Week 11: Getaltheorie II

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

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

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

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

Stelling 2 (Wilson)**.** *Zij $p > 1$. Dan geldt $(p-1)! \equiv -1 \mod p$ precies wanneer p is priem.*

Bewijs. Als p niet priem is, dan bevat $(p-1)!$ het product van d en $\frac{p}{d}$ voor een zekere niet-triviale deler d van p en geldt er $(p-1)! \equiv 0 \mod p$. 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 $-1 \cdot 1 = -1$. □

Tot slot een laatste nuttige stelling.

Stelling 3 (Kwadratische wederkerigheid)**.** *Zijn $p, q > 2$ verschillende priemgetallen. Als $p \equiv q \equiv 3 \mod 4$, dan is p een kwadraat modulo q dan en slechts dan als q* geen *kwadraat is modulo p. Anders is p een kwadraat modulo q dan en slechts dan als q een kwadraat is modulo p.*

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

Opgave 3. *Laat zien dat $5^n \cdot (5^n + 1) - 6^n \cdot (3^n + 2^n)$ deelbaar is door 91 voor alle $n \in \mathbb{N}$.*

Opgave 4. *Zij p een priemgetal. Bewijs dat iedere deler van $2^p - 1$ die groter is dan 1, ook groter is dan p.*

Opgave 5. *Bepaal $2^{2^n} \mod 2^n - 1$ indien n*

a) een tweemacht is;

b) een priemgetal is.

Opgave 6. *Laat m en a natuurlijk getallen zijn en neem aan dat $a^5 + 1$ deelbaar is door m. Laat zien dat $a + 1$ deelbaar is door m of $\varphi(m)$ deelbaar is door 5.*

Opgave 7. *Bestaat er een positief geheel getal n dat deelbaar is door 103 met de eigenschap $2^{2n+1} \equiv 2 \mod n$?*

Opgave 8. *Zij p een oneven priemgetal. Bewijs dat als -1 een kwadraat is modulo p dan geldt $4 \mid p-1$.*

Opgave 9. *Zij p een priemgetal. Bewijs dat $\binom{2p}{p} \equiv 2 \mod p$.*

Opgave 10. *Laat p en q priemgetallen zijn zodat $q \neq 5$ en $q \mid 2^p + 3^p$. Bewijs dat $q > 2p$.*

Opgave 11. *Bepaal alle priemgetallen p zodat het aantal oplossingen (x, y) met $0 \leqslant x, y < p$ van*

$$y^2 \equiv x^3 - x \mod p$$

gelijk is aan p.

Opgave 12. *Zij n een natuurlijk getal, zij p een priemgetal en zij d een deler van het getal $(n+1)^p - n^p$. Bewijs dat $d-1$ deelbaar is door p.*

Opgave 13. *Laat $m, n \geqslant 3$ oneven gehele getallen zijn. Bewijs dat $2^m - 1$ geen deler is van $3^n - 1$.*

Opgave 14. *Vind voor elk priemgetal p een geheel getal n zodanig dat $2^n + 3^n + 6^n - 1$ deelbaar is door p.*

Opgave 15. *Laat $x, y \geqslant 2$ positieve gehele getallen zijn met $\text{ggd}(x, y) = 1$. Bewijs dat $x^7 + y^7$ deelbaar is door 7 of door een priemgetal dat 1 modulo 7 is.*

Opgave 16. *Zij n een natuurlijk dat een kwadraat is modulo ieder priemgetal p. Bewijs dat n het kwadraat is van een natuurlijk getal.*