Numerieke benadering van constanten in de getaltheorie

Charles Mathy en Vincent van der Noort
Begeleider: Dr. Pieter Moree

Samenvatting

Ons doel is het uitrekenen van constanten van de vorm $\prod_{p>p_n}(1-\frac{f(p)}{g(p)})$. f en g zijn monische polynomen in $\mathbb{Z}[t]$, en het product loopt over alle priemgetallen groter of gelijk aan een startpriem p_{n+1}. Rechtstreeks uitrekenen convergeert te langzaam: daarom is het nuttig om de constanten te herschrijven, in de vorm van $\prod_{j=2}^{\infty}\zeta_n(j)^{e_j}$, met ζ_n de Partiele Riemann Zeta functies.
De theorie wordt in dit verslag uitgewerkt, met bewijzen. Het blijkt uit de theorie dat de getallen e_j gehele getallen zijn.
Er zal ook uitgelegd worden hoe men een programma schrijft dat de constanten uitrekent.
Daarnaast wordt er speciale aandacht besteed aan de priemtweelingconstante en Artin-constante.

Inhoudsopgave

Hoofdstuk 1

Inleiding

In de getaltheorie probeert de mensheid al eeuwen grip te krijgen op het onvoorspelbare gedrag van positieve gehele getallen. Nergens vindt men zoveel onbewezen vermoedens als hier. Veel van deze vermoedens hebben betrekking op getallen met bepaalde eigenschappen. Het is meestal niet duidelijk hoeveel er van deze soort getallen zijn, en waar ze zich bevinden. Dan dient er zich op natuurlijke wijze het concept dichtheid aan: de frequentie waarmee deze bijzondere getallen voorkomen in de eerste N getallen, als N nadert tot oneindig. Dit is vaak het enige waar men nog wat zinnigs over kan zeggen.

In de getaltheorie heeft men ontdekt, dat veel van de bestudeerde dichtheden een bepaalde bijzondere vorm hebben: ze zijn namelijk te schrijven als een oneindig product over alle priemgetallen, vanaf een startpriem p_{n+1}:

$$C_F(n) = \prod_{p>p_n}^{\infty} F(p)$$

F is een functie, de getallen p zijn priemgetallen, en p_k is het k-de priemgetal:

$$p_1 = 2, p_2 = 3, ...$$

Hier zijn een paar voorbeelden van constanten van deze vorm:

$\prod_{p>1}^{\infty}(1 - \frac{1}{p(p-1)})$ Artin-constante

$\prod_{p>1}^{\infty}(1 - \frac{1}{p^2(p-1)})$ #2 Artin-constante

$\prod_{p>2}^{\infty}(1 - \frac{1}{(p-1)^2})$ Priemtweelingconstante

$\prod_{p>3}^{\infty}(1 - \frac{3p-1}{(p-1)^3})$ Hardy Littlewood constante C_3

$\prod_{p>3}^{\infty}(1 - \frac{6p^2-4p+1}{(p-1)^4})$ Hardy Littlewood constante C_4

$\prod_{p>1}^{\infty}(1-\frac{1}{p(p+1)})$ "Carefree"constante

$\prod_{p>1}^{\infty}(1-\frac{1}{(p+1)^2})$ "Strongly Carefree"constante

$\prod_{p>1}^{\infty}(1-\frac{p^9-(p-1)^7(p^2+7p+1)}{p^9})$ Constante van Heath-Brown en Moroz

In hoofdstuk 3 wordt er in detail getreden over de Artin-constante en de priemtweelingconstante.

Het kan zo zijn dat zo'n constante divergeert (Bijoorbeeld: voor F(p)=p). De constanten die wij behandelen, convergeren. Voor de hand ligt, deze constantes te benaderen door de achtereenvolgende termen met elkaar te vermenigvuldigen. Dit is over het algemeen niet de meest efficiente manier: wanneer men tot een zeer grote nauwkeurigheid wil komen (1000 decimalen achter de komma) is een computer al gauw maanden bezig. Er kan bewezen worden dat de convergentie van het rechtstreeks vermenigvuldigen heel traag is.

Er is een betere methode voor het benaderen van constanten van de volgende vorm:

$$\prod_{p>p_n}^{\infty}(1-\frac{f(p)}{g(p)})$$

met f en g polynomen $\in \mathbb{Z}[t]$, met graad(f) + 2 $\leq$ graad(g). Merk op dat de voorbeelden hierboven allemaal deze vorm hebben.

De eerste stap is het herschrijven van het product, als een product van partiele zeta functies ζ_n. De partiele zeta functies $\zeta_n(j)$ lijken sterk op de Riemann-zeta functie $\zeta(j)$. Ze zijn als volgt gedefinieerd:

$$\zeta(j)=\sum_{k=1}^{\infty}k^{-j}=\prod_{k=1}^{\infty}\frac{1}{1-p_k^{-j}}$$

$$\text{en } \zeta_n(j):=\zeta(j)\times\prod_{k=1}^{n}(1-p_k^{-j})=\prod_{k=n+1}^{\infty}\frac{1}{1-p_k^{-j}}$$

Het oorspronkelijke product kan dan herschreven worden:

$$\prod_{p>p_n}^{\infty}(1-\frac{f(p)}{g(p)})=\prod_{j=2}^{\infty}\zeta_n(j)^{e_j}$$

De coefficienten e_j worden theoretisch bepaald en blijken gehele getallen te zijn.

Deze methode kan nog verder verbeterd worden. Je kunt tijd besparen door de constante niet vanaf p_{n+1}, maar vanaf een grotere p_{m+1} uit te rekenen (m > n). Naarmate m groter wordt, wordt de gewenste nauwkeurigheid sneller bereikt. Om de echte constante eruit te krijgen, moet de uitkomst echter nog wel vermenigvuldigd worden met het product over de overgeslagen priemgetallen: $\prod_{p_n<p\leq p_m}(1-\frac{f(p)}{g(p)})$. Omdat dit een product is over eindig veel getallen, rekenen we dit gewoon uit door de termen met elkaar te vermenigvuldigen. Voor dit deel van het product geldt dus juist dat de rekentijd stijgt, naarmate m groter wordt.

Een goede keuze van de waarde van m kan leiden tot een totale rekentijd van een half uur. Dit is een duidelijke verbetering ten opzichte van de rechtstreekse vermenigvuldiging. Welke keuze van m de gewenste nauwkeurigheid oplevert in zo weinig mogelijk rekentijd, is echter niet van tevoren voorspelbaar. Daarom gaan wij in dit project op zoek naar de beste waarde voor m, bij berekening van de priemtweelingconstante.

Hoofdstuk 2

Theorie

2.1 Het idee

De constanten die wij behandelen zijn van de vorm

$$C_{f,g}(n) = \prod_{p>p_n} (1 - \frac{f(p)}{g(p)})$$

waarin de getallen p priem zijn. Als de constante rechtstreeks uitgerekend wordt, is de convergentie tragisch traag. Als men de constante herschrijft in de vorm

$$\prod_{j=2}^{\infty} \zeta_n(j)^{e_j}$$

en dan de factoren van dit product met elkaar vermenigvuldigt, is de convergentie volgens de theorie sneller. En de constante kan inderdaad in deze vorm herschreven worden, zoals later blijkt. Het blijkt ook dat de getallen e_j geheel zijn.

2.2 Achtergrondkennis

Een beetje wiskundige kennis is nodig om de theorie te begrijpen. Deze kennis wordt nu uiteengezet. Maar eerst een beetje notatie.

Notatie

Noem $(p_n)_{n=1}^{\infty}$ de rij van alle priemgetallen: $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$
Elk getal n $\in \mathbb{N}$ kan op eenduidige wijze ontbonden worden in priemfactoren:

$$n = p_1^{a_1} p_2^{a_2} \ldots$$

met $a_i \in \mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$

2.2.1 De Partiele Riemann Zeta functie

Riemann zeta functie

De Riemann zeta functie is gedefinieerd als

$$\zeta(j) = \sum_{k=1}^{\infty} k^{-j} \tag{2.1}$$

Bijvoorbeeld

$$\zeta(1) = 1 + \frac{1}{2} + \frac{1}{3} + \cdots = \infty$$
$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \cdots = \frac{\pi^2}{6}$$
$$\zeta(3) = 1 + \frac{1}{8} + \frac{1}{27} + \cdots = 1.2020569\ldots$$

De $\zeta(j)$'s met even j zijn volledig bepaald. Voor oneven j bestaan er benaderingen, dankzij bijvoorbeeld Ramanujan (of, volgens hem, dankzij de Indiase godin Namagiri, die hem in zijn dromen inspireerde ...).

Dankzij Euler weten we dat $\zeta(j)$ herschreven kan worden als een oneindig product, over alle priemgetallen:

$$\zeta(j) = \prod_p \frac{1}{1-p^{-j}} = \prod_{k=1}^{\infty} \frac{1}{1-p_k^{-j}} \tag{2.2}$$

Het product wordt hier in twee equivalente representaties weergegeven.

Dit is een heel handige manier om de zeta functie op te schrijven: dat de formule klopt, wordt duidelijk wanneer men herkent dat $\frac{1}{1-p^{-j}}$ een meetkundige reeks is met rede p^{-j}. Kijk in de Appendix: sectie 5.1.2. voor uitleg.

Partiele Riemann Zeta functie

$\zeta_n(j)$ is de partiele Riemann Zeta functie en lijkt sterk op $\zeta(j)$:

$$\zeta_n(j) := \prod_{p>p_n} \frac{1}{1-p-j} = \prod_{k=n+1}^{\infty} \frac{1}{1-p_k^{-j}} \tag{2.3}$$

Nu is het makkelijk om $\zeta_n(j)$ te schrijven in termen van $\zeta(j)$. Volgens (2.2)

$$\zeta(j) = \prod_{k=1}^{\infty} \frac{1}{1-p_k^{-j}}$$

Dus

$$\zeta_n(j) = \zeta(j) \prod_{k=1}^{n} (1-p_k^{-j}) \tag{2.4}$$

Opgave: wat is $\zeta_0(j)$? Antwoord:

$$\zeta_0(j) = \prod_{k=1}^{\infty} \frac{1}{1 - p_k^{-j}} = \zeta(j)$$

2.2.2 Möbius inversie

De Möbius μ-functie

De Möbius μ-functie werkt op natuurlijke getallen, en vertelt iets over de ontbinding van deze getallen in priemfactoren.

Wij hebben al opgemerkt dat een getal n $\in \mathbb{N}$ op eenduidige wijze ontbonden kan worden in priemfactoren:

$$n = p_1^{a_1} p_2^{a_2} \dots$$

De Möbius μ-functie is gedefinieerd volgens

$$\mu : \mathbb{N} \mapsto \{-1, 0, 1\}$$
$$\mu(1) = 1$$

$$\mu(n) = \begin{cases} 0 & \text{als een van de getallen } a_i \geq 2 \text{ is} \\ -1 & \text{als alle } a_i \leq 1 \text{ zijn en het aantal } p_i \text{ met } a_i = 1 \text{ oneven is} \\ 1 & \text{als alle } a_i \leq 1 \text{ zijn en het aantal } p_i \text{ met } a_i = 1 \text{ even is} \end{cases}$$

Möbius inversie

Möbius inversie is een trucje dat je in de getaltheorie tegenkomt.

Neem twee functies f(n) en g(n) zodanig dat

$$f(n) = \sum_{k|n} g(k)$$

'$k|n$' betekent 'k deelt n'. De som loopt dus over alle positieve delers van n (bv neem n = 6, dan k = 1, 2, 3, 6). Dan geldt

$$g(n) = \sum_{k|n} \mu(\frac{n}{k}) f(k)$$

In hoofdstuk 5.2 wordt in detail getreden over de Möbius μ-functie en wordt Möbius inversie bewezen.

2.3 Het echte werk

Neem een polynoom

$$F(t) = t^\delta + a_1 t^{\delta-1} + \ldots + a_\delta$$

Dit is een monisch polynoom $\in \mathbb{Z}[t]$: monisch omdat de factor vóór t^δ 1 is; in $\mathbb{Z}[t]$ omdat de coefficienten a_i in $\mathbb{Z}$ zitten. Men noemt δ de graad van F, $\delta \in \mathbb{N}$.

Volgens de Hoofdstelling van de Algebra heeft F δ nulpunten in $\mathbb{C}$: noem ze $\alpha_1, \alpha_2, \ldots, \alpha_\delta$. Deze nulpunten hoeven niet allemaal verschillend te zijn. F(t) wordt vaak als volgt herschreven:

$$F(t) = \prod_{j=1}^{\delta}(t - \alpha_j)$$

2.3.1 Newton recursie

Definieer

$$s_F(k) = \alpha_1^k + \ldots + \alpha_\delta^k$$

Dan geldt dat $s_F(k)$ in $\mathbb{Z}$ zit en aan de volgende recursie relatie voldoet

$$s_F(k) + a_1 s_F(k-1) + \ldots + a_{k-1} s_F(1) + k a_k = 0 \tag{2.5}$$

met $a_{\delta+1} = a_{\delta+2} = \ldots = 0$. Dankzij deze formule is het duidelijk dat de getallen $s_F(k)$ geheel zijn, omdat de getallen a_i geheel zijn. In deze relatie komen de nulpunten van F niet voor: Men hoeft de nulpunten van F dus niet te kennen om $s_F(k)$ uit te rekenen! Deze recursie relatie was Newton al bekend.

2.3.2 Reciproke polynoom herschrijven

Reciproke polynoom

Het reciproke polynoom van F(t) is $\widehat{F}(t)$. Het wordt gedefinieerd als

$$\widehat{F}(t) = t^\delta F(\frac{1}{t}) = 1 + a_1 t + \ldots + a_\delta t^\delta$$

Het is eigenlijk F(t) met de coefficienten gespiegeld. $\widehat{F}(t)$ kan herschreven worden in termen van de nulpunten van F(t) :

$$\widehat{F}(t) = \prod_{j=1}^{\delta}(1 - \alpha_j t)$$

Voorbeeld

Neem $F(t) = t^3 + t^2 - 6t$. Dan zijn de nulpunten

$$\alpha_1 = 0, \alpha_2 = 2, \alpha_3 = -3$$

Volgens de introductie van 2.3 kan F dan gefactoriseerd worden:

$$F(t) = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3) = t(t-2)(t+3)$$

Dan is het reciproke polynoom

$$\widehat{F}(t) = t^3 F(\frac{1}{t}) = 1 + t - 6t^2$$

Merk op dat de graad van $\widehat{F}$ kleiner is dan de graad van F. Dit is het geval als $a_\delta = 0$, dus als t=0 een nulpunt is van F (Ga dit na).
We hadden gezien dat $\widehat{F}(t)$ herschreven kon worden in termen van de nulpunten van F. Laten we zien of de formule hier geldt:

$$(1-\alpha_1 t)(1-\alpha_2 t)(1-\alpha_3 t) = (1-0)(1-2t)(1+3t) = 1 + t - 6t^2 = \widehat{F}(t)$$

Het klopt dus.
Opgave: Wat zijn de nulpunten van $\widehat{F}(t)$ voor een willekeurig monisch polynoom F in $\mathbb{Z}[t]$?
Antwoord: $\widehat{F}(t) = t^\delta F(\frac{1}{t})$.
De nulpunten van $\widehat{F}(t)$ zijn dus de inversen van de nulpunten van F, die ongelijk 0 zijn: $\frac{1}{\alpha_j}$. Kijk of dit klopt voor het vorige voorbeeld.

Een slag in de lucht

Neem een willekeurige getal α. Probeer getallen $\vartheta_k \in \mathbb{R}$ te vinden om $1 - \alpha t$ te herschrijven:

$$1 - \alpha t = \prod_{k=1}^{\infty} (1 - t^k)^{\vartheta_k} \tag{2.6}$$

Wat moet er voor de getallen ϑ_k gelden?
Neem van (2.6) links en rechts de logaritme, en dan de afgeleide:

$$\begin{aligned} \log(1-\alpha t) &= \log(\prod_{k=1}^{\infty}(1-t^k)^{\vartheta_k}) \\ &= \sum_{k=1}^{\infty} \vartheta_k \log(1-t^k) \\ \frac{-\alpha}{1-\alpha t} &= \sum_{k=1}^{\infty} \frac{\vartheta_k(-k)t^{k-1}}{(1-t^k)} \\ &= -\sum_{k=1}^{\infty} \frac{\vartheta_k k t^{k-1}}{1-t^k} \end{aligned}$$

Vermenigvuldig links en rechts met $-t$:

$$\frac{\alpha t}{1-\alpha t} = \sum_{k=1}^{\infty} k\vartheta_k \frac{t^k}{1-t^k}$$

Men herkent links een meetkundige reeks, met reden αt (zie Hoofdstuk 5.2). Men herkent ook rechts een meetkundige reeks, met reden t^k.

$$\sum_{i=1}^{\infty}(\alpha t)^i = \sum_{k=1}^{\infty} k\vartheta_k \sum_{j=1}^{\infty}(t^k)^j$$

De formules links en rechts van de gelijkteken zijn van de vorm $\sum_{n=1}^{\infty} a_n t^n$. Bij iedere n moeten de factoren vóór t^n links en rechts gelijk zijn.

Links is de factor vóór t^n gelijk aan α^n. Rechts is de factor vóór t^n gelijk aan $\sum_{k|n} k\vartheta_k$ (k moet n delen, anders kan de exponent van t, kj, nooit gelijk aan n zijn). Dus

$$\alpha^n = \sum_{k|n} k\vartheta_k$$

Het is nu eindelijk tijd om Möbius inversie toe te passen, om een formule voor ϑ_n te krijgen:

$$n \cdot \vartheta_n = \sum_{k|n} \alpha^k \mu(\frac{n}{k})$$

$$\Rightarrow \vartheta_n = \frac{1}{n}\sum_{k|n} \alpha^k \mu(\frac{n}{k})$$

En nu $\widehat{F}(t)$ zo schrijven

In de vorige sectie is bewezen hoe $1-\alpha t$ met de goede exponenten ϑ_k herschreven kan worden als $\prod_{k=1}^{\infty}(1-t^k)^{\vartheta_k}$.

Het reciproke polynoom van F(t) kon geschreven worden in termen van de nulpunten van F(t):

$$\widehat{F}(t) = \prod_{j=1}^{\delta}(1-\alpha_j t)$$

Volgens de vorige sectie geldt voor elke factor $1-\alpha_j t$:

$$1-\alpha_j t = \prod_{n=1}^{\infty}(1-t^n)^{\vartheta_{j,n}}$$

met $\vartheta_{j,n} = \frac{1}{n}\sum_{k|n}\alpha_j^k\mu(\frac{n}{k})$. Pas dit toe op elke factor van $\widehat{F}(t)$:

$$\widehat{F}(t) = \prod_{n=1}^{\infty}(1-t^n)^{\vartheta_{1,n}} \prod_{n=1}^{\infty}(1-t^n)^{\vartheta_{2,n}} \cdots \prod_{n=1}^{\infty}(1-t^n)^{\vartheta_{\delta,n}}$$

Door de exponenten van $(1-t^n)$ voor elke n samen te brengen krijgt men

$$\widehat{F}(t) = \prod_{n=1}^{\infty}(1-t^n)^{b_F(n)} \tag{2.7}$$

met

$$b_F(n) = \frac{1}{n}\sum_{k|n}(\alpha_1^k + \alpha_2^k + \cdots + \alpha_\delta^k)\mu(\frac{n}{k})$$

Hierin herkennen we de getallen $s_F(k)$, gedefinieerd in 2.3.1:

$$s_F(k) = \alpha_1^k + \ldots + \alpha_\delta^k$$

Dus

$$b_F(n) = \frac{1}{n}\sum_{k|n} s_F(k)\mu(\frac{n}{k})$$

Dit is goed nieuws, omdat we dan de nulpunten van F niet hoeven te kennen om $b_F(n)$ uit te rekenen. We weten ook dat de getallen $s_F(k)$ geheel zijn, en dat maakt het uitrekenen van $b_F(n)$ voor een computer makkelijker.
Maar het samenbrengen van de exponenten mag eigenlijk niet zomaar: men kan de factoren van een oneindig product alleen in een andere volgorde zetten als het product convergeert.
Trouwens, zijn de getallen $b_F(n)$ geheel? Het volgende lemma zegt van wel.

Lemma over $b_F(n)$

Het blijkt dat de getallen $b_F(n)$ gehele getallen zijn! $b_F(n) \in \mathbb{Z}$. Dit wordt hier niet bewezen. Een bewijs is te vinden in het artikel van Dr. Pieter Moree [1].

2.3.3 Zeta verschijnt

In de vorige sectie is heel belangrijke vooruitgang geboekt. Er resteert nu alleen het toepassen van onze kennis, en het bestuderen van zaken zoals convergentie. Het gaat nu gebeuren: het herschrijven van de constante

$$C_{f,g}(n) = \prod_{p>p_n}(1 - \frac{f(p)}{g(p)}) \quad \text{naar} \quad \prod_{j=2}^{\infty}\zeta_n(j)^{e_j}$$

Daarvoor wordt de volgende stelling gebruikt. Omdat ons hele verslag berust op deze stelling noemen wordt zij de centrale stelling genoemd.

De centrale stelling

Neem f(t), g(t) $\in \mathbb{Z}[t]$ twee monische polynomen waarvoor geldt graad(f) + 2 $\leq$ graad(g). Neem alle wortels van g-f en g: deze wortels zitten in $\mathbb{C}$, en hebben een modulus (een lengte). Neem van deze wortels de wortel met de grootste modulus: noem zijn modulus β. Neem een geheel getal n_0 zo dat $p_{n_0+1} > \beta$. Dan geldt voor n alle $\geq n_0$

$$C_{f,g}(n) = \prod_{p>p_n}(1 - \frac{f(p)}{g(p)}) = \prod_{j=2}^{\infty}\zeta_n(j)^{b_g(j)-b_{g-f}(j)} \tag{2.8}$$

Het bewijs is heel interessant, maar ook heel lang. Hieronder zullen we het bewijs weergeven. We zullen alleen om het leesbaar te houden sommige tussenbewijzen niet hier laten zien. De overgeslagen bewijzen zijn in sectie 5.3. te vinden.

Reciproke polynomen in de constante

Neem twee monische polynomen in $\mathbb{Z}[t]$, f(t) en g(t), zodanig dat graad(f)+2 $\leq$graad(g). $\widehat{f}(t)$ en $\widehat{g}(t)$ zijn hun respectievelijke reciproke polynomen. Noem nu

$$h(t) = 1 - \frac{f(t)}{g(t)} = \frac{g(t) - f(t)}{g(t)}$$

Noem $r = \frac{1}{t}$. De teller en noemer van $h(r)$ kunnen allebei worden herschreven met behulp van onderstaande formule voor reciproke polynomen, die in hoofdstuk 2.3.2 is afgeleid:

Als F(t) een polynoom is dan geldt voor het reciproke-polynoom $\widehat{F}(t)$

$$\widehat{F}(t) = \prod_{n=1}^{\infty}(1 - t^n)^{b_F(n)}$$

met

$$b_F(n) = \frac{1}{n}\sum_{k|n} s_F(k)\mu(\frac{n}{k})$$

We gebruiken $r = \frac{1}{t}$, omdat we de theorie van reciproke polynomen gaan gebruiken. Reciproke polynomen zijn een functie van F($\frac{1}{t}$), en het gebruiken van r maakt de formules die hier volgen een beetje leesbaarder.

$$\widehat{F}(t) = t^{\delta}F(r)$$

met δ de graad van F, en $r = \frac{1}{t}$.

We herschrijven nu de teller en noemer van

$$h(r) = \frac{g(r) - f(r)}{g(r)} \tag{2.9}$$

De teller $= g(r) - f(r)$. Noem δ de graad van g. Wat is $\widehat{g-f}(t)$, het reciproke polynoom van g(t) - f(t)? δ is strikt groter dan de graad van f, volgens de eis

$$\text{graad}(f) + 2 \leq \text{graad}(g)$$

Dus de graad van g(t) - f(t) is δ. Dan geldt per definitie

$$\widehat{g-f}(t) = t^{\delta}(g(r) - f(r)) \Rightarrow g(r) - f(r) = t^{-\delta}\widehat{g-f}(t)$$

Pas nu vergelijking (2.7) toe op $\widehat{g-f}(t)$:

$$g(r) - f(r) = t^{-\delta}\widehat{g-f}(t) = t^{-\delta}\prod_{k=1}^{\infty}(1 - t^k)^{b_{g-f}(k)}$$

met

$$b_{g-f}(k) = \frac{1}{k}\sum_{d|k} s_{g-f}(d)\mu(\frac{k}{d})$$

De noemer $= g(r)$. $\widehat{g}(t)$, het reciproke polynoom van g(t), is per definitie $t^{\delta}g(r)$. Dus geldt volgens (2.7)

$$g(r) = t^{-\delta}\widehat{g}(t) = t^{-\delta}\prod_{k=1}^{\infty}(1-t^k)^{b_g(k)}$$

met

$$b_g(k) = \frac{1}{k}\sum_{d|k} s_g(d)\mu(\frac{k}{d})$$

Vul deze twee formules in (2.9), de formule voor h(r), in :

$$h(r) = \frac{t^{-\delta}\prod_{k=1}^{\infty}(1-t^k)^{b_{g-f}(k)}}{t^{-\delta}\prod_{k=1}^{\infty}(1-t^k)^{b_g(k)}} = \prod_{k=1}^{\infty}(1-t^k)^{b_{g-f}(k)-b_g(k)}$$

Vul in t = $\frac{1}{r}$:

$$h(r) = \prod_{k=1}^{\infty}(1-r^{-k})^{b_{g-f}(k)-b_g(k)}$$

Vul in $p = r$:

$$h(p) = \prod_{k=1}^{\infty}(1-p^{-k})^{b_{g-f}(k)-b_g(k)}$$

De bewering is nu: $b_{g-f}(1) = b_g(1)$. Dit wordt bewezen in sectie 5.3.1., en volgt uit de eis: graad(f) + 2 $\leq$ graad(g).
Het gevolg is dat de eerste term van het product als exponent 0 heeft. Hij is dus gelijk aan 1, en kan weggelaten worden. Dan wordt de formule voor h(p)

$$h(p) = \prod_{k=2}^{\infty}(1-p^{-k})^{b_{g-f}(k)-b_g(k)}$$

De constanten $C_{f,g}(n)$ die wij willen uitrekenen, zijn van de vorm $\prod_{p>p_n} h(p)$. Vul hier de net gevonden formule voor h(p) in:

$$C_{f,g}(n) = \prod_{p>p_n}\prod_{j=2}^{\infty}(1-p^{-j})^{b_{g-f}(j)-b_g(j)}$$

Zeta verschijnt

Er staan hier nu twee oneindige producten achter elkaar. Als aan de voorwaarden van de centrale stelling voldaan is, is het mogelijk de volgorde van de producten te verwisselen zonder dat de uitkomst daardoor verandert. Waarom dit zo is, is zeer interessant en wordt uitgelegd in sectie 5.3.2. Onder de voorwaarden van de centrale stelling geldt nu dus:

$$C_{f,g}(n) = \prod_{j=2}^{\infty} \prod_{p>p_n} (1-p^{-j})^{b_{g-f}(j)-b_g(j)}$$

Dit kan in een iets meer suggestieve vorm geschreven worden door te gebruiken dat $a^b = (\frac{1}{a})^{-b}$:

$$C_{f,g}(n) = \prod_{j=2}^{\infty} \prod_{p>p_n} (\frac{1}{1-p^{-j}})^{b_g(j)-b_{g-f}(j)} = \prod_{j=2}^{\infty} (\prod_{p>p_n} \frac{1}{1-p^{-j}})^{b_g(j)-b_{g-f}(j)}$$

Hierin herkennen we opeens formule (2.3) voor partiele ζ-functies uit paragraaf 2.2.1. Als we het tweede product door de n-de partiele zeta-functie vervangen vinden we opeens:

$$C_{f,g}(n) = \prod_{j=2}^{\infty} \zeta_n(j)^{b_g(j)-b_{g-f}(j)}$$

Dit is de formule waar we al die tijd naar op zoek waren! Gelukkig begint het product bij j=2, omdat $\zeta(1)$ divergeert. Het bijzondere aan deze formule is dat er geen priemgetallen meer in voorkomen, maar dat het product gewoon netjes over de natuurlijke getallen loopt. Dat gegoochel met Möbius inversie en het zomaar omwisselen van de producttekens blijft natuurlijk dubieus. We raden daarom iedereen aan om ook hoofdstuk 5 te lezen!

2.4 In de praktijk

Nu de theorie ons een prachtige stelling biedt, is het tijd voor praktisch denken. Het doel van het hele verhaal is het zo snel mogelijk uitrekenen van de constantes met een precisie van duizend decimalen. Omdat een computer al het rekenwerk doet, is het belangrijk om ons algoritme te optimaliseren voor de computer. In dit opzicht kunnen nog twee verbeteringen worden aangebracht aan het verhaal tot nu toe.

2.4.1 Liever een som dan een product

Een computer sommeert meestal sneller dan hij vermenigvuldigt (wij ook). Het uitrekenen van de constante kan makkelijk tot een som worden teruggebracht, met behulp van de logaritme functie.

$$C_{f,g}(n) = \prod_{j=2}^{\infty} \zeta_n(j)^{b_g(j)-b_{g-f}(j)}$$

$$\log(C_{f,g}(n)) = \sum_{j=2}^{\infty}(b_g(j) - b_{g-f}(j))\log(\zeta_n(j))$$

Als de som eenmaal is uitgerekend, wordt de inverse functie van de logaritme, de exponentiele functie, toegepast.

2.4.2 Dom uitrekenen, tot op zekere hoogte

Als men $C_{f,g}(n)$ moet uitrekenen, is het soms slim om een $m > n$ te nemen, en $C_{f,g}(m)$ eerst uit te rekenen. Het is dan makkelijk om $C_{f,g}(n)$ uit te rekenen, door de missende factoren apart toe te voegen. Er geldt

$$C_{f,g}(n) = C_{f,g}(m)\prod_{p_n < p \leq p_m}(1 - \frac{f(p)}{g(p)})$$

Men is op zoek naar de optimale waarde van m. Een grafiek kan getekend worden, met de rekentijd uitgezet tegen de waarde van m, en dan is het minimum van het grafiek de beste m. De grafiek hoeft niet te ver door getekend te worden, omdat het duidelijk is dat voor zeer hoge m de convergentie zeer traag is. Anders zou dit hele verhaal helemaal niet nodig zijn.

Hoe groter m is, hoe langzamer $\prod_{p_n < p \leq p_m}(1 - \frac{f(p)}{g(p)})$ convergeert, en hoe sneller $C_{f,g}(m)$ convergeert.

Hoofdstuk 3

De priemtweelingconstante en de Artin-constante

In dit hoofdstuk proberen we enig idee te geven hoe en waar de constanten die we berekenen een rol spelen in de wiskunde, en hoe de oneindige producten waarmee ze geschreven worden, gevonden zijn.

3.1 De priemtweelingconstante

3.1.1 Wat is de priemtweelingconstante?

Een priemtweeling bestaat uit twee priemgetallen die 'naast elkaar liggen' zoals 11 en 13, 29 en 31, 41 en 43. Het lijkt erop dat er oneindig veel priemtweelingen zijn, maar dat is nooit bewezen, ondanks dat men het duizenden jaren lang geprobeerd heeft. De priemtweelingconstante komt voor in een formule voor het aantal priemtweelingen onder een gegeven (groot) getal x.

Noem

$$N_2(x) = \#\{0 < n < x : n,\ (n+2) \in\ P\}$$

het aantal priemtweelingen kleiner dan x. P is de verzameling van alle priemgetallen. Dan geldt, volgens een vermoeden van Hardy en Littlewood:

$$N_2(x) \sim 2T \int_2^x \frac{dt}{(\log t)^2}$$

waarin T de priemtweelingconstante voorstelt. Met $f(x) \sim g(x)$ wordt bedoeld dat $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. Omdat het nog nooit iemand gelukt is te bewijzen dat er oneindig veel priemtweelingen zijn, is het niet zeker dat de formule klopt, maar we kunnen wel een heuristische (dwz wiskundig niet helemaal nette, maar wel geloofwaardige) afleiding van deze formule geven, gebaseerd op de Priemgetalstelling.

De Priemgetalstelling en de kans dat een getal priem is

De Priemgetalstelling werd voor het eerst geformuleerd rond 1800 door Gauss en Legendre, en bewezen in 1896 door Hadamard en de la Vallee Poussin. Zij stelt dat het aantal priemgetallen onder een gegeven x, $\pi(x)$ genoemd, naarmate x groter wordt, gelijk gaat lopen met de volgende integraal:

$$\pi(x) \sim \int_2^x \frac{dt}{\log t}$$

Voor grote x kunnen we de integraal benaderen met de som $\sum_{n \leq x} \frac{1}{\log n}$, zodat

$$\pi(x) \sim \sum_{n \leq x} \frac{1}{\log n}$$

Heuristisch sprekend kunnen we nu zeggen dat de 'kans' dat een willekeurig groot getal n een priemgetal is, gelijk is aan 1/log n.

Dit klinkt nogal onzinnig. De kans dat een getal priem is, is natuurlijk 1 of 0: hij is priem of hij is het niet. Laten we het toch even aannemen: We gaan nu laten zien dat we onder deze aanname de Priemgetalstelling krijgen.

Wat is het aantal priemgetallen onder x? Maak een functie f van $\mathbb{N}$ naar {0,1}, met

$$f(n) = \begin{cases} 1 & \text{als n priem is} \\ 0 & \text{als n niet priem is} \end{cases}$$

Het aantal priemgetallen onder x is nu

$$\pi(x) = \sum_{n \leq x} f(n)$$

Stel dat we niet weten van ieder getal n of hij priem is of niet, maar we weten wel dat de kans dat n priem is gelijk is aan $\frac{1}{\log n}$. Dan kunnen we f benaderen met een functie g gedefinieerd volgens:

$$g(n) = \begin{cases} 1 & \text{met kans } \frac{1}{\log n} \\ 0 & \text{met kans } 1 - \frac{1}{\log n} \end{cases}$$

Voor $\sum_{n \leq x} g(n)$ zijn nu een heleboel verschillende uitkomsten mogelijk, maar één ervan, de verwachtingswaarde, is het meest waarschijnlijk. Voor grote x zegt de wet van de grote aantallen zelfs dat deze uitkomst steeds meer op deze verwachtingswaarde gaat lijken. Onder onze aanname is $\pi(x) = \sum_{n \leq x} f(n)$ zelfs een voorbeeld van zo'n mogelijke uitkomst, die voor grote x dus ook steeds meer op die verwachting moet gaan lijken.

Laten we eens kijken wat de verwachting van g is. Verwachting is de som over 'waarde maal kans op die waarde'. De mogelijke waarden van g zijn 1 en 0, zodat de verwachting gelijk is aan

$$\sum_{n \leq x} (1 \cdot \frac{1}{\log n} + 0 \cdot (1 - \frac{1}{\log n})) = \sum_{n \leq x} \frac{1}{\log n}$$

Dus op grond hiervan verwachten we dat voor grote x geldt dat

$$\pi(x) = \sum_{n \leq x} f(n) \sim \sum_{n \leq x} \frac{1}{\log n}$$

En dat is precies wat de priemgetalstelling al zei! Dit 'rechtvaardigt' onze aanname.

Omdat dit rare idee van 'de kans dat een getal priem is' ons precies de priemgetalstelling teruggeeft, kan het bruikbaar zijn om eigenschappen van priemgetallen te voorspellen. Kijk naar het volgende voorbeeld.

Voorbeeld
Maak voor grote n een schatting van

$$\sum_{p \leq n} \frac{1}{p}$$

met de getallen p priem. Als de kans dat p priem is gelijk is aan $\frac{1}{\log n}$, dan kunnen we die som schrijven als

$$\sum_{m \leq n} \frac{1}{m} \cdot \mathrm{P(m\ priem)} = \sum_{m \leq n} \frac{1}{m \log m}$$

P(m priem) is de kans dat m priem is. Je kunt voor jezelf met een programma zoals Mathematica nagaan of dit ongeveer klopt, voor grote n.

De kans op een priemtweeling

We hebben nu een schatting van de kans dat een getal n priem is. Wat is de kans dat n+2 ook priem is, dus dat n en n+2 een priemtweeling vormen? Deze kans is gelijk aan de kans dat n een priemgetal is vermenigvuldigd met de kans dat n + 2 een priemgetal is *als je al weet dat n een priemgetal is.* Dus

$$P(n, n+2\,\text{priem}) = P(n\,\text{priem}) \cdot P(n+2\,\text{priem}|n\,\text{priem})$$

P(A | B) betekent "de kans op A als je al B weet".
P(n priem) weten we al: die is $\frac{1}{\log n}$. Over P(n + 2 priem | n priem) wordt gesteld dat

$$P(n+2\,\text{priem} \mid n\,\text{priem}) = 2 \cdot T \cdot P(n+2\,\text{priem})$$

met T de priemtweelingconstante. 2 T is de factor waarmee de kans dat n + 2 priem is verandert, doordat je weet dat n priem is.

3.1.2 berekening van T

Hoeveel wordt die kans nou groter of kleiner? Dat zien we door te kijken naar de waarde van n + 2 modulo een kleiner priemgetal p.

Modulo 2

We nemen aan dat n een groot getal is, in het bijzonder groter dan 2. Normaal gesproken is de kans dat $n+2$ even is 1/2 en de kans dat n oneven is ook. Als $n+2$ even is, is het in elk geval geen priemgetal. Nu we echter weten dat n een priemgetal is, en dus oneven, is de kans dat $n+2$ even is 0 geworden. En dus is de "kans"dat $n+2$ oneven en dus mogelijk een priemgetal is, van 1/2 veranderd in 1, en dus twee keer zo groot geworden. Dat is de factor 2 in de uitdrukking $2.T$.

Modulo 3

Nu kijken we modulo 3. Normaal gesproken is de kans dat $n+2 \equiv 1 \pmod 3$ gelijk aan 1/3, de kans dat $n+2 \equiv 2 \pmod 3$ is ook 1/3 en de kans dat n + 2 deelbaar is door 3 ook. De kans dat n + 2 op basis van deze gegevens in elk geval niet priem is, is dus 1/3: dit is alleen het geval als n + 2 deelbaar is door 3.

Als we nu echter al weten dat n priem is, en dus niet deelbaar door drie, weten we dus ook dat n + 2 niet congruent is aan 2 (mod 3). Er zijn dus nog twee mogelijkheden over: $n+2 \equiv 1 \pmod 3$ en $n+2$ is deelbaar door 3, elk met kans 1/2.

De kans dat n + 2 zeker geen priem is, verandert dus van 1/3 naar 1/2 en de kans dat n + 2 misschien wel priem is verandert dus van 2/3 in 1/2. Deze kans wordt dus 3/4 keer zo groot.

Modulo p

Ditzelfde kunnen we doen modulo alle priemgetallen p. Normaal gesproken zijn er p mogelijkheden, waarvan in 1 mogelijkheid (n + 2 deelbaar door p) geldt dat n + 2 in elk geval niet priem is. De kans dat n + 2 misschien wel priem is, is op basis van deze informatie dus $\frac{p-1}{p}$.

Als we nu weten dat n een priemgetal is, en dus niet deelbaar door p, dan weten we dat n + 2 niet congruent 2 (mod p) is. Het aantal mogelijkheden modulo p voor n + 2 is nu dus nog maar p - 1 en nog steeds geldt dat $n+2$ in *één* van deze mogelijkheden zeker niet priem is. De kans dat n + 2 misschien wel priem is, is nu dus nog maar $\frac{p-2}{p-1}$.

De verandering van de kans door de de wetenschap dat n priem is, is dus

$$\frac{(\frac{p-2}{p-1})}{(\frac{p-1}{p})} = \frac{p(p-2)}{(p-1)^2} = \frac{(p-1)^2-1}{(p-1)^2} = 1 - \frac{1}{(p-1)^2}$$

Dit is alleen de bijdrage aan de verandering van de kans die je vindt door modulo p te kijken. Om de totale verandering van de kans te weten moeten we deze bijdragen over alle priemgetallen $p > 2$ met elkaar vermenigvuldigen, dus

$$T = \prod_{p>2} (1 - \frac{1}{(p-1)^2})$$

Voor de totale kans stellen we dat P(n + 2 priem) = P(n priem) (voor n groot is die 2 toch verwaarloosbaar) zodat de kans op een priemtweeling

$$P(\text{n, n+2 priem}) = P(\text{n + 2 priem} \mid \text{n priem}) \cdot P(\text{n priem})$$

$$= 2 \cdot T \cdot \frac{1}{\log n} \cdot \frac{1}{\log n} = 2 \cdot T \cdot \frac{1}{(\log n)^2}$$

Het verwachte aantal priemtweelingen onder een getal x is dan de som van 2 tot x over deze kans:

$$N_2(x) \sim \sum_{n \leq x} 2T \frac{1}{(\log n)^2}$$

Deze som kan voor grote x benaderd worden door een integraal, zodanig dat het quotiënt van de som en de integraal naar 1 gaat als x naar oneindig gaat. Omdat 2 en T toch constantes zijn kunnen we ze voor het integraalteken halen, zodat het volledige Hardy-Littlewood-vermoeden luidt:

$$N_2(x) \sim 2 \prod_{p>2} (1 - \frac{1}{(p-1)^2}) \int_2^x \frac{dt}{(\log t)^2}$$

Dit is door computers voor grote x doorgerekend, en het lijkt te kloppen. Maar dat is geen bewijs. Wie zegt ons nou dat er oneindig veel priemtweelingen zijn? Dat blijft onbewezen. Stel dat er eindig veel priemtweelingen zouden zijn: dan wordt het vermoeden een steeds slechtere afschatting naarmate x groter wordt.

3.2 De Artin-constante

3.2.1 Het vermoeden van Artin

De Artin-constante speelt een rol in het vermoeden van Artin. Emil Artin (1898 - 1962) poneerde zijn vermoeden in 1927 en sindsdien hebben vele wiskundigen geprobeerd het te bewijzen. In 1967 bewees Hooley[4] het vermoeden onder aanname van de Gegeneraliseerde Riemann Hypothese.

Definitie: Zij G een groep met bewerking '$\cdot$' en a een element van G. Dan zeggen we dat a G *voortbrengt* of a *een voortbrenger is van* G als

$$G = \{\dots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^1, a^2, a^3, \dots\}$$

'1' is het eenheidselement van G.
Let op: niet iedere groep heeft maar één voortbrenger. Sommige groepen (zoals $\mathbb{R}$) hebben er zelfs overaftelbaar veel.

Zij p een priemgetal. Dan is $(\mathbb{Z}/p\mathbb{Z})^*$ een cyclische groep van orde p - 1 met vermenigvuldiging als bewerking. Merk op: De orde van een groep is het aantal elementen in de groep. De orde van een element a is het kleinste getal n waarvoor geldt: $a^n = 1$.

Stelling Een cyclische groep van orde p - 1 bevat minstens 1 element van orde p - 1, en zo'n element is een voortbrenger van de groep. Gauss bewees dit in 1801.

Stel dat $\overline{a}$ een voortbrenger is van $(\mathbb{Z}/p\mathbb{Z})^*$. Notatie: $(\mathbb{Z}/p\mathbb{Z})^* =< \overline{a} >$. Dan geldt dat $(\mathbb{Z}/p\mathbb{Z})^*$ precies bestaat uit de elementen $\overline{a}, \overline{a}^2, ... \overline{a}^{(p-2)}, \overline{a}^{(p-1)} \equiv \overline{1}$. Dit laatste gelijkteken zorgt ervoor dat $(\mathbb{Z}/p\mathbb{Z})^*$ precies uit p-1 elementen bestaat. Het is gebaseerd op de volgende stelling.

Stelling: $\overline{a}^{p-1} \equiv \overline{1}$ voor alle a ongelijk $0 \in \mathbb{Z}$ en alle priemgetallen p. Dit werd bewezen door Pierre de Fermat in 1640. Het staat bekend als de kleine stelling van Fermat. Deze stelling wordt ook wel genoteerd als: $a^p \equiv a$ (mod p) voor alle a in $\mathbb{Z}$.

Definitie: Als a een getal is waarvan de restklasse $\overline{a}$ de cyclische groep $(\mathbb{Z}/p\mathbb{Z})^*$ voortbrengt, dan heet a een *primitieve wortel modulo p*. Dus a is een primitieve wortel modulo p dan en slechts dan als a (mod p), a^2 (mod p), ... a^{p-1} (mod p) allen ongelijk zijn.

Lemma a is een primitieve wortel modulo p $\Leftrightarrow$ voor alle k $\in \mathbb{Z}$ met 0 < k < p - 1 geldt: $a^k \neq 1$(mod p).

Bewijs: Naar rechts is het duidelijk. Namelijk: a is een primitieve wortel modulo p betekent: voor alle k en m ongelijk en kleiner dan p geldt $a^k \neq a^m$. Dus in het bijzonder: $a^k \neq a^{p-1}$ als k < p - 1. En $a^{p-1} \equiv 1$ volgens de kleine stelling van Fermat.
Naar links: We moeten het volgende bewijzen: neem twee getallen k en m in {1, 2, ..., p-1} met k $\neq$ m. Dan moet gelden $a^k \neq a^m$. Stel dat het niet zo is, dus $a^k = a^m$. Dan geldt $a^{|k-m|} = 1$, met $|k - m| < p - 1$. Maar dit is in tegenspraak met onze aanname.

Voorbeeld: 2 is een primitieve wortel modulo 5 want

$$2^1 \equiv 2 (\text{mod } 5)$$

$$2^2 \equiv 4 (\text{mod } 5)$$

$$2^3 \equiv 3 (\text{mod } 5)$$

$$2^4 \equiv 1 (\text{mod } 5)$$

2 is echter geen primitieve wortel modulo 7:

$$2^1 \equiv 2 (\text{mod } 7)$$

$$2^2 \equiv 4 (\text{mod } 7)$$

$$2^3 \equiv 1 (\text{mod } 7)$$

En dan begint het weer opnieuw:

$$2^4 \equiv 2(\text{mod } 7)$$

$$2^5 \equiv 4(\text{mod } 7)$$

$$2^6 \equiv 1(\text{mod } 7) \text{ etc.}$$

Niet de hele groep wordt voorgebracht, maar een ondergroep met drie elementen. Het gaat mis omdat $2^3 \equiv 1(\text{mod } 7)$, de orde van het element 2 is dus kleiner dan de orde van de groep. Een voortbrenger van $(\mathbb{Z}/p\mathbb{Z})^*$ moet orde p - 1 hebben om de hele groep voort te brengen.

Het is dus duidelijk dat een getal a (bijvoorbeeld 2), voor sommige priemgetallen p wel en voor andere niet een primitieve wortel modulo p is.

Lemma: Als a een kwadraat is, dan is a nooit een primitieve wortel modulo p, welke p je ook kiest. *Bewijs*:
Laten we zeggen $a = b^2$. Er geldt dan altijd: $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1$ (modulo p) wegens de kleine stelling van Fermat. En $\frac{p-1}{2} < p - 1$, dus als a een kwadraat is, is a geen primitieve wortel modulo p. De orde van a is dus kleiner dan p - 1.

Het vermoeden van Artin stelt nu dat:
1) Voor ieder positief geheel getal $a > 1$, dat geen kwadraat is, zijn er oneindig veel priemgetallen p zodat a een primitieve wortel modulo p is.
2) De dichtheid van de priemgetallen p waarvoor a een primitieve wortel modulo p is, als fractie van alle priemgetallen, is gelijk aan de Artin-constante A, vermenigvuldigd met een rationeel getal.
Hierin is de Artin-constante A gelijk aan $\prod_p(1 - \frac{1}{p(p-1)})$ waarbij het product loopt over alle priemgetallen. Het rationale getal waarmee A vermenigvuldigd wordt om de dichtheid bij een bepaalde a te vinden, hangt af van de keuze van a. We geven hieronder een heuristische afleiding van hoe deze Artin-constante gevonden wordt. Hoe het rationale getal waarmee A vermenigvuldigd wordt afhangt van de keuze van a, laten we hier buiten beschouwing omdat het ons om de Artin-constante te doen is, en niet om het Vemoeden van Artin.

3.2.2 Eigenschappen van primitieve wortels

We bekijken alleen het geval a = 2. In dit geval geldt dat de dichtheid precies gelijk is aan A. Dit heeft Hooley[4] bewezen onderaanname van de beroemde onbewezen Gegeneraliseerde Riemann Hypothese. Helaas voert het te ver om hier uit te leggen wat deze hypothese inhoudt. Veel stellingen in getal theorie zijn onder aanname van deze hypothese te bewijzen, en het bewijs van de hypothese zelf behoort tot de Grote Onopgeloste Problemen in de wiskunde.

Zoals gezegd is 2 een primitieve wortel modulo p dan en slechts dan als $2^k \neq 1$ (mod p) voor alle $k < p - 1$. Dat $2^{p-1} \equiv 1$ (mod p) geldt voor alle p volgens de kleine stelling van Fermat.
Lemma:

$$2^k \neq 1(\text{mod p}) \ \forall\, k\text{met } 0 < k < p - 1 \Leftrightarrow 2^{\frac{p-1}{j}} \neq 1(\text{mod p}) \ \forall\, j > 1 \in \mathbb{Z}$$

Bewijs
De implicatie naar rechts is triviaal. De implicatie naar links is de bekende stelling dat de orde van een element (2 in dit geval) de orde van de groep (p - 1 in dit geval) moet delen. Als er een getal $k < p - 1$ zou bestaan zodat $2^k \equiv 1$ (mod p) dan moet deze k een veelvoud zijn van de orde van het element 2. Deze orde van het element 2 zou dan dus ook kleiner dan p - 1 zijn. Bovendien is de orde van 2 een deler van de orde van de groep, dus van p - 1. En dus is de orde van 2 te schrijven als $\frac{p-1}{j}$ voor een of andere $j \in \mathbb{Z}$ groter dan 1.

Wanneer je dus stelt dat er geen $j \in \mathbb{Z}$ groter dan 1 bestaat met $2^{\frac{p-1}{j}} \equiv 1$ (mod p) (zoals rechts in de equivalentie gedaan wordt), dan volgt dus onmiddelijk dat er ook nooit een k kan bestaan waarvoor geldt dat $2^k \equiv 1$ (mod p). Dit is precies de implicatie naar links.

We weten nu dus dat 2 een primitieve wortel modulo p is, dan en slechts dan als $2^{\frac{p-1}{j}} \neq 1(\text{mod p})\ \forall\, j > 1 \in \mathbb{Z}$. Maar het kan nog mooier.
Lemma

$$2^{\frac{p-1}{j}} \neq 1(\text{mod p})\ \forall\, j > 1 \Leftrightarrow 2^{\frac{p-1}{q}} \neq 1(\text{mod p})\ \forall \text{q met q priem}$$

Bewijs
De implicatie naar rechts is wederom triviaal. De implicatie naar links is ook waar: stel dat er wel een k zou zijn zodat $2^{\frac{p-1}{k}} \equiv 1$ (mod p) en q is een priemdeler van deze k, dan is $2^{\frac{p-1}{q}} = (2^{\frac{p-1}{k}})^{k/q} \equiv 1^{k/q}$ (mod p) $\equiv 1$ (mod p). Kortom: als er een k bestaat met $2^{\frac{p-1}{k}} \equiv 1$ (mod p) dan bestaat er ook een priemgetal q met $2^{\frac{p-1}{q}} \equiv 1$ (mod p) en als zo'n q niet bestaat kan zo'n k dus ook nooit bestaan. We weten nu dat 2 een primitieve wortel van p is dan en slechts dan als voor alle priemgetallen q geldt dat $2^{\frac{p-1}{q}} \neq 1$ (mod p). De Artin-constante is het aantal priemgetallen p die hier aan voldoen als fractie van alle priemgetallen. We zijn dus geinteresseerd in de 'kans' dat als p een priemgetal is, er ook geldt voor alle priemgetallen q dat $2^{\frac{p-1}{q}} \neq 1$ (mod p). Deze kans berekenen we als volgt: we rekenen eerst bij vaste q de kans uit dat als p een priemgetal is, er geldt $2^{\frac{p-1}{q}} \neq 1$ (mod p). En vervolgens vermenigvuldigen we al deze kansen (die uiteraard afhangen van q) met elkaar in een oneindig product over alle priemgetallen q. De makkelijkste manier om de kans uit te rekenen dat $2^{\frac{p-1}{q}} \neq 1$ (mod p) is het uitrekenen van de kans dat $2^{\frac{p-1}{q}} \equiv 1$ (mod p) en vervolgens 1 min die kans te nemen.

Wat gebeurt er als $2^{\frac{p-1}{q}} \equiv 1$ (mod p)?

Als $2^{\frac{p-1}{q}} \equiv 1$ (mod p) dan weten we twee dingen. Ten eerste moet p groter zijn dan q omdat anders $2^{\frac{p-1}{q}}$ nooit een geheel getal kan zijn. Ten tweede weten we dat q een deler is van p - 1 en dus dat $p \equiv 1$ (mod q). De kans dat een willekeurig priemgetal p congruent met 1 modulo q is, is $\frac{1}{q-1}$. Omdat p een priemgetal is, kan p niet congruent 0 modulo q zijn: $p \neq q$ want $p > q$ en alle getallen groter dan q die congruent 0 modulo q zijn, zijn deelbaar door q en dus niet priem. Dan blijven er nog q - 1 mogelijkheden over, met gelijke kans. Hier wordt stiekem aangenomen dat de priemgetallen willekeurig over de natuurlijke getallen verdeeld zijn , dus dat ze bij deling door q geen voorkeur hebben voor een van de restklassen: 1, 2, . . . , q - 1.

Dit volgt uit de stelling van Dirichlet (1839). Een rij getallen van de vorm a, a + d, a + 2d, . . . heet een rekenkundige rij. Als a en d onderling ondeelbaar zijn, spreekt men over een primitieve rekenkundige rij. Neem d vast. Dan zijn er $\phi(d)$ verschillende primitieve rekenkundige rijen. Namelijk, $\phi(d)$ (de Euler Totient functie) is gedefinieerd als het aantal getallen a met a < d, en gg(a,d)=1. Voor deze getallen is a, a + d, . . . een primitieve rekenkundige rij.

De stelling van Dirichlet zegt nu: iedere primitieve rekenkundige rij met d positief bevat oneindig veel priemgetallen. Bovendien zijn deze priemgetallen asymptotisch gelijkverdeeld over de $\phi(d)$ verschillende primitieve rijen. Dat wil zeggen: noem $\pi(x; d, a)$ het aantal priemgetallen ≤ x in de rij a, a + d, a + 2d, . . . Dan geldt dat $\pi(x; d, a)$ voor grote x gelijk gaat lopen met $\pi(x)/\phi(d)$.

Neem nu voor d een priemgetal q. Dan geldt $\phi(q) = q - 1$. De priemgetallen p zijn gelijkverdeeld over de restklassen 1, 2, . . . , q - 1.

De 'kans' dat q een deler is van p - 1 is dus $\frac{1}{q-1}$.

Daarnaast weten we dat $2^{\frac{p-1}{q}}$ een oplossing is van de vergelijking $X^q \equiv 1$ (mod p), omdat $(2^{\frac{p-1}{q}})^q = 2^{p-1} \equiv 1$ (mod p) volgens de kleine stelling van Fermat. Wij zijn geïnteresseerd in de oplossing waarvoor geldt $X \equiv 1$ (mod p).

3.2.3 De 'kans' dat $2^{\frac{p-1}{q}} \equiv 1$ (mod p)

Oplossingen van $X^q \equiv 1$ (mod p)

We hebben zojuist gezien dat we alleen geinteresseerd zijn in de situatie waarin q een deler is van p - 1. In die situatie kunnen we de volgende stelling gebruiken.

Stelling: Als q een deler is van p - 1 , geldt dat de vergelijking $X^q = 1$ in de groep $(\mathbb{Z}/p\mathbb{Z})^*$ precies q oplossingen heeft.

We bewijzen dit in twee stappen. Allereerst zullen we aantonen dat er maximaal q oplossingen zijn, en vervolgens dat er minimaal q oplossingen zijn.

Bewijs dat de vergelijking maximaal q oplossingen heeft
Zoals gezegd heeft de groep $(\mathbb{Z}/p\mathbb{Z})^*$ volgens Gauss minstens één voortbrenger. Kies een willekeurige voortbrenger a. Ieder getal in $(\mathbb{Z}/p\mathbb{Z})^*$ te schrijven als a^r voor een zekere r met $0 < r \leq p - 1$. In het bijzonder ook de getallen X met $X^q \equiv 1$ (mod p).

Vul in $X = a^r$. Er moet nu gelden $a^{(qr)} \equiv 1$ (mod p). Dit betekent dat qr een veelvoud is van p - 1. a is namelijk een voortbrenger en dus een primitieve wortel modulo p. Stel qr = b(p -1) + c met $0 \leq c < p$. Dan is

$$a^q r = a^{b(p-1)} \cdot a^c = (a^{p-1})^b \cdot a^c \equiv 1^b \cdot a^c = a^c (mod p)$$

Dus als $a^{b(p-1)+c} \equiv 1(modp)$ met $0 < c < p$ dan is $a^c \equiv 1$ en dus c = p - 1 (want a was een primitieve wortel).

qr is dus (b + 1)(p - 1) en r is dus $\frac{(b+1)(p-1)}{q}$ oftewel een veelvoud van $\frac{p-1}{q}$. In de vorige subparagraaf hebben we al gezien dat q een deler is van p - 1, zodat $\frac{p-1}{q}$ een geheel getal is. Voor iedere r in $(\mathbb{Z}/p\mathbb{Z})^*$ met $r \equiv 0$ (mod $\frac{p-1}{q}$) is $X = a^r$ dus een oplossing van $X^q \equiv 1$.
De vraag is nu hoeveel verschillende oplossingen a^r in $(\mathbb{Z}/p\mathbb{Z})^*$ dit oplevert. Zoals gezegd is r een veelvoud van $\frac{p-1}{q}$. Voor ieder geheel getal j kunnen we dus een r_j maken volgens

$$r_j := \frac{j(p-1)}{q}$$

met bijbehorende oplossing

$$X_j := a^{r_j}$$

Het is niet moeilijk in te zien dat $X_{j+q} = X_j$ in $(\mathbb{Z}/p\mathbb{Z})^*$:

$$r_{j+q} = \frac{(j+q)(p-1)}{q} = \frac{j(p-1)}{q} + \frac{(q)(p-1)}{q} = r_j + (p-1)$$

zodat

$$X_{j+q} = a^{r_{j+q}} = a^{r_j+(p-1)} = a^{r_j} \cdot a^{p-1} = X_j \cdot 1 = X_j$$

Hiermee is dus aangetoond dat er in elk geval niet meer dan q verschillende oplossingen zijn. Namelijk $X_1, X_2, \ldots, X_q$ want $X_{q+1} = X_1$.

Bewijs dat de vergelijking minimaal q oplossingen heeft
De vraag is nu: zijn er misschien minder dan q oplossingen? Het antwoord luidt nee. Stel dat twee van de oplossingen gelijk zijn, dus dat $a^{r_j} = a^{r_{j+k}}$ in $(\mathbb{Z}/p\mathbb{Z})^*$ voor een zekere $k < q$. Dan zou dus moeten gelden dat

$$a^{r_j} = a^{r_{j+k}} = \frac{a^{r_{j+k}}}{a^{r_j}} \cdot a^{r_j} = a^{r_{j+k}-r_j} \cdot a^{r_j}$$

en dus dat

$$a^{r_{j+k}-r_j} = 1$$

Omdat a een primitieve wortel modulo p is, is $(r_{j+k} - r_j)$ een veelvoud van (p - 1). Maar

$$r_{j+k} - r_j = \frac{(j+k)(p-1)}{q} - \frac{j(p-1)}{q} = \frac{k(p-1)}{q}$$

Omdat we aannamen dat $k < q$ is $\frac{k(p-1)}{q} < p-1$. Maar a is een primitieve wortel modulo p, dus er kan helemaal geen getal m kleiner dan p - 1 zijn met $a^m \equiv 1$ en dus hebben we een tegenspraak.
Kortom, als q een deler is van p - 1 heeft $X^q = 1$ in het lichaam $(\mathbb{Z}/p\mathbb{Z})^*$ precies q verschillende oplossingen.

Wat doen we hiermee?

We weten al dat onze $2^{\frac{p-1}{q}}$ een van de q oplossingen van $X^q \equiv 1 \pmod{p}$ is. We weten ook dat X = 1 een oplossing is: $1^q = 1$, ook in $(\mathbb{Z}/p\mathbb{Z})^*$. Door $2^{\frac{p-1}{q}}$ te bekijken kiezen we "willekeurig" 'e'en van de q oplossingen. Een van de oplossingen is in $(\mathbb{Z}/p\mathbb{Z})^*$ aan 1. De kans dat $2^{\frac{p-1}{q}}$ nou precies die oplossing is, is dus gelijk aan $\frac{1}{q}$.

Opmerking: We nemen aan dat alle mogelijke oplossingen van $X^q \equiv 1 \pmod{p}$ a priori van de vorm $2^{\frac{p-1}{q}}$ kunnen zijn, zodat we met $2^{\frac{p-1}{q}}$ echt willekeurig 'e'en van de q oplossingen kiezen.

We wilden de kans uitrekenen dat $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ Wat we nu weten, is dat de kans dat $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ gegeven dat q een deler is van p - 1 gelijk is aan $\frac{1}{q}$.

De Artin-constante

In het algemeen is de kans dat $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ gelijk aan de kans dat q een deler is van p - 1 maal de kans dat $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ gegeven dat q een deler is van p - 1.

De eerste kans was $\frac{1}{q-1}$, zoals we hebben gezien onder 'Wat gebeurt er als $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$?' en de tweede kans is $\frac{1}{q}$ zoals hierboven is aangetoond. De totale kans dat $2^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ wordt dan $\frac{1}{q(q-1)}$. Dus is de kans dat $2^{\frac{p-1}{q}} \neq 1 \pmod{p}$ gelijk aan $1 - \frac{1}{q(q-1)}$.

2 is een primitieve wortel modulo p als voor alle q met q priem geldt dat $2^{\frac{p-1}{q}} \neq 1 \pmod{p}$. De kans dat 2 een primitieve wortel modulo p is is gelijk aan onze kans vermenigvuldigd over alle q:

$$\prod_q (1 - \frac{1}{q(q-1)})$$

Deze kans hangt niet van p af! In de werkelijkheid is de kans dat 2 een primitieve wortel modulo p is gelijk aan 1 of 0: het is een primitieve wortel of het is het niet. Nogmaals, we zijn heuristisch bezig.

De Artin-constante A is gedefinieerd als de fractie priemgetallen p waarvoor 2 een primitieve wortel modulo p is. Omdat de kans dat 2 een primitieve wortel modulo p is, niet van p afhangt, is die fractie dus gelijk aan deze kans. Vergelijk dit met het volgende voorbeeld: Neem een munt, waarvoor de kans op munt A is, en de kans op kop 1-A. Als je de munt oneindig vaak opgooit, en elke keer opschrijft of het kop of munt was, bij welke fractie van het aantal worpen krijg je munt? Het antwoord is A.

Dit doen we hier ook: we werken de rij van priemgetallen af, en schrijven op of 2 een primitieve wortel modulo het priemgetal is of niet. Bij iedere priemgetal p is de kans dat 2 een primitieve wortel modulo p is gelijk aan $\prod_q (1 - \frac{1}{q(q-1)})$. De fractie van alle priemgetallen waarbij 2 een primitieve wortel modulo p is, is dus gelijk aan $\prod_q(1-\frac{1}{q(q-1)})$. Deze fractie hebben we de Artin-constante genoemd, dus

$$A=\prod_q(1-\frac{1}{q(q-1)})$$

waarbij q loopt over alle priemgetallen.

Hoofdstuk 4

Uitkomsten

Wij hebben met de computertaal C gewerkt. In C kan men niet zomaar met getallen van willekeurige precisie werken: daarom hebben we PARI/GP gebruikt [2]. PARI/GP is een getaltheoretisch pakket voor C. Men kan het als library gebruiken in een C programma, of men kan de "rekenmachine"GP gebruiken. Men kan GP commando's geven, of er kan ook een GP script worden geschreven met een rij commando's, die GP in een keer uitvoert.

We hebben eerst ons programma in pseudo-code opgeschreven. Daarna hebben we voor de priemtweelingconstante een GP script geschreven. Voor deze constante wordt het rekenen makkelijker als men van tevoren een beetje theorie uitwerkt, en dat wordt in dit hoofdstuk gedaan.

Opmerking: Men kan de PARI library aan een C programma koppelen, zodat de functies in de PARI library kunnen worden gebruikt. Dat is echter niet zo simpel: men moet de speciale functies van de library gebruiken, om met getallen van arbitraire precisie te werken. Om bijvoorbeeld op te tellen, moet in plaats van 'x+y', 'gadd(x,y)' geschreven worden, en dat maakt het erg onoverzichtelijk. Een GP script schrijven is voor de meeste programma's de beste keuze.

4.1 De pseudo-code voor een algemene constante

De eerste 1000 priemgetallen en Möbius waarden worden met Mathematica uitgerekend en in een array gezet. De polynomen worden als een array van hun coefficienten in het programma gezet. Als $g(t) = t^\delta + a_1 t^{\delta-1} + \ldots + a_\delta$, met δ de graad van g, dan heet α_i in het programma `g[i]` en δ heet dg. Hetzelfde met f waarvan de coefficienten `f[i]` heten en de graad df. In het programma wordt een functie h gebruikt: die is gedefinieerd als h = g - f.

We hebben in het programma een paar functies van Mathematica nodig. Dankzij Mathlink kan men in C functies van Mathematica gebruiken.
Opmerking: Deze methode om de constanten uit te rekenen is mogelijk, maar wordt niet door ons aangeraden. Mathlink gebruiken is naar, en men kan beter een GP script schrijven. We laten het hieronder zien omdat deze code goed

weergeeft wat we allemaal aan de computer moeten vertellen, zodat hij de constanten uitrekent.

———————————————————————————————-

```
#include <stdio.h>

int main()
{
// Array van de eerste 1000 priemgetallen
int Prime[1000]={1,2,3,5,7,...,7919};

// Array van de eerste 1000 moebius waarden
int MoebiusMu[1000]={1,-1,-1,0, ... ,0,0};

int sg[1000];
int sh[1000];
int bg[1000];
int bh[1000];
int g[100]; // graad dg
int f[100]; // graad df
int h[100]; // graad dh

sg[1] = - g[1];
h[i] = g[i] -f[i];
logC=0;
cout << "kies een m";
cin >> m;

for ( j = 2 ; T > 10e-1000 ; j++)
{
sg[j] = - j*g[j];
sh[j] = - j*h[j];

for (i=1;i<j && i<=dg;i++)
{
if (j<=dg)
{
sg[j] = sg[j] - g[i]*sg[j-i];
}
}

bg[j] = 0;

for (i=1;i<j && i<=dh;i++)
{
if (j<=dh)
```

```
{
sh[j] = sh[j] - h[i]*sh[j-i];
}
}

    bh[j] = 0;

    for (l=1; l<=j;l++)
{

    if (l
{
bg[j] = bg[j] + sg[l]*MoebiusMu[j/l]; //array van waardes
}
}
bg[j]= (1/j)*bg[j]; // allemaal integers!

    for (l=1; l<=j;l++)
{

    if (l%j==0)
{
bh[j] = bh[j] + sh[l]*MoebiusMu[j/l]; //array van waardes

    }
}
bh[j]= (1/j)*bh[j]; // allemaal integers!

    T = (bg[j] - bh[j])*Log(PZ(m,j)); // Mathematica functie

    logC += T;

    }

    C = exp(logC);
//n is het rangnummer van het eerst gebruikte priemgetal: bv priemtweelingen
n=2;

    for (i=n;i<=m;i++)
{
gp = 0;
for(l=0; l<=dg; l++)
{
gp = gp + g[l]*pow(Prime[i],l); // mathematica functie
}
fp=0;
```

```
for (l=0;l <=df;l++)
{
fp = fp + f[l]*pow(Prime[i],l); //mathematica functie
}

    C = C*(1. - (fp/gp));
}
}
cout << "C("<<m<<") is gelijk aan"<<C;
}
```
———————————————————————————

4.2 De priemtweeling constante

4.2.1 Een beetje theorie

In ons programma laten we de computer via Newton-recursie de s_g en s_{g-f} coefficienten uitrekenen, om daarmee, met behulp van de Möbius μ-functie de b_g en b_{g-f} coefficienten uit te rekenen. Wanneer je echter geluk hebt met de polynomen g en g - f, kan dit soms ook sneller. Toevallig is de priemtweelingconstante een voorbeeld van een constante met zeer gunstige polynomen.

De s-coëfficienten

In de theorie wordt een definitie gegeven van de coefficienten $s_g(j)$ waar j een natuurlijk getal is en g een polynoom van graad δ: als je de verschillende nulpunten van g $\alpha_1, \alpha_2, ..., \alpha_\delta$ noemt, dan is

$$s_g(j) := \alpha_1^j + \alpha_2^j + ... + \alpha_\delta^j$$

Normaal gesproken heeft een computer niet veel aan deze definitie. De nulpunten zijn over het algemeen complexe getallen, die moeilijk te representeren zijn, zodat er gauw afrondfouten gemaakt worden. En omdat het met de Newton-recursie mogelijk is de s_g-coefficienten in de coeffienten van g uittedrukken (die gehele getallen zijn) is het natuurlijk veel handiger om dat te doen.

Bij sommige polynomen zijn de nulpunten α_i echter zelf ook gehele getallen, en dan is het vaak sneller om de s_g's direct uit te rekenen. Voor de twee polynomen die we nodig hebben om de priemtweelingconstante uitterekenen geldt dit toevallig.

Zoals in het hoofdstuk 'De Priemtweelingconstante en Artin's Constante' wordt afgeleid, is de priemtweelingconstante gelijk aan:

$$T = \prod_{p>2}(1 - \frac{1}{(p-1)^2})$$

Volgens de definitie zoals gegeven in de inleiding en de theorie, geldt in dit geval dus dat

$$f(t) = 1$$
$$g(t) = (t-1)^2 = t^2 - 2t + 1$$
$$(g-f)(t) = g(t) - f(t) = t^2 - 2t = t(t-2)$$

Zowel g als g-f zijn polynomen van graad 2 en hebben dus slechts twee nulpunten. Voor g zijn dit 1 en 1, voor h zijn dit 2 en 0.

Voor de coefficienten $s_g(j)$ en $s_{g-f}(j)$ betekent dit dat

$$s_g(j) = 1^j + 1^j = 1 + 1 = 2$$
$$s_{g-f}(j) = 2^j + 0^j = 2^j$$

De s_g coefficienten zijn dus allen gelijk. De s_{g-f} coefficienten hangen nog wel van j af, maar zijn toch een stuk sneller direct uit te rekenen dan via de Newton-recursie.

De b-coëfficienten

In de theorie worden voor een polynoom f waarvan de s_f coefficienten bekend zijn, de b_f coefficienten gedefinieerd volgens:

$$b_f(j) = \frac{1}{j} \sum_{d|j} s_f(d)\mu(\frac{j}{d})$$

Voor de priemtweelingconstante betekent dit dus dat:

$$b_g(j) = \frac{1}{j} \sum_{d|j} 2\mu(\frac{j}{d})$$

en

$$b_{g-f}(j) = \frac{1}{j} \sum_{d|j} 2^d\mu(\frac{j}{d})$$

De b_g coefficienten zijn makkelijk uit te rekenen. In de formule voor $b_g(j)$ kunnen we 2 voor het somteken halen:

$$b_g(j) = \frac{2}{j} \sum_{d|j} \mu(\frac{j}{d})$$

In de appendix 'De Mobius μ-funtie en Mobiusinversie' (sectie 5.1.2.) wordt echter aangetoond dat

$$\sum_{d|j} \mu(\frac{j}{d}) = 0$$

voor alle $j > 1$ (Bij j = 1 levert het natuurlijk $\mu(\frac{1}{1}) = 1$ op). Deze stelling hebben we in de appendix 'lemma 1' genoemd en is terug te vinden in 5.2.3.

Het gevolg is dat nu dus:

$$b_g(j) = \frac{2}{j} \cdot 0 = 0$$

voor alle $j > 1$. We houden nu dus nog alleen de b_{g-f} coefficienten over. Deze zijn helaas (voor zover wij weten) niet eenvoudiger uit te rekenen dan volgens

$$b_{g-f}(j) = \frac{1}{j} \sum_{d|j} 2^d \mu(\frac{j}{d})$$

Voor de eerste 10 waarden van j levert dit op:
2, 1, 2, 3, 6, 9, 18, 30, 56, 99.
Met deze kennis is het mogelijk ons programma voor het geval van de priemtweelingconstante sterk te vereenvoudigen. Voor de priemtweelingconstante hebben we een GP-script geschreven dat gebruik maakt van bovenstaande afleidingen.

4.2.2 Het GP script

```
m=input
g(x)= x^2 - (2*x) + 1
h(x)= x^2 - 2x
bg=[2,0,0,0,0,0,...] // De eerste 100 waardes van b_g(n)
bh=[0,0,0,0,0,0,...] // De eerste 100 waardes van b_h(n). Deze zullen later door
het programma zelf veranderd worden.

g=[-2,1]
h = [-2]

dg=2
dh=2

sh(x)=2^x;
sg=2

for(j=2,100,

for (l=1,j,
if (Mod(l,j)==Mod(0,j),
bh[j] = bh[j] + sh(l)*moebius(j/l)
) ) bh[j]= (1/j)*bh[j]
;
pz = zeta(j)
; for(o=1,m,pz=pz*(1- ((prime(o))^-j))
;
T = (- bh[j]) * log(pz))
```

```
;
logC = logC + T
)

    C = exp(logC);

    F=1
for (i=2, m, F = F*(1.- (1. / g(prime(i)) ) ) )
F*C
```

———————————————————————————

Het getal m in het script is het getal m waar in de theorie over is gesproken (lees hierover in 2.4.2.). We hebben voor verschillende waardes van m de constante uitgerekend, en de uitkomst vergeleken met de waarde op de website van Gerhard Niklasch [3]:

m = 20 : C = 0.66016181607081697337068941 77
m = 30 : C = 0.6601618158468856143884257910
m = 40 : C = 0.6601618158468696146344375559
m = 50 : C = 0.6601618158469076114271493309
m = 45 : C = 0.6601618158468708256909878897
m = 35 : C = 0.6601618158468697170391321372
35 is de beste waarde: 16 decimalen nauwkeurig.

Hoofdstuk 5

Appendix

5.1 Meetkundige reeksen

Een meetkundige reeks is van de vorm

$$\sum_{k=n}^{\infty} x^k = x^n + x^{n+1} + x^{n+2} + \cdots$$

met x $\in \mathbb{C}$, en n $\in \mathbb{Z}_{\geq 0}$. Het getal x wordt de *rede* van de meetkundige reeks genoemd. Vraag: voor welke waarden van x convergeert deze reeks? Het volgende lemma vertelt ons dat $|x| < 1$ moet zijn.

5.1.1 Lemma

Als |x| < 1, convergeert $\sum_{k=n}^{\infty} x^k$ naar $\frac{x^n}{1-x}$.

Bewijs
Neem eerst een eindige som, tot een bepaalde r $\geq n$.

$$\sum_{k=n}^{r} x^k = x^n + x^{n+1} + \cdots + x^r$$

Vermenigvuldig deze som met (1-x). We weten dat we de getallen in een eindige som in een willekeurige volgorde bij elkaar mogen optellen.

$$(1-x)\sum_{k=n}^{r} x^k = x^n + x^{n+1} + \cdots + x^r - x^{n+1} - x^{n+2} - \cdots - x^{r+1} = x^n - x^{r+1}$$

Deel aan beide kanten door 1 - x (x$\neq$1):

$$\sum_{k=n}^{r} x^k = \frac{x^n}{1-x} - \frac{x^{r+1}}{1-x}$$

Neem de limiet van deze som, voor r naar oneindig.

$$\sum_{k=n}^{\infty} x^k = \lim_{r\to\infty} \sum_{k=n}^{r} x^k = \frac{x^n}{1-x} - \lim_{r\to\infty} \frac{x^{r+1}}{1-x}$$

De rechterterm, $\lim_{r\to\infty} \frac{x^{r+1}}{1-x}$, convergeert naar $0 \Leftrightarrow |x| < 1$. Dan gaat deze term naar nul, dus hebben we een nieuwe schrijfwijze voor de meetkundige reeks

$$\sum_{k=n}^{\infty} x^k = \frac{x^n}{1-x}$$

Voorbeelden

Voor n=0 krijgt men

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}$$

Voor n=1

$$\sum_{k=1}^{\infty} x^k = \frac{x}{1-x}$$

Dit zijn de vaakst voorkomende meetkundige reeksen.

Nu een paar waarden invullen voor x.

n=0, x=$\frac{1}{2}$:

$$\sum_{k=0}^{\infty} (\frac{1}{2})^k = \frac{1}{1-\frac{1}{2}} = 2$$

n=1, x = 0.9:

$$\sum_{k=1}^{\infty} 0.9^k = \frac{0.9}{1-0.9} = 8$$

n=1, x = 0.9995:

$$\sum_{k=1}^{\infty} 0.9995^k = \frac{0.9995}{1-0.9995} \simeq 2001$$

Als we nu een meetkundige reeks tegenkomen, kunnen we hem gelijk uitrekenen.

We kunnen ook het omgekeerde doen: als we een factor van de vorm $\frac{x^n}{1-x}$ tegenkomen, dan kunnen we het als een meetkundige reeks schrijven, $\sum_{k=n}^{\infty} x^k$. Dit wordt gebruikt in 5.3.

5.1.2 De Riemann zeta functie $\zeta(j)$ herschreven

De Riemann zeta functie $\zeta(j)$ is als volgt gedefinieerd

$$\zeta(j) = \sum_{k=1}^{\infty} k^{-j}$$

In 2.2.1., formule (2.2) werd er beweerd dat deze geschreven kan worden als een product over alle priemgetallen:

$$\zeta(j) = \prod_p \frac{1}{1-p^{-j}}$$

Dit werd door Euler bedacht, en zo'n product over alle priemgetallen wordt een Euler product genoemd. Dat dit zo is, kunnen we nu eenvoudig inzien, dankzij onze kennis van meetkundige reeksen.

De termen in het product zijn allemaal meetkundige reeksen! $\frac{1}{1-p^{-j}}$ is een meetkundige reeks, met rede p^{-j}. Dus

$$\frac{1}{1-p^{-j}} = \sum_{k=0}^{\infty}(p^{-j})^k = 1 + p^{-j} + p^{-2j} + \cdots$$

Wat krijgen we als we het product nemen over alle priemgetallen p van deze factoren?

$$\prod_p \frac{1}{1-p^{-j}} = (1 + p_1^{-j} + p_1^{-2j} + \cdots)(1 + p_2^{-j} + p_2^{-2j} + \cdots)\cdots$$

met $(p_n)_{n=1}^{\infty}$ de rij van alle priemgetallen: $p_1 = 2, p_2 = 3, \ldots$ Wat voor getallen krijgen we als we dit product gaan uitwerken? Het zijn allemaal getallen van de vorm

$$(p_1^{-j})^{a_1}(p_2^{-j})^{a_2}(p_3^{-j})^{a_3}\cdots$$

met $a_i \in \mathbb{Z}_{\geq 0}$. Bijvoorbeeld, voor alle $a_i = 0$ krijgen we 1. Voor $a_1 = 1$, alle andere $a_i = 0$, is het getal gelijk aan 2^{-j}.

De bewering is: dit zijn allemaal getallen van de vorm n^{-j}, met n in $\mathbb{Z}_{\geq 0}$. Als dit waar is, dan is het product gelijk aan de som over alle getallen n^{-j}, en dan is de bewijs klaar.

Is de bewering waar? We weten dat elk getal n $\in \mathbb{Z}$ op eenduidige wijze ontbonden kan worden in priemfactoren:

$$n = p_1^{a_1} p_2^{a_2} \ldots$$

met $a_i \in \mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$

Wat is dan n^{-j}?

$$n^{-j} = (p_1^{a_1})^{-j}(p_2^{a_2})^{-j} \ldots = (p_1^{-j})^{a_1}(p_2^{-j})^{a_2} \ldots$$

en zo zien de factoren van het uitgeschreven product er precies uit. Klaar:

$$\zeta(j) = \sum_{k=1}^{\infty} k^{-j} = \prod_p \frac{1}{1-p^{-j}}$$

5.2 De Möbius μ-functie en Möbiusinversie

Veel mensen kennen August Ferdinand Möbius (1790-1868) alleen als de uitvinder van de Möbiusband. Zijn bijdrage aan de wiskunde was echter lang niet zo eenzijdig. Wij maken bijvoorbeeld gebruik van de naar hem genoemde Möbiusinversie en de daarvoor onmisbare Möbius μ-functie. Er is in het hoofdstuk over theorie al uitgelegd wat deze woorden betekenen. Hier zullen we dit nog eens herhalen en bewijzen dat Möbiusinversie inderdaad altijd werkt.

5.2.1 De Möbius μ-functie

De Möbius μ-functie: μ is een functie van de natuurlijke getallen naar {-1, 0, 1}. Noem een geheel getal *kwadratenvrij* als het niet deelbaar is door een kwadraat van een geheel getal groter dan 1. Dan geldt dat hij al zijn priemfactoren maar een keer als priemfactor heeft. De Möbius μ-functie is nu gedefinieerd volgens:

$$\mu(n) = \begin{cases} 0 & \text{als n deelbaar is door een kwadraat groter dan 1} \\ 1 & \text{als n kwadratenvrij is en n een even aantal priemfactoren heeft} \\ -1 & \text{als n kwadratenvrij is en n een oneven aantal priemfactoren heeft} \end{cases}$$

Wat is dan $\mu(1)$? 1 is kwadratenvrij en heeft een even aantal priemfactoren, namelijk 0. Dus $\mu(1) = 1$.

Uit de definitie volgt dat de Möbius μ-functie de volgende eigenschap heeft:

Multiplicativiteit: μ(a) . μ(b) = μ(a . b) als $ggd(a, b) = 1$

Een plek waar de Möbiusfunctie heel natuurlijk opduikt, is bij het berekenen van ϕ (N), met ϕ de Euler ϕ-functie, en N een natuurlijk getal. $\phi(N)$ is het aantal getallen kleiner of gelijk aan N die onderling ondeelbaar zijn met N. Noem de priemdelers van N $p_1, p_2, ...p_k$. We willen ϕ(N) berekenen door eerst alle getallen kleiner of gelijk aan N te nemen, en vervolgens alle getallen die deelbaar zijn door een van deze priemfactoren eruit te gooien. Het aantal getallen dat je overhoudt is dan ϕ(N). Je neemt dus eerst alle getallen in het rijtje van 1 tot N. Dat zijn N getallen. Dan haal je alle getallen die deelbaar zijn door p_1 eruit. Dat zijn er N/p_1: $p_1, 2p_1, \ldots, (\frac{N}{p_1}) = N$. Je haalt alle getallen die deelbaar zijn door p_2 eruit, dus N/p_2 getallen, alle getallen die deelbaar zijn door p_3 ook, enz. totdat je alle priemdelers gehad hebt.

Maar nu heb je alle getallen die deelbaar zijn door twee priemgetallen en alle veelvouden daarvan, twee keer eruit gegooid. Daarvan moet je er dus weer een terugstoppen. Er zijn N/p_1p_2 veelvouden van p_1p_2, N/p_1p_3 veelvouden van p_1p_3 en N/p_2p_3 veelvouden van p_2p_3 en al deze getallen moeten dus weer worden 'teruggestopt'.

Maar nu zit je weer met getallen met drie priemdelers en hun veelvouden: ze zijn er drie keer uitgegooid ($p_1p_2p_3$ bijvoorbeeld als veelvoud van p_1, als veelvoud van p_2 en als veelvoud van p_3) maar ook drie keer weer teruggestopt (als veelvoud van p_1p_2, als veelvoud van p_1p_3 en als veelvoud van p_2p_3) en moeten er dus nog een keer uit. Uiteindelijk houd je dus over:

$$\begin{aligned}\phi(N) &= N - \frac{N}{p_1} - \frac{N}{p_2} - \frac{N}{p_3} - \cdots + \frac{N}{p_1p_2} + \frac{N}{p_1p_3} + \cdots - \frac{N}{p_1p_2p_3} - \cdots \\ &= \sum_{d|N} \mu(d)\frac{N}{d}\end{aligned}$$

Hierbij loopt de som over alle delers d van N. Je begint met N = $\mu(1)$. N/1 getallen en vervolgens geldt dat als een deler een veelvoud is van een oneven aantal verschillende priemgetallen, er N/d getallen uit moeten worden gegooid, zodat N/d van het totale aantal wordt afgetrokken, en dat als de deler een veelvoud is van een even aantal verschillende priemgetallen, er N/d getallen terug moeten worden gestopt, zodat N/d bij het totale aantal wordt opgeteld. Het teken voor N/d komt dus precies overeen met μ(d). Bovendien geldt dat als d deelbaar is door een kwadraat van een priemdeler p, alle N/d veelvouden van d er al uitgegooid zijn toen alle veelvouden van p er werden uitgegooid, en ze ook niet speciaal hoeven worden teruggestopt. Dit komt ook tot uitdrukking in de formule, omdat in dat geval μ(d) = 0, zodat de term N/d wordt opgeteld noch afgetrokken.

Omdat de som loopt over alle delers van N geldt er:

$$\phi(N) = \sum_{d|N} \mu(d)\frac{N}{d} = \sum_{d|N} d \cdot \mu(\frac{N}{d})$$

5.2.2 Möbiusinversie

Waar wij de Möbius μ-functie voor gebruiken is de zogenaamde Möbiusinversie. Als f en g functies zijn van $\mathbb{N}$ naar $\mathbb{N}$, dan stelt Möbiusinversie dat

$$\sum_{d|n} f(d) = g(n) \Leftrightarrow f(n) = \sum_{d|n} \mu(\frac{n}{d}) \cdot g(d)$$

Wanneer we dit toepassen op de formule voor ϕ van net, dan blijkt met $f(x) = \phi(x)$ en g(x) = x, dat $\sum_{d|n} \phi(d)$ = n.

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d} \Rightarrow n = \sum_{d|n} \phi(n)$$

Voor deze laatste formule bestaat ook een elegant bewijs zonder Möbiusinversie, wat we hier zullen geven.

Elegant bewijs

Neem alle breuken $\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \ldots \frac{n}{n}$. Dit zijn n getallen. Vereenvoudig nu al deze breuken zo ver mogelijk door teller en noemer door hun grootste gemene deler te delen. De noemers zijn nu delers van n en iedere deler d van n komt een

aantal keer als noemer voor. De getallen die als teller voorkomen in een breuk met noemer d, zijn allen onderling ondeelbaar met d. We beweren: alle getallen kleiner dan d die onderling ondeelbaar met d zijn, komen precies een keer als teller voor.
Bewijs
Neem een getal a kleiner dan d, die onderling ondeelbaar is met d. De bewering zegt dat $\frac{a}{d}$ voorkomt, als we alle breuken van de vorm $\frac{b}{n}$ maximaal vereenvoudigen. Welnu, $\frac{a}{d}$ is een maximale vereenvouding van ((a n) / d) / n. (a n)/d is een geheel getal omdat d een deler is van n, en het is kleiner dan n omdat a < d. $\frac{a}{d}$ is duidelijk een vereenvoudiging van ((a n)/d)/n (deel boven en onder de streep door n), en het is de maximale vereenvoudiging, omdat a en d onderling ondeelbaar zijn.

Er zijn dus precies $\phi(d)$ breuken met noemer d, en in totaal zijn er dus $\sum_{d|n} \phi(d)$ breuken. Maar dat zijn nog steeds n breuken, want we hebben geen breuken weggehaald, maar alleen vereenvoudigd. Dus er geldt $\sum_{d|n} \phi(d) =$ n.

5.2.3 Het Bewijs van Möbiusinversie

Terug naar Möbiusinversie. Voor de geldigheid hiervan hebben we zelf een bewijs gevonden, en hoewel er vast mooiere bewijzen zijn, willen we dat hier laten zien. We beginnen met een algemene eigenschap van de Möbius μ-functie, die we 'lemma 1' hebben genoemd.

Lemma 1

Voor alle n $\in \mathbb{N}$ met n ≥ 2 geldt:

$$\sum_{d|n} \mu(d) = 0$$

Bewijs
We beginnen met een definitie.

Definitie: Zij n een natuurlijk getal. Definieer dan n' als het getal dat alle verschillende priemfactoren van n precies 1 keer als priemfactor heeft. Dus als n = 6 is n' = 6, als n = 60 is n' = 30, als n = 8 is n' = 2 enz.
n' is de grootste kwadratenvrije deler van n en wordt wel de 'kwadratenvrije kern' van n genoemd. Als μ(n) = 1 of μ(n) = -1, dan geldt, n' = n, als μ(n) = 0, dan is $n' < n$ en geldt ggd(n/n', n') > 1. In beide gevallen gevallen geldt: $\sum_{d|n} \mu(d) = \sum_{d|n'} \mu(d)$.

Neem een getal d dat n deelt. Als d kwadratenvrij is, dan deelt het ook n'. Als d geen deler is van n', zijn er dus twee of meer van zijn priemfactoren hetzelfde. Dan geldt volgens de definitie van μ dat μ(d) = 0. Nu is

$$\sum_{d|n} \mu(d) = \sum_{d|n, d|n'} \mu(d) + \sum_{d|n, \text{d deelt n' niet}} \mu(d) = \sum_{d|n'} \mu(d) + 0 = \sum_{d|n'} \mu(d)$$

Goed, nu hoeven we alleen nog maar voor n', een kwadratenvrij getal, te bewijzen dat $\sum_{d|n'} \mu(d) = 0$. Een elegant bewijs is het volgende:

$$\sum_{d|n'} \mu(d) = \prod_{p|n'} (1 + \mu(p)) = 0$$

waarbij p loopt over de priemfactoren van n'.

Het eerste gelijkteken volgt uit de multiplicativiteit van μ bij uitschrijven van het product. Het tweede gelijkteken volgt uit het feit dat iedere term (1 + μ(p)) = 0 aangezien p priem is en dus μ(p) = -1.

Wij hadden zelf een iets omslachtiger bewijs met behulp van de driehoek van Pascal:

Definitie: $\omega(n)$ **en** $\Omega(n)$
$\omega(n)$ is het aantal verschillende priemfactoren van n.
$\Omega(n)$ is het totale aantal priemfactoren van n.
Voorbeeld $120 = 2^3 \,.\, 3 \,.\, 5$
$\omega(120) = 3$
$\Omega(120) = 5$

Merk op: Neem een getal n. Dan geldt voor n', de kwadratenvrije kern van n, dat $\omega(n) = \omega(n') = \Omega(n')$.

De delers van n' zijn allemaal producten van een aantal priemdelers van n'. Zeg: het product van 0 priemdelers van n' := 1.

Zij d een deler van n'. Alle priemfactoren van d zijn dus verschillend. Als het aantal priemfactoren van d even is, is μ(d) = 1 en als het aantal priemfactoren van d oneven is, is μ(d) = -1. Dus

$$\sum_{d|n'} \mu(d) = \#\{d|n', \omega(d) \text{ is even}\} - \#\{d|n', \omega(d) \text{ is oneven}\}$$

Noem N = $\omega(n')$, het aantal priemfactoren van n'. Omdat alle priemfactoren van n' verschillend zijn, zijn er precies 'N boven k' delers van n' met k priemfactoren. 'N boven k' is gedefinieerd als

$$\binom{N}{k} = \frac{N!}{(N-k)!k!}$$

met N, k $\in \mathbb{Z}_{\geq}0, k \leq N$. Er geldt dus

$$\sum_{d|n'} \mu(d) = \sum_{k \leq N, \text{k even}} \binom{N}{k} - \sum_{k \leq N, \text{k oneven}} \binom{N}{k}$$

Hierbij begint de even som te lopen bij 0 en de oneven som bij 1.

Nu weten we dat N boven k het getal is in de N-de rij op de k-de plaats van de driehoek van Pascal, en dat ieder getal in deze driehoek de som is van de twee getallen erboven. In wiskundetaal: $\binom{N}{k} = \binom{N-1}{k-1} + \binom{N-1}{k}$ Hierbij definieren we $\binom{N-1}{-1} = \binom{N-1}{N} = 0$.

Het gevolg is dat

$$\sum_{k \leq N, \text{ k even}} \binom{N}{k} = \sum_{k=0}^{N-1} \binom{N-1}{k}$$

en

$$\sum_{k \leq N, \text{ k oneven}} \binom{N}{k} = \sum_{k=0}^{N-1} \binom{N-1}{k}$$

oftewel de som over alle even getallen in de N-de rij is gelijk aan de som over alle getallen in de (N-1)de rij, en de som over alle oneven getallen in de N-de rij ook.

Dus $\sum_{k \leq N, \text{k even}} \binom{N}{k} = \sum_{k \leq N, \text{k oneven}} \binom{N}{k} = \sum_{0}^{N-1} \binom{N-1}{k}$ en dus:

$$\sum_{d|n'} \mu(d) = \sum_{k \leq N, \text{k even}} \binom{N}{k} - \sum_{k \leq N, \text{k oneven}} \binom{N}{k} = 0$$

En omdat $\sum_{d|n} \mu(d) = \sum_{d|n'} \mu(d)$, met n' de kwadraten vrije kern van n, geldt voor iedere n $\in \mathbb{N}$ dat

$$\sum_{d|n} \mu(d) = 0$$

Lemma 1 is zeer goed te gebruiken om de volgende twee, zeer vergelijkbare lemma's te bewijzen.

Lemma 2

Zij f een functie van $\mathbb{N}$ naar $\mathbb{R}$. Dan geldt

$$\sum_{k|n, k \neq n} f(k) + \sum_{d|n, d \neq n} (\mu(n/d) \sum_{e|d} f(e)) = 0$$

Bewijs

Om het linkerlid gelijk aan nul te praten, zouden we het willen herschrijven als een som over de delers van n, waarbij de termen in de som allemaal nul zijn. Preciezer gezegd herschrijven we het linkerlid als

$$\sum_{k|n, k \neq n} a_k f(k)$$

Men ziet gemakkelijk in dat voor a_k geldt:

$$a_k = 1 + \sum_{d|n, d \neq n \text{ met } k|d} \mu(n/d)$$

(ga na). Maar $1 = \mu(1) = \mu(\frac{n}{n})$, dus

$$a_k = 1 + \sum_{d|n, d\neq n \text{ met } k|d} \mu(n/d) = \mu(\frac{n}{n}) + \sum_{d|n, d\neq n \text{ met } k|d} \mu(n/d)$$

$$\Rightarrow a_k = \sum_{d|n \text{ met } k|d} \mu(n/d)$$

Nu geldt voor iedere deler d van n dat $k|d$ dan en slechts dan als $(\frac{n}{d})|(\frac{n}{k})$. Namelijk, 'k deelt d' betekent: er is een geheel getal a met d = a k. Dan geldt ook

$$\frac{d}{n} = a\frac{k}{n} \Leftrightarrow \frac{n}{k} = a\ \frac{n}{d} \Leftrightarrow (\frac{n}{d}) \mid (\frac{n}{k})$$

Substitueer r = n/d in de formule voor a_k. 'k | d' wordt dan 'r | $\frac{n}{k}$', volgens het verhaal van net. Wat wordt 'd | n' in termen van r? Het wordt 'r | n': Als men een som over alle delers d van n uitrekent, kan men ook de som over alle getallen $\frac{n}{d}$, met d de delers van n, nemen. Het is de som over dezelfde getallen: Als d een deler is van n, dan is $\frac{n}{d}$ dat ook. Namelijk, als d een deler is van n, dan is $\frac{n}{d}$ geheel, dus

$$\frac{n}{d} \cdot d = n$$

bewijst dat $\frac{n}{d}$ | n.
Onze som wordt nu in termen van r

$$\sum_{d|n \text{ met } k|d} \mu(n/d) = \sum_{r|n \text{ met } r|(n/k)} \mu(r)$$

De som loopt over alle r die n en $\frac{n}{k}$ delen. Maar als r $|\frac{n}{k}$, dan volgt gelijk $r|n$. We kunnen dus '$r|n$' weglaten. Er blijft over

$$\sum_{r|(n/k)} \mu(r)$$

Dit is gelijk aan 0 volgens lemma 1. Dus het oorspronkelijke linkerlid is gelijk aan 0:

$$\sum_{k|n, k\neq n} 0 \cdot f(k) = 0$$

Lemma 3

Zij g een functie van $\mathbb{N}$ naar $\mathbb{R}$. Dan geldt

$$\sum_{k|n, k\neq n} \mu(n/k)g(k) + \sum_{d|n, d\neq n} \sum_{e|d} \mu(d/e)g(e) = 0$$

Bewijs
Net als in lemma 2, herschrijven we het linkerlid als

$$\sum_{k|n, k\neq n} b_k g(k)$$

Ga zelf na dat voor b_k, met k een deler van n, geldt:

$$b_k = \mu(\frac{n}{k}) + \sum_{d|n, d \neq n \text{ met } k|d} \mu(\frac{d}{k}) = \sum_{d|n \text{ met } k|d} \mu(\frac{d}{k})$$

Noem r = $\frac{d}{k}$. Dan willen we de som schrijven in termen van r. De som gaat over alle getallen d met $d|n$ en $k|d$. We kunnen dan het volgende zeggen: Er zijn gehele getallen a en b met n = a d en d = b k. We kunnen nu twee gevolgen afleiden voor r = $\frac{d}{k}$. Ten eerste, d = b k, dus r = b, dus r moet geheel zijn. Ten tweede, n = a d, dus $\frac{n}{k} = a\frac{d}{k} = a\, r$, dus r moet $\frac{n}{k}$ delen. Onze som wordt dan

$$b_k = \sum_{r|\frac{n}{k}} \mu(r)$$

Dit is gelijk aan 0 volgens lemma 1. Dus het oorspronkelijke linkerlid is gelijk aan 0:

$$\sum_{k|n} b_k g(k) = \sum_{k|n} 0 g(k) = 0$$

Het eigenlijke bewijs

Dan is het nu tijd voor het bewijs van Möbiusinversie. Zoals gezegd stelt Möbiusinversie dat

$$\sum_{d|n} f(d) = g(n) \Leftrightarrow \sum_{d|n} \mu(n/d) \cdot g(d) = f(n)$$

Eerst bewijzen we de implicatie naar rechts.
Neem aan: $\sum_{d|n} f(d) = g(n)$
Dan is

$$\begin{aligned}
&\sum_{d|n} \mu(n/d) \cdot g(d) \\
&\qquad = g(n) + \sum_{d|n, d \neq n} \mu(n/d) \cdot g(d) \\
&\qquad = \sum_{k|n} f(k) + \sum_{d|n, d \neq n} \mu(n/d) \cdot g(d) \\
&\qquad = f(n) + \sum_{k|n, k \neq n} f(k) + \sum_{d|n, d \neq n} \mu(n/d) \cdot g(d) \\
&\qquad = f(n) + \sum_{k|n, k \neq n} f(k) + \sum_{d|n, d \neq n} \mu(n/d) \cdot \sum_{e|d} f(d)
\end{aligned}$$

Maar lemma 2 zegt dat $\sum_{k|n, k \neq n} f(k) + \sum_{d|n, d \neq n} \mu(n/d) \cdot \sum_{e|d} f(d) = 0$ dus $\sum_{d|n} \mu(n/d) \cdot g(d) = f(n)$.

Nu de implicatie naar links.

Neem aan: $\sum_{d|n} \mu(n/d) \cdot g(d) = f(n)$
Dan is:

$$\sum_{d|n} f(d)$$
$$= f(n) + \sum_{d|n, d \neq n} f(d)$$
$$= \sum_{k|n} \mu(n/k) \cdot g(k) + \sum_{d|n, d \neq n} f(d)$$
$$= g(n) + \sum_{k|n, k \neq n} \mu(n/k) \cdot g(k) + \sum_{d|n, d \neq n} f(d)$$
$$= g(n) + \sum_{k|n, k \neq n} \mu(n/k) \cdot g(k) + \sum_{d|n, d \neq n} \sum_{e|d} \mu(d/e) \cdot g(e)$$

Maar $\sum_{k|n,k\neq n} \mu(n/k) \cdot g(k) + \sum_{d|n,d\neq n} \sum_{e|d} \mu(d/e) \cdot g(e) = 0$ volgens lemma 3. Dus $\sum_{d|n} f(d) = g(n)$.

Hiermee is het bewijs van Möbiusinversie voltooid. Het kan vast sneller, maar ik we zijn erg tevreden dat we dit zelf gevonden hebben.

5.3 De centrale stelling: overgeslagen tussenbewijzen

In sectie 2.3.3. wordt de centrale stelling bewezen. Er werden om het leesbaar te houden een paar tussenbewijzen niet weergegeven. Deze tussenbewijzen zijn hier terug te vinden.

5.3.1 Lemma: $b_g(1) = b_{g-f}(1)$

Voor een willekeurige functie F zijn de getallen $b_F(k)$ gedefinieerd volgens

$$b_F(k) = \frac{1}{n} \sum_{k|n} s_F(k) \mu(\frac{n}{k})$$

$s_F(k)$ is in 2.3.1. gedefinieerd volgens de recursie-relatie

$$s_F(k) + a_1 s_F(k-1) + \cdots + a_{k-1} s_F(1) + k a_k = 0$$

Neem nu twee monische polynomen f en g $\in \mathbb{Z}[t]$. Neem aan dat graad(f) + 2 $\leq$ graad(g).
Dan geldt dat $b_g(1) = b_{g-f}(1)$.
Bewijs
Voor een willekeurige functie $F(t) = t^\delta + a_1 t^{\delta-1} + \cdots + a_\delta$ geldt

$$b_F(n) = \frac{1}{n} \sum_{k|n} s_F(k) \mu(\frac{n}{k})$$

dus

$$b_F(1) = s_F(1)$$

Volgens de recursie-relatie geldt dat $s_F(1) = -a_1$, dus $b_F(1) = -a_1$.

Neem nu onze twee functies f en g:

$$g(t) = t^\delta + b_1 t^{\delta-1} + \cdots + b_\delta$$

$$f(t) = t^\alpha + c_1 t^{\alpha-1} + \cdots + c_\alpha$$

Volgens onze aanname $\alpha + 2 \leq \delta$, geldt voor g - f :

$$(g-f)(t) = t^\delta + b_1 t^{\delta-1} + \cdots$$

De graad van g-f is dus δ, en de coefficient van $t^{\delta-1}$ is b_1.
Net werd bewezen dat voor een functie F geldt $b_F(1) = -a_1$. In dit geval geeft dit: $b_g(1) = -b_1$, en $b_{g-f}(1) = -b_1$. Dus $b_g(1) = b_{g-f}(1)$.

5.3.2 Lemma: Het omwisselen van de somtekens

In sectie 2.3.3. hebben we de constanten die we willen uitrekenen, $\prod_{p>p_n}(1-\frac{f(p)}{g(p)})$, weten te herschrijven als

$$C_{f,g}(n) = \prod_{p>p_n}\prod_{j=2}^{\infty}(1-p^{-j})^{b_{g-f}(j)-b_g(j)}$$

We hebben toen de twee producten van volgorde verwisseld, waarna makkelijk de centrale stelling volgt. Dit lemma beweert dat het mag: dus dat

$$\prod_{p>p_n}\prod_{j=2}^{\infty}(1-p^{-j})^{b_{g-f}(j)-b_g(j)} = \prod_{j=2}^{\infty}\prod_{p>p_n}(1-p^{-j})^{b_{g-f}(j)-b_g(j)}$$

Bewijs
We willen dat als de twee producten van volgorde verwisseld worden, de uitkomst hetzelfde blijft. Er moeten dan twee dingen gelden: dat het tweede product convergeert, en dat het dubbele product convergeert. In dit bewijs wordt duidelijk waarom er voorwaarden zijn in de centrale stelling: die zorgen ervoor dat aan deze twee eisen wordt voldaan.

We moeten dus twee dingen bewijzen : dat onder de voorwaarden in de stelling het tweede product convergeert, en dat het dubbele product convergeert. In beide gevallen wordt kennis uit de theorie van oneindige producten gebruikt: men zegt dat een product $\prod(1+\epsilon_n)$ absoluut convergeert als de som $\sum \epsilon_n$ absoluut convergeert. Absolute convergentie betekent : neem van elk getal in de som de absolute waarde voordat het bij de andere getallen wordt opgeteld. Neem dus $\sum |\epsilon_n|$. Absolute convergentie impliceert convergentie, maar de omgekeerde implicatie geldt niet. In een absoluut convergerend product mogen de factoren in een andere volgorde met elkaar worden vermenigvuldigd zonder de waarde van het product te veranderen.

We gaan nu aannemelijk maken dat

$$\sum |\epsilon_n| \text{ convergeert} \Rightarrow \prod (1+\epsilon_n) \text{ convergeert}$$

Kijk eerst naar $\prod(1+|\epsilon_n|)$. We gebruiken de volgende afschatting, die geldt voor alle x $\in \mathbb{R}$:

$$1 + x \leq \exp(x)$$

Dan geldt dus voor ons product dat

$$1 \leq \prod (1+|\epsilon_n|) \leq \prod \exp(|\epsilon_n|)$$

$$\Rightarrow 1 \leq \prod (1+|\epsilon_n|) \leq \exp(\sum |\epsilon_n|)$$

Als $\sum |\epsilon_n|$ convergeert, dan convergeert $\exp(\sum |\epsilon_n|)$, dus dan convergeert het product $\prod(1+|\epsilon_n|)$.

We hebben net bewezen

$$\sum |\epsilon_n| \text{ convergeert} \Rightarrow \prod (1+|\epsilon_n|) \text{ convergeert}$$

We gaan nu bewijzen:

$$\sum |\epsilon_n| \text{ convergeert} \Rightarrow \prod (1+\epsilon_n) \text{ convergeert}$$

Herschrijf het rechterlid als

$$(\prod_{\epsilon_n > 0} (1+|\epsilon_n|))(\prod_{\epsilon_n < 0} (1-|\epsilon_n|))$$

Dit mogen we alleen schrijven als de twee producten convergeren. Dat ze convergeren gaan we nu bewijzen.

Het linker product is kleiner dan $\prod(1+|\epsilon_n|)$ en groter dan nul, dus als $\prod(1+|\epsilon_n|)$ convergeert dan convergeert het linkerproduct ook.

Nu het rechter product: als $\sum |\epsilon_n|$ convergeert, moet op den duur gelden dat $0 \leq |\epsilon_n| < 1$. Dus op den duur is $0 < 1 - |\epsilon_n| \leq 1$. Dus convergeert $\prod_{\epsilon_n<0}(1-|\epsilon_n|)$.

Klaar: het product van twee convergerende producten convergeert.

Bewijs van convergentie van het tweede product

$\prod_{j=2}^{\infty}(1-p^{-j})^{b_{g-f}(j)-b_g(j)}$ onderzoeken we.

Lemma: Het product is convergent als $\sum_{j=1}^{\infty} |b_{g-f}(j) - b_g(j)|(\frac{1}{p})^j$ convergeert.

Bewijs

We willen ons product herschrijven als $\prod(1+\epsilon_n)$. Dan hebben we hierboven bewezen dat het product convergeert als $\sum |\epsilon_n|$ convergeert.

Noem $c_j = b_{g-f}(j) - b_g(j)$. c_j is geheel, omdat $b_{g-f}(j)$ en $b_g(j)$ geheel zijn. We moeten twee gevallen onderscheiden:

$c_j > 0$: Dan hebben in het product $(1-p^{-j})^{c_j}$ staan. Dit is van de vorm

$$(1-p^{-j}) \cdot (1-p^{-j}) \cdot \cdots \cdot (1-p^{-j})$$

De factor $(1-p^{-j})$ komt dus c_j keer voor.
$c_j < 0$: Dan hebben we in het product $(1-p^{-j})^{c_j}$ staan, met $c_j < 0$. Dit is hetzelfde als $\frac{1}{1-p^{-j}}^{|c_j|}$. Maar er geldt dat

$$\frac{1}{1-p^{-j}} = \frac{1-p^{-j}+p^{-j}}{1-p^{-j}} = 1 + \frac{p^{-j}}{1-p^{-j}}$$

Dus

$$\frac{1}{1-p^{-j}}^{|c_j|} = (1+\frac{p^{-j}}{1-p^{-j}})^{|c_j|} = (1+\frac{p^{-j}}{1-p^{-j}})\cdot\ldots\cdot(1+\frac{p^{-j}}{1-p^{-j}})$$

Nu willen we het product schrijven in de vorm van $\prod(1+\epsilon_n)$. Dat kan nu makkelijk:

$$\begin{array}{llll} c_j > 0 & (1-p^{-j})^{c_j} & \epsilon_j = -p^{-j} & \text{komt } c_j \text{ keer voor} \\ c_j < 0 & (1+\dfrac{p^{-j}}{1-p^{-j}})^{|c_j|} & \epsilon_j = \dfrac{p^{-j}}{1-p^{-j}} & \text{komt } |c_j| \text{ keer voor} \end{array}$$

Dit product convergeert als $\sum |\epsilon_j|$ convergeert. In dit geval is de som gelijk aan

$$\sum_{j \text{ met } c_j \geq 0} c_j p^{-j} + \sum_{j \text{ met } c_j < 0} |c_j| \frac{p^{-j}}{1-p^{-j}}$$

Merk op dat beide sommen niet alternerend kunnen zijn: de termen zijn allemaal positief. De sommen kunnen dus convergeren, of naar oneindig gaan.

We beweren nu dat de deze twee sommen convergeren als $\sum 2|c_j|p^{-j}$ convergeert.
De eerste som: deze som is duidelijk kleiner dan $\sum 2|c_j|p^{-j}$.
De tweede som: p begint bij 2, en j begint bij 2. Dus geldt voor alle p en j:

$$0 < p^{-j} < \frac{1}{2} \Rightarrow \frac{1}{2} < 1-p^{-j} < 1 \Rightarrow 1 < \frac{1}{1-p^{-j}} < 2$$

Dus geldt voor alle j dat

$$|c_j| \frac{p^{-j}}{1-p^{-j}} < 2|c_j|p^{-j}$$

dus zijn de termen van de tweede som allemaal kleiner dan de termen van $\sum 2|c_j|p^{-j}$.

Ons product convergeert dus als $\sum 2|c_j|p^{-j}$ convergeert. In deze som kunnen we de factor 2 voor het somteken halen. Deze som convergeert dus als $\sum |c_j|p^{-j}$ convergeert.

De som begint eigenlijk bij j=2, maar voor j=1 geldt $c_1 = |b_{g-f}(1) - b_g(1)| = 0$ volgens sectie 5.3.1. We zetten j = 1 er even bij in de som. Het product convergeert dus als $\sum_{j=1}^{\infty} |b_{g-f}(j) - b_g(j)|(\frac{1}{p})^j$ convergeert. Daarmee is het lemma bewezen.

Dat de som convergeert is simpel te bewijzen, en het bewijs geeft ons een paar handigheidjes voor later.

Men kan een bovengrens vinden voor $|b_{g-f}(j) - b_g(j)|$, en dat gaan we nu doen.

In de centrale stelling (zie hoofdstuk 2.2.3) wordt β gedefinieerd als modulus van de grootste wortel tussen alle wortels van g-f en g. Noem δ de graad van g. Een bovengrens voor de exponent is

$$|b_{g-f}(j) - b_g(j)| \leq 2\delta\beta^j$$

Bewijs
Per definitie $b_g(k) = \frac{1}{k}\sum_{d|k} s_g(d)\mu(\frac{k}{d})$, en $s_g(k) = \alpha_1^k + \cdots + \alpha_\delta^k$, met δ het graad van g. Omdat β de grootste wortel is, geldt: $s_g(k) \leq \delta\beta^k$. De som kan maximaal over k getallen zijn, omdat een geheel getal k maximaal k delers kan hebben. En neem aan dat de Möbius functie altijd 1 geeft, zodat $b_g(k)$ maximaal is. Men krijgt dan een bovengrens: $b_g(k) \leq \frac{1}{k}k\delta\beta^k$.

Voor $b_{g-f}(k)$ geldt precies hetzelfde, omdat we voor β de lengte van de grootste wortel onder de wortels van g en g-f genomen hebben.

De twee factoren kunnen, in het maximale geval, nog samenwerken, zodat er nog een factor twee voorkomt in de bovengrens:

$$|b_{g-f}(j) - b_g(j)| \leq 2\delta\beta^j$$

Dus $\sum_{j=1}^{\infty} |b_{g-f}(j) - b_g(j)|(\frac{1}{p})^j \leq 2\delta\sum_{j=1}^{\infty}(\frac{\beta}{p})^j$. Als $p > \beta$, dan is $\sum_{j=1}^{\infty}(\frac{\beta}{p})^j$ een convergerende meetkundige reeks met rede $\frac{\beta}{p}$. En de priemgetallen die in de constante voorkomen zijn allemaal groter dan β: In de centrale stelling worden alleen priemgetallen p_n groter dan p_{n_0} genomen, met $p_{n_0} > \beta$. Dus is de som convergent.
Dus is het tweede product convergent.

Bewijs van convergentie van het dubbele product
Volgens de theorie van oneindige producten :

$$C_{f,g}(n) = \prod_{j=2}^{\infty}\prod_{p>p_n}(1 - p^{-j})^{b_{g-f}(j) - b_g(j)} \text{ convergeert}$$

$$\text{als } \sum_{j=2}^{\infty}|b_{g-f}(j) - b_g(j)|\sum_{p>p_n}\frac{1}{p^j} \text{ convergeert.}$$

Lemma: $\sum_{j=2}^{\infty}|b_{g-f}(j) - b_g(j)|\sum_{p>p_n}\frac{1}{p^j}$ convergeert.
Bewijs
Een bovengrens voor $|b_{g-f}(j) - b_g(j)|$ is in het vorige bewijs al gevonden: $2\delta\beta^j$,

met δ de graad van g. Dus

$$\sum_{j=2}^{\infty} |b_{g-f}(j) - b_g(j)| \sum_{p>p_n} \frac{1}{p^j} \text{convergeert}$$
$$\text{als } \sum_{j=2}^{\infty} 2\delta\beta^j \sum_{p>p_n} \frac{1}{p^j} \text{convergeert.}$$

Het is bekend dat $\sum_{p>p_n} \frac{1}{p^j}$ convergeert voor $j \geq 2$ (het geldt voor $\sum_{n=1}^{\infty} \frac{1}{n^j}$ namelijk ook). Dit zal niet worden bewezen. Men kan dan opschrijven voor j $\geq$ 2

$$\sum_{p>p_n} \frac{1}{p^j} \leq \frac{A}{p_{n+1}^j}$$

Met A een bepaalde constante. A wordt bepaald door de som eerst voor j=2 te schrijven: $\sum_{p>p_n} \frac{1}{p^2} = \frac{A}{p_{n+1}^2}$. Voor grotere j worden de factoren in de som steeds kleiner.

De oorspronkelijke dubbele som is dus kleiner dan $\sum_{j=2}^{\infty} 2\delta A \frac{\beta^j}{p_{n+1}^j}$. En volgens de voorwaarden in de stelling is p_{n+1} groter dan β, dus hier hebben we een convergerende meetkundige reeks, met rede $\frac{\beta}{p_{n+1}}$ (Deze reeks begint bij j=2, maar dat maakt niet uit. Zie sectie 5.1 voor uitleg over meetkundige reeksen).

Het dubbele product convergeert dus absoluut en dus is het mogelijk te zeggen dat:

$$\begin{aligned} C_{f,g}(n) &= \prod_{j=2}^{\infty} \prod_{p>p_n} (1 - p^{-j})^{b_{g-f}(j) - b_g(j)} \\ &= \prod_{j=2}^{\infty} \prod_{p>p_n} (\frac{1}{1 - p^{-j}})^{b_g(j) - b_{g-f}(j)} \\ &= \prod_{j=2}^{\infty} \zeta_n(j)^{b_g(j) - b_{g-f}(j)} \end{aligned}$$

En dat is wat we de hele tijd al wilden.

Literatuur

Dr. P. Moree heeft ons een aantal goede verwijzingen gegeven, met commentaar. De commentaren zijn zeer handig, en worden daarom hier ook weergegeven, met een ster ervoor: *.

[1] Moree, P.
Approximation of singular series and automata (1999)
[2] Homepage van PARI/GP
http://www.parigp-home.de
[3] Website van Gerhard Niklasch
"Some number theoretical constants"
http://www.gn-50uma.de/alula/essays/Moree/Moree.en.shtml
[4] Hooley, Christopher
On Artin's conjecture.
J. Reine Angew. Math. 225 (1967), 209-220.
* Het klassieke artikel waarin Hooley Artin's vermoeden onder aanname van de Gegeneraliseerde Riemann Hypothese bewijst
[5] C. Hooley, Applications of sieve methods to the theory of numbers, Cambridge University Press, Cambridge-New York-Melbourne, 1976.
* Hierin is een hoofdstuk gewijd aan Hooley's bewijs in het bovenstaande artikel. Hooley beperkt zich hier tot het geval a=2.
[6] M. Ram Murty, Artin's conjecture for primitive roots,
Math. Intelligencer 10 (1988), 59-67.
* Inleiding tot het Artin vermoeden *
[7] P. Moree, Artin's primitive root conjecture-a survey, lecture notes
(available at http://turing.wins.uva.nl/ moree/varia.htm)
* Geeft overzicht van de literatuur aan het Artin primitieve wortel vermoeden en zijn generalisaties
[8] H. Cohen,
High precision computation of Hardy-Littlewood constants,
draft of a preprint, available at
http://www.math.u-bordeaux/ cohen/.
* Hier wordt ingegaan op het probleem Euler product