PWN Vakantiecursus 2015 Praktikum 1
Hoe snel kun je vermenigvuldigen?

Benne de Weger
Technische Universiteit Eindhoven
b.m.m.d.weger@tue.nl

versie 1.0, 22, 29 augustus 2015

De kern van dit praktikum is hoofdstuk 6. Probeer daar in ieder geval aan toe te komen.

1 Inleiding

Afhankelijk van de architectuur van je computer en van de programmeertaal die je gebruikt kun je getallen (voor het gemak in dit praktikum altijd positieve gehele getallen) maar tot een bepaalde grootte aan. De nu veel gebruikte 64-bits-architectuur kan met maximaal de gehele getallen van 0 tot en met $2^{64} - 1 = 18\,446\,744\,073\,709\,551\,615$ werken. Dat lijkt veel, maar als je cryptoloog bent (of je rekeningen in Zimbabwaanse dollars moet betalen) dan is het weinig, en wil je met veel grotere getallen kunnen rekenen.

De processor is zo ontworpen dat bewerkingen als optellen en vermenigvuldigen tot aan die grootte uiterst efficiënt uitgevoerd kunnen worden (dat gaat overigens voor een belangrijk deel met allerlei slimme tabellen waarin alleen maar gezocht hoeft te worden). Grotere getallen representeer je als rijtjes. Voor bewerkingen daarop moet je software hebben die de ingebouwde bewerkingen op de kleinere getallen combineert.

Eigenlijk is dit precies hetzelfde als het rekenen met de decimale schrijfwijze van getallen zoals we dat gewend zijn vanaf de basisschool. We hebben dan i.p.v. 2^{64} maar 10 cijfers tot onze beschikking, en grotere getallen representeren we als rijtjes cijfers. Optellen en vermenigvuldigen van die 10 cijfers doen we met behulp van tabellen (de vroeger tot vervelens toe uit het hoofd opgezegde *tafels*). Voor grotere getallen hebben we al gauw pen en papier nodig (dat is de ouderwetse versie van software), en brengen we de berekeningen terug tot combinaties van bewerkingen op cijfers. Voor het gemak gebruiken we in dit praktikum het decimale stelsel, de methoden in software werken met dezelfde principes.

Algorithmen die optellingen of vermenigvuldigen van grote getallen uit elkaar rafelen tot optellingen of vermenigvuldigen van cijfers, moeten, naast correct, natuurlijk ook snel zijn. Snelheid kun je implementatie-onafhankelijk (dus ook hardware-onafhankelijk) uitdrukken in het *aantal bewerkingen op cijfers* (optellingen, vermenigvuldigingen) dat je nodig hebt.

Opgave 1 Bereken `2181144` + `3507449`. Hoeveel optellingen van cijfers heb je gedaan?

Opgave 2 Als je twee getallen van elk n cijfers optelt, hoeveel optellingen van cijfers heb je minimaal en maximaal nodig?

Bewerkingen van getallen van een ongelijk aantal cijfers behandelen we niet apart. We gaan er voor het gemak van uit dat je de getallen dan maar even ziet als getallen van gelijke lengte, door voorloopnullen te plaatsen bij het kleinste getal. Dat is doorgaans niet de efficiëntste manier, maar dat zijn weinig significante effecten.

2 Complexiteit: lineair, kwadratisch, polynomiaal, exponentieel

Je zou kunnen zeggen: de *complexiteit* van het optellen van getallen van n cijfers is maximaal $2n-1$. Voor heel grote n is die -1 verwaarloosbaar. Minder voor de hand liggend is misschien dat we ook die factor 2 doorgaans verwaarlozen. Maar dat doen we toch, enerzijds omdat de snelheid van je computer toch ook betekent dat je vermenigvuldigt met een of andere constante (aantal microseconden per cijferbewerking bijvoorbeeld), anderzijds omdat in de complexiteitstheorie vooral het *groeigedrag* van functies van belang is, en $0.000002n$, $2n$ en $2000000n$ groeien alledrie lineair.

Lineair groeigedrag kan ook zo bezien worden: als $f(n)$ lineair groeit dan betekent een verdubbeling van n ook (in de limiet voor $n \to \infty$) een verdubbeling van $f(n)$. Dit is onafhankelijk van de coëfficiënt voor de n. Algemener en preciezer: $\lim_{n\to\infty} \dfrac{f(rn)}{f(n)} = r$. Een veelgebruikte notatie is de *grote-O-notatie*: $f(n) = O(n)$, dit betekent *hoogstens lineair groeigedrag* (een precieze definitie: er is een constante C zodat $f(n) < Cn$ voor alle n).

Optellen heeft dus complexiteit $O(n)$. Dat wisten we op de basisschool al. Een betere dan lineaire methode voor optellen is niet bekend; dat is ook niet waarschijnlijk, omdat alleen al het opschrijven van het antwoord complexiteit $O(n)$ heeft.

Kwadratisch groeigedrag betekent: $f(n)$ groeit maximaal als een uitdrukking waarin een kwadratische term de dominante term is, bijvoorbeeld $f(n) \leq an^2 + bn + c$. Voor grote n zijn de termen bn en c weer verwaarloosbaar, en ook de constante a vinden we weer niet interessant. We zeggen nu: $f(n) = O(n^2)$. Verdubbeling van n betekent nu een verviervoudiging van $f(n)$.

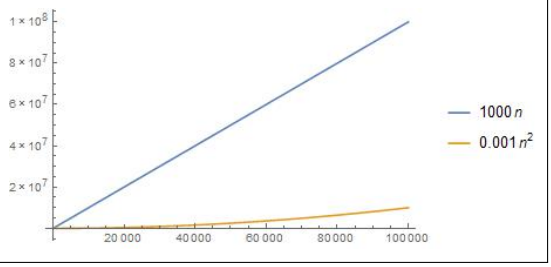
Opgave 3

(a) Als $f(n) = O(n^2)$ is dan $f(n) = O(n)$, of is $f(n) = O(n^3)$?

(b) Als $f(n) = O(n^2)$ en $g(n) = O(n)$, wat is dan de groeiorde van $f(n) + g(n)$, van $f(n) + ng(n)$, van $f(n)g(n)$?

(c) Als $f(n) = O(n^2)$ en $g(n) = O(n^2)$ is dan $f(n) - g(n) = 0$?

(d) Als $f(n) = 1000n$ en $g(n) = 0.001n^2$, welke groeit dan het snelst? Zie de grafiek.



Polynomiaal groeigedrag betekent: er is een exponent α zodat $f(n) = O(n^\alpha)$. Er is ook sneller dan polynomiale groei, bijvoorbeeld exponentiële groei: 2^n groeit sneller dan elke polynomiale uitdrukking n^α, hoe groot α ook is.

3 Vermenigvuldigen door herhaald optellen: exponentieel

Vermenigvuldigen kun je zien als herhaald optellen. Bijvoorbeeld:
$5 \times 483 = 483 + 483 + 483 + 483 + 483$,
en dat reken je dan bijvoorbeeld van links naar rechts uit:

$483 + 483 = 966$ (4 cijferoptellingen),
$966 + 483 = 1449$ (4 cijferoptellingen),
$1449 + 483 = 1932$ (5 cijferoptellingen),
$1932 + 483 = 2415$ (5 cijferoptellingen),
totaal 18 cijferoptellingen.

Opgave 4 Als je de getallen a en b, beide van n cijfers, vermenigvuldigt door op de boven beschreven wijze te werk te gaan, wat is dan de complexiteit? Er moet een functie uitkomen die alleen van n afhangt, niet van a of b.

Het is de bedoeling dat je schrikt van het antwoord: dat is exponentieel, en exponentiële groei betekent doorgaans dat je er gauw mee ophoudt.

4 Vermenigvuldigen door herhaald verdubbelen: al veel beter

Het kan natuurlijk veel slimmer. Waarom niet opmerken dat als je eenmaal $483 + 483$ hebt berekend, je dit kunt hergebruiken? Zet strategische haakjes in de herhaalde som:
$5 \times 483 = (483 + 483) + (483 + 483) + 483$,
en nu reken je de uitdrukking binnen de haakjes maar één keer uit:
$483 + 483 = 966$ (4 cijferoptellingen),
dus $5 \times 483 = 966 + 966 + 483$,
$966 + 966 = 1932$ (5 cijferoptellingen),
$1932 + 483 = 2415$ (5 cijferoptellingen),
totaal 14 cijferoptellingen.

Dit kun je recursief doen. Om dat te laten zien hebben we een wat langere som nodig:
$11 \times 483 = (483 + 483) + (483 + 483) + (483 + 483) + (483 + 483) + (483 + 483) + 483$
$= 966 + 966 + 966 + 966 + 966 + 483 = (966 + 966) + (966 + 966) + 966 + 483$
$= 1932 + 1932 + 966 + 483 = 3864 + 966 + 483 = \ldots$.
We kunnen er ook zo tegenaan kijken: schrijf 11 in het tweetallig stelsel: $11 = 8 + 2 + 1$, bereken dan door telkens te verdubbelen 2×483, 4×483, 8×483, verder hoeft niet, en zoek even uit welke je uiteindelijk moet optellen. Dus zo:
$2 \times 483 = 483 + 483 = 966$, $4 \times 483 = 966 + 966 = 1932$, $8 \times 483 = 1932 + 1932 = 3864$, en
$11 \times 483 = (8 + 2 + 1) \times 483 = 3864 + 966 + 483 = 4830 + 483 = 5313$.

Opgave 5 Ga na dat we zojuist 25 cijferoptellingen hebben gedaan. Hoeveel was het met de oude methode van herhaald optellen?

Opgave 6 We vermenigvuldigen de getallen a en b, beide van n cijfers, op de boven beschreven wijze.

(a) Hoe groot is maximaal het aantal verdubbelingen van b dat je moet doen?
Het gaat om de juiste vorm in n, niet om precieze constanten.

(b) Hoe groot kan het aantal optellingen worden dat na de verdubbelingen nog gedaan moet worden?

(c) Geef een bovengrens van het aantal cijfers van de op te tellen getallen.

(d) Hoe groot is het totale aantal optellingen van cijfers dat je maximaal moet doen?

Als het goed is vind je kwadratische complexiteit. Dat is aanzienlijk beter dan exponentieel.

5 Vermenigvuldigen op de basisschool: kwadratisch

Een voorbeeld:

```
       3 5 0 7
       2 1 8 1
       -------
       3 5 0 7 (4 cijfervermenigvuldigingen, geen overdracht)
   2 8 0 5 6   (4 cijfervermenigvuldigingen, 2 overdrachten dus 2 cijferoptellingen)
   3 5 0 7     (4 cijfervermenigvuldigingen, geen overdracht)
 7 0 1 4       (4 cijfervermenigvuldigingen, 2 overdrachten dus 2 cijferoptellingen)
 -------------
 7 6 4 8 7 6 7 (12 cijferoptellingen, waarvan 2 overdrachten)
 totaal 16 cijfervermenigvuldigingen en 16 cijferoptellingen)
```

Cijfervermenigvuldigen met 0 en met 1 heb ik gewoon vol meegeteld. Eigenlijk werkt de basisschoolmethode bijna net zo als de methode van herhaald verdubbelen. Er zijn twee verschillen: niet de tweetallige schrijfwijze van a wordt gebruikt maar de 10-tallige, en om een cijfer van a met heel b te vermenigvuldigen wordt niet herhaald opgeteld, maar wordt met vermenigvuldigingen van cijfers gewerkt.

Opgave 7 Analyseer hoeveel vermenigvuldigingen van cijfers er maximaal nodig zijn bij het vermenigvuldigen van twee getallen van n cijfers met de basisschoolmethode.
Analyseer ook hoeveel optellingen van cijfers (inclusief overdrachten) er nodig zijn.
Hint: zowel bij cijferoptellingen als bij cijfervermenigvuldigingen komen overdrachten voor.

De complexiteit is weer kwadratisch, maar (in de constante) beter dan bij herhaald optellen.

6 Sneller vermenigvuldigen: beter dan kwadratisch

Weinig mensen, óók weinig wiskundigen, weten dat vermenigvuldigen echt beter dan kwadratisch kan. Wij behoren straks tot deze selecte groep.

De volgende methode is in 1960 bedacht door de (toen) jonge Rus Anatolii Karatsuba, en bracht een schok teweeg onder de wiskundigen en 'cybernetici' van die tijd. Want iedereen geloofde het vermoeden dat vermenigvuldigen niet sneller dan kwadratisch kon, zoals duidelijk was uitgesproken door de wereldberoemde wiskundige en grondlegger van de complexiteitstheorie Andrej Kolmogorov, de leermeester van Karatsuba. Moraal: soms weet de leerling het inderdaad beter dan de leraar.

Eerst een voorbeeld. We doen weer 3507×2181. We delen de getallen in tweeën op en werken haakjes uit, daarmee brengen we het probleem terug tot rekenen met getallen van 2 cijfers: $(35 \times 10^2 + 07) \times (21 \times 10^2 + 81) = (35 \times 21) \times 10^4 + (35 \times 81 + 07 \times 21) \times 10^2 + 07 \times 81$, dus nu te berekenen: 35×21, $35 \times 81 + 07 \times 21$, 07×81. Merk op dat vermenigvuldigen met een macht van 10 geen tijd kost, dat is gewoon je getal op de juiste positie zetten. Verder hebben we wellicht wat extra optellingen door overdracht, maar dat is hooguit van lineaire complexiteit, dus vermoedelijk wel te verwaarlozen.

Het lijkt erop dat we nu 4 vermenigvuldigingen van halve lengte nodig hebben: 35×21, 35×81, 07×21, 07×81. Als we die halve-lengte-vermenigvldigingen met dezelfde methode doen, dan voldoet de complexiteitsfunctie $f(n)$ aan $f(n) = 4f\left(\frac{1}{2}n\right)$ (met verwaarlozing van lineaire termen), en dat geeft precies kwadratische complexiteit. Dat schiet dus nog niet op.

De geniale gedachte van Karatsuba is om de middelste term $35 \times 81 + 07 \times 21$ als volgt uit te rekenen: $(35 + 07) \times (21 + 81) - 35 \times 21 - 07 \times 81$.

Opgave 8

(a) Waarom geeft deze manier van berekenen een correct antwoord?

(b) Beargumenteer dat er nu in totaal maar 3 vermenigvuldigingen van halve lengte nodig zijn in plaats van 4.

Dus we moeten 3 vermenigvuldigingen van 2 cijfers doen: 35×21, 42×102, en 07×81 (nou ja, eentje van 3 cijfers, maar deze 3 is bijna een 2).

Opgave 9

(a) Voer deze drie vermenigvuldigingen uit met behulp van de methode van Karatsuba (vat een eventuele 1 als derde cijfer niet op als een apart cijfer, dus de 10 in 102 telt als één cijfer), en houd bij hoeveel cijfervermenigvuldigingen je doet.

(b) Maak vervolgens de opgave 3507×2181 af, gebruik alléén nog optellingen (en aftrekkingen, maar dat is hetzelfde).

De methode van Karatsuba heeft twee basisideeën: na opsplitsen in tweeën van je getallen doe je niet 4 vermenigvuldigingen van halve lengte maar het kan met 3; en je kunt dit vervolgens recursief toepassen: 3 vermenigvuldigen van halve lengte kan in 9 vermenigvuldigingen van kwart-lengte, dat kan in 27 vermenigvuldigingen van achtste lengte, enzovoorts. Als overhead heb je wel telkens wat extra optellingen (en halve lengte is niet precies halve lengte maar maximaal één meer dan dat), maar die effecten zijn hooguit een lineaire bijdrage en daarmee ongetwijfeld te verwaarlozen.

Nu gaan we de complexiteit van deze methode analyseren. Maar eigenlijk is dat heel simpel. Stel dat de complexiteit van Karatsuba gegeven wordt door de functie $K(n)$, voor getallengte n. Hierbij meten we alleen vermenigvuldigingen, geen optellingen en overdrachten.

Opgave 10

(a) Wat is het verband tussen $K(n)$ en $K(\frac{1}{2}n)$?

(b) Als we $K(n) = Cn^\alpha$ veronderstellen, voor constanten C en α, wat moet α dan zijn?

(c) Laat zien dat de methode van Karatsuba sneller dan kwadratisch is, m.a.w. $\alpha < 2$.

Opgave 11 Voor thuis, voor de programmeurs: schrijf een programma dat zowel de basisschoolmethode als de methode van Karatsuba implementeert, en dat bijhoudt hoeveel cijfervermenigvuldigingen gedaan worden. Doe daarmee wat experimenten, en ga na vanaf hoeveel cijfers Karatsuba inderdaad sneller wordt. Houd ook het aantal cijferoptellingen bij, en kijk hoe dat zich ontwikkelt.

7 Echt snel vermenigvuldigen: bijna lineair

Na Karatsuba's publikatie in 1962 was de beer los in de complexiteitswereld. Je kunt een variant van de methode van Karatsuba in termen van polynomen vatten, als volgt.

We nemen het aantal cijfers even, zeg $n = 2m$, en schrijven $a = a_1 10^m + a_0$, $b = b_1 10^m + b_0$, en $z = ab = z_2 10^{2m} + z_1 10^m + z_0$. Het probleem is: gegeven a_0, a_1, b_0, b_1, bereken z_0, z_1, z_2. Dat is hetzelfde als: gegeven polynomen $A(t) = a_1 t + a_0$ en $B(t) = b_1 t + b_0$, bereken de coëfficiënten z_0, z_1, z_2 van het polynoom $Z(t) = A(t)B(t)$.

Een polynoom $p(t)$ van graad r wordt vastgelegd door $r+1$ punten $(t, p(t))$. Voor de variabele t kunnen we dan kiezen wat we willen, en het ligt voor de hand zo klein mogelijke waarden te nemen, omdat daarmee het snelste gerekend kan worden. De coëfficiënten van het polynoom $Z(t)$ kun je vinden uit bijvoorbeeld $Z(-1), Z(0)$ en $Z(1)$. De methode wordt dan als volgt: bereken $A(t)$ en $B(t)$ voor $t = -1, 0, 1$; dat kan in lineaire tijd (want vermenigvuldigen van de relatief grote coëfficienten a_i, b_i met de relatief kleine t kan in lineaire tijd); bereken dan $Z(t) = A(t)B(t)$ voor $t = -1, 0, 1$ (dat zijn 3 vermenigvuldigingen van halve lengte, die je natuurlijk recursief met dezelfde methode kunt doen), en los nu z_0, z_1, z_2 op uit de drie vergelijkingen $Z(t) = z_2 t^2 + z_1 t + z_0$. Dat laatste kan met uitsluitend lineaire operaties.

Een voorbeeld: voor $\texttt{3507} \times \texttt{2181}$ vinden we:
$A(t) = \texttt{35}t + \texttt{07}$, $A(-1) = -\texttt{28}$, $A(0) = \texttt{07}$, $A(1) = \texttt{42}$ (lineair),
$B(t) = \texttt{21}t + \texttt{81}$, $B(-1) = \texttt{60}$, $B(0) = \texttt{81}$, $B(1) = \texttt{102}$ (lineair),
$Z(-1) = -\texttt{28} \times \texttt{60} = -\texttt{1680}$, $Z(0) = \texttt{07} \times \texttt{81} = \texttt{567}$, $Z(1) = \texttt{42} \times \texttt{102} = \texttt{4284}$ (duur),
en nu dus op te lossen het stelsel

$$\begin{array}{rcccccc} -\texttt{1680} & = & z_2 & - & z_1 & + & z_0 \\ \texttt{567} & = & & & & & z_0 \\ \texttt{4284} & = & z_2 & + & z_1 & + & z_0 \end{array}$$

(weer lineair).

Opgave 12 Los dit stelsel op, en reconstrueer daarmee het antwoord `7648767`.

Het voordeel van deze methode is dat ze direct te generaliseren is. Waarom zou je je getallen in maar twee stukken ophakken, waarom niet in meer dan twee? Stel je doet het in r stukken. De polynomen A en B krijgen dan graad $r-1$, het polynoom Z krijgt graad $2r-2$, en heeft $2r-1$ coëfficiënten. Eén vermenigvuldiging van n cijfers kan dus gedaan worden in $2r-1$ vermenigvuldigingen van $\frac{n}{r}$ cijfers.

Laten we de complexiteit van deze methode $K_r(n)$ noemen, en laten we veronderstellen dat de overhead van optellingen, overdrachten en het oplossen van het stelsel van $2r-1$ vergelijkingen in $2r-1$ onbekenden nog altijd verwaarloosd kan worden.

Opgave 13

(a) Wat is het verband tussen $K_r(n)$ en $K_r\left(\frac{n}{r}\right)$?

(b) Als we $K_r(n) = C_r n^{\alpha_r}$ veronderstellen, voor constanten C_r en α_r, wat wordt α_r dan?

(c) Laat zien dat $\lim_{r\to\infty} \alpha_r = 1$.

Voor groot genoege r komt de complexiteit dus willekeurig dicht bij lineair. In de praktijk wordt de overhead toch al gauw groot, en het punt waar de methode praktisch wordt komt al

gauw ver weg te liggen, ook voor relatief kleine r. Maar in theorie werkt het, en in de praktijk met kleine r ook. Cryptografen zijn er blij mee, en jij ook omdat je bij de kassa minder lang hoeft te wachten op de berekeningen die je bankpasje moet doen.

Als een wiskundige een term als $a_0b_1 + a_1b_0$ ziet, roept zij al gauw: hee, een convolutieproduct, kunnen we niet iets met Fouriertransformaties doen? Fouriertransformaties zetten een convolutieproduct namelijk om in één enkel gewoon product. Dat is een slimme opmerking: dat kan inderdaad, en als je het een beetje slim aanpakt is de overhead van de Fouriertransformatie en de inverse Fouriertramsformatie ook efficiënt uit te voeren. De beste methode, die in de praktijk ook wel gebruikt wordt voor vermenigvuldigingen van zeer grote getallen (miljoenen cijfers), is dan ook de zogenaamde FFT-techniek ('Fast Fourier Transform').

8 Modulair machtsverheffen

Tenslotte: waar vermenigvuldigen begon als herhaald optellen (dom) en vervolgde met herhaald verdubbelen (al best slim), begint machtsverheffen als herhaald vermenigvuldigen (dom) en vervolgt met herhaald kwadrateren (al een stuk minder dom, het blijft een beetje tobben, maar iets echt slimmers hebben we hier niet).

Machtsverheffen a^b met twee getallen a, b van veel cijfers is wat nooit iemand zomaar doet.

Opgave 14 Als a en b beiden 100 cijfers hebben, hoeveel cijfers heeft a^b dan ongeveer? Hoeveel van zulke getallen passen op je mooie nieuwe harde schijf van 10 TB?

Maar als we modulo-rekenen doen, blijven de getallen gegarandeerd klein. Met een modulus m van n cijfers is een modulaire machtsverheffing $a^b \pmod m$ voor getallen a, b van ook n cijfers, best uit te voeren: na iedere vermenigvuldiging van twee getallen van n cijfers moet je het resultaat van $2n$ cijfers ook weer modulo m nemen, en kom je weer terug op n cijfers. Het is maar goed ook dat dat kan, want veel cryptografische methoden gebruiken modulaire machtsverheffingen van getallen van enkele honderden cijfers.

Machtsverheffen door herhaald kwadrateren werkt als volgt. Stel we willen a^{3840} berekenen (in Praktikum 2 willen we dat inderdaad).

Schrijf eerst 3840 in het tweetallig stelsel uit: $3840 = 2048 + 1024 + 512 + 256$. Bereken dan achtereenvolgens, door telkens te kwadrateren: $a^2, a^4, a^8, a^{16}, a^{32}, a^{64}, a^{128}, a^{256}, a^{512}, a^{1024}, a^{2048}$ (11 vermenigvuldigingen) en dan kost $a^{3840} = a^{2048} \cdot a^{1024} \cdot a^{512} \cdot a^{256}$ nog maar 3 vermenigvuldigingen. Vergeet niet na iedere vermenigvuldiging te reduceren modulo m.

Zonder bewijs vermelden we dat reduceren $\bmod m$ voor een m van n cijfers complexiteit $O(n^2)$ heeft.

Opgave 15

(a) Beargumenteer dat modulair machtsverheffen met getallen van n cijfers een kubische complexiteit ($O(n^3)$) heeft als je voor de vermenigvuldigingen de basisschoolmethode gebruikt.

(b) Wat zal de complexiteit van modulair machtsverheffen worden als je voor het vermenigvuldigen Karatsuba gebruikt?

(c) En wat als je een bijna-lineaire vermenigvuldigingsmethode gebruikt?

Antwoorden deel 1

1 Ik kwam op 8 optellingen en 0 vermenigvuldigingen, namelijk 7 keer een optelling van cijfers op dezelfde positie, en 1 keer vond ik een uitkomst ≥ 10 zodat een overdracht nodig was, dat kost een extra optelling. Een optelling met het cijfer 0 tel ik gewoon mee (waarom?).

2 Minimaal n (als er geen overdracht is) en maximaal $2n-1$.

3(a) Als $f(n) = O(n^2)$ dan is altijd ook $f(n) = O(n^3)$, maar niet per se $f(n) = O(n)$.
(b) $f(n) + g(n) = O(n^2)$, $f(n) + ng(n) = O(n^2)$, $f(n)g(n) = O(n^3)$.
(c) Nee, $f(n) - g(n)$ is nog steeds $O(n^2)$.
(d) $g(n) = 0.001n^2$ groeit op den duur het snelst. Het overgangspunt ligt bij $n = 1\,000\,000$, en de grafiek is dus erg misleidend omdat die niet verder gaat dan $n = 100\,000$.

4 Veronderstel $a \leq b$. Je telt $(a-1)$ maal een getal van n cijfers op bij een getal van maximaal $2n$ cijfers, dat geeft, vanwege maximaal $2n-1$ overdrachten maximaal $(a-1)(3n-1)$ cijferoptellingen. Dit schatten we af met het makkelijker $3an$. We kunnen inderdaad a wel afschatten in termen van n, maar dat wordt wel exponentieel: $a < 10^n$. Een bovenafschatting is dan $3n10^n$ cijferoptellingen. Daar worden we niet vrolijk van.

5 $483 + 483$ geeft 4 cijferoptellingen, $966 + 966$ geeft er 5, $1932 + 1932$ geeft er 5, $3864 + 966$ geeft er 6, en $4830 + 483$ geeft er 5, totaal 25. Op de oude manier kwam ik tot 47.

6(a) De hoogste macht van 2 onder a heeft exponent $\leq {}^2\log a < {}^2\log(10^n) = \left({}^2\log 10\right) n < 3.33n$. Dat is ook het aantal verdubbelingen.
(b) Eén minder dan het aantal 1-en in de tweetallige ontwikkeling van a, dat is hooguit $3.33n$.
(c) Wat er wordt opgeteld blijft altijd onder ab, dat is een getal van hooguit $2n$ cijfers.
(d) Het aantal verdubbelingen en optellingen is $< 6.66n$. Per berekening zijn er hooguit $4n$ cijferoptellingen, inclusief overdrachten. Totaal minder dan $26.7n^2$ cijferoptellingen. Met wat preciezer kijken kun je het denk ik wel onder de $15n^2$ krijgen, maar waarom zouden we.

7 Ieder cijfer van het ene getal wordt een keer vermenigvuldigd met ieder cijfer van het andere getal, totaal dus n^2 cijfervermenigvuldigingen. Dan heb je maximaal $(n-1)^2$ cijferoptellingen en evenveel overdrachten, totaal $2n^2 - 4n + 2$ cijferoptellingen.

8(a) $(a+b)(c+d) = ac+ad+bc+bd = (ad+bc)+ac+bd$, dus $ad+bc = (a+b)(c+d)-ac-bd$.
(b) Als je ac en bd eerst uitrekent (die heb je toch nodig) dan vind je $(ad+bc)$ dus ook als $(a+b)(c+d) - ac - bd$, met maar één extra vermenigvuldiging.

9(a) $3 \times 2 = 6$, $5 \times 1 = 5$, $(3+5)(2+1) = 8 \times 3 = 24$, $24 - 6 - 5 = 13$, $600 + 130 + 5 = 735$.
$4 \times 10 = 40$, $2 \times 2 = 4$, $(4+2)(10+2) = 6 \times 12 = 72$, $72 - 40 - 4 = 28$, $4000 + 280 + 4 = 4284$.
$0 \times 8 = 0$, $7 \times 1 = 7$, $(0+7)(8+1) = 7 \times 9 = 63$, $63 - 0 - 7 = 56$, $000 + 560 + 7 = 567$.
(b) $4284 - 735 - 567 = 2982$, $7350000 + 298200 + 567 = 7648767$.

10(a) $K(n) = 3K\left(\frac{1}{2}n\right)$.
(b) $Cn^\alpha = 3C\left(\frac{1}{2}n\right)^\alpha = 3Cn^\alpha 2^{-\alpha}$, nu vallen C en n^α weg en houden we over $2^\alpha = 3$, dus $\alpha = {}^2\log 3$.
(c) ${}^2\log 3 \approx 1.58$.

11 –

12 $z_0 = 567$ is gratis. Die invullen in de andere twee geeft:
$z_2 - z_1 = -1680 - 567 = -2247$,

$z_2 + z_1 = 4284 - 567 = 3717$,
$z_2 = (-2247 + 3717)/2 = 735$,
$z_1 = (2247 + 3717)/2 = 2982$,
en het antwoord is $Z(100) = 7350000 + 298200 + 567 = 7648767$.

13(a) $K_r(n) = (2r-1)K_r\left(\frac{n}{r}\right)$.
(b) $C_r n^{\alpha_r} = (2r-1)C_r\left(\frac{n}{r}\right)^{\alpha_r} = (2r-1)C_r n^{\alpha_r} r^{-\alpha_r}$, nu vallen C_r en n^{α_r} weg en houden we over $r^{\alpha_r} = 2r-1$, dus $\alpha = {}^r\log(2r-1)$.
(c) $\alpha_r = {}^r\log(2r-1) = \dfrac{\log(2r-1)}{\log r} = \dfrac{\log r + \log(2-1/r)}{\log r} = 1 + \dfrac{\log(2-1/r)}{\log r} \to 1$ als $r \to \infty$.

14 Het aantal cijfers is ongeveer ${}^{10}\log a^b = b\,{}^{10}\log a \approx 10^{100} \cdot 100 = 10^{102}$. Let wel, het aantal cijfers is niet 102, maar 1000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Per cijfer heb je 3.33 bits nodig, dus op je harde schijf van 80×10^{12} bits kun je pakweg 24000000000000 cijfers kwijt. Als je evenveel harde schijven zou hebben als atomen in het heelal dan heb je nog niet genoeg.

15(a) Voor een machtsverheffing van n cijfers doe je $3.33n$ kwadrateringen, en maximaal evenveel vermenigvuldigingen daarna. Elke vermenigvuldiging / kwadratering heeft complexiteit $O(n^2)$, totaal geeft dat $O(n^3)$.
(b) Elke vermenigvuldiging / kwadratering wordt nu $O(n^{{}^2\log 3})$, dus totaal wordt de complexiteit $O(n^{1+{}^2\log 3}) \approx O(n^{2.58})$.
(c) Je kunt willekeurig dicht in de buurt van $O(n^2)$ komen.

PWN Vakantiecursus 2015 Praktikum 2
Elementair is niet hetzelfde als triviaal

Benne de Weger
Technische Universiteit Eindhoven
b.m.m.d.weger@tue.nl

versie 1.01, 22, 29 augustus 2015

De kern van dit praktikum is paragraaf 2.3–5. Probeer daar in ieder geval aan toe te komen.

1 Inleiding

Diophantische vergelijkingen zijn vergelijkingen waarbij we alleen in geheeltallige oplossingen geïnteresseerd zijn. Kijk bijvoorbeeld naar de rij van machten van gehele getallen (met exponent ≥ 2, anders wordt het flauw): $1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, 100, \ldots$. Het lijkt erop dat de afstanden groter worden. Zijn wellicht 8 en 9 de enige machten die afstand 1 hebben? In een Diophantische vergelijking geformuleerd: wat zijn de oplossingen van $x^a - y^b = 1$ in gehele getallen x, y, a, b met $x \geq 1, y \geq 1, a \geq 2, b \geq 2$? Het vermoeden dat inderdaad $(x, y, a, b) = (3, 2, 2, 3)$ de enige oplossing is werd voor het eerst geuit in 1844 door Eugène-Charles Catalan. In 1976 bewees Robert Tijdeman dat er maar eindig veel oplossingen zijn, en zijn bewijs leidt tot een expliciete bovengrens voor x, y, a, b die echter zo onhandelbaar groot is dat je er niks aan hebt om het vermoeden echt te bewijzen. Tijdemans bewijs gebruikt zeer geavanceerde getaltheorie; niemand zou dat elementair durven noemen, laat staan triviaal. In 2002 bewees Preda Mihăilescu het vermoeden van Catalan met totaal andere methoden. Ook Mihăilescu's bewijs is verre van triviaal, maar het is in tegenstelling tot Tijdemans bewijs wel gebaseerd op klassieke algebraische getaltheorie. Nog niet iets wat ik elementair wil noemen.

Laten we het ons wat makkelijker maken, en x, y vast nemen als $2, 3$. De vraag wordt dan: welke machten van 2 en van 3 verschillen slechts 1? De bijbehorende Diophantische vergelijking is $2^a - 3^b = \pm 1$. Nu nemen we a, b als niet-negatieve gehele getallen.

Opgave 1 Zoek 4 oplossingen (a, b) van $2^a - 3^b = \pm 1$ met $a \geq 0$, $b \geq 0$.

Hint: doe dit systematisch, door bijvoorbeeld $b = 0, 1, 2, \ldots$ af te lopen.
Zoek niet door naar een vijfde oplossing. Die is er namelijk niet. En dat is makkelijk te bewijzen. Eerst de ene helft.

Opgave 2 We bepalen alle oplossingen van $3^b - 2^a = 1$ met $a \geq 0, b \geq 0$.

(a) Laat zien: $3^b \equiv 1$ of $3 \pmod 4$, al naar gelang b even of oneven is.

(b) Laat zien: als $a \geq 2$ dan is b even.

(c) Laat zien: de enige machten van 2 die onderling 2 verschillen zijn 2 en 4.

(d) Bepaal alle oplossingen van $z^2 - 1 = 2^a$ met $z \geq 0$ en $a \geq 0$.
Hint: ontbind $z^2 - 1$ in factoren, bedenk wat delers van 2^a kunnen zijn, gebruik (c).

(e) Bepaal alle oplossingen van $3^b - 2^a = 1$ met $a \geq 0, b \geq 0$.

Dat was niet zo moeilijk. Op z'n minst elementair, wat mij betreft zelfs triviaal. Maar daar mag je anders over denken. Dit was een vingeroefening, maar wel een belangrijke, want het resultaat gebruiken we verderop.

En dan, voor de volledigheid, de andere helft. Die is wat makkelijker, en hebben we verderop niet nodig, dus je kunt het ook eerst even overslaan.

Opgave 3 We bepalen alle oplossingen van $2^a - 3^b = 1$ met $a \geq 0, b \geq 0$.

(a) Bepaal de mogelijke machten van 3 modulo 8.

(b) Laat zien dat er geen oplossingen van $2^a - 3^b = 1$ zijn met $a \geq 3$.

(c) Bepaal alle oplossingen van $2^a - 3^b = 1$ met $a \geq 0, b \geq 0$.

2 Kan een som of verschil van een macht van 2 en een macht van 3 een kwadraat zijn?

2.1 Inleiding

De opgeloste vergelijking $2^a - 3^b = \pm 1$ gaan we nu generaliseren, door de 1 te vervangen door x^2 (met $x \geq 0$), en in plaats van het minteken ook een plusteken toe te staan.

Opgave 4

(a) Zoek vijf oplossingen van $3^b - 2^a = x^2$ met $a \geq 0$, $b \geq 0$, $x \geq 0$.

(b) Zoek drie oplossingen van $2^a - 3^b = x^2$ met $a \geq 0$, $b \geq 0$, $x \geq 0$.

(c) Zoek drie oplossingen van $2^a + 3^b = x^2$ met $a \geq 0$, $b \geq 0$, $x \geq 0$.

Ons doel is te laten zien dat er geen andere zijn.

2.2 Trivialiteiten

TIP: stel Opgaven 5 en 6 uit tot later. Ze zijn voor het vervolg niet nodig.

We beginnen met de makkelijkste, dat is $2^a - 3^b = x^2$.

Opgave 5

(a) Bepaal alle mogelijke kwadraten modulo 8.

(b) Gebruik Opgave 2(a) om alle mogelijke waarden van $x^2 + 3^b \pmod 8$ te vinden.

(c) Bepaal alle oplossingen van $2^a - 3^b = x^2$ met $a \geq 0$, $b \geq 0$, $x \geq 0$.

Ik hoop dat je dit intussen ook triviaal vindt. De volgende, $2^a + 3^b = x^2$, is een tikje moeilijker.

Opgave 6

(a) Bepaal de mogelijke kwadraten modulo 3. Bepaal dan de oplossingen met oneven a. Hint: gebruik Opgave 2(d).

(b) Vanaf nu is a dus even. We schrijven $y^2 = 2^a$. Laat zien dat uit $x^2 - y^2 = 3^b$ volgt dat $y = \frac{1}{2}(3^b - 1)$.

(c) Gebruik de uitkomst van Opgave 2 om alle oplossingen van $2^a + 3^b = x^2$ met $a \geq 0$, $b \geq 0$, $x \geq 0$ te bepalen.

Tenslotte $3^b - 2^a = x^2$. Die is echt niet meer triviaal. Maar ik hoop je ervan te overtuigen dat deze nog wel elementair is op te lossen.

We beginnen met de trivialiteiten. Eerst het geval $a = 0$.

Opgave 7 Bepaal de oplossingen van $x^2 + 1 = 3^b$ met $b \geq 0$, $x \geq 0$.

Hint: werk modulo 3.

Dan het geval $a \geq 2$.

Opgave 8

(a) Laat zien dat b even is.
Hint: werk modulo 4.

(b) Laat zien dat uit $y^2 - x^2 = 2^a$ met oneven x volgt dat $y = 2^{a-2} + 1$.

(c) Maak je bewijs af met behulp van de uitkomst van Opgave 2.

Blijft het geval $a = 1$, oftewel de vergelijking $x^2 + 2 = 3^b$. We hebben (hopelijk) gezien dat er twee oplossingen zijn: $(x, b) = (1, 1), (5, 3)$.

Opgave 9 Laat zien dat b oneven is.

Hint: er bestaan geen kwadraten die 2 verschillen.

Vanaf nu is b dus oneven, en schrijven we $b = 2p + 1$, en $y = 2^p$, zodat $3^b = 3y^2$. Ons op te lossen probleem is nu:

$$\boxed{x^2 - 3y^2 = -2 \text{ met } y = 3^p.}$$

En nu verlaten we zo langzamerhand toch wel echt het triviale...

2.3 Een Pell-vergelijking

Een vergelijking als $x^2 - 3y^2 = d$ heet een *Pell-vergelijking*. Wij zijn geïnteresseerd in $d = -2$, maar we bekijken ook $d = 1$. Het charmante van dit type vergelijkingen is dat de linkerkant ervan ontbonden kan worden als $(x + y\sqrt{3})(x - y\sqrt{3})$, en dat we oplossingen (x, y) ervan kunnen associëren met getallen van de vorm $x + y\sqrt{3}$.

Lemma 1. Als $x_1 + y_1\sqrt{3} = x_2 + y_2\sqrt{3}$ voor gehele getallen x_1, y_1, x_2, y_2, dan is $x_1 = x_2$ en $y_1 = y_2$.

Opgave 10 Bewijs Lemma 1.

Hint: veronderstel dat $y_1 \neq y_2$. De vergelijking kan dan omgewerkt worden tot een breukvoorstelling van $\sqrt{3}$. Bedenk waarom dat een tegenspraak oplevert.

Lemma 2. Laten x_1, y_1, x_2, y_2 gegeven zijn, en schrijf $x_1^2 - 3y_1^2 = d_1$, $x_2^2 - 3y_2^2 = d_2$. Definieer $x_3 = x_1x_2 + 3y_1y_2$ en $y_3 = x_1y_2 + x_2y_1$. Dan is $x_3^2 - 3y_3^2 = d_1d_2$.

Opgave 11 Bewijs Lemma 2.

Hint: werk met factoren $x_i \pm y_i\sqrt{3}$.

2.4 Recurrente rijen

De kleinste oplossing van $x^2 - 3y^2 = 1$ is $(x, y) = (2, 1)$. Hierbij hoort het getal $2 + \sqrt{3}$. Uit Lemma 1 volgt dat er voor iedere gehele k unieke gehele getallen u_k, v_k bestaan zodat $u_k + v_k\sqrt{3} = (2 + \sqrt{3})^k$ (voor negatieve k ook, want $(2 + \sqrt{3})^{-1} = 2 - \sqrt{3}$). En Lemma 2 zegt dan dat voor iedere k geldt dat $u_k^2 - 3v_k^2 = 1$. We geven een paar van deze getallen:

k	$\ldots$	-4	-3	-2	-1	0	1	2	3	$4\ldots$
u_k	$\ldots$	97	26	7	2	1	2	7	26	$97\ldots$
v_k	$\ldots$	-56	-15	-4	-1	0	1	4	15	$56\ldots$

Opgave 12

(a) Laat zien dat $(2 + \sqrt{3})^2 = 4(2 + \sqrt{3}) - 1$.

(b) Vermenigvuldig dit met $(2 + \sqrt{3})^{k-1}$, en gebruik Lemma 1 om te concluderen dat $u_{k+1} = 4u_k - u_{k-1}$ en $v_{k+1} = 4v_k - v_{k-1}$ gelden voor alle k.

(c) Laat zien dat voor $k \geq 1$ geldt dat $v_{k+1} \leq 4v_k$.

Deze getallenrijen lijken dus wel op de Fibonacci-rij: het zijn *binaire recurrente rijen.*

We hebben nu oneindig veel oplossingen gevonden van onze Pell-vergelijking $x^2 - 3y^2 = 1$, namelijk $(x, y) = (u_k, v_k)$. Ook $(x, y) = (\pm u_k, \pm v_k)$ zijn oplossingen. Zijn er nog meer? Nee:

Lemma 3 Alle oplossingen van $x^2 - 3y^2 = 1$ zijn van de vorm $(x, y) = (\pm u_k, \pm v_k)$ voor de boven gedefinieerde u_k, v_k.

Het bewijs komt straks. Nu doen we eerst hetzelfde voor de Pell-vergelijking $x^2 - 3y^2 = -2$.

Opgave 13

(a) Wat is de kleinste oplossing van $x^2 - 3y^2 = -2$?

(b) Maak hierbij rijen x_k en y_k (met k geheel, mag ook negatief zijn) zodat $(x, y) = (x_k, y_k)$ ook oplossingen $x^2 - 3y^2 = -2$ van zijn.

(c) Laat zien dat deze rijen ook voldoen aan de recurrente betrekking $x_{k+1} = 4x_k - x_{k-1}$, $x_{k+1} = 4x_k - x_{k-1}$.

(d) Maak een tabelletje met enkele waarden van x_k en y_k (bijvoorbeeld voor $-4 \leq k \leq 3$). Concludeer dat negatieve k verder buiten beschouwing kunnen blijven.

Als je de goede x_k, y_k gevonden hebt geldt het volgende lemma.

Lemma 4 Alle oplossingen van $x^2 - 3y^2 = -2$ zijn van de vorm $(x, y) = (\pm x_k, \pm y_k)$.

De Lemma's 3 en 4 moeten natuurlijk wel bewezen worden. Het bewijs van Lemma 3 schrijf ik voor je uit, dan zou je daarna zelf het bewijs van Lemma 4 kunnen proberen.

TIP: stel deze bewijzen uit tot later, en lees eerst verder bij paragraaf 2.5.

Bewijs van Lemma 3. Laat $(x, y) = (U, V)$ een willekeurige oplossing zijn van $x^2 - 3y^2 = 1$. Zonder verlies van algemeenheid mogen we aannemen dat $U \geq 1$ en $V \geq 0$. Omdat v_k voor $k \geq 0$ strict stijgend is, is er een $\ell \geq 0$ waarvoor geldt $v_\ell \leq V < v_{\ell+1}$. We definiëren nu de gehele getallen U_0, V_0 door $U_0 + V_0\sqrt{3} = (U + V\sqrt{3})(u_\ell - v_\ell\sqrt{3})$. Uit Lemma 2 volgt dat $(x, y) = (U_0, V_0)$ ook een oplossing is van $x^2 - 3y^2 = 1$. We laten zien dat deze oplossing niet erg groot kan zijn.

Lemma 2 geeft $V_0 = Vu_\ell - Uv_\ell$. Dit schrijven we als $V_0 = V(u_\ell - v_\ell\sqrt{3}) - (U - V\sqrt{3})v_\ell$, omdat we de twee uitdrukkingen tussen haakjes goed kunnen afschatten. Namelijk, $u_\ell - v_\ell\sqrt{3} = \dfrac{1}{u_\ell + v_\ell\sqrt{3}}$ en dus is $0 < u_\ell - v_\ell\sqrt{3} < \dfrac{1}{v_\ell\sqrt{3}}$, en $U - V\sqrt{3} = \dfrac{1}{U + V\sqrt{3}}$, en dus is $0 < U - V\sqrt{3} < \dfrac{1}{V\sqrt{3}}$. Samen geeft dit $\dfrac{-v_\ell}{V\sqrt{3}} < V_0 < \dfrac{V}{v_\ell\sqrt{3}}$. De keuze van ℓ zorgt er nu voor dat $\dfrac{-v_\ell}{v_\ell\sqrt{3}} < V_0 < \dfrac{v_{\ell+1}}{v_\ell\sqrt{3}}$, en Opgave 12(c) geeft dan $0 \leq V_0 \leq 2$ (omdat $-1 < \dfrac{-1}{\sqrt{3}}$ en $\dfrac{4}{\sqrt{3}} < 3$). Nu is direct na te gaan dat $(U_0, V_0) = (1, 0)$ of $(2, 1)$, en deze zijn beide van de vorm (u_k, v_k), dus is (U, V) dat ook, want $U + V\sqrt{3} = (U_0 + V_0\sqrt{3})(u_\ell + v_\ell\sqrt{3})$. ☺

Opgave 14 Laat $(x, y) = (X, Y)$ een willekeurige oplossing zijn van $x^2 - 3y^2 = -2$. Zonder verlies van algemeenheid mogen we aannemen dat $X \geq 1$ en $Y \geq 1$.

(a) Hoe definieer je nu (X_0, Y_0) zodat $(x, y) = (X_0, Y_0)$ een oplossing van $x^2 - 3y^2 = -2$ is, en vermoedelijk een kleine?

(b) Druk Y_0 uit in $u_\ell - v_\ell\sqrt{3}$ en $X - Y\sqrt{3}$.

(c) Bepaal onder- en bovengrens voor $X - Y\sqrt{3}$, en vervolgens voor Y_0.
Hint: ik kom uit op $1 \leq Y_0 \leq 3$.

(d) Concludeer dat Lemma 4 waar is.

2.5 Periodieke modulaire recurrente rijen

We hadden het probleem $x^2 - 3y^2 = -2$ met $y = 3^p$ op te lossen, en we hebben gezien dat $y = \pm y_k$, waarbij y_k een heel specifieke recurrente rij is. Vanwege de symmetrie in de rij en omdat $y_k > 0$ en $3^p > 0$ kunnen we ons beperken tot $y_k = 3^p$ met $k \geq 0$. Je hebt vermoedelijk de twee oplossingen al gezien: 1 en 3 komen voor.

Opgave 15 Herleid de oplossingen $y_0 = 3^0$ en $y_1 = 3^1$ tot de oplossingen $(x, a, b) = (1, 1, 1)$ resp. $(5, 1, 3)$ van de vergelijking $3^b - 2^a = x^2$.

Alle andere mogelijke oplossingen hebben $p \geq 2$. We gaan nu kijken naar y_k modulo 9, of daar misschien iets nuttigs te vinden is.

Een binaire recurrente betrekking ligt vast door twee opeenvolgende beginwaarden: als y_0 en y_1 bekend zijn, dan kunnen alle y_k berekend worden door $y_{k+1} = 4y_k - y_{k-1}$ herhaald toe te

passen; ook voor negatieve k werkt dit want de recurrente betrekking werkt in dit geval ook achteruit: $y_{k-1} = 4y_k - y_{k+1}$. Bekijken we zo'n rij nu modulo m, dan zijn er maar m mogelijke waarden die optreden, en voor twee opeenvolgende getallen in de rij dus maar hooguit m^2 mogelijkheden. Dat betekent dat we na enige tijd (hooguit m^2+2 stappen) een tweetal gaan tegenkomen dat we al eerder hebben gehad, en vanaf dat moment gaat het patroon zich exact herhalen. Ook achterstevoren werkt dit zo. Hieruit volgt dat de rij y_k modulo een of andere m periodiek zal zijn. Het ligt, zoals al aangegeven, voor de hand om modulo 9 te gaan kijken.

Opgave 16

(a) Bereken $y_k \pmod 9$ voor opeenvolgende k tot je een hele periode te pakken hebt. Hint: de periodelengte is 18, het is slim om te gebruiken dat de rij symmetrisch is, dan kun je twee kanten tegelijk uitwerken.

(b) Bepaal voor welke k geldt dat $y_k \equiv 0 \pmod 9$. Hierin zitten namelijk de mogelijke $y_k = 3^p$ met $p \geq 2$.

Nu gaat het wonder gebeuren.

Het blijkt dat $k = 4$ de eerste is met $y_k \equiv 0 \pmod 9$. Inderdaad, $y_4 = 153 = 9 \times 17$. Dus $y_4 \equiv 0 \pmod{17}$ is ook waar. Maar vanwege de symmetrie is dan ook $y_{-5} \equiv 0 \pmod{17}$.

Opgave 17

(a) Bereken $y_k \pmod{17}$ voor opeenvolgende k tot je een hele periode te pakken hebt. Hint: zelfde hint als in Opgave 16(a).

(b) Bepaal voor welke k geldt dat $y_k \equiv 0 \pmod{17}$.

(c) Concludeer dat $y_k = 3^p$ geen oplossingen heeft voor $p \geq 2$.

Einde wonder.

Dit bewijs was overduidelijk niet meer triviaal. Maar ik vind het nog wel elementair: er wordt geen diepe wiskunde gebruikt. Ik ben benieuwd of jullie vinden of hier met geïnteresseerde leerlingen (bijvoorbeeld bij Wiskunde D) iets mee te doen is.

3 De vergelijking van Ramanujan-Nagell

3.1 Inleiding

De vergelijking van Ramanujan-Nagell is $x^2 + 7 = 2^n$. Zoals in de syllabus al aangegeven, is deze vergelijking nogal beroemd, en zijn er vijf oplossingen. Dat kan aangetoond worden met de methode uit de vorige paragraaf, dus volledig elementair, maar het is wel meer werk.

Opgave 18 Laat zien dat $(x, n) = (3, 4)$ de enige oplossing met even n is.

3.2 Op weg naar een recurrente rij

Vanaf nu nemen we $n = 2p + 1$, en we schrijven het op te lossen probleem als

$$\boxed{x^2 - 2y^2 = -7 \text{ met } y = 2^p.}$$

We definiëren u_k, v_k nu door $u_k + v_k\sqrt{2} = (3 + 2\sqrt{2})^k$. Een klein tabelletje:

k	$\ldots$	-3	-2	-1	0	1	2	3	$\ldots$
u_k	$\ldots$	99	17	3	1	3	17	99	$\ldots$
v_k	$\ldots$	-70	-12	-2	0	2	12	70	$\ldots$

Opgave 19

(a) Laat zien dat alle oplossingen van $x^2 - 2y^2 = 1$ gegeven zijn door $(x, y) = (\pm u_k, \pm v_k)$.

(b) Laat zien dat de recurrente betrekkingen $u_{k+1} = 6u_k - u_{k-1}$ en $v_{k+1} = 6v_k - v_{k-1}$ gelden.

(c) Laat zien dat $v_{k+1} \leq 6v_k$ voor $k \geq 1$.

We definiëren x_k, y_k nu door $x_k + y_k\sqrt{2} = (1 + 2\sqrt{2})(3 + 2\sqrt{2})^k$. Een klein tabelletje:

k	$\ldots$	-3	-2	-1	0	1	2	3	$\ldots$
x_k	$\ldots$	-181	-31	-5	1	11	65	379	$\ldots$
y_k	$\ldots$	128	22	4	2	8	46	268	$\ldots$

Opgave 20

(a) Laat zien dat alle oplossingen van $x^2 - 2y^2 = -7$ gegeven zijn door $(x, y) = (\pm x_k, \pm y_k)$.

(b) Laat zien dat de recurrente betrekkingen $x_{k+1} = 6x_k - x_{k-1}$ en $y_{k+1} = 6y_k - y_{k-1}$ gelden.

Merk op dat de rij y_k nu niet meer symmetrisch is, en dat tot hiertoe het werk nog wel meeviel.

3.3 Periodieke modulaire recurrente rijen

Vanwege de grote oplossing $y_{-3} = 128$ ligt het voor de hand om als modulus 256 te kiezen. Het vervelende is echter dat de periode nu 128 lang is, en dat betekent wel wat meer werk. De ijverige doorzetter doet het wel in een uurtje. We geven de totale periode, om het je gemakkelijk te maken:

```
  2    8   46   12   26  144   70   20   50   24   94   28   74  160  118   36
 98   40  142   44  122  176  166   52  146   56  190   60  170  192  214   68
194   72  238   76  218  208    6   84  242   88   30   92   10  224   54  100
 34  104   78  108   58  240  102  116   82  120  126  124  106  [0]  150  132
130  136  174  140  154   16  198  148  178  152  222  156  202   32  246  164
226  168   14  172  250   48   38  180   18  184   62  188   42   64   86  196
 66  200  110  204   90   80  134  212  114  216  158  220  138   96  182  228
162  232  206  236  186  112  230  244  210  248  254  252  234  128   22    4
  2    8  ...
```

In paragraaf 3.5 geef ik aan waarom het berekenen van deze hele tabel niet nodig is om toch de benodigde informatie te verkrijgen.

Opgave 21 Voor welke k geldt dat $y_k \equiv 0 \pmod{256}$?

Nu zoeken we een andere modulus, waarvoor de periodelengte mooi is, liefst ook 128, maar 64 of 256 is vast ook wel goed. Merk op dat we nu niet het argument uit het vorige

hoofdstuk kunnen gebruiken dat toen de modulus 17 opleverde, alleen al niet omdat we nu y_{61} zouden moeten uitrekenen en factoriseren, en dat is toch echt een groot getal ($y_{61} = 676252684784883474368851846170474433564452846 08 = 2^8 \times 1007965417 \times 7037044669 \times 35699070317 \times 1043220688369273$), maar vooral ook vanwege het ontbreken van symmetrie: we hebben nu geen enkele garantie meer dat de periodelengtes modulo factoren van y_{61} op 256 passen (de periodelengte modulo 1007965417 is 251991354). We moeten wat anders verzinnen.

Een idee is om de computer aan te zetten en priemgetallen als modulus te proberen, net zolang tot je een prettige periodelengte tegenkomt (theorie die we niet behandelen voorspelt dat je grotere kans hebt bij priemgetallen die $\pm 1 \pmod{128}$ zijn). Dit blijkt bij 7681 te gebeuren: modulo 7681 heeft de periode een lengte van 256, en hier is die periode dan:

```
   2    8   46  268 1562 1423 6976 2028 5192 6081  570 5020 6507  3298 5600 7259
7230 5397 2109 7257 3028 3230  990 2710 7589 4419 3563 1597 6019  3793 1377 4469
2394 2214 3209 1678 6859 1071 7248 4012 1462 4760 4055 4208 5831    54 2174 5309
6637 3789  735  621 2991 1963 1106 4673 3889 3299  543 7640 6892 [2988] 3355 1780
7325 3765 7584 3334 4739 2057 7603 5156  290 4265 2257 1596 7319  3913  797  869
4417 2590 3442 2700 5077 4719  194 4126 1519 4988 5366 4165 4262  6045 1284 1659
 989 4275 1618 5433  256 3784 7086  327 2557 7334 3042 3237 1018  2871  846 2205
4703 2970 5436 6603 3458 6464 4602 5786 7071 5916 5382 3333 6935  7553 7659 7677
7679 7673 7635 7413 6119 6258  705 5653 2489 1600 7111 2661 1174  4383 2081  422
 451 2284 5572  424 4653 4451 6691 4971   92 3262 4118 6084 1662  3888 6304 3212
5287 5467 4472 6003  822 6610  433 3669 6219 2921 3626 3473 1850  7627 5507 2372
1044 3892 6946 7060 4690 5718 6575 3008 3792 4382 7138   41  789 [4693] 4326 5901
 356 3916   97 4347 2942 5624   78 2525 7391 3416 5424 6085  362  3768 6884 6812
3264 5091 4239 4981 2604 2962 7487 3555 6162 2693 2315 3516 3419  1636 6397 6022
6692 3406 6063 2248 7425 3897  595 7354 5124  347 4639 4444 6663  4810 6835 5476
2978 4711 2245 1078 4223 1217 3079 1895  610 1765 2299 4348  746   128   22    4
   2    8  ...
```

Opgave 22 Laat zien: als $y_k \equiv 0 \pmod{256}$ dan $y_k \equiv 2988$ of $4693 \pmod{7681}$.

Alweer een tegenvaller: er komen modulo 7681 geen nullen op de juiste plekken tevoorschijn, zoals in hoofdstuk 2. Maar ook daar weten we wel weer wat op. We moesten hebben dat $y_k = 2^p$, en we kunnen een tabel maken met alle mogelijke machten van 2 (mod 7681), en kijken of 2988 en 4693 erin staan. Het vervelende is dan weer dat dat een vrij grote tabel wordt: er staan 3840 getallen in, want $e = 3840$ is de eerste positieve exponent waarvoor $2^e \equiv 1 \pmod{7681}$. Maar als je het toch doet, dan wordt je moeite wel beloond: inderdaad staan 2988 en 4693 niet in de tabel met machten van 2 (mod 7681).

En daarmee is het bewijs rond. Verre van triviaal, maar ik vind het nog steeds elementair.

Overigens is het verschijnen van 7681 als modulus wel te verklaren, zie paragraaf 3.6.

3.4 Kortsluitingen

Met de techniek van het 'machtsverheffen door herhaald kwadrateren' kun je die twee laatste grote tabellen ook nog wel vermijden. Om te vinden wat y_{61} en y_{189} (mod 7681) zijn (nodig voor Opgave 22) kun je ook als volgt te werk gaan:

$x_{61} + y_{61}\sqrt{2} = (x_{-3} + y_{-3}\sqrt{2})(3 + 2\sqrt{2})^{64}$, $x_{189} + y_{189}\sqrt{2} = (x_{61} + y_{61}\sqrt{2})(3 + 2\sqrt{2})^{128}$, en $x_{-3} + y_{-3}\sqrt{2} = -181 + 128\sqrt{2}$, en om de hoge machten van $3 + 2\sqrt{2}$ modulo 7681 te berekenen hoeven we maar een paar keer te kwadrateren:

$(3+2\sqrt{2})^2 = 17+12\sqrt{2}$,
$(3+2\sqrt{2})^4 = (17+12\sqrt{2})^2 = 577+408\sqrt{2}$,
$(3+2\sqrt{2})^8 = (577+408\sqrt{2})^2 = 665857+470832\sqrt{2} \equiv 5291+2291\sqrt{2} \pmod{7681}$,
$(3+2\sqrt{2})^{16} \equiv (5291+2291\sqrt{2})^2 \equiv 2552+2126\sqrt{2} \pmod{7681}$,
$(3+2\sqrt{2})^{32} \equiv (2552+2126\sqrt{2})^2 \equiv 6112+5532\sqrt{2} \pmod{7681}$,
$(3+2\sqrt{2})^{64} \equiv (6112+5532\sqrt{2})^2 \equiv 0+7325\sqrt{2} \pmod{7681}$,
$(3+2\sqrt{2})^{128} \equiv (0+7325\sqrt{2})^2 \equiv -1 \pmod{7681}$,

en dus $x_{61}+y_{61}\sqrt{2} \equiv (-181+128\sqrt{2})7325\sqrt{2} \equiv 1036+2988\sqrt{2} \pmod{7681}$, en $x_{189}+y_{189}\sqrt{2} \equiv -1036-2988\sqrt{2} \equiv 6645+4693\sqrt{2}$. Dat is met een rekenmachientje op een regenachtige zaterdagmiddag nog wel te doen.

Overigens, het verschijnen van de 0 bij de 64-e macht is een wonder, maar wel een verklaarbaar wonder; het is nauw gerelateerd aan de reden dat 7681 hier een goede keuze is voor de modulus.

Net zo is kort te sluiten de controle dat 2988 geen macht van 2 is modulo 7681 (en voor 4693 gaat het precies zo, omdat $4693 \equiv -2988 \pmod{7681}$): we berekenen hun 3840e macht modulo 7681:

$\pmod{7681}$	$a=2$	$a=2988$	$\pmod{7681}$	$a=2$	$a=2988$
a^1	2	2988	$a^{64}=(a^{32})^2$	5564	6919
a^2	4	2822	$a^{128}=(a^{64})^2$	3666	4569
$a^4=(a^2)^2$	16	6168	$a^{256}=(a^{128})^2$	5487	6484
$a^8=(a^4)^2$	256	231	$a^{512}=(a^{256})^2$	5330	4143
$a^{16}=(a^8)^2$	4088	7275	$a^{1024}=(a^{512})^2$	4562	5095
$a^{32}=(a^{16})^2$	5569	3535	$a^{2048}=(a^{1024})^2$	4015	4926

Nu zien we dat $2^{3840} = 2^{2048}\cdot 2^{1024}\cdot 2^{512}\cdot 2^{256} \equiv 4015\cdot 4562\cdot 5330\cdot 5487 \equiv 1 \pmod{7681}$, en dus ook $(2^p)^{3840} \equiv 1 \pmod{7681}$, en $2988^{3840} \equiv 2988^{2048}\cdot 2988^{1024}\cdot 2988^{512}\cdot 2988^{256} \equiv 4926\cdot 5095\cdot 4143\cdot 6484 \equiv -1 \pmod{7681}$. Deze berekening past er op die zaterdagmiddag nog net bij.

De 3840-e machten van 2988 en elke macht van 2 zijn $\pmod{7681}$ verschillend, namelijk -1 resp. 1! Dan kan 2988 dus zelf ook geen macht van 2 zijn.

Wie de theorie van kwadraatresten modulo priemgetallen kent, ziet dat deze argumenten allemaal nog korter kunnen: 2988 (en 4693) zijn geen kwadraatresten $\pmod{7681}$, en 2 is dat wel; alleen voor 2988 is die controle een klein beetje rekenwerk, maar dat kan makkelijk met de hand.

3.5 Hoe de tabel van de periode $\pmod{256}$ te vermijden

Het doel is om controle te krijgen over wanneer $y_k \equiv 0 \pmod{256}$. Dit gaan we opbouwen $\pmod 8$, $\pmod{16}$, $\pmod{32}$, ... Eerst maar eens een tabelletje:
$y_k \pmod 8$: 2, 0, 6, 4, en dan periodiek,
$y_k \pmod{16}$: 2, 8, 14, 12, 10, 0, 6, 4, en dan periodiek,
$y_k \pmod{32}$: 2, 8, 14, 12, 26, 16, 6, 20, 18, 24, 30, 28, 10, 0, 22, 4 en dan periodiek,
en dat geeft al een beetje een patroon: kennelijk wordt de periode telkens tweemaal zo lang: de periode $\pmod{2^p}$ lijkt altijd 2^{p-1} te zijn, en de getallen in de tweede helft van de periode verschillen kennelijk altijd precies 2^{p-1} met die in de eerste helft van de periode. Dat is wel

aan te tonen. We bewijzen eerst het volgende:

$$(3+2\sqrt{2})^{2^{p-2}} \equiv 1+2^{p-1}\sqrt{2} \pmod{2^p} \text{ voor alle } p \geq 3.$$

(NB: voor $p=2$ is het niet waar: $3+2\sqrt{2} \not\equiv 1+2\sqrt{2} \pmod 4$.) Voor $p=3$ staat er $17+12\sqrt{2} \equiv 1+4\sqrt{2} \pmod 8$, en dat is waar. Veronderstel nu dat $(3+2\sqrt{2})^{2^{p-2}} \equiv 1+2^{p-1}\sqrt{2} \pmod{2^p}$ waar is voor één of andere $p \geq 3$, dan berekenen we $(3+2\sqrt{2})^{2^{p-1}} \pmod{2^{p+1}}$: er geldt $(3+2\sqrt{2})^{2^{p-1}} = \left((3+2\sqrt{2})^{2^{p-2}}\right)^2 \equiv \left(1+2^{p-1}\sqrt{2}+\alpha 2^p\right)^2$ voor de een of andere gehele α, en dat geeft dan $1+2^p\sqrt{2}+2^{2p-1}+\alpha 2^{p+1}+2^{2p}\alpha\sqrt{2}+\alpha^2 2^{2p}$, en $\pmod{2^{p+1}}$ wordt dit $1+2^p\sqrt{2}$, omdat $2p-1 \geq p+1$. Het inductiebewijs is nu compleet. Een direct gevolg is dat $(3+2\sqrt{2})^{2^{p-2}} \equiv 1 \pmod{2^{p-1}}$, en dus ook dat $(3+2\sqrt{2})^{2^{p-1}} \equiv 1 \pmod{2^p}$.

Nu kijken we eerst naar $x_{i+2^{p-1}}+y_{i+2^{p-1}}\sqrt{2} \pmod{2^p}$, en we merken op dat $x_{i+2^{p-1}}+y_{i+2^{p-1}}\sqrt{2} = (x_i+y_i\sqrt{2})(3+2\sqrt{2})^{2^{p-1}} \equiv (x_i+y_i\sqrt{2}) \pmod{2^p}$, dus de periode $\pmod{2^p}$ is een deler van 2^{p-1}. Dan een slagje dieper: $x_{i+2^{p-2}}+y_{i+2^{p-2}}\sqrt{2} \pmod{2^p} = (x_i+y_i\sqrt{2})(3+2\sqrt{2})^{2^{p-2}} \equiv (x_i+y_i\sqrt{2})(1+2^{p-1}\sqrt{2}) \pmod{2^p}$, en dus $y_{i+2^{p-1}} \equiv y_i+2^{p-1}x_i \pmod{2^p}$, en omdat x_i altijd oneven is, staat hier precies wat we observeerden: $y_{i+2^{p-2}} \equiv y_i+2^{p-1} \pmod{2^p}$. Hieruit volgt meteen dat de periode $\pmod{2^p}$ inderdaad tweemaal zo groot is als de periode $\pmod{2^{p-1}}$.

Nu zoeken we waar $y^k \equiv 0 \pmod{2^{256}}$, en dat kunnen we van onderaf opbouwen: we beginnen met $y_k \equiv 0 \pmod 8 \iff k \equiv 1 \pmod 4$, en nu weten we dat $y_k \equiv 0 \pmod{16}$ alleen kan optreden voor $k \equiv 1 \pmod 8$ of voor $k \equiv 5 \pmod 8$, maar niet voor beiden. Makkelijk is te vinden dat het de 5 is. Dan weten we dat $y_k \equiv 0 \pmod{32}$ alleen kan optreden voor $k \equiv 5 \pmod{16}$ of voor $k \equiv 13 \pmod{16}$, maar niet voor beiden. Makkelijk (hoe?) is te vinden dat het de 13 is. Enzovoorts.

3.6 Waarom 7681 hier opduikt

We willen een priemgetal q vinden waarvoor de periode van $y_k \pmod q$ een prettige macht van 2 is. Voor periode 2^r hebben we $x_{i+2^r}+y_{i+2^r}\sqrt{2} = (x_i+y_i\sqrt{2})(3+2\sqrt{2})^{2^r} \equiv x_i+y_i\sqrt{2} \pmod q$, We willen dus $(3+2\sqrt{2})^{2^r} \equiv 1 \pmod q$. Hoe kunnen we dat bereiken?

Definieer de gehele getallen a_k, b_k door $a_k+b_k\sqrt{2} = (3+2\sqrt{2})^{2^k}$, met dus $a_0=3, b_0=2$, en $a_k+b_k\sqrt{2} = (a_{k-1}+b_{k-1}\sqrt{2})^2$, met andere woorden, $a_k = a_{k-1}^2+2b_{k-1}^2$, $b_k = 2a_{k-1}b_{k-1}$. Hier zijn er een paar: $(a_0,b_0) = (3,2)$,
$(a_1,b_1) = (17,12)$,
$(a_2,b_2) = (577,408)$,
$(a_3,b_3) = (665857,470832)$,
$(a_4,b_4) = (886731088897,627013566048)$,
$(a_5,b_5) = (1572584048032918633353217,1111984844349868137938112)$,
$(a_6,b_6) = (4946041176255201878775086487573351061418968498177,$
$3497379255757941172020851852070562919437964212608)$,
en dat gaat dus gauw uit de hand lopen. Maar bedenk nu het volgende: neem voor een zekere r een priemfactor q van a_{r-2}. Dan geldt $a_{r-2}^2-2b_{r-2}^2=1$, en dus $2b_{r-2}^2 \equiv -1 \pmod q$. Dan volgt $a_{r-1} = a_{r-2}^2+2b_{r-2}^2 \equiv -1 \pmod q$, en $b_{r-1} \equiv 2a_{r-2}b_{r-2} \equiv 0 \pmod q$, en vervolgens dus $a_r = a_{r-1}^2+2b_{r-1}^2 \equiv 1 \pmod q$, en $b_r \equiv 2a_{r-2}b_{r-2} \equiv 0 \pmod q$, precies wat we willen.

Omdat we op zoek zijn naar periode $128 = 2^7$ ligt het voor de hand om $r = 7$ te kiezen. De priemfactoren van a_5 zijn 11777, en twee grotere, die we eigenlijk te groot vinden. Er blijkt dat $y_{61} \equiv 11649 \pmod{11777}$, maar helaas gaat dit niet direct tot een tegenspraak leiden, want 11649 is wel degelijk een macht van 2 (mod 11777). Maar we kunnen ook met $r = 8$ werken, en dan blijkt $q = 7681$ een deler te zijn van a_6, en zoals we gezien hebben gaat dat inderdaad werken. Daar komt het priemgetal 7681 dus vandaan.

Het eigenlijke wonder is dus niet zozeer het optreden van 7681, maar het feit dat op de juiste plekken in de periodieke rij modulo 7681 getallen blijken te staan die geen macht van 2 kunnen zijn modulo deze priem.

NB: het factoriseren van grote getallen is natuurlijk lastig. Veel handiger is om de rijen a_k en b_k te berekenen modulo een heleboel kleine priemgetallen (met een computer is dat een peuleschil), dan komen de goede kandidaat-factoren zoals 11777 en 7681 vanzelf bovendrijven.

Antwoorden deel 2

1 $(a,b) = (1,0), (1,1), (2,1), (3,2)$.

2(a) $3 \equiv -1 \pmod 4$, dus $3^b \equiv (-1)^b \pmod 4$, en $(-1)^b = 1$ als b even is, en is $-1 \equiv 3 \pmod 4$ als b oneven is.
(b) Als $a \geq 2$ dan is $2^a \equiv 0 \pmod 4$, en de vergelijking geeft dan $3^b \equiv 1 \pmod 4$. Dan zegt (a) dat b even moet zijn.
(c) Stel de twee machten zijn 2^r en 2^s, met $r > s$, en $2^r - 2^s = 2$. Dan is $r \geq s+1$, en $2 = 2^r - 2^s \geq 2^{s+1} - 2^s = 2^s$, en dus $s \leq 1$. Met $s = 1$ volgt $r = 2$, en met $s = 0$ volgt niets.
(d) $z^2 - 1 = (z+1)(z-1)$, en als dit een macht van 2 is dan moeten de factoren dat ook zijn, dus er zijn r, s zodat $z + 1 = 2^r$ en $z - 1 = 2^s$. Aftrekken geeft $2^r - 2^s = 2$, en (c) zegt dan $r = 2, s = 1$, en er volgt $z = 3$, en $a = r + s = 3$.
(e) Als $a \geq 2$ dan is volgens (a) b even, en schrijven we $3^b = z^2$. De vergelijking luidt dan $z^2 - 1 = 2^a$, en volgens (d) heeft dit slechts één oplossing: $(z, a) = (3, 3)$. dat geeft $(a, b) = (3, 2)$. En als $a \leq 1$ dan geeft $a = 1$ de oplossing $(a, b) = (1, 1)$, en $a = 0$ geeft geen oplossing. De oplossingen zijn dus $(a, b) = (1, 1), (3, 2)$.

3(a) 1 en 3.
(b) Als $a \geq 3$ dan is $2^a \equiv 0 \pmod 8$, en de vergelijking geeft dan $3^b \equiv -1 \pmod 8$. Dit kan niet volgens (a).
(c) Uit (b) volgt dat $a \leq 2$. Met $a = 2$ is $b = 1$, met $a = 1$ is $b = 0$, en met $a = 0$ is er geen oplossing. De oplossingen zijn dus $(a, b) = (1, 0), (2, 1)$.

4(a) $(a, b, x) = (0, 0, 0), (1, 1, 1), (3, 2, 1), (1, 3, 5), (5, 4, 7)$.
(b) $(a, b, x) = (0, 0, 0), (1, 0, 1), (2, 1, 1)$.
(c) $(a, b, x) = (0, 1, 2), (3, 0, 3), (4, 2, 5)$.

5(a) $0, 1, 4$.
(b) Er zijn zes mogelijkheden: $0 + 1 = 1, 0 + 3 = 3, 1 + 1 = 2, 1 + 3 = 4, 4 + 1 = 5, 4 + 3 = 7$.
(c) Als $a \geq 3$ dan geeft de vergelijking dat $x^2 + 3^b \equiv 0 \pmod 8$, maar dat is onmogelijk volgens (b). Dus is $a \leq 2$. Als $a \leq 2$ dan is $3^b = 2^a - x^2 \leq 4 - 0 = 4$, dus $b \leq 1$. Alle mogelijkheden afgaan geeft als oplossingen uitsluitend $(a, b, x) = (0, 0, 0), (1, 0, 1), (2, 1, 1)$.

6(a) Kwadraten $\pmod 3$ zijn $0, 1$. Als $b \geq 1$ dan geeft de vergelijking $2^a \equiv x^2 \equiv 0, 1 \pmod 3$, en dan moet a wel even zijn. Als er oplossingen met oneven a zijn, dan dus met $b = 0$. Dat geeft $2^a + 1 = x^2$, en Opgave 2(d) zegt dan $(a, b, x) = (3, 0, 3)$.
(b) Uit $x^2 - y^2 = 3^b$ volgt dat er een c is met $x - y = 3^c$ en $x + y = 3^{b-c}$, met $0 \leq c \leq b - c$. Aftrekken geeft $y = \frac{1}{2}(3^{b-a} - 3^a)$, en omdat y een macht van 2 is heeft-ie geen factor 3, en daarom moet $a = 0$.
(c) We moeten nu oplossen: $\frac{1}{2}(3^b - 1) = 2^{a/2}$. Opgave 2 geeft als mogelijkheden slechts $(1 + \frac{1}{2}a, b) = (1, 1), (3, 2)$, dus $(a, b, x) = (0, 1, 2), (4, 2, 5)$. Alle oplossingen zijn dus $(a, b, x) = (0, 1, 2), (3, 0, 3), (4, 2, 5)$.

7 Als $b \geq 1$ dan geeft de vergelijking $x^2 + 1 \equiv 0 \pmod 3$. Volgens Opgave 6(a) heeft dit geen oplossingen. Dus is $b = 0$ en $x = 0$. Dit geeft dus alleen de oplossing $(a, b, x) = (0, 0, 0)$.

8(a) Als $a \geq 2$ dan geeft de vergelijking $3^b \equiv x^2 \pmod 4$. Dit kan alleen met even b.
(b) Uit $y^2 - x^2 = 2^a$ volgt $y + x = 2^c$ en $y - x = 2^d$, met $c > d$ en $c + d = a$. Aftrekken geeft $2^c - 2^d = 2x$, en omdat x oneven is moet nu $d = 1$ zijn, en $c = a - 1$. Optellen geeft dan

$y = 2^{c-1} + 2^{d-1} = 2^{a-2} + 1$.
(c) We schrijven nu $y^2 = 3^b$, de vergelijking wordt dan $y^2 - x^2 = 2^a$. Dan zegt (b) dat $2^{a-2} + 1 = 3^{b/2}$, en Opgave 2 geeft de oplossingen $(a-2, \frac{1}{2}b) = (1,1), (3,2)$. Dit leidt tot $(a,b,x) = (3,2,1), (5,4,7)$.

9 Als b even is dan zijn 3^b en x^2 twee kwadraten die 2 verschillen. Die bestaan niet.

10 Stel dat $y_1 \neq y_2$. We kunnen de vergelijking nu onschrijven tot $\sqrt{3} = \dfrac{x_1 - x_2}{y_2 - y_1}$, en hier staat dat $\sqrt{3}$ een rationaal getal is, quod non. Dus is $y_1 = y_2$, en nu volgt meteen dat ook $x_1 = x_2$.
Waarom was $\sqrt{3}$ ook al weer irrationaal? Stel $\sqrt{3} = \dfrac{p}{q}$, waarbij p en q geen deler gemeen hebben. Dan is $p^2 = 3q^2$, dus p is een drievoud, zeg $p = 3r$, en kan q niet ook nog een drievoud zijn. Maar er volgt wel $q^2 = \frac{1}{3}(3r)^2 = 3r^2$, dus zou q wel een drievoud zijn. Tegenspraak.

11 Merk op dat $(x_1 + y_1\sqrt{3})(x_2 + y_2\sqrt{3}) = (x_1x_2 + 3y_1y_2) + (x_1y_2 + x_2y_1)\sqrt{3} = x_3 + y_3\sqrt{3}$, en net zo volgt $(x_1 - y_1\sqrt{3})(x_2 - y_2\sqrt{3}) = x_3 - y_3\sqrt{3}$. Nu hebben we

$$\begin{aligned} x_3^2 - 3y_3^2 &= (x_3 + y_3\sqrt{3})(x_3 - y_3\sqrt{3}) \\ &= (x_1 + y_1\sqrt{3})(x_2 + y_2\sqrt{3}) \cdot (x_1 - y_1\sqrt{3})(x_2 - y_2\sqrt{3}) \\ &= (x_1 + y_1\sqrt{3})(x_1 - y_1\sqrt{3}) \cdot (x_2 + y_2\sqrt{3})(x_2 - y_2\sqrt{3}) \\ &= (x_1^2 - 3y_1^2)(x_2^2 - 3y_2^2) = d_1d_2. \end{aligned}$$

12(a) $(2+\sqrt{3})^2 = 4 + 4\sqrt{3} + 3 = 4(2+\sqrt{3}) - 1$.
(b) $(2+\sqrt{3})^{k+1} = 4(2+\sqrt{3})^k - (2+\sqrt{3})^{k-1}$, en in termen van u_k en v_k staat hier $u_{k+1} + v_{k+1}\sqrt{3} = (4u_k - u_{k-1}) + (4v_k - v_{k-1})\sqrt{3}$. Pas nu Lemma 1 toe.
(c) Als $k \geq 1$ dan is $v_{k-1} \geq 0$ en dus $v_{k+1} = 4v_k - v_{k-1} \leq 4v_k$.

13(a) $(x,y) = (1,1)$.
(b) We definiëren x_k, y_k, volgens Lemma 1, door $x_k + y_k\sqrt{3} = (1+\sqrt{3})(2+\sqrt{3})^k$. Volgens Lemma 2 zijn dit oplossingen van $x^2 - 3y^2 = -2$.
(c) Net zo als Opgave 12(b).
(d)

k	$\ldots$	-4	-3	-2	-1	0	1	2	3	$\ldots$
u_k	$\ldots$	-71	-19	-5	-1	1	5	19	71	$\ldots$
v_k	$\ldots$	41	11	3	1	1	3	11	41	$\ldots$

Vanwege symmetrie hoeven we alleen naar $k \geq 0$ te kijken.

14(a) We nemen $\ell \geq 0$ zodat $v_\ell \leq Y < v_{\ell+1}$, en dan nemen we X_0, Y_0 met $X_0 + Y_0\sqrt{3} = (X + Y\sqrt{3})(u_\ell - v_\ell\sqrt{3})$.
(b) $Y_0 = Yu_\ell - Xv_\ell = Y(u_\ell - v_\ell\sqrt{3}) - (X - Y\sqrt{3})v_\ell$.
(c) $X - Y\sqrt{3} = \dfrac{-2}{X + Y\sqrt{3}}$, dus $\dfrac{-2}{Y\sqrt{3}} < X - Y\sqrt{3} < 0$. Met de grens $0 < u_\ell - v_\ell\sqrt{3} < \dfrac{1}{v_\ell\sqrt{3}}$ uit het bewijs van Lemma 3 krijgen we nu $0 < Y_0 < \dfrac{Y}{v_\ell\sqrt{3}} + \dfrac{2v_\ell}{Y\sqrt{3}}$. Uit de keuze van ℓ volgt $0 < Y_0 < \dfrac{v_{\ell+1}}{v_\ell\sqrt{3}} + \dfrac{2}{\sqrt{3}}$, Opgave 12(c) geeft dan $0 < Y_0 < \dfrac{4}{\sqrt{3}} + \dfrac{2}{\sqrt{3}} = \dfrac{6}{\sqrt{3}}$, dus $1 \leq Y_0 \leq 3$.

(d) De enige mogelijkheden voor (X_0, Y_0) zijn $(1,1)$ en $(5,3)$, en die zijn beiden van de juiste vorm. Dus is (X,Y) dat ook, vanwege $X + Y\sqrt{3} = (X_0 + Y_0\sqrt{3})(u_\ell + v_\ell\sqrt{3})$.

15 $y = 1,3$ geeft $x = 1,5$ en $p = 0,1$ dus $b = 1,3$, terwijl $a = 1$ was.

16(a)

k	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
$y_k \pmod 9$	8	8	6	7	4	0	5	2	3	1	1	3	2	5	0	4	7	6	8	8

(b) Er geldt: $y_k \equiv 0 \pmod 9$ als en slechts als $k \equiv 4 \pmod 9$.

17(a)

k	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
$y_k \pmod{17}$	16	16	14	6	10	0	7	11	3	1	1	3	11	7	0	10	6	14	16	16

(b) Er geldt: $y_k \equiv 0 \pmod{17}$ als en slechts als $k \equiv 4 \pmod 9$.
(c) Zodra $p \geq 2$ is, is $y_k = 3^p \equiv 0 \pmod 9$. Volgens Opgave 16(b) is dan $k \equiv 4 \pmod 9$. Volgens (b) is dan $y_k \equiv 0 \pmod{17}$, dus 17 is een deler van y_k zodra 9 een deler is van y_k. Dan kan y_k dus niet meer gelijk zijn aan een macht van 3.

18 Schrijf $y^2 = 2^n$, dan geeft de vergelijking $y^2 - x^2 = 7$, dus omdat 7 een priemgetal is, is $y + x = 7$ en $y - x = 1$. Dit geeft meteen $y = 4$ en $x = 3$. Toevallig is y inderdaad een macht van 2. We vinden als enige oplossing $(x, n) = (3, 4)$.

19 We doen dit op dezelfde manier als in paragraaf 2.4, en we doen eerst (b) en (c), en dan pas (a). Natuurlijk gelden Lemma's 1 en 2 ook als daarin $\sqrt{3}$ (resp. 3) vervangen worden door $\sqrt{2}$ (resp. 2).
19(b) Er geldt $(3 + 2\sqrt{2})^2 = 6(3 + 2\sqrt{2}) - 1$ (schrijf uit!). Dan volgt $(3 + 2\sqrt{2})^{k+1} = 6(3 + 2\sqrt{2})^k - (3 + 2\sqrt{2})^{k-1}$, en het aangepaste Lemma 1 zegt dan dat $u_{k+1} = 6u_k - u_{k-1}$ en $v_{k+1} = 6v_k - v_{k-1}$ voor alle k.
19(c) Als $k \geq 1$ is dan volgt uit (b) meteen dat $v_{k+1} = 6v_k - v_{k-1} \leq 6v_k$.
19(a) De kleinste oplossing van $x^2 - 2y^2 = 1$ is $(x, y) = (u_1, v_1) = (3, 2)$. Het aangepaste Lemma 2 zegt nu dat voor iedere k geldt dat $u_k^2 - 2v_k^2 = 1$. Een paar van deze getallen staan in de tabel boven opgave 19.
We bewijzen nu het aangepaste Lemma 3, dat alle oplossingen van $x^2 - 2y^2 = 1$ van de vorm $(x, y) = (\pm u_k, \pm v_k)$ zijn. Laat $(x, y) = (U, V)$ een willekeurige oplossing zijn van $x^2 - 2y^2 = 1$. Zonder verlies van algemeenheid mogen we aannemen dat $U \geq 1$ en $V \geq 0$. Omdat v_k voor $k \geq 0$ strict stijgend is, is er een $\ell \geq 0$ waarvoor geldt $v_\ell \leq V < v_{\ell+1}$. We definiëren nu de gehele getallen U_0, V_0 door $U_0 + V_0\sqrt{2} = (U + V\sqrt{2})(u_\ell - v_\ell\sqrt{2})$. Uit het aangepaste Lemma 2 volgt dat $(x, y) = (U_0, V_0)$ ook een oplossing is van $x^2 - 2y^2 = 1$. We laten zien dat deze oplossing niet erg groot kan zijn.
Het aangepaste Lemma 2 geeft $V_0 = Vu_\ell - Uv_\ell$. Dit schrijven we als $V_0 = V(u_\ell - v_\ell\sqrt{2}) - (U - V\sqrt{2})v_\ell$, omdat we de twee uitdrukkingen tussen haakjes goed kunnen afschatten. Namelijk, $u_\ell - v_\ell\sqrt{2} = \dfrac{1}{u_\ell + v_\ell\sqrt{2}}$ en dus is $0 < u_\ell - v_\ell\sqrt{2} < \dfrac{1}{v_\ell\sqrt{2}}$, en $U - V\sqrt{2} = \dfrac{1}{U + V\sqrt{2}}$, en dus is $0 < U - V\sqrt{2} < \dfrac{1}{V\sqrt{2}}$. Samen geeft dit $\dfrac{-v_\ell}{V\sqrt{2}} < V_0 < \dfrac{V}{v_\ell\sqrt{2}}$. De keuze van ℓ zorgt er nu voor dat $\dfrac{-v_\ell}{v_\ell\sqrt{2}} < V_0 < \dfrac{v_{\ell+1}}{v_\ell\sqrt{2}}$, en (b) zegt $v_{k+1} \leq 6v_k$, dus volgt $0 \leq V_0 \leq 4$ (omdat $-1 < \dfrac{-1}{\sqrt{2}}$ en $\dfrac{6}{\sqrt{2}} < 5$). Nu is direct na te gaan dat $(U_0, V_0) = (1, 0)$ of $(3, 2)$, en deze zijn beide van de vorm (u_k, v_k), dus is (U, V) dat ook, want $U + V\sqrt{2} = (U_0 + V_0\sqrt{2})(u_\ell + v_\ell\sqrt{2})$.

20 Eenvoudig is na te rekenen dat de kleinste positieve oplossing van $x^2 - 2y^2 = -7$ gegeven wordt door $(x, y) = (x_0, y_0) = (1, 2)$.
20(b) Volgens het aangepaste Lemma 2 zijn (x_k, y_k) allemaal oplossingen van $x^2 - 2y^2 = -7$. En ook deze rijen voldoen aan de recurrente betrekkingen $x_{k+1} = 6x_k - x_{k-1}$ en $y_{k+1} = 6y_k - y_{k-1}$, met het inmiddels bekende argument.
20(a) Laat $(x, y) = (X, Y)$ een oplossing zijn van $x^2 - 2y^2 = -7$. Zonder verlies van algemeenheid mogen we aannemen dat $X \geq 1$ en $Y \geq 1$. We nemen $\ell \geq 0$ zodat $v_\ell \leq Y < v_{\ell+1}$, en dan nemen we X_0, Y_0 met $X_0 + Y_0\sqrt{2} = (X + Y\sqrt{2})(u_\ell - v_\ell\sqrt{2})$. Dan schrijven we $Y_0 = Yu_\ell - Xv_\ell = Y(u_\ell - v_\ell\sqrt{2}) - (X - Y\sqrt{2})v_\ell$. We schatten af: $X - Y\sqrt{2} = \dfrac{-7}{X + Y\sqrt{2}}$, dus $\dfrac{-7}{Y\sqrt{2}} < X - Y\sqrt{2} < 0$. Met de grens $0 < u_\ell - v_\ell\sqrt{2} < \dfrac{1}{v_\ell\sqrt{2}}$ uit het bewijs van Opgave 19(a) krijgen we nu $0 < Y_0 < \dfrac{Y}{v_\ell\sqrt{2}} + \dfrac{7v_\ell}{Y\sqrt{2}}$. Uit de keuze van ℓ volgt $0 < Y_0 < \dfrac{v_{\ell+1}}{v_\ell\sqrt{2}} + \dfrac{7}{\sqrt{2}}$, Opgave 19(c) geeft dan $0 < Y_0 < \dfrac{6}{\sqrt{2}} + \dfrac{7}{\sqrt{2}} = \dfrac{13}{\sqrt{2}}$, dus $1 \leq Y_0 \leq 9$. De enige mogelijkheden voor (X_0, Y_0) zijn nu makkelijk te vinden: $(1, 2)$ en $(11, 8)$, en die zijn beiden van de juiste vorm. Dus is (X, Y) dat ook, vanwege $X + Y\sqrt{2} = (X_0 + Y_0\sqrt{2})(u_\ell + v_\ell\sqrt{2})$.

21 Voor alle $k \equiv 61 \pmod{128}$.

22 Uit Opgave 21 volgt $k \equiv 61 \pmod{128}$. Dat betekent $k \equiv 61$ of $189 \pmod{256}$, en de tabel leert dan $y_k \equiv 2988$ of $4693 \pmod{7681}$.