

WPO2

Injectiviteit: $f: A \rightarrow B$ injectief \Leftrightarrow

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2$$

Voorbeeld: $\cdot f: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto |x|$ niet injectief vb. $f(-1) = f(1)$ niet surjectief $\text{Im}(f) = \mathbb{R}^+$

- $g: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto \sin(x)$ niet injectief vb. $g(0) = g(\pi)$ niet surjectief $\text{Im}(g) = [-1, 1]$
- $k: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto x^2$ niet injectief vb. $k(-1) = k(1)$ niet surjectief $\text{Im}(k) = \mathbb{R}^+$
- $i: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto \frac{x^2}{2} - x$ niet injectief vb. $i(0) < i\left(\frac{1}{2}\right)$ niet surjectief, parabool
- $j: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto 2x - 3$ wel injectief wel surjectief open niet compleet in \mathbb{R} zijn $y \geq -\frac{1}{8}$

$$j(x_1) = j(x_2) \Leftrightarrow 2x_1 - 3 = 2x_2 - 3 \Leftrightarrow 2x_1 = 2x_2 \Leftrightarrow x_1 = x_2$$

$$j(x) = y \Leftrightarrow 2x - 3 = y \Leftrightarrow x = \frac{y+3}{2}$$

$\cdot k: \mathbb{R}_0 \rightarrow \mathbb{R} : x \mapsto \frac{2x-3}{x}$ wel injectief

$$k(x_1) = k(x_2) \Leftrightarrow \frac{2x_1-3}{x_1} = \frac{2x_2-3}{x_2} \Leftrightarrow (2x_1-3)x_2 = (2x_2-3)x_1$$

$$\Leftrightarrow 2x_1x_2 - 3x_2 = 2x_2x_1 - 3x_1 \Leftrightarrow -3x_2 = -3x_1 \Leftrightarrow x_2 = x_1$$

$$k(x) = y \Leftrightarrow \frac{2x-3}{x} = y \Leftrightarrow 2x-3 = yx \Leftrightarrow -3 = yx - 2x \Leftrightarrow (2-y)x = 3$$

geval 1: $y \neq 2 \Rightarrow x = \frac{3}{2-y}$

geval 2: $y = 2 \Rightarrow 0 \cdot x = 3 \Rightarrow \left. \begin{array}{l} \\ \end{array} \right\} \text{Im}(k) = \mathbb{R} \setminus \{2\}$

$\cdot l: \mathbb{Z} \rightarrow \mathbb{Z} : x \mapsto \frac{2x^2-x}{x}$ wel injectief

$$l(x_1) = l(x_2) \Leftrightarrow 2x_1^2 - x_1 = 2x_2^2 - x_2 \Leftrightarrow 2(x_1^2 - x_2^2) = x_1 - x_2$$

$$\Leftrightarrow 2(x_1 - x_2)(x_1 + x_2) = x_1 - x_2 \Leftrightarrow 2(x_1 + x_2) = 1 \quad (\text{erstel als de factor niet } 0 \text{ is})$$

$$\Leftrightarrow x_1 - x_2 = 0 \vee 2(x_1 + x_2) = 1 \Leftrightarrow x_1 = x_2 \vee x_1 + x_2 = \frac{1}{2}$$

$$\Leftrightarrow x_1 = x_2 \quad (\text{omdat } 0 \text{ en } \frac{1}{2} \text{ niet geldig is in } \mathbb{Z})$$

Surjectiviteit: $f: A \rightarrow B$ $f(A) = \text{Im}(f)$

f is surjectief $\Leftrightarrow \text{Im}(f) = B$

$$\Leftrightarrow \forall b \in B \ \exists a \in A : f(a) = b$$

Bijectiviteit: Functies die zowel injectief als surjectief zijn. Deze hebben exact één origineel per punt. Bijectieve functies hebben altijd een inverse.

Een gegeven functie bijection maken door domein en codomein aan te passen en de inverse functie kunnen berekenen. (injectief door domein, surjectief door codomein)

(18) $f: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto \sqrt[3]{2x+2}$ wel injectief wel surjectief

$$f(x_1) = f(x_2)$$

$$f(x) = y$$

$$\sqrt[3]{2x_1+2} = \sqrt[3]{2x_2+2}$$

$$\Leftrightarrow \sqrt[3]{2x_1+2} = y$$

$$\Leftrightarrow 2x_1+2 = y^3$$

$$\Leftrightarrow 2x_1 = y^3 - 2$$

$$\Leftrightarrow x_1 = \frac{y^3 - 2}{2}$$

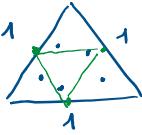
$$\Leftrightarrow x_1 = x_2$$

$$f^{-1}: \mathbb{R} \rightarrow \mathbb{R} : x \mapsto \frac{(x-2)^3}{2}$$

WPO3

Dwurendig principe

$$|A|=k \quad |B|=n \quad f: A \rightarrow B \quad k > n \Rightarrow f \text{ is niet injectief}$$

- ④  Het is niet mogelijk om 5 punten in zo'n driehoek te zetten zodat elke punt van $\frac{1}{2}$ van elkaar zijn.

⑤ $\{a_1, a_2, \dots, a_m\} \subseteq \mathbb{Z} \quad \exists i \neq j : a_i = a_j$

$$\exists i \neq j : a_i = a_j = n + r_i \quad (0 \leq r_i \leq 10)$$

$$a_j = a_i = n + r_j \quad (0 \leq r_j \leq 10)$$

$$\text{met } r_i = r_j$$

$$a_i - a_j = (n + r_i) - (n + r_j) = (r_i - r_j) \cdot 1$$

Dubbel tellingsprincipe

$$A, B \quad S \subseteq A \times B \quad |S| = \sum_{a \in A} k_a \quad (k_a = |\{(x, y) \in S \mid x = a\}|)$$

$$= \sum_{b \in B} c_b \quad (c_b = |\{(x, y) \in S \mid y = b\}|)$$

⑯ $|J| = 32 \quad |M| = x$

$$S = \{(j, m) \in J \times M \mid j \text{ en } m \text{ even elkaar}\}$$

$$k_j = 5 \quad \forall j \in J \quad c_m = 8 \quad \forall m \in M$$

$$\begin{aligned} |S| &= \sum_{j \in J} k_j = \sum_{j \in J} 5 = 3 \cdot 5 \\ &= \sum_{m \in M} c_m = \sum_{m \in M} 8 = 8 \cdot x \end{aligned} \quad \Rightarrow x = 20$$

Telfformules

$$|A|=k \quad |B|=n$$

$$\# f: A \rightarrow B = \boxed{n^k} \quad H \vee$$

$$(k \leq n) \quad \# \text{ injectieve } f: A \rightarrow B = \boxed{\frac{n!}{(n-k)!}} = n \cdot (n-1) \cdot (n-2) \cdots (n-k+1) \quad H \vee$$

$$(k = n) \quad \# \text{ bijectieve } f: A \rightarrow B = \boxed{n!} \left(\begin{array}{l} |\text{Im}(f)| = k = n = |B| \\ \text{Im}(f) \subseteq B \end{array} \right) \Rightarrow \text{Im}(f) = B \quad H \vee$$

$$(k < n) \quad \# k\text{-deelverzamelingen v. } B = \boxed{\binom{n}{k}} = \frac{n!}{k!(n-k)!} \quad H \times$$

$$\# \text{ kerk. combinaties v. } k \text{ uit } n = \binom{n+k-1}{k} \quad H \vee$$

$$(20) A \vee \frac{10!}{(10-4)!} = \frac{10!}{6!}$$

$$(35) HX \quad \binom{6+3-1}{3} = \frac{8!}{3!5!} = 56$$

$$(23) HX \quad \binom{7+2-1}{2} = \frac{8!}{2!6!} = \frac{8 \times 7}{2} = 28$$

$$(25) m! (n+r) r!$$

Inclusive & exclusive

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

$$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D|$$

$$\begin{aligned} & - |A \cap B| - \dots - |C \cap D| \\ & + |A \cap B \cap C| + \dots + |B \cap C \cap D| \\ & - |A \cap B \cap C \cap D| \end{aligned}$$

$$(44) |W| = 67 \quad |F| = 47 \quad |D| = 35 \quad |F \cap D| = 23$$

$$* |W| - |F \cup D| = 67 - (47 + 35 - 23) = 67 - 59 = 8$$

$$|R| = 20 \quad |R \cap F| = 12 \quad |R \cap D| = 11 \quad |D \cap R \cap F| = 5$$

$$* |W \setminus (R \cup F \cup D)| = 67 - (20 + 47 + 35 - 12 - 11 - 23 + 5) = 67 - (102 - 46 + 5) = 67 - 51 = 6$$

$$(45) A, E, M, O, U, Y \quad \text{ME YOUT}$$

$$|W \setminus (W_{ME} \cup W_{YOUT})| = |W| - |W_{ME}| - |W_{YOUT}| + |W_{ME} \cap W_{YOUT}|$$

$$= 6! - 5! - 4! + 3!$$

Bewijs per induktie

(15) $P(1) : \mathcal{U} = 1, 2, 3 \quad RL = \frac{1}{4} \cdot 1 \cdot 2 \cdot 3 \cdot 4 \quad \text{WAPQ4}$

$\forall k \in \mathbb{N}_0 : P(k) \Rightarrow P(k+1)$

Veronderstel $1 \cdot 2 \cdot 3 + \dots + k(k+1)(k+2) = \frac{1}{4} k(k+1)(k+2)(k+3)$

TB $1 \cdot 2 \cdot 3 + \dots + (k+1)(k+2)(k+3) = \frac{1}{4} (k+1)(k+2)(k+3)(k+4)$

B $\mathcal{U} = 1 \cdot 2 \cdot 3 + \dots + k(k+1)(k+2) + (k+1)(k+2)(k+3)$

$$< \frac{1}{4} k(k+1)(k+2)(k+3) + (k+1)(k+2)(k+3)$$

$$= \frac{1}{4} (k+1)(k+2)(k+3)(k+4) = RL$$

Intermezzo (op zoek zonder induktie te gebruiken)

$$\begin{aligned} 1+2+3+\dots+n &= x \\ n+(n-1)+(n-2)+\dots+1 &= x \\ \hline (n+1)+(n+1)+\dots+(n+1) &= 2x \\ \Rightarrow x &= \frac{n(n+1)}{2} \end{aligned}$$

(2) $S_1 = 1 \quad S_2 = 9 \quad S_3 = 36 \quad S_4 = 100 \quad S_5 = 225$
 $= 1^2 \quad = 3^2 \quad = 6^2 \quad = 10^2 \quad = 15^2$
 $= 1+2 \quad = (1+2)^2 \quad = (1+2+3)^2 \quad = (1+2+3+4)^2 \quad = (1+2+3+4+5)^2$

Hypothese: $S_n = \frac{n^2(n+1)^2}{4} \quad \forall n \geq 1$

$P(1) : S_1$

$\forall k \in \mathbb{N}_0 : P(k) \Rightarrow P(k+1)$

Veronderstel: $1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{k^2(k+1)^2}{4}$

TB: $1^2 + 2^2 + \dots + (k+1)^2 = \frac{(k+1)^2(k+2)^2}{4}$

B: $\mathcal{U} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2$

$$= \frac{k^2(k+1)^2}{4} + (k+1)^2$$

$$= \frac{(k+1)^2}{4} (k^2 + 4k + 4) < \frac{(k+1)^2}{4} (k+2)^2 = RL$$

(*) Bewijs dat voor elke $n \in \mathbb{N}$ geldt dat $7 \mid (2^{3n+1} - 14n + 26)$

$f(0) : 2^1 - 0 + 26 = 28 = 4 \times 7$

$\forall k \in \mathbb{N}_0 : P(k) \Rightarrow P(k+1)$

Veronderstel dat $7 \mid (2^{3k+1} - 14k + 26)$

m.e.o. $\exists a \in \mathbb{Z} : 2^{3k+1} - 14k + 26 = a \times 7$

TB $7 \mid 2^{3k+4} - 14k - 14 + 26$

B $2^{3k+4} - 14k + 12 = 8 \times 2^{3k+1} - 14k + 12$

$$= 7 \times 2^{3k+1} + 2^{3k+1} - 14k + 12$$

$$= 7 \times 2^{3k+1} + \underline{2^{3k+1} - 14k + 26} - 14$$

$$= 7 \times 2^{3k+1} + a \times 7 - 14 = 7 \times (2^{3k+1} + a - 2)$$

WPO5

Delings algoritme

$a \in \mathbb{Z}, b \in \mathbb{N}_0 \exists! q, r \in \mathbb{Z}:$

$$a = bq + r \quad \text{en} \quad 0 \leq r < b$$

als $r = 0$ dan $b | a$ (a is dan een veelvoud van b)

$$d = \text{ggd}(a, b)$$

$$d = lk_a + lb$$

(93) $k_7 + l_9 = 1$

$$4 \times 7 - 3 \times 9 = 1$$

Euclidische algoritme

$$a = bq + r \Rightarrow \text{ggd}(a, b) = \text{ggd}(b, r)$$

$$b = r_1 + r_2 \Rightarrow \text{ggd}(b, r) = \text{ggd}(r, r_2)$$

(9) $\text{ggd}(721, 448)$

$$721 = 1 \times 448 + 273$$

$$448 = 1 \times 273 + 175$$

$$273 = 1 \times 175 + 98$$

$$175 = 1 \times 98 + 77$$

$$98 = 1 \times 77 + 21$$

$$77 = 3 \times 21 + 14$$

$$21 = 1 \times 14 + 7$$

$$14 = 2 \times 7 + 0$$

$$\text{ggd}(721, 448) = \text{ggd}(448, 273)$$

$$\text{ggd}(448, 273) = \text{ggd}(273, 175)$$

$$\text{ggd}(273, 175) = \text{ggd}(175, 98)$$

$$\text{ggd}(175, 98) = \text{ggd}(98, 77)$$

$$\text{ggd}(98, 77) = \text{ggd}(77, 21)$$

$$\text{ggd}(77, 21) = \text{ggd}(21, 14)$$

$$\text{ggd}(21, 14) = \text{ggd}(14, 7)$$

$$\text{ggd}(14, 7) = \text{ggd}(7, 0) = 7$$

Het stopt altijd op mind.

$$721 = 1 \times 448 + 273$$

$$448 = 1 \times 273 + 175$$

$$273 = 1 \times 175 + 98$$

$$175 = 1 \times 98 + 77$$

$$98 = 1 \times 77 + 21$$

$$77 = 3 \times 21 + 14$$

$$21 = 1 \times 14 + 7$$

$$14 = 2 \times 7 + 0$$

$$\begin{aligned} 7 &\leq 21 - 14 = 21 - (77 - 3 \times 21) \\ &= 4 \times 21 - 77 < 4 \times (98 - 77) - 77 \\ &= 4 \times 98 - 5 \times 77 = 4 \times 98 - 5 \times (175 - 98) \\ &= 9 \times 98 - 5 \times 175 = 3 \times (273 - 175) - 5 \times 175 \\ &= 3 \times 273 - 14 \times 175 = 3 \times 273 - 14 \times (448 - 273) \\ &= 23 \times 273 - 14 \times 448 \\ &= 23 \times (721 - 448) - 14 \times 448 \\ &= 23 \times 721 - 37 \times 448 \end{aligned}$$

Modulo

$n \in \mathbb{N}_0, a, b \in \mathbb{Z} \quad a \equiv_n b \iff n | a - b$
 $\iff a \text{ en } b \text{ dezelfde rest hebben bij deling door } n.$

$$\begin{array}{l|l} a \equiv_n b & a' \equiv_n b' \\ \hline \Rightarrow a + a' \equiv_n b + b' & 10 \equiv_3 1 \quad 10^2 = 10 \times 10 \equiv_3 1 \times 1 \equiv 1 \\ \Rightarrow aa' \equiv_n bb' & 10^2 \equiv_3 1 \\ \hline \end{array}$$

$$\begin{aligned} (a_m a_{m-1} \dots a_0)_n &= a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_0 \\ &\equiv_3 a_m + a_{m-1} + \dots + a_0 \end{aligned}$$

$$34 \quad \text{Q. } 5783 \equiv_9 5+7+8+3 = 23 \equiv_9 8+3 = 5$$

$$40162 \equiv_9 13 \equiv_9 4$$

$$233256846 \equiv_9 2+3+3+2+5+6+8+4+6 = 38 \equiv_9 12 \equiv_9 3$$

$$\underbrace{5+4}_{20} \equiv_9 3$$

$$20 \equiv_9 2 \quad \boxed{2 \neq 3} \quad \text{Verv. steht nicht}$$

$$35 \quad 10 \equiv_{-1} -1 \quad 10^4 \equiv_{-1} (-1)^4$$

$$\begin{aligned} (a_n a_{n-1} \dots a_0)_{-1} &= a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_0 \\ &\equiv_{-1} (-1)^n a_n + (-1)^{n-1} a_{n-1} + \dots + a_0 \\ &= a_0 - a_1 + a_2 - \dots + (-1)^n a_n \end{aligned}$$

$$35 \quad \text{Zähl } 3^{15} (\text{mod } 17) \text{ en } 15^{81} (\text{mod } 13)$$

$$15 = 8 + 4 + 2 + 1$$

$$3^{15} = 3^8 \times 3^4 \times 3^2 \times 3 \equiv_{17} (-1) \times (-4) \times (-8) \times 3 = 12 \times (-8) \equiv_{17} (-5) \times (-8) = \frac{30}{\equiv_{17} 16}$$

$$3 = 3$$

$$3^2 = 9 \equiv_{17} -8$$

$$3^4 \equiv_{17} (-8)^2 = 64 \equiv_{17} -4$$

$$3^8 \equiv_{17} (-4)^2 = 16 \equiv_{17} -1$$

$$81 = 64 + 16 + 1$$

$$15^{81} = 15^8 \times 15^4 \times 15 = 3 \times 3 \times 2 = 18 \equiv_{15} \boxed{5}$$

$$15 \equiv_{13} 2$$

$$15^2 \equiv_{13} 2^2$$

$$15^4 \equiv_{13} 4^2 = 16 \equiv_{13} 3$$

$$15^8 \equiv_{13} 9 \equiv_{13} -4$$

$$15^{16} \equiv_{13} (-4)^2 = 16 \equiv_{13} 3$$

$$15^{32} \equiv_{13} 3^2 = 9 \equiv_{13} -4$$

$$15^{64} \equiv_{13} (-4)^2 = 16 \equiv_{13} 3$$

Ontbindingen

$$A^2 - B^2 = (A - B)(A + B)$$

$$A^3 - B^3 = (A - B)(A^2 + AB + B^2)$$

$$A^4 - B^4 = (A - B)(A^3 + A^2B + AB^2 + B^3)$$

$$A^n - B^n = (A - B)(A^{n-1} + A^{n-2}B + \dots + AB^{n-2} + B^{n-1})$$

$$= (A - B) \sum_{i=0}^{n-1} A^{n-1-i} B^i$$

15 TB: n niet priem $\Rightarrow 2^{n-1}$ niet prim (contrapositie)

B: Als n niet prim dan $\exists l \leq n, l \leq n-1 : ll = n$

$$2^{n-1} \text{ ontbinden} \Rightarrow 2^{n-1} = 2^{ll-1} = (2^l)^l - 1 = (2^l - 1)(2^{l(l-1)} + 2^{l(l-2)} + \dots + 1)$$

$2^{l-1} + 1$ want dan $2^{l-1} \leq l$

$2^{l-1} + 2^{n-1}$ want dan $2^{l-1} \leq n$

WPO 6

\mathbb{Z}

$$a+b = b+a$$

$$0+a = a = a+0$$

$$1 \cdot a = a = a \cdot 1$$

$$\forall a \exists b : a+b = 0 = b+a \Rightarrow b = -a$$

Voor welke $a \exists b : ab = 1 = ba$:

in $\mathbb{Z} : 1, -1$ in $\mathbb{R} : \mathbb{R}_0$ in $M_{nn}(\mathbb{R})$ = de invertible matrices

→ invertible elements

$a \equiv_n b \Leftrightarrow n | b-a \Leftrightarrow a \text{ en } b \text{zelfde rest bij deling door } n$

$n=3$

$$E_0 = \{0, 3, -3, 6, -6, \dots\}$$

$$E_1 = \{1, 4, -2, 7, \dots\}$$

$$E_2 = \{2, 5, -1, \dots\}$$

$$E_3 = E_0, \quad E_4 = E_1, \quad E_5 = E_2$$

$$E_i + E_j = E_{i+j}, \quad E_i \cdot E_j = E_{i+j}$$

$$\mathbb{Z}_n = \{E_0, E_1, E_2, E_3, \dots, E_{n-1}\} = \{0, 1, 2, \dots, n-1\}$$

$$\begin{aligned} \mathbb{Z}_4 &= \{E_0, E_1, E_2, E_3\} \quad E_2 \cdot E_2 = E_{2+2} = E_4 = E_0 \\ &\subseteq \{0, 1, 2, 3\} \quad 2 \times 2 = 0 \end{aligned}$$

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\} \quad 2 \times 3 = 6 = 1$$

(40) Zoek de invertible elementen van $\mathbb{Z}_6, \mathbb{Z}_7$ en \mathbb{Z}_8

$\ell \in \mathbb{Z}_n$ invertibel als $\text{ggd}(\ell, n) = 1$ (priem)

Bijvout: $\exists \ell, \ell' \in \mathbb{Z} : \ell \cdot \ell' + \ell' \cdot n = 1$

in \mathbb{Z}_5 $\cancel{\{0, 1, 2, 3, 4\}}$ $5^{-1} = 5$ ($5 \times 5 = 25 \equiv_5 1$)

↳ heeft inv.

↳ altijd inv. en heeft altijd zichzelf als inv.

in \mathbb{Z}_7 $\cancel{\{0, 1, 2, 3, 4, 5, 6\}}$ (omdat 7 een priem getal is)

in \mathbb{Z}_8 $\cancel{\{0, 1, 2, 3, 4, 5, 6, 7\}}$

↳ laatste getal is altijd invertibel, omdat het -1 is.

(42) Vind de inversen

(b) 7 in \mathbb{Z}_{16}

We zoeken $\ell, \ell \in \mathbb{Z}$ zodat $7 \cdot \ell + \ell \cdot 16 = 1$

$$16 = 2 \cdot 7 + 2 \quad | \quad 1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (16 - 2 \cdot 7)$$

$$7 = 3 \cdot 2 + 1 \quad | \quad = 7 \cdot 7 - 3 \cdot 16$$

$$\text{Dus } 7^{-1} = 7 \text{ (in } \mathbb{Z}_{16})$$

(d) 5 in \mathbb{Z}_{13}

We zoeken $\ell, \ell \in \mathbb{Z}$ zodat $5 \cdot \ell + 13 \cdot \ell = 1$

Dus $5^{-1} = -5 \equiv 8$ (in \mathbb{Z}_{13})

$$13 = 2 \cdot 5 + 3 \quad | \quad 1 = 3 - 2 \cdot 2 = 3 - (5 - 3) = 3 - 5 + 3 = 3 - 5 + 2 \cdot 2 = 3 - 5 + 4 = 8$$

$$5 = 1 \cdot 3 + 2 \quad | \quad = 2 \cdot (13 - 2 \cdot 5) - 5 = 2 \cdot 13 - 5 \cdot 2 = 2 \cdot 13 - 10 = 2 \cdot 13 - 5 \cdot 2 = 8$$

$$3 = 1 \cdot 2 + 1$$

RSA algoritme

Kies p, q priem stel $n = pq$, $b = (p-1)(q-1)$

Kies e : $\text{ggd}(e, b) = 1$

Stel $d = e^{-1}$ in \mathbb{Z}_b

$m \xrightarrow{\text{vers}} m^e \pmod{n} \xrightarrow{\text{ontdek}} c^d \pmod{n}$

$$\textcircled{58} \quad c=8 \quad n=55 \quad e=7$$

$$n = 55 = 5 \times 11 \quad b = 4 \times 10 = 40 \quad d = e^{-1} \text{ in } \mathbb{Z}_b \\ = 7^{-1} \text{ in } \mathbb{Z}_{40}$$

$$\begin{array}{l|l} 40 = 5 \times 7 + 5 & 1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 5) \\ 7 = 1 \times 5 + 2 & = 3 \times 5 - 2 \times 7 = 3 \times (40 - 5 \times 7) - 2 \times 7 \\ 5 = 2 \times 2 + 1 & = 3 \times 40 - 17 \times 7 \end{array}$$

dus $d = -17 = 23$ (van d willen we een positief getal en nemen we)
 (dus de invers van -17)

$$m = c^d \pmod{n} = 8^{23} \pmod{55}$$

$$8^{16} + 8^4 + 8^2 + 8^1$$

$$\text{in } \mathbb{Z}_{55}: \begin{array}{l} 8 = 2 \\ 8^2 = 4 \end{array}$$

$$8^4 = 4^2 = 16$$

$$8^8 = 16^2 = 256 = 36 \equiv -19 \quad (\text{hier liever nemen de absolute waarde})$$

$$8^{16} = (-19)^2 = 361 = 31 = -24$$

$$8^{16} + 8^4 + 8^2 + 8^1 \equiv_{55} 7 \times 16 + 4 \equiv_{55} 7 \times 3 = 63 \equiv_{55} \boxed{8}$$

Test (verificatie)

$$8^7 \equiv 2 \pmod{55}$$

$$\textcircled{*} \quad c=83 \quad n=91 \quad e=25$$

$$n = 91 = 7 \times 13 \quad b = 6 \times 12 - 72 \quad d = 85^{-1} \text{ in } \mathbb{Z}_{72}$$

$$\begin{array}{l|l} 72 = 8 \times 9 + 24 & 1 = 24 - 7 \times 3 = 24 - 7 \times (25 - 22) \\ 25 = 1 \times 22 + 3 & = 8 \times 9 - 7 \times 25 = 8 \times (9 - 2 \times 5) - 7 \times 25 \\ 22 = 7 \times 3 + 1 & = 8 \times 72 - 23 \times 25 \end{array}$$

Dus $d = -23 = 49$ in \mathbb{Z}_{72} (hier gebruiken we mod 6, maar bij de berekening gebruikten we mod 91)

$$\text{Dus } n = 83^{49} \pmod{91} = 83^{32} \times 83^{16} \times 83^1 \pmod{91}$$

$$\text{in } \mathbb{Z}_{91}: 83 = -8$$

$$83^2 = (-8)^2 = 64 \equiv -28$$

$$83^4 = (-28)^2 = (8 \times 3)^4 = 81 \times 81 = -10 \times 81 = 80 = -1$$

$$83^8 = (-1)^2 = 1$$

$$83^{16} = 1$$

$$83^{32} = 1$$

$$1 \times 1 \times 83 = \boxed{83}$$

Chinese Reststelling

(55) $\begin{array}{l} \text{a}_1 = 3 \in \mathbb{Z}_{m_1} \\ \text{a}_2 = 10 \in \mathbb{Z}_{m_2} \\ \text{a}_3 = 0 \in \mathbb{Z}_{m_3} \end{array}$

$$\begin{array}{ll} M_1 = m_2 m_3 = 16 \times 15 = 240 & \\ M_2 = m_1 m_3 = 17 \times 15 = 255 & \\ M_3 = m_1 m_2 = 17 \times 16 = 272 & \end{array}$$

$$y_1 = M_1^{-1} \text{ in } \mathbb{Z}_{m_1} = 240^{-1} \text{ in } \mathbb{Z}_{17} = 70^{-1} \text{ in } \mathbb{Z}_{17} = 2^{-1} = 9$$

$$y_2 = M_2^{-1} \text{ in } \mathbb{Z}_{m_2} = 255^{-1} \text{ in } \mathbb{Z}_{16} = 95^{-1} \text{ in } \mathbb{Z}_{16} = 15^{-1} = -1$$

$$y_3 = M_3^{-1} \text{ in } \mathbb{Z}_{m_3} = \text{overbodig omdat } m_3 = 0$$

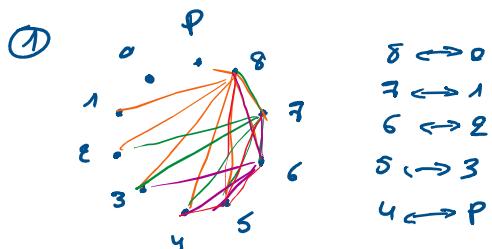
$$n = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + k M_1 M_2 M_3 \quad (k \in \mathbb{Z})$$

$$= 3 \times 240 \times 9 + 10 \times 255 \times (-1) + k \cdot 240 \cdot 255 \quad (k \in \mathbb{Z})$$

$$= 6480 - 2550 + k \cdot 240 \cdot 255 \quad (k \in \mathbb{Z})$$

$$= 3930 + k \cdot 240 \cdot 255 \rightarrow \text{kleinst mogelijk is voor } k = 0, \boxed{2930}$$

WPO7



② n knopen $0 \leq \text{graad}(v) \leq n-1$

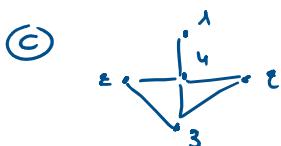
$\vdots \quad ; \quad ; \quad \dots \quad \vdots \quad n-1$



Handshake principe

$\sum_{v \in V(G)} \deg(v) = 2|E(G)|$ De som vpt + bogen moet even zijn
 v.v $\in V(G)$ even

⑤ | Neen

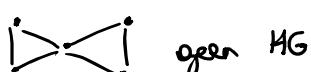


⑦ Alle 4 verschillend, dus het kan niet

Hamilton graf



Is een graf die een Hamilton cycle heeft, een Hamilton cycle is een cyclus die exact één keer door elke knoop gaat.



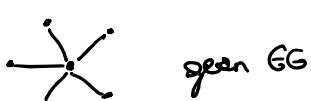
⑧



Euler graf



Een Euler graf is een graf die een Euler cycle heeft, een Euler cycle is een cyclus die exact één keer door elke boog gaat.



15 a)  Onwaar

b) G_7 moet even zijn (laadstatische principie) dus is het G_8 en voor G_8 is deze uitspraak waar.

c)

$$\left. \begin{array}{l} \sum_{v \in V(G)} \deg(v) \text{ even} \\ V(G) = E \cup O \\ \text{even } g. \quad \text{even } g. \end{array} \right\} \quad \left. \begin{array}{l} \sum_{v \in V(G)} \deg(v) = \sum_{v \in E} \deg(v) + \sum_{v \in O} \deg(v) \\ |O| \rightarrow \text{even} \end{array} \right\} \quad \text{Waar}$$

d) Onwaar



e) Onwaar

Kubus voorbeeld



"Afstand" is altijd het korte afstand

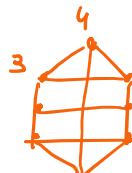
Onwaar



Hier zijn precies
0 toppen op afstand 2



Er bestaat geen
3-reguliere graf met
5 toppen ($3 \times 5 = 15$ toppen)



17)

$$\left. \begin{array}{l} \sum_{v \in V(G)} \deg(v) = 2|E(G)| \\ 2+2+\dots+2 = 2|V(G)| \\ |V| \text{ is even} \end{array} \right\} \quad \left. \begin{array}{l} |E(G)| = \frac{\text{even}}{2} \times \frac{\text{even}}{2} \\ \frac{2 \times |V(G)|}{2} \end{array} \right\}$$

24)

$$\sum_{v \in V(G)} \deg(v) = 2|E(G)|$$

$$2|V(G)| \Rightarrow |V(G)| = \frac{2|E(G)|}{2} = \frac{64}{2}$$

1 2 4 11 22 14 (delen van 64)

niet
samenhangend



HG eigenschappen

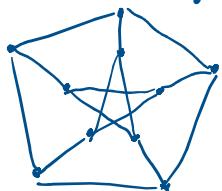
- Als de graad van alle top gelijk is aan minstens de helft van de toppen, dan is het sowieso een HG. (omgekeerde redenering werkt niet)
- Een graf is niet Hamilton, als een graf een schanselpunt bevat (omgekeerde redenering geldt niet) (dit geldt ook voor 2 toppen die de graf in 3 samenhangende comp. splitsen)

WPO8

④ Deze graf is geen HG

→ Dit is te bewijzen doel de topfen b en g weg doen. Dan wordt de graf verdeeld in drie delen.

⑤ Peterson graf



- eigenschappen v. PG:
- 3-regulier
 - Lengte langste cycle is 5
 - 10 topfen

PG bevat een Hamiltonpad, maar geen Hamilton cycle

⑥



$$\sum_{v \in V(G)} \deg(v) \geq 2|E(G)|$$

$$= 2 \times 28 = 56$$

$$\Rightarrow \exists v_0 \in V(G) \text{ met } \deg(v_0) \geq 6$$

$$\sum_{v \in V(G) \setminus \{v_0\}} \deg(v) \geq 56 - 6 = 50$$

$$\Rightarrow \exists v_1 \in V(G) \text{ met } \deg(v_1) \geq 6$$

Bomen & bossen

Boom = samenkondigende graf zonder cycle (= gesloten punten)



$$|E(G)| = |V(G)| - 1$$

Bos = Bestaat uit verschillende bomen



⑦



graad 3
pad van X naar Y
3 is (bij de bosreeks
is het 2) dus isomorf



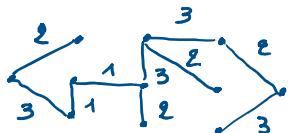
(34)



(35)

Gierigheidsalgoritme

Elke keer de minimaal gewicht boog nemen (behalve als deze een gesloten pad vormt)



Wat is een eindige 2-reguliere graf?



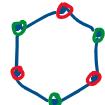
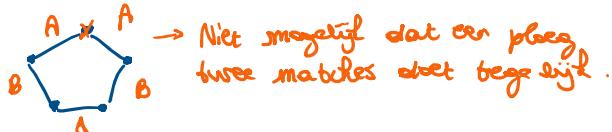
→ Een graf waarin elke s.t. component een cirkel is.
(bij oneindig geldt dit niet)

(36)

$$\text{G } |V(G)| = \{ \text{p-lingen} \}$$

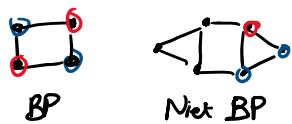
$$|E(G)| = \{ p \cap q \mid p, q \in V(G) \text{ zodat } p \text{ reeds tegen } q \text{ heeft gespeeld} \}$$

G 2-regulieren



Bipartiete graffer

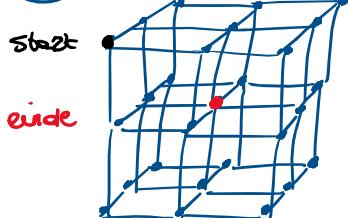
Toppen kunnen verdeeld zijn in twee groepen, zodanig dat 2 toppe v/dzelfde groep niet gebonden zijn.



Om na te gaan of een graf bipartiet is, moeten we een willekeurige top nemen die alleen een zijn buren in een andere kleur hebben enz.

(Om aan te tonen dat het niet bipartiet is, moeten we een oneven cycli vinden)

(13)



elke top stelt een kleine laaglus voor
(deze graf is bipartiet)

De start-top en eind-top zijn niet in dezelfde kleur
(bij het scheiden v/d toppen in partities)

Koppeling

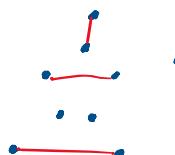
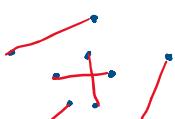
geen koppeling:



↳ Maximale

↳ Maximale \times Maximale \times Volledig

(35)

Toewijzing (koppeling in bipartiete graff)

$(X \cup Y, \cup)$ bip.

toewijzing v. W = koppeling die W verzaagtigt

stelling v. Hall

\exists bestaat een toewijzing van W ase $\forall W' \subset W : |H(W')| \geq |W'|$

④5 $(S \cup \{\}, \sim)$ bip. g. $\omega \subset S$ willkürlich

TB: $|H(\omega)| \geq |\omega|$

B