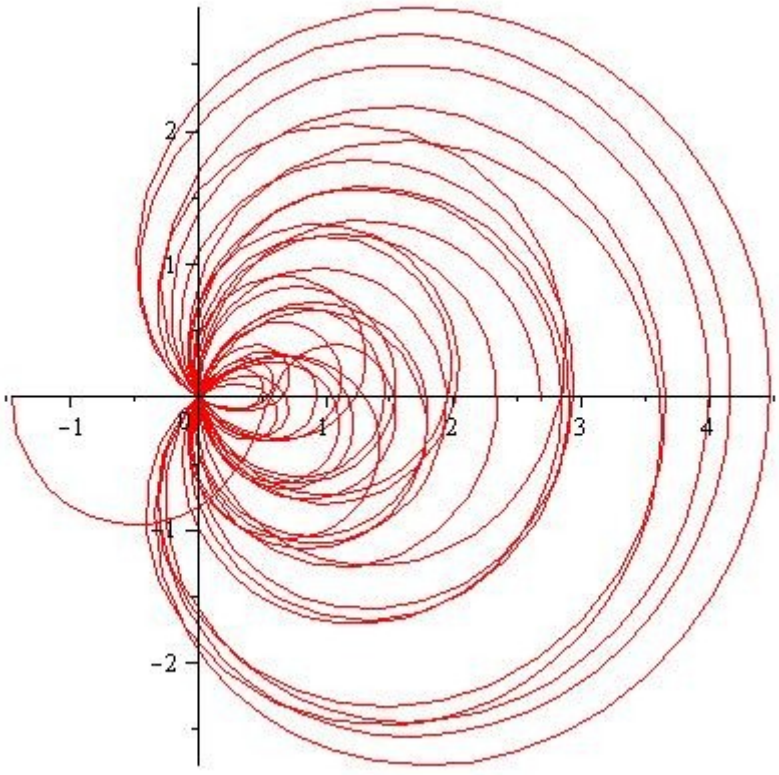
rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

# Over het tellen van priemgetallen.




Bacheloronderzoek Wiskunde

Juni 2010

Student: J.G. Mast

Begeleider: prof dr J. Top

## 1. Inleiding

Priemgetallen, de getallen die alleen deelbaar zijn door zichzelf en door het getal 1, fascineren al eeuwen wiskundigen. Zo kan het een vraag zijn hoeveel priemgetallen er zijn, zowel in het algemeen, onder een bepaalde grens of zelfs tussen twee grenzen. Op de eerste en tweede vraag wordt in deze scriptie ingegaan.
Euclides, bijvoorbeeld, heeft een manier gevonden om te laten zien dat er oneindig veel priemgetallen bestaan. Dit wordt bekeken in hoofdstuk 2, inclusief een paar verscherpingen.
Een voordehandliggende manier om priemgetallen onder een bepaalde grens te tellen, is, mits de grens klein genoeg is, alle getallen onder die bepaalde grens op te schrijven en getallen weg te strepen die veelvouden van priemgetallen zijn. De oude Griek Eratosthenes kwam op dit idee. Het is een leuk idee als de grens lekker klein is, maar bij een wat grotere grens is het op papier niet meer te doen. Dan is een andere oplossing nodig. Dit probleem bekijken we in hoofdstuk 3.
Het zou natuurlijk nog handiger zijn als er gewoon een formule zou bestaan die, zonder al te veel rekenwerk, een goede benadering vindt voor het aantal priemgetallen onder een bepaalde grens. Zo'n formule heeft Riemann bedacht en belichten we in hoofdstuk 4.
In hoofdstuk 5 passen we de formule van Riemann toe op het verschil tussen het aantal priemgetallen van de vorm $\pm 1 \bmod 4$ en op het verschill tussen het aantal priemgetallen van de vorm $\pm 1 \bmod 6$. Dan blijkt wat voor goede benadering de formule van Riemann is.
Hoofdstuk 6 wordt besteed aan conclusies.

## 2. Hoeveel priemgetallen zijn er?

Er zijn oneindig veel priemgetallen. Het simpelste bewijs is van Euclides: Neem het product van een aantal priemgetallen en tel er één bij op. Noem het resultaat $n$. Dit is niet deelbaar door een priemgetal dat net gebruikt is. Er zijn twee mogelijkheden: $n$ is priem, en dan hebben we er een nieuw priemgetal bij, of $n$ is niet priem. Bij de tweede mogelijkheid geldt dat als $n$ gefactoriseerd wordt, dit minstens één priemgetal oplevert en zo'n priemgetal is nog niet gebruikt. Zodoende is door het product van $k$ priemgetallen te nemen en er één bij op te tellen altijd een priemgetal te vinden dat niet in de gebruikte $k$ priemgetallen zit. Dus er zijn oneindig veel priemgetallen.
In dit hoofdstuk geven we een aantal verscherpingen van dit resultaat.

**Stelling 2.1.** *Er bestaan oneindig veel priemgetallen* $3 \bmod 4$.

Bewijs: er bestaan priemgetallen $3 \bmod 4$, zo heb je bijvoorbeeld 3 en 7, en ook 11 en 19.
Neem nu een $k$-tal verschillende priemgetallen $3 \bmod 4$: $\{p_1, p_2, \ldots, p_k\}$.
Noem het product van deze priemgetallen $n$, dus $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.
Kijk naar het getal $4n - 1$. Omdat dit getal $3 \bmod 4$ is, levert het factoriseren tenminste één priemgetal $q$ dat $3 \bmod 4$ is. Zo'n priemgetal $q$ is geen deler van $n$, want als dat wel het geval zou zijn, dan zou gelden dat $q|n$, dus ook $q|4n$.
We weten al dat $q|4n-1$, dus dat $q$ een deler is van $4n-1$. Maar $q$ kan natuurlijk niet twee opeenvolgende getallen delen.

Dus $q$ is een priemgetal 3 mod 4 en hij was nog niet gebruikt. Hieruit is te concluderen dat hoeveel priemgetallen 3 mod 4 er ook zijn, er altijd weer een nieuwe gevonden kan worden. Er zijn dus oneindig veel priemgetallen 3 mod 4.

□

Zo kan er ook gekeken worden naar alle priemgetallen die bij deling door vier rest één opleveren. Dit bewijs lijkt veel op het voorgaande bewijs, maar kan toch niet precies hetzelfde gedaan worden.

**Stelling 2.2.** *Er bestaan oneindig veel priemgetallen* 1 mod 4.

Bewijs: er bestaan priemgetallen 1 mod 4, bijvoorbeeld 5 en 13.
Neem een $k$-tal verschillende priemgetallen 1 mod 4: $\{p_1, p_2, \ldots, p_k\}$.
Noem het product van deze priemgetallen $n$, dus $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.
Kijk naar $n^2+1$. Factoriseren levert een priemgetal $q \neq 2$, dus $q|n^2+1$. Factoriseren levert ook een priemgetal $q = 2$, maar niet alleen priemgetallen $q = 2$. Dat komt door de vorm van $n$. Deze is namelijk $n \equiv 1 \bmod 4$. Waardoor: $n^2 \equiv 1 \bmod 4$ en dus $n^2 + 1 \equiv 2 \bmod 4$. Dus dat $q = 2$ ook een priemfactor is, is voordehandliggend, maar verder niet storend of relevant.
Voor $q$ geldt $q \notin \{p_1, p_2, \ldots, p_k\}$, want als $q$ wel in die verzameling zat, dan geldt $q|n^2$. Maar er gold al: $q|n^2 + 1$ en $q$ kan geen twee opeenvolgende getallen delen.

Het getal $n^2+1$ heeft de handige eigenschap dat al haar oneven priemdelers 1 mod 4 zijn. Het volgende lemma geeft het bewijs van deze uitspraak.
Dus $q \notin \{p_1, p_2, \ldots, p_k\}$ èn $q \equiv 1 \bmod 4$.
Conclusie: hoeveel priemgetallen 1 mod 4 je ook hebt, je kunt altijd weer een nieuwe vinden.

□

**Lemma 2.3.** *Stel $n$ is geheel, $f$ is positief en $p \neq 2$ is een priemdeler van $n^{2^{f-1}}+1$. Dan is $p \equiv 1 \bmod 2^f$.*

Bewijs: Gebruik de groep $(\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}$. Er moet bewezen worden dat $2^f$ een deler is van $\#(\mathbb{Z}/p\mathbb{Z})^*$. Gegeven is: $p|n^{2^{f-1}} + 1$, dat is te schrijven als:

$$n^{2^{f-1}} + 1 \equiv 0 \bmod p,$$

ofwel

$$n^{2^{f-1}} \equiv -1 \bmod p.$$

Dus $(n^{2^{f-1}})^2 = n^{2^f} \equiv 1 \bmod p$.
Hieruit volgt dat $\bar{n} = n \bmod p \in (\mathbb{Z}/p\mathbb{Z})^*$ en $\bar{n}^{2^f} = \bar{1}$.

In de groepentheorie bestaat er een handige stelling:
*Gegeven een groep $G$ en een element $x \in G$, als $x^n = e$, dan is $ord(x)|n$.*
De positieve delers van $2^f$ zijn: $\{1, 2, 2^2, 2^3, \ldots, 2^{f-1}, 2^f\}$.
Stel de orde van $n$ mod $p$ is $2^k$, met $0 \leq k \leq f - 1$.

$$-1 = \bar{n}^{2^{f-1}} = \bar{n}^{2^k \cdot 2^{f-k-1}} = (\bar{n}^{2^k})^{2^{f-k-1}} = \bar{1}^{2^{f-k-1}} = 1.$$

Tegenspraak.

Hieruit volgt dat: $orde(n \bmod p) = 2^f$.
Conclusie: $2^f$ deelt het aantal elementen van de groep, dus $2^f | p-1$, dwz:

$$p \equiv 1 \bmod 2^f.$$

□

**Stelling 2.4.** *Er bestaan oneindig veel priemgetallen* $1 \bmod 2^f$.

Bewijs: deze getallen bestaan, voorbeelden van $f = 2$ zijn 5 en 13, en van $f = 3$ zijn 17 en 41. Nog algemener gezegd: neem $m = 2^{2^{f-1}} + 1$. Dan is $m \geq 3$ en $m$ is oneven. Laat $p$ een priemdeler zijn van $m$. Dan is $p$ oneven, dus uit lemma 2.3 volgt $p \equiv 1 \bmod 2^f$.
Neem nu een $k$-tal verschillende priemgetallen $1 \bmod 2^f$: $\{p_1, p_2, \ldots, p_k\}$.
Noem het product van deze priemgetallen $n$, dus $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.
Kijk naar het getal $n^{2^{f-1}} + 1$.
Factoriseren levert een priemgetal $q \neq 2$, dus $q | n^{2^{f-1}} + 1$. Factoriseren levert niet uitsluitend priemgetallen $q = 2$, dit komt door de manier waarop $n$ samengesteld is. Deze is namelijk $n \equiv 1 \bmod 2^f$, waardoor $n^{2^{f-1}} \equiv 1 \bmod 2^f$ en zodoende $n^{2^{f-1}} + 1 \equiv 2 \bmod 2^f$. Dus $q = 2$ is een priemfactor, maar niet storend of relevant.
Voor $q$ geldt $q \notin \{p_1, p_2, \ldots, p_k\}$, want als $q$ wel in die verzameling zat, dan gold $q | n$, en ook $q | n^{2^{f-1}}$, dus:

$$n^{2^{f-1}} \equiv 0 \bmod q \Leftrightarrow n^{2^{f-1}} + 1 \equiv 1 \bmod q.$$

Maar er gold al:

$$q | n^{2^{f-1}} + 1 \Leftrightarrow n^{2^{f-1}} + 1 \equiv 0 \bmod q.$$

Hieruit volgt dat: $1 \bmod q \equiv 0 \bmod q$. Dit kan alleen maar als $q = 1$, maar $q$ is een priemgetal. Tegenspraak.
$n^{2^{f-1}} + 1$ heeft de handige eigenschap dat al haar priemdelers $1 \bmod 2^f$ zijn. Lemma 2.3 geeft het bewijs van deze uitspraak.

Dus $q \notin \{p_1, p_2, \ldots, p_k\}$ èn $q \equiv 1 \bmod 2^f$.
Conclusie: hoeveel priemgetallen $1 \bmod 2^f$ je ook hebt, je kunt altijd weer een nieuwe vinden.

□

**Stelling 2.5.** *Er bestaan oneindig veel priemgetallen* $5 \bmod 6$.

Bewijs: er zijn priemgetallen $5 \bmod 6$, bijvoorbeeld 5 en 11.
Neem nu een $k$-tal verschillende priemgetallen $5 \bmod 6$: $\{p_1, p_2, \ldots, p_k\}$.
Noem het product van deze priemgetallen $n$, dus $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.
Kijk naar het getal $6n - 1$. Omdat dit getal $5 \bmod 6$ is, levert het factoriseren tenminste één priemgetal $q$ dat $5 \bmod 6$ is. Een oneven priemgetal $\neq 3$ is of van de vorm $1 \bmod 6$ of $5 \bmod 6$. Het is vast te stellen dat $q$ geen deler is van $n$, als dit wel het geval zou zijn, dan geldt $q | n$, dus ook $q | 6n$. Maar $q$ kan natuurlijk geen twee opeenvolgende getallen delen.

Dus $q$ is een priemgetal $5 \bmod 6$ en hij was nog niet gebruikt. Hieruit is te concluderen dat hoeveel priemgetallen $5 \bmod 6$ er ook zijn, er altijd weer een nieuwe gevonden kan worden. Er zijn dus oneindig veel priemgetallen $5 \bmod 6$.

□

**Stelling 2.6.** *Er bestaan oneindig veel priemgetallen* 1 mod 6.

Bewijs: er bestaan priemgetallen 1 mod 6, bijvoorbeeld 7 en 13.
Neem een $k$-tal verschillende priemgetallen 1 mod 6: $\{p_1, p_2, \ldots, p_k\}$.
Noem het product van deze priemgetallen $n$, dus $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.
Kijk naar $n^2 + n + 1$. Factoriseren levert een priemgetal $q \neq 3$, dus $q|n^2 + n + 1$.
Voor $q$ geldt $q \notin \{p_1, p_2, \ldots, p_k\}$, want als $q$ wel in die verzameling zat, dan geldt $q|n^2 + n$ en $q$ kan geen twee opeenvolgende getallen delen.

Het getal $n^2 + n + 1$ heeft de handige eigenschap dat al haar priemdelers die niet 3 zijn, 1 mod 6 zijn.
Er geldt $n \equiv 1$ mod 6, dus $n$ mod $9 \in \{\bar{1}, \bar{4}, \bar{7}\}$ en daarom is $(n^2 + n + 1)$ mod $9 =$ 3 mod 9.
Dus $q \notin \{p_1, p_2, \ldots, p_k\}$ èn $q \equiv 1$ mod 6.
Conclusie: hoeveel priemgetallen 1 mod 6 je ook hebt, je kunt altijd weer een nieuwe vinden.

□

**Lemma 2.7.** *Stel $n$ is geheel en $p \neq 3$ is een priemdeler van $n^2 + n + 1$. Dan is $p \equiv 1$ mod 6.*

Bewijs: Gebruik de groep $(\mathbb{Z}/p\mathbb{Z})^* = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}$. Er moet bewezen worden dat 6 een deler is van $\#(\mathbb{Z}/p\mathbb{Z})^*$. Gegeven is dat $p|n^2 + n + 1$, dat is te schrijven als:

$$n^2 + n + 1 \equiv 0 \text{ mod } p,$$

ofwel

$$n^2 + n \equiv -1 \text{ mod } p \text{ en ook } n^2 \equiv -n - 1 \text{ mod } p.$$

Kijk nu naar $-\bar{n} = -n$ mod $p$. Er geldt

$$(-\bar{n})^3 = -\bar{n}^3 = -\bar{n}(-1 - \bar{n}) = \bar{n} + \bar{n}^2 \equiv -1 \text{ mod } p.$$

Hieruit volgt dat $-\bar{n} \in (\mathbb{Z}/pmathbbZ)^*$.
De orde van $-\bar{n}$ is dan een deler van 6, want

$$(-n)^6 = ((\overline{-n})3)2 = (\overline{-1} = \bar{1}.$$

De orde is geen deler van 3, want $(-\bar{n})^3 = \overline{-1} \neq \bar{1}$ omdat $p > 2$.
De orde is ook niet 2, want dan zou gelden $\overline{-n} = \overline{-1}$ en dus $\bar{n} = \bar{1}$, dus $\bar{3} = \bar{1}^2 + \bar{1} + \bar{1} = \bar{n}^2 + \bar{n} + 1 = \bar{0}$ en dat kan niet, omdat $p \neq 3$.

Hieruit volgt dat: $orde(-n \text{ mod } p) = 6$. Conclusie: 6 deelt het aantal elementen van de groep, dus $6|p - 1$, dwz:

$$p \equiv 1 \text{ mod } 6.$$

□

Het bewijs van de volgende stelling komt uit [1].

**Lemma 2.8.** *Als voor $a$ en $b$ geldt* $\text{ggd}(a, b) = 1$*, dan is elk oneven priemgetal dat deler is van $a^2 + b^2$ van de vorm* 1 mod 4.

Bewijs: Stel $p$ is priem en $p|a^2+b^2$. Dan is $p$ is geen deler van $a$, want:

$$p|a \Leftrightarrow p|a^2,$$

dus omdat ook $p|a^2+b^2$, volgt $p|b^2$, dus $p|b$.
Hieruit volgt dat $a \bmod p \in (\mathbb{Z}/p\mathbb{Z})^*$. Omdat $a$ en $b$ een gemeenschappelijke deler $p$ hebben, in tegenspraak met $\text{ggd}(a,b)=1$, $p|a^2+b^2$, volgt $b^2 \bmod p = -a^2 \bmod p$.

Neem $x := (b \bmod p)(a \bmod p)^{-1}$. Dan:

$$\begin{aligned} x^2 &= (b^2 \bmod p)(a^2 \bmod p)^{-1} \\ &= -(a^2 \bmod p)(a^2 \bmod p)^{-1} \\ &= \overline{-1}. \end{aligned}$$

Dus $x^4 = 1$, dus $\text{orde}(x) = 4$, als we aannemen dat $p \neq 2$ zodat $\overline{-1} \neq \bar{1}$. Dus in $(\mathbb{Z}/p\mathbb{Z})^*$ zit minstens één element van orde 4. Hieruit volgt dat $p$ van de vorm 1 mod 4 is.

□

**Stelling 2.9.** *Er bestaan oneindig veel priemgetallen* 5 mod 8.

Bewijs: er zijn priemgetallen 5 mod 8, bijvoorbeeld 5, 11 en 19.
Neem $n = (3^2 \cdot 5^2 \cdot 7^2 \cdot \ldots \cdot p^2) + 2^2$. Dit is dus het product van de kwadraten van alle oneven priemgetallen tot en met $p$, plus $2^2$, waarbij $p$ ook een priemgetal is. De termen hebben geen factor gemeen. Het kwadraat van een oneven getal $2m+1$ is $4m(m+1)+1$ en is 1 mod 8, zó dat $n \equiv 5 \bmod 8$.
Vanwege Lemma 2.8 en omdat $n$ oneven is, zijn alle priemgetallen van $n$ van de vorm 1 mod 4, dus modulo 8 zijn ze 1 of 5. Ze kunnen niet allemaal 1 mod 8 zijn, want dan was hun product $n$ dat ook. Dus $n$ heeft een priemfactor $q \equiv 5 \bmod 8$.
Factoriseren van $n$ levert dus tenminste één priemgetal $q$ dat 5 mod 8 is op. Deze $q$ is geen deler van $3^2 \cdot 5^2 \cdot 7^2 \cdot \ldots \cdot p^2$, want stel wel, dan zou $q$ een deler zijn van $n - 3^2 - \ldots - p^2 = 4$ zijn en dat kan niet. Dus $q$ is een nieuwgevonden priemgetal. En $q \equiv 5 \bmod 8$.
Conclusie: bij elke eindige verzameling priemgetallen is een nieuw priemgetal 5 mod 8 te vinden.

□

**Stelling 2.10.** *Er bestaan oneindig veel priemgetallen* 3 mod 8.

Bewijs: er bestaan priemgetallen 3 mod 8, bijvoorbeeld 3 en 11.
Neem nu een $k$-tal verschillende priemgetallen 3 mod 8: $\{p_1, p_2, \ldots, p_k\}$.
Noem het product van deze priemgetallen $n$, dus $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.
Kijk naar $n^2+2$. Factoriseren levert een priemgetal $q \neq 2$, dus $q|n^2+2$. Dit komt doordat $n$ oneven is, en daardoor ook $n^2+2$ oneven is.
Voor $q$ geldt $q \notin \{p_1, p_2, \ldots, p_k\}$, want $n^2 \equiv 2 \bmod q$, anders zou $q$ ook $2 = (n^2+2) - n^2$ delen.
Gebruikmakend Lemma 2.11, zijn de priemdelers van $n^2+2$ óf 1 mod 8, óf 3 mod 8. Ze kunnen niet allemaal 1 mod 8 zijn, want kun product is $n^2+2 \equiv 3 \bmod 8$ Dus moet er minstens één priemfactor 3 mod 8 in $n^2+2$ zitten.
Dus hoe groot $k$ ook genomen is, er is altijd wel weer een nieuw priemgetal 3 mod 8

te vinden.
Er zijn dus oneindig veel priemgetallen 3 mod 8.

□

**Lemma 2.11.** *Als $p$ priem is, en $n$ oneven en $p|n^2+2$, dan is $p \equiv 1 \bmod 8$ of $p \equiv 3 \bmod 8$.*

Bewijs: Het eerste deel van het lemma is ook te schrijven als: er is een $\alpha \in \mathbb{F}_p$ die voldoet aan $\alpha^2 = -2$. Verder is $n$ oneven, dus ook $n^2+2$ en $p$ zijn oneven.
De groep $\mathbb{F}_{p^2}^*$ is cyclisch en het aantal elementen van $\mathbb{F}_{p^2}^* = p^2 - 1 \equiv 0 \bmod 8$. Dus dan zit er een element van orde 8 in.
Neem $\zeta \in \mathbb{F}_{p^2}$ die orde 8 heeft, dan heeft $\zeta^4$ orde 2, dus $\zeta^4 = \overline{-1}$.
Dan $(\zeta - \zeta^{-1})^2 = \zeta^2 - \bar{2} + \zeta^{-2} = -\bar{2} + \zeta^{-2} \cdot (1 + \zeta^4) = -\bar{2}$.
Dus $(\zeta - \zeta^{-1}) = \pm\alpha$, dus $(\zeta - \zeta^{-1}) \in \mathbb{F}_p$, dus $(\zeta - \zeta^{-1})^p = \zeta - \zeta^{-1}$.
En ook $(\zeta - \zeta^{-1})^p = \zeta^p - \zeta^{-p}$.
Nu zijn er vier gevallen:

(1) $p \equiv 1 \bmod 8$ Dan is $\zeta^p = \zeta$. Dat kan.
(2) $p \equiv 3 \bmod 8$ Dan is $\zeta^p = \zeta^3$. Dus $\zeta^3 - \zeta^{-3} = \zeta - \zeta^{-1}$, dus volgt:
$$\begin{gathered}\zeta^3 - \zeta^{-3} = \zeta^1 - \zeta^{-1} \\ \Leftrightarrow \zeta^3 - \zeta^5 = \zeta - \zeta^7 \\ \Leftrightarrow -\zeta^5 - \zeta^7 = \zeta - \zeta^3 \\ \Leftrightarrow -\zeta^4(\zeta - \zeta^3) = \zeta - \zeta^3 \\ \Leftrightarrow -\zeta^4 = 1 \\ \Leftrightarrow \zeta^4 = -1.\end{gathered}$$
Dit klopt, immers orde$(\zeta) = 8$.
(3) $p \equiv 5 \bmod 8$ Dan is $\zeta^p = \zeta^5$. Dus $\zeta^5 - \zeta^{-5} = \zeta - \zeta^{-1}$, dus volgt:
$$\begin{gathered}\zeta^5 - \zeta^{-5} = \zeta - \zeta^{-1} \\ \Leftrightarrow \zeta^5 - \zeta^3 = \zeta - \zeta^7 \\ \Leftrightarrow \zeta^5 + \zeta^7 = \zeta + \zeta^3 \\ \Leftrightarrow \zeta^4(\zeta + \zeta^3) = \zeta + \zeta^3 \\ \Leftrightarrow \zeta^4 = 1.\end{gathered}$$
Dus orde$(\zeta) = 4$, dat is in tegenspraak met orde$(\zeta) = 8$, dus $p \not\equiv 5 \bmod 8$.
(4) $p \equiv 7 \bmod 8$ Dan is $\zeta^p = \zeta^7$. Dus $\zeta^7 - \zeta^{-7} = \zeta - \zeta^{-1}$, dus volgt:
$$\begin{gathered}\zeta^7 - \zeta^{-7} = \zeta - \zeta^{-1} \\ \Leftrightarrow \zeta^7 - \zeta = \zeta - \zeta^7 \\ \Leftrightarrow 2\zeta^7 = 2\zeta \\ \Leftrightarrow \zeta^6(2\zeta) = 2\zeta \\ \Leftrightarrow \zeta^6 = 1.\end{gathered}$$
Dus orde$(\zeta) = 6$, maar dit is in tegenspraak met orde$(\zeta) = 8$, dus $p \not\equiv 7 \bmod 8$.

Dus $p \equiv 1 \bmod 8$ of $p \equiv 3 \bmod 8$.

□

**Stelling 2.12.** *Er bestaan oneindig veel priemgetallen* 7 mod 8.

Bewijs: er bestaan priemgetallen 7 mod 8, bijvoorbeeld 7 en 23.
Neem nu een $k$-tal verschillende priemgetallen 7 mod 8: $\{p_1, p_2, \ldots, p_k\}$.
Noem het product van deze priemgetallen $n$, dus $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$.
Kijk naar $n^2 - 2$. Factoriseren levert een priemgetal $q \neq 2$, dus $q|n^2 - 2$. Dit komt doordat $n$ oneven is, en daardoor ook $n^2 - 2$ oneven is.
Voor $q$ geldt $q \notin \{p_1, p_2, \ldots, p_k\}$, anders zou $q$ een deler zijn van $n^2 - (n^2 - 2) = 2$.
Dus:

$$q|n^2 - 2 \Leftrightarrow n^2 - 2 \equiv 0 \bmod q.$$

Daarnaast, vanwege Lemma 2.13, zijn alle priemdelers van $n^2 - 2$ ofwel 1 mod 8, ofwel 7 mod 8. Ze kunnen niet allemaal 1 mod 8 zijn, want hun product $n^2 - 2$ is 7 mod 8. Dus er bestaat een priemdeler $q|n^2$ met $q \equiv 7 \bmod 8$.
Dus hoe groot $k$ ook genomen is, er is altijd wel weer een nieuw priemgetal 7 mod 8 te vinden. Er zijn dus oneindig veel priemgetallen 7 mod 8.

□

**Lemma 2.13.** *Als $p$ priem is, en $n$ oneven en $p|n^2 - 2$, dan is $p \equiv 1 \bmod 8$ of $p \equiv 7 \bmod 8$.*

Bewijs: Het eerste deel van het lemma is ook te schrijven als: er is een $\alpha \in \mathbb{F}_p$ die voldoet aan $\alpha^2 = 2$. Verder is $n$ oneven, dus ook $n^2 - 2$ en $p|n^2 - 2$ zijn even.
$\mathbb{F}^*_{p^2}$ is cyclisch en het aantal elementen van $\mathbb{F}^*_{p^2} = p^2 - 1 \equiv 0 \bmod 8$. Dus dan zit er een element van orde 8 in.
Neem $\zeta \in \mathbb{F}_{p^2}$ die orde 8 heeft, dan heeft $\zeta^4$ orde 2, dus $\zeta^4 = \overline{-1}$.
Dan $(\zeta + \zeta^{-1})^2 = \zeta^2 + \bar{2} + \zeta^{-2} = \bar{2} + \zeta^{-2} \cdot (1 + \zeta^4) = \bar{2}$.
Dus $(\zeta + \zeta^{-1}) = \pm\alpha$, dus $(\zeta + \zeta^{-1}) \in \mathbb{F}_p$, dus $(\zeta + \zeta^{-1})^p = \zeta + \zeta^{-1}$.
En ook $(\zeta + \zeta^{-1})^p = \zeta^p + \zeta^{-p}$.
Nu zijn er vier gevallen:

(1) $p \equiv 1 \bmod 8$ Dan is $\zeta^p = \zeta$. Dat kan.
(2) $p \equiv 3 \bmod 8$ Dan is $\zeta^p = \zeta^3$. Dus $\zeta^3 + \zeta^{-3} = \zeta + \zeta^{-1}$.

$$\begin{aligned} &\zeta^3 + \zeta^{-3} = \zeta + \zeta^{-1} \\ \Leftrightarrow\ &\zeta^3 + \zeta^5 = \zeta + \zeta^7 \\ \Leftrightarrow\ &\zeta^5 - \zeta^7 = \zeta - \zeta^3 \\ \Leftrightarrow\ &\zeta^4(\zeta - \zeta^3) = \zeta - \zeta^3 \\ \Leftrightarrow\ &\zeta^4 = 1. \end{aligned}$$

Dus orde$(\zeta) = 4$, dat is in tegenspraak met orde$(\zeta) = 8$, dus $p \not\equiv 3 \bmod 8$.
(3) $p \equiv 5 \bmod 8$ Dan is $\zeta^p = \zeta^5$. Dus $\zeta^5 + \zeta^{-5} = \zeta + \zeta^{-1}$. Hieruit volgt dezelfde tegenspraak als bij het geval $p \equiv 3 \bmod 8$, immers:

$$\zeta^5 + \zeta^{-5} = \zeta^5 + \zeta^3 = \zeta^3 + \zeta^{-3}.$$

Dus ook $p \not\equiv 5 \bmod 8$.
(4) $p \equiv 7 \bmod 8$ Dan is $\zeta^p = \zeta^7$. Dus $\zeta^7 + \zeta^{-7} = \zeta + \zeta^{-1}$.

$$\begin{aligned} &\zeta^7 + \zeta^{-7} = \zeta + \zeta^{-1} \\ &\zeta^7 + \zeta = \zeta + \zeta^7. \end{aligned}$$

Dat kan.

Dus $p \equiv 1 \bmod 8$ of $p \equiv 7 \bmod 8$.

□

**Stelling 2.14.** *Er bestaan oneindig veel priemgetallen* $1 \bmod 8$.

Bewijs: dit is stelling 2.4 met $f = 3$.

□

Nu volgt de algemene stelling waarvan we al een boel voorbeelden hebben gezien. Deze stelling is geformuleerd en gebruikt door Legendre en is bewezen door Dirichlet.

**Stelling 2.15.** *Laat* $a$ *en* $m$ *relatief priem zijn, met* $a, m \geq 1$. *Er bestaan oneindig veel priemgetallen* $p$ *zo dat* $p \equiv a(\mod m)$.

Het bewijs van deze stelling gaat te ver voor deze scriptie en is terug te vinden in hoofdstuk VI van [2]. In het bewijs wordt gebruik gemaakt van de eigenschappen van $L$-functies. Voorbeelden van zulke functies zien we in hoofdstuk 6 van dit onderzoek.

## 3. Priemgetallen tellen

Het aantal priemgetallen kleiner of gelijk aan de grens $x$ wordt $\pi(x)$ genoemd. Dit is ook te schrijven als:

$$\pi(x) := \{\#p \mid p \text{ is priem }, p \leq x\}$$

Om $\pi(x)$ te bepalen, ligt het voor de hand om, in het geval dat $x$ al te groot is, alle getallen die nietpriem zijn weg te strepen. Dit nog overzichtelijk voor bijvoorbeeld $x = 100$, dus alle getallen tot en met honderd op een papiertje schrijven en dan één voor één alle niet-priemgetallen wegstrepen, maar voor een wat grotere grens, zeg 10.000, gaat de lol er snel vanaf.
Het is dan handiger om de getallen te gaan zeven, zodat de priemgetallen overblijven. De oude Griek Eratosthenes vond een oplossing: je streept eerst alle even getallen weg, met uitzondering van het getal 2, hierbij heb je ongeveer $\frac{x}{2}$ wegstreepacties. Daarna alle drietallen, met uitzondering van het getal 3, hier ongeveer $\frac{x}{3}$ wegstreepacties. Zo ga je alle priemgetallen langs, zolang ze $\leq \sqrt{x}$ zijn. In totaal heb je dus ongeveer $\displaystyle\sum_{p \leq \sqrt{x}} \frac{x}{p} = x \sum_{p \leq \sqrt{x}} \frac{1}{p}$ wegstreepacties. De laatste som kun je schatten met behulp van partiële sommatie. Hoe dat werkt, zien we in hoofdstuk 4. In het bijzonder wordt daar (4.2) uitgelegd, dat $\displaystyle\sum_{p \leq \sqrt{x}} \frac{1}{p} \approx \log\log x$, als $x \to \infty$, dus in totaal doe je ongeveer $x \log\log x$ wegstreepacties. Deze methode heeft een nadeel: je streept veel getallen meer dan eens weg.
Legendre ([3], pagina 11 en 12) bedacht voor dit probleem een formule waardoor het aantal wegstreepacties verminderd wordt, al blijft het toch aardig bewerkelijk:

$$1 + \pi(x) = \pi(\sqrt{x}) + [x] - \sum_{p_i \leq \sqrt{x}} \left[\frac{x}{p_i}\right] + \sum_{p_i < p_j \leq \sqrt{x}} \left[\frac{x}{p_i p_j}\right] - \sum_{p_i < p_j < p_k \leq \sqrt{x}} \left[\frac{x}{p_i p_j p_k}\right] + \cdots$$

$[z]$ is het grootste gehele getal $\leq z$, dus het deel van $z$ voor de komma.
Wat de formule zegt is: 1 + het aantal priemgetallen = het aantal getallen − het

aantal samengestelde getallen in het interval $[2, x]$.
Met deze formule is met de hand $\pi(x)$ te bepalen en dit is ook goed te implementeren in een programma zoals Mathematica of Maple.

Nog specifieker zijn we geïnteresseerd in vergelijken van het aantal priemgetallen 1 mod 4 en 3 mod 4. Later vergelijken we ook de aantallen priemen 1 mod 6 en 5 mod 6. Om het probleem te illustreren is het handig om te kijken wat er op kleine schaal gebeurt, dus bij kleine priemgetallen. Mathematica en Maple hebben een ingebouwde functie die bepaalt hoeveel priemgetallen er onder een bepaalde grens zijn. Het enige wat dus nog gedaan moest worden, is een functie schrijven die uit die priemgetallen alle priemgetallen 3 mod 4 vist, of zeeft. In Mathematic ziet dat er zo uit:

```
Zeven[x_] := Module[{lijst, lengte},
  lijst = Table[4 k + 3, {k, 0, Floor[(x - 3)/4]}];
  For[i = 2, Prime[i] <= Sqrt[x], i++,
    If[Mod[Prime[i], 4] == 3,
     lijst =
      Complement[lijst,
       Table[Prime[i] (4 k + 1), {k, 1,
         Floor[(x - Prime[i])/(4*Prime[i])]}]],
     lijst =
      Complement[lijst,
       Table[Prime[i] (k + 3), {k, 1, Floor[(x - Prime[i])]}]]
     ]
    ]
   Print[Length[lijst]];
  (*Return[lijst]*)
  ]
```

Deze functie doet het volgende: de bovengrens, $x$, wordt meegegeven bij het aanroepen van de functie. Vervolgens wordt er een lijst aangemaakt met alle getallen 3 mod 4 $\leq x$. Daarna gaat de functie alle priemgetallen $\leq \sqrt{x}$ langs en haalt hij alle veelvouden van deze priemgetallen uit de lijst. Zodoende blijft er een lijst over met alle priemgetallen 3 mod 4 onder de bovengrens en het aantal priemgetallen in deze lijst wordt vervolgens afgedrukt.
Om het aantal priemgetallen 1 mod 4 te bepalen, hoef je alleen maar het resultaat van de bovenstaande functie van het totaal aantal priemgetallen af te trekken.
Zoals al opgemerkt wordt dit bewerkelijk bij grote getallen.
Een algemenere functie om priemgetallen $a$ mod $b$ te zeven is het volgende. Deze is geschreven in Maple.

```
piab:=proc(x::posint,a::posint,b::posint)
aantal:=0;
a0:=a mod b;
for i from a0 by b to floor(x/b)*b
     do
          if isprime(i)=true then aantal := aantal +1
          end if;
     end do;
print(aantal);
end proc;
```

Deze functie werkt, maar het is geen zeeffunctie. Het gaat gewoon elk getal $a$ mod $b$ na en als hij een priemgetal tegen komt, gaat de teller 1 omhoog. Daarnaast gaat hij echt elk getal van deze vorm langs en dat kan nogal veel tijd in beslag nemen als de $x$ groot is. Daarom de volgende twee functies. Het zijn beide zeeffuncties, maar hebben een andere insteek.
Beide functies beginnen met het maken van een lijst met $\lfloor \frac{x-a}{b} \rfloor$ elementen. En kijken naar de priemgetallen $p_i \leq \sqrt{x}$.
Het idee is dat je bekijkt welke veelvouden van de priemgetallen $p_i$ van de vorm $a$ mod $b$ zijn en $\leq x$ zijn. Die veelvouden worden 'weggestreept'. Je vindt ze als vvolgt. Er geldt

$$p_i | a + xb \Leftrightarrow xb \equiv -a \bmod p_i.$$

Is $p_i$ een deler van $b$, dan is dit niet mogelijk, want we nemen aan dat $\text{ggd}(a, b) = 1$. En als $p_i \not| b$, dan is $x \equiv -a(b \bmod p)$.
Het in het onderstaande programma wordt de informatie opgeslagen in een array. In een eerdere versie werd daarvoor een lijst gebruikt, maar ik de praktijk werkt de versie met arrays beter, omdat dan kennelijk efficienter met geheugen wordt omgegaan.

```
zeven:=proc(x::posint,a::posint,b::posint)
local lijst, grens, priem, i, j, t, k, p, strt, fin:
grens:=floor((x-a)/b):
lijst:=array(0..grens): for i from 0 to grens do lijst[i]:=1 end do:
priem:=pi(floor(sqrt(x)));
for j from 1 to priem do
      p:=ithprime(j):
      if evalb(p<=b) then
         if ((b mod p)<>0) then
             t:=(-a/b)mod p; if p=a+t*b then strt:=1 else strt:=0 end if:
             fin:=floor((grens-t)/p):
             for k from strt to fin
             do lijst[t+k*p]:=0: end do:
         end if;
      else
         t:=(-a/b)mod p; if p=a+t*b then strt:=1 else strt:=0 end if:
             fin:=floor((grens-t)/p):
             for k from strt to fin
             do lijst[t+k*p]:=0: end do:
      end if;
   end do;
if a=1 then strt:=1 else strt:=0 end if:
return add(lijst[i], i=strt..grens)
end proc;
```

Tot slot van dit hoofdstuk een tabel met rekentijden van Maple met de twee beschreven programma's. De tijden zijn afhankelijk van de computer waarop gerekend wordt en de versie van Maple, dus herhaling van de proef kan andere resultaten opleveren. Er is gekozen voor $a = 3$ en $b = 4$. Er is goed te zien dat *zeven* een stuk efficiënter is dan *paib*.

| $x$ | $10^6$ | $2 \cdot 10^6$ | $3 \cdot 10^6$ | $4 \cdot 10^6$ | $5 \cdot 10^6$ | $6 \cdot 10^6$ | $7 \cdot 10^6$ | $8 \cdot 10^6$ |
|---|---|---|---|---|---|---|---|---|
| piab | $5,8s$ | $35,8s$ | $46,9s$ | $132,2s$ | $188,5s$ | $254,4s$ | $320,9s$ | $405,8s$ |
| zeven | $3,7s$ | $11,3s$ | $22,9s$ | $38,4s$ | $56,0s$ | $77,5s$ | $104,2s$ | $136,2s$ |

## 4. Het benaderen van het aantal priemgetallen

Het precies uitrekenen van het aantal priemgetallen onder een grens neemt veel tijd in beslag als die grens maar een beetje groot wordt gekozen, zelfs al rekent een computer het uit. Daarom is het interessant om te onderzoeken of er een functie geconstrueerd kan worden die het aantal priemgetallen onder een bepaalde grens goed benaderd.
In 1859 kwam de wiskundige Riemann met een opmerkelijke manier om het aantal priemgetallen te benaderen, namelijk langs de weg van de complexe analyse. Hier volgt een versimpelde vorm van zijn methode. De sleutel van zijn methode is:

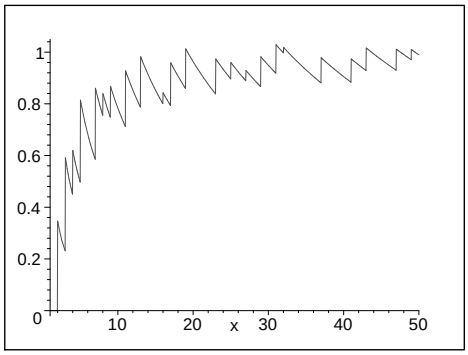
$$\text{kgv}[1, 2, 3, \cdots, x] \approx e^x \text{ als } x \to \infty$$

Dit verschijnsel is goed te illustreren met een paar voorbeelden.
De volgende twee figuren zijn beide een plot van de functie $\frac{\log(\text{kgv}[1,\ldots,n])}{\log(e^n)}$. Zoals, vooral in het eerste plaatje, goed te zien is, schokt de functie wat op en neer, maar blijf al snel rond de waarde 1 hangen. De uitschieters worden veroorzaakt doordat de teller op die plekken vermenigvuldigd wordt door een (redelijk) grote priem. Het werkt als volgt: de noemer wordt elke stap vermenigvuldigd met $e$. De teller wordt vermenigvuldigd met een priem $p$, alleen als $n$ een macht van $p$ is.

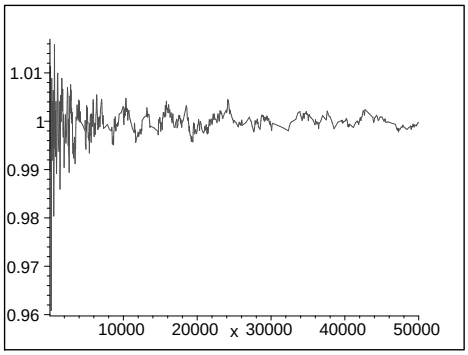
$$\text{kgv}[1, \ldots, n] = \prod_{\substack{p \text{ priem} \\ p \leq n}} p^{m_p},$$

waarbij $m_p$ het maximale gehele getal $m$ is met $p^m \leq n$, dus $m_p = \lfloor \frac{\log n}{\log p} \rfloor$.

De machten van 2 zorgen er niet voor dat de breuk groter wordt, al helpen ze wel de breuk niet heel veel kleiner te laten worden. Vanaf de machten van 3 wordt de breuk weer groter. Hieronder staan de twee grafiekjes van $\frac{\log(\text{kgv}[1,\ldots,n])}{x}$. Het is opvallend hoe snel de grafiek naar de waarde 1 toe gaat en daar blijft hangen. Het lijkt er dus op dat $e^x$ inderdaad een goede benadering is van $\text{kgv}[1, \cdots, x]$ als $x \to \infty$.




Het grafiekje van $1 \leq n \leq 50$.




Het grafiekje van $50 \leq n \leq 50000$.

De kgv$[1,2,3,\cdots,x]$ is ook anders te schrijven, namelijk:

$$(1) \qquad (\prod_{p\leq x} p)\times(\prod_{p^2\leq x} p)\times(\prod_{p^3\leq x} p)\times\cdots = \text{kgv}[1,2,3,\cdots,x],$$
$$\Leftrightarrow e^{\log((\prod_{p\leq x} p)\times(\prod_{p^2\leq x} p)\times(\prod_{p^3\leq x} p)\times\cdots)} = e^{\psi(x)},$$

waarbij

$$\psi(x) = (\sum_{p\leq x}\log p) + (\sum_{p^2\leq x}\log p) + (\sum_{p^3\leq x}\log p) + \ldots = \log \text{kgv}[1,\ldots,x].$$

Deze $\psi(x)$ is de Chebyshevfunctie.

We gebruiken hier een eigenschap van $\psi$ die we niet gaan bewijzen, namelijk dat $\lim_{x\to\infty}\frac{\psi(x)}{x} = 1$. Anders gezegd, $\psi(x)\approx x$ als $x\to\infty$. Voor het bewijs, zie [4], stelling 3 op pagina 13.

Eerder is al geformuleerd dat kgv$[1,2,3,\cdots,x]$ te schrijven is als een product van machten van priemgetallen, waarbij van elk priemgetal gekeken wordt wat z'n hoogste macht $\leq n$ is, en alleen die macht van het priemgetal wordt dan opgenomen in het product. Het linkerlid van (1) is het product van producten. De eerste factor is het product van alle priemgetallen $\leq n$. Bij de tweede factor wordt bekeken van welke priemgetallen het kwadraat $\leq n$ is, en de derde factor van welke de derde macht $\leq n$ is, enzovoort. Zo kom je ook op machten van priemgetallen uit, en wel precies die die ook al in de eerdere formulering gevonden waren. Nu wordt het rechterlid van (1) vervangen door $e^x$ en wordt aan beide kanten de logaritme genomen. Het resultaat is dan als volgt:

$$(\sum_{p\leq x}\log p) + (\sum_{p^2\leq x}\log p) + (\sum_{p^3\leq x}\log p) + \cdots \approx x \text{ als } x\to\infty.$$

Nu gaan we de Li$(x)$ beschouwen. Dit is de zogenaamde *logarithmische integraal*, bedacht door Gauss. Het is een belangrijk ingrediënt in de priemgetalstelling, een stelling die we nu buiten beschouwing laten. Li$(x)$ wordt gedefinieerd als:

$$\text{Li}(x) \overset{def}{=} \int_2^x \frac{dt}{\log t}.$$

Als deze integraal één keer partiëel geïntegreerd wordt, volgt het volgende resultaat:

$$\int_2^x \frac{dt}{\log t} = \left[\frac{t}{\log t}\right]_2^x + \int_2^x \frac{dt}{(\log t)^2}.$$

Nu gaan we eens kijken wat er gebeurt als $x\to\infty$. Het linkerlid en de integraal van het rechterlid blijven gelijk. Alleen in het eerste deel van het rechterlid verandert, immers:

$$\left[\frac{t}{\log t}\right]_2^x = \frac{x}{\log x} - \frac{2}{\log 2}.$$

De bijdrage van $\frac{2}{\log 2}$ als $x\to\infty$ is te verwaarlozen. Dus:

$$(2) \qquad \text{Li}(x) = \int_2^x \frac{dt}{\log t} \approx \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} \text{ als } x\to\infty.$$

Om deze benadering te kunnen koppelen aan de aanname die eerder gesteld is, namelijk $\psi(x)\approx x$ als $x\to\infty$, moet er partiëel gesommeerd worden. De manier

van partiëel sommeren die hier gebruikt wordt, komt uit [4], pagina 18, stelling A. De stelling luidt als volgt:

**Stelling 4.1.** *Gegeven twee rijen $(\lambda_n)_{n\geq 1}$ en $(c_n)_{n\geq 1}$ met $\lambda_j \in \mathbb{R}$ voor alle $j$ en $(\lambda_n)_{n\geq 1}$ een niet-dalende rij met $\lim_{n\to\infty} \lambda_n = \infty$. Verder $c_j \in \mathbb{C}$. Definiëer verder voor $x \in \mathbb{R}$:*

$$C(x) = \begin{cases} 0 & \text{als } x < \lambda_1, \\ \sum_{\{n|\lambda_n \leq x\}} c_n & \text{anders.} \end{cases}$$

*Neem een functie $\phi : [\lambda_1, \infty\} \to \mathbb{C}$ die continu differentiëerbaar is, en neem $X \in \mathbb{R}$ met $X \geq \lambda_1$.*
*Dan geldt*

$$\sum_{\{n|\lambda_n \leq X\}} c_n \phi(\lambda_n) = C(X)\phi(X) - \int_{\lambda_1}^{X} C(x)\phi'(x)dx. \tag{3}$$

*Is bovendien $\lim_{X\to\infty} C(X)\phi(X) = 0$, dan is*

$$\sum_{n=1}^{\infty} c(n)\phi(\lambda_n) = -\int_{\lambda_1}^{\infty} C(x)\phi'(x)dx$$

*mits ofwel de reeks $\sum_{n=1}^{\infty} c(n)\phi(\lambda_n)$, ofwel de oneigenlijke integraal $\int_{\lambda_1}^{\infty} C(x)\phi'(x)dx$ convergeert.*

We laten het (elementaire) bewijs voor deze stelling achterwege, zie daarvoor Ingham, bladzijde 19.

**Voorbeeld 4.2.** Als voorbeeld volgt het schatten van de som $x\sum_{p\leq\sqrt{x}} \frac{1}{p}$, hiernaar is verwezen in hoofdstuk 3, bij de zeefmethode van Eratosthenes. Voor het gemak kijken we naar de som $\sum_{p\leq\sqrt{x}} \frac{1}{p}$.
We kiezen als $\lambda_n$ het n$^{\text{de}}$ priemgetal. Daarnaast kiezen we $c_n = 1$ voor alle $n$, zodat

$$C(x) = \begin{cases} 0 & \text{als } x < 2, \\ \sum_{n|\lambda_n \leq x} c_n = \pi(x) & \text{anders.} \end{cases}$$

Tenslotte kiezen we $\phi(x) = \frac{1}{x}$ en $X = \sqrt{x}$. Nu kan de vergelijking (3) uit de stelling (4.1) ingevuld worden.

$$\sum_{p\leq\sqrt{x}} \frac{1}{p} = \sum_{\{n|\lambda_n \leq \sqrt{x}\}} c_n \phi(\lambda_n) = \frac{\pi(\sqrt{x})}{\sqrt{x}} + \int_2^{\sqrt{x}} \frac{\pi(t)}{t^2} dt \tag{4}$$

Nu bekijken we het rechterlid van (4) per term. Bij beide termen gebruiken we $\pi(x) \approx \frac{x}{\log x}$ als $x \gg 0$. Deze benadering volgt uit de priemgetalstelling. Eerst de eerste term:

$$\lim_{x\to\infty} \frac{\pi(\sqrt{x})}{\sqrt{x}} = \lim_{x\to\infty} \frac{1}{\log\sqrt{x}} = 0.$$

Nu de tweede term:

$$\int_2^{\sqrt{x}} \frac{\pi(t)}{t^2} dt \approx \int_2^{\sqrt{x}} \frac{t}{t^2 \log t} dt \approx \int_2^{\sqrt{x}} \frac{dt}{t \log t} = [\log\log t]_2^{t=\sqrt{x}}$$

$$= \log\log\sqrt{x} - \log\log\frac{1}{2} = \log\frac{1}{2}\log x + \log\log 2$$
$$= \log\log x - \log 2 + \log\log 2 \approx \log\log x.$$

Dus, samenvattend:

$$\sum_{p\leq\sqrt{x}} \frac{1}{p} \approx \log\log x \text{ en dus } x\sum_{p\leq\sqrt{x}} \frac{1}{p} \approx x\log\log x.$$

Einde voorbeeld.

Nu weer terug naar het verhaal. Het is nu zaak een handige $\phi(x)$, $\lambda_n$ en $c_n$ te kiezen. Neem $\phi(x) = \frac{1}{\log x}$, $\lambda_n = n$ en $c_n = \Lambda(n)$. De laatste term is als volgt gedefiniëerd:

$$\Lambda(n) \stackrel{\text{def}}{=} \begin{cases} \log p & \text{als } n = p^m \text{ met } m \in \mathbb{Z}_{>0}; \\ 0 & \text{anders.} \end{cases}$$

Deze $\Lambda$ heet de "von Mangoldt-functie".
Met deze keuze is het interessant om naar het linkerlid van (3) te kijken, we hebben $c_1 = 0$, dus:

$$\sum_{\lambda_n\leq X} c_n\phi(\lambda_n) = \sum_{2\leq n\leq X} \frac{\Lambda(n)}{\log n}$$
$$= \sum_{p^m\leq X} \frac{\log p}{m\cdot\log p} = \sum_{p^m\leq X} \frac{1}{m}$$
$$= \pi(X) + \frac{1}{2}\pi(X^{\frac{1}{2}}) + \frac{1}{3}\pi(X^{\frac{1}{3}}) + \ldots.$$

Het is handig om het volgende op te merken:

$$C(x) = \sum_{n\leq x} \Lambda(n) = \sum_{p^m\leq x} \log p =: \psi(x)$$

en dus $C(x)\phi(x) = \dfrac{\psi(x)}{\log(x)}$.

Als we de stelling toepassen, wordt het rechterlid van (3) het volgende:

$$C(X)\phi(X) - \int_{\lambda_1}^{X} C(x)\phi'(x)dx = \psi(X)\frac{1}{\log X} - \int_2^X \psi(x)\frac{-1}{x\log(x)^2}dx$$
$$= \psi(X)\frac{1}{\log X} + \int_2^X \psi(x)\frac{1}{x\log(x)^2}dx.$$

Het resultaat van het partiëel sommeren is dus het volgende:

$$\pi(x) + \frac{1}{2}\pi(x^{\frac{1}{2}}) + \frac{1}{3}\pi(x^{\frac{1}{3}}) + \ldots = \psi(X)\frac{1}{\log X} + \int_2^X \psi(x)\frac{1}{x\log(x)^2}dx.$$

Het rechterlid van deze vergelijking lijkt verdacht veel op (2), vooral als de $x$ vervangen wordt door $t$ en de $X$ vervangen wordt door $x$. Dus als de bovenstaande

vergelijking gecombineerd wordt met (2) en we de aanname gebruiken dat $\psi(x) \approx x$ als $x \to \infty$, dan gebeurt er het volgende:

$$\pi(x) + \frac{1}{2}\pi(x^{\frac{1}{2}}) + \frac{1}{3}\pi(x^{\frac{1}{3}}) + \ldots = \psi(x)\frac{1}{\log x} + \int_2^x \psi(t)\frac{1}{t\log(t)^2}dt$$

$$\approx \frac{x}{\log x} + \int_2^x \frac{dt}{(\log t)^2} \text{ als } x \to \infty.$$

$$\approx \mathrm{Li}(x) \text{ (zie de definitie).}$$

Omdat dit ongeveer $\mathrm{Li}(x)$ is, kom je op de onderstaande vergelijking:

$$\pi(x) + \frac{1}{2}\pi(x^{\frac{1}{2}}) + \frac{1}{3}\pi(x^{\frac{1}{3}}) + \ldots \approx \int_2^x \frac{dt}{\log t} = \mathrm{Li}(x).$$

Het linkerlid hier is precies de functie $J(x)$ die Riemann bedacht. Er staat dus, dat $J(x) \approx \mathrm{Li}(x)$.
Riemann liet, met behulp van de $J(x)$, ook een verband zien tussen $\zeta(s)$ en $\pi(x)$. Hier is $\zeta(s)$ is de zogenaamde *Riemann zeta-functie*, gedefiniëerd als:

$$\zeta(s) \stackrel{def}{=} \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots,$$

waarbij $s$ een complex getal is met $\Re(s) > 1$. Hieronder volgt een beschijving wat het verband is en hoe erop gekomen is.

**Lemma 4.3.** *Eulers productformule*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ priem}} \frac{1}{1-p^{-s}} \tag{5}$$

*voor* $\Re(s) = a > 1$.

Bewijs: Voor elk priemgetal $p$ en elke $s \in \mathbb{C}$ geldt

$$|p^{-s}| = |e^{-s\log p}| = e^{-\Re(s)\log p} = p^{-\Re(s)}$$

en $p^{-\Re(s)} < 1$ precies als $\Re(s) > 0$. Onder deze voorwaarde is dan

$$\frac{1}{1-p^{-s}} = 1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \ldots.$$

Er geldt absolute convergentie van de meetkundige reeks. Als we een product over een eindig aantal absoluut convergente reeksen nemen, is het product ook weer absoluut convergent en kunnen we de termen van deze reeks op welke volgorde dan ook zetten zonder dat som verandert. Neem een priemgetal $q$ en kijk naar de formule:

$$|\zeta(s) - \prod_{p \le q} \frac{1}{1-p^{-s}}| = |\sum \frac{1}{n^s}|,$$

waar in het rechterlid wordt gesommeerd over alle $n$ die minstens één priemdeler hebben die groter dan $q$ is. We kunnen de volgende afschatting maken voor dit rechterlid:

$$|\sum \frac{1}{n^s}| \le \sum_{n=q+1}^{\infty} |\frac{1}{n^s}| = \sum_{n=q+1} \frac{1}{n^{\Re(s)}} = \sum_{n=q+1}^{\infty} \frac{1}{n^a}$$

met $s = a + it$ en $a > 1$. Omdat $a > 1$, convergeert de reeks $\sum_{n\geq 1} \frac{1}{n^a}$, en omdat deze reeks convergeert, geldt

$$\lim_{q\to\infty} \sum_{n=q+1}^{\infty} \frac{1}{n^a} = 0$$

en daarom:

$$\lim_{q\to\infty} |\zeta(s) - \prod_{p\leq q} \frac{1}{1-p^{-s}}| = 0.$$

□

Vervolgens gebruiken we het rechterlid van Eulers productformule (5) om $\log \zeta(s)$ te herschijven:

$$\log \zeta(s) = \log \prod_p \frac{1}{1-p^{-s}} = -\sum_p \log(1-p^{-s}).$$

Voor $-\log(1-x)$ hebben we de Taylorreeks

$$-\log(1-x) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{1}{4}x^4 + \ldots,$$

die convergeert voor $|x| < 1$. Invullen $x = p^{-s}$ geeft nu:

$$\log \zeta(s) = \sum_p \sum_{n=1}^{\infty} n^{-1} p^{-ns}.$$

Hierin kunnen we de sommatievolgorde veranderen en dan gaat het er zo uitzien:

$$\log \zeta(s) = \sum_p p^{-s} + \frac{1}{2}\sum_p p^{-2s} + \frac{1}{3}\sum_p p^{-3s} + \ldots.$$

**Definitie 4.4.** *De indicatorfunctie* $1_{[a_1,a_2]}(x)$ *wordt gedefiniëerd als:*

$$1_{[a_1,a_2]}(x) := \begin{cases} 1 & \text{als } a_1 \leq x \leq a_2, \\ 0 & \text{elders.} \end{cases}$$

**Lemma 4.5.**

$$s\int_2^{\infty} 1_{[p^n,\infty)}(x) \cdot x^{-s-1} dx = s\int_{p^n}^{\infty} x^{-s-1} dx = p^{-ns}.$$

Bewijs: De eeste gelijkheid is triviaal, die volgt uit de definitie van de indicatorfunctie. $-x^{-s}$ is een primitieve van $sx^{-s-1}$. Nu is $\lim_{x\to\infty} x^{-s} = 0$ als $\Re(s) > 0$, dus heeft de integraal als uitkomst $(p^n)^{-s} = p^{-ns}$.

□

De $n$-de term in onze uitdrukking voor $\log \zeta(s)$ is $\frac{1}{n}\sum_p p^{-ns}$. Deze herschrijven we met bovenstaand lemma als

$$\frac{1}{n}\sum_p s\int_2^{\infty} 1_{[p^n,\infty)}(x) \cdot x^{-s-1} dx = s\int_2^{\infty} x^{-s-1}(\frac{1}{n}\sum_p 1_{[p^n,\infty)}(x))dx.$$

Merk op: voor een vaste $x \geq 2$ is

$$\frac{1}{n}\sum_p 1_{[p^n,\infty)}(x) = \frac{1}{n}\sum_{\substack{p \text{ priem} \\ \text{met } p^n \leq x}} 1 = \frac{1}{n}\pi(x^{\frac{1}{n}}).$$

Dus onze integraal is gelijk aan

$$s\int_2^\infty \frac{1}{n}\pi(x^{\frac{1}{n}})x^{-s-1}dx.$$

Alle termen samen geeft dan:

$$\begin{aligned}\log\zeta(s) &= \sum_{n=1}^{\infty} s\int_2^\infty \frac{1}{n}\pi(x^{\frac{1}{n}})x^{-s-1}dx\\ &= s\int_2^\infty \Big(\sum_{n=1}^{\infty}\frac{1}{n}\pi(x^{\frac{1}{n}})\Big)x^{-s-1}dx\\ &= s\sum_{2}^{\infty} J(x)\cdot x^{-s-1}dx\end{aligned}$$

Opmerking: we gaan hier niet verder in op de vraag waarom de diverse integratie- en sommatievolgordes verwisseld mogen worden, zie ook [5], hoofdstuk 3, §1.
Dus dan krijgen we het resultaat:

$$\frac{\log\zeta(s)}{s} = \int_2^\infty J(x)x^{-s-1}dx.$$

De volgende stap is om $\pi(x)$ te schrijven als functie van $J(x)$. We schrijven het resultaat als lemma dat we daarna meteen bewijzen.

**Definitie 4.6.** *De Möbiusfunctie wordt gedefiniëerd als:*

$$\mu(n) := \begin{cases} 1 & \textit{als } n=1,\\ (-1)^t & \textit{als } n = p_1\cdot\ldots\cdot p_t \textit{ allemaal verschillend,}\\ 0 & \textit{anders.}\end{cases}$$

**Lemma 4.7.**

$$\pi(x) = \sum_{n=1}^{\infty}\frac{\mu(n)}{n}J(x^{\frac{1}{n}})$$

Bewijs: een eigenschap van de Möbiusfunctie is:

$$\sum_{d|n}\mu(d) = \begin{cases} 1 & \text{als } n=1,\\ 0 & \text{elders.}\end{cases}$$

Voor een bewijs, zie hoofdstuk *XXII* van [6]. Dan krijgen we:

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{\mu(n)}{n}J(x^{\frac{1}{n}}) &= \sum_{n=1}^{\infty}(\frac{\mu(n)}{n}\sum_{m=1}^{\infty}\frac{\pi(x^{\frac{1}{mn}})}{m}) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{\mu(\frac{mn}{m})}{mn}\pi(x^{\frac{1}{mn}})\\ \overset{mn=t}{=}\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{\mu(\frac{t}{m})}{t}\pi(x^{\frac{1}{t}}) &= \sum_{t=1}^{\infty}\frac{\mu(\frac{t}{m})}{t}\pi(x^{\frac{1}{t}}) = \sum_{t=1}^{\infty}(\frac{\pi(x^{\frac{1}{t}})}{t}\sum_{d|t}\mu(d)) = \pi(x).\end{aligned}$$

□

Nu hebben we een verband tussen de $\zeta$-functie en de $\pi(x)$ via $J(x)$, want we zagen dat de logaritme van de $\zeta$-functie een soort Fouriergetransformeerde is van de functie $J(x)$ en ook $\pi(x)$ kunne we uitdrukken in $J(x)$. Hoewel de berekening wat te ver gaat voor deze scriptie, noteren we het resultaat:

$$\pi(x) = \frac{1}{2\pi i}\sum_{n=1}^{\infty}\frac{\mu(n)}{n}\int_{a-i\infty}^{a+i\infty}\frac{x^{\frac{s}{n}}}{s}\log\zeta(s)ds, \tag{6}$$

waarbij $a > 1$ vast en willekeurig gekozen mag worden.

Een dieper verband dat uit (6) volgt is onderstaande vergelijking. Het idee is dat je het tellen van priemgetallen ziet als een som van golven.

$$\frac{\mathrm{Li}(x) - \pi(x)}{\sqrt{x}/\log x} \approx 1 + 2 \sum_{\substack{\text{Alle reële getallen } \gamma>0 \\ \text{zodanig dat } \frac{1}{2}+i\gamma \\ \text{een nulpunt van } \zeta(s) \text{ is.}}} \frac{\sin(\gamma \log x)}{\gamma} \tag{7}$$

Het bewijs hiervoor gaat te ver voor deze scriptie.
De formule is ook te vinden in [7], maar ook dan zonder bewijs.

Er zijn een aantal zaken te vertellen over (7).

- Deze formule is nog niet bewezen. Het zou een gevolg zijn van de *Riemann hypothese* voor $\zeta(s)$, die beweert dat alle nulpunten van $\zeta(s)$ met $0 < \Re(s) < 1$ voldoen aan $\Re(s) = \frac{1}{2}$.
- Mocht de *Riemann hypothese* niet kloppen, dan is er toch een formule als boven, waarin dan ook de overige nulpunten van $\zeta(s)$ met $0 < \Re(s) < 1$ voorkomen.
- Als $\mathrm{Li}(x)$ en $\pi(x)$ voor kleine $x$ worden berekend, vind je altijd $\mathrm{Li}(x) > \pi(x)$. Maar met behulp van de formule (7) wist Littlewood al in 1914 dat ook $\mathrm{Li}(x) < \pi(x)$ voorkomt. Te Riele liet in 1986 zien dat dit moet gebeuren bij een $x$ van 371 decimale cijfers. Voor zo'n grote $x$ kan tegenwoordig nog niemand $\pi(x)$ bepalen.
- Omdat alle termen in (7) behalve $\pi(x)$ redelijk goed numeriek te benaderen zijn, is met de formule vrij goed te bepalen hoeveel $\pi(x)$ ongeveer is.

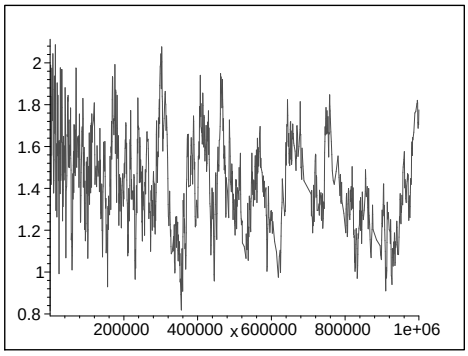
Hier volgen wat getallenvoorbeelden ter illustratie. De $\mathrm{Li}(x)$ is voor het gemak afgerond op een geheel getal, in werkelijkheid is het dat niet.

| $x$ | $\pi(x)$ | $\mathrm{Li}(x)$ | $\frac{\mathrm{Li}(x)-\pi(x)}{\sqrt{x}/\log(x)}$ | (*) mbv $10^2$ nulpunten | (*) mbv $10^3$ nulpunten | (*) mbv $10^4$ nulpunten |
|---|---|---|---|---|---|---|
| 10 | 4 | 5 | 0,8158 | 1,1040 | 1,1037 | 1,1020 |
| $10^2$ | 25 | 28 | 1,8794 | 1,4554 | 1,4211 | 1,4195 |
| $10^3$ | 168 | 177 | 1,8708 | 1,1374 | 1,0407 | 1,0500 |
| $10^4$ | 1229 | 1245 | 1,4821 | 0,7910 | 0,8011 | 0,8488 |
| $10^5$ | 9592 | 9629 | 1,3385 | 0,9204 | 0,8232 | 0,8224 |
| $10^6$ | 78498 | 78627 | 1,7754 | 1,3560 | 1,3709 | 1,4127 |
| $10^7$ | 664579 | 664917 | 1,7246 | 1,3374 | 1,4481 | 1,4570 |
| $10^8$ | 5761455 | 5762208 | 1,3876 | 1,2671 | 1,2195 | 1,1680 |

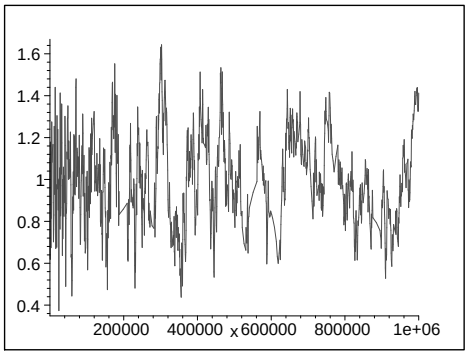
$(*) = 1 + 2 \sum_{\substack{\text{Alle reële getallen } \gamma>0 \\ \text{zodanig dat } \frac{1}{2}+i\gamma \\ \text{een nulpunt van } \zeta(s) \text{ is.}}} \frac{\sin(\gamma \log x)}{\gamma}$

Er vallen een aantal dingen op aan de bovenstaande tabel en de twee onderstaande grafiekjes. De vorm van de grafiekjes lijken sprekend op elkaar, maar de ene is verschoven van hoogte ten opzichte van de andere. Dit fenomeen is ook te zien in de tabel. Met meer nulpunten wordt de schatting nauwkeuriger, maar hij blijft toch een vaste afstand afwijken van het origineel. Hierdoor is met (7) een inschatting te maken waar de originele grafiek door de as gaat, maar moet je altijd rekening

houden met het feit dat de grafiek wat naar onderen is geschoven.
Hetzelfde gedrag is overigens ook te zien bij de grafieken in het volgende hoofdstuk.
Ik heb geen verklaring voor deze afwijking gevonden.




Dit is het linkerlid van (7).




Dit is het rechterlid van (7).

In de grafieken zie je het al eerde genoemde verschijnsel, namelijk dat $\mathrm{Li}(x) > \pi(x)$ voor heel veel $x$. Immers, de grafiek ligt boven de $x$-as. De reden waarom we weten dat $\mathrm{Li}(x) < \pi(x)$ voorkomt, is dat er heel grote $x$ zijn gevonden waarvoor de rechter grafiek onder de $x$-as komt.

## 5. Rekenen met priemen $a$ mod 4 en $a$ mod 6.

Analoog aan (7) kan je ook sommige andere functies dan $\mathrm{Li}(x)$ en $\pi(x)$ vergelijken. We gaan dat hier voor twee gevallen doen, namelijk voor $\pi_{-1,4}(x) - \pi_{1,4}(x)$, en voor $\pi_{-1,6}(x) - \pi_{1,6}(x)$. Hier is $\pi_{a,b}(x) := \#\{p \text{ priem} \mid p \equiv a \bmod b, p \leq x\}$.
Ook het rechterlid in (7) moet dan worden veranderd. In plaats van $\zeta(s)$ moet daar een complexe functie $\mathrm{L}_4(s)$ respectivelijk $\mathrm{L}_6(s)$ woren gebruikt.

**Definitie 5.1.**

$$\mathrm{L}_4(s) := \sum_{k=0}^{\infty} \left( \frac{1}{(4k+1)^s} - \frac{1}{(4k+3)^s} \right)$$

*en*

$$\mathrm{L}_6(s) := \sum_{k=0}^{\infty} \left( \frac{1}{(6k+1)^s} - \frac{1}{(6k+5)^s} \right).$$

Zodoende kom je op de volgende twee vergelijkingen:

$$\frac{\pi_{-1,4}(x) - \pi_{1,4}(x)}{\sqrt{x}/\log x} \approx 1 + 2 \sum_{\substack{\text{Alle reële getallen } \gamma>0 \\ \text{zodanig dat } \frac{1}{2}+i\gamma \\ \text{een nulpunt van } \mathrm{L}_4(s) \text{ is.}}} \frac{\sin(\gamma \log x)}{\gamma} \tag{8}$$

en

$$\frac{\pi_{-1,6}(x) - \pi_{1,6}(x)}{\sqrt{x}/\log x} \approx 1 + 2 \sum_{\substack{\text{Alle reële getallen } \gamma>0 \\ \text{zodanig dat } \frac{1}{2}+i\gamma \\ \text{een nulpunt van } \mathrm{L}_6(s) \text{ is.}}} \frac{\sin(\gamma \log x)}{\gamma}. \tag{9}$$

De functies $L_4$ en $L_6$ zijn voorbeelden van Dirichlet L-functies.
Een Dirichlet L-functie kan als volgt geconstrueerd worden: men neme de groep $(\mathbb{Z}/b\mathbb{Z})^*$. En een homomorfie $\chi$ van $(\mathbb{Z}/b\mathbb{Z})^*$ naar de vermenigvuldigingsgroep $\mathbb{C}^*$.

$$\chi : (\mathbb{Z}/b\mathbb{Z})^* \to \mathbb{C}^*$$

Maak vervolgens met $\chi$ een afbeelding.

$$\tilde{\chi} : \mathbb{Z} \to \mathbb{C} \text{ door}$$
$$n \mapsto \begin{cases} \chi(n \bmod b) & \text{als } \gcd(n,b) = 1, \\ 0 & \text{anders.} \end{cases}$$

De Dirichlet L-functie wordt als volgt geconstrueerd:

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\tilde{\chi}(n)}{n^s}.$$

**Voorbeeld 5.2.** Ter illustratie het voorbeeld $b = 4$.
$(\mathbb{Z}/4\mathbb{Z})^* = \{\overline{1}, \overline{3}\}$. Er is dus maar één niet-triviale keuze mogelijk voor $\chi$, namelijk:

$$\chi : \overline{1} \mapsto 1,$$
$$\overline{3} \mapsto -1.$$

Dit levert $L_4$. Want oneven getallen zijn te schrijven als $2n + 1$, waarbij $n \in \mathbb{N}$, zodoende is $\tilde{\chi}(2n + 1) = (-1)^n$. Dus:

$$L_4(s) = L_4(\chi, s) = \sum_{n=0}^{\infty} \frac{\tilde{\chi}(2n+1)}{(2n+1)^s} = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)^s}.$$

$$= \sum_{n=0}^{\infty} \left( \frac{1}{(4k+1)^s} - \frac{1}{(4k+3)^s} \right)$$

**Voorbeeld 5.3.** Een andere illustratie is het voorbeeld $b = 4$.
We kijken hier naar het product

$$\prod_{p>3} \frac{1}{1 - \chi(p)p^{-s}} = \sum_{m=1}^{\infty} \frac{\chi(2m-1)}{(2m-1)^s}.$$

$(\mathbb{Z}/6\mathbb{Z})^* = \{\overline{1}, \overline{5}\}$. Er is dus maar één niet-triviale keuze mogelijk voor $\chi$, namelijk:

$$\chi : \overline{1} \mapsto 1,$$
$$\overline{5} \mapsto -1.$$

Als we nu de som invullen, krijgen we:

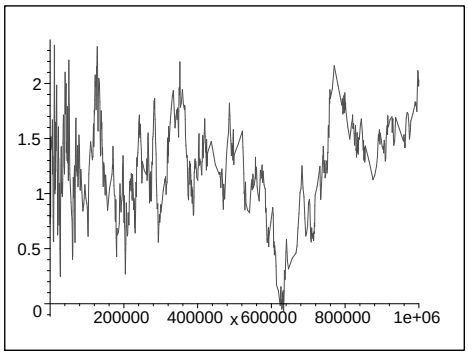
$$L_6(s) = 1 - \frac{1}{5^s} + \frac{1}{7^s} - \frac{1}{11^s} + \frac{1}{13^s} - \dots$$

$$= \sum_{k=0}^{\infty} \left( \frac{1}{(6k+1)^s} - \frac{1}{(6k+5)^s} \right).$$

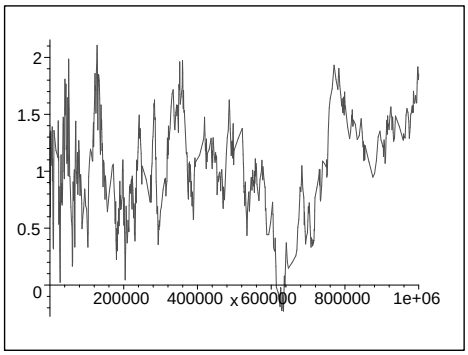
Dirichlet L-functies worden gebruikt in de stelling dat als $\text{ggd}(a,b)=1$, dan zijn er oneindig veel priemen $a$ mod $b$; zie [2].
Om met (8) en (9) te kunnen rekenen, zijn er nulpunten van $\mathrm{L}_b(s)$ nodig. En om het rechterlid aardig precies te maken zijn er veel nulpunten nodig. Wiskundeprogramma's zoals Maple en Mathematica hebben wel functies om nulpunten te bepalen maar het resultaat is dan één nulpunt per keer. Dus is het handiger om zelf maar een functie te schrijven om een heleboel nulpunten te kunnen bepalen. Dit is gedaan in Mathematica, aangezien Maple niet mee wilde werken als er iets met een $\zeta$-functie of een $\zeta$-achtige functie, zoals de Dirichlet L-functie moet worden gedaan.

| $x$ | $\pi_{3,4}(x)$ | $\pi_{1,4}(x)$ | $\frac{\pi_{3,4}(x)-\pi_{1,4}(x)}{\sqrt{x}/\log(x)}$ | (*) mbv $10^2$ nulpunten | (*) mbv $10^3$ nulpunten | (*) mbv $10^4$ nulpunten |
|---|---|---|---|---|---|---|
| 10 | 2 | 1 | 0,7281 | 0,8773 | 0,8828 | 0,8829 |
| $10^2$ | 13 | 11 | 0,9210 | 0,9648 | 0,9692 | 0,9708 |
| $10^3$ | 87 | 80 | 1,5291 | 1,3281 | 1,2614 | 1,2709 |
| $10^4$ | 619 | 609 | 0,9210 | 0,7174 | 0,6956 | 0,6751 |
| $10^5$ | 4808 | 4783 | 0,9102 | 0,6772 | 0,6284 | 0,6533 |
| $10^6$ | 39322 | 39175 | 2,0309 | 1,7275 | 1,8345 | 1,8527 |
| $10^7$ | 332398 | 332180 | 1,1111 | 1,2076 | 1,1400 | 1,0028 |
| $10^8$ | 2880950 | 2880504 | 0,8216 | 0,6682 | 0,62164 | 0,6377 |

$$(*) = 1 + 2\sum_{\substack{\text{Alle reële getallen } \gamma>0 \\ \text{zodanig dat } \frac{1}{2}+i\gamma \\ \text{een nulpunt van } \mathrm{L}_4(s) \text{ is.}}} \frac{\sin(\gamma \log x)}{\gamma}$$

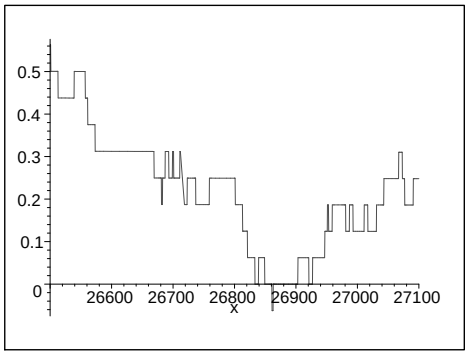



Dit is het linkerlid met $\mathrm{L}_4$.

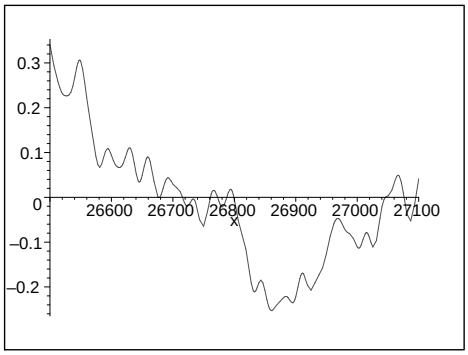



Dit is het rechterlid met $\mathrm{L}_4$.

Een extra illustratie is de plek waar voor de kleinste $x$ er meer priemgetallen 1 mod 4 dan 3 mod 4 zijn. Om precies te zijn: er geldt $\pi_{1,4}(26861) = 1473 > 1472 = \pi_{3,4}(26861)$. Ook hier valt de verschuiving op, maar er is duidelijk te zien dat beide grafieken ruwweg dezelfde vorm hebben.



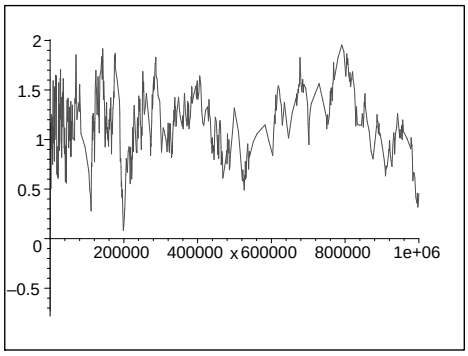

Dit is het linkerlid met $L_4$.



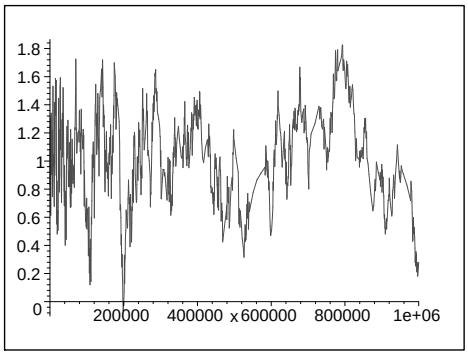

Dit is het rechterlid met $L_4$.

| $x$ | $\pi_{5,6}(x)$ | $\pi_{1,6}(x)$ | $\frac{\pi_{5,6}(x)-\pi_{1,6}(x)}{\sqrt{x}/\log(x)}$ | (*) mbv $10^2$ nulpunten | (*) mbv $10^3$ nulpunten | (*) mbv $10^4$ nulpunten |
|---|---|---|---|---|---|---|
| 10 | 1 | 1 | 0 | $0,8363$ | $0,8288$ | $0,8280$ |
| $10^2$ | 12 | 11 | $0,4605$ | $0,8061$ | $0,7835$ | $0,7736$ |
| $10^3$ | 86 | 80 | $1,3107$ | $1,3078$ | $1,1683$ | $1,1966$ |
| $10^4$ | 616 | 611 | $0,4605$ | $0,4068$ | $0,3184$ | $0,3404$ |
| $10^5$ | 4806 | 4784 | $0,8010$ | $0,5775$ | $0,6148$ | $0,5737$ |
| $10^6$ | 39265 | 39231 | $0,4697$ | $0,1924$ | $0,2700$ | $0,2806$ |
| $10^7$ | 332383 | 332195 | $0,9633$ | $0,8293$ | $0,8628$ | $0,8245$ |
| $10^8$ | 2880936 | 2880517 | $2,1356$ | $0,6710$ | $0,5727$ | $0,5937$ |

$$(*) = 1 + 2\sum_{\substack{\text{Alle reële getallen } \gamma>0 \\ \text{zodanig dat } \frac{1}{2}+i\gamma \\ \text{een nulpunt van } L_6(s) \text{ is.}}} \frac{\sin(\gamma \log x)}{\gamma}$$




Dit is het linkerlid met $L_6$.

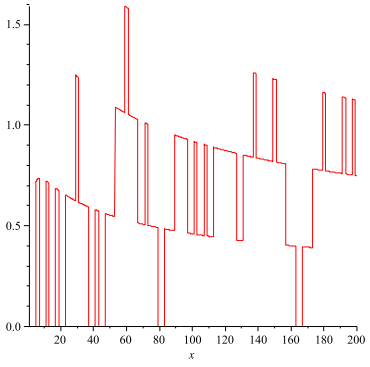



Dit is het rechterlid met $L_6$.

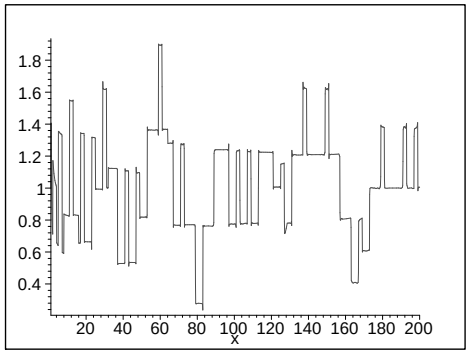
Ook hieronder een detail van de bovenstaande grafieken, met het verschil dat dit keer niet is gekozen voor de kleinste $x$ waar er meer priemgetallen 1 mod 6 zijn dan 5 mod 6, maar voor het beginstuk van de bovenstaande beide grafieken. Even rekenen met Maple leverde namelijk, dat $\pi_{5,6}(x) \geq \pi_{1,6}(x)$ als $x < 10^8$.

In eerste instantie heb ik zelf de nulpunten van $L_4$ en $L_6$ bepaald. De eerste functie waarvoor dat gedaan werd, was $L_4$.

```
L[s_] := Sum[(-1)^(k - 1)*(2 k - 1)^(-1/2 - I*s), {k, 1, Infinity}]
```




Dit is het linkerlid met $L_6$.

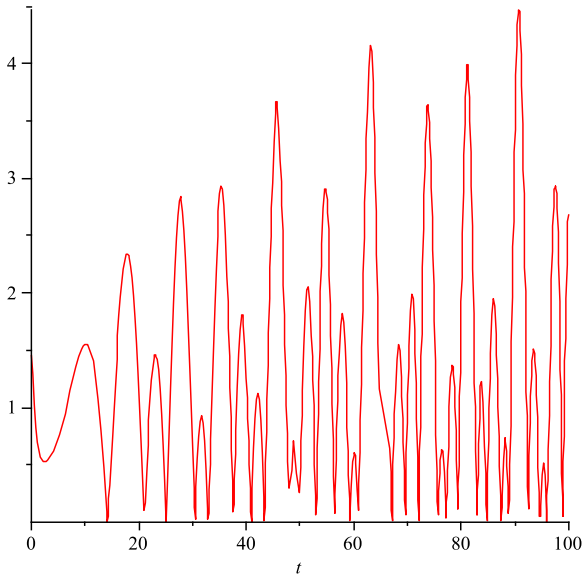



Dit is het rechterlid met $L_6$.

De $s$ in bovenstaande functie is $\gamma$, dus het nulpunt waarnaar we op zoek zijn. Zoals de lezer wellicht opgevallen is, is dit een Mathematicacode. Mathematica heeft een ingebouwde functie om nulpunten te vinden:

```
FindRoot[f, {x, x0}]
```

Deze functie zoekt een numeriek nulpunt van $f$, beginnend bij het punt $x = x_0$. Een nadeel van deze standaardfunctie is dat als je te ver van het nulpunt af zit, de kans bestaat dat de functie een extremum terug geeft van de meegegeven functie. Een ander nadeel is, dat er zo maar één nulpunt gevonden wordt, tewijl we bij de eerste plaatjes die we tekenden duizend nulpunten wilden hebben. Het is te veel werk om een grafiek van $L_4$ te tekenen, daaruit duizend verschillende plekken af te lezen waar de functie dicht bij in de buurt door de $x$-as gaat en die punten één voor één in de functie van mathematica te stoppen.




Grafiek van $\left|\zeta(\frac{1}{2} + it)\right|$.

Het is handiger om een functie te ontwerpen die dat doet. Het resultaat is dit:

```
Nulpunten[ondergrens_, bovengrens_] :=
 Module[{lijst, hulp},
  lijst = {};
  hulp = 0;
  For[n = ondergrens, n <= bovengrens, n++,
   Print[n];
   hulp = m /. FindRoot[L[m] == 0, {m, n}];
   (*Print[hulp];*)
   hulp = Round[hulp, .0001];
   If[MemberQ[lijst, hulp] == False && Head[hulp] == Real,
    lijst = Join[lijst, {hulp}];
    ]
   ];
  Print[Length[lijst]];
  Return[lijst];
  ]
```

Deze functie roept de *FindRoot*functie van Mathematica aan voor elke combinatie van een geheel getal $n$ en de functie $L_4$, waarbij ondergrens $\leq n \leq$ bovengrens. Vervolgens wordt het resultaat afgerond en wordt gekeken of het een reëel getal is. Immers, we zoeken een nulpunt $\gamma$ van een complexe functie, dus zo'n nulpunt heeft de eigenschap $\Im(\gamma) = 0$. In het geval dat het resultaat reëel is, wordt het toegevoegd aan de lijst van nulpunten, genaamd *lijst*. Mocht *FindRoot* een complex getal opleveren, dan is dat een extremum van onze $L_4$ en wordt er niks gedaan met dit resultaat. Tot slot wordt de gehele lijst met nulpunten teruggegeven.
Opmerking: er staan twee *Print*commando's in. De eerste print $n$, zodat in één oogopslag gezien kan worden hoe ver het programmaatje is en in het geval van een te lange berekening bij een specifieke $n$, de invoer aangepast kan worden, zodat deze specifieke $n$ vermeden kan worden. De andere print het aantal nulpunten dat in totaal gevonden is. Dit kan handig zijn als naar er een specifiek aantal nulpunten gezocht wordt.
Een andere opmerking: de functie in *FindRoot*, *L[m]*, kan vervangen worden door een andere functie, zodat met dit programmaatje ook nulpunten voor de zetafunctie en $L_6$ kunnen worden bepaald.

Zoals al in het begin van dit hoofdstuk vermeld is, is in eerste instantie gewerkt met eigenhandig gevonden nulpunten. Om deze nulpunten te verifiëren, is op internet gezocht naar databases met nulpunten van de drie functies die we beschouwen. Deze databases zijn gevonden. Het bleek dat met het programmaatje dat hierboven beschreven is dezelfde nulpunten gevonden kunnen worden als die in de databases staan, alleen zijn ze minder nauwkeurig door de afronding van slechts vier cijfers achter de komma. Om deze reden is gekozen om bij het tekenen van de plaatjes in dit en in het vorige hoofdstuk gebruik te maken van de nulpunten in de databases. Met als extra reden dat er in de gevonden databases per functie tienduizend nulpunten voorhanden zijn en het minder tijd kost deze nulpunten te gebruiken dan om tienduizend nulpunten met ons programmaatje te bepalen, gezien het feit dat het geen snel programma is.
Deze nulpunten zijn te vinden op de webside [8] van Tomás Oliveira e Silva.

## 6. Conclusies

In hoofstuk twee van deze scriptie hebben we bewezen dat er oneindig veel priemgetallen van de vormen 1 mod 4, 3 mod 4, 1 mod 6, 5 mod 6, 1 mod 8, 3 mod 8, 5 mod 8, 7 mod 8 en 1 mod $2^f$ zijn.

Maple en Mathematica hebben functies om priemgetallen (onder een bepaalde grens) te tellen. Om priemgetallen van een speciaal soort te kunnen tellen, moeten er zelf functies geschreven worden. Dat wordt in dit onderzoek gedaan voor het tellen van priemgetallen van de vorm 3 mod 4 en de algemene vorm $a$ mod $b$.

We hebben vervolgens laten zien hoe een versie van 'partiëel sommeren' en het feit dat $\text{kgv}(1,\ldots,n) \sim e^n$ voor $n \to \infty$ leiden tot een verband tussen het aantal priemgetallen onder een grens $x$, en de integraal $\int_2^\infty \frac{dt}{\log(t)}$. Dit wordt door numerieke voorbeelden mooi geïllustreerd.

Tenslotte hebben we gekeken of we de formule van Riemann ook konden gebruiken om te kunnen voorspellen onder welke grens er meer priemgetallen van de vorm 1 mod 4 zijn dan van de vorm 3 mod 4 en wanneer er meer priemgetallen van de vorm 1 mod 6 zijn dan van de vorm 5 mod 6. Dit bleek heel goed mogelijk.
Hierbij heb ik in eerste instantie gebruik gemaakt van, door mijzelf met behulp van Mathematica berekende, nulpunten van de Riemann zeta-functie en van zekere Dirichlet L-functies. Later heb ik dit ook gedaan met datebases vol nulpunten die beschikbaar zijn op [8].

## Referenties


[1] G.H. Hardy en E.M. Wright, An Introduction to the Theory of Numbers,plaats: uitgever, Oxford: Clarendon Press, 1945.

[2] Jean-Pierre Serre, A Course in Arithmetic, New York: Springer-Verlag, 1973.

[3] Hans Riesel, Prime Numbers and Computer Methods for Factorization, Boston: Birkhäuser, 1985.

[4] A.E. Ingham, The Distribution of Prime Numbers, New York:Hafner Publishing Company, 1971.

[5] Pieter Leopold, On Methods for Computing pi(x), Masterscriptie, Augustus 2007.
`http://scripties.fwn.eldoc.ub.rug.nl/FILES/scripties/Wiskunde/Masters/2007/Leopold.R.P./Pieter_Leopold_doctoraal.pdf`

[6] Joe Roberts, Elementary Number Theory, Cambridge: MIT-press, 1977.

[7] Andrew Granvill, Greg Martin, Prime Number Races, The American Mathematica Monthly, vol. 113, (2006), pp. 1-33.
`http://mathdl.maa.org/images/upload_library/22/Ford/granville1.pdf`

[8] `http://www.ieeta.pt/~tos/zeta.html`