IT Fundamentals Hoofdstuk 9

Eindige Velden

Jens Buysse, Karine Van Driessche, Koen Mertens, Lieven Smits, Lotte Van Steenberghe

5 oktober 2020

HO GENT

Inhoud. I

Eindige velden
- Definities en eigenschappen
- Het eindig veld $\mathbb{Z}_p$
- Voorbeelden
- Rekenen in $\mathbb{Z}_p$
- Vergelijkingen in $\mathbb{Z}_p$
- Oefeningen

HO GENT

Eindige velden

HO
GENT

Een veld

HO
GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen.*

HO
GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

HO
GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

- F *is gesloten voor* $+$ *en* $\cdot$*:* $a + b \in F$ *en* $a \cdot b \in F$*.*

HO GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

- F *is gesloten voor* $+$ *en* $\cdot$*:* $a + b \in F$ *en* $a \cdot b \in F$*.*
- *commutatief:* $a + b = b + a$ *en* $a \cdot b = b \cdot a$*.*

HO GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

- F *is gesloten voor* $+$ *en* $\cdot$*:* $a + b \in F$ *en* $a \cdot b \in F$*.*
- *commutatief:* $a + b = b + a$ *en* $a \cdot b = b \cdot a$*.*
- *associatief:* $(a + b) + c = a + (b + c)$ *en* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*

HO GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

- F *is gesloten voor* $+$ *en* $\cdot$*:* $a + b \in F$ *en* $a \cdot b \in F$*.*
- *commutatief:* $a + b = b + a$ *en* $a \cdot b = b \cdot a$*.*
- *associatief:* $(a + b) + c = a + (b + c)$ *en* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*
- *distributief:* $a \cdot (b + c) = a \cdot b + a \cdot c$*.*

HO GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

- F *is gesloten voor* $+$ *en* $\cdot$*:* $a + b \in F$ *en* $a \cdot b \in F$*.*
- *commutatief:* $a + b = b + a$ *en* $a \cdot b = b \cdot a$*.*
- *associatief:* $(a + b) + c = a + (b + c)$ *en* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*
- *distributief:* $a \cdot (b + c) = a \cdot b + a \cdot c$*.*
- *neutraal element:* $a + 0 = a$ *en* $a \cdot 1 = a$*.*

HO GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen, 0 en 1, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

- F *is gesloten voor* $+$ *en* $\cdot$*:* $a + b \in F$ *en* $a \cdot b \in F$*.*
- *commutatief:* $a + b = b + a$ *en* $a \cdot b = b \cdot a$*.*
- *associatief:* $(a + b) + c = a + (b + c)$ *en* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*
- *distributief:* $a \cdot (b + c) = a \cdot b + a \cdot c$*.*
- *neutraal element:* $a + 0 = a$ *en* $a \cdot 1 = a$*.*
- *invers element voor* $+$*: er bestaat een element* $-a \in F$ *zodat* $a + (-a) = 0$*.*

HO GENT

Een veld

Definitie

Een veld F *is een verzameling van elementen met twee operatoren,* $+$ *en* $\cdot$*, en twee constante elementen,* 0 *en* 1*, die voldoet aan de volgende eigenschappen. Stel* $a, b, c \in F$*:*

- F *is gesloten voor* $+$ *en* $\cdot$*:* $a + b \in F$ *en* $a \cdot b \in F$*.*
- *commutatief:* $a + b = b + a$ *en* $a \cdot b = b \cdot a$*.*
- *associatief:* $(a + b) + c = a + (b + c)$ *en* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$*.*
- *distributief:* $a \cdot (b + c) = a \cdot b + a \cdot c$*.*
- *neutraal element:* $a + 0 = a$ *en* $a \cdot 1 = a$*.*
- *invers element voor* $+$*: er bestaat een element* $-a \in F$ *zodat* $a + (-a) = 0$*.*
- *invers element voor* $\cdot$*: voor elke* $a \in F$*, met* $a \neq 0$ *bestaat er een element* a^{-1} *zodat* $a \cdot a^{-1} = 1$*.*

HO GENT

Eigenschappen van een veld

HO
GENT

Eigenschappen van een veld

Eigenschap

In een willekeurig veld F is het element 0 opslorpend element voor de vermenigvuldiging:

$$a \cdot 0 = 0$$

voor alle $a \in F$.

HO GENT

Eigenschappen van een veld

Eigenschap

In een willekeurig veld F is het element 0 opslorpend element voor de vermenigvuldiging:

$$a \cdot 0 = 0$$

voor alle $a \in F$.

Eigenschap

Een veld F heeft geen nuldelers:

$$a \cdot b = 0 \quad \textit{als} \quad a = 0 \textit{ of } b = 0,$$

voor alle $a, b \in F$.

HO GENT

Een eindig veld

HO
GENT

Een eindig veld

Definitie

*Een **eindig veld** is een veld waarvoor de verzameling van elementen eindig is. Het aantal elementen van deze verzameling is de **orde** van het veld.*

HO GENT

Een eindig veld

Definitie

*Een **eindig veld** is een veld waarvoor de verzameling van elementen eindig is. Het aantal elementen van deze verzameling is de **orde** van het veld.*

Stelling

Er bestaat een veld van de orde q als en slechts als q de macht van een priemgetal p is ($q = p^h$, met $h \in \mathbb{N}$).

HO GENT

Een eindig veld

Definitie

*Een **eindig veld** is een veld waarvoor de verzameling van elementen eindig is. Het aantal elementen van deze verzameling is de **orde** van het veld.*

Stelling

Er bestaat een veld van de orde q als en slechts als q de macht van een priemgetal p is ($q = p^h$, met $h \in \mathbb{N}$).
Twee velden van de orde q met $q = p^h$ zijn isomorf.

HO GENT

Een eindig veld

Definitie

*Een **eindig veld** is een veld waarvoor de verzameling van elementen eindig is. Het aantal elementen van deze verzameling is de **orde** van het veld.*

Stelling

Er bestaat een veld van de orde q als en slechts als q de macht van een priemgetal p is ($q = p^h$, met $h \in \mathbb{N}$).
Twee velden van de orde q met $q = p^h$ zijn isomorf.

Definitie

*Een veld van de orde q noemen we een **Galois veld van de orde** q, of* GF(q).

HO GENT

De verzameling $\mathbb{Z}_m$

HO GENT

De verzameling $\mathbb{Z}_m$

Definitie

$\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$

$(m \in \mathbb{N}_0)$

HO GENT

De verzameling $\mathbb{Z}_m$

Definitie
$\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$
$(m \in \mathbb{N}_0)$

Probleem:

HO GENT

De verzameling $\mathbb{Z}_m$

Definitie
$\mathbb{Z}_m = \{0, 1, \ldots, m - 1\}$
$(m \in \mathbb{N}_0)$

Probleem:
Bestaat er een $+$ en $\cdot$ zodat $\mathbb{Z}_m, +, \cdot$ een veld is?

HO GENT

De bewerking *modulo*

HO
GENT

De bewerking *modulo*

Definitie

Stel $a, b \in \mathbb{Z}$. a ***is congruent met*** *b* ***modulo*** *m als en slechts als de deling van a en van b door m dezelfde rest oplevert.*

HO GENT

De bewerking *modulo*

Definitie

Stel $a, b \in \mathbb{Z}$. a ***is congruent met*** *b* ***modulo*** *m als en slechts als de deling van a en van b door m dezelfde rest oplevert.*

- *Notatie: $a \equiv b \,(mod\, m) \Leftrightarrow a = m.k + b$ met $m \in \mathbb{N}_0, k \in \mathbb{Z}$*
- *Dit houdt dus in dat $a mod\, m$ de positieve rest na deling is door m.*

HO GENT

De bewerking *modulo*

Definitie

Stel $a, b \in \mathbb{Z}$. a ***is congruent met*** b ***modulo*** m *als en slechts als de deling van* a *en van* b *door* m *dezelfde rest oplevert.*

- *Notatie:* $a \equiv b \,(mod\, m) \Leftrightarrow a = m.k + b$ *met* $m \in \mathbb{N}_0, k \in \mathbb{Z}$
- *Dit houdt dus in dat* $a mod\, m$ *de positieve rest na deling is door* m.

Eigenschap

Stel $a \equiv a' \,(mod\, m)$ *en* $b \equiv b' \,(mod\, m)$.

- $a + b \equiv a' + b' \,(mod\, m)$

HO GENT

De bewerking *modulo*

Definitie

Stel $a, b \in \mathbb{Z}$. a ***is congruent met*** b ***modulo*** m *als en slechts als de deling van* a *en van* b *door* m *dezelfde rest oplevert.*

- *Notatie:* $a \equiv b \,(mod\, m) \Leftrightarrow a = m.k + b$ *met* $m \in \mathbb{N}_0, k \in \mathbb{Z}$
- *Dit houdt dus in dat* $a \bmod m$ *de positieve rest na deling is door* m.

Eigenschap

Stel $a \equiv a' \,(mod\, m)$ *en* $b \equiv b' \,(mod\, m)$.

- $a + b \equiv a' + b' \,(mod\, m)$
- $a \cdot b \equiv a' \cdot b' \,(mod\, m)$

HO GENT

De structuur $\mathbb{Z}_m, +, \cdot$

HO GENT

De structuur $\mathbb{Z}_m, +, \cdot$

Definitie
Stel $a, b \in \mathbb{Z}_m$.
In $\mathbb{Z}_m$ *kunnen* $+$ *en* $\cdot$ *als volgt gedefinieerd worden*

HO GENT

De structuur $\mathbb{Z}_m, +, \cdot$

Definitie

Stel $a, b \in \mathbb{Z}_m$.

In $\mathbb{Z}_m$ *kunnen* $+$ *en* $\cdot$ *als volgt gedefinieerd worden*

- $a + b \equiv a + b \pmod{m}$

HO GENT

De structuur $\mathbb{Z}_m, +, \cdot$

Definitie

Stel $a, b \in \mathbb{Z}_m$.

In $\mathbb{Z}_m$ *kunnen* $+$ *en* $\cdot$ *als volgt gedefinieerd worden*

- $a + b \equiv a + b \pmod{m}$
- $a \cdot b \equiv a \cdot b \pmod{m}$

HO GENT

De structuur $\mathbb{Z}_m, +, \cdot$

Definitie

Stel $a, b \in \mathbb{Z}_m$.

In $\mathbb{Z}_m$ *kunnen* $+$ *en* $\cdot$ *als volgt gedefinieerd worden*

- $a + b \equiv a + b \pmod{m}$
- $a \cdot b \equiv a \cdot b \pmod{m}$

HO GENT

De structuur $\mathbb{Z}_m, +, \cdot$

Definitie

Stel $a, b \in \mathbb{Z}_m$.

In $\mathbb{Z}_m$ *kunnen* $+$ *en* $\cdot$ *als volgt gedefinieerd worden*

- $a + b \equiv a + b \pmod{m}$
- $a \cdot b \equiv a \cdot b \pmod{m}$

Stelling

De structuur $\mathbb{Z}_m, +, \cdot$ *is een veld als en slechts als* m *een priemgetal is.*

HO GENT

Het eindig veld met 2 elementen

HO
GENT

Het eindig veld met 2 elementen

$GF(2) = \mathbb{Z}_2 = \{0, 1\}$ met

HO GENT

Het eindig veld met 2 elementen

$GF(2) = \mathbb{Z}_2 = \{0, 1\}$ met

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

HO GENT

Het eindig veld met 3 elementen

HO
GENT

Het eindig veld met 3 elementen

$GF(3) = \mathbb{Z}_3 = \{0, 1, 2\}$ met

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

HO GENT

Het eindig veld met 4 elementen

HO
GENT

Het eindig veld met 4 elementen

$\mathrm{GF}(4) = \{0, 1, a, b\}$ met

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

HO GENT

Het eindig veld met 5 elementen

HO
GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0

HO GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1

HO GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2

HO GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

HO GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4

HO GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3

HO GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2

HO GENT

Het eindig veld met 5 elementen

$GF(5) = \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

HO GENT

De verzameling $\mathbb{Z}_6$

HO GENT

De verzameling $\mathbb{Z}_6$

Er is geen eindig veld met 6 elementen.

HO GENT

Het eindig veld met 11 elementen

HO
GENT

Het eindig veld met 11 elementen

$GF(11) = \mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

HO GENT

Het eindig veld met 11 elementen

GF(11) = $\mathbb{Z}_{11}$ = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10}.
met

a	$-a$
0	0
1	10
2	9
3	8
4	7
5	6
6	5
7	4
8	3
9	2
10	1

a	a^{-1}
0	/
1	1
2	6
3	4
4	3
5	9
6	2
7	8
8	7
9	5
10	10

HO GENT

Rekenen in $\mathbb{Z}_p$ I

- $3 \mod 5$:
  - De berekening gebeurt in $\mathbb{Z}_5$. Dit houdt in dat het resultaat enkel een element kan zijn van $\mathbb{Z}_5$ of dus van $\{0, 1, 2, 3, 4\}$.
  - $3 \mod 5$ = de rest na gehele deling door 5. Bijgevolg is $3 \mod 5 = 3$
- $23 \mod 7$:
  - De berekening gebeurt in $\mathbb{Z}_7$. Dit houdt in dat het resultaat enkel een element kan zijn van $\mathbb{Z}_7$ of dus van $\{0, 1, 2, 3, 4, 5, 6\}$.
  - $23 \mod 7$ = de rest na gehele deling door 7. Bijgevolg is $23 \mod 7 = 2$

HO GENT

Rekenen in $\mathbb{Z}_p$ II

- $-7 \mod 5$:
  - De berekening gebeurt in $\mathbb{Z}_5$. Dit houdt in dat het resultaat enkel een element kan zijn van $\mathbb{Z}_5$ of dus van $\{0, 1, 2, 3, 4\}$, dus de oplossing kan **geen** negatief getal zijn.
  - Tel bij -7 een veelvoud op van 5 zodat het resultaat positief wordt en in $\mathbb{Z}_5$ ligt $-7 + 2 \times 5 = 3 \Rightarrow -7 \mod 5 \equiv 3 \mod 5 of -7 \mod 5 = 3$:
- $-8 \mod 3$
  - De berekening gebeurt in $\mathbb{Z}_3$. Dit houdt in dat het resultaat enkel een element kan zijn van $\mathbb{Z}_5$ of dus van $\{0, 1, 2\}$.
  - Tel bij -8 een veelvoud op van 3 zodat het resultaat positief wordt en in $\mathbb{Z}_3$ ligt $-8 + 3 \times 3 = 1 \Rightarrow -8 \mod 3 \equiv 1 \mod 3 of -8 \mod 3 = 1$:

HO GENT

Rekenen in $\mathbb{Z}_p$ III

- $3 \times 2^{-1} \mod 5$
  - Berekening gebeurt in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$
  - 2^{-1} in $\mathbb{Z}_5 = 3$:
    - Het inverse van een element a uit een eindige verzameling $\mathbb{Z}_p$ vind je door een getal uit $\mathbb{Z}_p$ te nemen b zodat $a \times b \mod p = 1$. Dan is $a^{-1} = b$
    - Om $2^{-1} in \mathbb{Z}_5$ te bepalen zoeken we dus naar een getal x in $\mathbb{Z}_5$, zodat $2 \times x \mod 5 = 1 \rightarrow x = 3$ of dus $2^{-1} = 3$
  - $3 \times 2^{-1} \mod 5 \equiv 3 \times 3 \mod 5 = 4$

HO GENT

Rekenen in $\mathbb{Z}_p$ IV

- $(117 \times 6^{-1} + 1004) \mod 7$
  - Bepaal voor alle getallen eerst de rest na deling door 7:
    - $117 = 16 \times 7 + 5 \rightarrow$ rest is 5
    - $1004 = 143 \times 7 + 3 \rightarrow$ rest is 3
  - Herschrijf $(117 \times 6^{-1} + 1004) \mod 7 \equiv (5 \times 6^{-1} + 3) \mod 7$
  - Bepaal 6^{-1} in $\mathbb{Z}_7 \rightarrow 6^{-1} = 6$
  - Herschrijf $(5 \times 6^{-1} + 3) \mod 7 \equiv (5 \times 6 + 3) \mod 7 \equiv 33 \mod 7 \equiv 5 \mod 7 = 5$

HO GENT

Vergelijkingen in $\mathbb{Z}_p$ I

Los volgende vergelijking op naar x:

1. In $\mathbb{Z}_{17}$: $x + 5 \equiv 35$
   - $(x + 5 \equiv 35) \mod 17 \rightarrow x$ moet een element zijn van $\mathbb{Z}_{17}$
   - Deel eerst alle veelvouden van 17 weg: $(x + 5 \equiv 1) \mod 17$
   - $(x + 5 \equiv 1) \mod 17 \Leftrightarrow (x \equiv -4) \mod 17 \Leftrightarrow (x \equiv -4 + 17) \mod 17 \Leftrightarrow (x \equiv 13) \mod 17$ of dus $x = 13$
   - **Controle**: $(13 + 5 \equiv 35) \mod 17 \Leftrightarrow (18 \equiv 35) \mod 17 \Leftrightarrow (1 \equiv 1) \mod 17$

HO GENT

Vergelijkingen in $\mathbb{Z}_p$ II

2. In $\mathbb{Z}_5$: $23x + 13 \equiv 0 \mod 5$
   - $23x + 13 \equiv 0 \mod 5 \rightarrow x$ moet een element zijn van $\mathbb{Z}_5$
   - Deel eerst alle veelvouden van 5 weg: $(3x + 3 \equiv 0) \mod 5 (3x + 3 \equiv 0) \mod 5 \rightarrow (3x \equiv -3) \mod 5 \rightarrow (3x \equiv -3 + 5) \mod 5 \rightarrow (3x \equiv 2) \mod 5$
   - Om de factor 3 voor de x weg te werken, vermenigvuldigen we beide leden met 3^1 **(let op dit is 3^{-1} uit $\mathbb{Z}_5$ en niet $\frac{1}{3}$ uit $\mathbb{R}$!)** : $(3x \equiv 2) \mod 5 \rightarrow (3^{-1} \times 3x \equiv 3^{-1} \times 2) \mod 5 \rightarrow (1 \times x \equiv 3^{-1} \times 2) \mod 5 \rightarrow (x \equiv 3^{-1} \times 2) \mod 5$
   - Bepaal 3^{-1} in $\mathbb{Z}_5 \rightarrow 3^{-1} = 2$
   - Herschrijf $(x \equiv 3^{-1} \times 2) \mod 5 \rightarrow (x \equiv 2 \times 2) \mod 5 \rightarrow (x \equiv 4) \mod 5$ of $x = 4$
   - **Controle**: $(23 \times 4 + 13 \equiv 0) \mod 5 \rightarrow (105 \equiv 0) \mod 5 \rightarrow (0 \equiv 0) \mod 5$

HO GENT

Oefening 1

1 Noteer alle inverse elementen voor de optelling en de vermenigvuldiging in:

HO GENT

Oefening 1

1 Noteer alle inverse elementen voor de optelling en de vermenigvuldiging in:
   a) $\mathbb{Z}_7$

HO GENT

Oefening 1

1 Noteer alle inverse elementen voor de optelling en de vermenigvuldiging in:
   a) $\mathbb{Z}_7$
   b) $\mathbb{Z}_{13}$

HO GENT

Oefening 1

1 Noteer alle inverse elementen voor de optelling en de vermenigvuldiging in:

a) $\mathbb{Z}_7$
b) $\mathbb{Z}_{13}$
c) $\mathbb{Z}_{17}$

HO GENT

Oefening 2

- Bereken in $\mathbb{Z}_7$
  - $3 \times 4 + 6 \equiv \ldots$
  - $2^{-1} \equiv \ldots$
  - $-5 \equiv \ldots$
- Bereken in Z_{11}
  - $5 \times 3 + 5 \equiv \ldots$
  - $-4 \equiv \ldots$
  - $8^{-1} \equiv \ldots$
- Bereken in Z_5
  - $8002 \times 333 \equiv$
  - $24 \times a = 108 \equiv \ldots$
- Bepaal $(122 \times a + 34) \mod 9$

HO GENT

Oefening 3

1. Los op in $\mathbb{Z}_5$:
   - 1.1 $2x + 2 \equiv 5$
   - 1.2 $4x \equiv 1$
   - 1.3 $-14 + x \equiv 0$
2. Los op in $\mathbb{Z}_{11}$:
   - 2.1 $4 + x \equiv 0$
   - 2.2 $3x + 5 \equiv 0$
   - 2.3 $4x + 6 \equiv 0$
3. Los op in $\mathbb{Z}_{17}$:
   - 3.1 $3x \equiv 1$

HO GENT

Oefening 4

Is $\mathbb{Z}_8, +, .$ een veld? Motiveer je antwoord.

- Bestaat er een eindig veld met 8 elementen?

HO GENT

Oefening 5 I

1. Vul aan: $129 \mod 29 \equiv \ldots$
2. Bepaal de inverse van $3 \in \mathbb{Z}_{29}$, ofte indien $3 \times x \mod 29 \equiv 1$ dan is $x \equiv \ldots$.
3. $494 \times 129 \mod 29 \equiv \ldots$

HO GENT

Oefening 5 II

4. Laat de 26 letters van het alfabet respectievelijk overeen komen met de getallen 0 tot en met 25 . Dit wil zeggen:
   - $A \rightarrow 0$
   - $B \rightarrow 1$
   - ...
   - $Y \rightarrow 24$
   - $Z \rightarrow 25$

   Voorts definiëren we het volgende:
   - leesteken punt :. → 26
   - leesteken komma :., → 27
   - leesteken uitroepteken :.! → 28

HO GENT

Oefening 5 III

Ontcijfer dan volgend bericht waar alle getallen modulo 29 dienen beschouwd te worden:

$$\begin{bmatrix} 36 & 72 & -81 & 4 & -132 & 19 & 28 \end{bmatrix}$$

Er staat : ...

HO GENT