Elementaire Getaltheorie (WISB321)

Tentamen, 5 november 2014, 8:30 -11:30 uur

Bij dit tentamen is gebruik van boeken, dictaat of aantekeningen niet toegestaan. Als rekenhulp kun je een eenvoudige calculator gebruiken (dus geen GR of smartphone). Als je een onderdeel mist mag je wel het resultaat ervan in de volgende onderdelen gebruiken. Motiveer je antwoorden!
Veel succes!

1. (a) (1 pt) Los $x^2 \equiv 1 (\text{mod } 1000)$ op in $x \in \mathbb{Z}$.

   (b) (1 pt) Zij k geheel en ≥ 3. Hoeveel restklassen x modulo 10^k heeft $x^2 \equiv 1 (\text{mod } 10^k)$ als oplossing?

   Oplossing (a). Wegens de Chinese Reststelling is $x^2 \equiv 1 (\text{mod } 1000)$ dan en slechts dan als $x^2 \equiv 1 (\text{mod } 8)$ en $x^2 \equiv 1 (\text{mod } 125)$. We weten dat $x^2 \equiv 1 (\text{mod } 8)$ precies geldt voor oneven x, oftewel voor $x \equiv 1 (\text{mod } 2)$. Stel dat $x^2 \equiv 1 (\text{mod } 125)$, oftewel dat 125 een deler is van $x^2 - 1 = (x-1)(x+1)$. Omdat $x-1$ en $x+1$ verschil 2 hebben, kunnen ze niet allebei deelbaar zijn door 5. We concluderen dat één van $x-1$ en $x+1$ deelbaar moet zijn door 125, oftewel dat $x \equiv \pm 1 (\text{mod } 125)$. Andersom is het duidelijk dat zulke x voldoen aan $x^2 \equiv 1 (\text{mod } 125)$. Met de Chinese Reststelling weten we nu dat de oplossingen worden gegeven door twee restklasses modulo 250, en dit zijn duidelijk $\pm 1 (\text{mod } 250)$. □

   Oplossing (b). Wegens de Chinese Reststelling is $x^2 \equiv 1 (\text{mod } 10^k)$ dan en slechts dan $x^2 \equiv 1 (\text{mod } 2^k)$ en $x^2 \equiv 1 (\text{mod } 5^k)$. Als $x^2 \equiv 1 (\text{mod } 2^k)$, dan is 2^k een deler van $x^2 - 1 = (x-1)(x+1)$. Nu moeten $x-1$ en $x+1$ allebei even zijn. Omdat ze 2 verschillen, kunnen ze niet allebei deelbaar zijn door 4, dus één van $x-1$ en $x+1$ moet deelbaar zijn door 2^{k-1}. Dit geeft modulo 2^k de vier restklassen $\pm 1, 2^{k-1} \pm 1$, en deze voldoen allemaal. We kunnen op een manier analoog aan opgave (a) laten zien dat $x^2 \equiv 1 (\text{mod } 5^k)$ dan en slechts dan als $x \equiv \pm 1 (\text{mod } 5^k)$. We concluderen dat er modulo 10^k precies $4 \cdot 2 = 8$ oplossingen zijn. □

2. Zij $x \in \mathbb{N}$ en p een oneven priemdeler van $x^2 + 3$.

   (a) (1 pt) Bewijs dat $p = 3$ of $p \equiv 1 (\text{mod } 3)$ (gebruik hiervoor de kwadratische weder-kerigheidswet).

   (b) (1/2 pt) Stel bovendien dat x even is. Bewijs dat $x^2 + 3$ deelbaar is door een priemgetal p van de vorm $4k - 1$.

   (c) (1/2 pt) Bewijs dat er oneindig veel priemgetallen bestaan van de vorm $12k + 7$.

Oplossing (a). Stel dat p een priemdeler is van x^2+3. Dan is $x^2 \equiv -3 (\text{mod } p)$, oftewel -3 is een kwadraatrest modulo p. Als $p \notin \{2,3\}$, dan vinden met kwadratische wederkerigheid dat

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{3-1}{2}} \left(\frac{p}{3}\right) = (-1)^{p-1}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)$$

en dit is gelijk aan 1 dan en slechts dan als $p \equiv 1 (\text{mod } 3)$. □

Oplossing (b). Stel dat x^2+3 geen priemdelers van de vorm $4k-1$ heeft. Omdat x even is, is x^2+3 oneven, dus 2 is geen priemdeler van x^2+3. Dit betekent dat alle priemdelers van x^2+3 congruent zijn aan $1 (\text{mod } 4)$, dus dan is x^2+3 zelf ook $1 (\text{mod } 4)$. Echter, omdat x even is, is x^2 deelbaar door 4, dus volgt $x^2+3 \equiv 3 (\text{mod } 4)$, tegenspraak. □

Oplossing (c). Stel dat er maar eindig veel priemgetallen van de vorm $12k+7$ zijn, zeg $p_1, \ldots, p_r$ voor een zekere $r \in \mathbb{N}$. Definieer nu $N = (2p_1 \cdots p_k)^2 + 3$. Wegens opgave (b) heeft N een priemdeler q congruent aan $-1 (\text{mod } 4)$. Omdat 3 niet van de vorm $12k+7$ is, is $2p_1 \cdots p_k$ niet deelbaar door 3, en N ook niet. Uit opgave (a) volgt nu dat $q \equiv 1 (\text{mod } 3)$. Nu volgt dat $q \equiv 7 (\text{mod } 12)$, dus q moet gelijk zijn aan p_i voor een i met $1 \leq i \leq r$. Nu is q een deler van $2p_1 \cdots p_k$ en van N, dus ook van 3. Maar dan volgt $q = 3$, tegenspraak. □

3. (1 pt) Zij p, q en tweetal priemgetallen met de eigenschap dat $q = 2p+1$. Bewijs dat

$$\left(\frac{a}{q}\right) = -1,\ a \not\equiv -1 (\text{mod } q) \iff a \text{ is primitieve wortel modulo } q.$$

Oplossing. De orde van a modulo q is een deler van $\varphi(q) = q-1 = 2p$, dus $\text{ord}(a) \in \{1, 2, p, 2p\}$. Nu geldt dat a *geen* primitieve wortel modulo q is dan en slechts dan als $\text{ord}(a) \neq 2p$; dan en slechts dan als $\text{ord}(a) \in \{1, 2, p\}$; dan en slechts dan als $a \equiv 1 (\text{mod } q)$, $a^2 \equiv 1 (\text{mod } q)$ of $a^p \equiv 1 (\text{mod } q)$. We weten dat $a^2 \equiv 1 (\text{mod } q)$ precies als $a \equiv \pm 1 (\text{mod } q)$. Verder is $a^p \equiv a^{\frac{q-1}{2}} \equiv \left(\frac{a}{q}\right) (\text{mod } q)$. We vinden dus dat a een primitieve wortel modulo q is dan en slechts dan als $a \not\equiv \pm 1 (\text{mod } q)$ en $\left(\frac{a}{q}\right) \equiv -1 (\text{mod } q)$. Omdat 1 altijd een kwadraatrest modulo q is, is dit laatste weer equivalent met $a \not\equiv -1 (\text{mod } q)$ en $\left(\frac{a}{q}\right) \equiv -1 (\text{mod } q)$. □

4. Beschouw de vergelijking $3x^2 + 3y^2 = z^2$ in $x, y, z \in \mathbb{Z}$.

   (a) (1/2 pt) Bewijs dat voor elke oplossing geldt $3|x, 3|y, 3|z$.

(b) (1/2 pt) Bepaal alle oplossingen.

Oplossing (a). Het is duidelijk dat $3 \mid z^2$ en omdat 3 priem is, moet 3 nu ook een deler zijn van z. Maar dan is 9 en deler van $z^2 = 3(x^2 + y^2)$, dus $3 \mid x^2 + y^2$. Omdat kwadraten gelijk zijn aan 0 of 1 modulo 3, kan dit alleen gelden als x en y beide deelbaar zijn door 3. □

Oplossing (b). Het is duidelijk dat $(0, 0, 0)$ een oplossing is. Stel nu dat $(x, y, z) \neq (0, 0, 0)$. Door sommige van x, y en z te vervangen door resp. $-x$, $-y$ en $-z$, kunnen we aannemen dat x, y en z allemaal niet-negatief zijn. Definieer nu $d = \text{ggd}(x, y, z)$; deze is gedefinieerd omdat minstens één van x, y en z positief is. Nu is $\text{ggd}(x/d, y/d, z/d) = 1$. Echter, $(x/d, y/d, z/d)$ is ook weer een oplossing van de gegeven vergelijking, dus uit opgave (a) volgt dat ze alledrie deelbaar zijn door 3, tegenspraak. We concluderen dat $(0, 0, 0)$ de enige oplossing is. □

5. Zij $m \in \mathbb{N}$.

   (a) (1 pt) Bepaal de kettingbreuk van $\sqrt{9m^2 + 3}$.

   (b) (1/2 pt) Bepaal de oplossing van $x^2 - (9m^2 + 3)y^2 = 1$ in $x, y \in \mathbb{N}$ met kleinst mogelijke y.

   (c) (1/2 pt) Zelfde vraag, maar nu met de één na kleinst mogelijke y.

Oplossing (a). Gebruik makend van $3m = \sqrt{9m^2} < \sqrt{9m^2 + 3} < \sqrt{9m^2 + 6m + 1} = 3m + 1$ vinden we

$$\begin{aligned} \sqrt{9m^2 + 3} &= 3m + (\sqrt{9m^2 + 3} - 3m); \\ \frac{1}{\sqrt{9m^2 + 3} - 3m} &= \frac{\sqrt{9m^2 + 3} + 3m}{3} = 2m + \frac{\sqrt{9m^2 + 3} - 3m}{3}; \\ \frac{3}{\sqrt{9m^2 + 3} - 3m} &= \sqrt{9m^2 + 3} + 3m = 6m + (\sqrt{9m^2 + 3} - 3m). \end{aligned}$$

We concluderen dat $\sqrt{9m^2 + 3} = \langle 3m, \overline{2m, 6m} \rangle$. □

Oplossing (b). We berekenen $\langle 3m, 2m \rangle = 3m + \frac{1}{2m} = \frac{6m^2+1}{2m}$ en gaan na dat

$$(6m^2 + 1)^2 - (9m^2 + 1)(2m)^2 = (36m^4 + 12m^2 + 1) - (9m^2 + 3) \cdot 4m^2 = 1.$$

Uit stelling 16.1.3 volgt nu dat $(6m^2 + 1, 2m)$ de oplossing met minimale y is. □

Oplossing (c). Deze vinden we door $(6m^2 + 1) + \sqrt{9m^2 + 3} \cdot 2m$ te kwadrateren of door $\langle 3m, 2m, 6m, 2m \rangle$ uit te rekenen. Het antwoord is $(72m^4 + 24m^2 + 1, 24m^3 + 4m)$. □

6. (2 pt) Zij $A \in \mathbb{N}$. Bewijs, uitgaande van het *abc*-vermoeden, dat er hooguit eindig veel viertallen $x, y, p, q \in \mathbb{Z}_{\geq 2}$ zijn zó dat

$$x^p - y^q = A$$

en $\min(p, q) \geq 3$.

Oplossing. We lossen eerst het geval op dat $\text{ggd}(x^p, y^q, A) = 1$. Voor elke $\epsilon > 0$ bestaat er een constante $c_0(\epsilon)$ zodat, als $x^p > c_0(\epsilon)$, er geldt dat $x^p < \text{rad}\,(x^p y^q A)^{1+\epsilon}$. We vinden,

$$\begin{aligned} x^p &< \text{rad}\,(x^p y^q A)^{1+\epsilon} \leq \text{rad}\,(x^p y^q A)^{1+\epsilon} \\ &= \text{rad}\,(xy \cdot A)^{1+\epsilon} \leq (xy \cdot A)^{1+\epsilon} \leq (xyA)^{1+\epsilon} \end{aligned}$$

Er geldt $y^q = x^p - A < x^p$, dus $y < x^{\frac{p}{q}}$. Verder geldt $\frac{1}{p} + \frac{1}{q} \leq \frac{1}{2} + \frac{1}{3} = \frac{5}{6}$, omdat $p, q \geq 2$ en bovendien minstens één van p en q minstens 3 is. Dit gebruiken we om te vinden

$$x^p < (xyA)^{1+\epsilon} < \left(x \cdot x^{\frac{p}{q}}\right)^{1+\epsilon} A^{1+\epsilon} = \left((x^p)^{\frac{1}{p}+\frac{1}{q}}\right)^{1+\epsilon} A^{1+\epsilon} \leq (x^p)^{\frac{5}{6}(1+\epsilon)} A^{1+\epsilon}.$$

Kies nu $\epsilon = \frac{1}{6}$ (of een andere $\epsilon < \frac{1}{5}$). Dan geldt, als $x^p > c_0\left(\frac{1}{6}\right)$, dat $x^p < (x^p)^{\frac{35}{36}} A^{\frac{7}{6}}$, waaruit volgt dat $(x^p)^{\frac{1}{36}} < A^{\frac{7}{6}}$, en dus $x^p < A^{42}$. We concluderen dat $x^p \leq c_0\left(\frac{1}{6}\right)$ en $x^p < A^{42}$, en dus dat x^p, en daarmee ook y^q, van boven begrensd is door $\max\left(A^{42}, c_0\left(\frac{1}{6}\right)\right)$, oftewel door een constante. Er zijn dus maar eindig veel waarden mogelijk voor x^p en y^q. Omdat $x, y > 1$ kunnen er ook maar eindig veel viertallen (x, y, p, q) voldoen aan het gegevene.

In het algemene geval definiëren we $d = \text{ggd}(x^p, y^q, A)$ en passen het *abc*-vermoeden toe met $a = y^q/d$, $b = A/d$ en $c = x^p/d$. Voor elke $\epsilon > 0$ bestaat er een constante $c_0(\epsilon)$ zodat voor $x^p/d > c_0(\epsilon)$ geldt dat $x^p/d < \text{rad}\left(\frac{x^p y^q A}{d^3}\right)^{1+\epsilon}$. Omdat $\frac{x^p y^q A}{d^3}$ een deler is dan $x^p y^q \cdot \frac{A}{d}$, vinden we

$$\begin{aligned} x^p/d &< \text{rad}\left(\frac{x^p y^q A}{d^3}\right)^{1+\epsilon} \leq \text{rad}\left(x^p y^q \cdot \frac{A}{d}\right)^{1+\epsilon} \\ &= \text{rad}\left(xy \cdot \frac{A}{d}\right)^{1+\epsilon} \leq \left(xy \cdot \frac{A}{d}\right)^{1+\epsilon} \leq (xyA)^{1+\epsilon} \cdot \frac{1}{d} \end{aligned}$$

Vermenigvuldig met d en we gaan nu verder als in het bovenstaande geval. □