts dan als n een priemgetal is.

Het lichaam $\mathbb{F}_2$ gebruikt U vele malen er dag. Het bestaat uit 0 en 1 en computers, tekstverwerkers en ga zo maar door werken door de gegevens eerst in rijtjes 1-en en nullen om te zetten.

Het classificeren van alle eindige lichamen is elegant en overzichtelijk opgelost. Het is de basis voor veel crypto- en factorizatie-systemen.

9 Appendix C: De ring van de gehele getallen

In deze paragraaf bespreken we een paar eigenschappen van de ring $\mathbb{Z}$, en van het rekenen "modulo n", m.a..w. rekenen in $\mathbb{Z}/n$.

(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 priem factoren. 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

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

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. 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 $d = \mathrm{ggd}(a_1,a_2) = \ldots = \mathrm{ggd}(a_{i+1},a_{i+2}) = \cdots$. 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 $d = \mathrm{ggd}(a_{s-1}, a_s) = a_s$. 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 $d = \mathrm{ggd}(a_1,a_2)$ 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 $\mathrm{ggd}(p,b) = p$. Als p niet een deler is van b dan geldt $\mathrm{ggd}(p,b) = 1$ 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 $\equiv 1 \pmod 4$.

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) geldt 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; 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 gevalen van FLT zo bewezen met een uitgebreide bestudering van factorizaties in $\mathbb{Z}[\zeta_p]$. Een prachtig stuk wiskunde.

In de rest van de paragraaf noemen we een paar aspecten over rekenen modulo n.

(9.9) 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.

De vergelijking $T^2 = 2$ heeft niet een oplossing in $\mathbb{Z}$. Geef een bewijs.

(9.10) 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. Zie (16.4).

(9.11) 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 (16.29). Zie (16.5).

(9.12) 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:

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

We zien dat er voor elke n een j is met $-10 < s^j(N) < 10$.
Opgave. Bewijs:
(n is deelbaar door 11) $\iff$ $(\exists j : \ a^j(n) = 0)$.
Zie (16.30). Zie (16.6).

(9.13) 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: bewijs dat de vergelijking een oplossing heeft 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

$$3X^3 + 4Y^3 + 5Z^3 = 0; \quad \text{beschouw oplossingen met} \quad XYZ \neq 0.$$

Hij 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 [71]. Dat was een doorbraak, en nieuwe methoden werden ontwikkeld om verder te komen.

10 Appendix D: De kalender

(10.1) Het doel van de **"kalender methode"**: geef een datum, en bereken daaruit op welke dag van de week die valt (of viel). Het blijkt dat die methode gemakkelijk te gebruiken en eenvoudig te onthouden is. Ik gebruik deze methode vaak.

Eerst enkele bekende begrippen. We zullen de maanden nummeren door: januari = I, februari = II, maart = III, $\cdots$, oktober = X, november = XI, december = XII.

Dit doe ik om verwarring te voorkomen. In het Nederlands zeggen we "3 januari", in het Engels "January 3", wat wordt er bedoeld met "03-01-1993", is dat 3 januari of 1 maart? Op formulieren schrijven we dan meestal "03-01-1993", en we bedoelen 3 januari, ik geef de voorkeur aan "03-I-1993". Zo is 3-X = 3 oktober (de dag dat deze cursus in 2007 begint).

We weten dat het aantal dagen van de verschillende maanden is:
I (31), **II (28 of 29)**, III (31), IV (30), V (31), VI (30),
VII (31), VIII (31), IX (30), X (31), XI (30), XII (31).

Wat is de reden van dat springen van het aantal dagen van februari? De aarde loopt niet precies in 365 dagen om de zon heen, maar we willen wel dat Kerstmis ergens in de winter valt, en dat juli ergens in de zomer valt, en dat het zo blijft in de loop van de eeuwen. De *gregoriaanse kalender* corrigeert dit door de meeste jaren uit 365 dagen te laten bestaan, maar in sommige andere jaren gaat er één dag meer in een kalenderjaar:

Een **schrikkeljaar** is een jaar waarin februari 29 dagen heeft;
in alle andere jaren heeft februari 28 dagen.

De jaren $\cdots$, 2004, 2008, 2012, $\cdots$ zijn schrikkeljaren
(het jaartal is wél deelbaar door 4),
de jaren $\cdots$ 2001, 2002, 2003, 2005, $\cdots$ zijn niet schrikkeljaren.
(het jaartal is níét deelbaar door 4)
Verder is er de afspraak: 1700, 1800, 1900, 2100 zijn niet schrikkeljaren,
en 1600, 2000, 2400 zijn wél schrikkeljaren
(d.w.z. als een getal n deelbaar is door 4, dan is n $\times$ 100 wel een schrikkeljaar, als n niet deelbaar is door 4, dan is het niet een schrikkeljaar). Ja, het is een beetje gecompliceerd, maar zo bereiken we dat voorlopig het gemiddeld aantal dagen in een jaar met grote nauwkeurigheid gelijk is aan de omloopstijd van de aarde om de zon.

(10.2) **Opgave.** 3 maart 1788 en 3 maart 1788+28 vallen op dezelfde dag, maar 3 maart 1888 en 3 maart 1888+28 vallen niet op dezelfde dag. (Algemeen: periodiciteit van 28 jaar als in die periode niet een eeuw-jaar bevat, want $7 \times 366 + 21 \times 365$ is deelbaar door 7, allicht).
Opgave. Bewijs dat het aantal dagen in een periode van precies 400 jaar deelbaar is door 7 (en concludeer: 3 maart 1788 en 3 maart 2188 vallen op dezelfde dag van de week).
Opgave. Bereken in een periode van 400 jaar voor getal $\{1, 2, \cdots, 30, 31\}$ hoe vaak dat getal voorkomt op welke dag van de week. Concludeer dat "vrijdag de 13-de"de grootste frequentie heeft!

(10.3) **De jaardag.** Om deze kalender methode te gaan gebruiken definiëren we de **jaardag** van een zeker jaar: het is de dag van de week waarop de laatste dag van februari valt in dat

jaar.
Voorbeeld: In 1993 valt 1 maart op een maandag (het is níét een schrikkeljaar, februari 1993 heeft daarom 28 dagen, 28-II-1993 is een zondag), en we schrijven:

$$\text{jd}(1993) = \text{zondag} = \text{zo}.$$

Kijken we b.v. naar 1992, dan is 1-III-1992 een zondag (1992 is wél een schrikkeljaar, en 29-II-1992 valt op een zaterdag), we schrijven:

$$\text{jd}(1992) = \text{zaterdag} = \text{za}.$$

Natuurlijk kunnen we zodra we één jaardag weten, alle andere berekenen (merk op: van 2001 naar 2002 schuift de jaardag een naar voren, van 2003 naar 2004 schuift de jaardag 2 naar voren). Het is wel handig om een paar gegevens in een tabel te hebben:

jaartal = n	jaardag= jd(n)
1700	zo
1800	vrij
1900	woe
2000	di
...	...
1980	vrij
1990	woe
1991	do
1992	za
1993	zo
1994	ma
...	...
1999	zo
2000	di
2001	woe
2002	do
2003	vrij
2004	zo
2005	ma
2006	di
2007	woe
2008	vrij
2009	zat
2010	zo
...	... etc.

Hoe berekenen we uit jd(1900)=woe de jaardag van bv. 1978? Als we van 1900 naar 1978 gaan, dan is dat 78 jaren verder, en we passeren van 1901 t/m 1978 precies 19 schrikkeljaren. De jaardag schuift dus 78+19 dagen op, en schuift daarom van een woensdag naar een dinsdag. Oefenen: jd(1800)=vrij, wat is jd(1888)?

(10.4) Verder onthouden we voor elke maand een getal:

III = maart		7 = 3+4
IV = april	4	
V = mei		9 = 5+4
VI = juni	6	
VII = juli		11 = 7+4
VIII = augustus	8	
IX = september		5 = 9-4
X = oktober	10	
XI = november		7 = 11-4
XII = december	12	
II = februari		laatste
I = januari		laatste (+1 als s.)

Wat is de betekenis van deze getallen? In de tabel staat achter maart het getal 7, en daarmee bedoelen we dat 7 maart op dezelfde dag valt als de laatste dag van februari, dus 7 maart valt op de jaardag:

$$\text{dag(7-III-2024)} = \text{jd(2024)}.$$

Idem voor 4 april, die valt ook op de jaardag, evenzo voor 9 mei en zo gaan we door. De reden dat we het zo doen, is dat dit gemakkelijk te onthouden is:

- voor de "even"maanden april, $\cdots$, december nemen we gewoon het rangnummer van de maand,
- voor maart, mei, juli tellen we 4 op bij het rangnummer,
- voor september en november trekken we er 4 vanaf.

(10.5) We passen de kalender-methode toe:
Voorbeeld. Neem 13 oktober 1993, de eerste tabel geeft: jd(1993) =zo, dus de laatste dag van februari 1993 is een zondag, evenzo is 10-X-1993 een zondag (gebruik de tweede tabel), en we zien direct dat 13-X-1993 op een woensdag valt.
Voorbeeld. Op welke dag viel StNicolaas in 1979? Eerste tabel: jd(1979) = woe, gebruik tweede tabel, en concludeer dat 12-XII-1979 een woensdag was.
Voorbeelden. dag(5-V-1945) = za; jd(1940) = jd(1968) = jd(1996) = do, en we zien dat dag(10-V-1940) = vrij.
Voorbeeld. Neem 14-II-1992, merk op dat 1992 een schrikkeljaar is, uit de tabel zien we daarom dat dag(29-II-1992)= za, en we concluderen dag(14-II-1992)= vrij.

Evenzo proberen we 5-I-1993: we zien dag(28-II-1993)= zo = dag(31-I-1993), en concluderen: dag(5-I-1993) = di. Oefenen!
Opgave: Bereken de dag van Uw eigen verjaardag.
Strikvraag: Op welke dag van de week viel 29-II-1978?

Opmerking. De kalender die we nu gebruiken werd in 1582 ingevoerd door Paus Gregorius XIII; we noemen deze jaartelling de *gregoriaanse kalender*. Daarvóór gebruikte men de *Juliaanse kalender*, ingevoerd door Julius Caesar in 46 voor Chr. Die jaartelling had een kleine onnauwkeurigheid, die in de loop van de jaren tot steeds grote afwijkingen aanleiding gaf. De datum 5-X-1582 (Juliaans) werd gelijk gesteld aan 15-X-1582 (Gregoriaans).

Het verschil tussen de twee jaartellingen: 1300, 1400, 1500, 1700, 1800, 1900, 2100, etc. zijn in de juliaanse wél in de gregoriaanse kalender níét een schrikkeljaar. Dit verschil van 3 dagen per 400 jaar bleek net voldoende om de nodige correctie uit te voeren.

NB Er zijn ook heel andere jaartellingen. De joodse, de islamitische, de Japanse jaartelling zijn daar voorbeelden van, die nu nog steeds intensief (naast "onze"jaartelling) gebruik worden.

NB Het is niet zo dat in 1582 de Gregoriaanse kalender overal direct ingevoerd werd. Hoe dat gebeurde is een ingewikkelde geschiedenis (zie bv. W. E. van Wijk - Onze kalender. Wereld-Bibliotheek, Amsterdam, 1955). Het is mij b.v. niet duidelijk in welke kalender de

geboortedag van Johann Sebastian Bach 21-III-1685 gerekend is (data ná 1776 zijn in heel **Duitsland** in de gregoriaanse kalender, tussen 1582 en 1776 kan dat van plaats tot plaats verschillen).

1582: Gregoriaanse kalender in **Frankrijk** en **Spanje**,
1752: **Engeland** en de kolonies daarvan,
Rusland: na de revolutie van 1917.

De bovenstaande methode is afkomstig van J. H. Conway. Zie ook H. M. Stark - An introduction to number theory. Markham, 1970, pp. 113 - 116.

11 Appendix E: Het 15-spel

(11.1) Men zegt dat de grote puzzel-expert Sam Loyd (soms gespeld als Sam Lloyd, of Samuel Loyd) 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. Zie [S-Nl-FLT] pag. 154. 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", 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

(11.2) 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?

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.

(11.3) 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 $p(S) = +$.

(11.4) 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:

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

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

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 $p(S) = -$.

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

Conclusie. We zien dat deze situatie zoals beschreven in (11.4) 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 (11.5). 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

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

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

(11.8) 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: $d(S') - d(S) = 7 - 1 = 6$.

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

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

12 Appendix F: RSA

Wiskunde is als zuurstof. Als het er is, merk je het niet.
Als het er niet zou zijn, merk je dat je niet zonder kan.
Lex Schrijver, zie [53], pagina 31.

(12.1) Dit hoofdstuk gaat over *coderingstheorie*. U maakt daar veel gebruik van. Elke keer dat U geld pint wordt de boodschap versleuteld naar de bank gestuurd. Zo kan die boodschap niet ontcijferd worden door mensen die de sleutel niet kennen.

De opgave van coderingstheorie: vind een methode die een bericht versleuteld (en liefst op een manier die publiekelijk bekend is), maar zo dat het ontcijferen (als je een geheim mechanisme niet kent) moeilijk is.

U zult zeggen: als je kunt versleutelen (eindig veel symbolen) dan hoef je toch alleen maar alle mogelijkheden op te schrijven, en terug te zoeken als je wilt ontcijferen. Ja, dat klopt. Maar het is de vraag of dit practisch uitvoerbaar is. Als ik U een dik telefoonboek geef, dan is het gemakkelijk om bij een gegeven naam het bijbehorende telefoonnummer te vinden. Maar, omgekeerd, bij een gegeven telefoonnummer de naam vinden is een enorme klus. Op dit principe berust de RSA publieke-sleutelcrytografie.

In het prachtige boek van Simon Singh hierover vindt U een mooie beschrijving van allerlei coderings-methoden uit het verleden, en ook een beschrijving van RSA, zie [83], §6 en Aanhangsel J. De afkorting RSA staat voor: Ron Rivest - Adi Shamir - Leonard Adleman, de bedenkers van deze cryptografie.

(12.2) Beschrijving van RSA.
Geheim: $p,\ q,\ d$,
Openbaar: N, e.
Een bericht bestaat uit getallen v met $0 \leq v < N$.
Het versleutelde bericht bestaat ook uit getallen w met $0 \leq w < N$.

Hier geldt: de getallen p en q zijn priemgetallen en $N := p{\cdot}q$; verder is $1 < e < N$ met $\text{ggd}(e,(p-1)(q-1)) = 1$ en $1 < d < N$ met $ed \equiv 1 \pmod{(p-1)(q-1)}$.
Versleutelen: $w = \varphi(v)$; voor gegeven v is w bepaald door $w \equiv v^e \pmod{N}$.
Decoderen: $v = \psi(w)$; voor gegeven w is v bepaald door $v \equiv w^d \pmod{N}$.

Omdat N en e openbaar zijn kan versleutelen van een bericht door iedereen gedaan worden. U zult tegenwerpen dat het bepalen van w met de gewenste eigenschappen een hele klus is (in de praktijk is N een heel groot getal); daar heeft U gelijk in, als je het met de hand zou moeten doen, maar met de moderne computer-techniek is dit een fluitje van een cent.

We zullen zien dat φ en ψ bijectieve afbeeldingen zijn van $W = \{0, 1, \cdots, N-1\}$ naar zichzelf, die bovendien elkaars inverse zijn. We zien dat

$$\varphi : W \xrightarrow{\sim} W \quad \text{de afbeelding} \quad \varphi^{-1} = \psi : W \to W$$

eenduidig vastlegt. Met andere woorden, $\psi(\varphi(v)) = v \quad \forall v \in W$: het ontcijferde bericht komt overeen met het oorspronkelijke.

Hoe valt deze code te breken? Bedenk wel dat N heel groot is (denk aan een getal van 400 cijfers). Daarom is de weg:

[φ helemaal uitschrijven, en in dat "telefoonboek"
voor elke w de ontcijferde $\psi(w)$ opzoeken]
practisch niet uitvoerbaar.

Maar als we d zouden weten, dan kunnen we ontcijferen. In de praktijk blijkt dat we voor het vinden van d met de gewenste eigenschappen de factorizatie $N = p{\cdot}q$ in priemfactoren p en q moeten kennen. Hier zit de bottle-neck: het factoriseren van grote getallen is een enorme klus. Het uitproberen van alle factoren $\leq \sqrt{N}$ is practisch onuitvoerbaar. Er zijn algoritmen om getallen de factoriseren. En nu komt er de wedloop: de code is veilig als N niet gefactoriseerd kan worden; zodra de methoden daartoe efficiënter worden, en de rekenmachines sneller, dan past men de codering aan: grotere p en q (die je moet produceren of kopen).

We leggen uit wat de wiskunde is achter deze cryptografie.

Voor $M \in \mathbb{Z}_{>0}$ schrijven we $\mathbb{Z}/M$ voor de verzameling

$$\mathbb{Z}/M = \{\overline{0}, \overline{1}, \cdots \overline{i}, \cdots, \overline{N-1}\}.$$

Dit is een eindige verzameling. Bovendien kunnen we in deze verzameling "optellen", "aftrekken" en "vermenigvuldigen": we voeren deze handelingen uit alsof we in $\mathbb{Z}$ zijn, en reduceren dan weer modulo M.
Voorbeeld: $M = 7$,; dan is $\overline{5} + \overline{4} = \overline{2}$, omdat $5 + 4 = 2 + 7$ en $\overline{2} \times \overline{4} = \overline{1}$, omdat $2 \times 4 = 1 + 7$.

(12.3) Lemma (de Chinese rest-stelling). *Onderstel gegeven $m, n \in \mathbb{Z}_{>0}$ met* $\mathrm{ggd}(m, n) = 1$*; schrijf $N = m{\cdot}n$. De natuurlijke afbeelding*

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

is bijectief.
Opmerking: Dit is ook een afbeelding die verwisselt met $+$ en met $\times$: het is een "homomorfisme".

(12.4) Lemma. *Neem de gegevens als in* RSA*. De afbeelding*

$$\varphi : \mathbb{Z}/N \longrightarrow \mathbb{Z}/N, \quad \textit{gegeven door} \quad w \equiv v^e \pmod{N}$$

is bijectief. Uit $ed \equiv 1 \pmod{(p-1)(q-1)}$ volgt $\psi{\cdot}\varphi = \mathrm{Id}$.

(12.5) Feit. * *Zij p een priemgetal. Beschouw $(\mathbb{Z}/p)^*$, de multiplicatieve groep van eenheden in $\mathbb{Z}/p$. Merk op: $(\mathbb{Z}/p)^* = \{\overline{1}, \cdots, \overline{p-1}\}$. Beschouw $\mathbb{Z}/(p-1)$ met de optelling als structuur; dit is een groep. Er is een isomorfisme van groepen*

$$\mathbb{Z}/(p-1) \quad \xrightarrow{\sim} \quad (\mathbb{Z}/p)^*.$$

Voorbeelden

$$\mathbb{Z}/6 \longrightarrow (\mathbb{Z}/7)^*, \quad i \bmod 6 \mapsto 3^i \bmod 7,$$

en

$$\mathbb{Z}/96 \longrightarrow (\mathbb{Z}/97)^*, \quad i \bmod 96 \mapsto 2^i \bmod 97,$$

zijn isomorfismen.

Suggestie: schrijf het eerste isomorfisme uit voor alle elementen.

(12.6) Opgave.* Bewijs deze lemma's.

We zien dat de gedachte, en de wiskunde achter der RSA-cryptografie verbluffend eenvoudig is.

Voor een prachtige beschrijving van de geschiedenis en allerlei aspecten van coderingstheorieën, zie [83].

13 Appendix G: Sprouts

Er is een wiskundig spel dat "Sprouts" heet. Een vertaling van deze term zou kunnen luiden "spruiten" maar dat kan misverstanden wekken. Bedoeld wordt aan te geven dat er steeds nieuwe loten ontstaan, dat er knoppen opengaan. Hier zal ik de term onvertaald overnemen.

Dit spel werd uitgevonden door M. S. Paterson en J. H. Conway in 1967. Voor een beschrijving zie [7], pp. 564 – 573. Ze ook
`http://en.wikipedia.org/wiki/Sprouts_(game)`

(13.1) Het spel wordt gespeeld door twee spelers A en B, op een vel papier, en elk van de spelers heeft een pen of een potlood. Het spel begint door het plaatsen van een eindig aantal punten op het papier. Dit aantal geven we aan met n. Om beurten doen de spelers een zet:

- een zet bestaat uit het trekken van een lijnstuk (krom of recht) van één van de punten die er dan zijn naar één van die punten (een lus, beginpunt en eindpunt zijn hetzelfde punt, is toegestaan), en het plaatsen van een nieuw punt op het inwendige van dat lijnstuk; Hierbij gelden de volgende regels:
- lijnstukken mogen elkaar niet snijden of raken, behalve in de getekende punten;
- elke nieuw lijnstuk heeft alleen begin- en eindpunt gemeen met de reeds bestaande structuur;
- op elk lijnstuk komt er behalve begin- en eindpunt precies één nieuw punt;
- in elk punt komen hooguit drie einden van lijnstukken samen; gevolg: bij een nieuw punt kan er nog maar hooguit één eindpunt van een nieuw lijnstuk komen.
- Winnaar is de speler die de laatste legitieme zet doet.

Opmerking. Er zijn allerlei varianten van dit spel. Bij voorbeeld kan men afspreken ("misère play") dat de speler die de laatste legitieme zet doet verliest.

(13.2) Opgave. Laat zien dat bij een begin situatie met n punten voor het aantal zetten m in een spel dat klaar is er geldt:

$$2n \leq m \leq 3n - 1.$$

Merk op, allicht: de tweede speler, die we B noemen, wint dan en slechts dan als m even is.

Omdat elk spel een winnaar heeft, is er voor elke keuze van n óf geforceerde winst voor A óf geforceerde winst voor B (maar je kunt gemakkelijk niet optimaal spelen, en geforceerde winst uit handen geven).

Eenvoudig: voor $n = 1$ bestaat het spel uit 2 zetten, en B wint

(13.3) Voorbeeld / Opgave. Neem $n = 2$. Geef een lijst van alle mogelijkheden van de volgorde van de zetten in dit geval. Bewijs dat B in het geval $n = 2$ winst kan forceren.

(Er zijn 19 spelverlopen mogelijk in dit geval, 14 gewonnen door A, en 5 met winst voor B; allebei "willekeurig spelen" geeft A een grotere winst kans, maar B kan winst forceren. Zie Fig. 6 on page 565 van [7].)

(13.4) Open probleem. Voor een aantal gevallen (n klein) is het bekend welke van de twee spelers winst kan forceren. Maar dat is niet bekend voor alle n.
Vermoeden (D. Applegate, G. Jacobson & D. Sleator, 1991).

$$A \text{ kan winst forceren} \quad \stackrel{?}{\Longleftrightarrow} \quad n \equiv 3, 4, 5 \pmod 6.$$

$$B \text{ kan winst forceren} \quad \stackrel{?}{\Longleftrightarrow} \quad n \equiv 1, 2, 6 \pmod 6.$$

`http://www.cs.cmu.edu/ sleator/papers/sprouts.pdf`

(13.5) Oplossing van (13.2). Zie [7], pp. 564, 567. We noemen een leven van een punt een mogelijk einde van een lijnstuk dat daar nog aan vastgehecht mag worden. Een punt dat nog nergens mee verbonden is heeft 3 levens. De begin situatie heeft $3n$ levens. Bij elke zet gaan er twee levens verloren (de eind punten van het lijnstuk), en komt er een leven bij (vanuit het nieuwe punt). We zien dat elke zet het totaal aantal levens met één vermindert. Na de laatste zet is nog minstens één leven over (gehecht aan het laatst toegevoegde punt). Conclusie: $m \leq 3n-1$. Pro memorie: we bewezen dat het het aantal levens ℓ in de eindsituatie gelijk is aan $\ell = 3n - m$.

We noemen een punt in de eind situatie een dood punt als er 3 uiteinden van een lijnstuk aan vast gehecht zijn, en anders noemen we het punt levend. Voor elk levend punt L in de eind situatie geven we de twee dichtstbijzijnde buren aan door $bL = \{P, P'\}$. We zien (omdat we in een eind situatie zitten):

bij gegeven levend punt L zijn er precies twee dichtsbijzijnde buren;

die punten P en P' zijn dood,

en elk dood punt kan maar op hooguit één manier optreden in een bL.

Een dood punt dat niet in een bL voorkomt noemen we een uithoek, "Pharisee" op [7], p. 567. Het aantal uithoeken in de eind situatie geven we aan met u. Er volgt:

$$u = (n + m) - (\ell + 2\ell) = (n - m) - 3(3n - m) = 4m - 8n.$$

Conclusie: u een veelvoud is van 4, en $u \geq 0$ geeft $m \geq 2n$.

14 Appendix H: Enkele notaties en symbolen

Wiskundigen gebruiken sommige notaties, symbolen. Die zijn bedoeld als stenografie. Ze geven een snelle en preciese 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.

(14.1) 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.

(14.2) 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.

(14.3) 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.

(14.4) Gehele getallen. Met $\{z \mid \cdots\}$ geven we aan de verzameling van alle elementen z die voldoen aan de restricties rechts van $|$.
Voorbeeld: met $\{n \mid n \text{ is een geheel getal}\}$ 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.

(14.5) 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 $n/1 \in \mathbb{Q}$.

(14.6) *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 m^2 is *even*. Het aantal factoren 2 in n^2 is *oneven*. Dit is een tegenspraak. Dit 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.

We kunnen nog en algemener getal begrip invoeren. Dit kunnen we doen door bij voorbeeld de verzameling van alle decimale breuken te beschouwen, waar we oneindig veel decimalen achter de komma toelaten. 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 $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

(14.7) Opmerking. Getallen die beschreven kunnen worden als oplossing van een polynoom-vergelijking worden *algebraïsche getallen* genoemd. Gebruikmakend van het begrip *aftelbaarheid*, zie (14.8), 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 (14.9), 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.*

(14.8) 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 (14.9). Hier is dat principe zoals dat door Cantor ontwikkeld werd. Bij voorbeeld zie
http://en.wikipedia.org/wiki/Cantor's_diagonal_argument

(14.9) 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

(14.10) 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: $\{x \mid x \in \mathbb{Z},\ \ x \geq 0\} \cap \{x \mid x \in \mathbb{Z},\ \ x \leq 0\} = \{0\}$,
$\{x \mid x \in \mathbb{Z},\ \ x \geq 0\} \cup \{x \mid x \in \mathbb{Z},\ \ x \leq 7\} = \mathbb{Z}$.

(14.11) 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.

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.

(14.12) $\exists$: er betaat/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: $(a \equiv 0 \pmod{2}) \Longleftrightarrow (a \text{ is even})$.

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

Veronderstel dat $a_1, \cdots, a_n$ getallen zijn. De som daarvan wordt genoteerd als

$$\sum_{1 \leq i \leq n} a_i := a_1 + \cdots + a_n.$$

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;
$\Longrightarrow$ logische implicatie; $\Longleftrightarrow$ logische equivalentie;
:= links wordt gedefiniëerd door middel van wat er rechts staat;
$a \equiv b \pmod{c}$ "a is equivalent met b modulo c".

15 Appendix I: Enkele 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 1180s - 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-Nl-FLT] 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)

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 Valle Poussin (België, 1866 - 1962)

Godfrey Harold G. H. 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 Grothendieck (Duitsland, Frankrijk, 1928)

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)

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)

16 Een paar puzzels

(16.1) Puzzel. Een lp. Daphne heeft een lp (of elpee, of langspeelplaat) in haar hand, en ze vraagt aan Wesley: hoeveel groeven heeft deze grammofoonplaat? Wat is het antwoord?

(16.2) Puzzel. Een boeken-wurm. Johan is student Arabisch, en hij heeft een prachtig Arabisch boek in 5 delen gekocht. Thuis gekomen zet hij deze 5 boeken op de plank, natuurlijk zoals het hoort. Hij kijkt ernaar als hij de ruggen van de 5 boeken ziet, deel 1 rechts, daarnaast deel 2, en tenslotte deel 5 helemaal links. Behalve de kaften heeft elk deel 200 pagina 's (de titel pagina en de lege pagina's meegeteld). Maar, er zit tussen het kaft en de eerste pagina van deel 1 een Boekenwurm. En die knaagt rechtdoor, tot hij aangeland is tussen het kaft en de laatste pagina van deel 5.
-- Hoeveel gaten zitten er in de kaften?
-- Hoeveel bladzijden hebben een gat?
(We zeggen hier pagina voor een kant van een bladzijde; een bladzijde hier is een vel papier; elk boek hierboven heeft 200 pagina's, en dus 100 bladzijden in onze terminologie. Elk boek heeft een voor-kaft en een achter-kaft.)

(16.3) Puzzel. Bepaal het laatste cijfer van 7^{511} in decimale schrijfwijze.

(16.4) Puzzel. Is dit een kwadraat ? Is het getal 87618160696635058683 het kwadraat van een geheel getal?
[Nadenken is vaak beter dan het gebruik van een rekenmachine.]

(16.5) Puzzel. Is dit een een kwadraat ? Is het getal 3339590081146975295 het kwadraat van een geheel getal?
[Nadenken is vaak beter dan het gebruik van een rekenmachine.]

(16.6) Puzzel. Is dit een kwadraat ? Is het getal $C = 1156553944297325629695$ het kwadraat van een geheel getal?
[Nadenken is vaak beter dan het gebruik van een rekenmachine.]

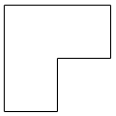
(16.7) Puzzel. Wat zijn de rationale punten op deze kromme ? Beschrijf alle $(x, y) \in \mathbb{Q} \times \mathbb{Q}$ zodanig dat

$$(E) \qquad y^2 = x^3 - 4x^2 + 5x - 2.$$

(16.8) Puzzel. Wat zijn de gehele oplossingen? Bewijs dat er niet een paar $(x, y) \in \mathbb{Z}^2$ bestaat zodanig dat

$$x^3 + y^4 = 2613527.$$

(16.9) Puzzel. Is een dergelijke betegeling mogelijk? Gegeven is $N \in \mathbb{Z}_{>0}$. Gegeven is een vloer van afmeting $3 \times N$. Verder zijn er N tegels gegeven die de vorm hebben van een 2×2 vierkant waar een 1×1 vierkant uitgeknipt is:



Bewijs:
(3e) Als N even is, dan is betegeling mogelijk.
(3o) Als N oneven is, dan is betegeling niet mogelijk.

(16.10) Puzzel. Een pad in de 4-dimensionale ruimte. In de 3-dimensionale ruimte zijn gegeven:
een boloppervlak S door de vergelijking $X^2 + Y^2 + Z^2 = 1$,
een punt P binnen de bol: $P = (0, 0, 0)$,
en een punt Q buiten de bol: $Q = (2, 0, 0)$.
We bedden de ruimte in in een 4-dimensionale ruimte door een punt $Z = (x, y, z)$ af te beelden op $Z' = (x, y, z, 0)$.
Geef een pad in de 4-dimensionale ruimte dat begint in P', het oppervlak S' niet snijdt, en eindigt in het punt Q'.
[Een pad van A naar B in een ruimte R: een continue afbeelding van het interval $[0, 1]$ naar R, die 0 op A en 1 op B afbeeldt: in de tijd die loopt van 0 naar 1 ''loop'' je van A naar B zonder sprongen te maken.]

(16.11) Puzzel. 3 deuren. Bij een quiz krijgt de candidaat 3 deuren te zien. Achter één daarvan is een auto, die je kunt winnen als je in tweede instantie die deur laat openen. (En, de folklore wil, dat achter de andere deuren een geit zit; maar misschien wil je wel liever een geit dan een auto winnen ..?) Je wijst één van de drie deuren aan, de quizmaster opent een andere deur, om te laten zien dat daar de auto niet staat, en vraagt of je bij de oorspronkelijke keus blijft, of dat je wilt veranderen. Wat is de beste strategie? (Deze puzzel wordt wel ''de mekkerende geit genoemd.'')

(16.12) Puzzel. 3 deuren en een echtpaar. (Hier is een variant op het welbekende vraagstuk hierboven, dat veel stof heeft doen opwaaien.)
Een echtpaar mag proberen een auto te winnen. Er zijn drie deuren, met daarachter een auto, een autosleutel, of een geit - n per deur natuurlijk. De man moet de auto vinden, de vrouw de autosleutel. Alleen als ze beiden slagen krijgen ze de auto mee.
Eerst mag de man proberen de auto te vinden. Hij krijgt twee kansen. Hij opent een deur en als daar de auto niet staat mag hij nog een deur proberen. Kans van twee op drie volgens Bartjens. Intussen is zijn vrouw elders. De deuren worden weer dicht gedaan, de man wordt afgevoerd en nu mag de vrouw proberen om de sleutel te vinden. Ook zij mag twee deuren openen. Weer kans van twee op drie volgens Bartjens.
Het echtpaar mag van tevoren overleggen, maar er is geen contact tussen ze zodra het spel begonnen is. Nu komt het ongelofelijke: Ze kunnen een strategie afspreken die een kans van twee op drie op de auto levert!
Wie ziet hoe het echtpaar moet spelen?

(16.13) Puzzel. Deelbaar door 7. Bewijs dat het getal $2222^{5555} + 5555^{2222}$ deelbaar is door 7.
http://www.vierkantvoorwiskunde.nl/puzzels/db.html

(16.14) Puzzel. Van Cardano aan Del Fiore.

Een ton is met pure wijn gevuld. Iedere dag haalt men er twee emmers uit, die vervangen worden door twee emmers water. Na zes dagen is de helft wijn en de andere helft water. Wat is (ongeveer) de inhoud van de ton?

(16.15) Oplossing van groeven op een lp (16.1). Een lp heeft twee kanten, en aan elke kant één groef.

(16.16) Oplossing van (16.2): de boeken-wurm. Arabische boeken beginnen op de meest rechtse pagina, en gaan door (precies andersom als ‘‘onze boeken’’) tot de laatste pagina, de meest linkse als je het boek openslaat. De wurm begint tussen (Arabische voor-)kaft en pagina 1 van deel 1, en eindigt tussen (Arabische achter-)kaft en pagina 200 van deel 5. Daarbij zijn er 300 bladzijden doorgeknaagd, de bladzijden van deel 1, en de bladzijden van deel 5 blijven heel. Daarbij zijn er 8 kaften doorgeknaagd.
Opmerking. De analoge puzzel voor een boek in 5 delen met ‘‘onze’’ manier van pagineren geeft hetzelfde antwoord; mee eens?

(16.17) Oplossing laatste cijfer (16.3). Merk op dat $7^3 = 343$, $7^4 = 2401$ en $511 \equiv 3 \pmod 4$. Dus $7^{511} \equiv 7^3 \pmod{10}$ en we zien $7^{511} \equiv 3 \pmod{10}$.

(16.18) Oplossing is dit een kwadraat (16.4): niet een kwadraat. Kwadraten van gehele getallen geschreven als 10-talig cijfer, eindigen op een 0, 1, 4, 5, 6 of 9. We zien dat een getal dat eindigt op een 3 niet een kwadraat is.
Mijn rekenmachine geeft $\sqrt{87618160696635058683} = 9360457291$. Is dat antwoord goed? Nadenken is vaak beter dan het gebruik van een rekenmachine.

(16.19) Oplossing van (16.5): niet een kwadraat. We zien dat

$$3339590081146975295 \equiv 6 \pmod 9.$$

Daarom is dit getal wel deelbaar door 3, maar niet deelbaar door 9. In de priemfactorontbinding van dit getal komt 3^1 voor, en niet 3^2; dus is dit getal niet een kwadraat.

Andere oplossing: laat zien dat het getal wel door 5, maar niet door 25 deelbaar is.
Mijn rekenmachine geeft $\sqrt{3339590081146975295} = 1827454536$. Is dat antwoord goed? Nadenken is vaak beter dan het gebruik van een rekenmachine.

(16.20) Oplossing van (16.6): niet een kwadraat. We zien dat

$$1156553944297325629695 \equiv 2 \pmod{11}.$$

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

Merk op dat $C \equiv 5 \pmod{10}$ en $C \equiv 0 \pmod 9$.

Andere oplossing: laat zien dat het getal wel door 5, maar niet door 25 deelbaar is.
Mijn rekenmachine geeft $\sqrt{1156553944297325629695} = 34008145264$. Is dat antwoord goed? Nadenken is vaak beter dan het gebruik van een rekenmachine.

(16.21) Oplossing rationale punten op een kromme (16.7). (We gebruiken dat dit een singuliere kromme geeft.) Het antwoord is:

$$\{(1,0)\} \cup \{(x = \alpha^2 + 2,\ \ y = \alpha(\alpha^2 + 1)) \mid \alpha \in \mathbb{Q}\}.$$

Bewijs. Voor elk punt $P = (x, y) \neq (1, 0)$ kiezen we de lijn die P verbindt met $S := (1, 0)$; merk op: als $(x, y) \neq S$ voldoet aan (E) dan is $x \neq 1$. Die lijn wordt gegeven door de vergelijking

$$(L) = (L_\alpha) \qquad y = \alpha \cdot (x - 1).$$

Merk op dat

$$x^3 - 4x^2 + 5x - 2 = (x - 1)^2(x - 2).$$

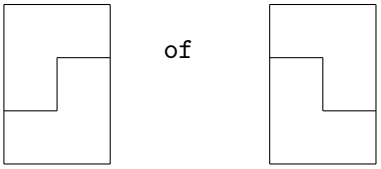
Substitutie van (L) in (E) geeft:

$$(\alpha \cdot (x - 1))^2 = (x - 1)^2(x - 2).$$

Uit $\alpha^2 = x - 2$ volgt $x = \alpha^2 + 2$. Met (L) geeft dit $y = \alpha(\alpha^2 + 1)$. We zien dat elk van de gevraagde punten ongelijk aan S een eenduidig bepaalde α geeft, en dat elke $\alpha \in \mathbb{Q}$ de lijn $(L) = (L_\alpha)$ geeft, die behalve het S ook het punt $(x = \alpha^2 + 2,\ \ y = \alpha(\alpha^2 + 1))$ geeft.

(16.22) Oplossing gehele getallen (16.8). Merk op dat $261352 \equiv 7 \pmod{13}$.
We bewijzen dat er niet een oplossing bestaat in $(\mathbb{F}_{13})^2$.
De derde-machten in $\mathbb{F}_{13}$ zijn de restklassen van $0, \pm 1, \pm 8$ in $\mathbb{F}_{13}$.
De vierde-machten in $\mathbb{F}_{13}$ zijn de restklassen van $0, 1, 3, 9$ in $\mathbb{F}_{13}$.
We zien dat de restklasse van 7 niet van de vorm $\overline{x}^3 + \overline{y}^4$ geschreven kan worden met $\overline{x}, \overline{y} \in \mathbb{F}_{13}$.
Dus is er geen oplossing in $(\mathbb{F}_{13})^2$. Dus is er geen oplossing in $\mathbb{Z}^2$.

(16.23) Oplossing betegelen (16.9) Twee tegels kunnen aaneen gelegd worden tot een 3×2 patroon.



Als $N = 2n$ dan vullen n van zulke patronen een $3 \times 2n$ vloer.
Oplossing (3o). De uitspraak is waar voor $N = 1$: één tegel van deze vorm kan niet een vloer van afmeting 3×1 betegelen. We gaan verder met inductie van $N - 2$ naar N. Als een betegeling mogelijk is, dan wordt de linker-bovenhoek belegd, en ook de linker-onderhoek. Dit bewijst dat de linker twee tegels in een betegeling een 3×2 patroon vormen. Als betegeling in het geval $N - 2$ niet gaat, dan volgt dat ook betegeling in het geval N niet mogelijk is.

(16.24) Oplossing van (16.10): een pad. Als ik de vraag gesteld had over een cirkel in een vlak in de 3-dimensionale ruimte, en een pad van een punt A binnen die cirkel naar een punt B buiten de cirkel, dan ziet iedereen wat je moet doen. Van 0 tot $1/3$ naar boven, dan van $1/3$ tot $2/3$ horizontaal lopen tot je boven B bent, dan van $2/3$ tot 1 naar beneden lopen tot je in B bent.

Imiteer dit tot een oplossing van ons vraagstuk volgt: van 0 tot $1/3$ lopen van $P' = (0,0,0,0)$ naar $(0,0,0,1)$, van $1/3$ tot $2/3$ van $(0,0,0,1)$ naar $(2,0,0,1)$ (ga na dat bij de vierde coödinaat constant $= 1$ dit pad S' niet snijdt), van $2/3$ tot 1 van $(2,0,0,1)$ naar $(2,0,0,0)$.

(16.25) Oplossing van (16.11): 3 deuren. Bij niet-veranderen is de kans 1/3 dat je de auto wint. Laat zien dat bij wel veranderen de kans 2/3 is. Conclusie: veranderen vergroot de kans. Bewijs. Als je de deur aanwijst waar de auto achter staat, en je verandert, dan krijg je de auto niet. Als je een van de twee andere deuren aanwijst, en je verandert, dan krijg je de auto wel. Dus: bij veranderen is de kans 2/3 dat je de auto wint.

(16.26) Oplossing van (16.12): 3 deuren en een echtpaar. Als je een willekeurige deur aanduidt heb je een kans van 1 op 3 dat het geitje daar zit. M.a.w. als je twee deuren aanduidt heb je een kans van 2 op 3 dat je het geitje niet vindt. In dat geval heb je zowel de auto als de sleutel. Het echtpaar moet dus gewoon afspreken welke deur ze geen van beiden zullen openen om een kans van 2 op 3 te hebben op de auto en de sleutel.

Als je een willekeurige deur aanduidt heb je een kans van 1 op 3 dat het geitje daar zit. M.a.w. als je twee deuren aanduidt heb je een kans van 2 op 3 dat je het geitje niet vindt. In dat geval heb je zowel de auto als de sleutel. Het echtpaar moet dus gewoon afspreken welke deur ze geen van beiden zullen openen om een kans van 2 op 3 te hebben op de auto en de sleutel.

(16.27) Oplossing: deelbaar door 7: (16.13). Voor voor elk priemgetal p en elke $a \in \mathbb{Z}$ niet deelbaar door p geldt $a^{p-1} \equiv \pmod p$. Ga na:

$$2222 = 317 \times 7 + 3, \quad 5555 = 925 \times 6 + 5, \quad 5555 = 793 \times 7 + 4, \quad 2222 = 370 \times 6 + 2.$$

Daarom:

$$2222 \equiv 3 \pmod 7, \quad 5555 \equiv 5 \pmod 6, \quad \text{dus} \quad 2222^{5555} \equiv 3^5 \pmod 7;$$

omdat $3^5 \equiv 5 \pmod 7$ geeft dit $2222^{5555} \equiv 5 \pmod 7$;

$$5555 \equiv 4 \pmod 7, \quad 2222 \equiv 2 \pmod 6, \quad \text{dus} \quad 5555^{2222} \equiv 4^2 \pmod 7;$$

omdat $4^2 \equiv 2 \pmod 7$ geeft dit $5555^{2222} \equiv 2 \pmod 7$;.
Hieruit volgt het resultaat.

(16.28) Oplossing van (16.14): de inhoud van een ton. Stel: inhoud ton $= x$. Het water van de eerste dag is na 6 dagen gelijk aan $\frac{x-1}{x} \times \frac{1}{x}$, etc. Al het water na 6 dagen is

$$((\frac{x-1}{x})5 + \cdots + \frac{x-1}{x})1 + 1) \times \frac{1}{x} =$$

$$= (\frac{x-1}{x})^6 - 1)/(\frac{x-1}{x}) - 1) \times \frac{1}{x} =$$
$$= (\frac{x-1}{x})^6 - 1)/(-1) = 1 - (\frac{x-1}{x})^6.$$

Omdat gegeven is dat $1 - (\frac{x-1}{x})^6 = 1/2$ volgt $x = \sqrt[6]{2}(x-1)$; dus

$$x = \sqrt[6]{2}/(\sqrt[6]{2} - 1) \approx 9.165795149.$$

(zie [35], p.306)

(16.29) Oplossing van (9.11). 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.

(16.30) Oplossing van (9.12). Omdat $10 \equiv -1 \pmod{11}$ geldt $n \equiv a(n) \pmod{11}$. Herhaald toepassen hiervan geeft het resultaat.

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

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

Bewijs: 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 zal ik een oplossing bespreken. Graag hoor ik hoe iemand er aan begint, en wat voor bewijs er uit komt.)

De onderstaande literatuur lijst bevat veel meer dan wat we nodig hebben. Maar ik dacht dat het goed is dat u voldoende verwijzingen heeft om nog heel lang veel pleizier te hebben. Een deel van dit materiaal hier beneden is niet elementair. Hier volgen wat aanwijzingen.

Elementaire getal theorie en algebra.
In het boek [37] vinden we veel materiaal over algebra en getal theorie; zeer aanbevolen. Zie ook [10].
Algebra (meer geavanceerd): [93] (een klassieker), [47] (geavanceerd, nogal volledig).

Elliptische krommen.
Op veel internet sites vinden we prachtige artikelen. Zie b.v.
http://en.wikipedia.org/wiki/Elliptic_curve
of zoek met Google. Er zijn veel inleidende en gedegen boeken over dit onderwerp.

Het boek [81] is prachtig en redelijk elementair. De boeken [79] en [80] compleet, maar niet elementair. De boeken [12], [41], [52] geven prachtige overzichten, deels elementair. Zie ook [86].

Congruente getallen.
Zie [15], [62], [63] (met veel literatuurverwijzingen).

Het Poncelet probleem.
Zie [9], [24].

Romans.
Er zijn veel boeken waar wiskundigen als hoofdpersoon opgevoerd worden. Ik bedoel niet biografiën, maar fictie. Daar zijn juweeltjes onder. Zie:

[19], een prachtige beschrijving van iemand die het Goldbach vermoeden probeert op te lossen;

[57], een fascinerende beschrijving van de jonge jaren van Sophie Germain; ik vond dit erg mooi;

[40], een bestseller, een fictieve beschrijving van een ontmoeting, die echt heeft plaats gevonden, tussen de wiskundige Carl Friedrich Gauss (1777 -- 1855) en Alexander von Humboldt (1769 --1859); ik vond dit een vreselijk boek; zie de boekrecensie
http://www.ams.org/notices/200806/tx080600681p.pdf;

[35], een vermakelijk boek; voor een boekrecensie zie:
http://www.nieuwarchief.nl/serie5/deel01/mrt2000/pdf/papegaai.pdf

[48], een magistrale beschrijving van het universitaire leven in Cambridge, UK, in de eerste helft van de 20-ste eeuw, en van S. Ramanujan die daar komt werken met G. H. Hardy; voor een boekrecensie zie:
http://www.nytimes.com/2007/09/16/books/review/Freudenberger-t.html

Een vraag die me bezig houdt: is het toegestaan om in fictie een persoon op te voeren die bestaan heeft, herkenbaar is in de beschrijving, terwijl historische gegevens of karakter eigenschappen duidelijk anders wrden

weergegeven dan aantoonbaar juist? Sommige mensen vinden dat in fictie alles toegestaan is wat dat betreft. Graag hoor ik Uw mening!

Referenties

[1] Anonymous Arab manuscript (before 972) in the Imperial Library of Paris. French translation by F. Woepcke: *Recherches sur plusieurs ouvrages de Léonard de Pise.*
III: *Traduction d'un fragment anonyme sur la formations des triangles rectangles en nombres entiers, et d'un traité sur je même sujet par Aboū Dja'far Mohammed Ben Alhoçain.* Vol. **14** pp 211 -- 227, 241 -- 269, 301 -- 324, 343 -- 356.
Also published: F. Woepcke -- *Études sur les mathématiques Arabo-Islamiques.* Band II. Nachdruck aus den Jahren 1842 -- 1974. Herausgegeben von Fust Sezgin. Inst. Geschichte Arabisch-Islamischen Wissensch., Goethe-Universität, Frankfurt am Main, 1986.

[2] R. Alter -- *The congruent number problem.* American Math. Monthly **87** (1980), 43 -- 45.

[3] A. Anbouba -- *Un traité d'Abu Ja'fa* [al-Khazin] *sur les trangles rectangle numériques.* Journal for the history of Arabic sciences. Vol **3** (1979), 134 -- 156.

[4] L. Bastien -- *Nombres congruents.* Intermédiare des Math. **22** (1915), 231 -- 232.

[5] A. H. Beiler -- *Recreations in the theory of numbers: The queen of mathematics untertains.* Dover Publ., pocket, 1964.

[6] E. Bell -- *Men of mathematics.* Simon & Schuster. 1937.

[7] E. Berlekamp, J. Conway & R. Guy -- *Winning ways for mathematical plays.* Volume 2: games in particular. Academic Press, 1982.
http://homepages.math.uic.edu/ kauffman/Conway.pdf

[8] B. Birch & H. Swinnerton-Dyer -- *Notes on elliptic curves II.* Journ. reine angew. Math **218** (1965), 79-108.

[9] H. Bos, C. Kers, F. Oort & D. Raven -- *Poncelet's closure theorem.* Expos. Math. **5** (1987), 269 -- 364.

[10] D. Burton -- *Elementary number theory.* Allyn & Bacon, 1980.

[11] J. Cassels -- *Diophantine equations with special reference to elliptic curves.* Survey article. Journ. London Math. Soc. **41** (1966), 193 -- 291.

[12] J. Cassels -- *Lectures on elliptic curves.* London Mathematical Society Student Texts, 24. Cambridge University Press, Cambridge, 1991.

[13] V. Chandrasekar -- *The congruent number problem.* Resonance August 1998, 33 -- 45.

http://www.ias.ac.in/resonance/Aug1998/pdf/Aug1998p33-45.pdf

[14] J. Coates & A. Wiles -- *On the Conjecture of Birch and Swinnerton-Dyer.* Invent. Math. **39** (1977), 223-251.

[15] J. Coates -- *Congruent number problem.* Quarterly Journal of pure and Applied Mathematics **1** (2005), 14 -- 27.

[16] H. Darmon, F. Diamond & R. Taylor -- *Fermat's Last Theorem.* In: Curr. Developments in Math., 1995. Internat. Press, Harvard Univ.

[17] B. Datta & A. Singh -- *History of Hindu mathematics.* Asia Publ. House, Part I: 1935, Part II: 1938, Single volume edition: 1962.

[18] L. Dickson -- *History of the theory of numbers.* Volume II: Diophantine analysis. Chelsea publ. Cy. New York, 1952.

[19] A. Doxiadis -- *Oom Petros en het vermoeden van Goldbach.* De Bezige Bij, 2000. Voor een bespreking van dit boek zie:

http://www.math.leidenuniv.nl/ naw/serie5/deel02/mrt2001/pdf/goldbach.pdf

[20] H. Edwards -- *Fermat's last theorem. A genetic introduction to algebraic number theory.* Grad. Texts Math. 50, Springer -- Verlag, 1977.

[21] N. Elkies -- *Curves $Dy^2 = x^3 - x$ of odd analytic rank.* Proceedings of ANTS-5, 2002 (C.Fieker and D.R.Kohel, eds.), Lecture Notes in Computer Science 2369, pp. 244-251.

[22] *Leonhard Euler und Christian Goldbach, Briefwechsel, 1729 – 1764.* Consult the book with correspondence og Euler, editors A. P. Juškevič & E. Winter. Berlin 1965.

[23] G. Faltings -- *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), 349-366. (see Erratum Invent. Math. 75 (1984).)

[24] L. Flatto -- *Poncelet's theorem.* A.M.S., 2009.

[25] G. Frey -- *Some aspects of the theory of elliptic curves over number fields.* Expos. Math. 4 (1986), 35 - 66

[26] G. Frey -- *Links between stable elliptic curves and certain Diophantine equations.* Ann. Univ. Sarav. Ser. Math. 1 (1986), 1 -- 40.

[27] 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 -- Verlag 1989, pp. 31-62.

[28] A. Fröhlich & M. Taylor -- *Algebraic number theory.* Cambridge Std. Advanc. Math. 27, Cambridge Univ. Press, 1991.

[29] Leonardo Pisano Fibonacci -- *The book of squares.* An annotated translation into modern English by L. E Sigler. Academic Press, 1987.

[30] D. Fowler & E. Robson -- *Square root approximations in old Babylonian mathematics.* YBC 7289 in context, Historia Math. **25** (1998), 366-378.

[31] M. Gardner -- *Mathematical games.* Scientific American, 1977, 101 -- 121.

[32] M. Gardner -- *Penrose tiles to trapdoor ciphers.* W. H. Freeman & Cy, New York 1987.

[33] M. Gardner -- *The Colossal Book of Mathematics.* W. W. Norton & Co 2001. Chapter 7: ‘‘Penrose Tiles’’.

[34] G. Giorello & C. Sinigaglia -- *Fermat. De meester van de moderne mathematica.* NWT, Veen Magazines, 2006; ISBN: 9076988889.
Oorspronkelijk titel: ‘‘Fermat -- i sogni di un magistro all’origine della matematica moderna.’’

[35] 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,

[36] R. Guy -- *Unsolved problems in number theory.* Springer -- Verlag, 3rd Edition 2004.

[37] 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.

[38] T. Heath -- *A history of Greek mathematics.* Oxford, Clarendon Press, 1921.

[39] Y. Hellegouarch -- *Invitation to the mathematics of Fermat-Wiles.* Academic Press, 2002.

[40] D. Kehlmann -- *Die Vermessung der Welt.* Rowohlt 2005 (ook vertaald in het Engels, in het Nederlands en...).

[41] A. Knapp -- *Elliptic curves.* Math. Notes 40, Princeton Univ. Press, 1992.

[42] N. Koblitz -- *Introduction to elliptic curves and modular forms.* Grad. Texts Math. 97, Springer -- Verlag, 1984.

[43] G. Kramarz -- *All congruent numbers less than 2000.* Math. Ann. **273** (1986), 337 -- 340.

[44] D. Kubert -- *Universal bounds on the torsion of elliptic curves.* Proc. London Math. Soc. **33** (1976), 193 - 237.

[45] S. Lang -- *Die abc-Vermutung.* El. Math. 48 (1993), 89 -- 99.

[46] S. Lang -- *Algebraic number theory.* Grad. Texts Math. 110, Springer Verlag, 1986.

[47] S. Lang -- *Algebra.* Addison -- Wesley Publ. Cy, 1965. Third edition. Addison-Wesley Publ. Cy, 1993.

[48] D. Leavitt -- *The Indian clerk.* Bloomsbury, 2007.

[49] B. Mazur -- *Rational isogenies of prime degree* (with an appendix by D. Goldfeld). Invent. Math. 44 (1978), 129 - 162.

[50] B. Mazur -- *Number theory as a gadfly.* Amer. Math. Monthly 98 (1991), 593-610.

[51] B. Mazur & J. Tate -- *Points of order* 13 *on elliptic curves.* Invent. Math. 22 (1973/74), 41 - 49.

[52] J. Milne -- *Elliptic curves.* Kea books. BookSurge Publishers, Charleston, SC, 2006.

[53] B. Mols -- *Opgelost. Toepassingen van wiskunde en informatica.* Veen Magazines, 2006; ISBN: 10-9085710286

[54] P. Monsky -- *Mock Heegner points and congruent numbers.* Math. Zeitschrift **204** (1990), 45-67.

[55] L. Mordell -- *On the rational solutions of indeterminate equations of the third and the fourth degree.* Proceed. Cambridge Philosoph. Soc. **21**. 1922/1923, 179 -- 192.

[56] L. Mordell -- *Diophantine equations.* Pure and Applied Mathematics, Vol. 30 Academic Press, 1969.

[57] D. Musielak -- *Sophie's diary: a historical fiction.* AuthorHouse (April 16, 2004).

[58] A. Néron -- *Propriétés arithmétiques de certaines familles de courbes algébriques.* Proceedings of the International Congress of Mathematicians, 1954, Amsterdam, Vol. III, pp. 481 - 488, Noordhoff N.V., Groningen; North-Holland Publishing Co., Amsterdam, 1956.

[59] O. Neugebauer and A. Sachs -- *Mathematical Cuneiform Texts.* New Haven, CT., 1945.

[60] J. Oesterlé -- *Nouvelles approaches du "théorème"de Fermat.* Sém. Bourbaki **40** (1987/88), Exp. 694. Astérisque 161-162 (1988), 165-186.

[61] 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.

[62] 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.

[63] F. Oort -- *Congruente getallen.* Syllabus bij de Kaleidoscoop voordracht 10 -- II -- 2009. http://www.staff.science.uu.nl/ oort0109/
Zie voor verdere literatuurverwijzingen daarin.

[64] E. Picutti -- *Sui numeri congruo-congruenti di Leonardo Pisano.* Physis **23** (1981), 141 -- 170.

[65] K. Plofker -- *Mathematics in India.* Priceton Univ. Press, 2008.

[66] K. Ribet -- *From the Taniyama-Shimura conjecture to Fermat's last theorem.* Ann. Fac. Sc. Univ. Toulouse 11 (1990), 116-139.

[67] K. Ribet -- *Wiles proves Taniyama's conjecture; Fermat's last theorem follows.* Notices A.M.S. 40 (1993), 575-576.

[68] H. Riesel -- *Prime numbers and computer methods for factorization.* Progress Math. 57, Birkhäuser, 1985.

[69] K. Rosen -- *Elementary number theory and its applications.* Addison Wesley, 2000.

[70] K. Rubin & A. Silverberg -- *Ranks of elliptic curves.* Bull. AMS (New Series) **39** (2002), 455 -- 474.

[71] 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

[72] E. Selmer -- *The diophantine equation* $ax^3+by^3+cz^3=0$. *Completion of the tables.* Acta Math. **92** (1954), 191 -- 197.

[73] J-P. Serre -- *Nombre de points des courbes algébriques sur* $\mathbb{F}_q$. Sém. de Théorie des Nombres de Bordeaux , Exp. no. 22. (= Oeuvres III, No. 129, pp. 664-668), (1982/83).

[74] J-P. Serre -- *Sur les représentations modulaires de degré* 2 *de Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Math. Journ. **54**, (1987), 179-230.

[75] J-P. Serre -- *Lectures on the Mordell-Weil theorem.* Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt. Aspects of Mathematics, E15. Friedr. Vieweg & Sohn, Braunschweig, 1989.

[76] J-P. Serre -- *Topics in Galois theory.* Lecture notes prepared by Henri Darmon. With a foreword by Darmon and the author. Research Notes in Mathematics, 1. Jones and Bartlett Publishers, Boston, MA, 1992.

[77] J. Sesiano -- *Books IV to VII of Diophantus' Arithmetica.* Sources Hist. Math. Phys. Sciences **3**. Springer -- Verlag 1982.

[78] D. Shanks -- *Solved and unsolved problems in number theory.* Chelsea Publ. Cy., 1978.

[79] J. Silverman -- *The arithmetic of elliptic curves.* Grad. Texts Math. 106, Springer -Verlag, 1986.

[80] J. Silverman -- *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[81] J. Silverman & J. Tate -- *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[82] Simon Singh -- *Fermats Last Theorem.* Fourth Estate, 1997.
Simon Singh -- *Het Laatste Raadsel van Fermat*. Arbeiderspers, 1998.

[83] 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

[84] 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.

[85] I. Stewart & D. Tall -- *Algebraic number theory.* Second edition. Chapman and Hall Mathematics Series. Chapman & Hall, London, 1987.

[86] J. Tate -- *The arithmetic of elliptic curves.* Invent. Math. **23** (1974), 179 -- 206.

[87] J. Tate & I. Shafarevich -- *The rank of elliptic curves.* Soviet Math. Dokl. **8** (1967), 917 -- 920. [Dokl. Akad.Nauk **175** (1967).]

[88] N. M. Stephens -- *Congruence properties of congruent numbers.* Bull. London Math. Soc. **7** (1975), 182-184.

[89] ‘‘*De laatste stelling van Fermat*", Syllabus van lezingen gehouden op 6-XI-1993. WG & Universiteit Utrecht.

[90] J. Top -- *Néron's proof of the existence of elliptic curves over* $\mathbb{Q}$ *with rank at least* 11. Utrecht Preprint 476, July 1987.

[91] B. de Smit, J. Top e.a. -- *Speeltuin van de wiskunde.* Veen Magazines, NWT, 2003. ISBN: 907698820X paperback

[92] J. Tunnell -- *A classical diophantine problem and modular forms.* Invent. Math. **72** (1983), 323 -- 334.

[93] B. van der Waarden -- *Moderne Algebra.* Eerste uitgave in 1931. Vierde uitgave: Heidelberger Taschenbuch, 2 delen, Springer-Verlag, 1967.

[94] A. Weil -- *Number theory, an approach through history, from Hammurapi to Legendre.* Birkhäuser 1984.

[95] E. Weiss -- *Algebraic number theory.* Mc-Graw-Hill Cy, 1963.

[96] A. Wiles -- *Modular elliptic curves and Fermat's Last Theorem.* Annals Math. **141** (1995), 443 -- 551.

Prof. Dr F. Oort
Mathematisch Instituut
P.O. Box. 80.010
NL - 3508 TA Utrecht
The Netherlands
email: oort@math.uu.nl

Van: http://www.asahi-net.or.jp/ KC2H-MSM/mathland/math10/matb2000.htm

Congruum g : $1 \leq g \leq 999$
Definition 1.
$k^2g=mn(m^2-n^2)$, k, m, n, g in N (integer $>$ 0)
Definition 2.
$x^2+gy^2=z^2$, $x^2-gy^2=w^2$, x, y, z, w in N (integer $>$ 0), $m=x^2$, $n=gy^2$
Definition 3.
$(x/z^2, y/z^3)$ on elliptic curve $Y^2=X^3-g^2X$, x, y, z in Z (integer), X, Y in Q (rational), $X=mg/n$, $Y=kg^2/n^2$
We are using the same characters x, y, z in the definition 2 and 3, but I think there's no confusion.
There are 361 congruent numbers in the range of $1 \leq g \leq 999$.
g, m, n
5, 5, 4
6, 2, 1
7, 16, 9
13, 325, 36
14, 8, 1
15, 4, 1
21, 4, 3
22, 50, 49
23, 24336, 17689
29, 4901, 4900
30, 3, 2
31, 1600, 81
34, 9, 8
37, 777925, 1764
38, 1250, 289
39, 13, 12,
41, 25, 16,
46, 72, 49,
47, 14561856, 2289169,
53, 1873180325, 1158313156,
55, 125, 44,
61, 12079525, 10227204
62, 39200, 22801,
65, 9, 4,
69, 192, 169,
70, 7, 2,
71, 3600, 121,
77, 2816, 2809,
78, 26, 1,
79, 169000000, 166952241,
85, 85, 36,
86, 338, 49
87, 17956, 169
93, 1444, 75
94, 14112, 529

95, 1445, 76
101, 44715091781, 3975302500
102, 50, 1
103, 8780605285453456, 7551929273974569
109, 2725, 1764
110, 10, 1
111, 37, 12
118, 716311250, 19298449
119, 144, 25
127, 306317326339867638016, 305111826865145547009
133, 256036, 143811
134, 2084882, 14161
137, 3425, 3136
138, 24, 1
141, 48, 1
142, 4918336200, 164070481
143, 101124, 1849
145, 29, 20
149, 93125, 56644
151, 115600, 35721
154, 9, 2
157, 443624018997429899709925, 166136231668185267540804
158, 768800, 579121
159, 33124, 11449
161, 16, 7
165, 16, 11
166, 197646962, 96020401
167, 115222229136, 3447686089
173, 2404644000341688241925, 2367961190733987384484
174, 27, 2
181, 3073858021, 1221502500
182, 343, 18
183, 17853541, 456300
190, 10, 9
191, 40472758 8018561600, 384957657745092721
194, 97, 72
197, 1991322221917925, 103880003159716
199, 13933945152400, 27368486201
··· etc. op die site tot ···
995, 320, 121
997, 422137097683075141716864298903634885273173164273488445043072653 29
655015861152197726745537308248325, 376155528445686424185441533115738655
613612025371648337903724412190017112652894274843193564492291 6
998, 990175074810417659190789298392472344 50, 456840925212009253253860257161127374 89