

Opgelet. Er is een apart multiple-choice gedeelte op de laatste bladzijde. Schrijf op dat blad je naam en lever het mee in met je overige tentamenkopij!

1. Rekenen modulo m

(a) Algemene kennis.

(i) Wat bedoelt men met " x is congruent modulo m met y " voor gehele getallen x, y en gehele $m \geq 2$?

x is congruent modulo m met y als m een deler is van $y - x$. Notatie: $x \equiv y \pmod{m}$.

(ii) Wat bedoelt men met "een standaard representant van een congruentieklasse modulo m "?

Een standaard representant van een congruentieklasse modulo m is een representant van die klasse die tot de verzameling $\{x: 0 \leq x < m\}$ behoort.

(iii) Formuleer het delingsalgoritme. N.B.: bedoeld wordt de stelling, niet het bijhorend algoritme).

Laat $a, b \in \mathbb{Z}$ met $b \neq 0$. Dan bestaat er een uniek paar getallen $q, r \in \mathbb{Z}$ zó dat

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

(b) Zij $m \geq 2$. Laat zien aan de hand van het delingsalgoritme dat voor iedere $z \in \mathbb{Z}$ geldt: de congruentieklasse $klas_m(z)$ van z modulo $m \geq 2$ heeft een standaard representant.

Neem $z \in \mathbb{Z}$ willekeurig en pas het delingsalgoritme toe met de deler m . Dat geeft $z = mq + r$ met $0 \leq r < m$. Uit de eerste betrekking volgt dat $mq = z - r$, waaruit weer volgt dat $r \equiv z \pmod{m}$. De tweede betrekking zegt dan dat r een standaard representant is van $klas_m(z)$.

(c) Los het volgende stelsel vergelijkingen op: $\bar{6} \cdot x + \bar{11} \cdot y = \bar{0}$ en $\bar{5} \cdot x + \bar{3} \cdot y = \bar{3}$ (modulus 37).

Matrixmethode: De determinant van het stelsel is

$$\bar{4} \cdot \bar{3} - \bar{5} \cdot \bar{11} = -\bar{37} = \bar{0}.$$

De matrixmethode is dus niet toepasbaar.

Eliminatiemethode: (1)-(2): $x + \bar{8}y = -\bar{3}$, dus $x = -\bar{3} - \bar{8}y$ (3). Ge-
lijkheid (3) in (1): $\bar{6} \cdot (-\bar{3} - \bar{8}y) + \bar{11} \cdot y = \bar{0}$. Dus $-\bar{18} - \bar{48}y + \bar{11}y = \bar{0}$,
waaruit volgt $-\bar{18} = \bar{0}$, tegenspraak. Het stelsel is strijdig.

2. Diversen.

(a) Algemene kennis.

(i) Wat is een priemgetal?

Een natuurlijk getal ≥ 2 heet een priemgetal wanneer het geen echte delers heeft. Een echte deler van een getal z is een deler ongelijk aan $\pm 1, \pm z$

- (ii) Wat zegt het Lemma van Euclides over priemdelers van een product?
 Lemma van Euclides: Is p een priemgetal en $p|a \cdot b$, dan is $p|a$ of $p|b$.
- (iii) Geef een precieze formulering van de Chinese reststelling in $\mathbb{Z}$ voor twee moduli.
 Laat $m_1, m_2 \geq 2$ relatief priem zijn, en laat $a_1, a_2 \in \mathbb{Z}$. Dan is het stelsel vergelijkingen

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

oplosbaar in x , en de oplossingsverzameling is precies een restklasse modulo $m_1 \cdot m_2$.

- (b) Zij p een priemgetal. Toon aan dat er géén gehele getallen a, b bestaan zó dat $a^2 = p \cdot b^2$.
Aanwijzing: het lemma van Euclides.

Stel integendeel dat a, b zo'n getallenpaar is: a, b ongelijk nul en $a^2 = p \cdot b^2$. Als a en b de gemene deler p hebben, kunnen we p^2 links en rechts in de gelijkheid wegdelen. We kunnen dit herhalen tot p geen gemene deler meer is van a, b .

Nu deelt p het rechterlid van de gelijkheid $a^2 = p \cdot b^2$ op zicht. Dus deelt p het linkerlid $a \cdot a$. Dus (Lemma van Euclides) deelt p het getal a . Dus deelt p^2 het linkerlid a^2 , en dus ook het rechterlid $p \cdot b^2$. Dus deelt p het getal b . Maar dan is $p > 1$ een gemene deler van a, b , een tegenspraak.

- (c) Bepaal, aan de hand van de Chinese reststelling, de kleinste mogelijke positieve oplossing voor het volgende probleem: twee opeenvolgende getallen, waarvan het eerste een 16-voud is, en het andere een 25-voud.

Je moet volgend stelsel vergelijkingen oplossen:

$$x \equiv 0 \pmod{16};$$

$$x + 1 \equiv 0 \pmod{25}.$$

De moduli $m_1 := 16$ en $m_2 := 25$ zijn relatief priem. Zoek eerst de Bezout coëfficiënten van m_1 en m_2 : $x_1 m_1 + x_2 m_2 = 1$. Oplossing: $11 \cdot 16 - 7 \cdot 25 = 1$. De vergelijkingen worden dan opgelost met de formule

$$x \equiv a_2 \cdot x_1 \cdot m_1 + a_1 \cdot x_2 \cdot m_2 \pmod{16 \cdot 25},$$

met $a_1 = 0$ en $a_2 = -1$. Dit geeft $x \equiv -176 \pmod{400}$. De kleinste positieve oplossing is het paar opeenvolgende getallen (224, 225).

3. Permutatiegroepen.

- (a) Algemene kennis.

- (i) Wat bedoelt men met: de orde van een element g in een groep G ?

De orde van een element g in een groep G is het kleinste getal $n \in \mathbb{N}$ met $g^n = e$; is zulke n er niet, dan heeft g orde oneindig.

- (ii) Wat bedoelt men met: de drager van een permutatie $\sigma \in S_n$?

De drager van een permutatie $\sigma \in S_n$ is de verzameling van alle elementen $x \in \{1, 2, \dots, n\}$ met $\sigma(x) \neq x$.

(iii) Wat bedoelt men met: de permutaties σ en τ in S_n zijn disjunct?"

Twee permutaties zijn disjunct als hun dragers disjunct zijn.

(b) Ontbind de volgende permutatie in een product van disjuncte cycli:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 1 & 2 & 6 & 3 & 4 \end{pmatrix}.$$

Standaard methode: herhaal zolang er nog niet gebruikte elementen zijn in $\{1, 2, \dots, n\}$: neem het eerste element $x \in \{1, 2, \dots, n\}$ dat nog niet gebruikt werd, en pas daarop σ toe tot je weer op x komt. Zet dit rijtje apart als een cykel. Dat geeft:

Neem $x=1$.

Opeenvolgende waarden van σ : 5, 6, 3, 1.

Cykel: (1563).

Neem $x=2$.

Opeenvolgende waarden van σ : 7, 4, 2.

Cykel: (274).

Antwoord: $\sigma = (1563) \circ (274)$.

De omgekeerde productvolgorde is ook goed, want disjuncte cycli commuteren.

(c) Bepaal de orde van de permutatie σ uit onderdeel (b). Geef toelichting bij het resultaat.

De orde van een product van disjuncte cycli is het kgv van de orde van de aparte cycli. De orde van een k -cykel is k ($k \geq 1$). In dit geval vinden we, met gebruik van het resultaat in (b), dat de orde van σ het kgv is van 4, 3, en dat is 12.

(d) Bereken op economische wijze: σ^{81} , waarbij σ de permutatie is uit onderdeel (b). Geef toelichting bij het resultaat.

σ^{81} kun je schrijven als $(\sigma^{12})^6 \circ \sigma^9$. Daarbij is σ^{12} de identieke permutatie. Het resultaat is dus σ^9 . In (b) vonden we twee disjuncte cycli $\tau = (1563)$ en $\mu = (274)$ met $\sigma = \tau \circ \mu$. Omdat disjuncte permutaties commuteren is $(\tau \circ \mu)^9 = \tau^9 \circ \mu^9$. Omdat τ van orde 4 is, vinden we $\tau^9 = \tau$. Omdat μ van orde 3 is, vinden we $\mu^9 = \text{identiteit}$. De uitkomst is dus:

$$\sigma^{81} = (1563)$$

4. Groepshomomorfismen en deelgroepen. In deze opgave bekijken we de kandidaat functie

$$f: \mathbb{Z}_{30}^* \rightarrow \mathbb{Z}_5^*, \quad \text{klas}_{30}(z) \mapsto \text{klas}_5(z).$$

(a) Controleer dat f een goed gedefiniëerde functie is, en controleer vervolgens dat f een (multiplicatief) homomorfisme is.

Goed gedefiniëerd: Er zijn twee potentiële problemen:

(1) Hangt het voorschrift af van een gekozen representant?

(2) Komt de functiewaarde terecht in de juiste verzameling ($\mathbb{Z}_5^*$)?

Ad (1). Stel z_1 en z_2 representeren dezelfde mod 30-klasse.

Dan is $z_1 \equiv z_2 \pmod{30}$. M.a.w., $30 \mid z_2 - z_1$, en bijgevolg $5 \mid z_2 - z_1$.

Dus: z_1 en z_2 representeren dezelfde mod 5-klasse.

Ad (2). Als $klas_{30}(z) \in \mathbb{Z}_{30}^*$ (priemrestklassen), dan heeft z geen delers gemeen met 30. A fortiori heeft z geen gemene delers met 5.

Multipliatief homomorfisme: We rekenen met twee moduli, hou de context in de gaten!

context $\mathbb{Z}_{30}^*$		context $\mathbb{Z}_5^*$
$klas_{30}(x)$	$\mapsto$	$klas_5(x)$
$klas_{30}(y)$	$\mapsto$	$klas_5(y)$
$\times$		$\times$
$klas_{30}(x) \cdot klas_{30}(y)$		$klas_5(x) \cdot klas_5(y)$
$= klas_{30}(x \cdot y)$	$\mapsto$	$= klas_5(x \cdot y)$

In de rechterkolom (context $\mathbb{Z}_5^*$) is het berekende product gelijk aan de functiewaarde op grond van de definitie van "product modulo 5".

- (b) Bepaal de kern H van f .

De kern is volgens definitie $f^{-1}(klas_5(1))$. In $\mathbb{Z}_{30}$ vinden we volgende restklassen $klas_{30}(z)$ met de eigenschap dat $klas_5(z) = klas_5(1)$:

$$klas_{30}(1), klas_{30}(6), klas_{30}(11), klas_{30}(16), klas_{30}(21), klas_{30}(26).$$

Slechts twee hiervan (met representanten 1 en 11) zijn in $\mathbb{Z}_{30}^*$ en we vinden: $H = \{klas_{30}(1), klas_{30}(11)\}$.

- (c) Hoeveel nevenklassen heeft de deelgroep H ?

We hebben $\phi(30)=8$ (Euler functie) dus $\#\mathbb{Z}_{30}^*=8$. Volgens deel (b) is $\#H=2$. Dus (Lagrange stelling) zijn er $8/2=4$ nevenklassen.

Expliciet (niet gevraagd): de nevenklassen zijn:

$$\begin{aligned} H &= \{klas_{30}(1), klas_{30}(11)\}, \\ 7 \cdot H &= \{klas_{30}(7), klas_{30}(17)\}, \\ 13 \cdot H &= \{klas_{30}(13), klas_{30}(23)\}, \\ 19 \cdot H &= \{klas_{30}(19), klas_{30}(29)\}. \end{aligned}$$

- (d) Geef, met de nodige argumentatie, een volledig representantensysteem voor de equivalentierelatie ' $\equiv$ ' in $\mathbb{Z}_{30}^*$ met voorschrift

$$x \equiv y \text{ betekent } x^{-1} \cdot y \in H.$$

Uit de theorie halen we de volgende wetenswaardigheden:

1) De equivalentieklassen van de equivalentierelatie ' $\equiv$ ' corresponderen aan de linker nevenklassen van H in $\mathbb{Z}_{30}^*$ (stelling 8.§7).

2) Volgens onderdeel (b) is de verzameling H precies de kern van het homomorfisme $f: \mathbb{Z}_{30}^* \rightarrow \mathbb{Z}_5^*$. Je krijgt dan de partitie in nevenklassen direct uit het homomorfisme f op de volgende manier:

$$\{f^{-1}(x) : x \in \mathbb{Z}_5^*\}.$$

(opgave 8.11).

Om een volledig representantensysteem te krijgen kies je (bijvoorbeeld) uit elke verzameling $f^{-1}(x)$ (met $x \in \mathbb{Z}_5^*$) die klasse modulo 30 met de kleinste standaard representant. Dat geeft:

Voor $x = klas_5(1)$: $klas_{30}(1)$.

Voor $x = klas_5(2)$: $klas_{30}(7)$ (let op, $klas_{30}(2) \notin \mathbb{Z}_{30}^*$).

Voor $x = klas_5(3)$: $klas_{30}(13)$ (let op, $klas_{30}(3), klas_{30}(8) \notin \mathbb{Z}_{30}^*$).

Voor $x = \text{klas}_5(4)$: $\text{klas}_{30}(19)$ (let op, $\text{klas}_{30}(4), \text{klas}_{30}(9), \text{klas}_{30}(14) \notin \mathbb{Z}_{30}^*$).

Conclusie: de verzameling

$\{\text{klas}_{30}(1), \text{klas}_{30}(7), \text{klas}_{30}(13), \text{klas}_{30}(19)\}$

is een volledig representantensysteem voor de relatie ' $\equiv$ '.

N.B.: Als je de nevenklassen uitgerekend hebt, kun je uit elke klasse het eerst opgesomde element kiezen. Omdat uit elke klasse precies één element komt, is dit inderdaad een volledig representantensysteem.

5. Ringen.

(a) Algemene kennis.

(i) Wat bedoelt men met een deelring van een ring?

Een deelring van een ring R is een deelverzameling $S \subseteq R$ met de volgende drie eigenschappen:

DR1) stabiliteit onder verschil: $x - y \in S$ voor $x, y \in S$.

DR2) stabiliteit onder vermenigvuldiging: $xy \in S$ voor $x, y \in S$.

DR3) eenheidselement: $1_R \in S$.

N.B.: bij conditie DR1) zou je ook de voorwaarde "S niet leeg" verwachten. Dat hoeft hier niet vanwege DR3). Je kan in DR1) ook meteen eisen dat S een deelgroep is voor optelling.

(ii) Wat bedoelt men met een ideaal in een ring?

Een ideaal in een ring R is een deelverzameling $I \subseteq R$ met de volgende twee eigenschappen:

I1) I is een additieve deelgroep van R .

I2) I is sterk stabiel onder vermenigvuldiging:

$rx, xr \in I$ als $x \in I$ en $r \in R$.

(iii) Leg uit waarom een ideaal, dat een eenheid van de ring bevat, noodzakelijk de hele ring is.

Stel: ideaal $I \subseteq R$ bevat een eenheid x . Dan is er een invers element y van x : $x \cdot y = 1$. Maar $x \in I$ geeft $x \cdot y \in I$ (sterk stabiel) en dus $1 \in I$. Maar dit heeft tot gevolg dat voor iedere $z \in R$ geldt $z = 1 \cdot z \in I$, zodat $I = R$.

Voor de rest van deze opgave werken we in de ring $\mathbb{Z}_{15}$ en de deelverzameling

$I := \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}\}$.

(b) Ga na dat I een ideaal van R is.

De eenvoudigste oplossing is om te controleren dat I van de vorm $(\bar{3})$ is (het ideaal van veelvouden van $\bar{3}$). De elementen uit dit veelvouden-ideaal zijn van de vorm $\bar{z} \cdot \bar{3}$, waar z een standaard representant is (d.w.z.: $0 \leq z < 15$). Duidelijk is dat $I \subseteq (\bar{3})$: $\bar{0} = \bar{0} \cdot \bar{3}$, $\bar{3} = \bar{1} \cdot \bar{3}$, $\bar{6} = \bar{2} \cdot \bar{3}$, $\bar{9} = \bar{3} \cdot \bar{3}$, $\bar{12} = \bar{4} \cdot \bar{3}$. Omgekeerd heeft een element van de vorm $\bar{z} \cdot \bar{3}$ een standaard representant van de vorm $3z - 15q$ (de rest bij deling van $3z$ door 15). Die rest is duidelijk een drievoud en is dus een van $0, 3, 6, 9, 12$.

Een iets uitvoeriger methode loopt via de definitie van ideaal: controleer dat I stabiel is onder de operatie "ver-

schil", $(x, y) \mapsto y - x$, en sterk stabiel is onder vermenigvuldiging: $x \cdot y \in I$ als tenminste één van x, y tot I behoort.

- (c) Ga na dat I onder de gebruikelijke optelling en vermenigvuldiging tegelijk ook een ring is. Omdat de verzameling I een ideaal is, is ze een deelgroep voor optelling en is ze stabiel onder vermenigvuldiging. De bewerkingen in I zijn die van $\mathbb{Z}_{15}$, en bijgevolg zijn de gebruikelijke commutatieve en distributieve wetten van kracht. Dit garandeert de wetten A1-A6 en A8. Rest nog, te controleren dat er een eenheidselement is (wet A7). Dat blijkt $\bar{6}$ te zijn:

x	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{9}$	$\bar{12}$
$\bar{6}x$	$\bar{0}$	$\bar{18} = \bar{3}$	$\bar{36} = \bar{6}$	$\bar{54} = \bar{9}$	$\bar{72} = \bar{12}$

- (d) Leg uit waarom I -- ondanks het resultaat in (c) -- geen deelring is van $\mathbb{Z}_{15}$. Een deelring moet het eenheidselement van de grote ring hebben (conditie DR3). Maar I heeft een "eigen" eenheidselement.

Normering:

1a	3	2a	3	3a	3	4a	4	5a	3	MC	20
1b	4	2b	5	3b	3	4b	4	5b	4		
1c	5	2c	6	3c	4	4c	4	5c	4		
				3d	4	4d	4	5d	3		
	12		14		14		16		14		20

Cijfer = Totaal/10 + 1

Multiple choice gedeelte: -3 ptn per foute keuze.

6. Multiple-choice gedeelte

- Bij iedere vraag is precies één van de onderdelen juist én (meest) volledig.
- Het antwoord (aangekruist of zwartgemaakt bolletje) hoeft niet te worden toegelicht.

6.1. Een verzameling $A \subseteq V$ is stabiel onder een binaire operatie f in V wanneer aan volgende voorwaarde is voldaan.

- ☐ Voor alle $x, y \in V$: als $f(x, y) \in A$ dan $x, y \in A$.
- ☐ Voor alle $x, y \in V$: $f(x, y) \in A$.
- ☐ Voor alle $x, y \in V$: als $x, y \in A$ dan $f(x, y) \in A$. ☞ JA
- ☐ Voor alle $x, y \in V$: als $y \in A$ dan $f(x, y) \in A$.

Optie 4 betekent "sterk stabiel".

6.2. De formule van Bezout in $\mathbb{Z}$ stelt dat voor iedere $a, b \neq 0$

- ☐ een uniek stel getallen q, r bestaat met $b = a \cdot q + r$ en $0 \leq r < |a|$.
- ☐ geldt: als $\text{ggd}(a, b) = 1$ en a deelt $b \cdot c$ dan a deelt c .
- ☐ een uniek stel getallen x, y bestaat met $x \cdot a + y \cdot b = 1$.
- ☐ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = \text{ggd}(a, b)$. ☞ JA

Optie 1 is het delingsalgoritme. Optie 2 is verwant aan het lemma van Euclides. Optie 3 is een speciaal geval van de stelling van Bezout voor getallen met $\text{ggd}=1$. Dit antwoord is dus minder volledig dan optie 4.

6.3. De Euler ϕ -functie $\phi(n)$ ($n \in \mathbb{N}$) heeft voor $n > 1$ als waarde

- ☐ het aantal positieve delers van n .
- ☐ het aantal priemdelers van n .
- ☐ de som van de exponenten in de priemfactorontbinding van n .
- ☐ het aantal positieve getallen relatief priem met n . ☞ JA

6.4. De orde van $\bar{6}$ in de multiplicatieve groep $(\mathbb{Z}/(13))^*$ is:

- ☐ twee.
- ☐ twaalf. ☞ JA
- ☐ dertien.
- ☐ de orde van dit element is niet gedefinieerd.

Je hoeft nauwelijks te rekenen: De orde van de groep $(\mathbb{Z}/(13))^*$ is $\phi(13)=12$ en de orde van 6 is hiervan een deler. Optie 4 is dus onzin, optie 3 is bij voorbaat uitgesloten. Voor optie 1 controleer je snel dat $6^2 \equiv 10$, dus de orde is niet twee.

6.5. De baanformule voor de werking van een eindige groep G op een eindige verzameling V zegt het volgende.

- ☐ De banen vormen een partitie van V in delen van gelijke grootte. In het bijzonder is het aantal elementen van een baan een deler van het aantal elementen van V .
- ☐ De stabilisator van een element uit V is een deelgroep van G , waarvan het aantal elementen een deler is van het aantal elementen van G .
- ☐ Voor iedere $v \in V$ is het product van het aantal elementen in zijn stabilisator met het aantal elementen in zijn baan precies $\#G$. ☞ JA
- ☐ Voor iedere $v \in V$ is het product van het aantal elementen in zijn stabilisator met het aantal

elementen in zijn baan precies $\#V$.

Optie 1: de banen vormen inderdaad een partitie, maar de banen hoeven niet even groot te zijn.

Optie 2: dat de stabilisator $S(v)$ van $v \in V$ een deelgroep is van G is waar, maar dat hoort niet bij de baanformule. Dat $\#S(v)$ een deler is van $\#G$ is waar voor alle deelgroepen (Lagrange).

Optie 4: niet $\#V$!

6.6. Zij $(G, *)$ een (multiplicatief geschreven) groep. Onder een deelgroep $H \subseteq G$ verstaat men:

- o Een groep H die deelverzameling is van G .
- o Een deelverzameling van de vorm $H := \{g^z : z \in \mathbb{Z}\}$, waar $g \in G$.
- o Een niet-lege deelverzameling $H \subseteq G$ die stabiel is onder de operatie $'*'$ van G .
- o Een niet-lege deelverzameling $H \subseteq G$ die stabiel is onder de operatie $(x, y) \mapsto x * y^{-1}$. ☞ JA

Optie 1: onvolledig antwoord; de bewerking van H staat niet los van de bewerking van G .

Optie 2: zulke verzamelingen zijn inderdaad deelgroepen, maar er zijn ook heel andere deelgroepen mogelijk.

Optie 3: onvolledig antwoord, je moet hier ook stabiliteit eisen van H m.b.t. inversen.

6.7. Een tweedegraads veelterm in $\mathbb{Z}_8[X]$

- o kan meer dan twee nulpunten hebben. ☞ JA
- o heeft altijd precies twee nulpunten (multipliciteit meegerekend).
- o heeft altijd ten hoogste twee nulpunten.
- o (..) Dit valt niet uit te maken, het hangt af van de "plaatshouder" X .

Opties 2 en 3 zijn niet voor iedere veelterm correct. Je vindt bijvoorbeeld vier nulpunten voor $X^2 - \bar{1}$. Optie 4 is volslagen onzin.

6.8. De graden formule in een veeltermring over een ITG zegt dat

- o de graad van het product van twee veeltermen $F, G \neq 0$ is de som van de graden van F en G .
☞ JA
- o de graad van de som van twee veeltermen $F, G \neq 0$ is het maximum van de graden van F en G .
- o de graad van een veelterm F is de hoogst voorkomende exponent in F .
- o elke veelterm $F \neq 0$ heeft een graad.

Optie 3 is de definitie van graad, en optie 4 is een triviaal gevolg van deze definitie. Optie 2 is een ware uitspraak over de som van twee veeltermen, maar dat is hier naast de kwestie: het gaat om producten. Optie 1 geeft de gradenformule weer.