# inverteerbare elementen in Z/m

Een element r ∈ Z/m bezit een invers element voor de vermenigvuldiging x ∈ Z/m indien rx $[1]_m$ in Z/m m.a.w. r'x' ≡ 1 (mod m) met r' en x' willekeurige representanten uit r en x.

---

Zij r ∈ Z. dan is het element [r] van Z/m inverteerbaar als en slechts als r en m onderling ondeelbaar zijn. In het bijzonder zal in Z/p met p een priemgetal elk element verschillend van [0] inverteerbaar zijn.

*bewijs*
veronderstel dat [r] inverteerbaar is. Dan bestaat er een geheel getal x,
zodanig dat rx ≡ 1(mod m). Bijgevolg bestaat er een k∈Z zodanig dat rx-1=km, of rx -km = 1

Elke gemene deler van r en van m is dus bijgevolg ook een delr van 1, of met andere woorden gcd(r,m)=1.
Omgekeerd, veronderstel dat r en m onderling ondeelbaar zijn, dan bestaan er gehele getallen x en y , zodanig dat rx + my= 1 gevolgen stelling bézout hetgeen gelijkwaardig is met xr ≡ 1 (mod m)

### stelling van Euler

Als y ∈ Z met gcd (y, m) =1, dan geldt $y^{\phi(m)} \equiv 1 \pmod m$

*afleiding naar kleine stelling van fermat*
als m=p een priemgetal is en dus $\phi$(p) = p-1, wordt de stelling van euler
als p ∤ y, dan is $y^{p-1} \equiv 1 \pmod p$