

Elementaire Getaltheorie

Deeltentamen, 14 jan 2013, 9-12 uur

OPGAVEN

1. (a) (1 pt) Los $y^2 = 4x^3 + 1$ op in $x, y \in \mathbb{Z}$.
(b) (1 pt) Geef aan hoe je oneindig veel drietallen $x, y, z \in \mathbb{N}$ kunt construeren met de eigenschap $x^2 + y^2 = z^3$.
2. (a) (1 pt) Bewijs dat 31 niet geschreven kan worden als som van 15 vierde machten.
(b) (1 pt) Bewijs dat er oneindig veel getallen zijn die niet kunnen worden geschreven als som van 15 vierde machten.
3. (2 pt) Stel $a, b, c \in \mathbb{Z}_{\geq 3}$. Laat zien dat uit het ABC-vermoeden volgt dat $x^a y^b - z^c = 1$ hooguit eindig veel oplossingen in $x, y, z \in \mathbb{N}$ heeft.
4. Gebruik in de volgende onderdelen de priemgetalstelling.
 - (a) (1 pt) Laat zien dat er een constante $c_1 > 0$ bestaat zó dat

$$\sum_{p \leq x, p \text{ priem}} p < c_1 \frac{x^2}{\log x}$$

voor alle $x \geq 10$.

- (b) (1 pt) Laat zien dat er een constante $c_2 > 0$ bestaat zó dat

$$\sum_{p \leq x, p \text{ priem}} p > c_2 \frac{x^2}{\log x}$$

voor alle $x \geq 10$.

5. Zij p een priemgetal en stel dat $p \equiv 1 \pmod{3}$. Met ω geven we de primitieve derde eenheidswortel $e^{2\pi i/3} = \frac{-1}{2} + \frac{1}{2}\sqrt{-3}$ aan.
 - (a) (1 pt) Laat zien dat er een karakter $\chi : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \mathbb{C}^*$ van orde 3 bestaat.
 - (b) (1/2 pt) Laat zien dat de Jacobisom $J = \sum_{x=2}^{p-1} \chi(x)\chi(1-x)$ van de vorm $a + b\omega$ is met $a, b \in \mathbb{Z}$. Verder is gegeven dat $|J| = \sqrt{p}$.
 - (c) (1/2 pt) Laat zien dat er gehele getallen a, b bestaan zó dat $p = a^2 - ab + b^2$.

UITWERKINGEN VANAF VOLGENDE PAGINA

OPGAVEN en UITWERKINGEN

1. (a) (1 pt) Los $y^2 = 4x^3 + 1$ op in $x, y \in \mathbb{Z}$.

Oplossing: Uit de vergelijking volgt: $y^2 - 1 = 4x^2$ en dus $\frac{y-1}{2} \frac{y+1}{2} = x^2$. De factoren $(y-1)/2$ en $(y+1)/2$ verschillen 1 en hebben dus ggd 1. Uit de vergelijking volgt nu dat er gehele u, v zijn zó dat $(y-1)/2 = u^2$ en $(y+1)/2 = v^2$. Neem het verschil: $v^2 - u^2 = 1$. Het verschil tussen twee derde machten kan alleen 1 zijn als $1^3 - 0^3 = 1$ en $0^3 - (-1)^3 = 1$. In elk van deze gevallen geldt $x = uv = 0$. En dus $y \equiv \pm 1$.

Om preciezer te zijn over het verschil van de derde machten, uit $v^3 - u^3 = 1$ volgt $(v-u)(v^2 + uv + u^2) = 1$ en dus $v - u = 1$ (want $v > u$). Samen met $v^3 - u^3 = 1$ geeft dit $(u+1)^3 - u^3 = 1$ en dus $3u^2 + 3u = 0$. Dus $u = 0$ of $u = -1$.

- (b) (1 pt) Geef aan hoe je oneindig veel drietallen $x, y, z \in \mathbb{N}$ kunt construeren met de eigenschap $x^2 + y^2 = z^3$.

Oplossing: Hier zijn talloos veel mogelijkheden voor zolang we neit eisen dat $\text{ggd}(x, y) = 1$ (en dat doen we niet). Kies bijvoorbeeld $x = y = 2^{3k+1}$. Dan volgt $x^2 + y^2 = 2 \cdot 2^{6k+2} = 2^{6k+3}$, een derde macht.

Een andere, neem de norm aan beide zijden van $a^3 - 3b^2a + i(3a^2b - b^3) = (a + bi)^3$. We krijgen dan, $(a^3 - 3b^2a)^2 + (3a^2b - b^3)^2 = (a^2 + b^2)^3$.

2. (a) (1 pt) Bewijs dat 31 niet geschreven kan worden als som van 15 vierde machten.

Oplossing: Stel 31 is som van 15 vierde machten. De grootste vierde macht kan niet groter dan 2^4 zijn, want $3^4 > 31$. Dus hebben we een aantal malen 1^4 en een aantal malen 2^4 nodig. Van de laatste kan hooguit 1 voorkomen, want 2 maal $2^4 = 32 > 31$. Verder moet er een term 2^4 voorkomen, want 15 maal 1^4 geeft bij elkaar $15 < 31$. Echter, 31 bestaat uit 1 maal 2^4 en 15 maal 1^4 . Dat zijn 16 termen. We concluderen dat 31 niet te schrijven is als som van 15 vierde machten.

- (b) (1 pt) Bewijs dat er oneindig veel getallen zijn die niet kunnen worden geschreven als som van 15 vierde machten.

Oplossing: Door inductie naar k laten we zien dat $16^k \cdot 31$ geen som van 15 vierde machten kan zijn. Het geval is in voorgaand onderdeel gebeurd. Stel $k \geq 0$ en onze bewering voor $16^k \cdot 31$ bewezen. Stel dat $16^{k+1} \cdot 31 = \sum_{i=1}^{15} u_i^4$. Neem de gelijkheid modulo 16: $0 \equiv \sum_{i=1}^{15} u_i^4 \pmod{16}$. Omdat een vierde macht ofwel 0 of 1 modulo 16 is, kan de rechterkant alleen 0 zijn als elk van de u_i even is. Deel aan beide zijden door 16, dan krijgen we $16^k \cdot 31 = \sum_{i=1}^{15} (u_i/2)^4$, in tegenspraak met onze inductiehypothese.

3. (2 pt) Stel $a, b, c \in \mathbb{Z}_{\geq 3}$. Laat zien dat uit het ABC-vermoeden volgt dat $x^a y^b - z^c = 1$ hooguit eindig veel oplossingen in $x, y, z \in \mathbb{N}$ heeft.

Oplossing: We passen ABC toe op $1 + z^c = x^a y^b$. Voor een nader te kiezen $\epsilon > 0$ geldt

$$x^a y^b < c(\epsilon) \text{rad}(x^a y^b z^c)^{1+\epsilon} = c(\epsilon) \text{rad}(xyz)^{1+\epsilon} \leq c(\epsilon) (xyz)^{1+\epsilon}.$$

Gebruik nu de schatting $z < (x^a y^b)^{1/c} \leq (x^a y^b)^{1/3}$. Hieruit volgt,

$$x^{2a/3-1-\epsilon a/3-\epsilon} y^{2b/3-1-\epsilon b/3-\epsilon} < c(\epsilon).$$

Kies nu $\epsilon > 0$ zó dat $2a/3 - 1 - \epsilon - \epsilon a/3 > 1/2$ en $2b/3 - 1 - \epsilon - \epsilon b/3 > 1/2$. Omdat $a, b \geq 3$ kan dat. Dus,

$$(xy)^{1/2} < c(\epsilon).$$

Hieruit volgt dat het product xy begrensd is en dus elk van x, y an, a fortiori, z .

4. Gebruik in de volgende onderdelen de priemgetalstelling.

(a) (1 pt) Laat zien dat er een constante $c_1 > 0$ bestaat zó dat

$$\sum_{p \leq x, p \text{ priem}} p < c_1 \frac{x^2}{\log x}$$

voor alle $x \geq 10$.

Oplossing: Merk op dat

$$\sum_{p \leq x, p \text{ priem}} p < \sum_{p \leq x, p \text{ priem}} x = x\pi(x).$$

Onze grens volgt doordat er een $c_1 > 0$ bestaat zó dat $\pi(x) < c_1 x / \log x$.

(b) (1 pt) Laat zien dat er een constante $c_2 > 0$ bestaat zó dat

$$\sum_{p \leq x, p \text{ priem}} p > c_2 \frac{x^2}{\log x}$$

voor alle $x \geq 10$.

Oplossing Er bestaat een x_0 zó dat $0.9x / \log x < \pi(x) < 1.1x / \log x$ voor alle $x > x_0$. Merk nu op,

$$\sum_{p \leq x, p \text{ priem}} p > \sum_{x/2 < p \leq x, p \text{ priem}} p > \sum_{x/2 < p \leq x, p \text{ priem}} (x/2) = x(\pi(x) - \pi(x/2))/2.$$

Als $x > 2x_0$, geldt

$$\pi(x) - \pi(x/2) > 0.9 \frac{x}{\log x} - 1.1 \frac{x/2}{\log(x/2)} = \frac{x}{\log x} \left(0.9 - 0.55 \frac{\log x}{\log x - \log 2} \right).$$

Voor x voldoende groot geldt dat de laatste factor > 0.3 is. Voor voldoende grote x vinden we dus de ondergrens $0.3x^2 / \log x$. Voor de kleinere $x > 10$ kan de constante c_2 geschikt gekozen worden.

5. Zij p een priemgetal en stel dat $p \equiv 1 \pmod{3}$. Met ω geven we de primitieve derde eenheidswortel $e^{2\pi i/3} = \frac{-1}{2} + \frac{1}{2}\sqrt{-3}$ aan.

- (a) (1 pt) Laat zien dat er een karakter $\chi : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \mathbb{C}^*$ van orde 3 bestaat.

Oplossing: Zij g een primitieve wortel modulo p . Een karakter wordt gekozen door als waarde voor $\chi(g)$ een $p-1$ -e éénheidswortel te kiezen. Als $p \equiv 1 \pmod{3}$ dan is ω een $p-1$ -e éénheids wortel, immers $\omega^{p-1} = 1$.

- (b) (1/2 pt) Laat zien dat de Jacobisom $J = \sum_{x=2}^{p-1} \chi(x)\chi(1-x)$ van de vorm $a + b\omega$ is met $a, b \in \mathbb{Z}$. Verder is gegeven dat $|J| = \sqrt{p}$.

Oplossing: De som J is een som van termen van de vorm ω^m voor diverse m . Omdat $\omega^3 = 1$ kunnen we $m = 0, 1, 2$ nemen. Merk op $\omega^2 = -\omega - 1$. Daarmee is J een lineaire combinatie van $1, \omega$ met gehele coëfficiënten.

- (c) (1/2 pt) Laat zien dat er gehele getallen a, b bestaan zó dat $p = a^2 - ab + b^2$.

Oplossing: We weten dat er $a, b \in \mathbb{Z}$ bestaan zó dat $J = a + b\omega$. Neem aan beide zijden de absolute in het kwadraat:

$$p = |J|^2 = (a + b\omega)(a + b\bar{\omega}) = a^2 + b^2 + (\omega + \bar{\omega})ab = a^2 + b^2 - ab.$$