

## Week 12: Getaltheorie II (set I)

Deze week gaan we verder met wat meer getaltheorie. Er zijn twee belangrijke stellingen die we gaan gebruiken.

**Stelling 1** (Euler-Fermat). *Zijn  $a, n \in \mathbb{N}$  copriem. Dan geldt dat  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .*

*Bewijs.* De groep  $(\mathbb{Z}/n\mathbb{Z})^*$  heeft orde  $\varphi(n)$  en de orde van een element deelt de groepsorde.  $\square$

Het bewijs laat zien dat de kleinste positieve  $k \in \mathbb{N}$  zo dat  $a^k \equiv 1 \pmod{n}$  een deler is van  $\varphi(n)$ . In het bijzonder geldt voor een priemgetal  $p$ , dat  $a^{p-1} \equiv 1 \pmod{p}$  voor alle gehele  $a$  niet deelbaar door  $p$  en zijn alle ordes delers van  $p-1$ .

**Stelling 2** (Wilson). *Zij  $p > 1$ . Dan geldt  $(p-1)! \equiv -1 \pmod{p}$  precies als  $p$  priem is.*

*Bewijs.* Als  $p$  niet priem is, dan bevat  $(p-1)!$  een factor  $d$  van  $p$  en is  $(p-1)!$  niet copriem met  $p$ . Als  $p$  priem is, paar dan elk element van  $\mathbb{F}_p^*$  met zijn inverse. De elementen  $-1$  en  $1$  zijn de enige die gelijk zijn aan hun eigen inverse. We zien dat dat het product  $(p-1)! \in \mathbb{F}_p^*$  gelijk is aan  $-1 \cdot 1 = -1$ .  $\square$

## Opgaven

**Opgave 1.** *Zij  $p > 6$  een priemgetal. Bekijk het getal bestaande uit  $p-1$  enen achter elkaar en laat zien dat dit getal deelbaar is door  $p$ .*

**Opgave 2.** *Zij  $\sigma : \mathbb{F}_p^* \rightarrow \mathbb{F}_p^*$  een bijectie voor een oneven priem  $p$ . Laat zien dat  $\mathbb{F}_p^* \rightarrow \mathbb{F}_p^* : i \mapsto i \cdot \sigma(i)$  geen bijectie is.*

**Opgave 3.** *Bepaal  $2^{2^n} \pmod{2^n - 1}$  indien  $n$*

a) *een tweemacht is;*

b) *een priemgetal is.*

**Opgave 4.** *Zij  $p$  een priemgetal. Bewijs dat  $\binom{2p}{p} \equiv 2 \pmod{p}$ .*

**Opgave 5.** *Zij  $p$  een priemgetal. Bewijs dat*

a) *als  $p \equiv 1 \pmod{4}$  er een  $n \in \mathbb{Z}$  bestaat met  $n^2 \equiv -1 \pmod{p}$ ;*

b) *als  $p \equiv 3 \pmod{4}$  er geen gehele  $n$  bestaat met  $n^2 \equiv -1 \pmod{p}$ .*

**Opgave 6.** *Vind alle  $(k, m) \in \mathbb{Z}^2$  zodanig dat  $3 \cdot 2^k = m^3 + 5m + 6$ .*

**Opgave 7.** *Vind voor elk priemgetal  $p$  een geheel getal  $n$  zodanig dat  $2^n + 3^n + 6^n - 1$  deelbaar is door  $p$ .*

**Opgave 8.** *Bepaal alle priemgetallen  $p$  zodat het aantal oplossingen  $(x, y)$  met  $0 \leq x, y < p$  van*

$$y^2 \equiv x^3 - x \pmod{p}$$

*gelijk is aan  $p$ .*