

## Deeltentamen II Elementaire Getaltheorie, 2-2-2007, 14-17 uur

Tijdens dit tentamen mogen boek en aantekeningen niet gebruikt worden. Alleen een eenvoudige calculator is toegestaan. Geef een goede onderbouwing van je antwoorden. Succes!

1. (2 pt) Beschouw de vergelijking  $x^2 + y^2 + z^2 = 2(x+y+z)^3$  in  $x, y, z \in \mathbb{Z}$ .
  - (a) Laat zien dat voor elke oplossing de waarden van  $x, y, z$  even zijn.
  - (b) Laat zien dat  $x = y = z = 0$  de enige oplossing is.

### Uitwerking.

- a)  $x^2 + y^2 + z^2$  is even. Dus ofwel  $x, y, z$  zijn allen even, of één van hen is even en de andere twee oneven. In het eerste geval zijn we klaar. In het tweede geval geldt dat, omdat kwadraten  $0, 1 \pmod{4}$  zijn,  $x^2 + y^2 + z^2 \equiv 2 \pmod{4}$ . De rechterzijde  $2(x+y+z)^2$  is echter deelbaar door 4. Het tweede geval kan dus niet optreden.
- b) Omdat  $x, y, z$  even zijn kunnen we  $x = 2x_1, y = 2y_1, z = 2z_1$  met  $x_1, y_1, z_1$  geheel veronderstellen. Onze vergelijking gaat over in

$$x_1^2 + y_1^2 + z_1^2 = 4(x_1 + y_1 + z_1)^3.$$

Net als in a) kunnen we laten dat  $x_1, y_1, z_1$  even zijn, dat wil zeggen  $x_1 = 2x_2, y_1 = 2y_2, z_1 = 2z_2$ . We vinden

$$x_2^2 + y_2^2 + z_2^2 = 8(x_2 + y_2 + z_2)^3.$$

Net als in a) vinden we dat  $x_2, y_2, z_2$  even zijn, etc. Zo doorgaand zien we dat  $x, y, z$  deelbaar zijn door willekeurig hoge machten van 2. Dit kan alleen als  $x = y = z = 0$ .

Een tweede, iets nettere, oplossing. Stel  $x, y, z$  niet alle drie nul en zij  $k$  het grootste gehele getal zó dat  $2^k$  zowel  $x, y$  als  $z$  deelt. Stel  $x = 2^k x', y = 2^k y', z = 2^k z'$ . Minstens één van de getallen  $x', y', z'$  is oneven. We vinden,

$$(x')^2 + (y')^2 + (z')^2 = 2^{k+1}(x' + y' + z')^3.$$

Net als in a) volgt nu dat  $x', y', z'$  alledrie even moeten zijn, in tegenspraak met het feit dat  $k$  maximaal gekozen was.

2. (2 pt) Beschouw de vergelijking  $x^3 + y^3 = z^4$  in  $x, y, z \in \mathbb{Z}$ .
- (a) Laat zien dat, onder aanname van het *abc*-vermoeden, de vergelijking hooguit eindig veel oplossingen heeft met  $\text{ggd}(x, y, z) = 1$ .
- (b) Laat zien dat er oneindig veel oplossingen zijn als we de conditie  $\text{ggd}(x, y, z) = 1$  laten vervallen.

### **Uitwerking.**

- a) We onderscheidem twee gevallen,  $x, y > 0$  en  $x, y$  tegengesteld teken. Het geval  $x, y < 0$  kan niet optreden omdat  $x^3 + y^3$  positief moet zijn. De gevallen met  $x$  of  $y$  gelijk aan nul zijn triviaal,  $0^3 + 0^3 = 0^4$  en  $0^3 + 1^3 = 1^4$ .

Eerst  $x, y > 0$ . We passen het *abc*-vermoeden met  $a + b = c$  toe met  $a = x^3, b = y^3$  en  $c = z^4$ . We krijgen,

$$z^4 < c(\epsilon)N(x^3y^3z^4)^{1+\epsilon} \leq c(\epsilon)(xyz)^{1+\epsilon}.$$

Uit  $x^3 + y^3 = z^4$  en  $x, y > 0$  volgt dat  $x, y < z^{4/3}$ . Gebruiken we dit, dan zien we

$$z^4 < c(\epsilon)z^{11(1+\epsilon)/3}.$$

Als we  $\epsilon$  zó kiezen dat  $11(1+\epsilon)/3 < 4$  dan volgt dat  $z$  begrensd is. Bijvoorbeeld  $\epsilon = 1/22$ . Dan volgt  $z^4 < c(1/22)z^{23/6}$  en dus  $z^{1/6} < c(1/22)$ . Met andere woorden,  $z$  is begrensd.

Nu het geval dat  $x, y$  tegengesteld teken hebben. Bijvoorbeeld  $x > 0$  en  $y < 0$ . Dan passen we *abc* toe op  $z^4 + |y|^3 = x^3$ . Nu volgt

$$x^3 < c(\epsilon)N(x^3|y|^3z^4)^{1+\epsilon} \leq c(\epsilon)(x|y|z)^{1+\epsilon}.$$

Gebruik nu dat  $z < x^{3/4}, |y| < x$ . We vinden

$$x^3 < c(\epsilon)x^{11(1+\epsilon)/4}.$$

Wederom geeft de keuze  $\epsilon = 1/22$  het gewenste resultaat.

- b) Merk op dat  $2^k + 2^k = 2^{k+1}$ . Als we  $k$  zó kiezen dat  $k$  deelbaar is door 3 en  $k + 1$  deelbaar door 4 dan zijn we klaar. Dit kan met de keuze  $k = 12m + 3$ .

3. (2 pt) Beschouw de vergelijking  $x^2 + y^2 = z^2 + 1$  in  $x, y, z \in \mathbb{Z}$  met  $x, y, z > 1$ .
- (a) Geef tenminste twee oplossingen.
  - (b) Laat zien dat er oneindig veel oplossingen zijn.
  - (c) Geef een expliciete formule die een oneindige deelverzameling van oplossingen geeft.

### **Uitwerking**

- a) Twee oplossingen zijn gauw gevonden:  $5^2 + 5^2 = 7^2 + 1$  en  $11^2 + 7^2 = 13^2 + 1$ .
- b) We weten dat als een getal alleen priemfactoren 2 en  $1 \pmod{4}$  heeft, het te schrijven is als som van twee kwadraten. Als er minstens twee verschillende priemfactoren  $1 \pmod{4}$  voorkomen, dan kan dat op meer dan 1 manier. Een getal van de vorm  $z^2 + 1$  heeft alleen maar priemfactoren 2 en  $1 \pmod{4}$ . Als we ervoor zorgen dat  $z^2 + 1$  meerdere priemdelers  $1 \pmod{4}$  heeft, zijn we klaar. Kies daartoe  $z \equiv 2 \pmod{10}$ . Dan is  $z^2 + 1$  oneven en deelbaar door 5. Als  $z$  groot genoeg is, zijn er naast 5 ook andere priemdelers  $1 \pmod{4}$ , en is  $z^2 + 1$  op meer dan 1 manier som van twee kwadraten.

De oplossing volgt ook uit onderdeel c).

- c) Herschrijf de vergelijking als  $x^2 - 1 = z^2 - y^2$ . We moeten dus  $x^2 - 1$  schrijven als verschil van twee kwadraten. Dit was een huiswerkopgave. Nemen we  $x$  even,  $x = 2m$  dan kunnen we  $z = 2m^2, y = 2m^2 - 1$  kiezen.

Maar, er zijn ook talloze andere oplossingen (ik heb er heel veel gezien in de uitwerkingen).

4. (2 pt) Laat zien dat de oneindige som

$$\sum_{n=0}^{\infty} \frac{1}{2^{n^2}}$$

een irrationale waarde heeft.

**Uitwerking.** Noem de som  $\alpha$  en stel dat  $\alpha = p/q$  rationaal is. Definieer voor willekeurige  $k$ ,

$$\alpha_k = \sum_{n=0}^k \frac{1}{2^{n^2}}.$$

Dan is  $\alpha - \alpha_k$  een positief rationaal getal met noemer die  $q2^{k^2}$  deelt. Dus

$$\alpha - \alpha_k \geq \frac{1}{q2^{k^2}}.$$

Anderzijds,

$$\begin{aligned} \alpha - \alpha_k &= \frac{1}{2^{(k+1)^2}} + \frac{1}{2^{(k+2)^2}} + \frac{1}{2^{(k+3)^2}} + \dots \\ &< \frac{1}{2^{(k+1)^2}} \left( 1 + \frac{1}{2} + \frac{1}{2^2} + \dots \right) \\ &= \frac{2}{2^{(k+1)^2}} \end{aligned}$$

Combinatie van onder- en bovengrens geeft

$$\frac{1}{q2^{k^2}} < \frac{2}{2^{(k+1)^2}},$$

waaruit volgt dat  $2^{2k} < q$ . Omdat  $k$  willekeurig gekozen kan worden krijgen we hier een tegenspraak als we  $k$  groot genoeg kiezen.

5. (2 pt) In het diktaat is bewezen dat  $\prod_{p \text{ priem}, p \leq n} p < 4^n$  voor alle  $n \in \mathbb{N}$ . Gebruik dit resultaat om te bewijzen dat er een constante  $C > 0$  bestaat zó dat

$$\text{kgv}(1, 2, \dots, n) < C^n$$

voor alle  $n \in \mathbb{N}$ .

**Uitwerking.** Deze vond men de moeilijkste en dat was ook wel zo. Het is een variant op opgave 10.3.8. Er geldt dat

$$\text{kgv}(1, 2, \dots, n) = \prod_{p \text{ priem}, p \leq n} p^{\lfloor \log n / \log p \rfloor}.$$

Merk op dat als  $p > \sqrt{n}$  dan geldt  $\lfloor \log n / \log p \rfloor = 1$  en als  $p \leq \sqrt{n}$ , dan geldt  $\lfloor \log n / \log p \rfloor \leq \log n / \log p$ . In het bijzonder,  $p^{\lfloor \log n / \log p \rfloor} \leq n$ . Deze twee combinerend vinden we dat

$$\text{kgv}(1, 2, \dots, n) < \prod_{p \text{ priem}, p \leq n} p \prod_{p \text{ priem}, p \leq \sqrt{n}} n.$$

Het eerste product schatten we af met  $4^n$ , het tweede met  $n^{\pi(\sqrt{n})} < n^{\sqrt{n}}$ . Dus,

$$\text{kgv}(1, 2, \dots, n) < 4^n n^{\sqrt{n}} = 4^n \exp(\sqrt{n} \log n).$$

Omdat  $\sqrt{n} \log n = O(n)$  volgt onze bewering.