Asymptotisch exacte heuristiek voor priemdelers van de reeks $\{a^k + b^k\}_{k=0}^{\infty}$

Szczepan Kowalczyk en Gerben Schooneveldt
Begeleider: Dr. Pieter Moree

Korteweg-de Vries Instituut voor Wiskunde
Universiteit van Amsterdam

7 maart 2004

Samenvatting

Dit artikel gaat over een onderwerp uit de getaltheorie. Het is onze bedoeling geweest om het ook voor de beginnende wiskunde student leesbaar en begrijpelijk te maken.

Laat $N_{a,b}(x)$ het aantal priemen $p \leq x$ zijn, zó, dat p een deler is van $(a^k + b^k)$ voor zekere $k \geq 0$. Het is bekend dat $N_{a,b}(x) \sim c(a,b)\, x/\log x$, met $c(a,b)$ een rationaal getal dat afhangt van a en b. We bekijken een heuristische formule voor $N_{a,b}(x)$. Verder controleren we deze heuristiek numeriek voor enkele waarden van a en b.

Dit verslag van ons tweedejaars project is grotendeels gebaseerd op een artikel van onze begeleider Pieter Moree: arXiv.math.NT/0311483, zie referentie [1].

Inhoudsopgave

1 Inleiding

1.1 Heuristieken en priemgetallen

In dit verslag zullen we twee heuristische formules voor de dichtheid van priemdelers van rijtjes $\{a^k + b^k\}_{k=0}^{\infty}$ bekijken. We noemen een functie $\hat{f}$ een asymptotisch exacte benadering van f, notatie $\hat{f} \sim f$, als geldt dat $\lim_{x\to\infty} \frac{\hat{f}(x)}{f(x)} = 1$. We zullen gebruik gaan maken van enkele begrippen en stellingen uit de getaltheorie, die we nu zullen introduceren.

Allereerst voeren we een priemtelfunctie in die aangeeft hoeveel priemen kleiner gelijk x er bestaan:

$$\pi(x) := \#\{p \,|p \leq x,\, p \in \mathbb{P}\},$$

met $\mathbb{P}$ de verzameling van priemgetallen. Voor $\pi(x)$ bestaan er redelijk goede benaderingen. Een simpele is $x/\log x$. Dit wordt de Priemgetal Stelling genoemd.

Stelling 1.1 *Voor $x \to \infty$ geldt de asymptotische gelijkheid $\pi(x) \sim \frac{x}{\log x}$.*

Deze beroemde stelling werd in 1896 onafhankelijk door Hadamard (Frankrijk) en De la Vallée-Poussin (België) bewezen. Het bewijs begint met de truc om de divergente harmonische reeks te vervormen tot een product over priemgetallen. Voor een convergente reeks $\sum_{n=1}^{\infty} 1/n^s$ geldt:

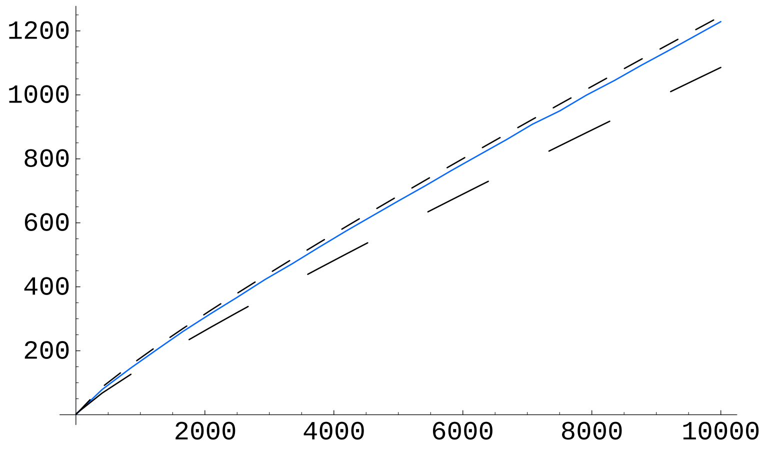
$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}}.$$

Een betere benadering wordt echter gegeven door de logaritmische integraal $\mathrm{Li}(x)$, gedefinieerd door

$$\mathrm{Li}(x) := \int_2^x \frac{1}{\log t} \mathrm{d}t.$$

Waar komen deze benaderingen vandaan? Om deze vraag te beantwoorden vragen we ons af hoe groot de kans is dat een getal priem is. In feite is die kans natuurlijk 1 of 0: een getal is wel priem of niet. De ‘kans’ waar wij het over willen hebben is een heuristische kans. Zij $f(x)$ een functie die de kans geeft dat x priem is. Dus $f(x)$ is de kans dat er geen kleiner getal dan x is dat x deelt. Grofweg deelt x een groter getal met kans $1/x$, immers één op de x getallen is een veelvoud van x.

De kans dat $x+1$ een priemgetal is, is ongeveer de kans dat x een priemgetal is maal de kans dat x een priemdeler is van $x + 1$. Dit klinkt vreemd,



Figuur 1: De doorgetrokken lijn is $\pi(x)$. De logaritmische integraal geeft er een goede benadering voor. De functie $x/\log x$ (onderste) is makkelijker maar doet het minder goed.

maar let op: we hebben het hier niet over een gewone kans. Als x wel een deler is, maar geen priemdeler, zal er ook een kleinere deler zijn van $x+1$, en daar wordt al rekening mee gehouden in de functie $f(x)$. De kans dat x een priemdeler van een getal is, is dus ongeveer $f(x) \cdot 1/x$. De kans dat $x+1$ priem is, ofwel $f(x+1)$, is dus ongeveer de kans dat het niet gedeeld wordt door een getal kleiner dan x, dus $f(x)$, maal de kans dat het *niet* gedeeld wordt door x, dus $1 - f(x)/x$. We krijgen zo (voor $x >> 1$) de volgende (differentie)vergelijking:

$$f(x+1) = f(x)(1 - \frac{f(x)}{x}).$$

Oplossen hiervan gaat als volgt.

$$\frac{f(x+1) - f(x)}{1} = \frac{-f^2(x)}{x} \Rightarrow f'(x) = \frac{-f^2(x)}{x}.$$

Integreren levert nu

$$f(x) = \frac{1}{\log x + c}.$$

We kunnen voor het gemak $c = 0$ kiezen. We zijn namelijk alleen geïnteresseerd in de limiet $\lim_{x\to\infty}$ en dan is $\log x + c \approx \log x$. Dus we hebben $\frac{1}{\log x}$ als ruwe schatting voor de kans dat een getal x priem is.

We weten nu dus dat de kans dat een getal n een priemgetal is, ongeveer gelijk is aan $1/\log n$. Daaruit kunnen we een benadering voor $\pi(x)$ afleiden. Daartoe gaan we eerst $\pi(x)$ herschrijven:

$$\pi(x) = \sum_{n \leq x,\, n \in \mathbb{P}} 1 + \sum_{n \leq x,\, n \notin \mathbb{P}} 0.$$

Dit is de som over een functie die 1 is als n priem is en 0 als n niet priem is. We kunnen een verwachtingswaarde opschrijven:

$$\pi(x) \approx \sum_{n \leq x} \big(1 \cdot \frac{1}{\log n} + 0 \cdot (1 - \frac{1}{\log n})\big).$$

Voor grote x is deze som te benaderen met een integraal, en dat levert ons de volgende uitdrukking:

$$\pi(x) \approx \int_2^x \frac{\mathrm{d}t}{\log t} := \mathrm{Li}(x).$$

We integreren hier vanaf 2, omdat dat het eerste priemgetal is. Met behulp van partiële integratie volgt hieruit het resultaat van de Priemgetalstelling.

$$\int_2^x 1 \cdot \frac{1}{\log t} \mathrm{d}t = \int_2^x \frac{\mathrm{d}}{\mathrm{d}t} t \cdot \frac{1}{\log t} \mathrm{d}t = \frac{x}{\log x} - \frac{2}{\log 2} - \int_2^x \frac{t}{-t \log^2 t} \mathrm{d}t.$$

Voor grote x is de constante term te verwaarlozen, en wordt ook de derde term verwaarloosbaar klein ten opzichte van de eerste. En hieruit volgt dus de andere benadering $\pi(x) \sim \frac{x}{\log x}$.

Onder aanname van de Riemann hypothese blijkt zelfs het volgende te gelden:

$$\pi(x) = \int_2^x \frac{\mathrm{d}t}{\log t} + O(\sqrt{x} \log x).$$

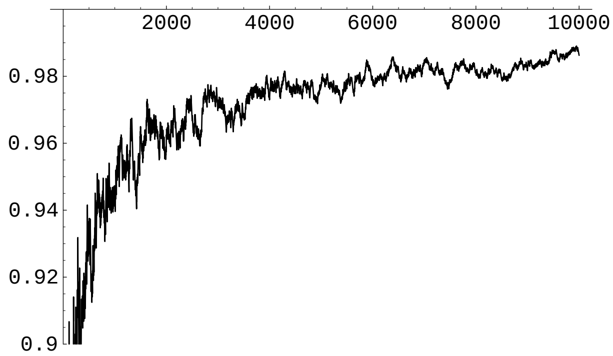
1.2 Riemann-hypothese (RH)

De Riemann hypothese gaat over de zeta-functie:

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

Dus bijvoorbeeld: $\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + ... = \frac{\pi^2}{6}$. Wat heeft dit eigenlijk met priemgetallen te maken? Wel, we kunnen de reeks op de volgende manier uitschrijven:

$$\sum_{n=1}^{\infty} \frac{1}{n^x} = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{2^x 2^x} + \frac{1}{5^x} + \frac{1}{2^x 3^x} + \frac{1}{7^x} + \frac{1}{2^x 2^x 2^x} + \frac{1}{3^x 3^x} + \dots$$



Figuur 2: Hier is $\pi(x)/\mathrm{Li}(x)$ geplot. Door x groot genoeg te kiezen kun je $\pi(x)/\mathrm{Li}(x)$ willekeurig dicht tot 1 laten naderen. Er geldt dat $\pi(x) \sim \mathrm{Li}(x)$.

We gebruiken hier dat elk getal een unieke ontbinding in priemfactoren heeft. In de som staan dus alleen nog maar priemgetallen. We willen dat elk natuurlijk getal één keer in de reeks voorkomt, dus moeten elke combinatie van priemgetallen er precies één keer in zitten. Dat is precies het geval bij het volgende oneindige product:

$$(1+\frac{1}{2^x}+\frac{1}{2^x 2^x}+\ldots)\cdot(1+\frac{1}{3^x}+\frac{1}{3^x 3^x}+\ldots)\cdot(1+\frac{1}{5^x}+\frac{1}{5^x 5^x}+\ldots)\cdot(1+\frac{1}{7^x}+\ldots)$$

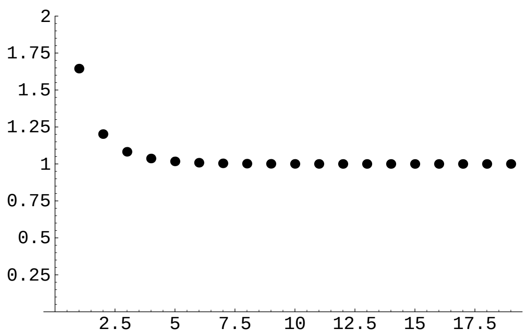
We gebruiken nu het idee van de meetkundige reeks om dit korter op te schrijven. Voor $x > 1$ geldt $1 + \frac{1}{x} + \frac{1}{x^2} + \frac{1}{x^3} + \ldots = \frac{1}{1-\frac{1}{x}}$.

Voor $x > 0$ geldt $p^x > 1$ en kunnen we $\zeta(x)$ dus herschrijven als

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} = \prod_p \sum_{n=0}^{\infty} \frac{1}{(p^x)^n} = \prod_p \frac{1}{1-p^{-x}}. \tag{1}$$

De hypothese van Riemann zegt: Alle niet triviale nulpunten van de Riemann-zeta functie hebben reëel deel een half. De eerste paar waarden van $\zeta(x)$ zijn:

$$\zeta(1) = \infty$$
$$\zeta(2) = \frac{\pi^2}{6} \approx 1.64493$$
$$\zeta(3) \approx 1.20206$$
$$\zeta(4) = \frac{\pi^4}{90} \approx 1.08232$$



Figuur 3: De reële Riemann-zeta functie voor gehele getallen tussen 2 en 20

De functie lijkt helemaal geen nulpunten te hebben! Het punt is dat de Riemann-hypothese over de complexe Riemann-Zeta functie gaat. Alleen hebben we dan een probleem: wat betekent het bijvoorbeeld dat je drie $(2+i)$ keer met zichzelf moet vermenigvuldigen? We kunnen niet zo maar complexe getallen voor x invullen in $\zeta(x)$. Alleen als het reële deel groter is dan 1, is er sprake van convergentie. Het blijkt dat we de functie tot heel $\mathbb{C}$ kunnen uitbreiden en dan kunnen we dus wel complexe getallen invullen. Alleen in $x = 1$ zit een pool (met residu 1). Rond $x = 1$ gedraagt de functie zich als $\frac{1}{x-1}$. We noemen deze nieuwe functie $\zeta(z)$. Het uitbreiden van de Riemann-Zeta functie is niet zo makkelijk maar wel uniek. De complexe Riemann-Zeta functie wordt:

$$\zeta(z) = \frac{1}{1-2^{1-z}} \sum_{n=0}^{\infty} \frac{1}{2^{n+1}} \sum_{k=0}^{n} (-1)^k \frac{(n+k)!}{n!k!} (k+1)^{-z}.$$

Er is ook een functionaalvergelijking voor de Riemann-Zeta functie. Deze luidt

$$\pi^{-\frac{1}{2}z}\Gamma(\frac{1}{2}z)\zeta(z) = \pi^{-\frac{1}{2}(1-z)}\Gamma(\frac{1}{2}(1-z))\zeta(1-z).$$

Riemann-hypothese: Alle niet triviale nulpunten van de complexe Riemann-Zeta functie hebben reëel deel $\frac{1}{2}$.

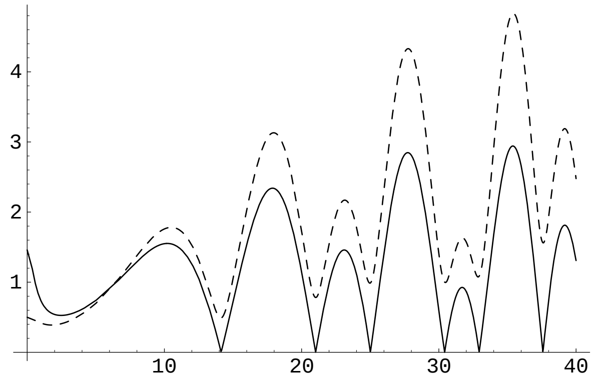
De triviale nulpunten zijn $-2, -4, -6, \ldots$.

Inmiddels is voor meer dan vijfhonderd miljard nulpunten bekend dat het reële deel gelijk is aan een half, maar dat bewijst natuurlijk nog niets. Als de Riemann-hypothese waar is zijn de priemgetallen redelijk regelmatig verdeeld. Ze gedragen zich dan ongeveer zoals de wet van de grote aantallen voorschrijft. Als de Riemann-hypothese niet geldt, is het gedrag veel wilder.

Misschien leuk om hier te noemen is een verhaal dat gaat over Ramanujan. Dit Indische genie schreef ooit op:

$$1 + 2 + 3 + ... = \frac{-1}{12}.$$

Strikt genomen is dit natuurlijk onzin. Merk op dat $n = 1/(1/n) = 1/n^{-1}$. Dus $1 + 2 + 3 + ...$ kun je opvatten als $\zeta(-1)$ en het blijkt dat $\zeta(-1) = \frac{-1}{12}$!



Figuur 4: De complexe Riemann-Zeta functie met reëel deel een half: $|\zeta(\frac{1}{2} + y \cdot i)|$ met y lopend van 0 to 40. De gestippelde lijn $|\zeta(0 + y \cdot i)|$ heeft geen nulpunten.

Het blijkt verder dat de Riemann-Zeta functie op de imaginaire as *geen* nulpunten heeft. Dit feit kan gebruikt worden om de Priemgetal Stelling te bewijzen. Dit zullen wij hier echter niet doen.

1.2.1 Uitgebreide Riemann-hypothese (ERH)

De Uitgebreide Riemann-hypothese (Engels: Extended Riemann Hypothesis) gaat over een generalisatie van de zeta-functie. Deze generalisatie is de zogenaamde Dirichlet L-functie en maakt gebruik van karakters. Een karakter modulo d is een functie $\chi : \mathbb{Z} \to \mathbb{C}$ met de eigenschappen

$$\begin{cases} \text{(i)} \;\; \chi(1) = 1 \\ \text{(ii)} \;\; \chi(n+d) = \chi(n) \text{ voor alle } n \\ \text{(iii)} \;\; \chi(n) = 0 \text{ als } \mathrm{ggd}(n,d) = 1 \\ \text{(iv)} \;\; \chi(mn) = \chi(m)\chi(n) \text{ voor alle } m \text{ en } n. \end{cases}$$

Bij een karakter χ hoort een L-functie die wordt gegeven door:

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

L-functies hebben veel gemeen met ζ-functies. Dat komt door eigenschap (iv). Er geldt:

$$\frac{\chi(m)}{m^s} \cdot \frac{\chi(n)}{n^s} = \frac{\chi(mn)}{(mn)^s}.$$

Net als $\zeta(z)$ kan $L(z, \chi)$ tot het hele complexe vlak voortgezet worden.

Uitgebreide Riemann-hypothese: Alle niet-triviale nulpunten van alle L-functies liggen op de as $x = \frac{1}{2}$

Dirichlet voerde zijn L-functies in om te bewijzen dat als a en d relatief priem zijn er oneindig veel priemgetallen p zijn die voldoen aan $p \equiv a($ mod $d)$. Veel resultaten uit de getaltheorie zijn onder aanname van de ERH of een variant ervan, de zogenaamde GRH (Grand Riemann Hypothesis) bewezen. Zo bewees Hooley in 1967 dat onder de GRH het vermoeden van Artin over primitieve wortels waar is.

1.3 Primitieve wortels

De eindige abelse groep $(\mathbb{Z}/p\mathbb{Z})^*$ is een vermenigvuldigings groep van gehele getallen modulo een priemgetal p. Het is een cyclische groep van orde $p-1$. De orde van een groep is het aantal elementen van een groep, terwijl de orde van een element a het kleinste getal n is waarvoor geldt $a^n = 1$. De kleine stelling van Fermat zegt dat als a niet deelbaar door p is er geldt dat $a^{p-1} = 1$ modulo p. De orde is dus maximaal gelijk aan $p-1$.

Definitie. Een getal a is een primitieve wortel modulo p als de restklasse a de cyclische groep $(\mathbb{Z}/p\mathbb{Z})^*$ voortbrengt.

Dus a is een primitieve wortel modulo p dan en slechts dan als geen van de $a^n (\text{mod } p)$ met n tussen 1 en $p-1$ aan elkaar gelijk zijn. Een andere karakterisatie is: a is een primitieve wortel modulo p dan en slechts dan als de orde van a modulo p gelijk is aan $p-1$.

Voorbeeld.
De multiplicatieve groep $(\mathbb{Z}/7\mathbb{Z})^*$ bestaat uit de restklassen $\{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$. Nu is 3 een primitieve wortel modulo zeven, omdat we door het element 3 in $(\mathbb{Z}/7\mathbb{Z})^*$ een aantal keren met zich zelf te vermenigvuldigen elke restklasse in de groep kunnen krijgen:

$$3^1 \equiv 3.$$

$$3^2 = 9 \equiv 2.$$

$$3^3 = 27 \equiv 6.$$
$$3^4 = 81 \equiv 4.$$
$$3^5 = 243 \equiv 5.$$
$$3^6 = 729 \equiv 1.$$

Twee is geen primitieve wortel modulo 7 aangezien $2^4 \equiv 2$ maar ook $2^1 \equiv 2$.

Lemma 1.2 *Een kwadraat a is nooit een primitieve wortel modulo p.*

Het maakt dus niet uit welke p je kiest. Voor het bewijs van dit Lemma hebben we de kleine stelling van Fermat nodig die zegt: $a^{p-1} \equiv 1 (\text{mod } p)$. Laten we zeggen dat $a = b^2$. Wegens de kleine stelling van Fermat geldt dan $b^{p-1} = a^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$. Dat betekent dat de orde van a kleiner is dan $p-1$ (zelfs $\leq \frac{p-1}{2}$) en dus is a geen primitieve wortel.

1.3.1 Artin's vermoeden

Laat $a \neq -1$ een geheel getal zijn dat geen kwadraat is. Dan is a een primitieve wortel modulo p voor oneindig veel priemgetallen. Verder is de dichtheid van priemgetallen p waarvoor a een primitieve wortel is, als fractie van alle priemgetallen, gelijk aan een positief rationaal getal keer A, de constante van Artin. Dit alles geldt onder de aanname van de GRH en is in 1967 door Hooley [2] bewezen. Laat $\pi_g(x)$ het aantal priemen $p \leq x$ zijn zodanig dat g een primitieve wortel van p is. Het vermoeden van Artin (1927) zegt nu:

Vermoeden van Artin: Als g geen kwadraat is en niet gelijk aan -1 dan geldt asymptotisch voor zekere positieve constante c_g dat $\pi_g(x) \sim c_g A \pi(x)$.

Als de GRH geldig is, dan is ook Artin's vermoeden waar. Tot nu toe is het nog voor geen enkele a gelukt om het vermoeden te bewijzen. Wel is bekend dat als we a beperken tot priemgetallen, voor hooguit twee priemgetallen het Artin vermoeden niet waar is. Dus er is een $a \in \{2, 3, 5\}$ waarvoor het Artin vermoeden waar is! Artin's constante A wordt gegeven door

$$A = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136...,$$

waar het product over alle priemgetallen p loopt. Het optreden van de Artin constante in deze setting kan ook met heuristische argumenten plausibel gemaakt worden.

1.4 Het Legendre symbool

We gaan nu het Legendre symbool invoeren, dat we later nodig zullen hebben bij het uitvoeren van sommaties. Zij

$$x^2 \equiv n(\text{mod } p).$$

Als er een x bestaat die hieraan voldoet voor een zekere n, dan noemen we die n een kwadratisch residu. We noteren dit als $n\mathbf{R}p$. Deze notatie gaat terug tot de *Disquisitiones Arithmeticae* van Gauss (1801).

Definitie. *Het Legendre symbool* $(\frac{n}{p})$ *wordt gedefinieerd als*:

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & \text{als } n \equiv 0 \pmod p, \\ 1 & \text{als } n\mathbf{R}p \text{ en} \\ -1 & \text{als } n\mathbf{R}p \text{ niet geldt.} \end{cases}$$

Euler bewees dat

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \bmod p. \quad \text{(Criterium van Euler)}$$

De kleine stelling van Fermat is erg handig om dit te bewijzen.

Een paar rekenregels voor het Legendre symbool.

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right). \tag{2}$$

$$\left(\frac{m+p}{p}\right) = \left(\frac{m}{p}\right). \tag{3}$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{als } p \equiv 1(4); \\ -1 & \text{als } p \equiv 3(4). \end{cases} \tag{4}$$

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{als } p \equiv \pm1(8); \\ -1 & \text{als } p \equiv \pm3(8). \end{cases} \tag{5}$$

De bewijzen van de rekenregels 2 en 3 zijn triviaal en worden aan de lezer overgelaten. Rekenregels 4 en 5 kunnen worden bewezen door gebruik te maken van het criterium van Euler. Een andere handigheid is de kwadratische wederkerigheid.

Stelling 1.3 *Voor oneven priemgetallen p en q, $p \neq q$ geldt:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \quad \text{(kwadratische wederkerigheid).} \tag{6}$$

Voorbeeld. Als voorbeeld gaan we kijken of er een x bestaat zodanig dat $x^2 \equiv 257 \pmod{137}$. De eerste stap is makkelijk: $257 \pmod{137} \equiv 120 \pmod{137}$. Dit is dus rekenregel 3.

$$\left(\frac{257}{137}\right) = \left(\frac{120}{137}\right) = \left(\frac{2^3 \cdot 3 \cdot 5}{137}\right).$$

Met rekenregel 2 krijgen we:

$$= \left(\frac{2}{137}\right)^3 \left(\frac{3}{137}\right)\left(\frac{5}{137}\right).$$

We zien dat de eerste term 1 is door op te merken dat $137 \equiv 1 \pmod{8}$ en rekenregel 5 toe te passen. Voor de andere twee termen gebruiken we de kwadratische wederkerigheid formule, waarbij we opmerken dat je één van de Legendresymbolen naar de andere kant van het is-teken mag brengen omdat er toch altijd 1, -1 of 0 uitkomt. Dus dit is gelijk aan:

$$\left(\frac{257}{137}\right) = 1 \cdot \left(\frac{137}{3}\right)(-1)^{\frac{1}{4}(3-1)(137-1)}\left(\frac{137}{5}\right)(-1)^{\frac{1}{4}(5-1)(137-1)}.$$

Met rekenregel 3 en weer kwadratische wederkerigheid zien we dat er 1 uitkomt:

$$\left(\frac{257}{137}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)^{\frac{1}{8}(3^2-1)}(-1)^{\frac{1}{8}(5^2-1)} = 1.$$

Hiermee is dus aangetoond dat 257 een kwadratisch residu is modulo 137. Helaas komen we op deze manier niet te weten welke x-en voldoen aan $x^2 \equiv 257 \pmod{137}$. In het algemeen lijkt het niet makkelijk om een procedure te vinden om x daadwerkelijk te bepalen.

In 1783 stelde Euler de stelling van de kwadratische wederkerigheid voor. Legendre publiceerde als eerste een bewijs, maar dat was onvolledig (hij nam -zonder bewijs- aan dat er oneindig veel priemen van de vorm $p \equiv a \pmod{d}$ zijn als a en d relatief priem zijn. Dit werd pas veel later door Dirichlet met zijn L-functies bewezen). Gauss kwam in 1796 met een bewijs dat wel volledig en correct was. De kwadratische wederkerigheids stelling was Gauss' favoriete stelling uit de getaltheorie (hij noemde deze dan ook Theorema Aureum, dat wil zeggen de Gouden Stelling). Hij kon er niet genoeg van krijgen en bedacht niet minder dan acht verschillende bewijzen. Een (andere) belangrijke reden voor deze overvloed aan bewijzen was dat Gauss hoopte een bewijs te vinden dat gemakkelijk gegeneraliseerd kon worden naar kubische en bikwadratische wederkerigheid. Uiteindelijk publiceerde Eisenstein als eerste bewijzen voor de hogere wederkerigheidswetten, die Gauss geformuleerd had.

1.5 Heuristieken voor primitieve wortels

Laat weer $\pi(x)$ het aantal priemen $p \leq x$ zijn en $\pi_g(x)$ het aantal priemen $p \leq x$ zijn zodanig dat g een primitieve wortel is modulo p. Het aantal primitieve wortels in $(\mathbb{Z}/p\mathbb{Z})^*$ wordt aangegeven door $\varphi(p-1)$ waarbij φ de Euler totiënt-functie is. Als g een primitieve wortel is modulo p, dan is g^n een primitieve wortel dan en slechts dan als $\text{ggd}(n, p-1) = 1$. Aangezien het aantal elementen in $(\mathbb{Z}/p\mathbb{Z})^*$ gelijk is aan $p-1$, is de dichtheid van primitieve wortels in $(\mathbb{Z}/p\mathbb{Z})^*$ gelijk aan $\varphi(p-1)/(p-1)$. Voor een heuristische formule $H_1(x)$ voor $\pi_g(x)$ hoeven we dus alleen de kans dat g een primitieve wortel is modulo p te sommeren over alle priemen kleiner gelijk x. Deze 'kans' is telkens gelijk aan $\varphi(p-1)/(p-1)$. Dus:

$$H_1(x) = \sum_{p \leq x} \frac{\varphi(p-1)}{p-1}.$$

Er geldt $H_1(x) \sim A\pi(x)$ waarbij A de Artin constante is en het slangetje weer betekent dat $\lim_{x\to\infty} \frac{H_1(x)}{A\pi(x)} = 1$. Dit kan bewezen worden door gebruik te maken van de Siegel-Walfisz stelling uit de analytische getaltheorie. We zullen hier verder niet op ingaan. Echter, de heuristiek $H_1(x)$ is, zelfs onder aanname van de GRH, niet altijd asymptotisch exact gelijk aan $\pi_g(x)$. Pieter Moree [3] heeft een modificatie, $H_2(x)$, gevonden (die gebruik maakt van het Legendre symbool, en daarom wel kwadratisch wordt genoemd) die wel asymptotisch exact is: $\pi_g(x) \sim H_2(x)$.

2 Heuristische formules

2.1 Voorbereidingen

We zullen laten zien dat er iets dergelijks als bij de primitieve wortels ook optreedt in het geval van heuristieken voor $N_{a,b}$. Er is een simpele heuristiek voor $N_{a,b}$ die in vele - maar niet alle - gevallen asymptotisch exact is. Daar is echter een modificatie van die wèl asymptotisch exact is, en die, net als $H_2(x)$, weer gebruik maakt van het Legendre symbool.

Om deze twee heuristieken te begrijpen zullen we onderstaande drie lemma's nodig hebben. Eerst even wat notatie.

Notatie.
Voor een beter overzicht schrijven we (a, b) voor $\operatorname{ggd}(a, b)$. Ieder geheel getal g kan uniek ontbonden worden in priemfactoren. Het aantal keren dat een priem p voorkomt in deze unieke factorisatie noteren we als $\nu_p(g)$. Als $\nu_p(g) = 0$, dan schrijven we $\operatorname{ord}_g(p)$ voor het kleinste positieve getal k zodanig dat $g^k \equiv 1 (\operatorname{mod} p)$. Merk op dat g een primitieve wortel is modulo p dan en slechts dan als $k = p - 1$.

Lemma 2.1 *Laat $h \geq 1$ en $w \geq 0$ gehele getallen zijn. Laat G een cyclische groep van orde n zijn. Laat verder $G^h = \{g^h : g \in G\}$ en $G^h_w = \{g^h : \nu_2(\operatorname{ord}(g^h)) = w\}$. Dan geldt:*

$$\#G^h = \frac{n}{(n, h)},$$

en

$$\#G^h_0 = 2^{-\nu_2(\frac{n}{(n,h)})} \frac{n}{(n, h)}.$$

Verder geldt voor $w \geq 1$,

$$\#G^h_w = \begin{cases} 2^{w-1-\nu_2(\frac{n}{(n,h)})} \frac{n}{(n,h)} & \textit{als } \nu_2(\frac{n}{(n,h)}) \geq w; \\ 0 & \textit{anders.} \end{cases}$$

Bewijs.
Het is duidelijk dat G^h en G^h_0 ondergroepen zijn van G. G is een cyclische groep en heeft dus een voortbrenger, g_0. Als $m_1 \equiv m_2 (\operatorname{mod} n)$ dan is $m_2 = m_1 + kn$ voor zekere k. Er geldt $g_0^{m_2} = g_0^{m_1+kn} = g_0^{m_1}$, omdat g_0^n de identiteit is. We bekijken G^h. Deze groep bestaat uit elementen $\{g_0^h, g_0^{2h}, ...\}$. We vragen ons hoeveel elementen deze groep heeft. Er geldt $g_0^{k_1 h} = g_0^{k_2 h}$ dan en slechts dan als $hk_1 \equiv hk_2 (\operatorname{mod} n)$. Beide zijdes van deze vergelijking zijn deelbaar door (n, h). Dat geeft $\frac{hk_1}{(n,h)} \equiv \frac{hk_2}{(n,h)} \ (\operatorname{mod} \frac{n}{(n,h)})$. Daar $(\frac{h}{(n,h)}, \frac{n}{(n,h)}) = 1$

volgt nu dat $k_1 \equiv k_2 (\text{mod } \frac{n}{(n,h)})$ en dus is $\#G^h = \frac{n}{(n,h)}$. G^h bestaat dus uit de elementen $g_0^h, g_0^{2h}, \ldots, g_0^{nh/(n,h)} = 1$. Dit zijn $n/(n,h)$ verschillende elementen.

Het bewijs voor G_w^h gaat op analoge wijze. Zie ook [1].

Lemma 2.2 *Als $\nu_2(h) \geq \nu_2(n)$, dan heeft elk element in G^h even orde. Als $\nu_2(h) < \nu_2(n)$ dan $G_0^h \subseteq G^{2h}$.*

Lemma 2.3 *Er geldt:*

$$G_1^h \subseteq \begin{cases} G^h \backslash G^{2h} & \text{als } \nu_2(n) = \nu_2(h) + 1; \\ G^{2h} & \text{als } \nu_2(n) > \nu_2(h) + 1. \end{cases}$$

Als $\nu_2(n) \leq \nu(h)$, dan is G_1^h leeg.

Voor een bewijs van Lemma's 2.2 en 2.3 verwijzen we naar [1].

2.2 Twee heuristische formules voor $N_{a,b}(x)$

In dit hoofdstuk stellen we twee heuristische formules voor $N_{a,b}(x)$ voor; de een wat verfijnder dan de andere. Definieer

$$S = \{a^k + b^k\}_{k=0}^{\infty} \qquad (a, b \in \mathbb{N}).$$

We zeggen dat een priemgetal p een rijtje van gehele getallen deelt als het tenminste één van de termen deelt. Dus

$$p | S \iff \exists k : p | (a^k + b^k).$$

Hiervan gebruik makend schrijven we $N_{a,b}(x)$ als volgt:

$$N_{a,b}(x) := \sum_{p \leq x, \; p|S} 1$$

Als voorbeeld nemen we nu $a = 2$ en $b = 1$. Een bekend resultaat is dat

$$N_{2,1}(x) = \frac{17}{24} \text{Li}(x) + O\Big(\frac{x(\log\log x)^4}{\log^3 x}\Big).$$

Voor $p \nmid 2ab$ geldt dat $p|S \iff \text{ord}_r(p)$ met $r = a/b$ is even. Dit is een belangrijke observatie.

Laat nu h het grootste (gehele) getal zijn zodanig dat voor zeker rationaal getal r_0 geldt dat $|r| = r_0^h$ en laat ϵ het teken van r zijn. De eerste heuristiek die we gaan bekijken is:

$$K_{a,b}^{(1)}(x) = \sum_{p \leq x, \; p \nmid 2ab} \frac{\#G_{p,(1-\epsilon)/2}^h}{\#G_p^h},$$

waarbij het dus de bedoeling is dat $K^{(1)}_{a,b}(x)$ een heuristiek is voor het aantal priemen $p \leq x$ zodanig dat $\mathrm{ord}_r(p)$ oneven is. Uit het werk van Moree, zie [1], blijkt dat $\lim_{x\to\infty} K^{(1)}_{a,b}(x)/\pi(x)$ bestaat. Een motivatie voor de definitie van $K^{(1)}_{a,b}(x)$ is dat (voor $\epsilon = 1$) in zekere zin $\#G^h_{p,0}/\#G^h_p$ de kans is dat $ord_r(p)$ *on*even is. Voor $N_{a,b}(x)$ willen we juist de even ordes hebben en dus krijgen we dan de volgende heuristiek voor $N_{a,b}(x)$, die we $H^{(1)}_{a,b}(x)$ noemen:

$$H^{(1)}_{a,b}(x) = \pi(x) - K^{(1)}_{a,b}(x).$$

Explicieter opsgeschreven, en met $w = \nu_2(h)$ de exponent van 2 in h:

$$H^{(1)}_{a,b}(x) = \pi(x; 2^{w+1}, 1) - 2^w \sum_{\substack{p\leq x\\ \nu_2(p-1)>w}} 2^{-\nu_2(p-1)}, \text{ voor } \epsilon = 1, \text{en} \tag{7}$$

$$H^{(1)}_{a,b}(x) = \pi(x) - 2^w \sum_{\substack{p\leq x\\ \nu_2(p-1)>w}} 2^{-\nu_2(p-1)}, \text{ voor } \epsilon = -1. \tag{8}$$

Deze naïve heuristiek $H^{(1)}_{a,b}(x)$ is in veel, maar niet in alle, gevallen asymptotisch exact. We schrijven $\pi(x; d, a)$ om het aantal priemgetallen $p \leq x$ aan te geven die congruent zijn aan a modulo d. Pieter Moree heeft een kwadratische modificatie van $H^{(1)}_{a,b}(x)$ gevonden, zie [1]. Dit houdt in dat deze (nauwkeurigere) heuristiek, die we $H^{(2)}_{a,b}(x)$ noemen, gebruik maakt van het Legendre symbool. Deze verbeterde heuristiek is wel asymptotisch exact en wordt gegeven door

$$H^{(2)}_{a,b} = \pi(x; 2^{w+1}, 1) - 2^{w+1} \sum_{\substack{p\leq x, (r_0/p)=1\\ \nu_2(p-1)>w}} 2^{-\nu_2(p-1)}, \text{ voor } \epsilon = 1, \text{en} \tag{9}$$

$$H^{(2)}_{a,b}(x) = \pi(x) - \sum_{\substack{p\leq x, (r_0/p)=-1\\ \nu_2(p-1)=w+1}} 1 - 2^{\epsilon+1} \sum_{\substack{p\leq x, (r_0/p)=1\\ \nu_2(p-1)>w+1}} 2^{-\nu_2(p-1)}, \text{ voor } \epsilon = -1. \tag{10}$$

Wat opvalt is dat voor $\epsilon = -1$ de som in twee delen wordt gesplitst. Eentje met Legendre symbool -1 en de andere met +1. Het deel met Legendre symbool -1 is het 'zekere' deel; dat wil zeggen dat als $(r_0/p) = -1$ en $\nu_2(p-1) = w+1$, dan wordt p niet geteld door $H^{(2)}_{a,b}(x)$. De daadwerkelijke heuristiek is in de tweede som met Legendre symbool +1 bevat.

De waarden van wat we voor $H^{(2)}_{a,b}(x)$ verwachten zijn te vinden in [1]. We hebben met behulp van de computer een controle uitgevoerd voor enkele waarden van a en b, met a/b zowel positief als negatief.

3 Numerieke controle

3.1 De gebruikte code

De numerieke controle van de heuristiek $H^{(2)}_{a,b}$ is gedaan met het computeralgebrapakket *Mathematica*. De code - met tussendoor uitleg - zag er voor $\epsilon = 1$ als volgt uit.

```
e2[x_] := IntegerExponent[x, 2]
```

e2(x) geeft $\nu_2(x)$, de exponent van 2 in de canonieke factorisatie van x.

```
Leg[a_, p_] := Mod[a^((p - 1)/2), p]
```

Om het Legendre symbool uit te rekenen gebruiken we het criterium van Euler. Leg[a, b] berekent $(\frac{a}{b})$.

```
Piefunc[x_, k_, l_] = Sum[If[p \[Element] Primes
&& Mod[p, k] == 1, 1, 0], {p, 1,x}];
```

Hier is Piefunc[x, k, l] $= \pi(x; k, l)$, het aantal priemen $p \leq x$ met $p \equiv l (\text{mod } k)$.

```
a = 2; b = 1; hmax = 200;
```

Hier worden $r = \frac{a}{b}$ en *hmax* gedefinieerd. In werkelijkheid zou h groter kunnen zijn dan *hmax*, maar we nemen aan dat dit een hele kleie fout geeft. Om h te bepalen gaan we alle waarden van h van 1 tot hmax na en kijken of r_0 een breuk is met $\mid r \mid = r_0^h$.

```
haa[r_] := Last[Sort[Table[If[(r)^(1/h)
\[Element] Rationals, h, 0], {h, 1, hmax}]]];
```

ee[r] $= \nu_2(h)$, het aantal factoren 2 in de priemontbinding van h. Verder is ee gelijk aan $\nu_2(h)$ voor de h die hoort bij de gekozen a en b.

```
ee[r_] := e2[haa[r]];
ee = ee[a/b];
r0 = (a/b)^(1/haa[a/b]);
```

$r0$ is de breuk die voldoet aan $\mid r \mid= r_0^h$.

```
H2ab[x_] := Piefunc[x, (2)^(ee + 1), 1] - 2^(ee + 1)
    Sum[If[ p <= x && e2[p - 1]> ee && Leg[r0, p] == 1,
        2^(-e2[p - 1]), 0], {p,1, x}];
```

Dit is formule (5) uit [1].

3.1.1 Opmerkingen

Voor negatieve $r = a/b$ moet de code een beetje worden aangepast omdat $H^{(2)}_{a,b}(x)$ dan anders gedefinieerd is. Van belang hierbij is om niet de fout

```
Leg[r0, p] == -1
```

te maken. *Mathematica* geeft de uitkomsten van een berekening modulo p tussen 0 en $p - 1$. De oplossing is dus eenvoudigweg

```
Leg[r0, p] == p-1.
```

Verder heeft onze begeleider ons erop gewezen dat het Legendre symbool al in *Mathematica* ingebouwd zit. Leg[a,p] = JacobiSymbol[a,p]. Het Jacobi symbool is een uitbreiding van het Legendre symbool, maar JacobiSymbol[a,p] met p priem is gewoon het Legendre symbool. Het kan zijn dat werken met het voorgeprogrammeerde Jacobi symbool het programma sneller maakt.

Wij nemen voor de simulatie aan $h \leq 200$. In de heuristieken gaat het niet om die h zelf, maar om $\nu_2(h)$ (de grootheid die we in onze heuristieken w hebben genoemd).

3.2 Resultaten

Controle van de heuristiek voor $r = 2$.

We verwachten voor $N_{2,1}$ volgens Tabel 1 uit [1] dat $\delta(r) = \frac{17}{24}$, dat wil zeggen dat $\lim_{x\to\infty} N^{(2)}_{2,1}(x)/\pi(x) = 17/24$. Voor verschillende waarden van x maken we (op logaritmische schaal) een tabel.

```
H2met21 = Table[H2ab[E^x]/PrimePi[E^x] // N, {x, 6, 13, 1}]
```

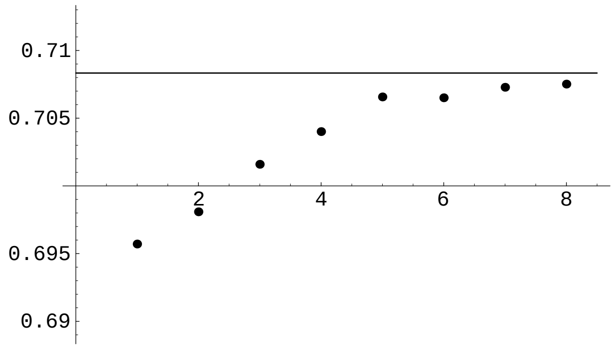
Dit geeft als resultaat voor $H_{2,1}(x)$ - met $x = e^n$, waarbij n van zes tot en met dertien loopt - de lijst

$$\{0.6957, 0.6980, 0.7015, 0.7040, 0.706, 0.7065, 0.7072, 0.7075\}.$$

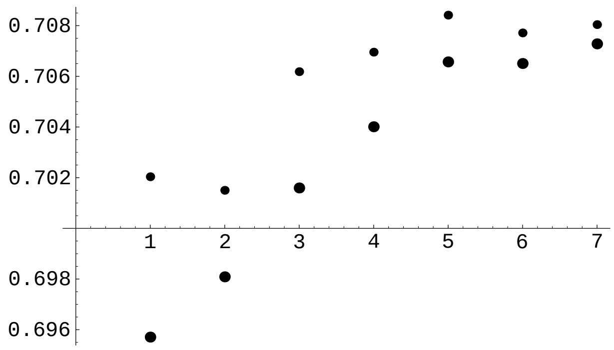
Numeriek is 17/24 gelijk aan 0.7083, dus het zit aardig in de buurt. Het resultaat van deze punten samen met de constante lijn $\frac{17}{24}$ staat in figuur 5. Dit is met onderstaande code gedaan.

```
a21 = Plot[17/24, {x,0, 8.5}, PlotRange ->
{17/24 - 0.02, 17/24 + 0.005}, DisplayFunction -> Identity];
c21 = ListPlot[H2met21, PlotStyle -> PointSize[0.016],
DisplayFunction -> Identity];
res21 = Show[a21, c21, DisplayFunction ->$DisplayFunction];
```

We kunnen de heuristiek $H_{2,1}$ ook rechtsreeks met $N_{2,1}$ vergelijken. De convergentie is dan mooi te zien. Zie figuur 6.



Figuur 5: In deze figuur staat $H^{(2)}_{2,1}(x)$ voor enkele waarden van x logaritmisch uitgezet. Ook de constant $17/24$ is geplot.

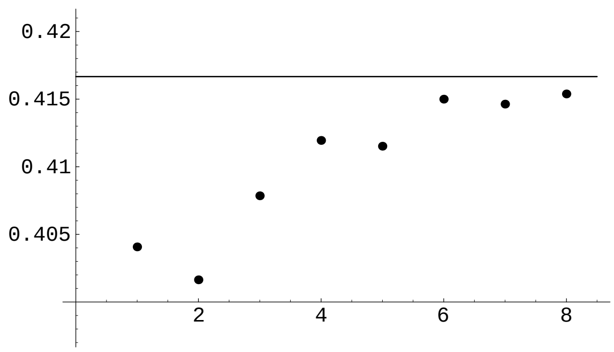


Figuur 6: $H^{(2)}_{2,1}(x)$ voor $x = e^6, e^7, ..., e^{12}$ (dikkere punten) rechtsreeks vergeleken met $N_{2,1}(x)$.

Controle van de heuristiek voor $r = 4$.

Voor $a = 4$ en $b = 1$ verwachten we als antwoord 5/12. Zie figuur 7 voor de resultaten. Voor deze a en b geeft *Mathematica* $h = 1$. We maken weer een tabel van waarden van $H_{4,1}(x)$ met $x = e^n$, waarbij n de waarden zes tot en met dertien aanneemt. Dit geeft

$$\{0.4040, 0.4016, 0.4078, 0.4119, 0.4115, 0.4149, 0.4146, 0.4153\}.$$



Figuur 7: $H^{(2)}_{4,1}(x)$ voor $x = e^6, e^7, ..., e^{13}$. De rechte lijn heeft een waarde van 5/12.

Controle van de heuristiek voor $r = 81$.

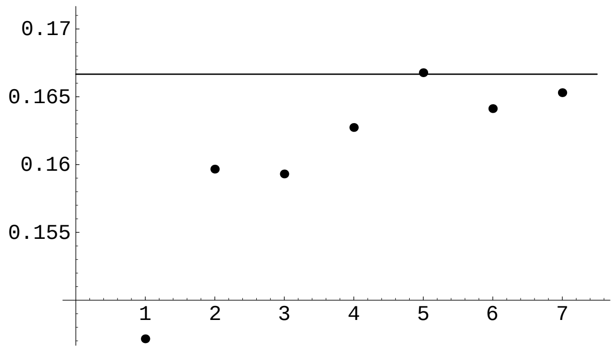
Voor $a = 81$ en $b = 1$ verwachten we als antwoord 1/6, zie weer Tabel 1 uit [1]. Er geldt $h = 2$. Merk op dat $L \neq \mathbb{Q}(\sqrt{2})$. In figuur 8 staan resultaten. De numerieke waardes zijn

$$\{0.1471, 0.1596, 0.1593, 0.1627, 0.1667, 0.1641, 0.1653\}.$$

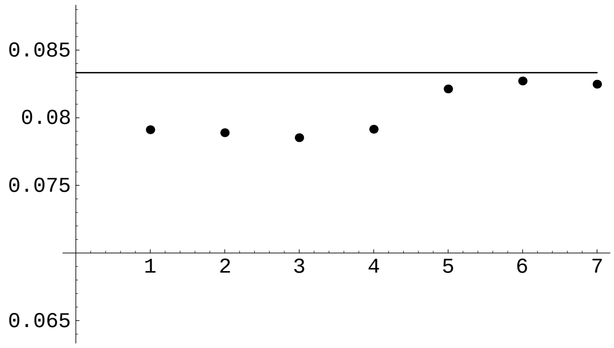
Controle van de heuristiek voor $r = 6561$.

Voor $a = 6561 = 3^8$ en $b = 1$ verwachten we als antwoord 1/12. Nu geldt $h = 3$. Merk weer op dat $L \neq \mathbb{Q}(\sqrt{2})$. Zie figuur 9 voor de resultaten. De heuristische waarden zijn

$$\{0.07911, 0.07889, 0.07852, 0.07915, 0.0821, 0.08271, 0.0824\}.$$



Figuur 8: $H^{(2)}_{81,1}(x)$ voor $x = e^6, e^7, ..., e^{12}$.

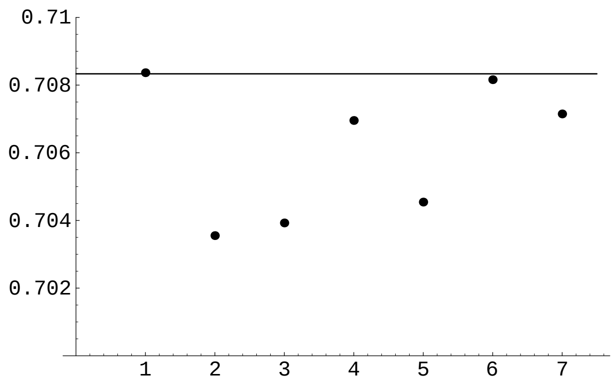


Figuur 9: $H^{(2)}_{6561,1}(x)$ voor $x = e^6, e^7, ..., e^{12}$.

Controle van de heuristiek voor $r = -2$.

Voor $a = -2$ en $b = 1$ verwachten we als antwoord 17/24. De numerieke waardes die in figuur 10 zijn geplot zijn

$$\{0.7083, 0.7035, 0.7039, 0.7069, 0.7045, 0.708, 0.7071\}.$$



Figuur 10: $H^{(2)}_{-2,1}(x)$ voor $x = e^6, e^7, ..., e^{12}$.

Controle van de heuristiek voor $r = -4$.

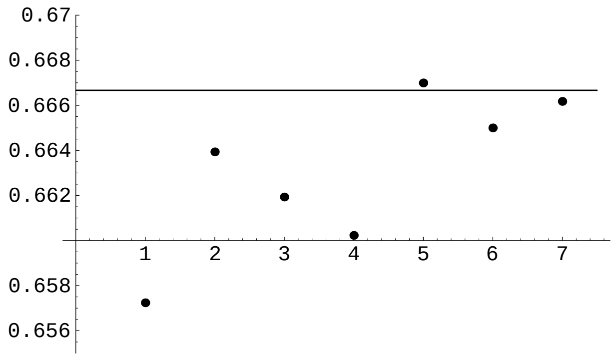
Volgens [1] moeten we vinden dat $N_{-4,1} = 17/24$. De heuristische formule convergeert hier inderdaad naar. Zie figuur 11 voor een grafische weergave van

$$\{0.6572, 0.6639, 0.6619, 0.6602, 0.6669, 0.6649, 0.6661\}.$$

Ook voor negatieve $r = a/b$ ziet het er dus goed uit. De heuristiek heeft onze numerieke controle overleefd. Interessant is dat bij bijna alle gevallen er geen sprake is van fluctuatie om de verwachte uitkomst, maar dat de benaderingen steeds aan één kant lijken te liggen. Dit is een bekend verschijnsel en wordt de Chebyshev bias genoemd.

De dichtheid van de priemen congruent aan $a(\text{mod } d)$ met $(a, d) = 1$ is gelijk aan $1/\varphi(d)$. Er zijn $\varphi(d)$ van dat soort restklassen (zogenaamde primitieve restklassen). Dus iedere primitieve restklasse heeft asymptotisch gezien een zelfde dichtheid aan priemen. Het blijkt dat in de praktijk voor kleine d deze zogenaamde Chebyshev bias optreedt. Dat wil zeggen dat priemen er een voorkeur voor hebben om een niet-kwadraat mod d te zijn, boven een kwadraat mod d.

Met grotere d, in de orde van 100, verdwijnt dit effect.



Figuur 11: $H^{(2)}_{-4,1}(x)$ voor $x = e^6, e^7, ..., e^{12}$.

4 Conclusie

Er is een naïve heuristiek voor $N_{a,b}(x)$ die in veel, maar niet alle, gevallen asymptotisch exact is. Er is een kwadratische modificatie van deze heuristiek, die gebruik maakt van het Legendre symbool, die altijd asymptotisch exact is. Deze kwadratische modificatie heeft onze toets der numerieke simulatie goed doorstaan.

Referenties

[1] P.Moree, Asymptotically exact heuristic for prime divisors of the sequence $\{a^k + b^k\}_{k=1}^{\infty}$, (2003), [arXiv:math.NT/0311483].

[2] C. Hooley, Artin's conjecture for primitive roots, *J. Reine Angew. Math.* **225** (1967), 209-220.

[3] P.Moree, On primes in arithmetic progression having a prescribed primitive root, *J. Number Theory* **78** (1999), 85-98.