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. Modulorekenen

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

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

Voorschrift:

$$x \equiv y \,(mod\ m) \quad :\leftrightarrow \quad m \mid y - x.$$

Daarbij staat "$a \mid b$" voor "a is een deler van b": er is een $z \in \mathbb{Z}$ met $a \cdot z = b$.

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

Voor $m = 0$ geldt $m \mid y - x$ alleen als $x = y$. We krijgen hier de triviale relatie "is gelijk aan".

Voor $m = 1$ geldt $m \mid y - x$ voor alle x en y. Dit is het andere uiterste van een triviale relatie.

Tenslotte geldt $m \mid a$ precies dan als $-m \mid a$. De relaties "congruent modulo $\pm m$" zijn dus dezelfde.

(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.

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

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

De inverse van 49 modulo 63 bestaat, precies dan als $ggd(49,63) = 1$. Maar $49 = 7^2$ en $63 = 7 \cdot 9$ en dus is de ggd 7. (Dat kun je ook snel narekenen met het algoritme van Euclides.)

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

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

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

Coderen. Bericht in cijfers omzetten: "GO" $\mapsto (7,15)$.

$$\begin{pmatrix} \bar{3} & \bar{5} \\ \bar{5} & \bar{2} \end{pmatrix} \cdot \begin{pmatrix} \bar{7} \\ \overline{15} \end{pmatrix} = \begin{pmatrix} \overline{15} \\ \overline{11} \end{pmatrix}.$$

Het resultaat is "OK".

Decoderen. Bericht in cijfers omzetten: "ODFS" $\mapsto (15,4,6,19)$. Per twee doorrekenen:

$$\begin{pmatrix} \bar{7} & -\bar{4} \\ -\bar{4} & -\bar{3} \end{pmatrix} \cdot \begin{pmatrix} \overline{15} \\ \bar{4} \end{pmatrix} = \begin{pmatrix} \bar{8} \\ \bar{9} \end{pmatrix}.$$

$$\begin{pmatrix} \bar{7} & -\bar{4} \\ -\bar{4} & -\bar{3} \end{pmatrix} \cdot \begin{pmatrix} \bar{6} \\ \overline{19} \end{pmatrix} = \begin{pmatrix} \overline{20} \\ \bar{0} \end{pmatrix}.$$

Het resultaat is "HIT " (spatie achteraan).

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?

Voor $m \geq 1$ is $\phi(m)$ het aantal gehele getallen x met $0 \leq x < m$ en $ggd(x, m) = 1$ ("relatief priem"). Alternatief: het is het aantal priemrestklassen modulo m.

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

Berekening:

$$\phi(91) = \phi(13 \cdot 7) \overset{(*)}{=} \phi(13) \cdot \phi(7) \overset{(**)}{=} 12 \cdot 6 = 72.$$

In de gelijkheid (*) gebruiken we de formule $\phi(m_1 \cdot m_2) = \phi(m_1) \cdot \phi(m_2)$. Deze geldt als $ggd(m_1, m_2) = 1$ voor getallen $m_1, m_2 \geq 1$,

In gelijkheid (**) gebruiken we de formule $\phi(p) = p - 1$, geldig voor een priemgetal p. (Alle getallen van 1 tot $p-1$ zijn relatief priem met p.)

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

Het RSA Lemma:

Laat $p_1, .., p_k$ verschillende priemgetallen zijn met product m en zij $e \equiv 1 \pmod{\phi(m)}$. Dan is $a^e \equiv a \pmod{m}$ voor alle $a \in \mathbb{Z}$.

(Diktaat p.20).

Bij RSA en/de/cryptie worden twee (grote) priemgetallen $p \neq q$ gebruikt en $m = p \cdot q$. Verder zijn twee gehele getallen d, e nodig met $d \cdot e \equiv 1 \pmod{\phi(m)}$. De eigenaar van de code maakt het product $m = pq$ en het getal e bekend aan haar/zijn correspondenten (publieke sleutel). De priemfactorontbinding $\{p, q\}$ en het getal d houdt zij/hij voor zichzelf (private sleutel).

(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.

We vinden de priemfactorontbinding $\{7, 13\}$ van m. De inverse d van e modulo $\phi(91) = 72$ (zie onderdeel (a)(iii)) kan nu worden berekend.

72	1	0	-
35	0	1	2
2	1	-2	17
1	-17	35	

Test: $72 \cdot (-17) + 35 \cdot 35 = -1224 + 1225 = 1$.
De inverse van 35 is ... 35 zelf!

Resultaat $d = 35$ is het ontbrekende deel van de privé-sleutel.

3. Ringen, Lichamen, en Veeltermringen

(a) Algemene kennis:

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

Een element $r \in R$ is een nuldeler als $r \neq 0_R$ en als bovendien een getal $s \in R$ bestaat met $s \neq 0_R$ en $s \cdot r = 1_R$.

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

$143 = 11 \cdot 13$ dus $\overline{11} \cdot \overline{13} = \bar{0}$ in $\mathbb{Z}/143$. Duidelijk is dat $\overline{11} \neq \bar{0}$ en $\overline{13} \neq \bar{0}$.

(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 $\mathbb{Z}/(7)$.

In $\mathbb{Z}/(3)$ vinden we een nulpunt $\bar{1}$. In $\mathbb{Z}/(7)$ bestaat volgens de tabel hierna géén nulpunt.

X	0	1	2	3	4	5	6
$F(X)$	1	3	4	3	6	5	6

(standaard representanten)

Dit volstaat voor irreducibiliteit vanwege $deg(F) = 3$.

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

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

Het lichaam K heeft 3 elementen en $K[X]/(F)$ is een drie-dimensionale vector ruimte over K. Dus heeft het quotiënt $3^3 = 27$ elementen.

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

Het lichaam K heeft 6 elementen en $K[X]/(F)$ is een drie-dimensionale vector ruimte over K. Dus heeft het quotiënt $7^3 = 343$ elementen.

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

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

Nee, want $F \in \mathbb{Z}/(3)[X]$ is reducibel.

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

Ja, want $F \in \mathbb{Z}/(7)[X]$ is irreducibel.

4. Vector ruimten

(a) Algemene kennis:

(i) Wat bedoelt men met de *dimensie* van een vector ruimte V over een lichaam $\mathbb{F}$?

Dimensie van V is het aantal vectoren in een basis van V (alle bases van V hebben evenveel elementen).

(ii) Als $\mathbb{F} = \mathbb{Z}/(3)$ en V heeft dimensie 4, hoeveel elementen heeft V dan?

Formule: aantal elementen van $\mathbb{F}$ tot de macht dimensie van V. Dat geeft $3^4 = 81$ elementen.

(iii) De veeltermen van graad ≤ 3 over een lichaam $\mathbb{F}$ vormen een vector ruimte over $\mathbb{F}$. Wat is de dimensie hiervan?

Een basis voor deze vector ruimte is, bijvoorbeeld, $\{1_F, X, X^2, X^3\}$. Elke veelterm van graad ≤ 3 is namelijk op precies één manier te zien als een lineaire combinatie

$$c_0 + c_1 X + c_2 X^2 + c_3 X^3$$

van deze "basisvectoren". De dimensie van deze vector ruimte is dus 4.

(b) Bepaal het *matrix product* $M \cdot N$ van de volgende twee matrices modulo 3:

$$M := \begin{bmatrix} -1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{bmatrix} \qquad N := \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & -1 \end{bmatrix}$$

Procedure: rijen van M "vervlechten" met kolommen van N. Bijvoorbeeld: 2e rij van M met 3e kolom van N geeft (modulo 3 gerekend)

$$(0 \cdot 0) + (1 \cdot 1) + (0 \cdot -1) + (1 \cdot -1) = 0$$

op positie (rij 2, kolom 3) in het product. Dat geeft (rekenen modulo 3)

$$M \cdot N = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 0 \\ 1 & -1 & -1 \end{pmatrix}.$$

(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?

De kolomruimte van M is de dimensie van de vector ruimte, voortgebracht door de kolomvectoren. Omdat een kolomvector uit drie elementen bestaat, is deze vector ruimte van dimensie ≤ 3. De eerste drie kolommen van M zijn duidelijk lineair onafhankelijk. Dus is de dimensie tenminste drie.
Conclusie: de kolomruimte heeft dimensie precies drie. De nulruimte is dan: aantal kolommen min drie, dus één.

5. Primitieve elementen.

(a) Algemene kennis:

(i) Wat bedoelt men met een *primitief element* van een lichaam $\mathbb{K}$?

Een primitief element van $\mathbb{K}$ is een voortbrenger van de (multiplicatieve) groep K^*. Expliciet: het is een element $g \in K^*$ van orde $\#K^*$.

(ii) Primitieve elementen komen aan bod in het *Diffie-Hellman protocol* voor sleuteluitwisseling in cryptografie. Leg dit protocol bondig uit.

Publiek gegeven: een (groot) priemgetal p en een primitief element $g \in \mathbb{Z}_p$. Twee deelnemers A en B kiezen elk een getal (a en b, respectievelijk) tussen 0 en p. Deze keuze houden ze elk voor zich geheim. A berekent $g^a \,(mod\ p)$ en B berekent $g^b \,(mod\ p)$. Ze maken beide hun resultaat bekend. A kent nu g^b en a en berekent $k := (g^b)^a \,(mod\ p)$. B kent g^a en b en berekent $k := (g^a)^b \,(mod\ p)$.

(b) Zoek methodisch een primitief element in $\mathbb{Z}/(13)$. (Goede toelichting scoort.)

De orde van een element van $\mathbb{Z}_{13}^*$ is een deler van de orde 12 van de groep: 1, 2, 3, 4, 6, of 12. We controleren alleen deze tussenmachten.

e	1	2	3	4	6
g^e	2	4	8	3	12
			$\equiv -5$		$\equiv -1$

(standaard representanten)

De eerste poging ($g=\bar{2}$) is meteen raak (orde 12).

(c) In het lichaam $(\mathbb{Z}/(3)[X])/(X^3-X+1)$ is $\alpha := \bar{X}$ een primitief element. Controleer dit. (Goede toelichting scoort.)

De veelterm $F := X^3-X+1$ is kennelijk irreducibel modulo 3. Het lichaam $\mathbb{K} := (\mathbb{Z}/3\mathbb{Z}[X])/(F)$ heeft $3^3=27$ elementen, dus K^* heeft 26 elementen.

Mogelijke ordes van een element van K^* zijn: $1, 2, 13, 26$. Duidelijk is dat X^2 en X^3 niet $\bar{1}$ zijn. We berekenen enkel X^{13} en maken handig gebruik van $X^3 \equiv X-1 \,(mod\ m)$. Exponent in binair: $13=(1101)_2$. Dat geeft de instructieketen "xsxssx".

e	0	1	2	3	6	12	13
X^e	$\bar{1}$	X	X^2	X^3	$(X-1)^2$	$X^4-X^3-X+\bar{1}$	$-\bar{1}$
				$\equiv X-1$	$\equiv X^2+X+\bar{1}$	$\equiv X^2-1$	

De eerste exponent e met $X^e \equiv \bar{1}$ is dus $e=26$ en $\alpha=\bar{X}$ is bijgevolg primitief.

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 $ggd(a, b) = 1$ 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 $x \cdot a + y \cdot b = ggd(a, b)$. ☞ DEZE

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. ☞ DEZE
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 $g^k = e$. ☞ DEZE
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. ☞ DEZE
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. ☞ DEZE

6.6. Er bestaat géén lichaam met
o 13 elementen.
o 15 elementen. ☞ DEZE
o 16 elementen.
o 17 elementen.