

**Opgelet:** er is een apart multiple-choice gedeelte op de laatste bladzijde (vraag 6). Schrijf op dat blad je naam en lever het mee in met je overige tentamenkopij!

## 1. Modularekenen

(a) Algemene kennis: Zij  $m \in \mathbb{Z}$ ,  $m \geq 2$ .

(i) Geef het relatievoorschrift voor de relatie *congruentie modulo*  $m$  in  $\mathbb{Z}$ .

(ii) Waarom neemt men (bijna) altijd aan dat de *modulus*  $m$  tenminste 2 is?

(iii) Hier zijn twee matrices  $M$  en  $M^{-1}$  modulo 27. Geef de berekeningen waaruit blijkt dat de tweede matrix inderdaad de *inverse* is van de eerste.

$$M := \begin{pmatrix} \bar{3} & \bar{5} \\ \bar{5} & \bar{2} \end{pmatrix}; \quad M^{-1} := \begin{pmatrix} \bar{7} & -\bar{4} \\ -\bar{4} & -\bar{3} \end{pmatrix}.$$

(b) Laat zien dat er géén (multiplicatieve) *inverse* is van 49 modulo 63. (Goede toelichting scoort.)

(c) Laat  $A=1, B=2, \dots, Z=26$  en spatie=0. Neem de volgende matrix  $M$  en zijn inverse matrix in  $\mathbb{Z}/(27)$  (cf onderdeel (a)(iii)).

$$M := \begin{pmatrix} \bar{3} & \bar{5} \\ \bar{5} & \bar{2} \end{pmatrix}; \quad M^{-1} := \begin{pmatrix} \bar{7} & -\bar{4} \\ -\bar{4} & -\bar{3} \end{pmatrix}.$$

Codeer "GO" en decodeer "ODFS" met de gebruikelijke matrixmethode.

## 2. De Euler functie en RSA encryptie.

(a) Algemene kennis:

(i) De *Euler functie* kent aan een natuurlijk getal  $m \geq 1$  een getal  $\phi(m)$  toe. Waar staat  $\phi(m)$  voor?

(ii) Bereken  $\phi(91)$ . Welke formule(s) heb je gebruikt en onder welke voorwaarde(n) zijn ze geldig?

(b) Formuleer in eigen woorden het *RSA lemma* en leg bondig uit hoe dit lemma functioneert bij *RSA encryptie/decryptie*.

(c) Iemand maakt als publieke sleutel voor RSA de gegevens  $m=91$  (modulus) en  $e=35$  bekend. *Breek* de code, dat wil zeggen: bereken het resterende deel van de sleutel, met name de privé sleutel  $d$ .

## 3. Ringen, Lichamen, en Veeltermringen

(a) Algemene kennis:

(i) Wat bedoelt men met een *nuldeler* in een commutatieve unitaire ring (CUR)  $R$ ?

(ii) Geef een voorbeeld van een nuldeler in  $\mathbb{Z}/(143)$ .

(iii) Bij een lichaam  $K$  hoort een veeltermring  $K[X]$ . Geef de benaming (of de bijhorende afkorting ervan) die de eigenschappen van  $K[X]$  het beste beschrijft:

Unitaire ring--UR, Commutatieve Unitaire ring--CUR, Integriteitsgebied--ITG, Lichaam--L

(b) Laat zien dat de veelterm  $F := X^3 + X + 1$  *reducibel* is over het lichaam  $\mathbb{Z}/(3)$  maar *irreducibel* over het lichaam  $\mathbb{Z}/(7)$ .

(c) (Vervolg (b)) Hoeveel elementen heeft het *quotiënt*  $K[X]/(F)$

(i) als  $K := \mathbb{Z}/(3)$ ?

(ii) als  $K := \mathbb{Z}/(7)$ ?

(d) (Vervolg (b)) Is  $K[X]/(F)$  een lichaam

(i) als  $K := \mathbb{Z}/(3)$ ?

(ii) als  $K := \mathbb{Z}/(7)$ ?

## 4. Vector ruimten

- (a) Algemene kennis:
- (i) Wat bedoelt men met de *dimensie* van een vector ruimte  $V$  over een lichaam  $\mathbb{F}$ ?
  - (ii) Als  $\mathbb{F} = \mathbb{Z}/(3)$  en  $V$  heeft dimensie 4, hoeveel elementen heeft  $V$  dan?
  - (iii) De veeltermen van graad  $\leq 3$  over een lichaam  $\mathbb{F}$  vormen een vector ruimte over  $\mathbb{F}$ . Wat is de dimensie hiervan?
- (b) Bepaal het *matrix product*  $M \cdot N$  van de volgende twee matrices modulo 3:
- $$M := \begin{bmatrix} -1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{bmatrix} \quad N := \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & -1 \end{bmatrix}$$
- (c) Wat bedoelt men met de *kolomruimte* van de matrix  $M$  en wat is (concreet) de dimensie hiervan? Wat is dan de dimensie van de *nulruimte* van  $M$ ?

## 5. Primitieve elementen.

- (a) Algemene kennis:
- (i) Wat bedoelt men met een *primitief element* van een lichaam  $\mathbb{K}$ ?
  - (ii) Primitieve elementen komen aan bod in het *Diffie-Hellman protocol* voor sleuteluitwisseling in cryptografie. Leg dit protocol bondig uit.
- (b) Zoek methodisch een primitief element in  $\mathbb{Z}/(13)$ . (Goede toelichting scoort.)
- (c) In het lichaam  $(\mathbb{Z}/(3)[X])/(X^3 - X + 1)$  is  $\alpha := \bar{X}$  een primitief element. Controleer dit. (Goede toelichting scoort.)

## Normering:

|       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|
| 1a: 3 | 2a: 3 | 3a: 3 | 4a: 4 | 5a: 3 | 6: 16 |
| 1b: 4 | 2b: 5 | 3b: 4 | 4b: 4 | b: 5  |       |
| 1c: 8 | 2c: 7 | 3c: 4 | 4c: 5 | c: 8  |       |
|       |       | 3d: 4 |       |       |       |
| 15    | 15    | 15    | 13    | 16    | 16    |

**Totaal = 90; Cijfer = Behaald totaal / 10 + 1**

**Multiple choice:** -3ptn per fout

naam, studierichting & jaar:

06-02-2007

## 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. De stelling van Bezout over  $\mathbb{Z}$  zegt dat bij iedere  $a, b \neq 0$  ...

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

6.2. Een monoïde voldoet i.h.a niet aan alle voorwaarden (axioma's) van een groep. Wat valt er precies weg uit die axioma's:

- o Het bestaan van inversen.
- o Het bestaan van een neutraal element en van inversen.
- o De associativiteit van de bewerking.
- o De stabiliteit onder de bewerking.

6.3. De orde van een element  $g$  in een eindige groep  $G$  met neutraal element  $e$  is:

- o het kleinste getal  $k > 0$  waarvoor  $g^k = e$ .
- o het grootste getal  $k > 0$  waarvoor  $g^k = e$ .
- o het rangnummer van  $g$  in de opsomming ( $e$  eerst) van alle elementen uit  $G$ .
- o het aantal elementen in  $G$  met dezelfde inverse als  $g$ .

6.4. Als  $R$  een UR (unitaire ring) is, dan staat  $R^*$  voor

- o de veeltermring van alle veeltermen over  $R$ .
- o de verzameling van nuldelers van  $R$ .
- o de groep van eenheden (inverteerbare elementen) van  $R$ .
- o de multiplicatieve monoïde die uit  $R$  ontstaat na weglaten van de optelling.

6.5. Gegeven een lichaam  $K$  en een veelterm  $M$  over  $K$ , dan is  $K[X]/(M)$  een lichaam precies dan als

- o de constante term van  $M$  niet nul is.
- o  $M$  geen nulpunten heeft.
- o de graad van  $M$  een priemgetal is.
- o  $M$  irreducibel is.

6.6. Er bestaat géén lichaam met

- o 13 elementen.
- o 15 elementen.
- o 16 elementen.
- o 17 elementen.