TENTAMEN GROEPENTHEORIE
21 JUNI 2012, 9.00–12.00 UUR

De onderstaande 7 opgaven zijn elk 5 punten waard. Daarbij krijg je 5 punten kado, zodat er in totaal 40 punten te behalen zijn.

(1) Deze opgave gaat over de vermenigvuldiggroepen $(\mathbb{Z}/51\mathbb{Z})^*$ en $(\mathbb{Z}/80\mathbb{Z})^*$.
  (a) [2 punten]. Laat zien dat deze groepen evenveel elementen hebben.
  (b) [3 punten]. Laat zien dat deze groepen niet isomorf zijn.

(2) In $\mathrm{SL}_2(\mathbb{Z})$ (dat is de groep van 2×2 matrices met gehele coëfficiënten en determinant 1) definiëren we

$$H := \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \ : \ n \in \mathbb{Z} \right\}.$$

  (a) [2 punten]. Toon aan dat H een ondergroep is van $\mathrm{SL}_2(\mathbb{Z})$.
  (b) [3 punten]. Bepaal de index $[\mathrm{SL}_2(\mathbb{Z}) : H]$ (Hint: Onder welke voorwaarde op $a, b \in \mathbb{Z}$ geldt $\left(\begin{smallmatrix} 1 & 0 \\ a & 1 \end{smallmatrix}\right)H = \left(\begin{smallmatrix} 1 & 0 \\ b & 1 \end{smallmatrix}\right)H$?).

(3) [5 punten]. Gegeven $\tau = (1\ 2\ 3)(2\ 3\ 4)(5\ 6\ 7)(7\ 8\ 9) \in S_9$ en $n = 2106^{2013} \in \mathbb{Z}$. Bereken τ^n.

(4) Laat $n \geq 3$, en nummer de hoekpunten van een regelmatige n-hoek als $1, 2, 3, \cdots, n$. Omdat elk element van de groep D_n een permutatie van deze hoekpunten levert, krijgen we zo een afbeelding $D_n \longrightarrow S_n$.
  Bewijs dat het beeld van deze afbeelding in A_n ligt, dan en slechts dan als $n \equiv 1 \bmod 4$.
  (Hint: kijk eerst ([2 punten]) welke permutatie er hoort bij een rotatie over $2\pi/n$; onder welke voorwaarde zit die permutatie in A_n? Kijk vervolgens hoe het zit met een spiegeling ([3 punten]).)

(5) [5 punten] Neem een priemgetal p en een groep G bestaande uit precies p^n elementen (voor zeker geheel getal $n \geq 1$). Laat zien dat het centrum van G uit tenminste p elementen bestaat.

(6) Gegeven een geheel getal $n \geq 2$. We duiden met G de groep aan, bestaande uit alle bijecties: $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ gegeven door een formule $f(x) = ax+b$, waarbij a de groep $(\mathbb{Z}/n\mathbb{Z})^*$ doorloopt en b de groep $\mathbb{Z}/n\mathbb{Z}$.
  Verder bestaat $N \subset G$ uit de bijecties f die voldoen aan

$$f(1 \bmod n) - f(0 \bmod n) = 1 \bmod n.$$

  (a) [2 punten].Toon aan dat N een normaaldeler in G is.
  (b) [3 punten]. Toon aan dat $G/N \cong (\mathbb{Z}/n\mathbb{Z})^*$.

(7) Gegeven is de ondergroep

$$H := \mathbb{Z} \cdot (2, 5, 5) + \mathbb{Z}(6, 6, 6) \subset \mathbb{Z}^3.$$

  (a) [3 punten]. Wat is de orde van $(1, 0, 0) + H \in \mathbb{Z}^3/H$?
  (b) [2 punten]. Wat is de orde van $(0, 0, 1) + H \in \mathbb{Z}^3/H$?

1 a). $\#(\mathbb{Z}/51\mathbb{Z})^* = \varphi(51) = \varphi(17)\cdot\varphi(3) = 16\cdot 2 = 32$

$\#(\mathbb{Z}/80\mathbb{Z})^* = \varphi(80) = \varphi(2^4\cdot 5) = \varphi(2^4)\cdot\varphi(5) = 2^3\cdot 4 = 32$.

En dus volgt $\#(\mathbb{Z}/51\mathbb{Z})^* = \#(\mathbb{Z}/80\mathbb{Z})^*$. □

b). voor $(\mathbb{Z}/80\mathbb{Z})^*$ geldt met behulp van de Chinese reststelling:

$(\mathbb{Z}/80\mathbb{Z})^* \cong (\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$, dus i.h.b. hebben de twee groepen evenveel elementen van een bepaalde orde. $\#(\mathbb{Z}/16\mathbb{Z})^* = 8$ en $\#(\mathbb{Z}/5\mathbb{Z})^* = 4$.

voor een $\bar{a} \in (\mathbb{Z}/16\mathbb{Z})^*$ geldt dus $\mathrm{ord}(\bar{a}) \mid 8$ en voor een $\bar{b} \in (\mathbb{Z}/5\mathbb{Z})^*$ geldt $\mathrm{ord}(\bar{b}) \mid 4 \mid 8$

Dus ~~kan~~ geldt ook $\mathrm{kgv}(\mathrm{ord}(\bar{a}), \mathrm{ord}(\bar{b})) \mid 8$, en dit is precies de orde van ~~de~~ $(\bar{a}, \bar{b}) \in (\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$. ~~We concluderen dat alle voorkomende ordes in de groep $(\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$ een machten zijn van 2, dus ook in $(\mathbb{Z}/80\mathbb{Z})^*$ komen alleen machten van 2 voor als orde, maar~~ . Dus in de groep $(\mathbb{Z}/16\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$ komen alleen ordes voor kleiner of gelijk aan 8, en dus geldt dit ook voor $(\mathbb{Z}/80\mathbb{Z})^*$.

~~Maar voor $(\mathbb{Z}/51\mathbb{Z})^*$ geldt mbv Chinese reststelling dat $(\mathbb{Z}/51\mathbb{Z})^* \cong (\mathbb{Z}/17\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$~~

Echter voor $(\mathbb{Z}/51\mathbb{Z})^*$ geldt mbv Chinese reststelling dat

$(\mathbb{Z}/51\mathbb{Z})^* \cong (\mathbb{Z}/17\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$.

$\#(\mathbb{Z}/17\mathbb{Z})^* = 16$. Dus voor $\bar{a} \in (\mathbb{Z}/17\mathbb{Z})^*$ geldt $\mathrm{ord}(\bar{a}) \mid 16 \Rightarrow \mathrm{ord}(\bar{a}) = 2^k$ voor een ~~zekere~~ $k \in \mathbb{Z}_{\geq 0}$.

Er geldt $\mathrm{ord}(\bar{3}) = 16$. ~~immers~~ in $(\mathbb{Z}/17\mathbb{Z})^*$, immers.

$\bar{3}^1 = \bar{3} \neq \bar{1}$, $\bar{3}^2 = \bar{9} \neq \bar{1}$, $\bar{3}^4 = \overline{81} = \overline{4\cdot 17 + 13} = \overline{13} \neq \bar{1}$, $\bar{3}^8 = \overline{13}^2 = \overline{-4}^2 = \overline{16} = \overline{-1} \neq \bar{1}$ en

dus $\bar{3}^{16} = \overline{-1}^2 = \bar{1}$. $\Rightarrow \mathrm{ord}(\bar{3}) = 16$ in $(\mathbb{Z}/17\mathbb{Z})^*$.

Dan heeft $(\bar{3}, \bar{1})$ ~~ook~~ ook orde 16 in $(\mathbb{Z}/17\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$, want

$\mathrm{ord}(\bar{3}, \bar{1}) = \mathrm{kgv}(\mathrm{ord}(\bar{3}), \mathrm{ord}(\bar{1})) = \mathrm{kgv}(16, 1) = 16$.

Dus $(\mathbb{Z}/17\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^*$ bevat een element van orde 16, en dus $(\mathbb{Z}/51\mathbb{Z})^*$ ook, maar $(\mathbb{Z}/80\mathbb{Z})^*$ niet

dus de groepen zijn niet isomorf. □

2 $H \leq SL_2(\mathbb{Z})$ gegeven door $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$.

a) i) Duidelijk is dat $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$. ii) Als $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \in H$, dan

$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix} \in H$, en iii) als $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in H$, dan $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$.

Dus H is een ondergroep ~~van~~ van $SL_2(\mathbb{Z})$. □

b) voor $a,b \in \mathbb{Z}$ geldt ~~$\begin{pmatrix}1&0\\a&1\end{pmatrix}\begin{pmatrix}1&0\\b&1\end{pmatrix}H$~~

$$\begin{pmatrix}1&0\\a&1\end{pmatrix}H = \begin{pmatrix}1&0\\b&1\end{pmatrix}H \iff \begin{pmatrix}1&0\\a&1\end{pmatrix}^{-1}\begin{pmatrix}1&0\\b&1\end{pmatrix} \in H$$

maar $\begin{pmatrix}1&0\\a&1\end{pmatrix}^{-1}\begin{pmatrix}1&0\\b&1\end{pmatrix} = \begin{pmatrix}1&0\\-a&1\end{pmatrix}\begin{pmatrix}1&0\\b&1\end{pmatrix} = \begin{pmatrix}1&0\\b-a&1\end{pmatrix}$

dus $\begin{pmatrix}1&0\\a&1\end{pmatrix}^{-1}\begin{pmatrix}1&0\\b&1\end{pmatrix} \in H \iff b-a=0 \iff a=b.$

merkop dat $\begin{pmatrix}1&0\\a&1\end{pmatrix} \in SL_2(\mathbb{Z})$ $\forall a \in \mathbb{Z}$

Dus als $a \neq b$, dan zijn $\begin{pmatrix}1&0\\a&1\end{pmatrix}H$ en $\begin{pmatrix}1&0\\b&1\end{pmatrix}H$ ~~verschillen~~ niet gelijk en dus disjunct. Dan zijn er dus oneindig veel, ~~on~~disjuncte nevenklassen ~~$\begin{pmatrix}1&0\\a&1\end{pmatrix}H$~~ gH voor $g \in SL_2(\mathbb{Z})$,

want neem hier. $\left\{\begin{pmatrix}1&0\\a&1\end{pmatrix}H : a \in \mathbb{Z}\right\}$. voor elke $a \in \mathbb{Z}$ is dit een andere nevenklasse, d.w.z. elke 2 elementen van de verzameling zijn onderling verschillend

$\Rightarrow [SL_2(\mathbb{Z}) : H] = \infty$. □

3. 5 $\tau = (1\,2\,3)(2\,3\,4)(5\,6\,7)(7\,8\,9) = (1\,2)(3\,4)(5\,6\,7\,8\,9)$, dit is een product van disjuncte cykels, en dus $\mathrm{ord}(\tau) = \mathrm{kgv}(\mathrm{ord}((1\,2)), \mathrm{ord}((3\,4)), \mathrm{ord}((5\,6\,7\,8\,9))) = \mathrm{kgv}(2,2,5) = 10$.

we bekijken 2106^{2013} modulo 10, dus $\bar{n} = n \bmod 10$ voor $n \in \mathbb{Z}$,

$\overline{2106^{2013}} = \overline{2106}^{2013} = \bar{6}^{2013} = \bar{6}$, immers, $\bar{6}^2 = \overline{36} = \bar{6}$, dus mbv inductie volgt $\bar{6}^n = \bar{6}$ $\forall n \in \mathbb{N}$.

$\Rightarrow 2106^{2013} = 6 + 10k$ voor een $k \in \mathbb{Z}$. Dus $\tau^n = \tau^{6+10k} = \tau^6 (\tau^{10})^k = \tau^6 \circ (id)^k = \tau^6$.

$\tau^2 = (5\,7\,9\,6\,8)$, $\tau^6 = (\tau^2)^3 = (5\,7\,9\,6\,8)^3 = (5\,6\,7\,8\,9)$.

$\Rightarrow \tau^n = (5\,6\,7\,8\,9)$ met $n = 2106^{2013}$. □

5. G groep met $\#G = p^n$ voor p priem en $n \in \mathbb{N}$.

5 $Z(G)$ is een ondergroep van G en dus geldt $\#Z(G) \mid \#G = p^n$ volgens Lagrange.

$\Rightarrow \#Z(G) = p^k$ voor een $k \in \{0,1,\dots,n\}$.

Als $k \geq 1$, dan $\#Z(G) = p^k \geq p$. ~~dus dan zijn we klaar.~~ ~~Het~~ ~~Test~~ dus dan klaar.

Dus we hoeven alleen maar $k=0$ uit te sluiten. Dus neem aan dat $k=0$, dan is dus $Z(G) = \{e\}$, dus alleen het eenheidselement commuteert met alles in G, dus $\forall g \in G \setminus \{e\}$ geldt $\exists h \in G$ zodat $hg \neq gh$. (want als zo'n h niet zou bestaan dan zou $g \in Z(G)$)

$\Rightarrow$ ~~$g \neq h$~~ $g \neq hgh^{-1} = \gamma_h(g) \Rightarrow g, hgh^{-1} \in C_g$. dus omdat $g \neq hgh^{-1}$, geldt dan $\#C_g \geq 2$. # van een conjugatieklasse moet ook een deler zijn van het aantal elementen van de groep.

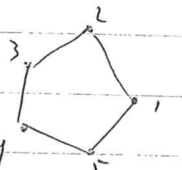
4 $n \geq 3$. $\varphi : D_n \to S_n$ door de hoekpunten te nummeren en φ stuurt dan de elementen van D_n naar de ~~[illegible]~~ cykels die de permutaties op die getallen van de hoekpunten verstellen.

We vragen ons af wanneer $\varphi(D_n) \subseteq A_n$. omdat φ een homomorfisme is, hoeven we alleen te weten wanneer ~~[illegible]~~ $\varphi(\rho)$ en $\varphi(\sigma) \in A_n$, want D_n wordt voortgebracht door σ en ρ. (immers een $x \in D_n$ is te schrijven als $\sigma^k \rho^m$ voor $k \in \{0,1\}$ en $m \in \{0,\dots,n-1\}$, dus dan geldt

$$\varphi(x) = \varphi(\sigma^k \rho^m) = (\varphi(\sigma))^k (\varphi(\rho))^m \in A_n \overset{\text{als}}{\Leftarrow} \varphi(\sigma), \varphi(\rho) \in A_n.)$$

(**)

~~we weten dat~~ $\cancel{\varphi(\rho) = (1\,2 \cdots n) \in A_n \Leftrightarrow n \equiv 1 \bmod 2}$.



Stel $n \equiv 1 \bmod 4$.
Dan is i.h.b. n oneven, dus $\varphi(\rho) = (1\,2 \cdots n) \in A_n$. want $\varepsilon((1\,2\,3 \cdots n)) = (-1)^{n-1} = 1$ want n oneven
schrijf $n = 1+2k$, voor $k \in \mathbb{Z}$. omdat $n \equiv 1 \bmod 4$ is dan k even.
Er geldt $\varphi(\sigma) = (2\ \ 2k+1)(3\ \ 2k)\cdots(k+1\ \ k+2)$, dit is een product van k 2-cykels en omdat k even is volgt dat $\varphi(\sigma)$ een product van een even aantal 2-cykels is, en dus $\varphi(\sigma) \in A_n$.
Dan volgt nu m.b.v. (**) dat $\varphi(D_n) \subseteq A_n$, omgekeerd, ~~stel~~ dat

Stel dat $\varphi(D_n) \subseteq A_n$, dan moet i.h.b. $\varphi(\rho) = (1\,2 \cdots n) \in A_n \Rightarrow n \equiv 1 \bmod 2$.
Dus $n = 1+2k$ voor een $k \in \mathbb{Z}$. ook geldt $\varphi(\sigma) = (2\ \ 2k+1)(3\ \ 2k)\cdots(k+1\ \ k+2)$ $\in A_n$, en dus moet dit een product zijn van een even aantal 2-cykels $\Rightarrow k$ even.
$\Rightarrow k = 2m$ voor een $m \in \mathbb{Z} \Rightarrow n = 1+4m \Rightarrow n \equiv 1 \bmod 4$. □

$5n + 6m = 5(1-3m) + 6m = 5 - 9m \neq 0 \ \forall m \in \mathbb{Z}$! dus ↯. $\mathrm{ord}(x) \neq 2$.

De orde kan ook niet 9 zijn want dan zou $(9,0,0) \in H$, maar de eerste coëfficiënt moet even zijn. ↯.

~~De orde~~ is verder geldt ~~$(n,0,0) \in H$~~ $18((1,0,0)+H) = (18,0,0) + H = H$

want $(18,0,0) \in H$, immers, ~~$(18,0,0) = 3\cdot(2,5,5) + 3\cdot(6,6,6)$~~

$(18,0,0) = -6\cdot(2,5,5) + 5\cdot(6,6,6)$.

Alle mogelijkheden voor $\mathrm{ord}(x) < 18$ waren al weggestreept. Dus $\mathrm{ord}(x) = 18$. □

b) $\forall n \in \mathbb{N}$ geldt $n((0,0,1)+H) = (0,0,n) \neq H$ ~~want~~ $\neq H$ want $(0,0,n) \notin H$, immers, voor alle elementen in H zijn ~~komen~~ de tweede en derde coördinaat ~~het~~ gelijk ~~overeen~~, en dat is niet zo bij $(0,0,n)$, want $n \geq 1$. Dus

5

$\mathrm{ord}((0,0,1)+H) = \infty$ in $\mathbb{Z}^3/H$. □

6. G groep van bijecties $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ gegeven door $f(\bar{x}) = \bar{a}\cdot\bar{x} + \bar{b}$, voor zekere $a \in (\mathbb{Z}/n\mathbb{Z})^*$ en $b \in \mathbb{Z}/n\mathbb{Z}$.

5

$N = \{ f \in G \mid f(1 \bmod n) - f(0 \bmod n) = 1 \bmod n \}$

a) als $f \in G$, dan $f(\bar{x}) = \bar{a}\cdot\bar{x} + \bar{b}$ voor $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ en $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$.

$\Rightarrow f(1 \bmod n) - f(0 \bmod n) = \bar{a}\cdot\bar{1} + \bar{b} - (\bar{a}\cdot\bar{0} + \bar{b}) = \bar{a} + \bar{b} - \bar{b} = \bar{a}$

dus $N = \{ f \in G \mid \bar{a} = \bar{1}$, (met $\bar{a}$ de $\bar{a}$ van $f(\bar{x}) = \bar{a}\bar{x} + \bar{b}$) $\}$ (*)

8

Laat $\varphi: G \to (\mathbb{Z}/n\mathbb{Z})^*$ gegeven door $f \mapsto \bar{a}$, waarbij $\bar{a}$ zodat $f(\bar{x}) = \bar{a}\bar{x} + \bar{b}$ $\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z}$. Dan is φ een homomorfisme, immers, als $f, g \in G$. ~~en $\bar{a}$ en $\bar{c}$ zijn zodat dat $\varphi(f) = \bar{a}$ en $\varphi(g) = \bar{c}$~~ Schrijf $f(\bar{x}) = \bar{a}\bar{x} + \bar{b}$ en $g(\bar{x}) = \bar{c}\bar{x} + \bar{d}$.

dan $(f \circ g)(\bar{x}) = f(g(\bar{x})) = \bar{a}(\bar{c}\bar{x} + \bar{d}) + \bar{b} = \bar{a}\cdot\bar{c}\cdot\bar{x} + \bar{a}\cdot\bar{d} + \bar{b}$, dus

$\varphi(f \circ g) = \bar{a}\cdot\bar{c} = \cancel{\varphi(f)\cdot\varphi(g)}\ \varphi(f)\varphi(g)$

Ook is φ duidelijk surjectief, want als $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ willekeurig, dan heeft bijv. $f \in G$, gegeven door $f(\bar{x}) = \bar{a}\bar{x}$ de eigenschap dat $\varphi(f) = \bar{a}$.

en m.b.v. (*) zien we dat $\ker(\varphi) = \{ f \in G \mid \bar{a} = \bar{1} \} = N$.

Dus N is de kern van een homomorfisme en dus een normaaldeler.

8

b) φ is een surjectief homomorfisme van G naar $(\mathbb{Z}/n\mathbb{Z})^*$ met als kern precies N. Dus:

$G/N \cong (\mathbb{Z}/n\mathbb{Z})^*$. □

Dus $\#C_g = p^m$ voor een $m \geq 1$ ~~(want kan dus niet want dan zou $\#C_g$ ...)~~

De groep G is te schrijven als een disjuncte vereniging van conjugatieklassen, dus i.h.b. is $\#G$ gelijk aan de som van ~~elke~~ ~~elementen~~ aantal elementen van die conjugatieklassen. Voor $g \in G \setminus \{e\}$ geldt $\#C_g = p^m$ voor een $m \geq 1$, dus $\#C_g \mid p$, en dus de som van al die ~~alle conjugatieklassen niet~~ $\#C_g$ ~~van conjugatieklassen~~ deelt nog steeds p.

Het eenheidselement vormt op zichzelf een conjugatieklasse, dus volgt dat $\#G$ de som is van 1 met allemaal getallen deelbaar door p. dus $\#G = 1 + kp$ voor een zekere $k \in \mathbb{Z}$. $\Rightarrow p^n = 1 + kp$. maar als we deze gelijkheid modulo p bekijken staat er $\bar{0} = \overline{p^n} = \overline{1+kp} = \bar{1}$, hetgeen een tegenspraak is.

$\Rightarrow \#Z(G) \neq 1 \Rightarrow \#Z(G) = p^k$ voor $k \geq 1 \Rightarrow \#Z(G) \geq p$. $\square$

7. Laat $H = \mathbb{Z}\cdot(2,5,5) + \mathbb{Z}(6,6,6) \subseteq \mathbb{Z}^3$.

We gaan vegen:
$$\begin{pmatrix} 2 & 6 \\ 5 & 6 \\ 5 & 6 \end{pmatrix} \sim \begin{pmatrix} 2 & 6 \\ 1 & -6 \\ 1 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & -6 \\ 2 & 6 \\ 1 & -6 \end{pmatrix} \sim \begin{pmatrix} 1 & -6 \\ 0 & 18 \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 0 & 18 \\ 0 & 0 \end{pmatrix}$$

~~Eerst~~ Dus de elementaire delers van $\mathbb{Z}^3/H$ zijn $d_1 = 18$, $d_2 = 1$. rang $= 3 - 2 = 1$.

$\Rightarrow \mathbb{Z}^3/H \cong \mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. (maal $\mathbb{Z}/1\mathbb{Z}$ maar die is $\{\bar{0}\}$ dus die laten we weg).

~~$\mathbb{Z}$~~ $\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ bevat elementen van oneindige orde (namelijk alles met eerste coördinaat ongelijk nul). als ~~ek~~ $(a, b \bmod 18) \in \mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ eindige orde heeft dan moet $a = 0$, en dan is dus
$\mathrm{ord}(a, b \bmod 18) = \mathrm{kgv}(\mathrm{ord}(a), \mathrm{ord}(b \bmod 18)) = \mathrm{kgv}(1, \mathrm{ord}(b \bmod 18)) = \mathrm{ord}(b \bmod 18) \mid 18$.
Dus de mogelijke ~~niet~~ eindige ordes zijn $1, 2, 9$ en 18.
Dus in $\mathbb{Z}^3/H$ zitten alleen maar elementen met oneindige orde, of met orde $1, 2, 9$ of 18.

a) ~~Als $\mathrm{ord}(x) = 1$, met~~ Laat $x = (1,0,0) + H = \overline{(1,0,0)} \in \mathbb{Z}^3/H$.
~~Als $\mathrm{ord}((1,0,0))$~~ Als $\mathrm{ord}(x) = 1$, dan zou $(1,0,0) + H = H \Rightarrow (1,0,0) \in H$, echter dat is niet zo, want elke element van H heeft als eerste coëfficiënt een even getal. ~~Dus~~ ↯. $\mathrm{ord}(x) \neq 1$.
Als $\mathrm{ord}(x) = 2$, dan ~~de~~ zou ~~(2,0,0)~~ $2((1,0,0) + H) = (2,0,0) + H = H \Rightarrow (2,0,0) \in H$
maar als $(2,0,0) \in H$, dan $(2,0,0) = n\cdot(2,5,5) + m\cdot(6,6,6)$ voor zekere $n, m \in \mathbb{Z}$.
$= (2n+6m, 5n+6m, 5n+6m)$. Dan zou $2n + 6m = 2 \Rightarrow n = 1 - 3m$, en $5n + 6m = 0$, echter dit geeft