

### Extra opgave 1, cursus 2003

Met deze opgave kun je maximaal één tentamenpunt bijverdienen. Uiterste inleverdatum: Vrijdag 7 november.

1. Zij  $n$  geheel en  $> 1$  met priemontbinding  $n = 2^k p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ . Hierin zijn  $p_1, p_2, \dots, p_r$  verschillende oneven priemgetalen,  $k \geq 0$  en  $k_1, k_2, \dots, k_r > 0$ . Hoeveel restklassen  $x$  modulo  $n$  heeft de congruentievergelijking  $x^2 \equiv 1 \pmod{n}$  als oplossing?
2. Zij  $p$  een oneven priemgetal en  $d$  positief geheel. Bewijs dat het aantal oplossingen van  $x^d \equiv 1 \pmod{p}$  gelijk is aan  $\text{ggd}(d, p-1)$ .
3. (Mathematica opdracht) Geef een priemgetal van de vorm  $C \cdot 2^k + 1$  van minstens 100 cijfers, waarin  $C$  je collegekaartnummer is. Gebruik de Lehmertest (zie Stelling 5.1.7) en geef ook de basis t.o.v. waarvan je primaliteit hebt getest. Mocht  $C \cdot 2^k + 1$  niet werken dan kun je altijd nog  $C \cdot p^k + 1$  voor een ander priemgetal  $p$  proberen of, als  $C$  oneven is,  $2Cp^k + 1$ .

De Mathematica opdrachten die hierbij kunt gebruiken zijn: **FactorInteger** (om je collegekaartnummer te ontbinden), **PowerMod** (machtsverheffing modulo  $N$ ) en eventueel **PrimeQ** (dit is een versie van de Rabin-test, geeft dus 99,999999... procent gegerandeerde uitkomst, maar geen 100 procent).

### Uitwerkingen

1. De vergelijking  $x^2 \equiv 1 \pmod{n}$  is volgens de chinese reststelling equivalent met het simultane stelsel

$$x^2 \equiv 1 \pmod{2^k} \quad x^2 \equiv 1 \pmod{p_1^{k_1}} \quad \dots \quad x^2 \equiv 1 \pmod{p_r^{k_r}}.$$

Zij  $p$  een oneven priemgetal en  $l > 0$ . Dan volgt uit  $x^2 \equiv 1 \pmod{p^l}$  dat  $p^l | x^2 - 1$  en dus  $p^l | (x-1)(x+1)$ . De factoren  $x-1$  en  $x+1$  kunnen geen factor  $p$  gemeen hebben, omdat hun verschil twee is. Dus òfwel  $p^l | x-1$  òfwel  $p^l | x+1$ . met andere woorden,

$$x^2 \equiv 1 \pmod{p^l} \Rightarrow x \equiv 1 \pmod{p^l} \text{ of } x \equiv -1 \pmod{p^l}.$$

Er zijn dus twee oplossingen modulo  $p^l$ .

Als  $k = 0$  volgt hieruit dat ons oorspronkelijke stelsel  $2^r$  oplossingen modulo  $n$  heeft.

Stel nu  $k = 1$ . Dan heeft  $x^2 \equiv 1 \pmod{2^k}$  precies één oplossing, namelijk  $x \equiv 1 \pmod{2}$ . Ons stelsel heeft dus weer  $2^r$  oplossingen modulo  $n$ .

Stel nu  $k = 2$ . Dan heeft  $x^2 \equiv 1 \pmod{2^k}$  precies twee oplossingen, namelijk  $x \equiv \pm 1 \pmod{4}$  en het oorspronkelijke stelsel  $2^{r+2}$  oplossingen.

Stel nu  $k > 2$ . Dan impliceert  $x^2 \equiv 1 \pmod{2^k}$  dat  $x$  oneven is en  $2^k | (x-1)(x+1)$  waaruit weer volgt  $2^{k-2} | \frac{x+1}{2} \frac{x-1}{2}$ . Omdat  $(x+1)/2, (x-1)/2$  één verschillen, hebben ze ggd 1. Dus ofwel  $2^{k-2} | (x-1)/2$  of  $2^{k-2} | (x+1)/2$ . In het eerste geval hebben we de oplossingen  $x = 1, 1 + 2^{k-1}$  in het tweede geval  $x = -1, -1 + 2^{k-1}$ . Er zijn dus vier oplossingen modulo  $2^k$ . Ons oorspronkelijke stelsel heeft  $2^{r+3}$  oplossingen.

2. Stel  $\delta = \text{ggd}(d, p-1)$ . dan geldt  $x^d \equiv 1 \pmod{p} \iff x^\delta \equiv 1 \pmod{p}$ . De implicatie  $\Leftarrow$  volgt direct. De implicatie  $\Rightarrow$  zien we door gehele  $a, b$  zo te kiezen dat  $ad + b(p-1) = \delta$  en de observatie  $x^\delta \equiv (x^d)^a (x^{p-1})^b \equiv 1 \pmod{p}$ . We moeten dus het aantal oplossingen tellen van  $x^\delta \equiv 1 \pmod{p}$ . Kies nu een primitieve wortel  $g$  modulo  $p$  en stel  $a = g^{(p-1)/\delta}$ . Dan heeft  $a \pmod{p}$  de orde  $d$ . Dit betekent dat  $1, a, a^2, \dots, a^{\delta-1} \pmod{p}$  allen verschillend zijn en oplossing van  $x^\delta \pmod{p}$ . Bovendien kan deze vergelijking niet meer dan  $\delta$  oplossingen hebben. Dus zijn er precies  $\delta$  oplossingen.