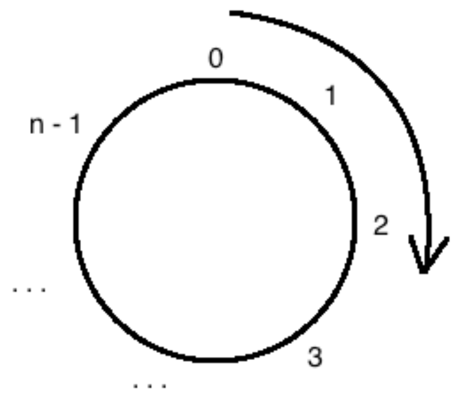
Modulorekenen

Herhaling hoofdstuk 1: gehele getallen modulo n

Definitie en notatie

$$\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}, n \in \mathbb{N}, n \geq 2$$



Eigenschappen

- $+$ en $\times$ verloopt zoals in $\mathbb{Z}$,
  maar de einduitkomst wordt vervangen door de rest bij deling door n
  "*modulo* n"

- In dat geval is $\mathbb{Z}_n$ gesloten onder $+$ en $\times$

Modulorekenen: de basics

Notaties:

$r = a \bmod n$

"r is de rest van a bij deling door n"

"r is a **modulo** n"

Gevolg: $0 \leq r < n$ en $r = a - \left\lfloor \frac{a}{n} \right\rfloor \cdot n$

$a \overset{n}{=} b$

"a is **congruent** met b modulo n"

"a en b hebben dezelfde rest bij deling door n"

Staat voor: $a \bmod n = b \bmod n$

Wordt ook vaak genoteerd als: $a = b \pmod n$

Equivalentierelaties

De congruentierelatie $\overset{n}{=}$ is een **equivalentierelatie** op $\mathbb{Z}$

Reflexief $a \overset{n}{=} a$

Symmetrisch $a \overset{n}{=} b \Rightarrow b \overset{n}{=} a$

Transitief $a \overset{n}{=} b$ en $b \overset{n}{=} c \Rightarrow a \overset{n}{=} c$

De congruentierelatie $\overset{n}{=}$ deelt $\mathbb{Z}$ op in n verschillende **equivalentieklassen**

Ook: **congruentieklassen**, **residuklassen**, **restklassen**

Notatie:

$$
\begin{aligned}
[a]_n &= \{x \mid x \in \mathbb{Z} \text{ en } x \overset{n}{=} a\} \\
&= \{a + k \cdot n \mid k \in \mathbb{Z}\}
\end{aligned}
$$

Om de notatie eenduidig te houden, verkiezen we $0 \leq a < n$

Een herziening van $\mathbb{Z}_n$

De verzameling van alle restklassen modulo n wordt genoteerd als

$$\mathbb{Z}_n = \{[a]_n \mid 0 \leq a < n\}$$

Let op!

Dit is equivalent met $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$

Indien we hierin 0 interpreteren als $[0]_n$, 1 als $[1]_n$, enz.

M.a.w. 1 is een **representant** van $[1]_n$

Voorbeeld:

$-2, 3, 18, \dots$ zijn representanten van $[3]_5$

Rekenregels in $\mathbb{Z}_n$

Congruentieklassen zijn **stabiel** onder optelling, vermenigvuldiging en machtsverheffing

Als $a \overset{n}{=} A$ en $b \overset{n}{=} B$

$$a + b \overset{n}{=} A + B$$

$$a - b \overset{n}{=} A - B$$

$$a \cdot b \overset{n}{=} A \cdot B$$

$$a^k \overset{n}{=} A^k$$

Daaruit volgt ook:

$$a \bmod n + b \bmod n \overset{n}{=} (a + b) \bmod n$$

$$a \bmod n - b \bmod n \overset{n}{=} (a - b) \bmod n$$

$$a \bmod n \cdot b \bmod n \overset{n}{=} (a \cdot b) \bmod n$$

$$(a \bmod n)^k \overset{n}{=} a^k \bmod n$$

Voorbeeld: $[2]_3 + [1]_3 = [3]_3 = [0]_3$ en $[12]_{32} \cdot [17]_{32} = [204]_{32} = [12]_{32}$

Toepassing: genereren van pseudorandom getallen

Veel computersimulaties vertrekken vanuit random gegenereerde getallen
Dit om toevalligheid en natuurlijke variatie na te bootsen

Monte-Carlosimulatie

Een (fysiek) proces wordt vele malen gesimuleerd

Telkens met andere startcondities

Resultaat = een distributie of gemiddelde (wet van grote aantallen)

Hoe kan een computer getallen “zo random mogelijk” genereren?

Toepassing: genereren van pseudorandom getallen

Lineaire-congruentiemethode

Beschouw volgende recurrente betrekking:

$$x_{i+1} = (a \cdot x_i + c) \bmod m$$

Hierbij kiezen we:

- m = modulus
- a = factor
- c = increment
- x_0 = kiem of ‘seed’

Voorbeeld: $m = 9, a = 7, c = 4, x_0 = 3$

Dit resulteert in de rij: 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, …

Na 9 stappen herhaalt de rij zichzelf: de **periode** = 9

Toepassing: genereren van pseudorandom getallen

In de praktijk wil men een zo groot mogelijke periode

Bijvoorbeeld:

$m = 2^{31} - 1, a = 7^5, c = 0$ heeft een periode van $2^{31} - 2$

Lehmer random number generator

m is een priemgetal of een macht van een priemgetal

x_0 is relatief priem met m

c is 0

a is een *generator* voor $\mathbb{Z}_m$ (i.e. $a, a^2, a^3, \ldots$ mod m doorlopen alle elementen van $\mathbb{Z}_m \setminus \{0\}$)

Bijv. 2 is een generator voor $\mathbb{Z}_5$ want $2 \overset{5}{=} 2, 2^2 \overset{5}{=} 4, 2^3 \overset{5}{=} 3, 2^4 \overset{5}{=} 1, 2^5 \overset{5}{=} 2, \ldots$

$\Rightarrow$ de periode is $m - 1$

Toepassing: genereren van pseudorandom getallen

Hull-Dobell theorema

m en c $(\neq 0)$ zijn relatief priem

$a - 1$ is deelbaar door alle priemfactoren van m

$a - 1$ is deelbaar door 4 als m deelbaar is door 4

$\Leftrightarrow$ de periode is maximaal en is gelijk aan m

Vergelijkingen

Eenvoudige vergelijking

Vergelijking van het type:

$$a + x \overset{n}{=} b$$
$$(a, b \in \mathbb{Z},\ n \in \mathbb{N}_0,\ x \in \mathbb{Z})$$

Oplossen:

$$a + x \overset{n}{=} b$$
$$\Leftrightarrow x \overset{n}{=} b - a$$
$$\Leftrightarrow \exists k \in \mathbb{Z}\colon\ x = b - a + k \cdot n \quad \text{(oplossingen in } \mathbb{Z}\text{)}$$
$$\Leftrightarrow [x]_n = [b - a]_n \quad \text{(oplossingen in } \mathbb{Z}_n\text{)}$$

Opmerking: er is slechts één oplossing in $\{0,1,2,\dots,n-1\}$

Lineaire congruentie

Vergelijking van het type:

$$a \cdot x \overset{n}{=} b$$

$$(a, b \in \mathbb{Z},\ n \in \mathbb{N}_0,\ x \in \mathbb{Z})$$

In principe vinden we de oplossing door te “delen door a”
Dit is onmogelijk in $\mathbb{Z}$ (niet gesloten voor de deling)

Wel mogelijk in $\mathbb{Z}_n$?
Opdracht:

Voor een gegeven getal x: zoek diens **multiplicatief inverse** y zodat

$$x \cdot y \overset{n}{=} 1 \overset{n}{=} y \cdot x$$

Lineaire congruentie

Stelling

Als ggd(a, n) = 1, dan bestaat er precies één geheel getal $x \in \{0,1,2,\dots,n-1\}$ waarvoor

$$a \cdot x \overset{n}{=} 1 \overset{n}{=} x \cdot a$$

Dit getal x is de **inverse van $\boldsymbol{a}$ modulo $\boldsymbol{n}$**

Bewijs:

a) Er bestaat ten minste één zo'n x

Uit het algoritme van Euclides: ggd(a, n) = $u \cdot a + v \cdot n$ = 1

Dus: $u \cdot a \overset{n}{=} 1$

M.a.w. $x = u \bmod n$ voldoet (en is te vinden via het uitgebreide algoritme van Euclides)

Lineaire congruentie

Stelling

Als ggd(a, n) = 1, dan bestaat er precies één geheel getal $x \in \{0,1,2,\dots,n-1\}$ waarvoor

$$a \cdot x \overset{n}{=} 1 \overset{n}{=} x \cdot a$$

Dit getal x is de **inverse van $\boldsymbol{a}$ modulo $\boldsymbol{n}$**

Bewijs:

b) Er bestaat ten hoogste één zo'n x

Ongerijmde: stel dat er twee oplossingen x_1 en x_2 zijn

$\Rightarrow a \cdot x_1 \overset{n}{=} 1$ en $a \cdot x_2 \overset{n}{=} 1$

$\Rightarrow a \cdot (x_1 - x_2) \overset{n}{=} 0$

$\Rightarrow n \mid a \cdot (x_1 - x_2)$

$\Rightarrow n \mid x_1 - x_2$ (want ggd(a, n) = 1)

Dit is een contradictie, want $0 \leq x_i < n$

Het zoeken van een invers element

Voorbeeld: zoek de inverse van 5 modulo 13

Via het uitgebreide algoritme van Euclides vinden we: ggd(5, 13) $= 1 = 8 \cdot 5 - 3 \cdot 13$

De gezochte inverse is dus $8 \bmod 13$

Check: $8 \cdot 5 \bmod 13 = 40 \bmod 13 = 1$

Kan ook via het opstellen van een vermenigvuldigingstabel in $\mathbb{Z}_{13}$:

$\boldsymbol{a}$	$\boldsymbol{x}$	$\boldsymbol{a \cdot x \bmod 13}$	$\boldsymbol{a}$	$\boldsymbol{x}$	$\boldsymbol{a \cdot x \bmod 13}$
5	1	5	5	7	9
5	2	10	5	8	1
5	3	2	5	9	6
5	4	7	5	10	11
5	5	12	5	11	3
5	6	4	5	12	8

Het oplossen van lineaire congruenties

Stelling

Het aantal gehele oplossingen $x \in \{0,1,2,\dots,n-1\}$ van

$$a \cdot x \overset{n}{=} b$$

hangt af van ggd(a, n) en b.

Stel $d =$ ggd(a, n)

1. Als $d \nmid b$: geen oplosisngen
2. Als $d \mid b$: precies d oplossingen in $\{0,1,2,\dots,n-1\}$

Bewijs (= oplossingsmethode):

1. <u>$d \nmid b$</u>

   Ongerijmde: stel dat er wel een oplossing $x \in \{0,1,2,\dots,n-1\}$

   $\Rightarrow \exists k \in \mathbb{Z}$: $a \cdot x = b + k \cdot n$

   $\Rightarrow \exists k \in \mathbb{Z}$: $b = a \cdot x - k \cdot n$

   Contradictie: linkerlid is niet deelbaar door d, het rechterlid wél

Het oplossen van lineaire congruenties

Vervolg bewijs (= oplossingsmethode):

2. $d \mid b$ en ggd(a, n) = 1

   We weten dus dat a een inverse bezit modulo n, noem deze i

   Een oplossing van de vergelijking moet dus voldoen aan:

   $i \cdot (a \cdot x) \overset{n}{=} i \cdot b$

   $\Rightarrow (i \cdot a) \cdot x \overset{n}{=} i \cdot b$

   $\Rightarrow x \overset{n}{=} i \cdot b$

   $\Rightarrow x = i \cdot b \bmod n$ (als $x \in \{0,1,2, \dots, n-1\}$)

Het oplossen van lineaire congruenties

Vervolg bewijs (= oplossingsmethode):

3. <u>$d \mid b$ en ggd$(a, n) > 1$</u>

 Dit betekent dat d een deler is van a, b en n

 Transformeer de vergelijking dan als volgt:

$$\frac{a}{d} \cdot x \overset{n/d}{=} \frac{b}{d}$$

 Nu geldt wel dat ggd$(a/d, n/d) = 1$

 Dit herleidt dus tot het vorige geval

 ⇒ één oplossing x in $\{0,1,2,\ldots,n/d-1\}$

 ⇒ alle gehele oplossingen van de gedaante $x + k \cdot \frac{n}{d},\ k \in \mathbb{Z}$

 ⇒ van deze oplossingen liggen er d in $\{0,1,2,\ldots,n-1\}$

Het oplossen van lineaire congruenties

Oefening: los op voor $x \in \mathbb{Z}$

$$10x \overset{14}{=} 8$$

Het oplossen van lineaire congruenties

Oefening: los op voor $x \in \mathbb{Z}$

$$10x \overset{14}{=} 8$$

Lineaire diofantische vergelijkingen

Een **lineaire diofantische vergelijking** in twee onbekenden $x, y \in \mathbb{Z}$ is van de vorm

$$ax + by = c$$

waarbij $a, b, c \in \mathbb{Z}$

Het is dus een vergelijking waarvoor we *enkel gehele oplossingen* zoeken

Constructieve oplossingsmethode:

Merk op: dit is equivalent met de lineaire congruentie $ax \stackrel{b}{=} c$

Als ggd(a, b) = 1:

Dit leidt tot de verzameling van oplossingen $x = x_0 + k \cdot b,\ k \in \mathbb{Z}$

Deze x kan vervolgens gesubstitueerd worden in de originele vergelijking

Zo verkrijg je ook de oplossingen $y = y_0 - k \cdot a,\ k \in \mathbb{Z}$

Als ggd(a, b) > 1 en ggd(a, b) | c:

Eerst de vergelijking vereenvoudigen

Lineaire diofantische vergelijkingen: methode 1

Oefening: los op voor $x, y \in \mathbb{Z}$

$$1734x + 221y = 340$$

Stap 1: vereenvoudig, want ggd(1734, 221) = 17 | 340

$$\Rightarrow 102x + 13y = 20$$

Stap 2: los de congruentie op

$$102x \overset{13}{=} 20 \Leftrightarrow 11x \overset{13}{=} 7$$

ggd(11, 13) = 1, dus er bestaat een oplossing: $x = 3 + k \cdot 13,\ k \in \mathbb{Z}$

Stap 3: substitueer in de oorspronkelijke (vereenvoudigde) vergelijking:

$$102 \cdot (3 + k \cdot 13) + 13y = 20, k \in \mathbb{Z}$$

$$\Rightarrow y = -22 - k \cdot 102, k \in \mathbb{Z}$$

De oplossing is dus $(x, y) = (3 + 13k, -22 - 102k),\ k \in \mathbb{Z}$

Lineaire diofantische vergelijkingen: methode 2 (zie syllabus)

Oefening: los op voor $x, y \in \mathbb{Z}$

$$1734x + 221y = 340$$

Stap 1: Bereken d = ggd(1734, 221) = 17 en stel via Euclides ook de lineaire combinatie op:

$$1734 \cdot 6 + 221 \cdot (-47) = 17$$

Stap 2: Dit staat in dezelfde vorm als de originele vergelijking. Enkel het rechterlid komt niet overeen. Vermenigvuldig dus beide leden met 340 / 17 = 20:

$$1734 \cdot (6 \cdot 20) + 221 \cdot (-47 \cdot 20) = 17 \cdot 20$$

$$\Rightarrow \ 1734 \cdot 120 + 221 \cdot (-940) = 340$$

Stap 3: Een particuliere oplossing is dus $(x_0, y_0) = (120, -940)$

Stap 4: Bereken de algemene oplossingenverzameling nu als volgt:

$$(x, y) = (x_0 + k \cdot \frac{b}{d}, y_0 - k \cdot \frac{a}{d}),\ k \in \mathbb{Z}$$

De oplossing is dus $(x, y) = (3 + 13k, -22 - 102k),\ k \in \mathbb{Z}$