Herman te Riele
CWI, Amsterdam
herman@cwi.nl

Onderzoek

Grootschalig rekenen in de getaltheorie

De getaltheorie kent bekende onbewezen beweringen, zoals het vermoeden van Goldbach en de Riemann-hypothese. Er is een tijd geweest dat wiskundigen nogal neerkeken op hen die aan dit soort problemen gingen rekenen. Met de komst van steeds snellere computers die enorm veel saai rekenwerk uit handen kunnen nemen, is echter een nieuw vakgebied ontstaan, dat van de 'Computationele getaltheorie'. Hierin wordt geprobeerd om algoritmen voor allerlei problemen uit de getaltheorie te vinden en/of te verbeteren en met behulp hiervan onze kennis van deze problemen te vergroten. Tegenwoordig worden hierbij allerlei soorten en maten van computers ingezet. Herman te Riele illustreert deze ontwikkelingen aan de hand van een aantal voorbeelden, inclusief toepassingen in de cryptografie. Dit artikel is een uitgewerkte versie van zijn voordracht tijdens het Wintersymposium van het KWG op 7 januari 2012 in Utrecht.

Aan de hand van de volgende vijf klassieke problemen uit de getaltheorie laten we zien hoe grootschalige computerberekeningen hebben geholpen om onze kennis van deze problemen aanzienlijk te vergroten en ons inzicht erin te verdiepen:

- het zoeken naar volmaakte getallen en generalisaties;
- het ontbinden in priemfactoren van zeer grote getallen (met implicaties voor de cryptografie);
- de Riemann-hypothese;
- het vermoeden van Goldbach met varianten;
- het vermoeden van Mertens.

In alle gevallen is bijzonder veel — vaak brute force — rekenkracht gebruikt, op allerlei soorten computers, inclusief supercomputers. Ook in alle gevallen, behalve voor zover bekend het laatste, is in grote *collectieve* rekenprojecten op tienduizenden thuiscomputers van vrijwilligers aan deze problemen gerekend.

De Riemann-hypothese staat op een lijst van de zeven grootste onderzoeksvragen van de moderne wiskunde [2]. Het waar zijn hiervan heeft belangrijke gevolgen voor onze kennis van de verdeling van de priemgetallen in de verzameling van de natuurlijke getallen. Steeds uitgebreidere numerieke verificaties van de Riemann-hypothese hebben de plausibiliteit van dit vermoeden alleen maar versterkt. De juistheid van het vermoeden van Mertens impliceert het waar zijn van de Riemann-hypothese en dit verklaart de belangstelling voor dit vermoeden, totdat het onjuist zijn hiervan werd bewezen. Het ontbinden in priemfactoren van grote getallen is voor zover bekend een lastig rekenprobleem. Hierop is de vermeende veiligheid van het veelgebruikte *RSA public-key cryptosysteem* gebaseerd. Aangetoond is dat er voor kwantumcomputers een snel algoritme voor het ontbinden in priemfactoren bestaat dat RSA in de praktijk onbruikbaar zou maken [6]. De huidige kwantumcomputers zijn echter hiervoor nog veel te primitief.

De problemen van het zoeken naar volmaakte getallen en het vermoeden van Goldbach behoren tot de categorie van wiskundi-

Gevolg waar zijn Riemann-hypothese
Zij $\pi(x)$ het aantal priemgetallen $\leq x$ en $\mathrm{li}(x) := \int_2^x dt/\log t$. De beroemde Priemgetalstelling zegt dat $\pi(x)$ van de orde van grootte $x/\log x$ is. Het waar zijn van de Riemann-hypothese impliceert dat het verschil $\pi(x) - \mathrm{li}(x)$ ruwweg van de orde van grootte $\sqrt{x}\log x$ is, veel kleiner dus dan de grootte van $\pi(x)$ zelf. Dit gedrag wordt bevestigd door berekeningen van $(\pi(x) - \mathrm{li}(x))/(\sqrt{x}\log x)$, uitgevoerd voor $x = 10^k, k = 1, 2, \ldots, 21$ [6, Table 1.1].

ge vragen die eenvoudig zijn te stellen — en die daardoor veel belangstelling trekken en hebben getrokken bij amateurs — maar die, naar blijkt, uiterst lastig zijn te beantwoorden. Toepassingen hiervan zijn niet bekend maar het zijn en blijven wel problemen die tot de verbeelding spreken en een voortdurende uitdaging vormen voor hen die geboeid worden door rekenkundige vragen.

Notatie: met 'de complexiteit van een algoritme (of formule) is $\mathcal{O}(f(t))$' geven we aan dat voor de hoeveelheid rekenwerk $R(t)$ om dit algoritme uit te voeren (of deze formule te berekenen) geldt dat $\lim_{t\to\infty} R(t)/f(t)$ begrensd is. Met 'CPU-tijd' geven we aan de Central Processing Unit-rekentijd van een computer om een gegeven rekenklus uit te voeren. Hierbij wordt niet de I/O-tijd meegeteld, dat is de tijd nodig om data in en uit te voeren die bij de rekenklus worden gebruikt, respectievelijk worden afgeleverd.

Volmaakte en bevriende getallen

Zij $s(n)$ de som van alle delers van n behalve n zelf, dus $s(n) := \sigma(n) - n$. Een *volmaakt* getal is een positief geheel getal n waarvoor geldt: $n = s(n)$. Bijvoorbeeld:

$$\begin{aligned} 6 &= 2\cdot 3 = 2\cdot(2^2-1) = 1+2+3,\\ 28 &= 2^2 7 = 2^2\cdot(2^3-1) = 1+2+4+7+14,\\ 496 &= 2^4 31 = 2^4\cdot(2^5-1)\\ &= 1+2+4+8+16+31+62+124+248. \end{aligned}$$

Er zijn geen *oneven* volmaakte getallen bekend. De *even* volmaakte getallen worden als volgt gekarakteriseerd:

Stelling 1 (Euclides, Euler). *Een even getal n is volmaakt dan en slechts dan als $n = 2^{k-1}M_k$ waarbij $M_k = 2^k - 1$ een (zogenaamde Mersenne-) priemgetal is.*

Momenteel zijn er 48 volmaakte getallen, en dus Mersenne-priemgetallen, bekend. Het tot nu toe grootste, op 25 januari 2013 ontdekt, heeft $k = 57\,885\,161$ en is een getal van $17\,425\,170$ cijfers. De veertien grootste bekende Mersenne-priemgetallen zijn gevonden in het 'Great Internet Mersenne Prime Search'-project, een wereldwijd zoekproject op vele tienduizenden PC's [12]. Voor het bewijzen van de primaliteit van M_k is de zeer snelle zogenaamde Lucas–Lehmer-test beschikbaar [6, Section 4.2.1]. De complexiteit van deze test is $\mathcal{O}(k^2 \log k \log\log k)$.

oneven volmaakte getallen zijn zoals gezegd niet bekend maar het is ook niet bekend of ze bestaan. Pomerance bewees in 1973 dat ieder oneven volmaakt getal tenminste zeven verschillende priemfactoren zou moeten hebben [39]. Nielsen verhoogde dit aantal naar negen in 2007 [28]. In 2001 heeft Brent met uitgebreide berekeningen aangetoond dat een oneven volmaakt getal, als het bestaat, groter is dan 10^{300} [3]. Deze ondergrens is kort geleden door Ochem en Rao verhoogd naar 10^{1500} [29]. Zij toonden daarbij ook aan dat de grootste priemmacht in een oneven volmaakt getal groter is dan 10^{62} en dat het aantal priemfactoren van een oneven volmaakt getal (multipliciteit meetellend) tenminste 101 is.

Volmaakte getallen kunnen worden beschouwd als dekpunten na één iteratie van de functie $s(n)$. Dekpunten na *twee* iteraties voldoen aan de vergelijkingen

$$m = s(n) \text{ en } n = s(m) = s(s(n)), \quad n \neq m.$$

Zo'n paar getallen (m, n) met $m < n$ heet *bevriend*. Voorbeeld:

$$(220, 284) = (2^2 5\cdot 11, 2^2 71)$$

is een bevriend getallenpaar omdat

$$\begin{aligned} 220 &= s(284) = 7\cdot 72 - 284 \text{ en}\\ 284 &= s(220) = 7\cdot 6\cdot 12 - 220. \end{aligned}$$

Analoog aan even volmaakte getallen is er een *regel* waarmee nieuwe bevriende getallenparen kunnen worden gevonden:

Regel van Thabit ibn Kurrah (negende eeuw). $2^k pq$ en $2^k r$ vormen een bevriend getallenpaar als $p = 3\cdot 2^{k-1} - 1$, $q = 3\cdot 2^k - 1$ en $r = 9\cdot 2^{2k-1} - 1$ alle priem zijn en $k > 1$.

Voor $k = 2$ geeft deze regel het bovengenoemde bevriende getallenpaar $(220, 284)$. Ook voor $k = 4$ en $k = 7$ vinden we zo bevriende getallenparen, maar dan lijkt de koek op: voor geen andere waarden van $k \le 6\,090\,515$ is deze regel succesvol [36].

Zij $a(X)$ het aantal bevriende getallenparen (m, n), $m < n$, met $m \le X$. Er is een tabel [33] met een totaal van $11\,994\,387$ bekende bevriende getallenparen (bijgewerkt tot 28 september 2007), met daarin *alle* bevriende getallenparen $\le 10^{14}$. Zie Tabel 1. Dit suggereert dat het quotiënt $\log a(X)/\log X$ naar een limiet convergeert, als $X \to \infty$, met mogelijke waarde $\frac{1}{3}$.

De meeste bekende bevriende getallenparen zijn gevonden met behulp van variaties van de Regel van Thabit ibn Kurrah. Voor een overzicht, zie [11]. Dekpunten van $s(n)$ na $j \ge 3$ iteraties zijn verder bekend voor $j = 4, 5, 6, 8, 9$, en $j = 28$, met aantallen, respectievelijk, $206, 1, 5, 3, 1, 1$ [26].

X	$a(X)$	$\log(a(X))/\log(X)$ (4 decimalen)
10^5	13	0,2228
10^6	42	0,2705
10^7	108	0,2905
10^8	236	0,2966
10^9	586	0,3075
10^{10}	1427	0,3154
10^{11}	3340	0,3203
10^{12}	7642	0,3236
10^{13}	17519	0,3264
10^{14}	39374	0,3282

Tabel 1 Aantallen bevriende getallenparen

Grote getallen en cryptografie

Het ontbinden in (priem)factoren van grote getallen is een getaltheoretisch probleem dat ook voorkomt in het leven van alledag. Het heeft vast al belangstelling getrokken in de oudheid, bijvoorbeeld met de vraag: hoe kan een herder een flink aantal schapen eerlijk verdelen over zijn kinderen? Daarvoor moet iets als een deling met rest worden uitgevoerd. Als die rest dan toevallig 0 is, zal dat de aandacht getrokken hebben omdat dat veel minder vaak voorkomt dan een rest die ongelijk is aan 0.

In 1978 hebben **R**ivest, **S**hamir en **A**dleman het *RSA public-key cryptosysteem* geïntroduceerd [41]. De mogelijkheid om dit systeem te kraken hangt af van de moeilijkheidsgraad van het ontbinden van grote getallen in priemfactoren. Deze eigenschap van RSA heeft de belangstelling voor het ontbindingsprobleem en voor snellere ontbindingsalgoritmen enorm gestimuleerd. Verscheidene nieuwe ontbindingsalgoritmen zijn dan ook sinds 1978 ontdekt: de kwadratische zeef van Pomerance [37–38] (waarvan het basis-idee teruggaat tot Kraitchik [20]), de getallenlichaamszeef van Pollard [35] met vele verbeteringen door Pomerance en H.W. en A.K. Lenstra [21], en de elliptische krommenmethode van H.W. Lenstra [22].

Om de complexiteit van deze algoritmen te beschrijven, definiëren we

$$L_x[v, \lambda] := \exp(\lambda(\log x)^v (\log\log x)^{1-v})$$

voor reële getallen x, v en λ met $x > e$.

Voor het gemak korten we de uitdrukking $L_x[v, \lambda + o(1)]$ af tot $L_x[v, \lambda]$, waarbij we met $o(1)$ een term aangeven die naar 0 conver-

geert als $x \to \infty$. Deze functie interpoleert tussen machten van n en machten van $\log n$:

$$L_n[1,\lambda] = n^{\lambda}, \quad L_n[0,\lambda] = (\log n)^{\lambda}.$$

De belangrijkste parameter is v. De traditionele probeermethode (probeer of het getal deelbaar is door de priemgetallen $2,3,5,7,\ldots$) heeft $v = 1$, exponentiële tijd. Polynomiale tijd heeft $v = 0$. Er zijn veel algoritmen waarvan men vermoedt dat $v = \frac{1}{2}$, dus deze liggen 'halverwege' tussen exponentiële en polynomiale tijd. Op basis van heuristische overwegingen wordt de complexiteit van de kwadratische zeef geschat op (n is het te ontbinden getal): $L_n[\frac{1}{2}, 1]$ en die van de getallenlichaamszeef op $L_n[\frac{1}{3}, c]$ met $c = (\frac{64}{9})^{1/3} \doteq 1{,}9230$. Voor de elliptische krommenmethode is de geschatte complexiteit gelijk aan $L_p[\frac{1}{2}, \sqrt{2}]$ waarbij p de kleinste priemfactor is van het te ontbinden getal. Hier zien we een belangrijk verschil tussen de elliptische krommenmethode en bovengenoemde zeefmethoden: de complexiteit van de eerstgenoemde hangt af van de kleinste priemdeler van het te ontbinden getal, terwijl die van de zeefmethoden afhangt van het te ontbinden getal zelf.

Het beste in 1978 gepubliceerde ontbindingsresultaat was een getal van 39 decimalen dat in twee uur CPU-tijd gekraakt was [27]. Extrapolatie van dit resultaat gaf aan dat het, op één computer met 1978-technologie, naar schatting 62 miljard jaar rekenen zou kosten om een getal van 512 bits te ontbinden. Getallen van 512 bits waren in die tijd een populaire keuze voor RSA-sleutels die toen als veilig werd beschouwd, dat wil zeggen onkraakbaar voor de best bekende algoritmen en snelste computers uit die tijd. De bovengenoemde nieuwe ontbindingsalgoritmen én de komst van steeds snellere computers met steeds meer geheugen, hebben ervoor gezorgd dat het ontbindingsrecord van 39 decimalen in 1978 naar 512 bits (155 decimalen) in 1999 [4] en naar 768 bits (232 decimalen) in 2009 is opgevoerd [17].

De twee genoemde zeefmethoden proberen het te factoriseren getal te schrijven als verschil van twee kwadraten. Bij de kwadratische zeef gaat dat in principe als volgt. Kies bijvoorbeeld $n = 1649$, dan geldt:

$$41^2 = 1681 \equiv 32 \bmod n,$$
$$42^2 = 1764 \equiv 115 \bmod n,$$
$$43^2 = 1849 \equiv 200 \bmod n.$$

Als we de eerste en de derde congruentie met elkaar vermenigvuldigen, krijgen we:

$$(41 \cdot 43)^2 \equiv 6400 = 80^2 \bmod n,$$
$$(41 \cdot 43)^2 = 1763^2 \equiv 114^2 \equiv 80^2 \bmod n,$$

dus $n = 1649$ is een deler van $(114 - 80) \cdot (114 + 80)$. Berekenen we nu de grootste gemeenschappelijke deler (ggd) van 1649 en $114 - 80 = 34$ dan vinden we:

$$\text{ggd}(1649, 34) = \text{ggd}(34, 17) = 17,$$

dus 17 is een deler van 1649. Het quotiënt is 97, de tweede (priem)factor van 1649. De ggd van twee getallen kan snel worden gevonden met behulp van het euclidische algoritme, dat gebaseerd is op de relatie $\text{ggd}(m, n) = \text{ggd}(n, m \bmod n)$.

Het principe van RSA werkt als volgt. Elke deelnemer heeft een *openbare* en een *geheime* sleutel die als volgt worden gegenereerd. Neem twee grote priemgetallen, p en q, en bereken hun product $n = pq$. Kies nu een getal e zodanig dat

$$1 < e < n \text{ en } \text{ggd}(e, (p-1)(q-1)) = 1.$$

Vind nu d zodanig dat

$$ed \equiv 1 \bmod (p-1)(q-1). \qquad (1)$$

Dit kan snel gebeuren met behulp van het euclidische algoritme [6, Section 2.1.1]. De openbare sleutel is nu het paar getallen (n, e) en de geheime sleutel is het getal d.

Stel nu dat Alice een boodschap m wil versturen aan Bob. Alice neemt Bobs openbare sleutel (n, e) uit het openbare sleutelboek, vercijfert haar boodschap door $c = m^e \bmod n$ uit te rekenen, en stuurt c naar Bob. Bob ontcijfert de ontvangen boodschap c met behulp van zijn geheime sleutel d door $c^d \bmod n$ te berekenen. Met behulp van de Stelling van Euler:

$$\text{als } \text{ggd}(m, n) = 1, \text{ dan } m^{\phi(n)} \equiv 1 \bmod n$$

(waarbij $\phi(n)$ Euler's ϕ-functie is die het aantal natuurlijke getallen m met $1 \le m \le n$ telt, die relatief priem zijn ten opzichte van n), leiden we af, gebruikmakend van (1), dat

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\phi(n)+1} \equiv m \bmod n.$$

Als nu m zo was gekozen dat $1 < m < n$ dan volgt dat $c^d \bmod n = m$. Als men de priemfactoren p en q van n zou weten, dan zou het niet moeilijk zijn om d (uit (1)) te vinden.

Alice kan op de boodschap die ze aan Bob wil versturen ook nog haar handtekening zetten met behulp van haar eigen geheime sleutel. Bob kan die handtekening verifiëren met behulp van de openbare sleutel van Alice. Dit illustreert een belangrijke eigenschap van RSA: symmetrie.

Het onderzoek van public-key cryptosystemen en hun betrouwbaarheid vraagt een brede kennis van wiskunde en informatica. Problemen die daarbij aan de orde komen zijn: het ontbinden in priemfactoren van (zeer) grote getallen; primaliteitstests; berekening van discrete logaritmen; analyse van elliptische krommen; complexiteitsanalyse; het vinden van polynomen met ongebruikelijk veel gladde waarden (dat wil zeggen waarden waarin veel kleine priemfactoren zitten); het oplossen van grote ijle stelsels van lineaire vergelijkingen over eindige lichamen; het berekenen van wortels van grote algebraïsche getallen; modulaire aritmetiek; multiprecisie-aritmetiek; computerproblemen zoals cache-optimalisatie, parallel programmeren en het efficiënt omgaan met grote hoeveelheden data.

De Riemann-hypothese

De Riemann-zeta-functie is de analytische functie van $s = \sigma + it$, voor $\sigma > 1$ gedefinieerd door:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

en, door middel van analytische voortzetting, voor $\sigma \le 1, \sigma \ne 1$. Deze functie heeft nulpunten in de negatieve even gehele getallen (de zogenaamde triviale nulpunten, zo genoemd omdat ze op tamelijk eenvoudige wijze zijn te vinden) en in de zogenaamde *kritieke strip* $0 < \sigma < 1$ (de zogenaamde niet-triviale nulpunten). Hierin liggen de nulpunten symmetrisch om de lijn $\sigma = \frac{1}{2}$ en symmetrisch om de lijn $t = 0$.

De *Riemann-hypothese* [40] is de bewering dat alle niet-triviale nulpunten *op* de zogenaamde kritieke lijn $\sigma = \frac{1}{2}$ liggen. Voorbeeld: met behulp van het *Mathematica*-pakket [24] vinden we (een numerieke benadering van) de nulpunten in respectievelijk $s = -2$ (bij startpunt $s = 0$) en $s = \frac{1}{2} + 14{,}1347\ldots$ (bij startpunt $s = 0{,}4 + 12i$). Zie Figuur 1. $\zeta(s)$ voldoet aan de volgende functionaal

```
In[39]:= FindRoot[Zeta[s] == 0, {s, 0}]
Out[39]= {s → -2.}

{s → -1.9999999999999973`}

In[40]:= FindRoot[Zeta[s] == 0, {s, 0.4 + 12 I}]
Out[40]= {s → 0.5 + 14.1347 ⅈ}

{s → 0.5000000000000071` + 14.134725141734693` ⅈ}
```

Figuur 1 Twee nulpunten van $\zeta(s)$

vergelijking [10]:

$$\xi(s) = \xi(1-s) \text{ met}$$
$$\xi(s) = \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Het is niet zo lastig om te laten zien [15, Theorem 15] dat $\xi(s)$ reëel is voor reële s en dat $\xi(s) = \overline{\xi(\overline{s})}$. Daaruit volgt dat ook $\xi(\frac{1}{2}+it)$ reëel is. Om de niet-triviale nulpunten van de *complexe* functie $\zeta(s)$ op de lijn $s = \frac{1}{2}$ te bestuderen kan men dus de *reële* functie $\xi(\frac{1}{2}+it)$ gebruiken, en proberen tekenwisselingen van deze — continue — functie op te sporen.

We schrijven nu, met $s = \frac{1}{2}+it$,

$$\xi\left(\frac{1}{2}+it\right) = \left[e^{\Re \log\Gamma(s/2)}\pi^{-1/4}\frac{(-t^2-\frac{1}{4})}{2}\right] \times \left[e^{i\Im \log\Gamma(s/2)}\pi^{-it/2}\zeta(s)\right].$$

Hierin is de factor binnen de eerste verzameling rechte haken een negatief reëel getal, dus is het teken van $\xi(\frac{1}{2}+it)$ tegengesteld aan het teken van de factor binnen de tweede verzameling rechte haken. De standaardnotatie voor deze tweede factor is $Z(t)$, dat wil zeggen

$$Z(t) = e^{i\theta(t)}\zeta\left(\frac{1}{2}+it\right),$$

waarbij $\theta(t)$ gedefinieerd wordt door

$$\theta(t) = \Im\left[\log\Gamma\left(\frac{1}{4}+\frac{it}{2}\right)\right] - \frac{t}{2}\log\pi.$$

Aangezien $|Z(t)| = |\zeta(\frac{1}{2}+it)|$, vallen de nulpunten van Z samen met de imaginaire delen van de nulpunten van $\zeta(s)$ *op* de kritieke lijn. $Z(t)$ staat bekend als de *Riemann–Siegel* functie. Zie Figuur 2. Zij $N(T)$ het totale aantal complexe nulpunten ρ van $\zeta(s)$ met $0 < \Im(\rho) < T$ (rekening houdende met multipliciteit van de nulpunten). In 1914 heeft Backlund bewezen [1] dat onder bepaalde voor waarden $N(T)$ gelijk is aan het natuurlijke getal dat het dichtst bij $\theta(T)/\pi + 1$ ligt. Om $\theta(t)$ uit te rekenen kan men gebruik maken van de expansie [10, Section 6.5]:

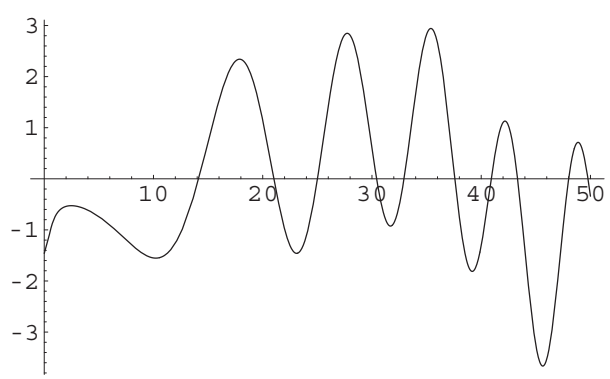
$$\theta(t) = \frac{t}{2}\log\frac{t}{2\pi} - \frac{t}{2} - \frac{\pi}{8} + \frac{1}{48t} + \mathcal{O}(t^{-3}),$$
voor $t \to \infty$.

In principe is het op deze manier mogelijk om alle niet-triviale nulpunten van $\zeta(s)$ in een gegeven deel $T_1 < \Im(s) < T_2$ van de kritieke strip te tellen, inclusief eventuele nulpunten die *niet* op de kritieke lijn $\Re(s) = \frac{1}{2}$ liggen: bepaal zo goed mogelijk het aantal tekenwisselingen van $Z(t)$ voor $T_1 < t < T_2$ ($Z(t)$ is continu, dus tussen elke tekenwisseling ligt tenminste één nulpunt) en pas het resultaat van Backlund toe om te verifiëren of daarmee *alle* nulpunten in het gebied $T_1 < \Im(s) < T_2$ zijn geteld. In de praktijk blijkt dit perfect te werken. Om de nulpunten van ζ in de kritieke strip te bepalen moeten we dus $\zeta(s)$ voor $s = \frac{1}{2}+it$ en $Z(t)$ kunnen uitrekenen, inclusief een veilige bovengrens voor de fout (want dan kunnen we het aantal tekenwisselingen van $Z(t)$ exact bepalen). Voor de eerste nulpunten kunnen we de zogenaamde Euler–Maclaurin-formule [10, Chapter 6] gebruiken, zoals ook de eerste zeta-nulpuntenrekenaars Gram, Backlund en Hutchinson hebben gedaan. De complexiteit van de Euler–Maclaurin-formule is $\mathcal{O}(t)$ (voor $s = \frac{1}{2}+it$). Voor hoger gelegen nulpunten is de Riemann–Siegel-formule geschikter. Deze is door Siegel in 1932 gepubliceerd [42] en afgeleid uit nagelaten aantekeningen van Riemann.

Vele wiskundigen vóór Siegel hadden tevergeefs geprobeerd deze aantekeningen te ontcijferen en uit te werken. De complexiteit van de Riemann–Siegel-formule is $\mathcal{O}(\sqrt{t})$. Dankzij deze formule was het mogelijk om de Riemann-hypothese te verifiëren tot het 10 biljoenste nulpunt. Tabel 2 geeft een overzicht van de geschiedenis van de partiële verificatie van de Riemann-hypothese. Odlyzko [30] en Gourdon [13] hebben de Riemann-hypothese geverifieerd in hogere stukken van de kritieke strip. Odlyzko deed dat voor 10^{10} nulpunten in de buurt van nulpunt met rangnummer 10^{22} en Gourdon voor 2×10^9 nulpunten in de buurt van de nulpunten met rangnummer 10^{23} en 10^{24}.

Het is hier niet de plaats om op details van het rekenen aan de Riemann-hypothese in te gaan. De lezer zij hiervoor verwezen naar het boek van Edwards [10]. Een mooie inleiding in de Riemann-hypothese is het boek [44] dat een neerslag is van een UvA-webklas wiskunde voor vwo-leerlingen in de periode 2006–2010.

```
In[63]:= Plot[RiemannSiegelZ[t], {t, 0, 50}]
```




```
Out[63]= - Graphics -
```

Figuur 2 De Riemann–Siegel-functie $Z(t)$ met de eerste 10 nulpunten op de kritieke lijn

De 3 Priemen-stelling

Het bekende Goldbach-vermoeden [32] beweert dat elk even getal ≥ 4 kan worden geschreven als de som van twee priemgetallen. Hoewel er sterke numerieke aanwijzingen zijn dat het Goldbach-vermoeden waar is,

jaar	n	auteur(s)
1903	15	Gram
1914	79	Backlund
1925	138	Hutchinson
1935	1 041	Titchmarsh
1953	1 104	Turing
1956	25 000	Lehmer
1958	35 337	Meller
1966	250 000	Lehman
1968	3 502 500	Rosser, Yohe, Schoenfeld
1979	81 000 001	Brent
1982	200 000 001	Brent, Van de Lune, Te Riele, Winter
1983	300 000 001	Van de Lune, Te Riele
1986	1 500 000 001	Van de Lune, Te Riele, Winter
2001	10 000 000 000	Van de Lune
2004	900 000 000 000	Wedeniwski [45]
2004	10 000 000 000 000	Gourdon en Demichel [13]

Tabel 2 Geschiedenis van partiële bewijzen van de Riemann-hypothese (voor de eerste n niet-triviale nulpunten)

is dit nooit bewezen. Het is geverifieerd voor alle even getallen $\leq 4 \times 10^{18}$ [32]. Als het Goldbach-vermoeden waar is, volgt daar triviaal de zogenaamde *3 Priemen-stelling* uit, namelijk dat ieder *oneven* getal ≥ 7 geschreven kan worden als de som van drie priemgetallen. Wat is hierover bekend, zonder aanname vooraf? In 1989 is bewezen [5] dat ieder oneven getal $> 10^{43\,000}$ kan worden geschreven als de som van drie priemgetallen. Onder aanname van het waar zijn van de zogenaamde Gegeneraliseerde Riemann-hypothese (GRH, namelijk dat het reële deel van alle niet-triviale nulpunten van elke Dirichlet-L-functie gelijk is aan $\frac{1}{2}$) is in 1997 bewezen [7] dat ieder oneven getal ≥ 7 kan worden geschreven als de som van drie priemgetallen. Het bewijs hiervan kan in drie delen worden opgesplitst:

a. (Zinoview, 1997) Onder de aanname van GRH kan ieder oneven getal $> 10^{20}$ worden geschreven als de som van drie priemgetallen.
b. Onder de aanname van GRH is er voor iedere $6 \leq n \leq 10^{20}$ een priemgetal p zodanig dat $4 \leq n-p \leq 1{,}615 \times 10^{12}$. Als n nu een oneven getal $\leq 10^{20}$ is dan is $m = n - p$ even en $m \leq 1{,}615 \times 10^{12}$. Dan passen we het volgende resultaat toe:
c. (Deshouillers en Te Riele, 1997) Ieder even getal m met $4 \leq m \leq 10^{13}$ kan geschreven worden als som van twee priemgetallen (dit verbeterde de toentertijd beste bovengrens voor het Goldbach-vermoeden van Sinisalo uit 1993: 4×10^{11}).

We zullen hier twee manieren beschrijven om het Goldbach-vermoeden (GV) te verifiëren.

1. Zij p_i het i-de oneven priemgetal. De gebruikelijke manier om GV op een gegeven interval $[a, b]$ te verifiëren is om bij ieder even getal $e \in [a, b]$ het kleinste priemgetal p_i te vinden waarvoor $e - p_i$ ook priem is. Een efficiënte manier om dit te doen is om eerst de verzameling priemgetallen

$$\mathcal{Q}(a, b) = \{q | q \text{ priem en } a - \epsilon_a \leq q \leq b\},$$

te genereren (met de bekende Zeef van Eratosthenes), waarbij ϵ_a op een geschikte manier gekozen wordt (niet te klein, zie verder) en om dan de verzamelingen van even getallen $\mathcal{E}_0 \subset \mathcal{E}_1 \subseteq \mathcal{E}_2 \subseteq \cdots$ te genereren, gedefinieerd door $\mathcal{E}_0 = \emptyset$,

$$\mathcal{E}_{i+1} = \mathcal{E}_i \cup (\mathcal{Q}(a, b) + p_{i+1}), \quad i = 0, 1 \ldots,$$

totdat, voor één of andere waarde van j, $\mathcal{E}_j$ *alle* even waarden in $[a, b]$ bevat. Hierbij moet ϵ_a groter zijn dan het grootste oneven priemgetal dat gebruikt wordt bij het genereren van de verzamelingen $\mathcal{E}_i$.
2. Een ander idee is om voor alle even getallen $e \in [a, b]$ een priemgetal q te vinden dat dichtbij a ligt, waarvoor $e - q$ priem is. Daarvoor genereren we een verzameling van k opeenvolgende priemgetallen $q_1, q_2, \ldots, q_k$ dichtbij a, voor geschikt gekozen k (zie verder), en een grote verzameling priemgetallen $\mathcal{P}$ van alle oneven priemgetallen tot ongeveer $b - a$ (met de Zeef van Eratosthenes) waarmee we $e - q$ testen op primaliteit. Voor de actuele check genereren we de verzamelingen van even getallen $\mathcal{F}_0 \subset \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \cdots$ gedefinieerd door $\mathcal{F}_0 = \emptyset$,

$$\mathcal{F}_{i+1} = \mathcal{F}_i \cup (\mathcal{P} + q_{i+1}), \quad i = 0, 1, \ldots,$$

totdat, voor één of andere waarde van j, $\mathcal{F}_j$ *alle* even waarden in $[a, b]$ bevat.

In de eerste genoemde aanpak om GV te verifiëren wordt een verzameling van kleine priemgetallen tot, zeg, 5000 gebruikt en voor ieder interval $[a, b]$ moeten dan alle priemgetallen in dat interval $[a, b]$ gegenereerd worden. In de tweede genoemde aanpak wordt eenmalig een grote verzameling van priemgetallen $\mathcal{P}$ tot ongeveer $10^8 + 10^4$ gegenereerd, en voor ieder interval $[a, b]$ moet men dan de k grootste priemgetallen $\leq a$ genereren. Dit is natuurlijk qua rekentijd veel goedkoper dan de eerste aanpak. Het *verschil* is dat in de eerste aanpak voor ieder even getal e het *kleinste* oneven priemgetal p wordt gezocht waarvoor $e - p$ priem is. In de tweede aanpak wordt *een of ander* priemgetal p gezocht waarvoor $e - p$ priem is, maar in het algemeen is dit noch het kleinste noch het grootste priemgetal met die eigenschap.

In hun experimenten om GV tot 10^{13} te verifiëren [8] hebben Deshouillers, Te Riele en Saouter de tweede aanpak gevolgd. De lengte van het te verifiëren interval $[a, b]$ werd steeds gelijk gekozen aan 10^8. Hoe groot moest hierbij k worden gekozen? De dichtheid van de priemgetallen in de verzameling van oneven getallen $< 10^8$ is ongeveer 0,115 (er zijn 5 761 454 oneven priemgetallen $< 10^8$ en 5×10^7 oneven getallen $< 10^8$). Dus een fractie van ongeveer 0,885 van de even getallen in $[a, b]$ wordt *niet* bedekt door de verzameling $\mathcal{F}_1 = \mathcal{P} + q_1$. Als we uniforme verdeling van de priemgetallen aannemen wordt ongeveer $0{,}885^2$ van de even getallen in $[a, b]$ *niet* bedekt door $\mathcal{F}_2$, enzovoorts. Na 151 stappen is deze fractie gereduceerd tot ongeveer 10^{-8}. Voor onze experimenten bleek $k = 360$ ruim groot genoeg te zijn. Voor $a \approx 10^{13}$ impliceert dit dat het grootste priemgetal in de verzameling $\mathcal{P}$ in de buurt van $10^8 + 10^4$ moet liggen. De hoeveelheid CPU-tijd nodig om zo GV tot 10^{13} te verifiëren bedroeg ongeveer vijftig uur op een Cray C98 vector computer, gemiddeld iets minder dan twee seconden CPU-tijd per interval $[a, b]$ ter lengte van 10^8.

Het vermoeden van Mertens

De Möbius-functie $\mu(n)$ wordt als volgt gedefinieerd:

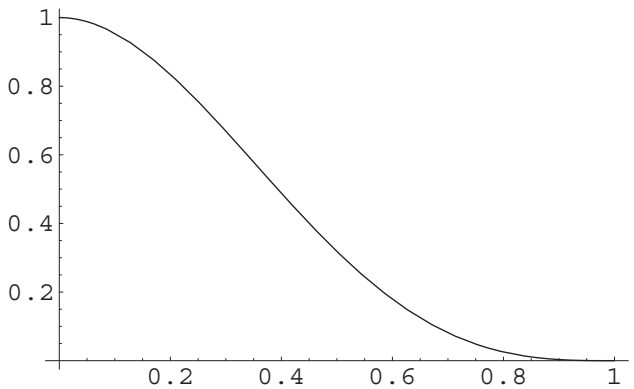
$$\mu(n) := \begin{cases} 1, & n = 1, \\ 0, & \text{als } n \text{ deelbaar is door het kwadraat van een priemgetal,} \\ (-1)^k, & \text{als } n \text{ het product is van k verschillende priemgetallen.} \end{cases}$$

Als we de waarden $\mu(n)$ voor $1 \leq n \leq x$ sommeren krijgen we de functie

$$M(x) = \sum_{1 \leq n \leq x} \mu(n),$$

die het verschil telt tussen het aantal kwa-

```
Plot[(1 - t) * Cos[Pi * t] + Sin[Pi * t] / Pi, {t, 0, 1}]
```



Figuur 3

draatvrije natuurlijke getallen $n \le x$ met een *even* aantal priemfactoren en dat met een *oneven* aantal priemfactoren. In 1885 claimde Stieltjes in een brief aan Hermite dat hij een bewijs had dat de functie $M(x)/\sqrt{x}$ tussen twee *vaste* grenzen oscilleert, ongeacht hoe groot x is. In het voorbijgaan merkte Stieltjes op dat men voor die grenzen waarschijnlijk -1 en $+1$ kan nemen. Het is mogelijk dat Stieltjes zijn bewering baseerde op tabellen van waarden van $M(x)$ (die in zijn nalatenschap zijn teruggevonden). De motivatie voor Stieltjes om $M(x)$ te bestuderen was dat de grootte van $M(x)$ nauw gerelateerd is aan de locatie van de complexe nulpunten van de Riemann-zeta-functie. Om precies te zijn: het begrensd zijn van $M(x)/\sqrt{x}$ impliceert de juistheid van de Riemann-hypothese! Dat is als volgt in te zien. Voor $\sigma = \Re s > 1$ geldt (met behulp van partiële sommatie):

$$\begin{aligned}
1/\zeta(s) &= \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \\
&= \sum_{n=1}^{\infty} \frac{M(n) - M(n-1)}{n^s} \\
&= \sum_{n=1}^{\infty} M(n) \left\{ \frac{1}{n^s} - \frac{1}{(n+1)^s} \right\} \\
&= \sum_{n=1}^{\infty} M(n) \int_n^{n+1} \frac{s\,dx}{x^{s+1}} \\
&= s \sum_{n=1}^{\infty} \int_n^{n+1} \frac{M(x)\,dx}{x^{s+1}} \\
&= s \int_1^{\infty} \frac{M(x)\,dx}{x^{s+1}},
\end{aligned}$$

omdat $M(x)$ constant is op ieder interval $[n, n+1)$. De begrensdheid van $M(x)/\sqrt{x}$ impliceert dat de laatste integraal in bovenstaande formule een functie definieert die analytisch is in het halfvlak $\sigma > \frac{1}{2}$, en dit zou een analytische voortzetting geven van $1/\zeta(s)$ van $\sigma > 1$ naar $\sigma > \frac{1}{2}$. In het bijzonder zou dat impliceren dat $\zeta(s)$ geen nulpunten heeft in het halfvlak $\sigma > \frac{1}{2}$ wat vanwege de functionaalvergelijking voor $\zeta(s)$ equivalent is met de Riemann-hypothese. Bovendien is het niet moeilijk om uit bovenstaande formules af te leiden dat alle complexe nulpunten van $\zeta(s)$ enkelvoudig zijn (aangenomen dat $M(x)/\sqrt{x}$ begrensd is) [31]. Na Stieltjes hebben ook anderen tabellen van $M(x)$ berekend met het doel om meer data te verzamelen omtrent het gedrag van $M(x)/\sqrt{x}$. In 1897 publiceerde Mertens een artikel met een tabel van $M(x)$ voor $n = 1, 2, \ldots, 10\,000$ die vijftig bladzijden in beslag nam [25]. Op basis van deze data concludeerde Mertens dat de ongelijkheid $|M(x)| < \sqrt{x}$, $x > 1$ 'zeer waarschijnlijk' is. Deze bewering staat bekend als 'het vermoeden van Mertens'. De meest recente systematische berekeningen van $M(x)$ (voor alle $x \in [1, X]$) zijn uitgevoerd door Kotnik en Van de Lune [18], voor $X = 10^{14}$. De grootste *positieve* waarde die ze voor $M(x)/\sqrt{x}$ vonden is $0{,}571$, voor $x = 7\,766\,842\,813$, en de grootste *negatieve* waarde is $-0{,}525$, voor $x = 71\,578\,936\,427\,177$ maar het is nu wel duidelijk dat op deze manier het vermoeden van Mertens niet kan worden weerlegd.

In 1942 publiceerde Ingham [9] een artikel dat de eerste serieuze twijfel uitsprak met betrekking tot het vermoeden van Mertens. Inghams artikel liet zien dat het mogelijk is om te bewijzen dat er bepaalde grote waarden van $|M(x)|/\sqrt{x}$ bestaan *zonder dat daarvoor* $M(x)$ *expliciet hoeft te worden berekend*. Dit stimuleerde verder onderzoek dat in 1985 resulteerde in een artikel van Odlyzko en Te Riele [31] met een bewijs van het *bestaan* van een x waarvoor $M(x)/\sqrt{x} > 1{,}06$ en een andere x waarvoor $M(x)/\sqrt{x} < -1{,}009$. Het vermoeden van Mertens was hiermee dus weerlegd. Odlyzko en Te Riele maakten gebruik van het toentertijd nieuwe *rooster-basis-reductie*-algoritme van A.K. Lenstra, H.W. Lenstra, Jr., en L. Lovász uit 1982 [23]. In 1987 gaf Pintz [34] een *effectieve* weerlegging van het vermoeden van Mertens in de zin dat hij bewees dat $|M(x)|/\sqrt{x} > 1$ voor een of andere $x \le \exp(3{,}21 \times 10^{64})$. Tegenwoordig wordt algemeen aangenomen dat de functie $M(x)/\sqrt{x}$ *onbegrensd* is, zowel in positieve als in negatieve richting.

We zullen hier een schets geven van de indirecte weerlegging van het vermoeden van Mertens door Odlyzko en Te Riele. We schrijven $x = e^y$, $-\infty < y < \infty$ en definiëren

$$m(y) := M(x)x^{-1/2} = M(e^y)e^{-y/2}$$

en

Berekeningen van Kotnik en Te Riele uit 2006

De waarde van y waarvoor het positieve lokale maximum van $h(\cdot, \cdot)$ werd gevonden is

$$y = -233029271\,5134531215\,0140181996\,7723401020\,4456785091$$
$$\backslash 6681557518\,6743434036\,9240230890\,8933261706\,9029233958\,2730162362{,}807965$$

met

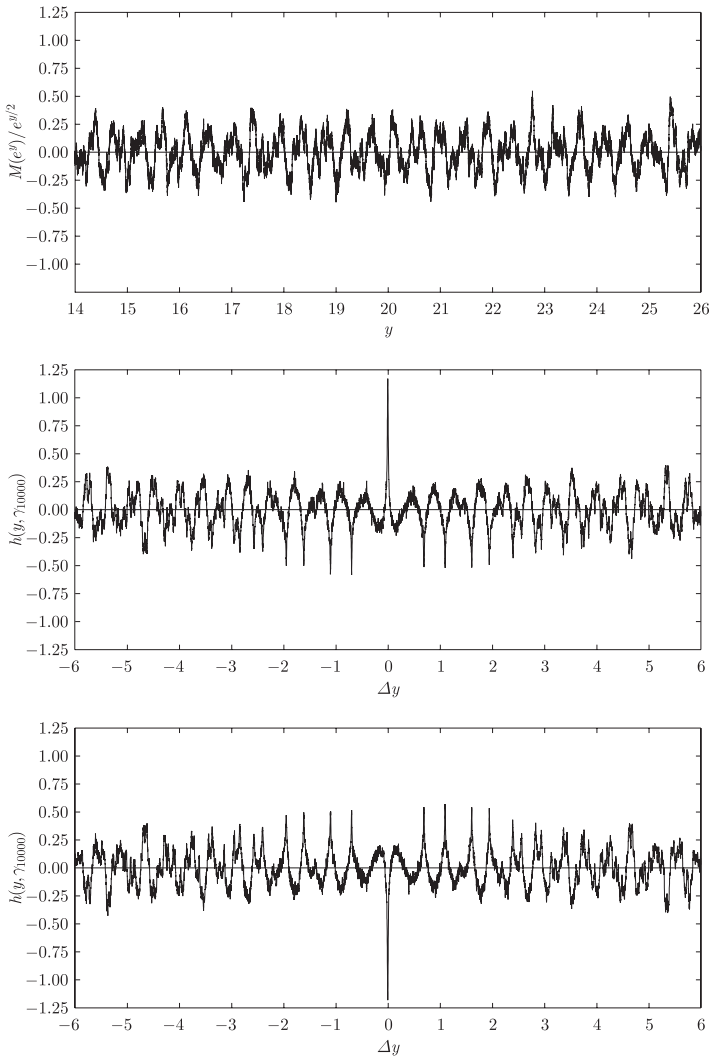
$$h(y, y_{10\,000}) = 1{,}218429$$

en de waarde van y waarvoor het negatieve lokale minimum werd gevonden is

$$y = -1608\,7349754400\,0919817483\,9640165505\,4685212472\,2284778177$$
$$\backslash 5539303027\,5350690810\,7957194829\,6433602695\,1442102295\,3212754000{,}679958$$

met

$$h(y, y_{10\,000}) = -1{,}229385.$$



Figuur 4 Typisch gedrag van $M(e^{\gamma})/e^{\gamma/2}$ vergeleken met atypisch gedrag

$$\underline{m} := \liminf_{\gamma\to\infty} m(\gamma), \qquad \overline{m} := \limsup_{\gamma\to\infty} m(\gamma).$$

Dan geldt [9, 16, 31]:

Stelling 2. *Zij*

$$h(\gamma,T) := 2\sum_{0<\gamma<T}\left[\left(1-\frac{\gamma}{T}\right)\cos\left(\pi\frac{\gamma}{T}\right) + \pi^{-1}\sin\left(\pi\frac{\gamma}{T}\right)\right] \cdot \frac{\cos\left(\gamma\gamma-\psi_\gamma\right)}{|\rho\zeta'(\rho)|} \qquad (2)$$

waarbij $\rho=\beta+i\gamma$ de complexe nulpunten van de Riemann-zeta-functie zijn met $\beta=\frac{1}{2}$ en enkelvoudig. Dan geldt voor ieder *reëel getal γ_0 dat $\underline{m} \le h(\gamma_0,T) \le \overline{m}$ en dat* iedere *waarde $h(\gamma,T)$ willekeurig dicht benaderd wordt, en oneindig vaak, door $M(x)/\sqrt{x}$.*

Dus, door grote waarden van $|h(\gamma,T)|$ te vinden — iets wat veel minder moeilijk is dan het vinden van grote waarden van $|M(x)|/\sqrt{x}$ — zou het misschien mogelijk zijn om het vermoeden van Mertens te weerleggen. Aangezien $(1-t)\cos(\pi t)+\pi^{-1}\sin(\pi t)>0$ voor $0<t<1$, zie Figuur 3, en de som $\sum_\rho |\rho\zeta'(\rho)|^{-1}$ divergeert [43, Section 14.27], kan de som van de *coëfficiënten* van $\cos(\gamma\gamma-\psi_\gamma)$ in Stelling 2 willekeurig groot gemaakt worden door T maar groot genoeg te kiezen. Daaruit volgt dat als we een waarde van γ zouden kunnen vinden zodanig dat *alle* $\gamma\gamma-\psi_\gamma$ dichtbij gehele veelvouden van 2π liggen (zodat de waarden van $\cos(\gamma\gamma-\psi_\gamma)$ alle dicht bij 1 liggen), we de waarde van $h(\gamma,T)$ willekeurig groot zouden kunnen maken. Dit zou dan, als we een γ en een T zouden vinden waarvoor $|h(\gamma,T)|>1$, de weerlegging van het vermoeden van Mertens inhouden. Als de γ's lineair onafhankelijk zouden zijn over de rationale getallen dan zouden er volgens een Stelling van Kronecker [14, Theorem 442] voor elke $\epsilon>0$ gehele waarden van γ bestaan en gehele getallen m_γ waarvoor

$$|\gamma\gamma-\psi_\gamma-2\pi m_\gamma|<\epsilon$$

voor alle $\gamma\in(0,T)$. Dit zou betekenen dat $h(\gamma,T)$, en dus $M(x)/\sqrt{x}$, willekeurig groot gemaakt kan worden. Onder dezelfde aannamen kan afgeleid worden dat $M(x)/\sqrt{x}$ willekeurig groot aan de negatieve kant kan worden gemaakt. Er is geen goede reden bekend waarom de γ's *niet* lineair onafhankelijk zouden zijn over de rationale getallen. Bovengenoemd probleem staat bekend als *een inhomogeen Diophantisch approximatieprobleem*.

Met behulp van het genoemde roosterbasis-reductie-algoritme van Lenstra, Lenstra en Lovász (LLL) kon het bovengenoemde inhomogene Diophantische approximatieprobleem worden opgelost voor een veel groter aantal termen dan met oudere bekende benaderingsmethoden. Enkele experimenten vooraf wezen uit dat de kans op slagen groot was als in de som in (2) de eerste $2\,000$ nulpunten van $\zeta(s)$ zouden worden meegenomen. De 'prijs' die hiervoor betaald moest worden was dat de waarden van γ in de met LLL gevonden oplossing behoorlijk groot konden zijn, namelijk orde van grootte 10^{70}. Om voor zulke γ-waarden de som in (2) te berekenen was het nodig om de γ's uit te rekenen met een precisie van tenminste 75 decimalen (in de praktijk werd voor de zekerheid met 100 decimalen gerekend). De beste boven- en ondergrens die gevonden werden voor $\underline{m}$ en $\overline{m}$ waren, respectievelijk, $-1{,}009$ en $+1{,}06$, waarmee het vermoeden van Mertens dus was weerlegd.

In 2006 hebben Kotnik en Te Riele [19] de berekeningen van Odlyzko en Te Riele uit 1985 verbeterd tot reep. $-1{,}229$ en $+1{,}218$. Bovendien hebben ze de expliciete bovengrens van Pintz voor het kleinste getal waarvoor het vermoeden van Mertens onjuist is, verlaagd van $\exp(3{,}21\times10^{64})$ naar $\exp(1{,}59\times10^{40})$. Hierbij werkten zij in de som in (2) met $10\,000$ in plaats van met $2\,000$ nulpunten van $\zeta(s)$. Zie kader voor de bijbehorende waarden van γ.

In Figuur 4 wordt het typische gedrag van $M(e^y)/e^{y/2}$ (bovenste grafiek) vergeleken met het gedrag van $h(\gamma,\gamma_{10\,000})$ in de buurt van de $1{,}218$-piek (middelste grafiek) en dat in de buurt van de $-1{,}229$-piek (onderste grafiek). Merk de vier betrekkelijk grote negatieve pieken links en rechts van de $1{,}218$-piek op en de vier betrekkelijk grote positieve

pieken links en rechts van de $-1{,}229$-piek. Als we de onderste grafiek spiegelen ten opzichte van de horizontale as krijgen we een grafiek die sterk lijkt op de middelste grafiek. Dat kan verklaard worden uit het feit dat de twee functies die hier zijn geplot lineaire combinaties van cosinussen zijn waarvan de eerste 98 termen ongeveer gelijk zijn op basis van het gebruikte LLL-algoritme [19].

Referenties

1 R. Backlund, Sur les zéros de la fonction $\zeta(s)$ de Riemann, *C.R. Acad. Sci. Paris* 158 (1914), 1979–1982.

2 Alex van den Brandhof, Roland van der Veen, Jan van de Craats en Barry Koren,*De zeven grootste raadsels van de wiskunde*, Bert Bakker, 2012.

3 R.P. Brent, G.L. Cohen en H.J.J. te Riele, Improved techniques for lower bounds for odd perfect numbers, *Math. Comp.* 57 (1991), 857–868.

4 Stefania Cavallar, Bruce Dodson, Arjen K. Lenstra, Walter M. Lioen, Peter L. Montgomery, Brian Murphy, Herman J.J. te Riele, Karen Aardal, Jeff Gilchrist, Gérard Guillerm, Paul C. Leyland, Joël Marchand, François Morain, Alec Muffett, Chris Putnam, Craig Putnam, Paul Zimmermann, Factorization of a 512-bit RSA modulus, pp. 1–18 in: Bart Preneel (ed.), *Advances in Cryptology–EUROCRYPT 2000*, Lecture Notes in Computer Science, Vol. 1807, Springer, 2000.

5 Jingrun Chen en Tianze Wang, On the odd Goldbach problem, *Acta Math. Sinica* 32 (1989), 702–718.

6 Richard Crandall en Carl Pomerance, *Prime Numbers – A Computational Perspective*, Springer, 2001.

7 J.-M. Deshouillers, G. Effinger, H. te Riele en D. Zinoviev, A complete Vinogradov 3-primes theorem under the Riemann hypothesis, *Electr. Res. Ann. of the AMS* 3 (Sept. 17, 1997), 99–104.

8 J.-M. Deshouillers, H.J.J. te Riele en Y. Saouter, New experimental results concerning the Goldbach conjecture, pp. 204–215 in: J.P. Buhler (ed.), *Proc. of ANTS III, Portland, Oregon, USA, June 21â£"25*, Lecture Notes in Computer Science, Vol. 1423, Springer, 1998.

9 A.E. Ingham, On two conjectures in the theory of numbers, *Amer. J. Math.* 64 (1942), 313–319.

10 H.M. Edwards, *Riemann's Zeta Function*, Dover, New York, 2001 (herdruk van de uitgave van Academic Press, Inc. uit 1974).

11 M. García, J.M. Pedersen en H.J.J. te Riele, Amicable numbers – a Survey, pp. 179–197 in: Alf van der Poorten en Andreas Stein (eds.), *High primes and Misdemeanours: Lectures in Honour of the Sixtieth Birthday of Hugh Cowie Williams*, Fields Institute Communications 41, AMS, 2004.

12 GIMPS, http://www.mersenne.org.

13 Xavier Gourdon, The 10^{13} first zeros of the Riemann zeta function, and zeros computation at very large height, oktober 2004, http://numbers.computation.free.fr/ Constants/Miscellaneous/ zetazeros1e13-1e24.pdf.

14 G.H. Hardy en E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford at the Clarendon Press, Fourth Edition, 1975.

15 A.E. Ingham, *The Distribution of Prime Numbers*, Cambridge Mathematical Library, 1990 (herdruk van de uitgave van Cambridge University Press uit 1932, met een voorwoord door R.C. Vaughan).

16 W. Jurkat, A. Peyerimhoff, A constructive approach to Kronecker approximations and its application to the Mertens conjecture, *J. reine angew. Math.* 286/287 (1976), 332–340.

17 Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen Lenstra, Emmanuel Thomé, Joppe Bos, Pierrick Gaudry, Alexander Kruppa, Peter Montgomery, Dag Arne Osvik, Herman te Riele, Andrey Timofeev en Paul Zimmermann, Factorization of a 768-bit RSA modulus, pp. 333–350 in: T. Rabin (ed.), *Advances in Cryptology – CRYPTO 2010*, Lecture Notes in Computer Science, Vol. 6223, Springer, 2010.

18 Tadej Kotnik en Jan van de Lune, *Further systematic computations on the summatory function of the Möbius function*, CWI Report MAS-R0313, 2003.

19 Tadej Kotnik en Herman te Riele, The Mertens Conjecture Revisited, pp. 156–167 in: F. Hess, S. Pauli en M. Pohst (eds.), *Proc. of the Seventh Algorithmic Number Theory Symposium*, Lecture Notes in Computer Science, Vol. 4076, Springer, 2006.

20 M. Kraitchik, *Recherches sur la Théorie des Nombres*, Tome II, Factorisation, Gauthiers-Villars, Paris, 1929.

21 A. Lenstra en H. Lenstra, Jr., eds., *The Development of the Number Field Sieve*, Lecture Notes in Mathematics, Vol. 1554, Springer, 1993.

22 H. Lenstra, Jr., Factoring integers with elliptic curves, *Ann. of Math.* 126 (1987), 649–673.

23 A.K. Lenstra, H.W. Lenstra, Jr. en L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* 261 (1982), 515–534.

24 Mathematica, http://www.wolfram.com/mathematica.

25 F. Mertens, Über eine zahlentheoretische Funktion, *Sitzungsberichte Akad. Wien* 106, Abt. 2a (1897), 761–830.

26 David Moews, *A list of aliquot cycles of length greater than two*, http://djm.cc/sociable.txt.

27 M. Morrison en J. Brillhart, A method of factoring and the factorization of F_7, *Math. Comp.* 29 (1975), 183–205.

28 P.P. Nielsen, Odd perfect numbers have at least nine distinct prime factors. *Math. Comp.* 76 (2007), 2109–2126.

29 Pascal Ochem en Michaël Rao, Odd perfect numbers are greater than 10^{1500}, *Math. Comp.* 81 (2012), 1869–1877.

30 A.M. Odlyzko, The 10^{22}-nd zero of the Riemann zeta function, pp. 139–144 in: M. van Frankenhuysen en M.L. Lapidus (eds.), *Dynamical, Spectral, and Arithmetic Zeta Functions*, Amer. Math. Soc., Contemporary Math. Series, no. 290, 2001.

31 A.M. Odlyzko en H.J.J. te Riele, Disproof of the Mertens conjecture, *J. reine angew. Math.* 357 (1985), 138–160.

32 Thomas Oliveira e Silva, Siegfried Herzog en Silvio Pardi, Empirical verification of the even Goldbach conjecture, and computation of prime gaps, up to $4 \cdot 10^{18}$, *Math. Comp.*, to appear.

33 J.M. Pedersen, *Known Amicable Pairs*, http://amicable.homepage.dk/knwnap.htm.

34 J. Pintz, An effective disproof of the Mertens conjecture, *Astérisque* 147/148 (1987), 325–333.

35 J.M. Pollard, *Factoring with cubic integers*, pp. 4–10 in [21].

36 *PrimeGrid*, http://www.primegrid.com.

37 C. Pomerance, The quadratic sieve factoring algorithm, pp. 169–182 in: *Advances in Cryptology, Proc. Eurocrypt 1984*, Lecture Notes in Computer Science, Vol. 209, Springer, 1985.

38 C. Pomerance, Analysis and comparison of some integer factoring algorithms, pp. 89–139 in: H.W. Lenstra, Jr. en R. Tijdeman, eds., *Computational methods in number theory, Part I*, Math. Centre Tracts, Vol. 154, Mathematisch Centrum, Amsterdam, 1982.

39 C. Pomerance, Odd perfect numbers are divisible by at least seven distinct primes, *Acta Arithm.* 25 (1973/74), 265–300.

40 Bernhard Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Grösse, *Monatsberichte Königl. Preu. Akad. Wiss. Berlin* (1859), 671–680. Herdrukt in [10].

41 R. Rivest, A. Shamir en L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM* 21 (1978), 120–126.

42 C.L. Siegel, Über Riemanns Nachlass zur analytischen Zahlentheorie, *Quellen Studien zur Geschichte der Math. Astron. und Phys. Abt. B: Studien* 2 (1932), 45–80.

43 E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford, 1951.

44 Roland van der Veen en Jan van de Craats, *De Riemann-hypothese – een miljoenenprobleem*, Epsilon Uitgaven, Utrecht, 2011.

45 Sebastian Wedeniwski, http://www.zetagrid.net.