VRAAG 1

Voor een gegeven $a \in \mathbb{Z}$ en $m \in \mathbb{N}_0$ vinden we een getal $x \in \mathbb{Z}_m$ zodat:

$$a \cdot x \overset{m}{=} 1 \overset{m}{=} x \cdot a.$$

Bewijs nu dat deze $x \in \mathbb{Z}_m$ uniek is (m.a.w. er bestaat geen andere $x \in \mathbb{Z}_m$).

Mogelijkheid 1 :

*) ongerijmde : stel dat er 2 oplossingen x_1 en x_2 bestaan, $x_1 \neq x_2$.

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

$\Rightarrow \quad a \cdot (x_1 - x_2) \overset{m}{=} 0 \quad (\dagger)$

$\Rightarrow \quad m \mid a \cdot (x_1 - x_2)$

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

dit is een contradictie gezien $0 \leq x_i < m$ voor $i \in \{1,2\}$.

*) dit is nog niet aangetoond :

ongerijmde : stel dat $ggd(a,m) \neq 1$

schrijf $ggd(a,m) = d$

en geldt : $ax = 1 + k \cdot m$, $k \in \mathbb{Z}$

$\Leftrightarrow \quad 1 = \underbrace{ax - km}_{\text{deelbaar door } d}$, $k \in \mathbb{Z}$

1: niet deelbaar door d $\Rightarrow$ contradictie.

Mogelijkheid 2 :

Start vanaf $(\dagger)$: $a \cdot (x_1 - x_2) \overset{m}{=} 0$

vermenigvuldig nu beide leden met x_1, waarvan we weten dat $a \cdot x_1 \overset{m}{=} 1$

$\Rightarrow \quad x_1 - x_2 \overset{m}{=} 0$

$\Rightarrow \quad x_1 \overset{m}{=} x_2$ ↯ contradictie.

(hier moet je dus niet aantonen dat $ggd(a,m) = 1$).

VRAAG 2

Gegeven is de relatie $f = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid y = x^3 + 3x^2 - 2\}$.
Beantwoord achtereenvolgens volgende vragen:

(a) Bereken de waarden: $f(0), f(1), f(2), f(3)$ en $f(-2), f(-3), f(-4), f(-5)$.

$f(0) = -2$ $f(-2) = 2$

$f(1) = 2$ $f(-3) = -2$

$f(2) = 18$ $f(-4) = -18$

$f(3) = 52$ $f(-5) = -52$

(b) Uit bovenstaand experiment zou je een bepaald verband moeten zijn opgevallen. We drukken dit verband nu wiskundig uit in de vorm van een predikaat. Vul aan:

$$\forall \_\_\_\_\_\_\_\_ : f(x) = \_\_\_\_\_\_\_\_$$

$\forall x \in \mathbb{Z} : f(x) = -f(-x-2)$

(bijvoorbeeld: $f(2) = -f(-4)$).

(c) Welke type redenering (deductief of inductief) gebruikte je om het verband in (b) uit te drukken? Leg uit.

Inductieve redenering:

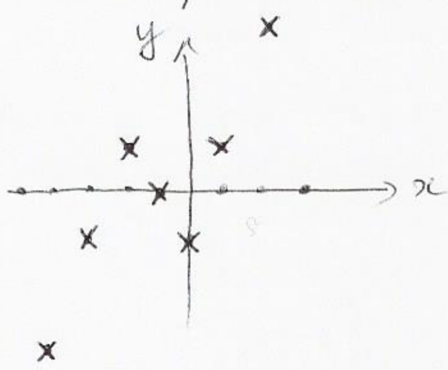
vanuit een beperkte set datapunten/metingen leiden we een algemeen geldende conclusie af.

(d) Bewijs het verband dat je vond in (b).

$$
\begin{aligned}
-f(-x-2) &= -\left(\left(-x-2\right)^3 + 3\left(-x-2\right)^2 - 2\right) \\
&= (x+2)(x^2+4x+4) - 3(x^2+4x+4) + 2 \\
&= x^3 + 2x^2 + 4x^2 + 8x + 4x + 8 - 3x^2 - 12x - 12 + 2 \\
&= x^3 + 3x^2 - 2 \\
&= f(x) \qquad \square
\end{aligned}
$$

(e) Wat is het meest specifieke type van de relatie f? Kies uit: functie, afbeelding, injectie, surjectie of bijectie. Leg uit.

We berekenen ook $f(-1) = 0$ en leggen dit samen met de datapunten uit (a):



- er vertrekt uit elke $x \in \mathbb{Z}$ één pijl.
- In $\mathbb{Z}$ komen 0, 1 of 2 pijlen toe

$\rightarrow$ f is een afbeelding

VRAAG 3

Noteer het n'de getal in de rij van Fibonacci als F_n. Er geldt:

$$F_0 = 1,$$
$$F_1 = 1,$$
$$F_n = F_{n-1} + F_{n-2} \text{ voor } n \geq 2.$$

De rij gaat dus als volgt: 1, 1, 2, 3, 5, 8, 13, 21, 45, ... Bewijs nu volgende eigenschap voor de rij van Fibonacci: voor alle $n \in \mathbb{N}$ geldt

$$1 + F_0 + F_1 + F_2 + \cdots + F_n = F_{n+2}.$$

Bewijs via inductie:

① Basisstap:

Voor $n = 0$: $1 + F_0 = 1 + 1 = F_2$ ✓

② Inductiestap:

Inductiehypothese (IH):

stel dat $\forall m \leq n : 1 + F_0 + F_1 + \dots + F_m = F_{m+2}$

~~Volgt~~

Volgt hier dan uit dat:

$1 + F_0 + F_1 + \dots + F_n + F_{n+1} = F_{n+3}$?

Bewijs: $1 + F_0 + F_1 + \dots + F_n + F_{n+1}$

$= F_{n+2} + F_{n+1}$ (wegens IH)

$= F_{n+3}$ (wegens eigenschap rij v. Fibonacci).

$\square$.

VRAAG 4

Waar of vals? Indien we een BCH-code zouden gebruiken om informatie versleuteld te versturen over een netwerk, dan is dit een voorbeeld van publieke-sleutelencryptie. Indien deze bewering waar is, geef je een bewijs of logische verklaring; indien vals, dan geef je een tegenvoorbeeld en corrigeer je indien nodig de bewering.

VALS

encodering en decodering in een BCH-code gebeurt door vermenigvuldiging met een irreducibele veelterm $h(x)$. Deze veelterm definieert het eindig veld waarin we werken.

$h(x)$ is dus onze "sleutel" mochten we deze BCH-code gebruiken als encryptiemechanisme.

$h(x)$ is geheim: wanneer iemand $h(x)$ kent /afluistert, dan kan deze persoon alle boodschappen ontcijferen.

=> dit is dus een voorbeeld van private-sleutelencryptie.

VRAAG 5

(a) Waar of vals? De periode van de pseudorandomgenerator $x_{i+1} = (\overset{a}{6}x_i + \overset{c}{81}) \bmod \overset{m}{625}$ is maximaal (en dus gelijk aan 625). Indien deze bewering waar is, geef je een bewijs of logische verklaring; indien vals, dan geef je een tegenvoorbeeld en corrigeer je indien nodig de bewering.

WAAR

Gebruik het Hull-Dobell-theorema:

- $c \neq 0$ ✓
- $ggd(c, m) = ggd(3^4, 5^4) = 1$ ✓
- $\underbrace{a-1}_{=5}$ deelbaar door $\underbrace{\text{alle priemfactoren van } m}_{=\{5\}}$? ✓
- $\underbrace{4 \mid m}_{\text{niet het geval}} \Rightarrow 4 \mid a-1$ ✓

  niet het geval, dus deze uitspraak is waar.

Alle voorwaarden vervuld $\Rightarrow$ periode is maximaal $= m = 625$.

(b) Waar of vals? Een pseudorandomgenerator met maximale periode is steeds een goede generator (dus met hoge willekeur). Indien deze bewering waar is, geef je een bewijs of logische verklaring; indien vals geef je een tegenvoorbeeld en corrigeer je indien nodig de bewering.

VALS

Tegenvoorbeeld: $x_{i+1} = (x_i + 1) \bmod m$

periode is maximaal, maar generator is absoluut niet willekeurig (telt gewoon 1 op bij het vorige getal).

VRAAG 6

Toon aan dat de uitspraak $(p \vee q) \wedge r \Rightarrow p \vee (q \wedge r)$ altijd waar is ongeacht p, q of r (met $p, q, r \in \mathbb{B}$). Werk gestructureerd en motiveer je werkwijze.

We stellen een waarheidstabel op:

p	q	r	$(p \vee q) \wedge r$ (*)	$p \vee (q \wedge r)$ (**)	(*) $\Rightarrow$ (**)
0	0	0	0	0	1
0	0	1	0	0	1
0	1	0	0	0	1
0	1	1	1	1	1
1	0	0	0	1	1
1	0	1	1	1	1
1	1	0	0	1	1
1	1	1	1	1	1

geeft altijd waarheidswaarde 'waar' ongeacht $p, q, r \in \mathbb{B}$.

Examen Discrete Wiskunde - DEEL 2

Naam en Voornaam:

VRAAG 7

Aan de kassa van het tuincentrum moet je 137 euro betalen. Je hebt slechts briefjes van 5 euro en muntjes van 2 euro op zak.

(a) Hoeveel briefjes en hoeveel muntjes moet je neertellen om het bedrag van 137 euro te vormen? Formuleer dit vraagstuk aan de hand van een diofantische vergelijking.

$$5x + 2y = 137$$

(b) Los de diofantische vergelijking uit (a) op. Geef alle tussenstappen.

- ggd $(5,2) = 1$ en $1 \mid 137 \Rightarrow$ oplosbaar.
- $5x + 2y = 137$

$\Rightarrow 5x \overset{2}{=} 137$

$\Rightarrow x \overset{2}{=} 1$

$\Rightarrow \boxed{x = 1 + 2k, \ k \in \mathbb{Z}}$

We vullen dit in (substitueren x) in de oorspr. vgl.:

$\Rightarrow 5(1+2k) + 2y = 137, \ k \in \mathbb{Z}$

$\Rightarrow 5 + 10k + 2y = 137, \ k \in \mathbb{Z}$

$\Rightarrow 2y = -10k + 132, \ k \in \mathbb{Z}$

$\Rightarrow \boxed{y = -5k + 66, \ k \in \mathbb{Z}}$

oplossing: $\begin{cases} x = 1 + 2k \\ y = 66 - 5k \end{cases} \ k \in \mathbb{Z}.$

Vervolg vraag (b).

(c) Op hoeveel verschillende manieren kan je het bedrag van 137 euro betalen? Bereken en leg uit.

De hoeveelheid muntjes dat we betalen (en de hoeveelh. briefjes) moet positief zijn:

$$\begin{cases} 1+2k \geq 0 \\ 66-5k \geq 0 \end{cases} \Leftrightarrow \begin{cases} k \geq -1/2 \\ k \leq \frac{66}{5} = 13,2 \end{cases} \quad k \in \mathbb{Z}.$$

Dus: $\underbrace{k \in \{0, 1, 2, 3, \dots, 13\}}_{}$

14 waarden voor k zijn mogelijk

dus $\underline{\underline{14}}$ manieren om te betalen.

VRAAG 8

Gegeven is de veelterm $h(x) = x^2 + x - 1$ die gebruikt wordt als voortbrengende veelterm van een eindig veld GF(9).

$\text{// } GF(3^2)$

(a) Toon aan dat $h(x)$ als voortbrengende veelterm van GF(9) irreduciebel is. Doe dit:

① Door te tonen dat $h(x)$ geen factoren van de eerste graad bevat.

② Door gebruik te maken van de Rabin test.

① check : $h(0) = -1$, $h(1) = 1$, $h(2) = 4 + 2 - 1 = 5 \equiv 2$

$GF(9) = GF(3^2)$ we werken dus in $\mathbb{Z}_3$.

$\Rightarrow$ geen nulptn $\Rightarrow$ geen factoren v/d 1ste graad

$\Rightarrow$ irreduciebel

② check : 1. $ggd(h, x^{3^1} - x) = 1$

2. h deelt $x^{3^2} - x$

1)
$$
\begin{array}{l|l}
x^3 - x & x^2+x-1 \\
\underline{-\,x^3+x^2-x} & x+2 \\
2x^2 & \\
\underline{-\,2x^2+2x-2} & \\
x+2 &
\end{array}
\qquad
\begin{array}{l|l}
x^2 + x + 1 & x+2 \\
\underline{-\,x^2+2x} & x+2 \\
2x+2 & \\
\underline{-\,2x+1} & \\
1 &
\end{array}
$$

$\Rightarrow ggd(h, x^3 - x) = 1$ ✓ (wegens algoritme v. Euclides).

2)
$$
\begin{array}{l|l}
x^9 + 2x & x^2+x+2 \\
\underline{-\,x^9+x^8+2x^7} & x^7+2x^6+2x^5+2x^3+x^2+x \\
2x^8+x^7+2x & \\
\underline{-\,2x^8+2x^7+x^6} & \\
2x^7+2x^6+2x & \\
\underline{-\,2x^7+2x^6+x^5} & \\
2x^5+2x & \\
\underline{-\,2x^5+2x^4+x^3} & \\
x^4+2x^3+2x & \\
\underline{-\,x^4+x^3+2x^2} & \\
x^3+x^2+2x & \\
\underline{-\,x^3+x^2+2x} & \\
0 &
\end{array}
$$

$\Rightarrow h$ deelt $x^9 - x$

m.a.w. alle voorwaarden van de Rabin-test zijn voldaan

$\Rightarrow h$ is irreduciebel.

Vervolg vraag (a).

(b) Stel de volledige Zech-log-tabel op voor GF(9) met $h(x)$ als voortbrengende veelterm en kies hierbij α als imaginair element. 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(9). In de 3de kolom komt $y+1$ en in de vierde kolom de macht van α die overeenkomt met $y+1$.

α^k	y	$y+1$	α^k+1
0	0	1	α^0
α^0	1	2	α^4
α^1	α	$\alpha+1$	α^7
α^2	$2\alpha+1$	$2\alpha+2$	α^3
α^3	$2\alpha+2$	2α	α^5
α^4	2	0	0
α^5	2α	$2\alpha+1$	α^2
α^6	$\alpha+2$	α	α^1
α^7	$\alpha+1$	$\alpha+2$	α^6

(c) Schrijf volgende elementen van GF(9) in de vorm α^k, $0 \leq k < 8$. Gebruik de tabel uit (b).

1. $(1+2\alpha)(2+\alpha)$

$(1+2\alpha)(2+\alpha)$ (aflezen uit tabel in (b)).

$= \alpha^2 \cdot \alpha^6$

$= \alpha^8 = \alpha^0$

2. $\alpha^2 + 2\alpha^3 + 2\alpha^5 + \alpha^7$

$\alpha^2 + 2\alpha^3 + 2\alpha^5 + \alpha^7$

$= \alpha^2 + \alpha^4\alpha^3 + \alpha^4\alpha^5 + \alpha^7$

$= \alpha^2 + \alpha^7 + \alpha^9 + \alpha^7$

$= \alpha^2 + \alpha^1 + 2\alpha^7$

$= \alpha^2 + \alpha^1 + \alpha^4\alpha^7$

$= \alpha^2 + \alpha^1 + \alpha^{11}$

$= \alpha^2 + \alpha^1 + \alpha^3$

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

$= \alpha \cdot \alpha^7 + \alpha^3$

$= \alpha^8 + \alpha^3 = \alpha^0 + \alpha^3 = 1 + \alpha^3 = \alpha^5$.

(er zijn ∞ veel verschillende manieren waarop je dit kan berekenen)

VRAAG 9

Los onderstaand stelsel van lineaire congruenties op en geef duidelijk aan in welke verzameling de gevonden oplossing uniek is. Leg je tussenstappen goed uit.

$$\begin{cases} x \overset{4}{=} 3 \\ x \overset{10}{=} 1 \end{cases}$$

• 4 en 10 zijn niet onderling priem => vgl. opsplitsen:

$$\begin{cases} x \overset{4}{=} 3 \\ x \overset{10}{=} 1 \end{cases} \Leftrightarrow \begin{cases} x \overset{4}{=} 3 & (1) \\ x \overset{2}{=} 1 & (2) \\ x \overset{5}{=} 1 & (3) \end{cases}$$

• vgl (2) is redundant t.o.v. vgl (1) → weglaten.

we lossen dus op: $\begin{cases} x \overset{4}{=} 3 \\ x \overset{5}{=} 1 \end{cases}$

• $M = 4 \cdot 5 = 20$

algemene opl: $x = a_1 M_1 y_1 + a_2 M_2 y_2 \mod M$

met $M_1 = 5 \qquad M_2 = 4$

$a_1 = 3 \qquad a_2 = 1$

• zoek y_1 als opl. van $M_1 \cdot y_1 \overset{m_1}{=} 1$

$\Leftrightarrow 5 \cdot y_1 \overset{4}{=} 1 \Leftrightarrow \boxed{y_1 \overset{4}{=} 1}$

• zoek y_2 als opl. van $M_2 \cdot y_2 \overset{m_2}{=} 1$

$\Leftrightarrow 4 \cdot y_2 \overset{5}{=} 1$

op het zicht of via Euclides:

4	5	1	0	0	1
4	1	1	0	−1	1
1	1	4	−3	−1	1

$\Rightarrow \boxed{y_2 \overset{5}{=} 4}$

• Dus: $x = 3 \cdot 5 \cdot 1 + 1 \cdot 4 \cdot 4 \mod 20$

$= 15 + 16 \mod 20 = 11 \mod 20$

x is uniek in $\{0, 1, 2, \ldots, 19\}$.