

Tentamen Algebra en Discrete Wiskunde 17-12-2003

1 *Priemrestklassen.*

- a) Bepaal alle priemrestklassen modulo 7 en modulo 8.
- b) Geef voor de priemrestklassen modulo 7 de vermenigvuldigtabel.
- c) Geef voor de priemrestklassen modulo 8 de vermenigvuldigtabel.
- d) Bepaal de kleinste veelterm in X over $\mathbb{Z}/(8)$ waarvan alle priemrestklassen modulo 8 nulpunten zijn.

2 *De Euler totient functie en RSA encryptie.*

- a) Wat bedoelt men met de *Euler totient functie* $\phi(m)$?
- b) Welke formule is er voor $\phi(m_1 \cdot m_2)$ en voor welke voorwaarde(n) op m_1 en m_2 is die geldig?
- c) Wat weten we van de orde van een element in de vermenigvuldiggroep modulo $m_1 \cdot m_2$?
- d) Leg kort uit hoe RSA encryptie/decryptie in zijn werk gaat.
- e) iemand maakt als publieke sleutel voor RSA de gegevens $m=77$ en $e=13$ bekend. Breek zijn code, dwz. bepaal het resterende deel van de sleutelgegevens.

3 *Ringen, Lichamen, Veeltermen(polynomen).*

- a) Wat bedoelt men met een *nuldeler* in een ring R ? Geef een voorbeeld van een nuldeler in $\mathbb{Z}/(24)$
- b) Geef de juiste, meest aangepaste, benaming of bijbehorende afkorting: Een veeltermring (of polynoomring) over een lichaam is een
(Kies: Unitaire Ring--UR, Commutatieve Unitaire Ring--CUR, Integriteitsgebied--ITG, of Lichaam--L).
- c) Laat zien dat de veelterm $F=X^3+X+1$ reducibel is over het lichaam $\mathbb{Z}/(3)$ maar irreducibel over het lichaam $\mathbb{Z}/(7)$.
- d) Hoeveel elementen heeft de ring $K[X]/F$ voor het geval dat met K het lichaam $\mathbb{Z}/(3)$ wordt bedoeld, en voor het geval dat met K het lichaam $\mathbb{Z}/(7)$ wordt bedoeld. Bedoeld wordt de F uit onderdeel b).
- e) Is de ring $K[X]/F$ zelf een lichaam, in het geval dat met K het lichaam $\mathbb{Z}/(3)$ wordt bedoeld, en in het geval dat met K het lichaam $\mathbb{Z}/(7)$ wordt bedoeld. Bedoeld wordt de F uit onderdeel b).

4 *Vectorruimten en polynomen.*

Zij k een lichaam, en $n > 0$ een geheel getal, n W de deelverzameling van $K[X]$ met alle veeltermen van graad $\leq n$ (inclusief de nulveelterm).

Z.O.Z.

- a) Ga na dat deze verzameling W bestaande uit alle veeltermen van graad $\leq n$ een lineaire deelruimte is van de vectorruimte $K[X]$.
- b) De verzameling van alle polynomen van graad precies n is geen deelruimte van de vectorruimte $K[X]$. Geef aan waarom niet.
- c) Is de verzameling van alle polynomen met constante term 0 een deelruimte van de ruimte $K[X]$?

5 *Efficient rekenen in $GF(27)$.*

Zie de tabel onder aan de pagina.

- a) Ga na dat de veelterm $M = X^3 - X + 1$ inderdaad irreducibel is in $k = \mathbb{Z}/(3)$
- b) Welke machten van $\alpha = \bar{X}$ moet U ten minste controleren of aan te tonen dat α inderdaad een primitief element is van $GF(27)$.
- c) Schrijf $\alpha^7 + \alpha^{12}$ als macht van α . Werk efficiënt.
- d) Schrijf $(\alpha^2 - \alpha + 1)^5$ als tweedegraads veelterm in α . Werk efficiënt.

NORMERING

1a 2 pt	2b 2 pt	3b 1 pt	4b 2 pt	5d 2 pt
1b 1 pt	2c 2 pt	3c 2 pt	4c 2 pt	Multiple Choice
1c 1 pt	2d 2 pt	3d 2 pt	5a 2 pt	7 pt
1d 2 pt	2e 2 pt	3e 2 pt	5b 2 pt	
2a 1 pt	3a 2 pt	4a 2 pt	5b 2 pt	$CIJFER = \frac{SOM}{5} + 1.$

Het eindige lichaam $GF(27)$ kan worden gerepresenteerd met een primitief element Y die een oplossing is van het polynoom $X^3 - X + 1 = 0$.

De vermenigvuldiggroep en de optelgroep hangen dan als volgt samen:

$1 = 1$	$Y^9 = Y + 1$	$Y^{18} = Y^2 - Y + 1$
$Y = Y$	$Y^{10} = Y^2 + Y$	$Y^{19} = -Y^2 - Y - 1$
$Y^2 = Y^2$	$Y^{11} = Y^2 + Y - 1$	$Y^{20} = -Y^2 + Y + 1$
$Y^3 = Y - 1$	$Y^{12} = Y^2 - 1$	$Y^{21} = Y^2 + 1$
$Y^4 = Y^2 - Y$	$Y^{13} = -1$	$Y^{22} = -Y - 1$
$Y^5 = -Y^2 + Y - 1$	$Y^{14} = -Y$	$Y^{23} = -Y^2 - Y$
$Y^6 = Y^2 + Y + 1$	$Y^{15} = -Y^2$	$Y^{24} = -Y^2 - Y + 1$
$Y^7 = Y^2 - Y - 1$	$Y^{16} = -Y + 1$	$Y^{25} = -Y^2 + 1$
$Y^8 = -Y^2 - 1$	$Y^{17} = -Y^2 + Y$	$Y^{26} = 1$

6. Multiple-choice gedeelte

- Bij iedere vraag is precies één van de onderdelen juist en (meest) volledig.
 - Het antwoord van een aangekruist bolletje hoeft niet te worden toegelicht
- 6.1. De orde van een element g in een eindige groep G met neutraal element e is:
- o het kleinste getal $k > 0$ waarvoor geldt $g^k = e$.
 - o het grootste getal $k > 0$ waarvoor geldt $g^k = e$.
 - o het rangnummer g in de opsomming van de elementen van G .
 - o het aantal elementen in G met dezelfde inverse als g .
- 6.2. De delingsalgorithme in $\mathbb{Z}$ stelt dat:
- o bij iedere $a, b \neq 0$ geldt: als $\text{ggd}(a, b) = 1$ en a deelt $b \cdot c$ dan a deelt c .
 - o bij iedere $a, b \neq 0$ een uniek stel getallen q, r bestaat met $b = a \cdot q + r$ en $0 \leq r < a$.
 - o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = 1$.
 - o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = \text{ggd}(a, b)$.
- 6.3. Een monoïde is:
- o een semigroep met een neutraal element.
 - o een vectorruimte met dimensie 1.
 - o een alternatieve benaming voor een unitaire ring.
 - o een veeltermring met uitsluitend veeltermen van graad 1.
- 6.4. Een basis in een vectorruimte (lineaire ruimte) V is:
- o een zo klein mogelijke lineaire deelruimte
 - o een verzameling van eenheidsvectoren.
 - o een lineair onafhankelijke deelverzameling die heel V voortbrengt.
 - o een zo groot mogelijke lineaire deelruimte
- 6.5. De formule van Bezout in $\mathbb{Z}$ stelt dat:
- o bij iedere $a, b \neq 0$ een uniek stel getallen q, r bestaat met $b = a \cdot q + r$ en $0 \leq r < a$.
 - o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = \text{ggd}(a, b)$.
 - o bij iedere $a, b \neq 0$ een stel getallen x, y bestaat met $x \cdot a + y \cdot b = 1$.
 - o bij iedere $a, b \neq 0$ geldt: als $\text{ggd}(a, b) = 1$ en a deelt $b \cdot c$ dan a deelt c .
- 6.6. Een ideaal van een commutatieve unitaire ring R is een deelverzameling van R die:
- o stabiel is onder optelling $x + y$ en vermenigvuldiging $x \cdot y$ van R .
 - o stabiel is onder aftrekking $x - y$ en vermenigvuldiging $x \cdot y$ van R die het eenheidselement van R bevat.
 - o stabiel is onder optelling $x + y$ en "superstabiel" is onder de vermenigvuldiging $x \cdot y$ van R .
 - o stabiel is onder aftrekking $x - y$ en "superstabiel" onder de vermenigvuldiging $x \cdot y$ van R die het eenheidselement van R bevat.
- N.B. Een verzameling $A \subset R$ is "stabiel" onder een bewerking $x \# y$ in R wanneer geldt:
als $x \in A$ en $y \in A$ dan $x \# y \in A$.
- Een verzameling $A \subset R$ is "superstabiel" onder een bewerking $x \# y$ in R wanneer geldt:
als $x \in R$ en $y \in A$ dan $x \# y \in A$.
- 6.7. Een primitief element van een lichaam K is:
- o een generator van de additieve groep van K .
 - o een irreducibele veelterm in $K[X]$.
 - o een element van K^* zonder multiplicatieve inverse.
 - o een generator van de multiplicatieve groep K^* .