

Bewijzen - Inleveropgave 4

B.H.J. van Boxtel

12 Oktober 2022 - Week 41

Gegeven is het volgende lemma:

Lemma 1. Zij $m, n \in \mathbb{Z}$ en p een priemgetal. Als $p \mid mn$, dan geldt dat $p \mid m$ of $p \mid n$.

Ook gegeven is de volgende relatie R op \mathbb{Z} , voor gehele getallen a en b door de voorwaarde dat $a R b$ dan en slechts dan als $b - a$ deelbaar is door zowel p als q .

(a). **Stelling 1.** R is een equivalentierelatie.

Om te laten zien dat R een equivalentierelatie is, moeten we laten zien dat R reflexief, symmetrisch en transitief is.

- **Claim 1.** R is reflexief. In andere woorden er geldt $a R a$.

Bewijs.

We weten dat $q \mid 0$.

Dus $q \mid a - a$.

Ook weten we dat $p \mid 0$.

Dus $p \mid a - a$.

Dus $a R a$.

Dus R is reflexief.

□

- **Claim 2.** R is symmetrisch. Dat wil zeggen $a R b$ impliceert $b R a$.

Bewijs.

Neem aan $a R b$.

Volgens de definitie van R geldt dan $q \mid b - a$.

Dus $b - a$ is te schrijven als $b - a = kq$ voor een $k \in \mathbb{Z}$.

Dus $a - b = -kq$.

Dus $q \mid a - b$.

Volgens de definitie van R geldt $p \mid b - a$.

Dus $b - a$ is te schrijven als $b - a = mp$ voor een $m \in \mathbb{Z}$.

Dus $a - b = -kp$.

Dus $p \mid a - b$.

Dus $q \mid a - b$ en $p \mid a - b$, dus $b R a$.

We zien dat $b R a$ volgt uit $a R b$, dus R is symmetrisch.

□

- **Claim 3.** R is transitief. Dat wil zeggen dat wanneer $a R b$ en $b R c$, dan $a R c$.

Bewijs.

Neem aan $a R b$ en $b R c$. Vanuit de definitie van R volgt dan dat q een deler is van $b - a$, en dat q een deler is van $c - b$.

Dus $b - a$ is te schrijven als $b - a = kq$ met $k \in \mathbb{Z}$.

En $c - b$ is te schrijven als $c - b = mq$ met $m \in \mathbb{Z}$.

Wanneer we deze twee vergelijkingen bij elkaar optellen, vinden we dat $c - a = q(k + m)$.

Omdat $(k + m) \in \mathbb{Z}$, geldt nu dus dat $q \mid c - a$.

Vanuit de definitie van R volgt ook dat p een deler is van $b - a$, en dat p een deler is van $c - b$.

Dus $b - a$ is te schrijven als $b - a = np$ met $n \in \mathbb{Z}$.

En $c - b$ is te schrijven als $c - b = lp$ met $l \in \mathbb{Z}$.

Wanneer we deze twee vergelijkingen bij elkaar optellen, vinden we dat $c - a = p(n + l)$.

Omdat $(n + l) \in \mathbb{Z}$, geldt nu dus dat $p \mid c - a$.

Dus omdat $q \mid c - a$ en $p \mid c - a$, geldt $a R c$.

Dus $a R b$ en $b R c$ impliceert $a R c$.

Dus R is transitief.

□

Dus R is een equivalentierelatie.

- (b). **Stelling 2.** De relatie $a R b$ geldt dan en slechts dan als $a \equiv b \pmod{pq}$.

Dit is een biconditienele implicatie, dus de implicatie moet allebei de kanten op gelden. Eerst bewijs ik de implicatie van links naar rechts, dat wil zeggen $a R b$ impliceert $a \equiv b \pmod{pq}$.

Bewijs.

Neem aan $a R b$.

Dan geldt vanuit de definitie van R dat $p \mid b - a$ en $q \mid b - a$.

Omdat p en q priemgetallen zijn, kunnen dit geen delers van elkaar zijn.

Omdat geldt $p \mid b - a$ én $q \mid b - a$, kunnen we $b - a$ schrijven als $b - a = kpq$ voor een $k \in \mathbb{Z}$.

Dus $b - a \equiv 0 \pmod{pq}$ en $b \equiv a \pmod{pq}$.

□

Om het bewijs van **Stelling 2.** af te maken, bewijzen we nu de implicatie de andere kant op. Dat wil zeggen $a \equiv b \pmod{pq}$ impliceert $a R b$.

Bewijs.

Neem aan $a \equiv b \pmod{pq}$.

Dus $a - b \equiv 0 \pmod{pq}$.

Dus $b - a \equiv 0 \pmod{pq}$.

Dus $pq \mid b - a$.

Dan kunnen we $b - a$ schrijven als $b - a = kpq$ voor een $k \in \mathbb{Z}$.

Dus $p \mid b - a$ en $q \mid b - a$.

□

(c). **Stelling 3.** De verzameling van equivalentieklassen van R is gelijk aan \mathbb{Z}_{pq} .

Bewijs.

Volgens **Stelling 2.** geldt $a R b$ dan en slechts dan als $a \equiv b \pmod{pq}$. Dit betekent dat een getal b alleen equivalent kan zijn aan a dan en slechts dan als b congruent is aan $a \pmod{pq}$. Dus alle getallen in de equivalentieklassen van R met representant a , zitten ook in de equivalentieklassen van de getallen \pmod{pq} met representant a . Ook geldt dat alle getallen in de equivalentieklassen van de getallen \pmod{pq} met representant a in de equivalentieklassen van R met representant a zitten. Dus de verzameling van equivalentieklassen van R is gelijk aan \mathbb{Z}_{pq} .

□