De Stelling van Zsigmondy

Bart Michels

De stelling van Zsigmondy kan heel vaak nuttig zijn in diverse problemen in de getaltheorie. De Oostenrijker Karl Zsigmondy ontdekte de stelling in 1882. De stelling was toen nog helemaal niet bekend. Wie snel even op het internet zoekt naar een elementair bewijs zal helaas gauw ondervinden hoe moeilijk dat te vinden is. In 1904 publiceerden G. D. Birkhoff en H.S. Vandiver een artikel [1] waar ze precies de stelling van Zsigmondy bewezen, zonder die naam te vermelden. Vermoedelijk wisten ze niet eens dat de stelling al bestond. Het bewijs dat hier wordt gegeven is een combinatie van [1, Theorem 4] en een veralgemening van [3, Key Lemma]. Om te kunnen volgen dien je vertrouwd te zijn met de Möbius-inversie en cyclotomische veeltermen. Basiseigenschappen van cyclotomische veeltermen kunnen gevonden worden in [2].

Stelling. *(Zsigmondy)* Zij $a, b \in \mathbb{N}_0$ met $\gcd(a,b) = 1$ en $n \in \mathbb{N}$, $n > 1$. Dan bestaat er een priemgetal dat een deler is van $a^n - b^n$ en niet van $a^k - b^k$ voor alle $k \in \{1, 2, \ldots, n-1\}$, behalve in de gevallen

1. $2^6 - 1^6$.
2. $n = 2$ en $a + b$ is een macht van 2.

Het bewijs stellen we uit tot na het volgende lemma:

Lemma. Als p priem is, $n = p^\alpha q$ een natuurlijk getal zodat $p \nmid q$ en $p \mid \Phi_n(a)$ voor een geheel getal a, dan is $O_p(a) = q$.

Bewijs.
Uit $p \mid \Phi_n(a) \mid a^n - 1 \equiv a^q - 1$ volgt dat $p \nmid a$. Stel dus $O_p(a) = k$, dan is $k \mid q$. Als $k < q$ dan is er een deler $d \mid k$ waarvoor $p \mid \Phi_d(a)$. Aangezien $d \mid q$ en $d < q$ heeft de veelterm $x^q - 1$ een dubbele wortel, a, modulo p, zodat $p \mid q$, wat onmogelijk is. □

Bewijs van de stelling van Zsigmondy.
Neem twee coprieme natuurlijke getallen a en b vast, met $a > b$.
Het volstaat te bewijzen dat er een priemdeler van $a^n - b^n$ is die $a^k - b^k$ niet deelt voor alle positieve delers $k \mid n$ met $k < n$: als $p \mid a^n - b^n$ en c is een inverse van b modulo p, dan geldt voor de kleinste $k > 0$ waarvoor $(ac)^k \equiv 1$ dat $k \mid n$.

We definiëren nu $z_n = a^n - b^n$ en

$$\Psi_n = \prod_{d \mid n} z_{\frac{n}{d}}^{\mu(d)}. \tag{1}$$

Hieruit volgt dat

$$\Psi_n = b^{\varphi(n)}\Phi_n\left(\frac{a}{b}\right). \tag{2}$$

Wegens een multiplicatieve variant op de Möbius-inversie hebben we

$$z_k = \prod_{d|k}\Psi_d. \tag{3}$$

Als $z_n = n = {p_1}^{a_1}\cdots{p_r}^{a_r}$ waarbij $p_{s_1},\ldots,p_{s_t}$ de primitieve priemdelers van z_n zijn, stel dan

$$P_n = {p_{s_1}}^{a_{s_1}}\cdots{p_{s_t}}^{a_{s_t}}.$$

Uit (2) hebben we dat $\Psi_n \in \mathbb{Z}$ en uit (1) volgt dat $P_n \mid \Psi_n$. Stel $\Psi_n = \lambda_n P_n$. We bewijzen dat $P_n > 1$ in alle gevallen die de stelling niet uitsluit.
Uit (3) volgt dat $\Psi_n \mid \frac{z_n}{z_d}$ voor elke positieve deler $d \mid n$ met $d < n$.
Zij p een priemdeler van Ψ_n. Als $p \nmid P(n)$ is p niet primitief, stel $p \mid z_d$. Als $p \nmid n$ zou wegens het Lifting The Exponent Lemma, $v_p(z_n) = v_p(z_d)$ en dus $p \nmid \frac{z_n}{z_d}$, contradictie. Dus $\mathrm{rad}(\lambda_n) \mid n$.
Merk verder op dat $\gcd(\lambda_n, P_n) = 1$. Zoniet zou er een priemgetal p zijn waarvoor $p \mid n = pr$ en $p \mid a^{pr} - b^{pr} \equiv a^r - b^r$, in tegenspraak met het feit dat p primitief is.
Stel dat $\lambda_n > 1$. Indien p een priemdeler van λ_n is met $p^\alpha \| n$ en $n = p^\alpha q$ geldt dus

$$p \mid \Psi_n \mid \Psi_q(a^{p^\alpha}, b^{p^\alpha}) \equiv \Psi_q \pmod{p},$$

waarbij we meer algemeen $\Psi_n(x,y)$ noteren voor

$$y^{\varphi(n)}\Phi_n\left(\frac{x}{y}\right).$$

Als p een priemdeler is van λ_n waarvoor $p \mid \Psi_q$, dan is ofwel $p \mid q$, wat onmogelijk is, of $p \equiv 1 \pmod{q}$. Dus $p > q = \frac{n}{p^\alpha}$. Als r een andere priemdeler is van n, dan is $r \mid q$ zodat $r < q < p$. Dit betekent dat p uniek bepaald is als de grootste priemdeler van n.
Stel dus $\lambda_n = p^\beta$. We zullen bewijzen dat $\beta = 1$.
Zij $d \mid n$ zodat $p \mid z_d$. Noem c een inverse van b modulo p, dan is $p \mid \Psi_n$ en dus $p \mid \Phi(ac)$, zodat wegens het lemma, $O_p(ac) = q$. Dus moeten we zeker hebben dat $q \mid d$.
Uit (1) hebben we nu dat $\beta = v_p(\Psi_n) = v_p(z_n) - v_p(z_{\frac{n}{p}}) = 1$, zoals gewenst.
Om te besluiten dat $P_n > 1$ zijn er drie gevallen:
Als $\lambda_n = 1$, dan is $P_n = \Psi_n \geq (a-b)^{\varphi(n)} \geq 1$. De ongelijkheid is strikt tenzij $n = 2$ en $a - b = 1$, maar dan is de stelling triviaal voldaan.
Als $\lambda_n = p \mid n$ en $a - b > 1$, dan is $P_n = \frac{1}{p}\Psi_n \geq \frac{1}{p}(a-b)^{\varphi(n)} \geq \frac{2^{p-1}}{p} \geq 1$. Opnieuw is de ongelijkheid strikt tenzij $a - b = 2$ en $n = 2$. In dat geval bevat $a + b$ een primitieve priemdeler tenzij $a + b$ een macht van 2 is, wat de stelling voorspelde.
Het geval $\lambda_n = p \mid n$ en $a - b = 1$ is iets ingewikkelder.
Stel dat de ongelijkheid niet strikt is, dus $\Psi_n = p$. Dit zal uiteindelijk het enige overblijvende tegenvoorbeeld opleveren, zijnde $2^6 - 1^6$. Uit $p \mid z_n$ volgt dat p oneven is. Stel opnieuw $n = p^\alpha q$ en c een inverse van b modulo p. Aangezien $p \mid \Psi_n$ hebben we dat $p \mid \Phi_n(ac)$, dus $O_p(ac) = q$ wegens het lemma.
Als $\alpha > 1$ zou $p = \Psi_n = \Psi_{pq}(a^{p^{\alpha-1}}, b^{p^{\alpha-1}})$, maar

$$\Psi_{pq}(a^{p^{\alpha-1}}, b^{p^{\alpha-1}}) \geq (a^{p^{\alpha-1}} - b^{p^{\alpha-1}})^{\varphi(pq)} \geq a^p - b^p = \sum_{k=0}^{p-1}\binom{p}{k}b^k > p$$

omdat $p > 2$, contradictie. Dus $n = pq$. Nu hebben we

$$p = \Psi_n = \frac{\Psi_q(a^p, b^p)}{\Psi_q} \geq \frac{(a^p - b^p)^{\varphi(q)}}{(a+b)^{\varphi(q)}} \geq \frac{a^p - b^p}{a+b} = \frac{1}{2b+1} \sum_{k=0}^{p-1} \binom{p}{k} b^k > \frac{b}{2b+1} \sum_{k=1}^{p-1} \binom{p}{k}.$$

Aangezien $\frac{b}{2b+1} \geq \frac{1}{3}$ hebben we dat $3p > 2^p - 2$.
Dit is onmogelijk als $p > 3$, dus $p = 3$ en $q \mid 2$ omdat $q = O_p(ac) \mid p - 1$.
Dus $n = 3$ of $n = 6$. Als $n = 3$ is de stelling duidelijk waar omdat 3 priem is en $a - b = 1$.
Het geval $n = 6$ blijft over, en inderdaad geldt de stelling hier niet. Uit $a = b + 1$ en $3 = \Psi_6 = a^2 - ab + b^2$ leiden we eenvoudig af dat $a = 2$ en $b = 1$ het enige tegenvoorbeeld is. □

Als gevolg van de stelling hebben we:

Stelling. Zij $a, b \in \mathbb{N}_0$ met $\text{ggd}(a, b) = 1$ en $n \in \mathbb{N}$, $n > 1$. Dan bestaat er een priemgetal dat een deler is van $a^n + b^n$ en niet van $a^k + b^k$ voor alle $k \in \{1, 2, \ldots, n-1\}$, behalve in het geval $2^3 + 1^3$.

Bewijs.
Voor elk natuurlijk getal $n > 1$ waarvoor $2n$ geen uitzondering vormt op de stelling van Zsigmondy, heeft $a^{2n} - b^{2n}$ een primitieve priemdeler p, die ofwel $a^n - b^n$ ofwel $a^n + b^n$ deelt. Echter, p kan geen deler zijn van $a^n - b^n$ omdat p dan niet primitief zou zijn. Dus hebben we $p \mid a^n + b^n$ en $p \nmid a^{2k} - b^{2k}$ voor alle $k < n$. Dit betekent dat $p \nmid a^k + b^k$ voor alle $k < n$, en de stelling volgt. □

Merk op dat de uitzondering $2^6 - 1^6$ weerspiegeld wordt in $2^3 + 1^3$. Het geval $n = 2$ en $a + b$ een macht van 2 verdwijnt omdat we hier enkel $n > 1$ beschouwen.

Referenties

[1] G.D. Brikhoff, H.S. Vandiver, *On the Integral Divisors of $a^n - b^n$*, 1904, `http://www.jstor.org/stable/info/2007263`

[2] Y. Ge, *Elementary Properties of Cyclotomic Polynomials*, `http://www.yimin-ge.com/doc/cyclotomic_polynomials.pdf`

[3] L. Thompson, *Zsigmondy's Theorem*, 2009, `www.artofproblemsolving.com/Forum/download/file.php?id=25872`