

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. Elementair modulorekenen en cryptografie

- (a) Algemene kennis.
- (i) Wat bedoelt men met " x is congruent modulo m met y " voor gehele getallen x, y en gehele $m \geq 2$?
 - (ii) Gegeven is een modulus $m := 54$. Bereken efficiënt: $(161 + 221)^3 \pmod{m}$. Goede toelichting scoort; je hoeft niets te bewijzen.
 - (iii) Wat bedoelt men met "een inverse restklasse modulo m van een restklasse"?
 - (iv) Heeft $\overline{28}$ een inverse restklasse modulo 51? Zo nee, waarom niet; zo ja, welke? Goede toelichting scoort; je hoeft niets te bewijzen.
- (b) Gegeven is een twee bij twee matrix M met elementen uit $\mathbb{Z}_{10}$ (modulus $m := 10$).
- (i) Leg beknopt uit hoe je een cijfertext kunt (de)coderen met M als sleutel. De symbolen uit de tekst zijn dus de cijfers 0 t/m 9.
 - (ii) Waarom is de volgende matrix M niet geschikt als sleutel?

$$M := \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{3} & \overline{4} \end{pmatrix}.$$

- (c) (vervolg onderdeel (b)) Codeer "1234" en decodeer "5678" met behulp van de volgende sleutel.

$$M := \begin{pmatrix} \overline{1} & \overline{2} \\ \overline{3} & \overline{3} \end{pmatrix}.$$

2. De Chinese reststelling

- (a) Algemene kennis.
- (i) Geef een precieze formulering van de Chinese reststelling voor twee moduli m_1 en m_2 .
 - (ii) Waarom zijn de moduli $m_1 := 91$ en $m_2 := 117$ niet geschikt voor deze stelling?
- (b) 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.

3. Project Gehele Getallen

Voor deze opgave kan je de aparte pagina (na het multiple choice deel) gebruiken met axioma's over $\mathbb{Z}$ en gevolgtrekkingen hieruit.

Spelregel. In het bewijs van een formule mag je uitsluitend wetten gebruiken die één of meer regels vóór de te bewijzen formule worden genoemd.

- (a) Toon aan dat $z \cdot 0 = 0$. Geef daarbij aan welke van de axioma's of afgeleide wetten gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.
- (b) Toon aan dat $(-1) \cdot z = -z$. Geef daarbij aan welke van de axioma's of afgeleide wetten gebruikt werden, en geef tenminste één stap aan waarin de gelijkheidsregel werd gehanteerd.

4. De Euler functie ϕ

(Zie ook multiple choice vraag 6.3).

- (a) Algemene kennis.
 - (i) Geef zonder bewijs een of twee belangrijke formules waarmee je (in principe) $\phi(n)$ kan berekenen voor elke $n \in \mathbb{N}$.
 - (ii) Bereken met je formule(s) uit (i) $\phi(360)$ en $\phi(6!)$ (zes faculteit).
- (b) De Stelling van Euler gaat over machten van een geheel getal a modulo m . Geef een precieze formulering.
- (c) Bereken, met toelichting, $16^{213} \pmod{21}$. (Werk efficiënt; eventuele resultaten mogen worden gebruikt zonder bewijs.)

5. Cyclische groepen

- (a) Algemene kennis.
 - (i) Wat bedoelt men met: de orde van een element in een groep?
 - (ii) Welk verband bestaat er tussen de orde van een element in een eindige groep, en het aantal elementen van die groep?
 - (iii) Wat bedoelt men met een cyclische groep?
 - (iv) Stel: van een eindige groep G ken je de orde van ieder element. Hoe kun je hieruit opmaken dat de groep al dan niet cyclisch is?
- (b) Laat zien dat de permutatiegroep S_3 niet cyclisch is.
- (c) Laat zien dat de groep $(\mathbb{Z}_{17}^*, \cdot)$ cyclisch is. Werk efficiënt; goede toelichting scoort.

Normering:

1a	6	2a	6	3a	7	4a	4	5a	4	MC	15
1b	5	2b	7	3b	7	4b	6	5b	6		
1c	5					4c	6	5c	6		
16		13		14		16		16		15	

Voor het multiple choice gedeelte geldt: -3 ptn per foute keuze.

Totaal = 90

Cijfer = Behaald Totaal / 10 + 1

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. Het Delingsalgoritme stelt dat

- o Een getal $a \neq 0$ deelbaar is door d precies dan als een uniek getal q bestaat met $a = d \cdot q$.
- o Bij iedere twee getallen a, b met $b \neq 0$ er een uniek paar getallen q, r bestaan met $a = b \cdot q + r$ en $|r| < b$.
- o Bij iedere twee getallen a, b met $b \neq 0$ er een uniek paar getallen q, r bestaan met $a = b \cdot q + r$ en $0 \leq r < |b|$.
- o (...) Geen van deze, het is de algoritme waarmee de staartdeling wordt uitgevoerd.

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

- o een unieke oplossing x bestaat van het stelsel vergelijkingen

$$x \equiv \begin{cases} a \bmod m \\ b \bmod n \end{cases},$$

waar de moduli m, n relatief priem zijn.

- o geldt: als $\text{ggd}(a, b) = 1$ en a deelt $b \cdot c$ dan a deelt c .
- o een uniek stel getallen x, y bestaat met $x \cdot a + y \cdot b = 1$.
- o een stel getallen x, y bestaat met $x \cdot a + y \cdot b = \text{ggd}(a, b)$.

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

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

6.4. Het ordeningsprincipe in $\mathbb{Z}$ stelt dat

- o De natuurlijke ordening een totale ordening is.
- o De verzameling van alle natuurlijke getallen naar beneden begrensd is.
- o Iedere niet-lege, naar beneden begrensde verzameling een kleinste element heeft.
- o Iedere niet-lege verzameling een kleinste benedengrens heeft.

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

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

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

- o twaalf.
- o acht.
- o twee.
- o de orde van dit element is niet gedefiniëerd.

Axioma's Gehele Getallen (zover nodig)

Gelijkheid

Gelijkheidswet: $x = x$.

Gelijkheidsregel: Gegeven een gelijkheid $t_1 = t_2$ van termen en een correcte formule, dan is ook de formule correct die ontstaat, wanneer ergens t_1 wordt vervangen door t_2 .

Symmetrie van gelijkheid: $x = y \rightarrow y = x$.

Transitiviteit van gelijkheid: $x = y$ en $y = z \rightarrow x = z$.

Axioma's voor optelling

(A1) Optelling is associatief: $(x + y) + z = x + (y + z)$.

(A2) Neutraal element 0: $x + 0 = 0 + x = x$.

(A3) Tegengestelde: Bij iedere x bestaat een tegengesteld element x' zo dat $x + x' = x' + x = 0$.

(A4) Optelling is commutatief: $x + y = y + x$.

Schrapwetten voor optelling:

$x + y = x + z \rightarrow y = z$ (linker -).

$x + z = y + z \rightarrow x = y$ (rechter -).

Uniciteit van tegengestelde:

$x + y_1 = 0$ en $x + y_2 = 0 \rightarrow y_1 = y_2$.

$y_1 + x = 0$ en $y_2 + x = 0 \rightarrow y_1 = y_2$.

De unieke tegengestelde van een getal x noteert men als $-x$.

Additieve wetten voor tegengestelde:

$-(-x) = x$.

$-(x + y) = (-x) + (-y)$.

Termen overbrengen naar ander lid:

$x = y \leftrightarrow 0 = y + (-x)$.

$x + y = z \leftrightarrow x = z + (-y)$.

Axioma's voor vermenigvuldiging

(A6) Vermenigvuldiging is associatief: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(A7) Neutraal element 1: $x \cdot 1 = 1 \cdot x = x$.

(A8) Vermenigvuldiging is commutatief: $x \cdot y = y \cdot x$.

(A5) Distributieve wet: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

(A9) Wet van nuldelers: Als $x \cdot y = 0$ dan is $x = 0$ of $y = 0$.

Vermenigvuldigen met nul:

$x \cdot 0 = 0 = 0 \cdot x$.

Multiplicatieve wetten voor tegengestelde:

$(-1) \cdot x = -x = x \cdot (-1)$.

$x \cdot (-y) = -(x \cdot y) = (-x) \cdot y$.

$(-x) \cdot (-y) = x \cdot y$.

Schrapwetten voor vermenigvuldiging:

$x \cdot y = x \cdot z$ en $x \neq 0 \rightarrow y = z$.

$x \cdot z = y \cdot z$ en $z \neq 0 \rightarrow x = y$.

In plaats van $x + (-y)$ wordt ook $x - y$ geschreven.