Groepen theorie

Luc Veldhuis

14 Februari 2016

Stelling

Chinese rest stelling
Zij $m, n \geq 2$ met $ggd(m, n) = 1$
Dan is de afbeelding:
$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
Met $mn\mathbb{Z} \in [a]_{mn} \to [a]_m[a]_n$
Een bijectie.

Bewijs welgedefinieerd

f is welgedefinieerd
$\bar{a} = \bar{b} \in \mathbb{Z}/mn\mathbb{Z} \Rightarrow$
$mn|b - a \Rightarrow m|b - a,\ n|b - a$ wegens $ggd(m, n) = 1$
$\Rightarrow \bar{a} = \bar{b} \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Groepen theorie

Bewijs injectief

f is injectief
$a, b \in \mathbb{Z}$ met $\bar{a} = \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ en $\bar{a} = \bar{b} \in \mathbb{Z}/n\mathbb{Z} \Rightarrow m|b - a,\ n|b - a$
We willen laten zien dat $mn|b - a(\Rightarrow \bar{a} = \bar{b} \in \mathbb{Z}/mn\mathbb{Z})$ via de formule van Bézout.
$ggd(m, n) = 1 \Rightarrow \exists x, y \in \mathbb{Z}$ met $1 = xm + yn$. Maar dan geldt $b - a = (b - a)xm + (b - a)yn$ deelbaar door $mn \Rightarrow$
$\bar{a} = \bar{b} \in \mathbb{Z}/mn\mathbb{Z}$

Bewijs surjectief

f is surjectief
is meteen duidelijk van de grootte van de verzamelingen. Namelijk
$\#(\mathbb{Z}/mn\mathbb{Z}) = \#\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$
$\#\{\bar{0}, \dots, \overline{mn - 1}\} = mn$ want hij is injectief.

Groepen theorie

Direct bewijs

Bézout $\Rightarrow 1 = xm + yn$

Vind x en y zodat:

$xm = 0 \bmod m$ of

$xm = 1 \bmod m$

$yn = 0 \bmod n$ of

$yn = 1 \bmod n$

Kies $(\bar{b}, \bar{c}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$f(\overline{byn + cxn}) = (\overline{byn + cxn}, \overline{byn + cxn}) = (\bar{b}, \bar{c})$

Voorbeeld

We hebben een getal b wat voldoet aan: $b = 2 \mod 3$
$b = 3 \mod 4$
Dus $m = 3$, $n = 4$ Vind x en y die voldoen aan voorwaardes.
$3x = 1 \mod 4 \Rightarrow x = 3$
$4y = 1 \mod 3 \Rightarrow y = 4$
$2 * 4 * 4 + 3 * 3 * 3 = 32 + 27 = 59 = 11 \mod 12$
$b = 11 \mod 12$

Groepen theorie

Definitie

$(\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \bar{a}' : \bar{a}\bar{a}' = \bar{1}\}$
Bézoet stelt: $\{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : ggd(a, n) = 1\} \subset \mathbb{Z}/n\mathbb{Z}$
$\#\mathbb{Z}/n\mathbb{Z} = n$ maar $\#(\mathbb{Z}/n\mathbb{Z})^* =?$

Definition

De Euler ϕ-functie
$\phi : \mathbb{N} \to \mathbb{N}$ is gedefinieerd
$\phi(1) = 1$
$\phi(n) = \#(\mathbb{Z}/n\mathbb{Z})^*$

Voorbeeld

$\#(\mathbb{Z}/12\mathbb{Z})^* = \{\bar{1}, \bar{5}\bar{7}, \bar{1}\bar{1}\} = 4$ $\phi(12) = 4$

Groepen theorie

Stelling

De afbeelding f geeft ook een bijectie
$f(\mathbb{Z}/mn\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$

Bewijs welgedefinieerd

$\bar{a} \in (\mathbb{Z}/mn\mathbb{Z})^* \Rightarrow \bar{a} \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$
$\exists \bar{a} \in (\mathbb{Z}/mn\mathbb{Z})^* : \bar{a}\bar{a}' = \bar{1} \in (\mathbb{Z}/mn\mathbb{Z})^*$
$(\bar{1}, \bar{1}) = f(\bar{1}) = f(\bar{a}, \bar{a}') = (\bar{a}\bar{a}', \bar{a}, \bar{a}') \Rightarrow \bar{a}\bar{a}' = \bar{1} \in \mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z} \Rightarrow$
$\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^*, (\mathbb{Z}/n\mathbb{Z})^*$

Bewijs surjectief

$(\bar{b}, \bar{c}) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow$ er is een uniek element
$\bar{a} \in \mathbb{Z}/mn\mathbb{Z}$ met $f(\bar{a}) = (\bar{b}, \bar{c})$
We moeten laten zien zien dat $\bar{a} \in (\mathbb{Z}/mn\mathbb{Z})^*$
$\bar{b} \in (\mathbb{Z}/m\mathbb{Z})^* \Rightarrow \exists \bar{b} : \bar{b}\bar{b}' = \bar{1} \in \mathbb{Z}/m\mathbb{Z}$
$\bar{c} \in (\mathbb{Z}/n\mathbb{Z})^* \Rightarrow \exists \bar{c} : \bar{c}\bar{c}' = \bar{1} \in \mathbb{Z}/n\mathbb{Z}$
$f : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$ is surjectief
$\Rightarrow \exists \bar{a} \in \mathbb{Z}/mn\mathbb{Z} : f(\bar{a}') = (\bar{b}', \bar{c}')$
$f(\bar{1}) = (\bar{1}, \bar{1}) = (\bar{b}\bar{b}', \bar{c}\bar{c}') = (\bar{a}\bar{a}', \bar{a}\bar{a}') = f(\bar{a}\bar{a}')$
$\bar{a}\bar{a}' = \bar{1}$ omdat f injectief is.

Bewijs injectief

f is injectief, want f is injectief.

Voorbeeld

$m = 4,\ n = 3$
$(\mathbb{Z}/12\mathbb{Z})^* = \bar{1}, \bar{5}, \bar{7}, \bar{1}\bar{1}$
$\bar{1}, \bar{3} \times \bar{1}, \bar{2} = (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* = (\bar{1}, \bar{1}), (\bar{1}, \bar{2}), (\bar{3}, \bar{1}), (\bar{3}, \bar{2}) =$
$(\bar{1}, \bar{1}), (\bar{5}, \bar{5}), (\bar{7}, \bar{7}), (\bar{1}\bar{1}, \bar{1}\bar{1})$

Gevolg

- $ggd(n, m) = 1 \Rightarrow \phi(m, n) = \phi(m)\phi(n)$
- $n = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$ met $p_1 < p_2 < \cdots < p_t$
  $\Rightarrow \phi(n) = \phi(p_1^{a_1}) \dots \phi(p_t^{a_t})$
  $= p_1^{a_1 - 1}(p_1 - 1) \dots p_t^{a_t - 1}(p_t - 1)$

Bewijs

Moeten laten zien dat: $\phi(p^a) = p^{a-1}(p-1)$
$\bar{b} \in \mathbb{Z}/p^a\mathbb{Z} \setminus (\mathbb{Z}/p^a\mathbb{Z})^*$ als $ggd(b, p^a) \neq 1$
$\#(\mathbb{Z}/p^a\mathbb{Z})^* = \#\{\bar{0}, \bar{p}, \bar{2p}, \ldots, \overline{p^a - p}\} = p^{a-1}$
Dus $\#(\mathbb{Z}/p^a\mathbb{Z} \setminus (\mathbb{Z}/p^a\mathbb{Z})^*) = p^a - p^{a-1} = p^{a-1}(p-1)$

Definitie Operatie

- Een binaire operatie is ee verzameling X met afbeelding $X \times X \to X$.
  $(a, b) \to a * b$
- Zo'n bewerking heet associatief als $(a * b) * c = c * (a * b)$ voor alle a, b, c
- Als $a * b = b * a$ dan zeggen we dat a en b commuteren. Als dit geldt voor alle a, b dan heet dit $(f(x, *))$ commutatief.

Voorbeeld

- $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(a, b) \to a + b$, is een binaire, commutatieve, associatieve operatie
- $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(a, b) \to a - b$, is een binaire, niet commutatieve, niet associatieve operatie
- $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$, $(a, b) \to b$, is een binaire, niet commutatieve, niet associatieve operatie

Groepen theorie

Definitie

Een groep is een paar $(G, *)$ met G een niet lege verzameling en een binaire operatie $* : G \times G \to G$ zodat:

- $*$ is associatief
- Er bestaat een element $e \in G$ zodat $a * e = e * a = a$
- Voor elke $a \in G$ bestaat er een element $a^{-1} \in G$ zodat $a * a^{-1} = a^{-1} * a = e$

Voorbeeld

$\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times \setminus 0$ onder multiplicatie
$\{\pm 1\}, \{z \in \mathbb{C} | |z| = 1\}$