Priemgetallen

Inhoud

1. Inleiding

Waarom priemgetallen?

Volgens de hoofdstelling van de rekenkunde is elk natuurlijk getal groter dan 1 op juist één manier te schrijven als product van priemgetallen, op de volgorde van de factoren na. Die stelling leert ons dat priemgetallen de bouwstenen van de natuurlijke getallen zijn. Dat is meteen ook de reden waarom ze priem genoemd worden. De benaming is afkomstig van het Latijnse primus wat eerste betekent. Alleen al daarom vinden we het zinvol om priemgetallen te behandelen in het wiskundeonderwijs.

Priemgetallen en de leerplannen

Noch in de eindtermen van het lager, noch in die van het secundair onderwijs vinden we het begrip ‘priemgetal’ terug. In de eerste graad komt het begrip meestal wel aan bod, net als de begrippen grootste gemeenschappelijke deler en kleinste gemeenschappelijk veelvoud van twee of meer natuurlijke getallen. De leerlingen leren deze begrippen voornamelijk in de ‘functionele zin’ bijvoorbeeld om gemeenschappelijke noemers te vinden bij het optellen van breuken.

De leerstof rond deelbaarheid en priemgetallen biedt anderzijds een uitgelezen kans om aandacht te besteden aan bewijsvormen en -technieken. Je komt er pareltjes van bewijzen tegen die de kracht van een elegante redenering prachtig illustreren. Om die reden stond er in de jaren ’80 en ’90 van de vorige eeuw een stukje getaltheorie op het leerplan van het vierde jaar. Bij de invoering van de eindtermen en de aanpassing van de leerplannen aan dat nieuwe kader, heeft de getaltheorie moeten plaats maken voor ruimtemeetkunde, statistiek en kansrekenen.

In de huidige leerplannen van de derde graad vind je het als een keuzonderwerp terug in de richtingen met 6 uur wiskunde (vrij onderwijs) of 7 uur wiskunde per week (gemeenschapsonderwijs). Het materiaal dat we in deze loep uitwerken kadert binnen een keuzeonderwerp of een stuk in de vrije ruimte en we richten ons op leerlingen uit een richting met 6 of meer uur wiskunde.

Het opzet van deze loep

Wat je in deze loep vindt, is niet zomaar een heruitgave van de leerstof van destijds in het vierde jaar. Onze bezorgdheid is hier niet zozeer een algemene, rigoureuze, axiomatische opbouw van de getaltheorie. Onze aandacht gaat bijvoorbeeld niet naar basisstellingen zoals ‘een deler van een deler van a is zelf een deler van a’, maar we focussen op allerlei aspecten van priemgetallen: eigenschappen, vermoedens, bewijzen, zoektocht naar (grote) priemgetallen... Je kunt er dieper of minder diep op ingaan afhankelijk van de voorkennis en de interesse van de leerlingengroep. Sommige resultaten (bijvoorbeeld de stelling over de priemontbinding) zijn zo vertrouwd voor de leerlingen dat ze geen moeite hebben om ermee te werken. Het kost je als leerkracht meestal heel wat moeite om de leerlingen te overtuigen van de noodzaak van een bewijs voor dergelijke stellingen. Daar gaan we hier dus niet op in en we maken liever plaats voor minder evidente stellingen en eigenschappen die hier en daar wel wat verwondering kunnen opwekken bij de leerlingen. Bij het bewijzen van die eigenschappen komen we een kleurrijk palet van bewijsvormen tegen: existentiebewijs, bewijs door contrapositie, bewijs uit het ongerijmde en bewijs door inductie.

Er komen niet alleen theoretische beschouwingen aan bod in deze loep, maar we proberen de theorie ook uit op voorbeelden. Als die getallen wat groter worden (en dus realistischer), ontstaat de nood aan rekenkracht. Het omzetten van een theoretische stelling naar een werkwijze die met de grafische rekenmachine kan worden uitgevoerd, is een nieuwe bijkomende uitdaging die bepaalde leerlingen zeker aanspreekt. Af en toe wordt de computer (als een black box) ingeschakeld om voorbeelden na te rekenen.

De werkteksten

De meeste werkteksten uit deze loep zijn niet bedoeld om zelfstandig door de leerlingen te laten doorwerken. Afhankelijk van de klasgroep worden sommige vragen beter samen met de leerkracht opgelost in een goed onderwijsleergesprek. De werktekst is dan eerder als een leidraad te gebruiken.

Het materiaal in deze loep is zeker geen ‘alles of niets’-verhaal. Je kunt er gerust enkele stukken uit nemen los van de rest.

In deze loep

In een eerste paragraaf frissen we enkele begrippen op die nodig zijn verder in de loep. Je zult er moeten voor zorgen dat de leerlingen ook over deze voorkennis beschikken. We staan hier niet stil bij de didactische aanpak van deze begrippen. Hiervoor verwijzen we naar twee vroegere nummers, namelijk UW4/4 en UW24/3.

In paragraaf 3 komen enkele eigenschappen van priemgetallen aan bod en onderzoeken we curiositeiten. Zo zullen we aantonen dat er oneindig veel priemgetallen zijn en dat de afstand tussen

twee opeenvolgende priemgetallen zo groot kan zijn als we maar willen. We proberen vat te krijgen op de spreiding van de priemgetallen. We sluiten de paragraaf af met het verschijnsel van priemtweelingen en priemmeerlingen.

Paragraaf 4 wordt besteed aan enkele open problemen. Het is verrassend dat er zo veel eenvoudig te formuleren vragen met priemgetallen zijn waar de wiskundige wereld tot op de dag van vandaag geen antwoord op heeft.

De laatste paragraaf gaat over priemtesten. (Grote) priemgetallen worden gebruikt bij de beveiliging van data. Je moet dus over testen beschikken om na te gaan of een getal een priemgetal is. We geven voorbeelden van deterministische en van probabilistische tests. Met de eerste soort kun je met zekerheid zeggen of het getal priem is of niet, bij de tweede kun je hoogstens zeggen dat het getal *waarschijnlijk* priem is.

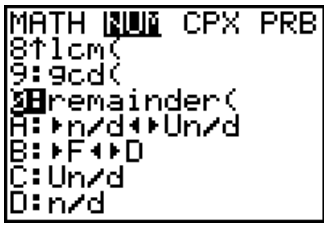
2. Enkele voorafgaande begrippen

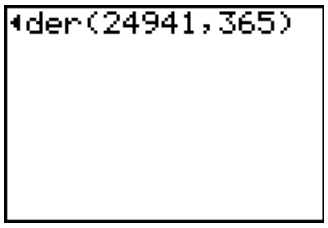
a. Modulorekenen

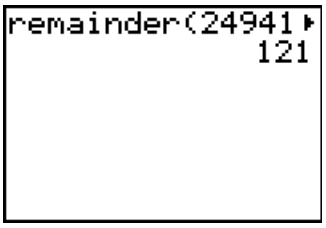
Als we het over priemgetallen hebben, zullen we moeten redeneren met gehele getallen. Een belangrijke techniek die we ook in deze loep nodig zullen hebben, is het modulorekenen. Het rekenen met uren in een dag, is een mooi voorbeeld van dit principe. Als je 's avonds om 22 uur naar een 3 uur durende film begint te kijken, dan eindigt deze film om 1 uur. Niemand zal zeggen dat die film duurt tot 25 uur. We rekenen "modulo 24", of met andere woorden, op een veelvoud van 24 na. In de wiskunde noteren we dit als $25 \equiv 1 (\mathrm{mod}\, 24)$ en lezen we dit als "25 is congruent met 1 modulo 24".

In het algemeen betekent de notatie $a \equiv b (\mathrm{mod}\, m)$ dat het getal $a - b$ deelbaar is door *m*, of anders gezegd, dat *a* gelijk is aan *b* op een veelvoud van *m* na. Zo is $349 \equiv 61 (\mathrm{mod}\, 96)$ omdat $349 - 61 = 288 = 3 \cdot 96$.

Een belangrijk kenmerk van twee getallen *a* en *b* die congruent zijn modulo *m* is dat ze bij de euclidische deling door *m* dezelfde rest opleveren. Omdat er slechts *m* verschillende resten mogelijk zijn bij deling door *m*, kunnen we dank zij het modulorekenen een willekeurig getal steeds reduceren tot een getal tussen 0 en $m - 1$, dat het *residu* van *a* modulo *m* wordt genoemd. Om voor kleinere getallen *a* en *m* het residu van *a* modulo *m* uit te rekenen voeren we gewoon de euclidische deling uit. Zo is $13 \equiv 3 (\mathrm{mod}\, 5)$ omdat $13 = 2 \cdot 5 + 3$. Voor grotere getallen kun je dit berekenen met behulp van het nieuwe besturingssysteem van de TI84plus (zie de schermafdrukken hieronder).







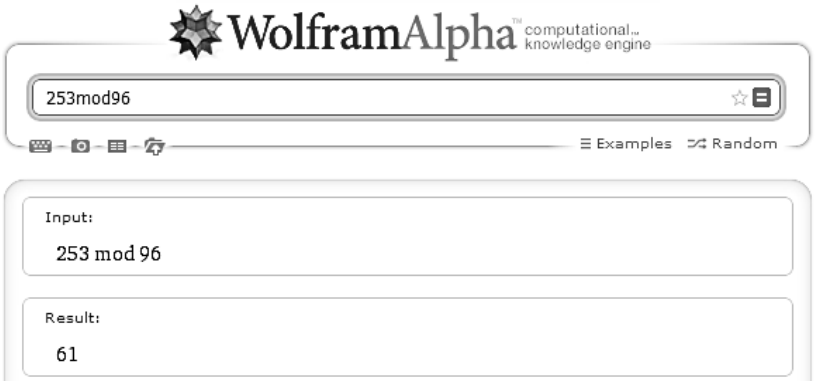
Je vindt dus dat $24\,941 \equiv 121 (\mathrm{mod}\, 365)$. Wie deze functie niet heeft op zijn rekentoestel, kan het volgende programmaatje op zijn toestel zetten. Je kunt het gewoon overtikken ofwel downloaden van onze site.

```
PROGRAM:MOD
:Input "A= ",A
:Input "M= ",M
:A-M*int(A/M)→A
:Disp A
:
```

```
prgmMOD
A= 24941
M= 365
                121
               Done
```

```
A= -13
M= 5
                  2
               Done
```

Een ander hulpmiddel vind je online bij WolframAlpha.



Verder zullen we gebruik maken van de *restklassen* modulo *m*. Hieronder verstaan we de verzameling van alle gehele getallen die congruent zijn met een bepaald getal. We noteren zo'n restklasse met $\overline{a}$. Er geldt dus:

$$\overline{a} = \{b \in \mathbb{Z} \mid b \equiv a (\text{mod}\, m)\}.$$

Merk op dat $\overline{a} = \overline{b}$ als en slechts als $a \equiv b (\text{mod}\, m)$. De bewerkingen op gehele getallen zijn over te dragen op de restklassen op de volgende manier:

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{en} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Deze definities zijn maar bruikbaar als de resultaten onafhankelijk zijn van de gekozen representanten. We illustreren dit voor de berekening van $\overline{3} + \overline{5}$ modulo 6. De definitie geeft $\overline{3} + \overline{5} = \overline{8} = \overline{2}$. Uit de restklasse $\overline{3}$ hadden we even goed de representant 27 kunnen nemen en de klasse $\overline{5}$ kunnen we laten vertegenwoordigen door het getal 59. De optelling geeft $\overline{27 + 59} = \overline{86} = \overline{2}$. We vinden dus hetzelfde resultaat! Ook bij de vermenigvuldiging maakt het niet uit welke van de koppels representanten we nemen.

$$\overline{3 \cdot 5} = \overline{15} = \overline{3} \text{ en } \overline{27 \cdot 59} = \overline{1593} = \overline{3}.$$

Uiteraard volstaat een voorbeeld niet om de geldigheid van de definitie te bewijzen, maar is daar een algemeen bewijs voor nodig. In de loep van UW24/3 vind je enkele suggesties om het modulorekenen aan te brengen in de klas.

b. Priemgetallen en ontbinden in priemfactoren

We gaan er van uit dat de definities en basiseigenschappen met betrekking tot deelbaarheid in $\mathbb{Z}$ gekend zijn. In deze loep worden regelmatig (soms impliciet) eigenschappen van priemgetallen en

priemdelers gebruikt. Voor de lezers die minder vertrouwd zijn met deze materie, volgt hier een opsomming van enkele van die definities, begrippen of eigenschappen.

- Als $a, d \in \mathbb{N}_0$ en *d* is een deler van *a*, dan is $d \leq a$
- Een natuurlijk getal *p* is een priemgetal als en slechts als *p* juist twee verschillende natuurlijke getallen als delers heeft (1 en zichzelf).
- Natuurlijke getallen groter dan 1 die geen priemgetallen zijn (en dus echte delers hebben buiten 1 en zichzelf) noemt men samengestelde getallen.
- Elk natuurlijk getal groter dan 1 is deelbaar door een priemgetal.
- Elk natuurlijk getal groter dan 1 kan op juist één manier ontbonden worden in priemfactoren, op de volgorde van de factoren na (hoofdstelling van de rekenkunde).

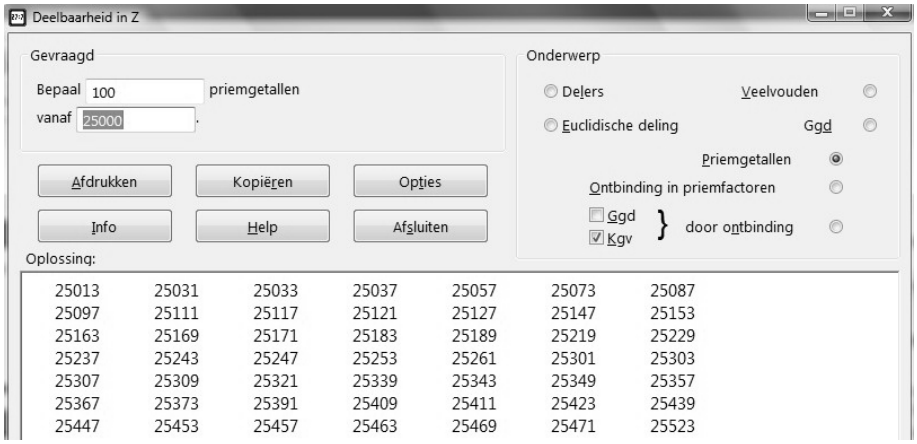
Merk nog op dat uit de definitie van een priemgetal volgt dat het getal 1 geen priemgetal is. 1 heeft slechts één natuurlijke deler namelijk 1 zelf. Tot de negentiende eeuw beschouwden de meeste wiskundigen het getal 1 wél als een priemgetal. De definitie stelde tot dan geen restricties aan het aantal verschillende delers. De aanpassing van de definitie werd gedaan met het oog op de hoofdstelling van de rekenkunde. Als 1 een priemgetal is, dan kan een natuurlijk getal op oneindig veel manieren geschreven worden als product van priemfactoren: $5 = 1 \cdot 5 = 1 \cdot 1 \cdot 5 = \ldots$

3. Eigenschappen en curiositeiten

Naar aanleiding van Einsteins vermeende uitspraak ‘God does not play dice with the universe’, zei de Amerikaanse wiskundige Carl Pomerance in een lezing (enkele maanden na de dood van de excentrieke Hongaarse wiskundige Paul Erdös in 1996) dat het antwoord van Paul Erdös hierop zou zijn: ‘God may not play dice with the universe, but something strange is going on with the prime numbers…’ (zie [8]).

In deze paragraaf bespreken we een aantal eigenschappen van priemgetallen en onderzoeken we enkele van die rariteiten. Het zoeken van priemgetallen, priemdelers, priemfactoren-ontbinding… vraagt meestal veel rekenwerk. Daarom is het aangewezen om de computer mee in te schakelen als je eigenschappen van priemgetallen wil onderzoeken. In deze loep maken we o.a. gebruik van het softwarepakket SoftMaths dat enkele onderdelen bevat die voornamelijk kunnen gebruikt worden in de wiskundelessen van de eerste en de tweede graad van het secundair onderwijs. Eén van deze onderdelen komt ondertussen niet meer voor in de leerplannen van de tweede graad, maar is wel te gebruiken in de eerste graad of bij keuze-onderwerpen uit de leerplannen van de derde graad: deelbaarheid in $\mathbb{Z}$.

Deze toepassing berekent de delers en veelvouden van een natuurlijk getal, voert de euclidische deling uit van gehele getallen, berekent de grootste gemene deler en het kleinste gemeen veelvoud van twee of drie natuurlijke getallen en bepaalt priemgetallen vanaf een zelf gekozen getal.



SoftMaths is gratis te downloaden op [12]. De software is heel gebruiksvriendelijk. Er is nagenoeg geen uitleg nodig zodat leerlingen er onmiddellijk mee van start kunnen gaan.

a. Hoeveel priemgetallen zijn er?

In deze paragraaf tonen we aan dat er oneindig veel priemgetallen zijn en bekijken we enkele oneindige rijen van priemgetallen. We krijgen regelmatig de gelegenheid om dieper in te gaan op verschillende bewijsvormen en -technieken. Het is echter niet onze bedoeling om een systematische bespreking te maken van alle bewijstechnieken. Het hangt van de klasgroep af hoe ver je kan gaan in de bespreking van bewijsvormen en hoe formeel je dat doet.

Vóór we ingaan op de kwestie van het aantal priemgetallen, gaan we op zoek naar die priemgetallen.

Op zoek naar priemgetallen, Mersennegetallen

De definitie zegt dat een getal priem is als het juist twee verschillende delers heeft: 1 en zichzelf. In deze werktekst laten we zien dat het zoeken naar priemgetallen slimmer kan dan alleen de definitie te gebruiken. Ook de zogenaamde Mersennegetallen komen een eerste keer aan bod.

1. Als je wilt nagaan of een natuurlijk getal n een priemgetal is, moet je dan voor alle getallen kleiner dan n onderzoeken of het delers zijn?

   Ga dit na door voorbeelden te bekijken. Als je wilt nagaan of 503 een priemgetal is, moet je dan voor alle getallen van 2 t.e.m. 502 onderzoeken of het delers zijn?

   (Nee. Vrij snel zullen de leerlingen inzien dat je zeker niet alle getallen moet onderzoeken. Het volstaat om priemdelers te onderzoeken en bovendien is er een bovengrens, $\sqrt{n}$.)

2. Een natuurlijk getal n groter dan 1 dat geen priemgetal is, heeft steeds minstens één priemdeler kleiner dan of gelijk aan $\sqrt{n}$. Toon dat aan.

   (Stel dat n geen priemgetal is, dan is $n = ab$, met $1 < a \leq b < n$ (dit kun je veronderstellen zonder afbreuk te doen aan de algemeenheid). Dan is $a^2 \leq ab = n$ en dus is $a \leq \sqrt{n}$. Het volstaat bijgevolg om delers kleiner dan of gelijk aan $\sqrt{n}$ te onderzoeken. Bovendien: een

deler die kleiner is dan of gelijk aan $\sqrt{n}$ *heeft een priemdeler die zeker kleiner is dan of gelijk aan* $\sqrt{n}$ *en ook een priemdeler is van* n*. Dus: om te onderzoeken of* $n \in \mathbb{N}_0 \setminus \{1\}$ *een priemgetal is, volstaat het om na te kijken of* n *deelbaar is door een priemgetal dat kleiner is dan of gelijk is aan* $\sqrt{n}$ *.)*

3. Mersennegetallen zijn getallen M_n van de vorm $M_n = 2^n - 1$ waarbij n een natuurlijk getal is. Marin Mersenne (1588-1648) was een Franse wiskundige die probeerde een formule te vinden die alle priemgetallen zou voortbrengen of bevatten. Hij bedacht daartoe o.a. de getallen van de vorm $2^n - 1$ die nu naar hem zijn vernoemd. Onderzoek met de methode van hierboven of het dertiende Mersennegetal, $2^{13} - 1$, een priemgetal is.

   ($\sqrt{2^{13} - 1} = \sqrt{8191} \approx 90{,}50$ *en omdat* 8191 *niet deelbaar is door de opeenvolgende priemgetallen tot en met* 89*, is* 8191 *een priemgetal)*

4. Is de volgende bewering correct:

   als p een priemgetal is, dan is $M_p = 2^p - 1$ ook priem?

   (De bewering is niet correct. Dit kan je makkelijk aantonen door een tegenvoorbeeld te geven. Het elfde Mersennegetal, $2^{11} - 1$*, is geen priemgetal. Het is deelbaar door* 23*. In onze tijd is het vinden van zo'n tegenvoorbeelden niet moeilijk met behulp van de ZRM of computer. In de tijd van Fermat en zelfs later bij Euler was dat helemaal niet evident en toch vonden ze die tegenvoorbeelden (zie* [9]*). Het is interessant om de leerlingen met deze bedenking te confronteren.)*

5. We bekijken de omgekeerde bewering:

   als $M_p = 2^p - 1$ een priemgetal is, dan is p ook priem. (1)

   Onderzoek m.b.v. SoftMaths of je deze hypothese zou kunnen steunen door voorbeelden te onderzoeken.

   (O.a. voor p gelijk aan 2, 3, 5, 7, 13, 17, 19, 31 *geldt dat* M_p *priem is. De hypothese houdt voorlopig stand.)*

6. Uitspraak (1) kan via een andere weg worden bewezen. Uit de logica (meer bepaald de wet van de contrapositie) weten we namelijk dat (1) gelijkwaardig is met:

   als p geen priemgetal is, dan is $M_p = 2^p - 1$ ook geen priemgetal. (2)

   En deze laatste bewering kan vrij eenvoudig worden bewezen, waardoor ook de gelijkwaardige uitspraak (1) tegelijkertijd bewezen is. Bewijs (2) door te veronderstellen dat $p = ab$ met $a > 1$ en $b > 1$ en vervolgens $M_p = 2^{ab} - 1$ in factoren te ontbinden.

   (Als $p = ab$ *met* $a > 1$ *en* $b > 1$ *dan geldt:*

   $M_p = 2^{ab} - 1 = \left(2^a\right)^b - 1^b = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1)$

   met $2^a - 1 > 1$ *en* $2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1 > 1$*. Bijgevolg is* M_p *niet priem.)*

Rechtstreeks bewijs

Na of tijdens deze werktekst zou de leerkracht even kunnen uitweiden over enkele bewijsvormen. Het bewijs dat gegeven werd bij vraag 2 van deze werktekst is een voorbeeld van een rechtstreeks bewijs

(of ook wel een bewijs door deductie genoemd). Je begint hierbij met een aantal aannames en je redeneert van daaruit rechtstreeks naar de te bewijzen stelling. De leerlingen kennen deze bewijsvorm en hebben al heel wat eigenschappen op deze manier bewezen. Bij vraag 6 gebruiken we een andere bewijsmethode, die de leerlingen meestal nog niet kennen, het bewijs door contrapositie.

Bewijs door contrapositie

Hier zou de leerkracht even dieper kunnen ingaan op een wet uit de logica: de contrapositiewet. Hiervoor hoef je niet meteen de hele theorie van de logica ter sprake te brengen. Het is voldoende dat je de uitspraak 'M_p is een priemgetal' vervangt door de afkorting *a* en de uitspraak '*p* is een priemgetal' door de letter *b*. In de logica is het niet langer van belang wat de inhoud is van *a* en *b*. Er bestaan bepaalde verbanden tussen uitspraken *a* en *b* die universeel zijn. Een van deze verbanden is de wet van de contrapositie:

$a \Rightarrow b$ is equivalent met niet $b \Rightarrow$ niet a

of in symbolen:

$$(a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a).$$

Als we $\neg b \Rightarrow \neg a$ bewijzen, dan hebben we omwille van deze equivalentie tegelijkertijd ook $a \Rightarrow b$ bewezen.

Het is uiteraard niet absoluut nodig dat je verder uitweidt over bewijstechnieken en de bijbehorende wetten uit de logica. Maar zeker in richtingen met een zwaarder wiskundepakket kan het zinvol zijn om regelmatig begrippen uit de logica toe te passen op wiskundige redeneringen. Het kan leerlingen houvast bieden, het leert hen meer formeel te werken, het geeft hen meer inzicht in een redenering (bijvoorbeeld bij het verduidelijken van redeneerfouten)… In de loep van UW27/2 vind je hierover meer uitleg en suggesties.

Bewijs uit het ongerijmde

In de les kunnen we dan nog andere methodes bestuderen om na te gaan of een getal priem is. Zo is er de bekende zeef van Eratosthenes en zijn er ook heel snelle methoden. In hoofdstuk 5 gaan we hier dieper op in. Je kunt echter nooit voor alle natuurlijke getallen onderzoeken of het priemgetallen zijn. Er is dus een meer algemene methode nodig om te bepalen hoeveel priemgetallen er zijn. Euclides bewees al in 325 v.Chr. in zijn verzameling van 13 boeken *De Elementen* (Στοιχεια) dat er oneindig veel priemgetallen bestaan. Zijn bewijs is eenvoudig, elegant en krachtig en is vandaag nog steeds een van de beroemdste bewijzen. Bij [14] vind je een vrije vertaling van Euclides' oorspronkelijke stelling en het bewijs zoals hij het formuleerde. Hierbij zijn natuurlijke getallen lengtes van lijnstukken en dat komt ons vreemd over. Wij kennen het bewijs van Euclides dan ook in een meer vertrouwde gemoderniseerde vorm. Het is een bewijs uit het ongerijmde.

> We tonen aan dat het aantal priemgetallen oneindig is. (1)
>
> Veronderstel dat de verzameling priemgetallen een eindig aantal elementen heeft. Of nog:
>
> stel dat $p_1, p_2, \ldots, p_n$ de enige priemgetallen zijn. (2)
>
> Beschouw het getal $P = 1 + p_1 p_2 \cdots p_n$. Dit getal is groter dan elk priemgetal uit de lijst p_1, p_2, …, p_n en is dus zelf geen priemgetal. Bijgevolg heeft P een unieke priemfactorenontbinding en bestaat er een priemgetal p dat een deler is van P. Hierbij kan p nooit een van de priemgetallen van de lijst $p_1, p_2, \ldots, p_n$ zijn, want bij deling van P door

p_1, p_2, … of p_n is de rest telkens 1. Dus is P deelbaar door een priemgetal dat niet in de lijst p_1, p_2, …, p_n voorkomt. Dit is een contradictie.

Bewering (2) leidt tot een contradictie en is dus niet waar. M.a.w. het aantal priemgetallen is niet eindig. Bijgevolg is de uitspraak uit (1) waar: er is een oneindig aantal priemgetallen.

Je kunt ook hier meer aandacht besteden aan de techniek van het bewijs uit het ongerijmde en eventueel een zijsprong maken naar de logica. De leerlingen kennen het bewijs uit het ongerijmde meestal nog uit de tweede graad (waar ze bewezen dat $\sqrt{2}$ irrationaal is). Deze bewijsvorm steunt op de wet van de negatie van een implicatie. In het bewijs van hierboven kunnen we de uitspraak uit (1), het aantal priemgetallen is oneindig, ook schrijven als volgt:

als *W* de verzameling is van alle priemgetallen dan heeft *W* een oneindig aantal elementen.

Door de uitspraak '*W* is de verzameling van alle priemgetallen' te vervangen door de letter *a* en de uitspraak 'W heeft een oneindig aantal elementen' te vervangen door *b*, wordt het te bewijzen:

$$a \Rightarrow b\,.$$

We kunnen nu met deze letters verder redeneren. Uit de logica kennen we volgend verband:

niet ($a \Rightarrow b$) is equivalent met a en niet b

of meer formeel:

$$\neg(a \Rightarrow b) \quad \Leftrightarrow \quad (a \wedge \neg b)\,.$$

Dit noemen we de wet van de negatie van een implicatie. Bij een bewijs uit het ongerijmde neemt men $a \wedge \neg b$ aan en laat men zien dat dit tot een contradictie leidt. Omwille van de bovenstaande equivalentie betekent dit dat $\neg(a \Rightarrow b)$ onwaar is of nog dat $a \Rightarrow b$ waar is. Meer concreet voor het bewijs van hierboven kunnen we uitspraak (2) herschrijven als

W is de verzameling van alle priemgetallen en *W* heeft een eindig aantal elementen.

Dit is $a \wedge \neg b$. We laten zien dat deze veronderstelling tot een contradictie leidt waaruit volgt dat het te bewijzen, $a \Rightarrow b$, waar is.

Existentiebewijs

In 2006 publiceerde Filip Saidak, een Slowaaks wiskundige, een nieuw bewijs van de stelling dat er oneindig veel priemgetallen bestaan (zie [14]). Net als het bewijs van Euclides blinkt Saidaks bewijs uit door eenvoud.

Stel dat n een geheel getal groter dan 1 is. De getallen n en $n+1$ hebben geen gemeenschappelijke priemfactoren omdat hun verschil 1 is. Dat betekent dat het getal $N_1 = n(n+1)$ ten minste twee verschillende priemfactoren heeft. Voor de getallen N_1 en N_1+1 geldt hetzelfde: omdat hun verschil 1 is, hebben ze ten minste twee verschillende priemfactoren. Het getal $N_2 = N_1(N_1+1) = n(n+1)\big[n(n+1)+1\big]$ heeft dus minimaal drie verschillende priemfactoren. Dit proces kan eindeloos worden voortgezet: het getal N_k heeft ten minste $k+1$ verschillende priemfactoren. Omdat dit voor elk natuurlijk getal k geldt, kan de rij priemgetallen nooit ophouden en zijn er oneindig veel priemgetallen.

Een belangrijk verschil tussen het bewijs van Euclides en dat van Saidak is dat de bewijs*vorm* van Saidak helemaal anders is. Terwijl het bewijs van Euclides een bewijs uit het ongerijmde is, is het bewijs van Saidak een existentiebewijs. Saidak construeert natuurlijke getallen met een willekeurig

groot aantal priemfactoren en laat zo zien dat er oneindig veel priemgetallen bestaan. Merk op dat Saidak de priemgetallen zelf niet construeert, maar wel een verzameling natuurlijke getallen met een willekeurig groot aantal priemfactoren.

In het boek [1] beschreven Martin Aigner en Günter Ziegler zes verschillende bewijzen voor de oneindigheid van het aantal priemgetallen. Dit werk is opgedragen aan Paul Erdös, die, hoewel hij ongelovig was, beweerde dat God een boek had waarin alle elegantste bewijzen voor wiskundige stellingen van het hele heelal genoteerd waren. In één van deze zes bewijzen tonen de auteurs aan dat alle Fermatgetallen (getallen van de vorm $2^{2^n}+1$) onderling ondeelbaar zijn, ze hebben geen gemeenschappelijke priemfactoren. Op deze manier wordt er een oneindige verzameling van priemgetallen opgesteld. We namen dit bewijs op in de bibwijzer van UW20/4.

Een existentiebewijs mag niet verward worden met een bewijs door constructie, hoewel het verschil ertussen vaak subtiel is. Bewijzen door constructie komen niet alleen voor in de wiskunde (bewijs dat er een geheel getal bestaat dat tussen een kwadraat en een derdemacht geklemd zit), maar ook bv. in de biologie (bewijs dat er een zoogdier is dat in zee leeft en eieren legt). Het komt er op aan om het gezochte object op te sporen en de vreemde eigenschappen ervan aan te tonen.

Ook al kennen we tot nu geen formule waarmee we alle priemgetallen kunnen genereren, toch kunnen we dus een oneindige rij van priemgetallen opstellen. In de volgende werktekst stellen we zelf zo enkele oneindige rijen van priemgetallen op.

Een oneindige verzameling van priemgetallen

Wiskundigen zoeken al heel lang naar een formule waarmee we alle priemgetallen kunnen genereren. Tot nu toe is deze formule nog niet gevonden. De rij van de opeenvolgende priemgetallen is een rij waarvan het voorschrift niet gekend is. Wel kunnen we de methode van het bewijs van Euclides gebruiken om een oneindige rij (u_n) van onderling verschillende priemgetallen op te stellen. Begin met $u_1 = 2$ en stel u_{n+1} het kleinste priemgetal dat $1 + u_1 u_2 ... u_n$ deelt. Gebruik SoftMaths.

1. Bereken u_2, u_3, u_4 en u_5.
   ($u_2 = 3, u_3 = 7, u_4 = 43$ en $u_5 = 13$)
2. Kan een getal twee keer voorkomen in die rij? Bewijs je antwoord.
   (Nee, een getal kan geen twee keer voorkomen in die rij. Stel dat een getal p wel een tweede keer voorkomt in de rij. Dit betekent dat p het kleinste priemgetal is dat

$1+u_1u_2\cdots u_n$ deelt terwijl één van de termen u_1, u_2,…, u_n gelijk is aan p. Dit is een contradictie want de rest bij de Euclidische deling van $1+u_1u_2\cdots u_n$ door p is dan altijd gelijk aan 1.*)*

Er kan dus geen herhaling optreden in de rij (u_n), het is een oneindige rij van onderling verschillende priemgetallen.

Analoog kunnen we een andere rij (v_n) van priemgetallen construeren: begin met $v_1 = 2$ en stel v_{n+1} het kleinste priemgetal dat $1+v_1^2v_2^2...v_n^2$ deelt.

3. Bepaal v_2, v_3, v_4 en v_5.

   ($v_2 = 5$, $v_3 = 101$, $v_4 = 1\,020\,101$ en $v_5 = 53$)

4. We zien dat 3 niet voorkomt in het beperkte rijtje priemgetallen v_1, v_2, ..., v_k uit de vorige vraag. Kan 3 dan een deler zijn van $1+v_1^2v_2^2...v_n^2$? Met ander woorden: kan v_{k+1} gelijk zijn aan 3?

   (Nee, want als 3 *niet in het rijtje voorkomt dan is* 3 *geen deler van $v_1v_2\cdots v_k$ en dus is $v_1v_2\cdots v_k \equiv 1 \pmod 3$ of $v_1v_2\cdots v_k \equiv 2 \pmod 3$. Bijgevolg is $(v_1v_2\cdots v_k)^2 \equiv 1 \pmod 3$ en dan is $1+v_1^2v_2^2\cdots v_k^2 \equiv 2 \pmod 3$. Het is hier niet strikt nodig dat leerlingen kunnen modulorekenen. Je kunt dit eenvoudig omzeilen door de modulonotatie niet te gebruiken en minder formeel te werken.)*

5. Kan 3 ooit voorkomen in (v_n)?

   (Nee. Bij vraag 3 *hebben we gezien dat* 3 *niet voorkomt in het beperkt rijtje v_1, v_2, …, v_5. In vraag* 4 *toonden we aan: als* 3 *niet voorkomt in een beperkt rijtje v_1, v_2, ..., v_k dan kan v_{k+1} ook niet gelijk zijn aan* 3*. Door deze twee resultaten te combineren, kunnen we besluiten dat v_6 niet gelijk is aan* 3*. We krijgen op die manier een nieuw rijtje v_1, v_2, ..., v_5, v_6 waarin* 3 *niet voorkomt. Door dit opnieuw te combineren met hetgeen we bewezen in vraag* 4*, vinden we dat v_7 niet gelijk is aan* 3*… We krijgen een kettingreactie waaruit we kunnen concluderen dat* 3 *nooit kan voorkomen in (v_n). Dit is een vorm van bewijs door inductie. Ook deze bewijsvorm kun je in de les eventueel verder toelichten. Bij een bewijs door inductie werk je in twee stappen. In een eerste deel toon je aan dat de bewering waar is voor de eerste elementen van een verzameling. Dit noemt men de basis van het bewijs. Daarna volgt de inductiestap waarin je de volgende uitspraak bewijst: áls de bewering waar is voor de eerste k elementen van de verzameling dan is ze ook waar voor het volgende element. Door deze twee resultaten iteratief toe te passen, krijg je een kettingreactie waaruit het te bewijzen volgt.)*

We zien dus dat niet alle priemgetallen voorkomen in (v_n).

6. Is de rij (v_n) een rij van onderling verschillende priemgetallen? Bewijs je antwoord.

   (Ja. Het bewijs verloopt volledig analoog als bij vraag 2*.)*

De rij (v_n) is dus een oneindige rij van onderling verschillende priemgetallen, maar toch bevat ze niet alle priemgetallen!

7. Komt 5 voor in de rij (u_n) met $v_1 = 2$ en v_{n+1} het kleinste priemgetal dat $1+v_1^2v_2^2...v_n^2$ deelt?

(Als je de volgende termen uit de priemgetallenrij berekent, vind je 53, 5 *en* 6 221 671. *Het priemgetal* 5 *komt wel degelijk voor.)*

8. Verzin zelf een recursief voorschrift van een nieuwe oneindige rij van onderling verschillende priemgetallen.

   (Een mogelijkheid is de rij (u_n) *die je verkrijgt als volgt: begin met* $u_1 = 2$ *en stel* u_{n+1} *het kleinste priemgetal dat* $1 + u_1^3 u_2^3 \cdots u_n^3$ *deelt.)*

Het beroemde bewijs van Euclides leert ons dat de lijst van priemgetallen nooit volledig is, hoe groot je die lijst ook maakt. Maar hoe zijn die priemgetallen dan verdeeld? Het lijkt logisch dat er steeds minder priemgetallen voorkomen naarmate de onderzochte getallen groter en groter worden. In de volgende paragraaf gaan we hier dieper op in.

b. Priemwoestijnen en de distributie van priemgetallen

Als we willen onderzoeken hoe de priemgetallen verdeeld zijn, dan komen we onvermijdelijk bij de vraag naar de afstand tussen twee opeenvolgende priemgetallen.

Afstand tussen priemgetallen

1. Onderzoek (met SoftMaths) de afstand tussen twee opeenvolgende priemgetallen. Is deze afstand constant? Neemt hij toe of af? Of zie je daar helemaal geen systeem in? Is er een minimale afstand? Is er een maximale afstand?

   (Bedoeling van deze vraag is dat de leerlingen patronen zoeken in de priemgetallen die zij heel eenvoudig met SoftMaths genereren. Verderop zullen hun vermoedens dan bevestigd of ontkracht worden. Men kan immers aantonen dat priemgetallen globaal gezien steeds schaarser worden naarmate de getallen groter worden, al zijn er daarop uitzonderingen: de priemtweelingen met onderlinge tussenafstand 2. Men vermoedt dat er zelfs oneindig veel priemtweelingen (paren priemgetallen van de vorm $(p, p+2)$*) zijn. Dat is één van de vele openstaande problemen uit de getaltheorie. We bespreken dit verderop.)*

2. Als p priem is, kan dan $p+1$ priem zijn? Verklaar!

   (Ja, voor $p =$ 2 *is* $p+1$ *priem. Maar als* $p > 2$ *en p is priem dan is* $p+1$ *altijd even en dus niet priem.)*

3. Kan $p+2$ priem zijn als p priem is?

   *(Ja, bv. (*3,5*), (*17,19*). Men zegt dan dat p en* $p+2$ *priemtweelingen zijn. Met SoftMaths kun je snel ook grote paren priemtweelingen vinden bv. (*30 137, 30 139*).)*

4. Bewijs dat in de rij van $k-1$ opeenvolgende getallen $k!+2$, $k!+3$, …, $k!+k-1$, $k!+k$ met $k > 1$ geen enkel priemgetal voorkomt.

   ($k!+2$ *is deelbaar door* 2, $k!+3$ *is deelbaar door* 3 *enz.)*

5. Als de afstanden tussen twee opeenvolgende priemgetallen groot zijn, spreken we van priemwoestijnen. Kunnen de gaten tussen twee opeenvolgende priemgetallen willekeurig groot worden?

   (Ja, dit kun je onmiddellijk afleiden uit de eigenschap die in de vorige opgave werd bewezen.)

De ‘gaten’ tussen twee opeenvolgende priemgetallen kunnen dus willekeurig groot worden! Er zijn wel oneindig veel priemgetallen, maar we vermoeden dat ze steeds dunner gezaaid zijn. De kans dat een heel groot getal priem is, wordt kleiner naarmate het getal groter wordt omdat er dan meer echte delers mogelijk zijn. In de volgende werktekst gaan we hier dieper op in.

Eenzame priemgetallen?

In 1975 merkte de Duitse wiskundige Don Zagier tijdens een lezing het volgende op:

> Er zijn twee feiten over de verdeling van priemgetallen, waarvan ik u zo overweldigend hoop te overtuigen dat zij permanent in uw geheugen gegrift staan. De eerste is dat, ondanks hun eenvoudige definitie en rol als bouwstenen van de natuurlijke getallen, de priemgetallen tussen de natuurlijke getallen als onkruid groeien, waarbij zij schijnbaar aan geen andere wet dan aan de wetten van het toeval gehoorzamen, en niemand kan voorspellen, waar het volgende priemgetal zal opduiken. Het tweede feit is des te meer verbazingwekkend, want het stelt precies het tegenovergestelde: de priemgetallen vertonen een verbluffende regelmaat, er bestaan wetten die hun gedrag regeren, en de priemgetallen gehoorzamen met bijna militaire precisie aan deze wetten.

Je hebt zeker al een indruk gekregen van het onkruid-karakter van de priemgetallen. In deze werktekst zal je meer te weten komen over het militaire karakter van deze bijzondere getallen.

In de wiskunde wordt het aantal priemgetallen kleiner dan of gelijk aan x genoteerd als $\pi(x)$.

1. Zoek het aantal priemgetallen tussen 1 en 100. Gebruik SofthMaths! Wat is de gemiddelde afstand tussen de priemgetallen tussen 1 en 100? Gebruik de juiste notaties voor de gevonden getallen.

   (Het aantal priemgetallen tussen 1 *en* 100 *is* $\pi(100)=25$*, dus de gemiddelde afstand tussen die priemgetallen is* $\dfrac{100}{\pi(100)}=4$*.)*

2. Doe hetzelfde voor de priemgetallen tussen 1 en 500, tussen 1 en 1000.

   $\left(\pi(500)=88;\ \frac{500}{\pi(500)}=5{,}68;\ \pi(1000)=168;\ \frac{1000}{\pi(1000)}=5{,}95\right)$

3. Vul nu de volgende tabel aan.

x	$\pi(x)$	$\frac{x}{\pi(x)}$
10^2		
$5\cdot10^2$		
10^3		
10^4	1 229	
10^5	9 592	
10^6	78 498	
10^7	664 579	
10^8	5 761 455	

   (De ingevulde tabel.)

x	$\pi(x)$	$\frac{x}{\pi(x)}$
10^2	25	4
$5\cdot10^2$	88	5,68
10^3	168	5,95
10^4	1 229	8,14
10^5	9 592	10,43
10^6	78 498	12,74
10^7	664 579	15,05
10^8	5 761 455	17,36

4. Maak een grafische voorstelling met op de *x*-as de waarden voor *x* en op de *y*-as de waarden van $\frac{x}{\pi(x)}$. Ken je een functie die een gelijkaardige grafiek heeft?

   (Een logaritmische functie.)

Het grondtal van de logaritmische functie die we verderop nodig hebben, is het getal *e*. Mocht je dit getal nog niet ontmoet hebben: het is, net zoals het getal π, een transcendent getal dat een belangrijke rol speelt in de wiskunde. Meer bepaald is

$$e=\lim_{x\to+\infty}\left(1+\frac{1}{x}\right)^x\approx 2{,}718\,281\,828\,459.$$

De logaritmische functie met grondtal *e* noemt men de natuurlijke logaritme. Ze wordt genoteerd als ln (en dus niet $^e\log$). Op je rekentoestel vind je een speciale toets voor de natuurlijke logaritme. Reken na dat ln 10 = 2,3025…

5. Vul nu de volgende tabel aan.

x	$\ln x$
10^2	
$5 \cdot 10^2$	
10^3	
10^4	
10^5	
10^6	
10^7	
10^8	

*(*4,61*;* 6,21*;* 6,91*;* 9,21*;* 11,51*;* 13,82*;* 16,12*;* 18,42*)*

6. Vergelijk de laatste kolommen van de tabellen die je moest invullen. Wat stel je vast?

(We stellen vast dat $\frac{x}{\pi(x)} \approx \ln x$ *. De waarden van* $\ln x$ *zijn telkens iets groter dan die van* $\frac{x}{\pi(x)}$*.)*

Jacques Hadamard (1865-1963), een Frans wiskundige, en Charles-Jean de La Vallée-Poussin (1866-1962), een Leuvense wiskundige, bewezen in 1896 dat $\pi(x)$ ongeveer gelijk wordt aan $\frac{x}{\ln x}$ wanneer x groot is. Meer bepaald bewezen zij dat $\lim_{x \to +\infty} \frac{\pi(x)}{x / \ln x} = 1$.

7. Kun je de bewering dat $\pi(x)$ ongeveer gelijk is aan $\frac{x}{\ln x}$ wanneer x groot is ook niet vertalen als $\lim_{x \to +\infty} \left(\pi(x) - \frac{x}{\ln x} \right) = 0$? Ga dit na door enkele waarden van dat verschil te berekenen. Vul de onderstaande tabel aan (gebruik je resultaten uit vorige vragen). Hierbij krijg je nog gegeven dat $\pi(10^{10}) = 455\,052\,511$ en $\pi(10^{15}) = 29\,844\,570\,422\,669$.

x	$\pi(x) - \frac{x}{\ln x}$
10^3	
10^4	
10^5	
10^{10}	
10^{15}	

(Nee, we kunnen niet concluderen dat $\lim_{x \to +\infty} \left(\pi(x) - \frac{x}{\ln x} \right) = 0$ *. De in te vullen getallen zijn:* 87,54*;* 143,26*;* 906,11*;* 20 758 029,12*;* $8{,}92 \cdot 10^{11}$ *)*

8. We kunnen uit de stelling van Hadamard-de La Vallée-Poussin afleiden dat de breedtes van de gaten tussen de priemgetallen kleiner dan x *gemiddeld* ongeveer $\ln x$ zijn. Verklaar.

   (De breedtes van de gaten tussen de priemgetallen kleiner dan x is gemiddeld gelijk aan $\frac{x}{\pi(x)}$*. Volgens Hadamard-de La Vallée-Poussin is* $\pi(x) \approx \frac{x}{\ln x}$ *en dus is* $\frac{x}{\pi(x)} \approx \ln x$ *als* x *groot is. Dit bevestigt wat wij vaststelden bij vraag 6.)*

9. Het aantal priemgetallen kleiner dan of gelijk aan x is dus ongeveer gelijk aan $x / \ln x$ wanneer x groot is. Schat aan de hand van deze bewering het aantal priemgetallen kleiner dan 100000.

   ($\frac{100000}{\ln 100000} \approx 8686$*)*

10. Hoeveel procent wijkt deze schatting af van de werkelijke waarde $\pi(100000) = 9592$?

    (De werkelijke waarde is ongeveer 10% *hoger.)*

11. Welk percentage (ruw geschat) van de getallen kleiner dan 100000 is priem?

    ($\frac{9592}{100000} \approx \frac{1}{10}$*, ongeveer* 10% *dus.)*

12. Wat is dat percentage bij de getallen onder 10^{15} als je weet dat $\pi(10^{15}) = 29\,844\,570\,422\,669$?

    (Ongeveer 3%*. Dit illustreert wat Hadamard en de La Vallée-Poussin formuleerden als* $\lim_{x \to +\infty} \frac{\pi(x)}{x / \ln x} = 1$*. Het percentage priemgetallen kleiner dan n neemt af naarmate n groter wordt.)*

13. Hoe groot moet je, ruwweg en afgaande op de schatting, n nemen om er voor te zorgen dat gemiddeld nog maar 1 op elke 100 getallen onder n priem is? Bepaal het aantal cijfers van dat getal n.

    (Je wilt dat $\frac{n}{\ln n} \leq \frac{n}{100}$ *of nog dat* $\ln n \geq 100$*. Dat betekent dat, ruwweg,* $n \geq e^{100}$*, een getal met 44 cijfers. Dit aantal cijfers kun je als volgt vinden:* $\log e^{100} = 100 \log e \approx 43,43$ *en dus is* $e^{100} = 10^{\log(e^{100})} \approx 10^{43+0,43} = 10^{43} \cdot 10^{0,43} \approx 2,7 \cdot 10^{43}$*.)*

14. Uit de stelling van Hadamard en de La Vallée-Poussin kunnen we afleiden dat de kans dat een getal met hoogstens n cijfers priem is, ongeveer gelijk moet zijn aan $\frac{1}{n \ln 10}$. Verklaar!

    (Stel $x \approx 10^n$*. Dan is* $\pi(x) \approx \frac{10^n}{n \ln 10}$*. De gevraagde kans is dus* $\frac{\frac{10^n}{n \ln 10}}{10^n} = \frac{1}{n \ln 10}$*.)*

De priemgetallen liggen dus steeds dunner gezaaid: naarmate p toeneemt, wordt de gemiddelde breedte $\frac{p}{\pi(p)} \approx \ln p$ tussen priemgetallen ook groter. Nochtans kunnen die gaten uitzonderlijk zeer klein zijn. Men spreekt dan van priemmeerlingen.

c. Priemmeerlingen

Tussen al de priemwoestijnen zijn er af en toe priemgetallen die wél heel dicht bij mekaar liggen. Meer nog: men vermoedt zelfs dat er zo oneindig veel zijn (zie verder). Het gaat dus niet helemaal op om, zoals bij het gekende boek uit 2010 van Paolo Giordano, te spreken over de 'eenzaamheid van de priemgetallen'. Want eigenlijk valt het soms best wel mee met die 'eenzaamheid'… of toch niet?

Priemmeerlingen

Priemtweelingen zijn priemgetallen die maar 2 van elkaar verschillen. In 2011 zijn twee priemgetallen ontdekt van 200 700 cijfers die maar 2 van elkaar verschillen: $3\,756\,801\,695\,685 \times 2^{666669} \pm 1$. De grootst gekende tweelingpriemgetallen tot nu! Maar er is meer: er zijn ook priemvierlingen, priemneven en zelfs sexy priemgetallen! In deze werktekst maken we kennis met deze exoten.

1. Naast priemtweelingen spreekt men ook van priemneven $(p, p+4)$ en sexy priemgetallen $(p, p+6)$. Zoek enkele voorbeelden van deze exotische priemparen.
2. Er bestaan geen priemdrielingen $(p, p+2, p+4)$ of neef-priemdrietallen $(p, p+4, p+8)$, behalve (3,5,7) en (3,7,11). Probeer dit te verklaren.

   (Telkens is minstens een van de getallen deelbaar door drie.)
3. Bestaan er sexy priemdrietallen $(p, p+6, p+12)$ of sexy priemviertallen?

   (Ja, bv. (7,13,19), (47,53,59), (11,17,23,29), (61,67,73,79)*)*
4. Bestaan er sexy priemvijftallen?

   (Nee, want minstens een van deze getallen is deelbaar door vijf.)
6. Hier zie je alle eerste priemgetallen van een aantal sexy priemviertallen:

   5, 11, 41, 61, 251, 601, 641, 1091, 1481, 1601, 1741, 1861, 2371, 2671, 3301, 3911, 4001, 5101, 5381, 5431, 5641, 6311, 6361, 9461, 11821, 12101, 12641, 13451, 14621, 14741, 15791, 15901, 17471, 18211, 19471, 20341, 21481, 23321, 24091, 26171, 26681

   Wat is er speciaal aan de eerste priemgetallen van de sexy priemviertallen, op het getal 5 na? Verklaar.

   (Ze eindigen alle op het cijfer 1. *Alleen zo zal geen enkele van de getallen* $p, p+6, p+12$ *en* $p+18$ *deelbaar zijn door vijf en zal pas het vijfde getal in de rij eindigen op een vijf.)*

Het lijstje met exotische priemgetallen is nog langer (we zouden er een tweede loep mee kunnen vullen): congruente priemgetallen, palindroompriemgetallen (onderverdeeld in Titanic-, Gigantic- en Megapalindroompriemgetallen), repunit-priemgetallen, circulaire priemgetallen, …; er bestaan zelfs illegale priemgetallen (zie [18]).

4. Enkele open problemen met priemgetallen

Leerlingen denken heel vaak dat de wiskunde ‘af’ is. Alles ligt vast en is bewezen. En natuurlijk zijn er heel wat bewezen stellingen en gevestigde theorieën, maar de theorie van de priemgetallen geeft niet het gevoel afgerond te zijn en wordt ook nu nog verder uitgebreid of bijgesteld. Heel wat vragen zijn nog niet opgelost en al werkend stellen wiskundigen steeds nieuwe vragen. Vaak raken dergelijke vragen snel opgelost, maar soms blijken ze moeilijk op te lossen. In die context worden geregeld vermoedens geformuleerd. De wiskundige vermoedt een bepaalde eigenschap en zoekt voorbeelden en tegenvoorbeelden. Op een bepaald ogenblik komt er een kantelmoment … blijft hij zoeken naar een tegenvoorbeeld of wordt het vermoeden sterker en sterker en neigt hij naar het zoeken van een bewijs? Dat is een vraag die ook in de klas erg interessant kan zijn en waarbij je als leerkracht advocaat van de duivel kunt spelen. Vanaf wanneer beslissen we om op zoek te gaan naar een bewijs als we een stelling vermoeden? Discussie verzekerd! De wiskundige formuleert heel precies wat reeds bewezen is en wat weliswaar nog onbewezen is, maar toch een vermoeden is. De geformuleerde vermoedens blijken een enorme stimulans te zijn voor verder onderzoek. Vaak moet voor het oplossen van dergelijke problemen veel nieuwe theorie ontwikkeld worden.

Het aantal vermoedens in de hedendaagse wiskunde is enorm (zie [20]). Heel wat problemen vragen nog steeds om een oplossing. Hieronder bespreken wij kort twee van de meest bekende vermoedens uit de getaltheorie. Inzet van ICT is in deze tak van de wiskunde tegenwoordig erg belangrijk. Niet alleen bij het zoeken van voorbeelden en tegenvoorbeelden (zoals bijvoorbeeld de zoektocht naar grote priemtweelingen), maar ook bij het bewijzen van sommige van die vermoedens. En dat brengt ons bij een andere interessante discussie: wat is de geldigheid van een bewijs dat op computerkracht steunt? Ook wiskundigen zijn het hierover niet helemaal eens (zie [11]). Sommigen beschouwen zo’n bewijs meer als een experimenteel resultaat dan als een echt wiskundig bewijs. Voorbeelden van problemen die met behulp van computerkracht bewezen werden zijn het vierkleurenprobleem (over de inkleuring van landkaarten) en het vermoeden van Kepler (over de stapeling van bollen).

a. Het vermoeden van Goldbach

Het is vaak zo dat problemen in de rekenkunde eenvoudig kunnen worden geformuleerd. Maar hoe eenvoudig ze daardoor ook lijken, ze zijn vaak heel moeilijk te bewijzen. Het vermoeden van Goldbach is hiervan een mooi voorbeeld. We bestuderen het in de volgende werktekst.

Het vermoeden van Goldbach

De Duits-Pruisische wiskundige Christian Goldbach (1690-1764) legde zich vooral toe op de getaltheorie. Hij correspondeerde hierover met de veel beroemdere wiskundige Leonhard Euler (1707-1783). In de marge van een van zijn brieven aan Euler, schreef Goldbach: ‘Het lijkt erop dat elk getal groter dan twee kan geschreven worden als de som van drie priemgetallen’. Goldbach beschouwde 1 nog als een priemgetal, wat wij ondertussen niet meer doen. Euler verwoordde de bewering in een iets vereenvoudigde vorm, die later bekend zou worden als het vermoeden van Goldbach:

elk even getal groter dan twee is de som van twee priemgetallen.

1. Controleer het vermoeden van Goldbach voor de eerste 10 even getallen groter dan 2.
   *(*4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 5 + 5, 12 = 5 + 7, 14 = 7 + 7, 16 = 5 + 11, 18 = 7 + 11, 20 = 7 + 13, 22 = 5 + 17*)*
2. Is 98 te schrijven als som van twee priemgetallen? En 220? En 346?
   (Ja, 98 = 19 + 79, 220 = 7 + 113, 346 = 29 + 317.*)*
3. Is er telkens slechts één schrijfwijze als som van twee priemgetallen mogelijk?
   (Nee, bijvoorbeeld: 22 = 5 + 17 = 3 + 19. *Voor de meeste getallen geldt zelfs: hoe groter het getal hoe groter het aantal paren priemgetallen. Zo kan* 10000 *al op* 127 *manieren geschreven worden als de som van twee priemgetallen!)*
4. Stel dat je denkt dat het vermoeden van Goldbach fout is. Hoe zou je dit kunnen bewijzen?
   (Door een tegenvoorbeeld te zoeken. Je zult niet alleen een getal moeten geven, maar ook bewijzen dat het niet te schrijven als de som van twee priemgetallen.)

Euler antwoordde aan Goldbach dat hij de bewering als waar beschouwde, maar dat hij ze niet kon bewijzen. Meer dan 250 jaar na de brief van Goldbach, blijft deze vraag nog steeds onopgelost en hebben al heel wat wiskundigen er hun tanden op stukgebeten. Het vermoeden van Goldbach is een probleem dat verbazingwekkend eenvoudig kan worden geformuleerd, maar niemand heeft ooit een bewijs of tegenvoorbeeld gevonden. Juist omdat het probleem zo eenvoudig schijnt, oefent het een grote aantrekkingskracht uit op iedereen die graag bezig is met getaltheorie. Zo schreef Apostolos Doxiados in 2000 een boek, getiteld *Oom Petros en het vermoeden van Goldbach*, over een man die zijn hele leven tevergeefs zocht naar een bewijs voor het vermoeden. Om publiciteit te maken voor het boek, beloofde de uitgever een beloning van een miljoen dollar aan wie het vermoeden voor april 2002 kon bewijzen. De prijs werd nooit opgeëist.

Dat het vermoeden van Goldbach nog niet bewezen werd, betekent niet dat er geen belangrijke stappen in de goede richting zijn gezet. Het beste resultaat staat op naam van de Franse wiskundige Olivier Ramaré. Hij bewees in 1995 dat elk even getal geschreven kan worden als een som van maximum zes priemgetallen. Maar een echt bewijs voor het vermoeden van Goldbach is voorlopig nog niet in zicht.

b. Priemtweelingen

Vermoeden: het aantal priemtweelingen is oneindig.

Er zijn overweldigende numerieke aanwijzingen voor dit vermoeden en er zijn veel deelresultaten, maar men slaagt er vooralsnog niet in om het te bewijzen. Met kansrekening kan men voorspellen hoeveel priemtweelingen er (ongeveer) beneden een gegeven grens of binnen een bepaald interval zouden moeten liggen (zie [10]). En die voorspellingen kloppen wonderwel met numerieke resultaten (noeste vlijt en rekenwerk)! Dit geeft vertrouwen dat men in de goede richting zoekt, maar een algemene theorie waaruit dit vermoeden zou kunnen worden bewezen, kent men nog niet.

5. Priemgetaltesten

a. Priemgetallen: pure schoonheid met een praktische toepassing

Heel wat van de eigenschappen en eigenaardigheden van priemgetallen zijn onderzocht omwille van de schoonheid ervan en zonder een bepaalde toepassing voor ogen. De wiskundige G.F. Hardy, die zich met theoretische getaltheorie heeft bezig gehouden, formuleerde het als volgt in zijn boek “A mathematician’s apology” (zie [7]):

> *“I have never done anything ‘useful’. No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world.”*

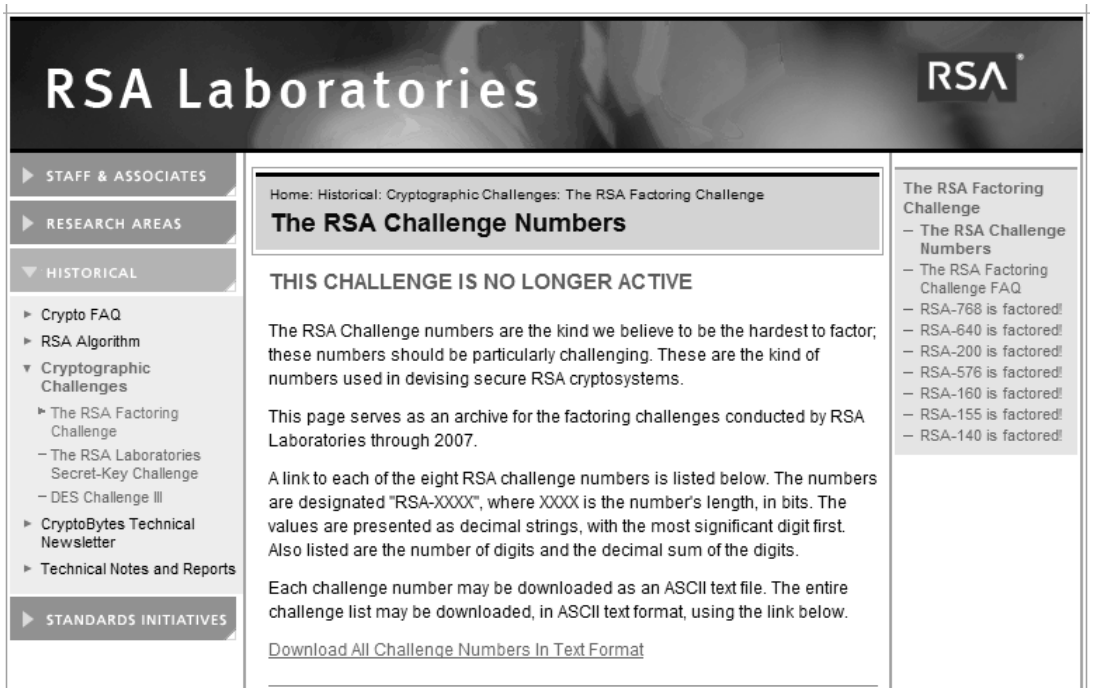
Het lijkt wel de ironie van het lot te zijn dat priemgetallen en bij uitbreiding de hele getaltheorie een halve eeuw later de basis vormden van een nieuwe toepassing die niet meer weg te denken is uit de moderne maatschappij. Priemgetallen spelen een essentiële rol in de cryptografie en meer bepaald bij RSA-codering. Zonder deze beveiligingsmethoden zouden we geen (betrouwbare) elektronische betalingen kunnen doen in winkels of via internet, zouden onze e-mails door de hele wereld te lezen zijn of zou het invullen van een belastingsbrief nog altijd met pen en papier moeten gebeuren omdat er geen veilige elektronische handtekening bestaat. Toen in de jaren ’70 van de vorige eeuw de behoefte aan beveiliging groeide, hadden wiskundigen de theorie al eeuwen tevoren uitgewerkt. Die wiskundigen waren vaak alleen gedreven door de schoonheid van de theorie.

In 1977 ontwikkelden Ron Rivest, Adi Shamir en Leonard Adleman een coderingssysteem met een publieke en geheime sleutel. Het werd RSA genoemd naar de beginletters van hun familienamen. Het feit dat er geen geheime sleutels moeten worden uitgewisseld, verhoogt in belangrijke mate de veiligheid van het systeem. RSA-codering steunt op het berekenen van een macht modulo n van het bericht (omgezet in een getal B). De exponent wordt de coderingsexponent e genoemd. Het getal n is het product van twee grote priemgetallen (elk met enkele honderden cijfers). Om te coderen moet je dus $B^e \pmod{n}$ berekenen. Het tweetal (n, e) is de publieke sleutel van het systeem en is dus door iedereen gekend. Iedereen kan dus een boodschap versleutelen. Om het gecodeerde bericht te decoderen moet je een gelijkaardige bewerking doen als bij het coderen, maar met een andere exponent. Deze decoderingsexponent d vormt de geheime sleutel. Alleen wie deze sleutel kent, kan het bericht ontcijferen.

Wie meer wil weten over de werking van RSA en hoe dit kan aangebracht worden in de klas vindt hierover materiaal in een vroeger nummer van Uitwiskeling, namelijk in de loep van UW4/4 (volledig te vinden op onze website). Ook op het internet zijn heel wat bruikbare documenten te vinden. Voor het vervolg van deze tekst heb je die kennis niet nodig.

Om een bericht te kraken dat met RSA versleuteld is, moet je de decoderingsexponent *d* vinden. Dit kan in principe uit de getallen *n* en *e* van de publieke sleutel. Een belangrijke stap hierbij is de ontbinding in priemfactoren van het getal *n* dat meer dan tweehonderd cijfers telt. Hoe eenvoudig dit ook moge lijken, dit blijkt zo'n zware opdracht te zijn dat het in de praktijk, zelfs voor krachtige computers, onmogelijk is.

De vooruitgang op het terrein van de priemontbindingen van grote getallen komt van twee kanten. Enerzijds worden computers krachtiger en vraagt het minder tijd om dezelfde bewerkingen te doen. Anderzijds zijn wiskundigen voortdurend op zoek naar betere algoritmen voor deze ontbindingen. Om het onderzoek rond dit thema te stimuleren daagde de RSA Laboratories, een onderzoekscentrum rond RSA, de hele wereld uit om een aantal grote getallen te ontbinden (zie [19]). Er waren met deze 'uitdagingen' grote bedragen (tot $200 000) te winnen. RSA Laboratories had dat geld er voor over omdat ze op die manier de ontwikkelingen konden volgen en inschatten.



Zoals je in de schermafdruk kunt lezen, is de 'challenge' ondertussen afgesloten. Dit gebeurde in 2007. De nieuwe technieken (betere computers en betere algoritmen) maakten dat de ontbindingen elkaar relatief snel begonnen op te volgen en het werd een te kostelijke zaak voor RSA Laboratories om de prijzen te blijven uitbetalen. De getallen die nog niet ontbonden waren, bleven wel op de site staan. In december 2009 is de ontbinding van het getal RSA-768 gevonden. Er blijven nog 5 van die grote getallen over. Je vindt ze terug op [19].

RSA-768 is een getal dat binair geschreven uit 768 cijfers bestaat. Decimaal geschreven zijn dit 232 cijfers. Om deze ontbinding te vinden hebben onderzoekers ongeveer 2000 computers (van professionelen en van hobbyisten) gedurende drie kalenderjaren laten samenwerken (zie [13]). Het resultaat lees je hieronder:

123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

=

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489

x

367460436667995904282446337996279526322791581643430876426760322838157396665112792333734171433968102700927987363089 17.

Er wordt tegenwoordig gewerkt met 1024-bitssleutels (getallen met 309 decimalen). Hoewel er een grote vooruitgang gemaakt is op het vlak van het ontbinden van grote getallen, beweren de onderzoekers dat als de vorderingen aan dit tempo verder gaan, we toch nog een 10-tal jaar gerust kunnen zijn in de veiligheid van de RSA-codering.

De zoektocht naar grote priemgetallen is nodig voor de veiligheid van RSA-codering. Daarvoor gaat men kandidaat-priemgetallen onderwerpen aan bepaalde tests. Een priemtest onderzoekt of een getal priem of niet priem is. In wat volgt in deze paragraaf bekijken we enkele van die priemtests.

b. Een eerste priemtest

Voor het gebruik van RSA hebben we (grote) priemgetallen nodig. Een manier om aan een lijst priemgetallen te komen, is alle getallen kleiner dan een bepaald getal te ‘zeven’. We doen dit in de onderstaande werktekst.

De zeef van Eratosthenes

We werken nu een werkwijze uit waarmee je alle priemgetallen van 1 tot een bepaald getal kunt vinden. In het voorbeeld zoeken we naar de priemgetallen kleiner dan 150.

In het rooster hieronder hebben we al deze getallen opgeschreven.

~~1~~	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

De uiteindelijke bedoeling is om alle getallen die geen priemgetallen zijn te schrappen uit de lijst. Het getal 1 is al geschrapt omdat het geen priemgetal is. Volg nu de onderstaande instructies.

- Het eerste niet geschrapte getal is 2. Schrap in de tabel alle veelvouden van 2, behalve 2 zelf.
- Het eerstvolgende niet geschrapte getal is 3. Schrap nu alle veelvouden van 3, behalve het getal 3 zelf.
- Ga verder door telkens de veelvouden van het volgende niet geschrapte getal te schrappen. Het getal zelf laat je staan.
- De overblijvende getallen zijn de priemgetallen.

De onderstaande vraagjes gaan wat dieper in op de werking van de zeef.

1. Waarom is telkens het eerstvolgende nog niet geschrapte getal een priemgetal?
   (Indien het geen priemgetal was, dan was het een veelvoud van een van voorgaande getallen en dan zou het al geschrapt zijn.)
2. Welk veelvoud van 7 was het eerste dat je moest schrappen? Waarom?
   *(*49*. De kleinere veelvouden waren al geschrapt als veelvouden van een kleiner priemgetal.)*
3. Welk getal was het laatste waarvan je veelvouden moest schrappen? Waarom?
   (Aangezien het eerstvolgende veelvoud dat moet geschrapt worden het kwadraat is, kunnen we stoppen van zodra $n^2 > 150$ *of* $n > \sqrt{150} \approx 12,2$*. Na* 11 *kunnen we het procedé dus stoppen.)*
4. Leg uit waarom alle overgebleven getallen in de lijst priemgetallen zijn.
   (Neem bijvoorbeeld het getal 89*. Indien dit geen priemgetal zou zijn, dan zijn er twee getallen a en b, beide strikt groter dan* 1*, waarvoor* $ab = 89$*. Veronderstel dat* $a \leq b$*. Dan volgt hieruit dat* $a^2 \leq ab = 89 < 150$*. Er geldt dus dat* $a \leq \sqrt{150}$*. Aangezien we alle veelvouden van getallen kleiner dan* $\sqrt{150}$ *geschrapt hebben, kan a geen factor van* 89 *zijn. Bijgevolg is* 89 *priem. De redenering kan voor elk getal uit de lijst over gedaan worden.)*

Aan de hand van je lijst van priemgetallen kun je van grotere getallen onderzoeken of ze priem zijn door na te gaan of het nieuwe getal deelbaar is door één van de getallen uit de lijst.

5. Onderzoek op deze manier of 373 priem is. Ga eerst na wat de bovengrens voor de echte priemdelers is.
   (We zoeken een kwadraat in de buurt van 373*, bijvoorbeeld* 400*. We moeten dus alleen maar de priemgetallen kleiner dan* 20 *uitproberen. Deze berekeningen zijn zelfs zonder rekentoestel goed te doen. Uit de verschillende delingen blijkt dat* 373 *priem is.)*
6. Wat is het grootste getal dat je op deze manier en met de lijst die we hier hebben opgesteld kunt onderzoeken op zijn priem zijn?
   (Je kunt getallen onderzoeken tot $150^2 = 22500$*.)*

De zeef van Eratosthenes kan mooi geïllustreerd worden met applets die op internet te vinden zijn (zie bijvoorbeeld [6]).

c. De priemtest van Fermat

De methode om priemgetallen te vinden en andere getallen te testen op hun priem zijn uit de vorige werktekst werkt prima voor kleine getallen, maar is bijzonder arbeidsintensief en dus niet geschikt

voor grote getallen. Computers kunnen wel heel wat rekenwerk overnemen, maar ook dan vraagt deze methode zeer veel computertijd. We moeten bijgevolg op zoek naar andere methoden. We zullen ons hiervoor baseren op eigenschappen uit de getaltheorie.

De kleine stelling van Fermat, die trouwens ook aan de basis ligt van RSA-codering, geeft ons een eerste manier om getallen te testen op hun priem zijn. De stelling luidt als volgt.

> Stel dat a en p natuurlijke getallen zijn, waarbij $a \geq 2$, $p \geq 2$ en $\text{ggd}(a, p) = 1$. Dan geldt:
>
> als p een priemgetal is, dan is $a^{p-1} \equiv 1 (\text{mod } p)$.

Het bewijs vraagt wat ervaring met modulo-rekenen. Wie erin geïnteresseerd is, kan dit vinden in bijvoorbeeld [3]. Om met deze stelling het priem zijn te kunnen onderzoeken moeten we er eerst de contrapositie op toepassen. Dit geeft:

> als $a^{p-1} \not\equiv 1 (\text{mod } p)$, dan is p niet priem.

We illustreren dit voor $p = 143$ en $a = 2$. We berekenen $2^{142} (\text{mod} 143)$ (bv. met WolframAlpha, want het getal 2^{142} is te groot voor de TI84). Dit geeft 114 als resultaat. Aangezien $114 \not\equiv 1 (\text{mod} 143)$, kunnen we besluiten dat 143 *geen* priemgetal is. Voor een klein getal als 143 is het uiteraard niet nodig om deze werkwijze te gebruiken. We konden het immers gewoon opzoeken in onze lijst uit de vorige werktekst. Maar voor grote getallen (met meer dan honderd cijfers) is dit niet zo.

We onderwerpen nu 137 aan dezelfde test. We vinden dat $2^{136} \equiv 1 (\text{mod} 137)$. Hieruit kunnen we echter niet besluiten dat 137 priem is. Toevallig is dat nu wel het geval (dat is eenvoudig te controleren), maar je kunt het niet besluiten uit de berekening. De stelling geeft immers alleen een nodige voorwaarde voor priemgetallen, maar geen voldoende voorwaarde. Er bestaan getallen die wel voldoen aan de stelling van Fermat, maar toch samengesteld zijn. Een voorbeeld van zo een getal is 341. Met WolframAlpha vinden we $2^{340} \equiv 1 (\text{mod} 341)$. Nochtans is 341 niet priem. Met de zeefmethode vinden we immers dat 341 deelbaar is door 11. Omdat 341 zich als een priemgetal gedraagt bij $a = 2$, zeggen we dat 341 *pseudopriem* is voor het grondtal 2. We zeggen ook dat 2 een *leugenaar* is voor het priem zijn van 341.

We nemen nu een andere waarde voor a, bv. $a = 3$ en we onderwerpen 341 opnieuw aan de test. We vinden dat $3^{340} \equiv 56 (\text{mod} 341)$. Deze keer valt het getal 341 door de mand en is er aangetoond dat 341 *geen* priemgetal is. We zeggen dat 3 een *getuige* is voor het niet priem zijn van 341.

Hiermee hebben we een test die de *priemtest van Fermat* genoemd wordt. Deze test is bruikbaar op voorwaarde dat we een methode hebben om machten modulo p uit te rekenen. Dit onderzoeken we in de volgende werktekst. Het programmaatje aan het einde van de werktekst kan gedownload worden via onze website.

Machten modulo *p*

Voor de berekening van $2^{142} (\text{mod} 143)$ hebben we WolframAlpha ingeschakeld. Het getal 2^{142} is immers te groot voor ons rekentoestel.

1. Waar zit het probleem precies?

   ($2^{142} \approx 5{,}575 \cdot 10^{42}$. *Overflow is dus niet het probleem. Omdat de rekenmachine TI84 met slechts* 14 *beduidende cijfers werkt, worden niet alle decimalen van dit getal berekend en*

opgeslagen. Voor de berekening van de rest bij de euclidische deling, moet het getal tot zijn laatste decimaal gekend zijn.)

Door het slimmer aan te pakken, zullen we in staat zijn om het resultaat toch te vinden met onze rekenmachine. We zullen de exponent schrijven als een som van kleinere getallen. Het getal wordt dan een product van kleinere getallen en die kleinere getallen zullen we eerst reduceren modulo 143 vóór we de vermenigvuldiging uitvoeren.

2. Schrijf 2^{142} als een product van factoren die je wel kunt reduceren met je rekentoestel. Bereken dan langs deze weg $2^{142} \pmod{143}$.

   (Een mogelijkheid is $2^{142} = 2^{30} \cdot 2^{30} \cdot 2^{30} \cdot 2^{30} \cdot 2^{22}$. *Verder is* $2^{30} \equiv 12 \pmod{143}$, $2^{22} \equiv 114 \pmod{143}$ *en* $2^{30} \cdot 2^{30} \equiv 12^2 \equiv 1 \pmod{143}$. *Tot slot vinden we dat* $2^{30} \cdot 2^{30} \cdot 2^{30} \cdot 2^{30} \cdot 2^{22} \equiv 1^2 \cdot 114 \equiv 114 \pmod{143}$.*)*

3. Op welke eigenschap van het modulorekenen steunen we hier?

   (De restklasse van een product is het product van de restklassen, of in formulevorm: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.*)*

Het is precies dit principe van stuksgewijs reduceren dat we zullen toepassen om dergelijke machten modulo *p* te berekenen. We zullen het wel wat systematischer moeten aanpakken.

We beginnen met het kwadrateren van een getal. Dit kwadraat kun je vervolgens nog eens kwadrateren.

4. Welke macht berekende je dan? En als je nog eens kwadrateert?

   (De 4*de macht. De* 8*ste macht.)*

Dit kunnen we verder zetten. De exponent kunnen we vervolgens schrijven als een som van machten van 2.

5. Doe dit voor de exponent 142 uit het voorbeeld.

   ($142 = 128 + 8 + 4 + 2$ *)*

6. Bereken nu $2^a \pmod{143}$ met *a* gelijk aan de machten van 2. Noteer de resultaten in de onderstaande tabel.

2^a	$2^a \pmod{143}$
2^1	2
2^2	4
2^4	
2^8	
2^{16}	
2^{32}	
2^{64}	
2^{128}	

   (De tabel wordt verder aangevuld met de getallen 16, 113, 42, 48, 16, 113*. Merk op dat je de tussenliggende machten nodig hebt als tussenstap bij de berekeningen.)*

7. Gebruik de splitsing van 143 (zie vraag 5) en je berekeningen uit de tabel hierboven om $2^{142} \pmod{143}$ te schrijven als een product van factoren en reken uit.

($2^{142} = 2^{128} \cdot 2^8 \cdot 2^4 \cdot 2^2 \equiv 113 \cdot 113 \cdot 16 \cdot 4 \equiv 114 (\mathrm{mod} 143)$ *)*

Deze werkwijze noemt men het machtsverheffen door herhaald kwadrateren.

Om te weten welke machten van 2 je moet meenemen in je berekening moet je de exponent schrijven als een som van machten van 2. Dit komt er in feite op neer dat je de exponent in het binair talstelsel schrijft. Zo is de binaire schrijfwijze van 143 gelijk aan 10001110.

Het onderstaande programma POWERMOD voor de TI83/4 berekent machten van een getal *a* modulo *m* volgens het principe dat we hierboven hebben uitgelegd.

8. Probeer de verschillende stappen te begrijpen. Kun je de stappen terugvinden waarin de exponent binair geschreven wordt? Vind je ook terug in welke stappen de tabel uit opdracht 6 berekend wordt? Hoe wordt de vermenigvuldiging aangepakt?

```
PROGRAM:POWERMOD
:Input "GRONDTAL
 =",A
:Input "EXPONENT
 =",E
:Input "MODULO =
",M
:ClrAllLists
:0→N
:While E>0
:N+1→N
:E-2*int(E/2)→R
:(E-R)/2→E
:R→L1(N)
:End
:A-M*int(A/M)→A
:A→L2(1)
:For(K,2,N)
:A²-M*int(A²/M)→
A
:A→L2(K)
:End
:If A=0
:Then
:0→T
:Else
:1→T
:For(K,1,N)
:T*L2(K)^L1(K)→T
:T-M*int(T/M)→T
:End
:End
:Disp T
:
```

```
prgmPOWERMOD
GRONDTAL =2
EXPONENT =142
MODULO =143
                  114
                Done
```

9. Hoe groot mogen de getallen maximaal zijn om geen problemen te hebben met verlies van cijfers?

   (Omdat je alle beduidende cijfers van a^2 *moet kunnen berekenen, mag a niet groter zijn dan* 10^7*. De TI84 onthoudt immers maar* 14 *cijfers. Verder moet je ook producten van residuen kunnen berekenen. Dat betekent dat die ook niet groter dan* 10^7 *mogen zijn. Daarom moet ook het getal m kleiner dan* 10^7 *zijn. Je zou het programmaatje kunnen verbeteren door een test in te voeren die een foutmelding geeft indien de getallen te groot zijn.)*

10. Gebruik nu het programma POWERMOD om na te gaan of 8 848 603 priem is of niet.

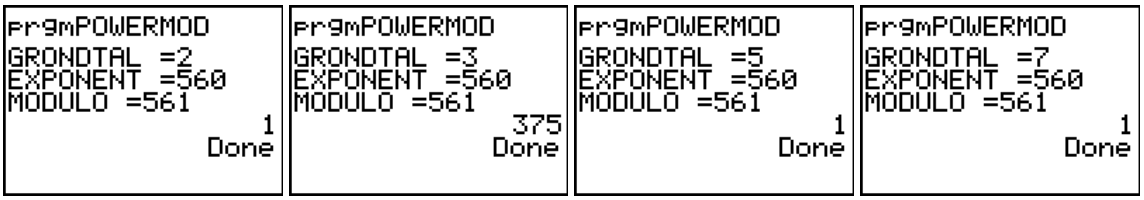
    (Je vindt dat $2^{8848602} \equiv 8251519 (\mathrm{mod} 8848603)$*. Het getal* 8 848 603 *is dus niet priem.)*

Carmichaelgetallen

De priemtest van Fermat werkt prima als we een getal *a* vinden waarvoor $a^{p-1} \not\equiv 1 (\text{mod } p)$. In dat geval kunnen we met zekerheid zeggen dat *p* niet priem is.

Indien we vinden dat $a^{p-1} \equiv 1 (\text{mod } p)$, dan kunnen we geen conclusie trekken. Indien we de test verschillende keren na elkaar uitvoeren met telkens een andere waarde voor *a*, vergroten we de kans dat het getal *p* inderdaad een priemgetal is indien we steeds vinden dat $a^{p-1} \equiv 1 (\text{mod } p)$. Voor de praktische uitvoering van de test mogen we ons beperken tot getallen *a* die priem zijn.

Helaas zijn er getallen *p* die alle tests met grondtallen *a* met $\text{ggd}(a, p) = 1$ doorstaan. Deze getallen noemt men de *Carmichaelgetallen* naar Robert Carmichael die deze getallen in 1910 ontdekte. Het kleinste Carmichaelgetal is het getal 561. Dit getal houdt hardnekkig de schijn op van priem te zijn, maar is het niet. Hieronder zie je enkele tests.



Het lijkt erop dat het tweede schermpje niet in overeenstemming is met wat we hierboven beweerden, maar dat is niet zo. Het getal 3 is immers een deler van 561 en bijgevolg is $\text{ggd}(361,3) = 3 \neq 1$ en gaat de stelling van Fermat niet meer op. Op deze manier hebben we 561 natuurlijk ook ontmaskerd!

Carmichaelgetallen zijn zeldzaam. Er bestaan slechts 2163 Carmichaelgetallen kleiner dan $25 \cdot 10^9$. Ondanks het feit dat ze zeldzaam zijn, heeft Alford in 1994 toch kunnen aantonen dat er oneindig veel van die getallen zijn (zie [2]).

Juist omdat de Carmichaelgetallen zo zeldzaam zijn, worden de meeste samengestelde getallen wel ontdekt door de test met enkele grondtallen *a* te herhalen. Maar honderd procent zekerheid heb je niet als een getal voor verschillende tests slaagt. De mogelijkheid bestaat nog steeds dat het een samengesteld getal is. Om die reden noemt men de priemtest van Fermat een probabilistische test.

d. Een verfijning van de priemtest van Fermat

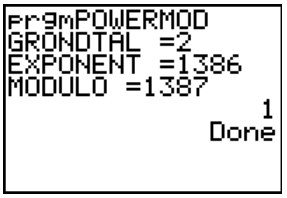
De kleine stelling van Fermat is niet de enige eigenschap van priemgetallen die we kunnen gebruiken als een priemtest. Een voorbeeld van een andere eigenschap is de volgende.

> Als *p* een priemgetal is met $p > 2$ en $a^2 \equiv 1 (\text{mod } p)$, dan is $a \equiv 1 (\text{mod } p)$ of $a \equiv -1 (\text{mod } p)$.

Deze stelling is eenvoudig te bewijzen. Als $a^2 \equiv 1 (\text{mod } p)$, dan is *p* een deler van $a^2 - 1 = (a-1)(a+1)$. Omdat *p* priem is, moet *p* een deler zijn van één van beide factoren. Dan is $a \equiv 1 (\text{mod } p)$ of $a \equiv -1 (\text{mod } p)$.

Hier verschijnt op natuurlijke wijze een negatief getal in de congruentiegelijkheid. Dit is op zich geen enkel probleem. Het programma voor de TI84 dat we opstelden, geeft uitsluitend positieve getallen als uitkomst. Bedenk dat $-1 \equiv p - 1 (\text{mod } p)$.

Op de bovenstaande eigenschap kunnen we weer contrapositie toepassen. Als we een getal a vinden waarvoor $a^2 \equiv 1 (\text{mod } p)$ en $a \not\equiv \pm 1 (\text{mod } p)$, dan weten we dat p onmogelijk een priemgetal kan zijn. Indien we een getal a hebben waarvoor $a^2 \equiv 1 (\text{mod } p)$ en $a \equiv \pm 1 (\text{mod } p)$, kunnen we niets met zekerheid besluiten: p kan priem zijn, maar ook niet.

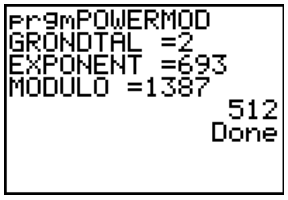


Deze bijkomende eigenschap kunnen we combineren met de priemtest van Fermat. Als voorbeeld onderzoeken we of het getal 1387 priem is. De priemtest van Fermat geeft $2^{1386} \equiv 1 (\text{mod} 1387)$.

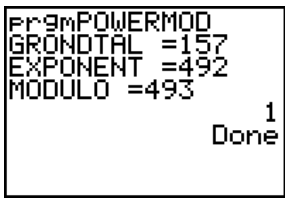
Hieruit kunnen we nog niets besluiten. Maar omdat p = 1387 als kandidaat priemgetal oneven is, is de exponent $p - 1 = 1386$ even. Het getal 2^{1386} kunnen we dan bekijken als een kwadraat. Dit geeft

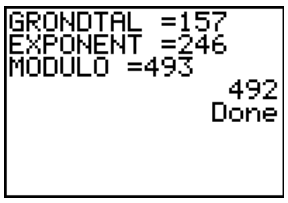
$$2^{1386} = \left(2^{693}\right)^2 \equiv 1 (\text{mod} 1387).$$

We testen dan of het getal 2^{693} congruent is met 1 of –1 modulo 1387. We vinden dat $2^{693} \equiv 512 (\text{mod} 1387)$. Er is dus buiten 1 en –1 nog een ander getal waarvan het kwadraat congruent is met 1 modulo 1387. Bijgevolg kan 1387 geen priemgetal zijn. De ontbinding in priemfactoren geeft inderdaad $1387 = 19 \cdot 73$.



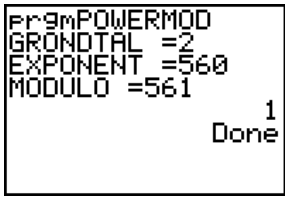
De combinatie van deze twee testen doet een aantal pseudopriemgetallen door de mand vallen, maar opnieuw zullen we ze niet allemaal vinden. We testen nu 493 op deze manier op priem zijn en gebruiken het grondtal 157. Deze bizarre keuze voor het grondtal is ingegeven door het feit dat we een bepaald effect willen illustreren. We vinden $157^{492} \equiv 1 (\text{mod } 493)$. De test van Fermat geeft dus geen uitsluitsel. We testen vervolgens het getal 157^{246}.

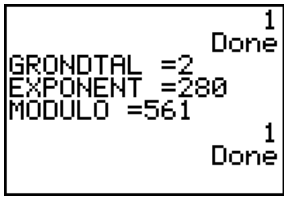


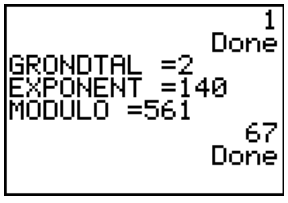


We vinden dat $157^{246} \equiv 492 \equiv -1 (\text{mod } 493)$. Dit geeft nog altijd geen uitsluitsel over het al dan niet priem zijn van 493. Het getal 493 zal met het grondtal 157 niet ontmaskerd worden als een samengesteld getal. Nochtans is $493 = 17 \cdot 29$. We noemen 157 een hardnekkige leugenaar voor de primaliteit van 493.

We proberen nog een laatste voorbeeld. We onderzoeken 561, het kleinste Carmichaelgetal, voor het grondtal 2.







In de derde stap laat 561 zijn ware aard zien! Zolang we 1 als resultaat uitkomen en de exponent even is, kunnen we de test verder zetten. Het proces stopt als ofwel het residu verschilt van 1 ofwel de exponent niet meer even is. Indien het residu ook nog verschilt van –1, dan weten we dat het getal niet priem is. In de andere gevallen geeft de test geen uitsluitsel.

e. De Lucas-Lehmertest voor Mersennepriemgetallen

Grote priemgetallen zijn niet alleen nuttig bij de beveiliging van informatie, al sinds Euclides zijn wiskundigen gefascineerd door grote priemgetallen. De zoektocht naar (grote) priemgetallen lijkt evident maar is dat absoluut niet. Geregeld verschijnt er in de media een bericht dat er een nieuw grootste priemgetal gevonden is.

In 1588 was het grootste gekende priemgetal $2^{19}-1=524\,287$. Dit is een getal van zes cijfers (in een tijd dat er nog geen ICT was!) dat ontdekt was door Pietro Cataldi, een Italiaans wiskundige. Gedurende 184 jaar kon Cataldi het record voor het grootste bekende priemgetal op zijn naam schrijven. In 1772 ontdekte Leonhard Euler het achtste Mersennepriemgetal, $2^{31}-1=2\,147\,483\,647$. In 1857 begon de Franse wiskundige Edouard Lucas (die we ook kennen van de toren van Hanoi) te testen of het getal $2^{127}-1$ (een getal met maar liefst 39 cijfers) priem is. Pas 19 jaar later, in 1876, kon hij zijn vermoeden bevestigen en bleek het inderdaad een priemgetal te zijn. Gedurende 75 jaar bleef dit getal het grootste bekende priemgetal. In de jaren vijftig van de twintigste eeuw namen computers het rekenwerk over en is het snel gegaan. Op dit moment is het grootste bekende priemgetal $2^{43112609}-1$, een getal dat bestaat uit bijna 13 miljoen cijfers! Op [9] kun je recent ontdekte priemgetallen vinden. Naast lijsten met grootste priemgetallen, grootste priemtweelingen, grootste Mersennepriemgetallen… vind je er ook veel algemene informatie over priemgetallen. De data op deze website worden dagelijks bijgewerkt en aangepast indien nodig.

Het is geen toeval dat de hierboven opgesomde 'grootste' priemgetallen alle van dezelfde vorm 2^p-1 zijn met *p* priem. Priemgetallen van deze vorm noemt men *Mersennepriemgetallen*. Deze priemgetallen worden relatief gemakkelijk gevonden omdat er een specifiek criterium voor bestaat: het criterium van Lucas-Lehmer. Dit is een vrij eenvoudig recept om na te gaan of een Mersennegetal $M_p=2^p-1$ al dan niet priem is.

Lucas-Lehmertest

Hieronder vind je het criterium dat Lucas en Lehmer hebben bewezen om een Mersennegetal M_p te testen op zijn priem zijn.

Construeer de volgende rij getallen S_1, S_2, …, S_{p-1}:

neem $S_1=4$ en stel S_k gelijk aan de rest van de deling van S_{k-1}^2-2 door M_p. Dan is M_p priem als en slechts als $S_{p-1}=0$.

1. Ga met het Lucas-Lehmer criterium na of 2^7-1 priem is. Gebruik SoftMaths ter controle.
   (Je kunt narekenen dat $S_2=14$, $S_3=67$, $S_4=42$, $S_5=111$ *en* $S_6=0$. 2^7-1 *is bijgevolg priem.)*
2. Ga op dezelfde manier na of 2047 priem is.
   ($2047=2^{11}-1$. *Reken na dat* $S_{10}=1736$*, waaruit volgt dat* 2047 *niet priem is.)*

In tegenstelling tot de test van Fermat en de verfijning ervan, geeft deze test 100% zekerheid. Het is bijgevolg een deterministische test.

Sinds januari 1996 maakt iedereen met een PC kans om het volgende Mersennepriemgetal vinden door mee te doen aan de GIMPS (Great Internet Mersenne Prime Search). Hierbij worden de berekeningen niet uitgevoerd door één centrale supercomputer, maar gebruikt men de rekenkracht van duizenden computers van liefhebbers over heel de wereld. Om deel te nemen moet je een programma downloaden van de site van GIMPS (zie [17]). Dat programma laat jouw computer mee zoeken naar een nieuw Mersennepriemgetal. Als je heel veel geluk hebt en jouw computer een nieuw priemgetal vindt, wordt de server verwittigd en krijg je zelf ook een geluid te horen. Het op dit moment grootste gekende priemgetal, $2^{43112609} - 1$, werd in 2008 gevonden door een deelnemer aan de GIMPS. De GIMPS kreeg hiervoor een geldprijs van $100 000 uitgereikt door de Electronic Frontier Foundation (EFF). Deze Amerikaanse non-profit-organisatie komt op voor digitale rechten en wil tegelijk een belangrijke stimulans zijn voor de ontwikkeling van computertechnologie en telecommmunicatie. Zij reikt daarom prijzen uit van $150 000 en $250 000 aan de ontdekker van priemgetallen van respectievelijk 100 miljoen en 1 miljard cijfers. Allen meedoen dus! Al is er wel een dosis geluk nodig opdat jouw computer het volgende priemgetal zou vinden!

Bibliografie

[1] M. Aigner, G. Ziegler, *Proofs from The Book* (4th edition), Springer (Berlin, New York), 2009.

[2] W.R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math139, 703-722, 1994. De eerste pagina van dit artikel is na te lezen op http://www.jstor.org/discover/10.2307/2118576?uid=3737592&uid=2129&uid=2&uid=70&uid=4&sid=47698852587317

[3] F. Beukers, *Getaltheorie voor beginners*, Epsilon Uitgaven (Utrecht), 2005.

[4] B. de Weger, *Elementaire getaltheorie en asymmetrische cryptografie*, Epsilon Uitgaven (Utrecht), 2011.

[5] R. Jeurissen, L. van den Broek, *Spelen met gehelen*, Epsilon Uitgaven (Utrecht), 2002.

[6] http://britton.disted.camosun.bc.ca/sieve/jberatosapplet.htm, geraadpleegd op 20 april 2012

[7] http://en.wikipedia.org/wiki/G._H._Hardy, geraadpleegd op 20 april 2012

[8] http://en.wikiquote.org/wiki/Paul_Erdos, geraadpleegd op 20 april 2012

[9] http://primes.utm.edu, geraadpleegd op 26 maart 2012

[10] http://primes.utm.edu/top20/page.php?id=1, geraadpleegd op 20 april 2012

[11] http://www.fondspascaldecroos.org/uploads/documentenbank/fbf96cf93a77dd3c37ec90a27f324e5e.pdf

[12] http://www.gedesasoft.be, geraadpleegd op 3 maart 2012

[13] http://www.kennislink.nl/publicaties/digitale-beveiliging-met-priemgetallen-nadert-houdbaarheidsdatum, geraadpleegd op 20 april 2012

[14] http://www.kennislink.nl/publicaties/oneindig-veel-priemgetallen, geraadpleegd op 26 maart 2012

[15] http://www.kennislink.nl/publicaties/priemgetallen, geraadpleegd op 3 maart 2012

[16] http://www.math.uu.nl/~oort0109/HOVO2-book.pdf, geraadpleegd op 22 april 2012

[17] http://www.mersenne.org, geraadpleegd op 26 maart 2012

[18] http://www.oxbridgewriters.com/essays/mathematics/de-geschiedenis-van-de-priemgetallen.php, geraadpleegd op 22 april 2012

[19] http://www.rsa.com/rsalabs/node.asp?id=2093, , geraadpleegd op 22 april 2012

[20] http://www.unsolvedproblems.org/, geraadpleegd op 26 maart 2012

Hilde en Els Vl