Bewijzen in de wiskunde inleveropgave 4

Casper Bakker

6413978

Laat p en q twee verschillende priemgetallen zijn en definieer voor gehele getallen a, b de relatie aRb door: aRb wanneer $b - a$ deelbaar is door zowel p als q. Voor deze relatie R laten we zien:

- dat R een equivalentierelatie is
- dat de equivalentieklassen van R overeenkomen met de elementen van $\mathbb{Z}_{pq}$. Dat wil zeggen: $[a] = [b]$ als equivalentieklassen van R dan en slechts dan als $[a] = [b]$ als elementen van $\mathbb{Z}_{pq}$.

Hierbij gebruiken we het volgende lemma: Als p een priemgetal is en $p|mn$ dan $p|m$ of $p|n$.

i)

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

Reflexiviteit

Om te laten zien dat R reflexief is moeten we aantonen dat aRa voor alle $a \in \mathbb{Z}$. Dit betekent dat voor een willekeurige $a \in \mathbb{Z}$ moet gelden dat $p|a-a$ en $q|a-a$. Merk op dat $a - a = 0 = 0p$ en 0 is een geheel getal. Dus omdat $\frac{a-a}{p} = \frac{0}{p} = 0$ concluderen we dat R reflexief is.

Symmetrie

Om te laten zien dat R symmetrisch is moeten we laten zien dat als $a, b \in \mathbb{Z}$ zodat aRb dan ook bRa.
We gebruiken een bewijs uit het ongerijmde. Stel dat er $a, b \in \mathbb{Z}$ bestaan zodat aRb en $b \not R\, a$. Als aRb dan weten we dat $p|b - a$ dus $\frac{b-a}{p} = k$ met $k \in \mathbb{Z}$ hieruit volgt $a - b = -pk$. Dan zien we dat $\frac{a-b}{p} = \frac{-pk}{p} = -k$. Echter hadden we aangenomen dat $p \not| \, a - b$ dus uit deze tegenspraak kunnen we concluderen dat als $p|b - a$ dan ook $p|a - b$. Op dezelfde wijze is te demonstreren dat als $q|b - a$ dan $q|a - b$ (het enige verschil is het priemgetal q in plaats van p). We concluderen dat R symmetrisch is.

Transitiviteit

Om te laten zien dat R transitief is moeten we aantonen dat als aRb en bRc dan aRc met $a, b, c \in \mathbb{Z}$.
Laat $a, b, c \in \mathbb{Z}$ zodat aRb en bRc. Omdat aRb weten we dat $p|b - a$ dus $\frac{b-a}{p} = k$. Dan ook $b = pk + a$. we weten dat $p|c - b$ dus ook $p|c - pk - a$ ofwel $\frac{c-pk-a}{p} = r$ met $r \in \mathbb{Z}$. Hieruit volgt dat $\frac{c-a}{p} = r + k$ dus $p|c - a$. Op een zelfde manier is aan te tonen dat $q|c - a$. We concluderen dat R transitief is.

Omdat R reflexief, symmetrische en transitief is concluderen we dat R een equivalentie relatie is.

ii)

We laten zien dat de equivalentieklassen van R overeenkomen met de elementen van $\mathbb{Z}_{pq}$. Dit is equivalent met laten zien dat de equivalentie klasse relatie R gelijk is aan de gehele getalen modulo pq. We laten dus zien dat $p|b - a$ en $q|b - a$ dan en slechts dan als $pq|b - a$.

We bewijzen eerst dat als $p|b - a$ en $q|b - a$ dan $pq|b - a$. Laat $b, a \in \mathbb{Z}$ en p en q twee verschillende willekeurige priemgetallen zodat $p|b - a$ en $q|b - a$. Omdat $p|b - a$ weten we dat $\frac{b-a}{p} = k$ waarbij $k \in \mathbb{Z}$. Dit betekent ook dat $b - a = kp$. We weten dat $q|b - a$ dus ook $q|kp$. Omdat q een priemgetal is volgt uit het lemma dat $q|k$ of $q|p$. Omdat p en q priemgetallen zijn weten we dat q geen deler is van p dus weten we dat $q|k$. Omdat $q|k$ volgt dat $\frac{k}{q} = r$ waarbij $r \in \mathbb{Z}$.
Omdat $\frac{b-a}{p} = k$ en $k = qr$ concluderen we dat $\frac{b-a}{pq} = r$ met $r \in \mathbb{Z}$ dus $pq|b - a$.

We laten zien dat als $pq|b-a$ dan $p|b-a$ en $q|b-a$.
Laat $b, a \in \mathbb{Z}$ en p en q twee verschillende priemgetallen zodat $pq|b-a$. Als $pq|b-a$ dan $\frac{b-a}{pq} = k$ waarbij $k \in \mathbb{Z}$. Dan volgt dat $\frac{b-a}{p} = qk$ en $\frac{b-a}{q} = pk$. Omdat pk en qk beide gehele getalen zijn is het duidelijk dat $p|b-a$ en $q|b-a$. We concluderen dat als $pq|b-a$ dan $p|b-a$ en $q|b-a$.

We hebben bewezen dat $p|b-a$ en $q|b-a$ dan en slechts dan als $pq|b-a$. Omdat voor $x, y \in [a]$ van R geldt dat xRy weten we dat $pq|x-y$ en $pq|y-x$ dus komt $[a]$ overeen met een element van $\mathbb{Z}_{pq}$