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:

(i) Zij $m \geq 2$ een geheel getal. Geef het relatievoorschrift voor de relatie *x is congruent met y modulo m*.

x is congruent met y modulo m, in symbolen, $x \equiv y \,(mod\, m)$, betekent: $m \mid y - x$ (m is een deler van $y - x$).

(ii) Laat a, b gehele getallen ongelijk nul zijn. Wat zegt de *Bezout formule* over deze getallen?

Gegeven $a, b \neq 0$ in $\mathbb{Z}$ bestaan $x, y \in \mathbb{Z}$ met

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

Het rechterlid is de grootste gemene deler van a, b.

(iii) De *ISBN code* bestaat uit een aantal symbolen (cijfers 0-9 of 'x' voor '10'). Het laatste symbool is een "check" symbool. Wat is de check voorwaarde?

Laat $(a_i)_{i=1}^{10}$ de code voostellen. Dan moet

$$\sum_{i=1}^{10} i \cdot a_i = a_1 + 2 \cdot a_2 + .. + 10 \cdot a_{10} \equiv 0 \,(mod\, 11).$$

(b) In $\mathbb{Z}/(65)$ met vermenigvuldiging zoeken we naar de inverse van een klasse x. Completeer de volgende tabel. Antwoorden volstaan.

x is:	inverse ja/nee:	(zo ja) inverse is:
$\overline{25}$	nee	--
$\overline{26}$	nee	--
$\overline{27}$	ja	$-12 \equiv 53$

(c) (opgave 1:14) Los het volgende stelsel vergelijkingen op (modulus 31):

$$\begin{cases} \bar{6} \cdot x + \overline{11} \cdot y = \bar{0} \\ \bar{5} \cdot x + \bar{3} \cdot y = \bar{3} \end{cases}$$

Nuttige veelvouden van de modulus: 31 62 93 124 155.

Eliminatie methode:

(1) $\bar{6} \cdot x + \overline{11} \cdot y = \bar{0}$

(2) $\bar{5} \cdot x + \bar{3} \cdot y = \bar{3}$

(1)-(2): $x + \bar{8} y = -\bar{3}$, dus $x = -\bar{3} - \bar{8} y$ (3).

Gelijkheid (3) in (1): $\bar{6}(-\bar{3} - \bar{8} y) + \overline{11} y = \bar{0}$, dus $\overline{13} - \bar{6} y = \bar{0}$.

De inverse van $\bar{6}$ is $-\bar{5}$. Dus $y = -\bar{5} \cdot \overline{13} = -\bar{3}$.

Dit geeft tenslotte: $x = -\bar{3} - \bar{8}(-\bar{3}) = -\overline{10}$. Resultaat: $x = -\overline{10}$, $y = -\bar{3}$.

Matrix rekening:

We hebben nodig: de matrix M van het stelsel en zijn determinant.

$$M := \begin{pmatrix} \bar{6} & \overline{11} \\ \bar{5} & \bar{3} \end{pmatrix}; \quad det(M) = \overline{18} - \overline{55} = -\bar{6};$$

Inverse determinant: $(-\bar{6})^{-1} = \bar{5}$.

$$M^{-1} = \bar{5}\cdot\begin{pmatrix} \bar{3} & -\overline{11} \\ -\bar{5} & \bar{6} \end{pmatrix} = \begin{pmatrix} \overline{15} & \bar{7} \\ \bar{6} & -\bar{1} \end{pmatrix}.$$

Oplossing:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \overline{15} & \bar{7} \\ \bar{6} & -\bar{1} \end{pmatrix}\cdot\begin{pmatrix} \bar{0} \\ \bar{3} \end{pmatrix} = \begin{pmatrix} -\overline{10} \\ -\bar{3} \end{pmatrix}.$$

2. Groepen

(a) Algemene kennis:

(i) Je heb een groep van orde 29 en een element x dat niet het neutrale element is. Wat weet je van de *orde van x?*

De orde is een deler van 29 en is niet 1 ($\rightarrow$ neutraal element). Omdat 29 een priemgetal is, moet de orde van de gegeven x wel 29 zijn.

(ii) Laat $m \geq 2$ geheel zijn. Welke informatie wordt er weergegeven met de *Euler functie* $\phi(m)$*?*

$\phi(m)$ is het aantal getallen x met $0 \leq x < m$ en $ggd(x, m) = 1$.
Alternatief: $\phi(m)$ is het aantal elementen van de multiplicatieve groep $\mathbb{Z}_m^*$. Dat is ook het aantal priemrestklassen modulo m.

(iii) Formuleer de *Chinese reststelling* in een situatie waar je precies twee moduli m_1, m_2 hebt.

Laat de getallen $m_1, m_2 \geq 2$ relatief priem zijn, en laat $a_1, a_2 \in \mathbb{Z}$. Dan is het stelsel vergelijkingen

$$x \equiv a_1 \,(mod\, m_1), \quad x \equiv a_2 \,(mod\, m_2)$$

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

(b) Zoek een geheel getal x dat tegelijk voldoet aan $x \equiv 11\,(mod\,14)$ en $x \equiv 8\,(mod\,15)$ (goede toelichting scoort).

De moduli $m_1 := 14$ en $m_2 := 15$ (met product 210) zijn relatief priem. Er bestaan dus getallen x_1 en x_2 met $x_1 \cdot m_1 + x_2 \cdot m_2 = 1$; op zicht: $x_1 = -1$ en $x_2 = 1$. Met $a_1 := 11$ en $a_2 := 8$ is de formule voor de oplossing:

$$x \equiv a_1 x_2 m_2 + a_2 x_1 m_1 \,(mod\, m_1 \cdot m_2).$$

Dat geeft: $x = 11 \cdot 1 \cdot 15 + 8 \cdot (-1) \cdot 14 = 165 - 112 = 53\,(mod\,210)$.

(c) Bereken $10^{74}\,(mod\,51)$ op een economische manier (goede toelichting scoort).

Berekening ϕ-functie: $\phi(51) = \phi(3) \cdot \phi(17) = 2 \cdot 16 = 32$.
$ggd(10, 51) = 1$ dus (Euler) $10^{32} \equiv 1$ modulo 51.
Exponent reduceren: $74 = 2 \cdot 32 + 10$ --> $10^{74} \equiv 10^{10}$.
Exponent in binair: 10 = "1010" --> instructie "xssxs".
Resultaat: 1--x-->10--s-->100=-2--s-->4--x-->40=-11--s-->121=19.

Zonder reductie via de Euler stelling is het rekenwerk wat omvangrijker:
74 = "1001010" --> instructie "xsssxssxs".
1--x-->10--s-->100=-2--s-->4--s-->16--x-->160=7--s-->49=-2--s-->4--x-->40=-1

3. Veeltermringen

(a) Algemene kennis:

(i) In sommige veeltermringen $R[X]$ geldt de *gradenformule.* Wat zegt deze formule en voor welk type van ringen R is ze geldig?

Graad van $F \cdot G$ is graad van F + graad van G: geldig voor veeltermen met coefficienten in een ITG (integriteitsgebied).

(ii) Gegeven zijn: een lichaam K en twee veeltermen $A, B \in K[X]$ ongelijk nul. Het *Delingsalgoritme* zegt iets over een formule van de vorm $A = B \cdot Q + R$. Wat wordt er precies gezegd?

Gegeven $A, B \in K[X] \setminus \{0\}$ is er een uniek paar veeltermen Q (quotient) en R (rest) die voldoen aan $A = B \cdot Q + R$ en hetzij $R = 0$ hetzij $deg(R) < deg(B)$.

(iii) Leg bondig uit hoe de *CRC* (*Cyclic Redundancy Check*) functioneert: sleutel, codering, decodering. Je hoeft niets aan te tonen.

(b) Zij K een lichaam. Laat zien dat een veelterm $P \in K[X]$ van graad ≥ 1 geen (multiplicatieve) inverse kan hebben in $K[X]$ (goede toelichting scoort).

Als P een inverse zou hebben (zeg: de veelterm Q), dan zou $P \cdot Q = 1$ en dus $deg(P \cdot Q) = 0$. Maar een lichaam is een ITG en dus geldt de gradenformule: $0 = deg(P \cdot Q) = deg(P) + deg(Q)$. Dit kan niet want $deg(P) \geq 1$ en $deg(Q) \geq 0$.

(c) Zij $K := \mathbb{Z}/(2)$. Het is bekend dat $X^2 + X + \bar{1}$ de enige tweedegraadse irreducibele veelterm is in $K[X]$ (niet aantonen). Gebruik dit resultaat om aan te tonen dat $M := X^4 + X^3 + \bar{1}$ irreducibel is in $K[X]$.

De veelterm M heeft geen nulpunten (vul $\bar{0}$ en $\bar{1}$ in). Dus heeft M geen ontbinding van de vorm 1e graads $\times$ 3e graads. Als er een ontbinding 2e graads $\times$ 2e graads is, dan moeten de 2e graads factoren wel irreducibel zijn (anders krijgen we een 1e graads factor van M!). We proberen de enige kandidaat en voeren de staartdeling uit:

```
X2  +X  +1  /  X4  +X3            +1  \  X2      +1
           -   X4  +X3  +X2
               ——  ———  ———  ——  ——
                        X2       +1
                    -   X2  +X   +1
                        ———  ——  ——
                             X
```

De rest is niet nul, dus heeft M geen enkele echte ontbinding.

4. Vector ruimten

(a) Algemene kennis:

(i) Wat bedoelt men met een *lineair onafhankelijk stel vectoren* $\{v_1, .., v_n\}$ in een vector ruimte V over een lichaam $\mathbb{F}$?

Een stel vectoren $v_1, v_2, .., v_n \in V$ heet lineair onafhankelijk wanneer de betrekking

$$\lambda_1 v_1 + \lambda_2 v_2 + .. + \lambda_n v_n = \mathbf{0}$$

in de onbekende scalairen $\lambda_1, \lambda_2, .., \lambda_n \in \mathbb{F}$ uitsluitend opgaat voor $\lambda_1 = \lambda_2 = .. = \lambda_n = 0$.

(ii) Wat bedoelt men met een *voortbrengend stel vectoren* $\{v_1, .., v_n\}$ in een vector ruimte V over een lichaam $\mathbb{F}$?

De vectoren $v_1, v_2, .., v_n \in V$ vormen een voortbrengend stel wanneer iedere vector $v \in V$ te schrijven is in de vorm

(*) $v = \lambda_1 v_1 + \lambda_2 v_2 + .. + \lambda_n v_n$

met $\lambda_1, \lambda_2, .., \lambda_n \in \mathbb{F}$.

(iii) Wat bedoelt men met *een basis* in een vector ruimte V over een lichaam $\mathbb{F}$?

Een basis is een onafhankelijk en voortbrengend stel vectoren.

(b) We bekijken de volgende drie vectoren achtereenvolgens over $\mathbb{Z}/(3)$ en $\mathbb{Z}/(5)$:

$$u := \begin{pmatrix} \bar{0} \\ \bar{1} \\ \bar{2} \end{pmatrix}, \quad v := \begin{pmatrix} \bar{1} \\ \bar{2} \\ \bar{0} \end{pmatrix}, \quad w := \begin{pmatrix} \bar{2} \\ \bar{0} \\ \bar{1} \end{pmatrix}.$$

Laat zien dat $\{u, v, w\}$ lineair afhankelijk is in $(\mathbb{Z}/(3))^3$, maar lineair onafhankelijk in $(\mathbb{Z}/(5))^3$. Beredeneer dat het in dit geval zelfs om een basis gaat.

In $(\mathbb{Z}/(3))^3$ zijn de vectoren lineair afhankelijk, want $u + v + w = \mathbf{0}$.

In $(\mathbb{Z}/(5))^3$ zijn de vectoren lineair onafhankelijk. Stel namelijk dat $\alpha \cdot u + \beta \cdot v + \xi \cdot w = \mathbf{0}$ $(\alpha, \beta, \xi \in \mathbb{Z}/(5))$.

Dat geeft drie betrekkingen:

(1) $\beta + \bar{2}\xi = \bar{0}$

(2) $\alpha + \bar{2}\beta = \bar{0}$

(3) $\bar{2}\alpha + \xi = \bar{0}$

(3) in (1) geeft $\beta = \bar{4}\alpha$. Dit in (2) geeft $\alpha = -\bar{8}\alpha = \bar{2}\alpha$. Hieruit $\alpha = \bar{0}$ en meteen ook $\beta = \xi = \bar{0}$.

In $(\mathbb{Z}/(5))^3$ is $\{u, v, w\}$ dus lineair onafhankelijk. Zo'n collectie kan worden aangevuld tot een basis voor $(\mathbb{Z}/(5))^3$ (via het uitwisselingslemma). Maar de dimensie van deze ruimte is 3; er kan dus geen vector bij. Daarom is de gegeven collectie een basis voor $(\mathbb{Z}/(5))^3$.

(c) Neem nu de volgende 3 bij 5 matrix over $\mathbb{Z}/(5)$.

$$M := \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{1} & \bar{2} \\ \bar{1} & \bar{2} & \bar{0} & \bar{1} & \bar{1} \\ \bar{2} & \bar{0} & \bar{1} & \bar{1} & \bar{2} \end{pmatrix}.$$

Bepaal de dimensie van de nulruimte van M (goede toelichting scoort).

N.B.: de eerste drie kolommen zijn precies de vectoren uit deel (b); je mag de resultaten uit dat onderdeel indien nodig hier gebruiken.

Met het resultaat uit onderdeel (b) weten we dat de kolomruimte van dimensie 3 is. Volgens de dimensiestelling is de dimensie van de nulruimte dan $5 - 3 = 2$.

5. Eindige lichamen

(a) Algemene kennis.

(i) Wat is een *primitief element* van een eindig lichaam?

Een voortbrenger van de multiplicatieve groep. Zo'n voortbrenger bestaat omdat het lichaam eindig is.

(ii) Welke getallen $m \geq 2$ komen in aanmerking als het *aantal elementen* van een eindig lichaam, en welke niet?

Machten van priemgetallen.

(iii) Leg bondig uit: het *Diffie-Hellman protocol* voor sleuteluitwisseling.

1. Twee deelnemers A en B komen een (groot) priemgetal p overeen alsook een voortbrenger (primitief element) g van het getallensysteem modulo p. Deze keuzes hoeven niet geheim te zijn.
2. Ieder kiest voor zich een willekeurig getal tussen 0 en p. Deelnemer A kiest a en deelnemer B kiest b. Deze keuze houden ze elk voor zich geheim.
3. A berekent $g^a \pmod p$ en B berekent $g^b \pmod p$, en ze maken beide hun resultaat bekend.
4. A kent nu g^b en a en berekent $k := (g^b)^a \pmod p$. B kent g^a en b en berekent $k := (g^a)^b \pmod p$.

Het getal k is de gemene sleutel.

Voor de rest van deze opgave bekijken we de veelterm $M := X^3 + X + \bar{1} \in \mathbb{Z}_2[X]$ en de quotiëntring $\mathbb{F} := \mathbb{Z}_2[X]) / (M)$.

(b) Laat zien dat M irreducibel is. Volgens de theorie is de quotiëntring $\mathbb{F}$ dus een lichaam (niet aantonen). Controleer nu dat $\alpha := \bar{X}$ een *primitief element* is van het lichaam $\mathbb{F}$. Goede toelichting scoort.

$\mathbb{F}$ heeft $2^3 = 8$ elementen, $\mathbb{F}^*$ heeft er dan 7. De (multiplicatieve) orde van een element van $\mathbb{F}^*$ is dus een deler van 7. Orde 1 heeft alleen het neutrale element $\bar{1}$; ieder ander element heeft orde 7. Ihb is $\alpha \neq \bar{1}$ primitief.

(c) Maak een *tabel* waarin de elementen van $\mathbb{F}^*$ weergegeven zijn als (i) macht van α, (ii) een veelterm, (iii) een 3-bit code. Geef voldoende toelichting; je hoeft je berekeningen niet te tonen.

Elk element van $\mathbb{F}^*$ heeft een standaard representant

$c_2 X^2 + c_1 X + c_0 \quad (c_0, c_1, c_2 \in \mathbb{Z}_2)$

die we weergeven met de 3-bit code (c_2, c_1, c_0).

Merk op:

- $\bar{X}^3 + \bar{X} + \bar{1} = \bar{0}$. In de berekeningen mag je dus overal X^3 vervangen door $X + \bar{1}$.
- Bij rekenen modulo 2 zijn geen min-tekens nodig!
- α^7 is het eenheidselement. Dus, in een macht van α mag bij de exponent altijd ± 7 worden toegevoegd.

Dit levert de volgende tabel op voor $\mathbb{F}^*$.

α^0	$\bar{1}$	001	α^4	X^2+X	110
α^1	X	010	α^5	$X^2+X+\bar{1}$	111
α^2	X^2	100	α^6	$X^2+\bar{1}$	101
α^3	$X+1$	011	α^7	$\bar{1}$	001

(d) Bereken efficiënt met behulp van je tabel:

(i) `110 * 101`

`110 is` α^4 `en 101 is` α^6`. Dus 110 * 101 is` $\alpha^4 \cdot \alpha^6 = \alpha^{10} = \alpha^3$`. Dit is 011.`

(ii) de inverse van `110`

`110 is` α^4`. De inverse is` $\alpha^{-4} = \alpha^3$`. Dit is 011.`

Normering:

1a:	4	2a:	4	3a:	4	4a:	4	5a:	4	6:	15
1b:	5	2b:	6	3b:	5	4b:	5	5b:	3		
1c:	6	2c:	5	3c:	6	4c:	5	5c:	5		
								5d:	4		
	15		15		15		14		16		15

Voor het multiple-choice deel geldt: –3 punten per fout.

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

naam, studierichting & jaar: 18-12-02

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. Welke bewering over *priemrestklassen* is waar?
o $\overline{13}$ is een priemrestklasse modulo 26.
o De som van twee priemrestklassen modulo 26 is weer een priemrestklasse modulo 26.
o Het product van twee priemrestklassen modulo 26 is weer een priemrestklasse modulo 26. ☞ DEZE
o Er zijn geen priemrestklassen modulo 26 want 26 is niet priem.

6.2. Een *deelgroep* H van een groep $(G,*)$ is
o Een deelverzameling H van G met een operatie $x\#y$, zó dat $(H,\#)$ een groep is.
o Een deelverzameling H van G die stabiel is onder de operatie $x*y$ van G.
o Een deelverzameling H van G die stabiel is onder de operatie y^{-1} (inverse) van G.
o Een deelverzameling H van G die stabiel is onder de operatie $x*y^{-1}$ van G. ☞ DEZE

6.3. De sleutel voor de cryptografische methode van *RSA* bestaat uit 5 getallen $m=p\cdot q$ (met p,q priem) en d,e, waarbij m,e publiek zijn en p,q,d privé. Aan welke voorwaarde moeten d,e voldoen:
o $ggd(m,d)=1=ggd(m,e)$.
o $d\cdot e\equiv 1\,(mod\ m)$.
o $d\cdot e\equiv 1\,(mod\ \phi(m))$. ☞ DEZE
o $\phi(d)\cdot\phi(e)\equiv 1\,(mod\ m)$.

6.4. Een *ideaal* van een commutatieve unitaire ring R is een deelverzameling van R die
o stabiel is onder de optelling $x+y$ en de vermenigvuldiging $x\cdot y$ van R.
o stabiel is onder de optelling $x+y$ en de vermenigvuldiging $x\cdot y$ van R, en die het eenheidselement van R bevat.
o stabiel is onder de optelling $x+y$ van R en sterk stabiel is onder de vermenigvuldiging $x\cdot y$ van R. ☞ DEZE
o sterk stabiel is onder de optelling $x+y$ van R en stabiel is onder de vermenigvuldiging $x\cdot y$ van R.
N.B.: Een verzameling $A\subseteq V$ is *sterk stabiel* onder een bewerking $x\#y$ in V wanneer geldt: als $x\in V$ en $y\in A$ dan $x\#y\in A$.

6.5. Zij V een *vectorruimte* van *dimensie* 3 over een lichaam $\mathbb{F}$ met 4 elementen. Dan is
o $\#V=64\ (=4^3)$. ☞ DEZE
o $\#V=81\ (=3^4)$.
o $\#V=12\ (=3\cdot 4)$.
o $\#V$ onbepaald want er zijn onvoldoende gegevens.

6.6. De *karakteristiek* van een eindig lichaam K is
o de additieve orde van het eenheidselement van K. ☞ DEZE
o de multiplicatieve orde van het nulelement van K.
o de orde van de additieve groep K.
o de orde van de multiplicatieve groep K^*.