Elementaire Getaltheorie, 18 januari 2010

Tijdens het tentamen is het gebruik van boeken, dictaat of aantekeningen niet toegestaan. Hoewel niet noodzakelijk, kun je een eenvoudige calculator gebruiken.
NB: Licht je antwoorden toe!
Succes!

1. Bepaal alle $x \in \mathbb{Z}$ zó dat $0 < x < 2000$ en

$$x \equiv 13 (\text{mod } 25), \quad x \equiv 3 (\text{mod } 10), \quad x \equiv 2 (\text{mod } 7).$$

2. Los op, $x^4 \equiv x (\text{mod } 1000)$ in $x \in \mathbb{Z}$.

3. (a) Voor welke priemgetallen is -2 een kwadraatrest ?
   (b) Zij p een priemgetal zó dat $q = 4p + 1$ priem is. Bewijs dat -2 een primitieve wortel modulo q is.

4. Stel dat het "abc"-vermoeden waar is. Laat zien dat er een $\gamma > 0$ bestaat met de volgende eigenschap: voor elke oplossing $x, y \in \mathbb{N}$ van een diophantische vergelijking van de vorm $x^3 = y^2 + k$ $(k > 0)$ geldt: $x < \gamma k^3$.

5. Bewijs dat

$$\sum_{n=1}^{\infty} \frac{3^n}{2^{n^2}}$$

   irrationaal is.

UITWERKINGEN

1. Uit $x \equiv 13 (\text{mod } 25)$ volgt dat er $y \in \mathbb{Z}$ bestaat zo dat $x = 13 + 25y$. Invullen in de congruentie $x \equiv 3 (\text{mod } 10)$ geeft $13 + 25y \equiv 3 (\text{mod } 10)$. Uitwerken: $5y \equiv 0 (\text{mod } 10)$. Maw $5y$ is deelbaar door 10 en dus is y even.

   Stel $y = 2z$. Daaruit volgt $x = 13 + 50z$. Invullen in $x \equiv 2 (\text{mod } 7)$ geeft $13 + 50z \equiv 2 (\text{mod } 7)$. Uitwerken: $z \equiv 3 (\text{mod } 7)$. Stel $z = 3 + 7u$, met $u \in \mathbb{Z}$, dan vinden we $x = 163 + 350u$. We willen graag de oplossingen tussen 0 en 2000. Daartoe moeten we $0 \leq u \leq 5$ nemen.

   We vinden: $x = 163, 513, 863, 1213, 1563, 1913$.

2. De congruentievergelijking $x^4 \equiv x(\text{mod } 1000)$ is via de Chinese reststelling equivalent met

$$x^4 \equiv x(\text{mod } 8) \qquad x^4 \equiv x(\text{mod } 125).$$

De eerste vergelijking is op te lossen door alle restklassen modulo 8 of op te merken dat 8 een deler is van $x^4 - x = x(x^3 - 1)$ en dat $\gcd(x, x^3 - 1) = 1$. Dus ofwel $x \equiv 0(\text{mod } 8)$ of $x^3 \equiv 1(\text{mod } 8)$. Omdat 3 geen deler van $\phi(8) = 4$ is volgt uit de tweede dat $x \equiv 1(\text{mod } 8)$. Conclusie $x \equiv 0(\text{mod } 8)$ of $x \equiv 1(\text{mod } 8)$.

Uit de congruentie $x^4 \equiv x(\text{mod } 125)$ volgt op analoge wijze $x \equiv 0(\text{mod } 125)$ of $x^3 \equiv 1(\text{mod } 125)$. (Merk op dat dit argument alleen bij priemmachten opgaat, uit $x^4 \equiv x(\text{mod } 1000)$ volgt dus NIET $x \equiv 0(\text{mod } 1000)$ of $x^3 \equiv 1(\text{mod } 1000)$, zoals diverse mensen meenden). Omdat 3 relatief priem is met $\phi(125) = 100$ volgt hieruit dat $x \equiv 1(\text{mod } 125)$.

We vinden dus dat $(x \equiv 0, 1(\text{mod } 8))$ en $(x \equiv 0, 1(\text{mod } 125))$. Dit levert vier combinaties

- $x \equiv 0(\text{mod } 8)$ en $x \equiv 0(\text{mod } 125)$ waaruit volgt $x \equiv 0(\text{mod } 1000)$
- $x \equiv 0(\text{mod } 8)$ en $x \equiv 1(\text{mod } 125)$ waaruit volgt $x \equiv 376(\text{mod } 1000)$
- $x \equiv 1(\text{mod } 8)$ en $x \equiv 0(\text{mod } 125)$ waaruit volgt $x \equiv 625(\text{mod } 1000)$
- $x \equiv 1(\text{mod } 8)$ en $x \equiv 1(\text{mod } 125)$ waaruit volgt $x \equiv 1(\text{mod } 1000)$

3. (a) Merk op, -2 is kwadraatrest modulo p in precies één van de volgende gevallen

   i. -1 en 2 zijn kwadraatrest modulo p

   ii. -1 en 2 zijn nietrest modulo p

   (Dit kun je ook met Legendre symbolen opschrijven). Uit de stellingen van het dictaat volgt dat deze gevallen equivalent zijn met

   i. $p \equiv 1(\text{mod } 4)$ en $p \equiv \pm 1(\text{mod } 8)$, maw $p \equiv 1(\text{mod } 8)$.

   ii. $p \equiv -1(\text{mod } 4)$ en $p \equiv \pm 3(\text{mod } 8)$, maw $p \equiv 3(\text{mod } 8)$.

   Conclusie: $p \equiv 1$ of 3 modulo 8.

   (b) Zij p een priemgetal zó dat $q = 4p + 1$ priem is. We bepalen de orde van -2 modulo q. Dit is een deler van $q - 1 = 4p$. Dus mogelijke ordes: $1, 2, 4, p, 2, 4p$ (waarom veel mensen de p vergeten is mij een raadsel).

$(-2)^1 \equiv 1 (\text{mod } q)$ en $(-2)^2 \equiv 1 (\text{mod } q)$ impliceren $q = 3$. $(-2)^4 \equiv 1 (\text{mod } q)$ impliceert $q = 3$ of 5. De ordes $1, 2, 4$ zijn dus uitgesloten.

Merk nu op dat uit $p = 2$ volgt $q = 9$, en dus mogen we aannemen p oneven. Uit $p \equiv 1 (\text{mod } 2)$ volgt $q \equiv 5 (\text{mod } 8)$. Dus -2 is geen kwadraatrest modulo q en dus $(-2)^{(q-1)/2} \equiv -1 (\text{mod } q)$, ofwel $(-2)^{2p} \equiv -1 (\text{mod } p)$. Hieruit volgt dat p en $2p$ niet de orde van $-2 (\text{mod } q)$ kunnen zijn. Dus blijft over de orde $4p$, waarme -2 een primitieve wortel is.

4. Laten we eerst aannemen dat $\gcd(x^3, y^2, k) = 1$. Pas "abc" toe met $a = y^2, b = k, c = x^3$. We vinden

$$x^3 < c(\epsilon) N(x^3 y^2 k)^{1+\epsilon}.$$

Gebruik nu $N(x^3 y^2 k) \leq xyk$ en $y < x^{3/2}$ (volgt uit $y^2 < y^2 + k = x^3$). We vinden

$$x^3 < c(\epsilon)(x^{5/2} k)^{1+\epsilon}$$

en daaruit

$$x^{1/2-5\epsilon/2} < c(\epsilon) k^{1+\epsilon}.$$

Kies nu $\epsilon = 1/17$ (iets kleiners werkt ook). Uitwerken geeft

$$x < \gamma k^3, \qquad \gamma = c(1/17)^{17/6}.$$

Blijft over het punt dat $d = \gcd(x^3, y^2, k)$ groter dan 1 kan zijn. Als hier iets over gezegd wordt, zonder de complete oplossing te geven, werd het al goed gerekend.

De complete oplossing is door slechts een paar mensen gegeven. Hier is de mooiste. Pas "abc" toe met $a = y^2/d, b = k/d, c = x^3/d$. Deze hebben ggd 1.

$$x^3/d < c(\epsilon) N(x^3 y^2 k/d^3)^{1+\epsilon}.$$

Nu gebruiken we dat $N(x^3 y^2 k/d^3) \leq N(x^3 y^2 k/d) \leq xyk/d$ (dit werkt want $x, y, k/d$ zijn allen geheel. Samen met $y < x^{3/2}$ geeft dit

$$x^3/d < c(\epsilon)(x^{5/2} k/d)^{1+\epsilon}.$$

Vermenigvuldig met d,

$$x^3 < c(\epsilon)(x^{5/2} k)^{1+\epsilon} d^{-\epsilon} < c(\epsilon)(x^{5/2} k)^{1+\epsilon}.$$

We hebben nu dezelfde ongelijkheid als boven en gaan op dezelfde manier verder.

5. Stel dat

$$\alpha := \sum_{n=1}^{\infty} \frac{3^n}{2^{n^2}}$$

rationaal is en gelijk aan p/q met $p, q \in \mathbb{N}$. De k-de partiele som

$$\sum_{n=1}^{k} \frac{3^n}{2^{n^2}}$$

geven we aan met α_k. Merk op dat α_k een breuk met noemer 2^{k^2} is. Het verschil $\alpha - \alpha_k$ is een positief rationaal getal met noemer die $q2^{k^2}$ deelt. Dus $\alpha - \alpha_k \geq 1/q2^{k^2}$.

Anderzijds

$$\alpha - \alpha_k = \sum_{n=k+1}^{\infty} \frac{3^n}{2^{n^2}}$$

De eerste term van deze rest is gelijk aan $3^{k+1}/2^{(k+1)^2}$, hetgeen een indicatie geeft voor de orde van grootte van $\alpha - \alpha_k$. Om een sluitend bewijs te geven moeten we echter een correcte bovengrens afleiden.

$$\begin{aligned}
\alpha - \alpha_k &= \sum_{n=k+1}^{\infty} \frac{3^n}{2^{n^2}} \\
&= \sum_{m=0}^{\infty} \frac{3^{k+1+m}}{2^{(k+1+m)^2}} \\
&= \frac{3^{k+1}}{2^{(k+1)^2}} \sum_{m=0}^{\infty} \frac{3^m}{2^{2(k+1)m+m^2}} \\
&< \frac{3^{k+1}}{2^{(k+1)^2}} \sum_{m=0}^{\infty} \frac{3^m}{4^m} \\
&= \frac{3^{k+1}}{2^{(k+1)^2}} \times \frac{1}{(1-3/4)} = 4 \times \frac{3^{k+1}}{2^{(k+1)^2}}
\end{aligned}$$

De een na laatste gelijkheid volgt door sommatie van een meetkundige reeks. Combineren van de ondergrens en bovengrens geeft

$$\frac{1}{q2^{k^2}} < 4 \times \frac{3^{k+1}}{2^{(k+1)^2}}.$$

Vermenigvuldigen met $q2^{k^2}$,

$$1 < 4q \times 3^{k+1}/2^{2k+1}.$$

Dit moet gelden voor elke k. Echter, $3^k/2^{2k} = (3/4)^k$ gaat naar 0 als $k \to \infty$. Dit is in tegenspraak met de ongelijkheid. Conclusie, α is irrationaal