Inlever opdracht 1

Luc Veldhuis

20 februari 2017

1. (a) Bepaal alle $\overline{a}$ in $\mathbb{Z}/n\mathbb{Z}$ met $\overline{a}^2 = \overline{1}$ voor $n = 2, 4, 8$ en 9.
$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$

$\overline{a}$	$\overline{a}^2$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$

Dus de verzameling rest klassen in $\mathbb{Z}/2\mathbb{Z}$ waarvoor geldt $\overline{a}^2 = \overline{1}$ is $\{\overline{1}\}$.

$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$

$\overline{a}$	$\overline{a}^2$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{0}$
$\overline{3}$	$\overline{1}$

Dus de verzameling rest klassen in $\mathbb{Z}/4\mathbb{Z}$ waarvoor geldt $\overline{a}^2 = \overline{1}$ is $\{\overline{1}, \overline{3}\}$.

$\mathbb{Z}/8\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}\}$

$\overline{a}$	$\overline{a}^2$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{0}$
$\overline{5}$	$\overline{1}$
$\overline{6}$	$\overline{4}$
$\overline{7}$	$\overline{1}$

Dus de verzameling rest klassen in $\mathbb{Z}/8\mathbb{Z}$ waarvoor geldt $\overline{a}^2 = \overline{1}$ is $\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

$\mathbb{Z}/9\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}\}$

Dus de verzameling rest klassen in $\mathbb{Z}/9\mathbb{Z}$ waarvoor geldt $\overline{a}^2 = \overline{1}$ is $\{\overline{1}, \overline{8}\}$.

$\overline{a}$	$\overline{a}^2$
$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$
$\overline{4}$	$\overline{7}$
$\overline{5}$	$\overline{7}$
$\overline{6}$	$\overline{0}$
$\overline{7}$	$\overline{4}$
$\overline{8}$	$\overline{1}$

(b) Zij p een oneven primegetal, $m \geq 1$ en a een geheel getal. Bewijs dat $a^2 \equiv 1$ modulo p^m dan en slechts dan als $a \equiv 1$ modulo p^m of $a \equiv -1$ modulo p^m.

Bewijs '$\Leftarrow$':
Stel $a \equiv 1$ modulo p^m of $a \equiv -1$ modulo p^m. Dan kunnen we dit schijven als $p^m | a-1$ of $p^m | a+1$. Neem zonder verlies van algemeenheid aan $p^m | a-1$. Neem nu $a+1 = l$ voor $l \in \mathbb{Z}$. Dit betekend $a-1 = kp^m$ voor $k \in \mathbb{Z}$. Dan is $(a-1)(a+1) = a^2 - 1 = klp^m$ voor $k, l \in \mathbb{Z}$. Neem $n = kl$, $n \in \mathbb{Z}$. Dan hebben we $a^2 - 1 = np^m$. Dit is de definitie van modulo. We kunnen dit nu schrijven als $a^2 \equiv 1$ modulo p^m.
Dus als $a \equiv 1$ modulo p^m of $a \equiv -1$ modulo p^m dan $a^2 \equiv 1$ modulo p^m.

Bewijs '$\Rightarrow$': Er is gegeven dat p priem is en oneven. Het kleinste oneven priemgetal is 3. Stel $a^2 \equiv 1$ modulo p^m. Dan kunnen we dit schrijven als $p^m | a^2 - 1 = (a-1)(a+1)$. Dit betekend $(a-1)(a+1) = kp^m$ voor een $k \in \mathbb{Z}$. De priemontbinding van een getal is uniek, dus we weten zeker dat er minstens m factoren van p in $(a-1)(a+1)$ zitten. Dit betekent dat de getallen van de volgende vorm moeten zijn: $a-1 = qp^{m-n}$ en $a+1 = wp^n$ voor $q, w \in \mathbb{Z}$ en $0 \leq n \leq m \in \mathbb{Z}$. We weten ook $a+1-(a-1) = 2$. Dus $wp^n - qp^{m-n} = 2$. Nu hebben we twee gevallen. $n \leq m-n$ of $n > m-n$. We behandelen eerst het geval $n \leq m-n$. Dan kunnen we $wp^n - qp^{m-n} = 2$ schijven als $p^n(w - qp^{m-2n}) = 2$. Omdat $p \geq 3$ en $n \geq 0$ weten we dat $p^n > 0$. Dus $w - qp^{m-2n} > 0$. We weten ook $p^n \neq 2$, want 2 is een priemgetal en kan dus niet worden opgebouwd uit andere priemgetallen. Omdat $w - qp^{m-2n} \in \mathbb{Z}$ en dus geen breuken kan vormen moet p^n wel gelijk zijn aan 1 en $w - qp^{m-2n}$ aan 2. p^n kan alleen gelijk zijn aan 1 als $n = 0$ omdat $p \geq 3$ en $0 \leq n \leq m$. Dit geeft $a - 1 = qp^{m-0} = qp^m$ en $a + 1 = wp^0 = w$. In het andere geval met $n > m - n$, kunnen we $wp^n - qp^{m-n} = 2$ schijven als $p^{m-n}(wp^n - q)$ en dit geeft precies dezelfde redenatie $m - n = 0$, dus $n = m$. Dit resulteert in $a - 1 = qp^{m-m} = q$ en $a + 1 = wp^m$. Volgens de definities kunnen we $a + 1 = wq^m$ schijven als $a \equiv -1$ modulo p^m en $a - 1 = qp^m$ als $a \equiv 1$ modulo p^m. Dus als $a^2 \equiv 1$ modulo p^m dan $a \equiv 1$ modulo p^m of $a \equiv -1$ modulo p^m.

(c) Bepaal nu met behulp van de Chinese reststelling de vier oplossingen van $\overline{a}^2 = \overline{1}$ in $\mathbb{Z}/5^2 7^2 \mathbb{Z}$.
De Chinese reststelling zegt dat als $m, n \geq 2$ en $ggd(m, n) = 1$ dan geldt dat de afbeelding:

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

gedefinieerd door $f(\overline{a}) = (\overline{a}, \overline{a})$ een bijectie is.
Uit het dictaat halen we dat $f(\overline{a}) = f(\overline{byn + cxm}) = (\overline{byn + cxm}, \overline{byn + cxm}) = (\overline{byn}, \overline{cxm}) = (\overline{b}, \overline{c})$. Waarin $1 = xn + ym$ als in de formule van Bézout en $\overline{b} \in \mathbb{Z}/m\mathbb{Z} = \overline{c} \in \mathbb{Z}/n\mathbb{Z} = \overline{a} \in Z/mn\mathbb{Z}$ onbekenden. We halen uit de vraag dat $m = 5^2$ en $n = 7^2$. We zien direct $ggd(5^2, 7^2) = 1$ omdat ze beiden priem zijn.
De formule van Euler zegt dat elke getallen waarvoor geldt $ggd(m, n) = 1$, kunnen worden geschreven

in de vorm $1 = xm + yn$. We passen de formule van Euler toe:

$$\begin{aligned} 25 &= 0 * 49 + 25 \\ 49 &= 1 * 25 + 24 \\ 25 &= 1 * 24 + 1 \\ 24 &= 24 * 1 \end{aligned}$$

Schrijf nu om:

$$\begin{aligned} 1 &= 25 - 24 \\ 24 &= 49 - 25 \\ 1 &= 25 - (49 - 25) \\ 1 &= 2 * 25 - 49 \end{aligned}$$

Hieruit lezen we af dat $x = 2$ en $y = -1$.
Invullen van $\overline{a}^2 \in \mathbb{Z}/5^2 7^2 \mathbb{Z}$ geeft, $f(\overline{a}^2) = (\overline{b}^2, \overline{c}^2)$. Maar ook $f(\overline{1}) = (\overline{1}, \overline{1})$.

We zijn dus opzoek naar gehele getallen b, c zodat $\overline{b}^2 = \overline{1} \in \mathbb{Z}/5^2\mathbb{Z}$ en $\overline{c}^2 = \overline{1} \in \mathbb{Z}/7^2\mathbb{Z}$.
In vraag 1b hebben we bewezen dat voor elk getal $a \equiv 1$ modulo p^m, voor p priem ≥ 3 en $m \geq 1$ er geldt dat $a \equiv 1$ modulo p^m of $a \equiv -1$ modulo p^m. Dit kunnen we nu toepassen. Dit geeft $\overline{b} = \overline{1} \in \mathbb{Z}/5^2\mathbb{Z}$ of $\overline{b} = \overline{-1} \in \mathbb{Z}/5^2\mathbb{Z}$ en $\overline{c} = \overline{1} \in \mathbb{Z}/7^2\mathbb{Z}$ of $\overline{c} = \overline{-1} \in \mathbb{Z}/7^2\mathbb{Z}$. Ook hebben we $f(\overline{a}) = f(\overline{byn + cxm})$. Omdat f een bijectie is geldt $\overline{a} = \overline{byn + cxm}$. Als we dit invullen krijgen we de volgende vergelijking:
$\overline{a} = \overline{-49b + 50c}$ voor $b, c \in \{-1, 1\}$.
Dit geeft $\overline{a} \in \{\overline{1}, \overline{-1}, \overline{99}, \overline{-99}\}$
De rest klassen van $\overline{a}$ waarvoor geldt $\overline{a}^2 = \overline{1}$ zijn dus $\overline{1}, \overline{99}, \overline{1224}, \overline{1126}$.