

Week 12: Getaltheorie II (set 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 $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

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

Tot slot een laatste nuttige stelling.

Stelling 3 (Kwadratische wederkerigheid). *Zijn $p, q > 2$ verschillende priemgetallen. Als $p \equiv q \equiv 3 \pmod{4}$, 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 een priemgetal. Bewijs dat iedere deler van $2^p - 1$ die groter is dan 1, ook groter is dan p .*

Opgave 2. *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 3. *Bestaat er een positief geheel getal n dat deelbaar is door 103 met de eigenschap $2^{2n+1} \equiv 2 \pmod{n}$?*

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

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

Opgave 6. *Bepaal of $712! + 1$ een priemgetal is.*

Opgave 7. *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 8. *Laat $m, n \geq 3$ oneven gehele getallen zijn. Bewijs dat $2^m - 1$ geen deler is van $3^n - 1$.*

Opgave 9. *Laat $x, y \geq 2$ 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 10. *Gegeven is een natuurlijk getal $n > 1$ dat aan de eigenschap $n \mid 3^n + 4^n$. Bewijs dat $7 \mid n$.*

Opgave 11. *Zij n een natuurlijk dat een kwadraat is modulo ieder priemgetal p . Bewijs dat n het kwadraat is van een natuurlijk getal.*