Examen Discrete Wiskunde – DEEL 1

dr. ir. Cedric De Boom en dr. Marleen Denert

28 augustus 2021, 8u30

Naam en Voornaam:

Lees eerst dit:

(i) Het examen bestaat uit twee fysieke delen. Naam en voornaam op beide delen invullen!

(ii) Nietje niet losmaken.

(iii) Schrijf duidelijk, gebruik bij voorkeur een donkere pen.

(iv) Respecteer de antwoordvakken zo veel mogelijk.

(v) Als je een stelling, eigenschap, ... gebruikt, formuleer die dan, toon aan dat de voorwaarden vervuld zijn, maar bewijs die niet.

(vi) Speciaal voor de waar-of-valsvragen: indien de bewering WAAR is, geef je een bewijs of logische verklaring; indien VALS, leg je uit waarom of geef je een tegenvoorbeeld, en corrigeer je indien nodig de bewering. Enkel indien de motivering correct is, wordt het antwoord goed bevonden.

(vii) Je hebt 3 uur tijd voor dit examen.

Puntenverdeling:

VRAAG	TOTAAL
1	/8
2	/10
3	/5
4	/8
5	/4
6	/10
7	/10
8	/10
	/65

VRAAG 1

Bewijs dat de commutatieve ring $\mathbb{Z}_n$ (met de operatoren $+$ en $\cdot$) een veld is als en slechts als n priem is.

Dit is het letterlijke bewijs van Stelling 4.1 in de cursus.

① n is priem $\Rightarrow$ $\mathbb{Z}_n$ is een veld

$\mathbb{Z}_n$ is een commutatieve ring, dus we moeten aantonen dat elk element in $\mathbb{Z}_n$ een inverse heeft opdat het een veld zou zijn.

We weten dat indien $ggd(a, n) = 1$, dan bestaat er één getal $x \in \mathbb{Z}_n$ waarvoor $a \cdot x \overset{n}{=} x \cdot a \overset{n}{=} 1$.

Vermits n priem is, is dit het geval $\forall a \in \mathbb{Z}_n$.

② $\mathbb{Z}_n$ is een veld $\Rightarrow$ n is priem

Contrapositie: $\neg(n \text{ is priem}) \Rightarrow \mathbb{Z}_n$ is geen veld.

$\neg(n \text{ is priem}) \Rightarrow \exists$ priemgetal $p : p \mid n$ en $p \neq n$ en $p \neq 1$.

Mocht p een inverse x hebben, dan:

$$p \cdot x = 1 + k \cdot n$$

Vermits $p \mid n \Rightarrow p \mid (p \cdot x - k \cdot n) \Rightarrow p \mid 1$.

Dit is een contradictie met

Bijgevolg heeft p geen inverse in $\mathbb{Z}_n$ en is $\mathbb{Z}_n$ dus ook geen veld

$\square$.

VRAAG 2

(a) Bepaal de periode van de pseudorandomgenerator

$$x_{i+1} = (5x_i + 4) \text{ mod } 9; \quad x_0 = 0$$

Reken uit:

$x_0 = 0$

$x_1 = (5 \cdot 0 + 4) \text{ mod } 9 = 4$

$x_2 = (5 \cdot 4 + 4) \text{ mod } 9 = 6$

$x_3 = (5 \cdot 6 + 4) \text{ mod } 9 = 7$

$x_4 = (5 \cdot 7 + 4) \text{ mod } 9 = 3$

$x_5 = (5 \cdot 3 + 4) \text{ mod } 9 = 1$

$x_6 = (5 \cdot 1 + 4) \text{ mod } 9 = 0$

De periode is dus 6.

(b) Toon aan dat de periode van volgende pseudorandomgenerator maximaal is:

$$y_{i+1} = (11y_i + 3) \text{ mod } 50; \quad y_0 = 0$$

Gebruik het Hull-Dobell-theorema:

- $c \neq 0$: voldaan
- $ggd(c, m) = 1$: $ggd(3, 50) = 1$: voldaan.
- $\underbrace{a-1}_{10}$ deelbaar door $\underbrace{\text{alle priemfactoren van } m}_{50 = 2 \cdot 5 \cdot 5}$: $2 | 10$ en $5 | 10$: voldaan.
- $\underbrace{a-1 \text{ deelbaar door } 4}_{4 \nmid 10}$ als $\underbrace{m \text{ deelbaar door } 4}_{4 \nmid 50}$: voldaan.

$\Rightarrow$ periode is maximaal $= 50$.

(c) Beschouw nu een residugetalsysteem a.d.h.v. de moduli 9 en 50. In dit getalsysteem construeren we volgende pseudorandomgenerator:

$$z_i = (x_i, y_i)$$

M.a.w. het getal z_i is een koppel met als eerste element x_i uit de pseudorandomgenerator van vraag (a) en als tweede element y_i uit de pseudorandomgenerator van vraag (b). We krijgen dus: $z_0 = (x_0, y_0), z_1 = (x_1, y_1), z_2 = (x_2, y_2)$, etc.

Wat is de periode van pseudorandomgenerator z? Beredeneer en leg uit.

9 en 50 zijn onderling priem, dus in het residutalstelsel kunnen we elk getal $\in \{0, 1, 2, \ldots, \underbrace{449}_{9 \cdot 50 - 1}\}$ uniek voorstellen door een koppel getallen (x, y) als $x \in \{0, 1, \ldots, 8\}$ en $y \in \{0, 1, \ldots, 49\}$. Dit is het geval voor beide generatoren uit (a) en (b): z_i is uniek voor elk uniek koppel (x_i, y_i).

We weten dat x zich om de 6 stappen herhaalt.

De generator y herhaalt zich om de 50 stappen.

Op welk punt vallen beide generatoren terug samen?

i.e. voor welke i is $(x_i, y_i) = (x_0, y_0)$?

Het is eenvoudig te zien dat $i = \text{kgv}(6, 50) = 150$.

De periode van generator z is dus 150.

VRAAG 3

Noteer het n'de getal in de rij van Fibonacci als F_n, met $n \in \mathbb{N}_0$. Er geldt:

$$\begin{aligned} F_1 &= 1, \\ F_2 &= 1, \\ F_n &= F_{n-1} + F_{n-2} \text{ voor } n > 2. \quad (*) \end{aligned}$$

De rij gaat dus als volgt: 1, 1, 2, 3, 5, 8, 13, 21, 34, ... Bewijs nu volgende eigenschap voor de rij van Fibonacci: elk vierde Fibonaccigetal is deelbaar door 3, of: voor alle $n \in \mathbb{N}_0$ geldt

$$3 \mid F_{4n}$$

Inductie:

- Basisstap: $n=1$: $3 \mid F_4$? Gezien $F_4 = 3$ is dit voldaan.
- Inductiestap: stel dat $3 \mid F_{4m}$ $\forall m \leq n$, $n \in \mathbb{N}_0$. (Inductiehypothese)

  geldt dan: $3 \mid F_{4(n+1)}$?

Bewijs:
$$\begin{aligned} F_{4(n+1)} &= F_{4n+4} \\ &= F_{4n+3} + F_{4n+2} \quad (\text{wegens } *) \\ &= F_{4n+2} + F_{4n+1} + F_{4n+1} + F_{4n} \quad (\text{wegens } *) \\ &= F_{4n+1} + F_{4n} + F_{4n+1} + F_{4n+1} + F_{4n} \quad (\text{wegens } *) \\ &= \underbrace{3 \cdot F_{4n+1}}_{\text{deelbaar door 3}} + \underbrace{2 F_{4n}}_{\text{deelbaar door 3}} \end{aligned}$$

$\Rightarrow F_{4(n+1)}$ deelbaar door 3.

$\square$.

VRAAG 4

Waar of vals? Indien de bewering waar is, geef je een bewijs of logische verklaring. Indien vals, dan leg je uit waarom of geef je een tegenvoorbeeld. Corrigeer indien nodig de bewering.

(a) Gegeven R is een equivalentierelatie. Als $(c,a) \in R$ en $(c,b) \in R$, dan moet ook $(a,b) \in R$.

Waar:

1) symmetrie: $(c,a) \in R \Rightarrow (a,c) \in R$.

2) transitiviteit: $(a,c) \in R$ en $(c,b) \in R \Rightarrow (a,b) \in R$

$\square$.

(b) Als p een priemgetal is en $p \mid a^2$, dan moet $p \mid a$.

Waar:

Gebruik de fundamentele stelling van de rekenkunde.
Stel a voor door diens unieke priemontbinding.

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_N^{k_N}$$

$$\Rightarrow a^2 = p_1^{2k_1} \cdot p_2^{2k_2} \cdots p_N^{2k_N}$$

elke priemfactor van a komt dus dubbel zo vaak voor in de priemontbinding van a^2. M.a.w. als $p \mid a^2$, moet $p = p_1$ of $p = p_2$ of $\cdots$ of $p = p_N$.
En dus moet ook gelden dat $p \mid a$.

$\square$.

Alternatief (formeler) via contrapositie: $p \nmid a \overset{?}{\Rightarrow} p \nmid a^2$
Als $p \nmid a$, dan komt p niet voor in priemontbinding van a.
Gezien alle priemfactoren van a dubbel voorkomen in a^2 (en geen extra) volgt hieruit dus dat ook $p \nmid a^2$.

(c) Veronderstel een binaire code met minimale Hammingafstand $d = 2$. Wanneer er 1 bitfout optreedt bij de verzending van een gecodeerd bitpatroon, kan het ontvangen bitpatroon altijd gecorrigeerd worden naar het originele bitpatroon.

Vals:

er kunnen slecht $< \frac{d}{2}$ 1 fouten gecorrigeerd worden opdat we het originele bitpatroon zouden terugvinden

Tegenvoorbeeld:

2 codewoorden: 000 en 110

min. Hammingafstand is duidelijk 2.

Introduceer 1 fout in 000: 010

000 ? 010 ? 110

We kunnen niet achterhalen of het originele codewoord 000 of 110 was, want 010 ~~ligt~~ verschilt in 1 bit van beide.

(d) Elk predikaat is een propositie, maar niet elke propositie is een predikaat.

Vals: het is omgekeerd: elke propositie is een predikaat, maar niet elk predikaat is een propositie.

e.g. $P: \mathbb{Z} \to \mathbb{B} : n \mapsto 5|n$ is een predikaat.

De waarheidswaarde hangt af van n, en is dus geen propositie

VRAAG 5

Een logicus heeft een aantal speelkaarten met een getal op één zijde en een letter op de andere. Hij legt vier kaarten op tafel, met daarop leesbaar de symbolen E, K, 4 en 7. Hij claimt nu voor deze vier kaarten dat als een kaart een klinker heeft op één zijde, ze dan een even getal heeft op de andere zijde. Welke kaarten moet je zeker omdraaien om zijn bewering te verifiëren? Leg grondig uit.

Waarheidstabel voor $p \Rightarrow q$:

p = "klinker"
q = "even getal".

p	q	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

$p \Rightarrow q$ is enkel vals als p waar is en q vals, m.a.w. als de kaart een klinker heeft op 1 zijde, maar een oneven getal op de andere zijde.

- Kaart E : omdraaien : we moeten controleren of de andere zijde een even getal is.
- Kaart K : niet omdraaien, p is toch vals.
- Kaart 4 : niet omdraaien, q is waar en dus maakt p niet uit.
- Kaart 7 : omdraaien, q is vals en dus moet gecontroleerd worden of p ook vals is, m.a.w. of de andere zijde een medeklinker heeft

Examen Discrete Wiskunde – DEEL 2

Naam en Voornaam:

VRAAG 6

Mevr. Vermeulen is in de wolken: ze heeft eindelijk eens geld gewonnen met een kraslotje en wil haar prijs zo snel mogelijk in ontvangst nemen in de krantenwinkel. De winkelbediende is helaas onzorgvuldig: mevr. Vermeulen heeft E euro's en C cent gewonnen, maar de bediende geeft haar C euro's een E cent. Mevr. Vermeulen merkt niets op en wandelt de winkel blij buiten. Echter, nadat ze 5 cent heeft geschonken aan een straatmuzikant wat verder in de straat, merkt ze dat ze nu dubbel zo veel geld heeft als wat ze normaal met het kraslotje gewonnen zou hebben. Achterhaal met behulp van deze informatie welk bedrag mevr. Vermeulen gewonnen heeft met het kraslotje.

Schrijf vraagstuk als lineaire diofantische vgl:

$$100 \cdot C + E - 5 = 2 \cdot (100 \cdot E + C)$$

$$\Leftrightarrow 100C - 2C + E - 200E = 5$$

$$\Leftrightarrow 98C - 199E = 5. \quad (*)$$

Beschouw deze vgl. modulo 98:

$$-199E \overset{98}{=} 5 \Leftrightarrow 95E \overset{98}{=} 5$$

Zoek de inverse van 95 modulo 98 via Euclides:

95	98	1	0	0	1
95	3	1	0	-1	1
2	3	32	-31	-1	1
2	1	32	-31	-33	32
1	1	$\boxed{65}$	-63	-33	32

$$\Rightarrow E \overset{98}{=} 65 \cdot 5 \Leftrightarrow E \overset{98}{=} 31 \Leftrightarrow \boxed{E = 31 + 98k, k \in \mathbb{Z}.}$$

Vul in in $(*)$:

$$98C - 199(31 + 98k) = 5$$

$$\Leftrightarrow 98C - 6169 - 19502k = 5$$

202

Vervolg vraag 6.

$$\Leftrightarrow \quad 98C = 6174 + 19502k$$

$$\Leftrightarrow \quad \boxed{C = 63 + 199k, \quad k \in \mathbb{Z}}$$

Antwoord: het gewonnen bedrag was 31 euro en 63 cent.

we controleren:

$$63{,}31 - 0{,}05 \overset{?}{=} 2 \cdot (31{,}63)$$

$$\Leftrightarrow \quad \underbrace{\frac{63{,}26}{2}}_{\substack{\parallel \\ 31{,}63}} \overset{?}{=} 31{,}63 \qquad \checkmark$$

VRAAG 7

Gegeven is de veelterm $h(x) = x^3 - x + 1$ die gebruikt wordt als voortbrengende veelterm van een eindig veld GF(27).

3^3

(a) Toon aan dat $h(x)$ als voortbrengende veelterm van GF(27) irreducibel is. Gebruik (een variant van) de Rabin test.

Graad van $h(x) = 3 = n \rightarrow$ heeft 1 unieke priemdeler $p_1 = 3$

$\Rightarrow n_1 = \frac{n}{p_1} = 1.$

Rabin test:

1) Check of $\text{ggd}(h, x^3 - x) = 1$.

$$\begin{array}{l|l} x^3 - x + 1 & x^3 - x \\ x^3 - x & 1 \\ \hline 1 & \end{array}$$

$\Rightarrow \text{ggd}(h, x^3 - x) = \text{ggd}(1, x^3 - x) = 1.$ ✓

2) Check of h deler is van $x^{3^3} - x = x^{27} - x$.

$$\begin{array}{l|l} x^{27} - x & x^3 - x + 1 \\ \hline & x^{24} + x^{22} + 2x^{21} + x^{20} + x^{19} + 2x^{18} + x^{16} \\ & + x^{15} + x^{14} + 2x^{11} + 2x^9 + x^8 + 2x^7 \\ & + 2x^6 + x^5 + 2x^3 + 2x^2 + 2x \end{array}$$

$$\begin{array}{l} x^{27} - x \\ - \; x^{27} + 2x^{25} + x^{24} \\ \hline x^{25} + 2x^{24} + 2x \\ - \; x^{25} + 2x^{23} + x^{22} \\ \hline 2x^{24} + x^{23} + 2x^{22} + 2x \\ - \; 2x^{24} + x^{22} + 2x^{21} \\ \hline x^{23} + x^{22} + x^{21} + 2x \\ - \; x^{23} + 2x^{21} + x^{20} \\ \hline x^{22} + 2x^{21} + 2x^{20} + 2x \\ - \; x^{22} + 2x^{20} + x^{19} \\ \hline 2x^{21} + 2x^{19} + 2x \\ - \; 2x^{21} + x^{19} + 2x^{18} \\ \hline x^{19} + x^{18} + 2x \\ - \; x^{19} + 2x^{17} + x^{16} \\ \hline x^{18} + x^{17} + 2x^{16} + 2x \end{array}$$

$$\begin{array}{l} x^{18} + x^{17} + 2x^{16} + 2x \\ - \; x^{18} + 2x^{16} + x^{15} \\ \hline x^{17} + 2x^{15} + 2x \\ - \; x^{17} + 2x^{15} + x^{14} \\ \hline 2x^{14} + 2x \\ - \; 2x^{14} + x^{12} + 2x^{11} \\ \hline 2x^{12} + x^{11} + 2x \\ - \; 2x^{12} + x^{10} + 2x^9 \\ \hline x^{11} + 2x^{10} + x^9 + 2x \\ - \; x^{11} + 2x^9 + x^8 \\ \hline 2x^{10} + 2x^9 + 2x^8 + 2x \\ - \; 2x^{10} + x^8 + 2x^7 \\ \hline 2x^9 + x^8 + x^7 + 2x \end{array}$$

$$\begin{array}{l} 2x^9 + x^8 + x^7 + 2x \\ - \; 2x^9 + x^7 + 2x^6 \\ \hline x^8 + x^6 + 2x \\ - \; x^8 + 2x^6 + x^5 \\ \hline 2x^6 + 2x^5 + 2x \\ - \; 2x^6 + x^4 + 2x^3 \\ \hline 2x^5 + 2x^4 + x^3 + 2x \\ - \; 2x^5 + x^3 + 2x^2 \\ \hline 2x^4 + x^2 + 2x \\ - \; 2x^4 + x^2 + 2x \\ \hline 0. \end{array}$$

✓

VEEL WERK !

in de variant moet je enkel controleren dat $\text{ggd}(h, x^3 - x) = 1$.

$\Rightarrow$ GEBRUIK VARIANT v/d TEST !

(b) Vul onderstaande tabel aan voor GF(27) met $h(x)$ als voortbrengende veelterm. Hierbij kozen we α als imaginaire eenheid. Deze tabel bevat in de 1ste kolom oplopende machten van α: $0, \alpha^0, \alpha^1, \alpha^2, \ldots$ en in de 2de kolom het overeenkomstige element y in GF(27). Gebruik de witruimte rechts (en eventueel de achterkant) voor berekeningen.

α^k	y
0	0
α^0	1
α^1	α
α^2	α^2
α^3	$\alpha+2$
α^4	$\alpha^2+2\alpha$
α^5	$2\alpha^2+\alpha+2$
α^6	$\alpha^2+\alpha+1$
α^7	$\alpha^2+2\alpha+2$
α^8	$2\alpha^2+2$
α^9	$\alpha+1$
α^{10}	$\alpha^2+\alpha$
α^{11}	$\alpha^2+\alpha+2$
α^{12}	α^2+2
α^{13}	2
α^{14}	2α
α^{15}	$2\alpha^2$
α^{16}	$2\alpha+1$
α^{17}	$2\alpha^2+\alpha$
α^{18}	$\alpha^2+2\alpha+1$
α^{19}	$2\alpha^2+2\alpha+2$
α^{20}	$2\alpha^2+\alpha+1$
α^{21}	α^2+1
α^{22}	$2\alpha+2$
α^{23}	$2\alpha^2+2\alpha$
α^{24}	$2\alpha^2+2\alpha+1$
α^{25}	$2\alpha^2+1$

We weten dat $h(x) = x^3 - x + 1$

$\Rightarrow \alpha^3 - \alpha + 1 = 0 \Rightarrow \alpha^3 = \alpha + 2.$

$\alpha^3 = \alpha + 2.$

$\alpha^4 = \alpha(\alpha+2) = \alpha^2 + 2\alpha$

$\alpha^5 = \alpha(\alpha^2+2\alpha) = \alpha^3 + 2\alpha^2 = \alpha + 2 + 2\alpha^2.$

$\alpha^6 = \alpha(2\alpha^2+\alpha+2) = 2\alpha^3 + \alpha^2 + 2\alpha = 2\alpha + 1 + \alpha^2 + 2\alpha$
$= \alpha^2 + \alpha + 1$

$\alpha^7 = \alpha(\alpha^2+\alpha+1) = \alpha^3 + \alpha^2 + \alpha = \alpha + 2 + \alpha^2 + \alpha$
$= \alpha^2 + 2\alpha + 2$

$\alpha^8 = \alpha(\alpha^2+2\alpha+2) = \alpha^3 + 2\alpha^2 + 2\alpha = \alpha + 2 + 2\alpha^2 + 2\alpha$
$= 2\alpha^2 + 2$

$\alpha^9 = \alpha(2\alpha^2+2) = 2\alpha^3 + 2\alpha = 2\alpha + 1 + 2\alpha$
$= \alpha + 1$

$\alpha^{10} = \alpha(\alpha+1) = \alpha^2 + \alpha$

$\alpha^{11} = \alpha(\alpha^2+\alpha) = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 2$

$\alpha^{12} = \alpha(\alpha^2+\alpha+2) = \alpha^3 + \alpha^2 + 2\alpha = \alpha + 2 + \alpha^2 + 2\alpha$
$= \alpha^2 + 2$

$\alpha^{13} = \alpha(\alpha^2+2) = \alpha^3 + 2\alpha = \alpha + 2 + 2\alpha = 2.$

(c) Los volgende vierkantsvergelijking in X op in GF(27):

$$X^2 + \alpha^5 X + \alpha^9 = 0$$

Herinner: de oplossingen van de vergelijking $aX^2 + bX + c = 0$ zijn $X_{1,2} = \frac{1}{2a}(-b \pm \sqrt{D})$ met $D = b^2 - 4ac$. Tip: schrijf D eerst als macht van α.
Schrijf je finale oplossingen $X_{1,2}$ in de vorm α^k (met $k \leq 25$), en gebruik uiteraard de tabel uit (b).

$$\begin{aligned} D &= b^2 - 4\alpha c \\ &= (\alpha^5)^2 - 4 \cdot 1 \cdot \alpha^9 \\ &= \alpha^{10} - 4\alpha^9 \\ &= \alpha^{10} + 2\alpha^9 \\ &= \alpha^9 (\alpha + 2) \quad \text{zoek op in tabel} \\ &= \alpha^9 \cdot \alpha^3 \\ &= \alpha^{12} \end{aligned}$$

$\Rightarrow \sqrt{D} = \sqrt{\alpha^{12}} = \alpha^6.$

We vinden dus:

- $X_1 = \frac{1}{2}(-\alpha^5 + \alpha^6) = \frac{1}{2}(2\alpha^5 + \alpha^6)$
$= \frac{1}{2}(\alpha^5(2+\alpha)) = \frac{1}{2}(\alpha^5\alpha^3) = \frac{1}{2}\alpha^8 = \frac{1}{2}(2\alpha^2 + 2)$
$= \alpha^2 + 1$
$= \boxed{\alpha^{21}}.$

- $X_2 = \frac{1}{2}(-\alpha^5 - \alpha^6) = \frac{1}{\cancel{2}}(\cancel{2}\alpha^5 + \cancel{2}\alpha^6)$
$= \alpha^5 + \alpha^6$
$= \alpha^5(1+\alpha)$
$= \alpha^5 \cdot \alpha^9$
$= \boxed{\alpha^{14}}.$

VRAAG 8

Herinner de kleine stelling van Fermat die stelt dat $a^p \overset{p}{=} a$ voor p een priemgetal en a een willekeurig geheel getal. Een andere formulering van de stelling is: $a^{p-1} \overset{p}{=} 1$ (als $p \nmid a$).

(a) Gebruik makende van de kleine stelling van Fermat, toon aan dat:

- $3^{302} \bmod 5 = 4$
- $3^{302} \bmod 7 = 2$
- $3^{302} \bmod 11 = 9$

- $3^{302} \bmod 5 = \underbrace{(3^4)}_{\overset{5}{=}\, 1}{}^{75} \cdot 3^2 \bmod 5 = 3^2 \bmod 5$
  $= 9 \bmod 5 = 4.$

- $3^{302} \bmod 7 = \underbrace{(3^6)}_{\overset{7}{=}\, 1}{}^{50} \cdot 3^2 \bmod 7 = 3^2 \bmod 7$
  $= 9 \bmod 7 = 2.$

- $3^{302} \bmod 11 = \underbrace{(3^{10})}_{\overset{11}{=}\, 1}{}^{30} \cdot 3^2 \bmod 11 = 3^2 \bmod 11$
  $= 9 \bmod 11 = 9.$

(b) Gebruik nu de resultaten uit (a) en de Chinese reststelling om 3^{302} mod 385 te berekenen. Merk op dat $385 = 5 \cdot 7 \cdot 11$. Werk alles volledig uit volgens de werkwijze uit de cursus!

$$\begin{cases} x \overset{5}{=} 4 \\ x \overset{7}{=} 2 \\ x \overset{11}{=} 9 \end{cases}$$

uit (a). Zoek x. Deze x is uniek modulo 385, en zo vinden we 3^{302} mod 385.

Algemene oplossing: $x \overset{385}{=} \underbrace{a_1}_{4} \underbrace{M_1}_{77} y_1 + \underbrace{a_2}_{2} \underbrace{M_2}_{55} y_2 + \underbrace{a_3}_{9} \underbrace{M_3}_{35} y_3$

- y_1? $M_1 \cdot y_1 \overset{m_1}{=} 1 \Leftrightarrow 77 \cdot y_1 \overset{5}{=} 1 \Leftrightarrow 2 \cdot y_1 \overset{5}{=} 1$

  $\Rightarrow y_1 \overset{5}{=} 3.$

- y_2? $M_2 \cdot y_2 \overset{m_2}{=} 1 \Leftrightarrow 55 \cdot y_2 \overset{7}{=} 1 \Leftrightarrow 6 \cdot y_2 \overset{7}{=} 1$

  $\Rightarrow y_2 \overset{7}{=} 6.$

- y_3? $M_3 \cdot y_3 \overset{m_3}{=} 1 \Leftrightarrow 35 \cdot y_3 \overset{11}{=} 1 \Leftrightarrow 2 \cdot y_3 \overset{11}{=} 1$

  $\Rightarrow y_3 \overset{11}{=} 6.$

$\Rightarrow x \overset{385}{=} 4 \cdot 77 \cdot 3 + 2 \cdot 55 \cdot 6 + 9 \cdot 35 \cdot 6$

$\Rightarrow x \overset{385}{=} 9$

Antwoord: 3^{302} mod $385 = 9$.