

Hertentamen Elementaire Getaltheorie

23-3-2007, 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. (a) Bepaal alle $x \in \mathbb{Z}$ die tegelijkertijd voldoen aan de zes volgende congruentievergelijkingen,

$$\begin{aligned}x &\equiv -1 \pmod{2}, & x &\equiv -1 \pmod{4}, & x &\equiv -1 \pmod{6}, \\x &\equiv -1 \pmod{3}, & x &\equiv -1 \pmod{5}, & x &\equiv 0 \pmod{7}.\end{aligned}$$

- (b) Zij $a, b \in \mathbb{Z}$ en m, k een tweetal natuurlijke getallen. Stel dat $a^k \equiv b^k \pmod{m}$ en $a^{k+1} \equiv b^{k+1} \pmod{m}$.

Laat zien, onder de aanname $\text{ggd}(a, m) = 1$, dat $a \equiv b \pmod{m}$.

Geldt dezelfde conclusie als $\text{ggd}(a, m) > 1$?

Uitwerking

Deel a) is standaard rekenwerk. Dat kan nog vereenvoudigd worden door op te merken dat de eerste 5 vergelijkingen allemaal van de vorm $x + 1 \equiv 0 \pmod{m}$ zijn. Dus $x + 1$ moet deelbaar zijn door 2, 3, 4, 5, 6. Anders gezegd, $x + 1$ is deelbaar door het kgv van 2, 3, 4, 5, 6 en dat is 60. Dus $x \equiv -1 \pmod{60}$. Samen met $x \equiv 0 \pmod{7}$ geeft dit op de standaard manier $x \equiv 119 \pmod{420}$.

Deel b). Stel $\text{ggd}(a, m) = 1$. Merk op dat $a^{k+1} \equiv b^{k+1} \equiv ba^k \pmod{m}$, waarbij we $b \equiv a^k \pmod{m}$ voor de tweede gelijkheid gebruikten. We vinden dus $a^{k+1} \equiv ba^k \pmod{m}$. Neem aan beide kanten de inverse van $a^k \pmod{m}$ en we houden over, $a \equiv b \pmod{m}$.

Als $\text{ggd}(a, m) > 1$ geldt de conclusie niet. Neem bijv $m = 4, a = 2, b = 4, k = 2$. Er geldt zeker $2^3 \equiv 4^3 \pmod{4}$ en $2^2 \equiv 4^2 \pmod{4}$ maar NIET $2 \equiv 4 \pmod{4}$.

2. (a) Zij a een oneven geheel getal. Bewijs dat $a^2 + 4$ een priemdelers p heeft met $p \equiv 5 \pmod{8}$.
- (b) Laat zien, gebruikmakend van het vorige onderdeel, dat er oneindig veel priemgetallen p van de vorm $p \equiv 5 \pmod{8}$ zijn.

Uitwerking

Het principe van deze som is Exercise 5.7.12 van het diktaat.

Deel a) Zij p een priemdelers van $a^2 + 4$. Om te beginnen is p oneven, want $a^2 + 4$ is oneven. Verder geldt $a^2 \equiv -4 \pmod{p}$. Dus -4 is kwadraatrest modulo p en daarmee is ook -1 kwadraatrest modulo p . Dus $p \equiv 1 \pmod{4}$. Modulo 8 kan p dus 1 of 5 zijn. Echter, a is oneven, dus $a^2 \equiv 1 \pmod{8}$ en daarmee $a^2 + 4 \equiv 5 \pmod{8}$. Dat betekent dat niet alle priemdelers van $a^2 + 4$ van de vorm $1 \pmod{8}$ kunnen zijn. Dus is er een priemdelers $5 \pmod{8}$.

Deel b) Dit is het standaard argument á la Euclides. Stel er zijn eindig veel priemgetallen $5 \pmod{8}$. Noem ze p_1, \dots, p_r . Beschouw het getal $(p_1 \cdots p_r)^2 + 4$. Deze is volgens onderdeel a) deelbaar door een priemgetal q dat $5 \pmod{8}$ is. Dus q deelt $p_1 \cdots p_r$ (naast $(p_1 \cdots p_r)^2 + 4$). Gevolg q deelt 4 en we hebben een tegenspraak.

3. (a) Laat zien dat er oneindig veel drietallen x, y, z van natuurlijke getallen bestaan zó dat $x^2 + y^2 = 5z^2$ en $\text{ggd}(x, y) = 1$.
- (b) Laat zien dat er oneindig veel drietallen x, y, z van natuurlijke getallen bestaan zó dat $x^2 + y^2 = x^3$ en $\text{ggd}(x, y) = 1$.

Uitwerking

Deel a). Beschouw het getal $x + iy = (2 + i)(a + bi)^2$. Neem aan beide zijden de norm: $x^2 + y^2 = 5(a^2 + b^2)^2$. Uitwerking geeft $x + iy = 2(a^2 - b^2 - 2ab) + i(a^2 - b^2 + 4ab)$ en $z = a^2 + b^2$.

Kies a, b met verschillende pariteit en met $\text{ggd} = 1$. Dan is x even en y oneven. Stel dat ze een oneven priemfactor p gemeenschappelijk hebben. Dan deelt p zowel $a^2 - b^2$ als ab . Als $p|a$, dan volgt uit $p|(a^2 - b^2)$ dat p ook b deelt, in tegenspraak met $\text{ggd}(a, b) = 1$. Evenzo, als $p|b$ dan volgt meteen dat $p|a$.

Deel b). De x^3 rechts had een z^3 moeten zijn, excuus, in depuntentelling is er rekening mee gehouden. De vergelijking zoals die er nu staat heeft precies één oplossing, namelijk $x = 1, y = 0$. De afleiding hiervan is als goed gerekend. De som die er had moeten staan was een vereenvoudigde versie van Exercise 9.8.3 van het diktaat.

4. Zij $m \in \mathbb{Z}$ en $m > 2$. In de volgende onderdelen van deze opgave zullen we laten zien dat, onder aanname van de juistheid van het *abc*-vermoeden, de vergelijking

$$\binom{n}{2} = x^m$$

hooguit eindig veel oplossingen heeft in positieve gehele getallen n, x .

- (a) Stel dat n even is. Laat zien dat er positief gehele getallen u, v zijn, zó dat $n = 2u^m$ en $n - 1 = v^m$.
- (b) Stel dat n even is. Laat nu zien dat het *abc*-vermoeden impliceert dat $\binom{n}{2} = x^m$ hooguit eindig veel oplossingen heeft met n even.
- (c) Bewijs dezelfde uitspraak als daarnet, maar nu voor n oneven.

Uitwerking

Deel a). Uit de vergelijking volgt dat $n(n - 1) = 2x^m$. Gegeven is dat n even is. Dus $(n/2)(n - 1) = x^m$. De getallen $n/2$ en $n - 1$ zijn relatief priem, hun product is een m -de macht, dat betekent dat $n/2$ en $n - 1$ beiden m -de macht zijn. Er zijn dus $u, v \in \mathbb{N}$ zó dat $n/2 = u^m$ en $n - 1 = v^m$.

Deel b). Uit $n = 2u^m, n - 1 = v^m$ volgt dat $2u^m = v^m + 1$. Gebruik nu het *abc*-vermoeden met $\epsilon = 0.1$. Hieruit volgt $2u^m < C \cdot N(2u^m v^m)^{1.1} \leq C \cdot (2uv)^{1.1}$. Uit $v^m < 2u^m$ volgt zeker dat $v < 2u$. Gebruiken we dit in onze afchatting,

$$2u^m < C \cdot (4u^2)^{1.1} < 5Cu^{2.2}$$

Dus $u^{m-2.2} < 5C/2$. Omdat $m \geq 3$ volgt hieruit dat u begrensd is.

Deel c) Deze gaat helemaal analoog aan a)b), maar nu met $n = u^m, n - 1 = 2v^m$. In de puntentelling is deze niet meegeteld.

5. Zij q een natuurlijk getal ≥ 2 .

(a) Bewijs dat

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

irrationaal is.

(b) Zij $a \in \mathbb{Z}_{>0}$. Bewijs dat

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

irrationaal is.

Uitwerking Deel a). Noem de oneindige som α en stel

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

Stel dat $\alpha = a/b$ rationaal. Dan is $\alpha - \alpha_k$ positief, rationaal met een noemer die bq^{k^2} deelt. Dus $\alpha - \alpha_k \geq 1/bq^{k^2}$. Anderzijds geldt dat

$$\begin{aligned} \alpha - \alpha_k &= \frac{1}{q^{(k+1)^2}} + \frac{1}{q^{(k+2)^2}} + \frac{1}{q^{(k+3)^2}} + \dots \\ &= \frac{1}{q^{(k+1)^2}} \left(1 + \frac{1}{q^{2k+3}} + \frac{1}{q^{4k+8}} + \dots \right) \\ &< \frac{1}{q^{(k+1)^2}} \left(1 + \frac{1}{q} + \frac{1}{q^2} + \dots \right) \\ &\leq \frac{2}{q^{(k+1)^2}} \end{aligned}$$

Zetten we onder- en bovengrens achter elkaar, $1/bq^{k^2} < 1/q^{(k+1)^2}$. Na vermenigvuldigen met $q^{(k+1)^2}$ krijgen we: $q^{2k+1} < b$. Dit geeft een tegenspraak als we k groot genoeg kiezen.