Algebra & Security, code 151141

Datum : 29-06-2010
Zaal : SP 5
Tijd : 08:45-11:45

Schrijf de uitwerkingen van de vraagstukken 1-2-3 (algebradeel) en de vraagstukken 4-5 op aparte papieren, dit in verband met parallelle correctie.
Motiveer al uw antwoorden
Besteed niet te veel tijd aan een afzonderlijk onderdeel. Indien u een onderdeel niet kunt oplossen dan kunt het resultaat van dat onderdeel in latere onderdelen toch gebruiken.

1. Zij G de verzameling matrices gegeven door:

$$G = \{\begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix} \mid \alpha, \beta \in \mathbb{R} \ \ \alpha^2 + \beta^2 \neq 0\}.$$

   Op G beschouwen we de bewerking matrixvermenigvuldiging.

   (a) Laat zien dat G met matrixvermenigvuldiging een groep is.

   (b) Laat zien dat G isomorf is met $(\mathbb{C}\backslash\{0\}, \cdot)$, de complexe getallen ongelijk nul met vermenigvuldiging.

2. Zij $R = \{a + bi \mid a, b \in \mathbb{Z}\}$, hierbij is i de imaginaire eenheid.

   (a) Laat zien dat R met de gewone optelling en vermenigvuldiging een ring is.

   (b) Bepaal alle eenheden van R, dat wil zeggen alle elementen van R die een inverse met betrekking tot de vermenigvuldiging hebben. Geef van elk van de door u gevonden eenheid ook de inverse.

3. Gegeven is het polynoom $p(x) = 1 + x + x^3 + x^4 + x^5 \in \mathbb{Z}_2[x]$.

   (a) Laat zien dat er geen polynomen $a(x), b(x) \in \mathbb{Z}_2[x]$ bestaan zodanig dat $a(x)b(x) = p(x)$ en $\mathrm{gr}\, a(x) = 2$ en $\mathrm{gr}\, b(x) = 3$. Hint: Laat zien dat er slechts acht paren $(a(x), b(x))$ bestaan die in aanmerking komen en probeer ze alle acht uit en concludeer dat geen enkele combinatie tot $p(x)$ leidt.

   (b) Beredeneer dat $p(x)$ irreducibel is.

Definieer $\mathbb{F} = \mathbb{Z}_2[x]/\langle p(x) \rangle$

(c) Is $\mathbb{F}$ een lichaam?

(d) Hoeveel elementen heeft $\mathbb{F}$?

(e) Wat is de dimensie van $\mathbb{F}$ als vectorruimte over $\mathbb{Z}_2$?

(f) Laat $\mathbb{K}$ een lichaam zijn van dimensie d als vectorruimte over $\mathbb{Z}_2$ en $\mathbb{Z}_2 \subset \mathbb{K} \subset \mathbb{F}$.

Hoeveel elementen heeft $\mathbb{K}$? Wat is de dimensie van $\mathbb{F}$ opgevat als vectorruimte over $\mathbb{K}$? Concludeer dat er geen lichamen strikt tussen $\mathbb{Z}_2$ en $\mathbb{F}$ zitten.

(g) Stel $\mathbb{L}$ is een deellichaam van $\mathbb{M}$, i.e., $\mathbb{L} \subset \mathbb{M}$. Zij verder gegeven dat de dimensie van $\mathbb{M}$ opgevat als vectorruimte over $\mathbb{L}$ gelijk is aan n. Onder welke voorwaarde op n bestaat er geen lichaam $\mathbb{K}$ zodanig dat

$$\mathbb{L} \subsetneq \mathbb{K} \subsetneq \mathbb{M}?$$

4. Consider a 2x2 Hill cipher over Z_{26}. (Hint: affine cipher)

(a) Which of the following matrices can be used as a key in such a Hill cipher: $Key1 = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}$ or $Key2 = \begin{pmatrix} 2 & 17 \\ 8 & 3 \end{pmatrix}$? Explain why. (5p)

(b) Suppose that the plaintext "twente" is encrypted to the ciphertext "xzcdjx". Find the key using a known plaintext attack and verify it. (8p)

5. Consider RSA encryption scheme with primes $p = 11$, $q = 23$ and public exponent $e = 3$.

(a) Compute the corresponding private key d. Can $e = 11$ be used as a public exponent? Explain why. (5p)

(b) Demonstrate the RSA encryption scheme by encrypting the string 11100 (in binary form) and decrypt back the obtained ciphertext. (7p)

(c) Demonstrate the RSA signature scheme (without hash function) by signing the string 111000 (in binary form) and then verify the signature. (7p)

5. Ga uit van een 2x2 Hill cipher over Z_{26}. (Hint: affine cipher, matrices over Z_{26})

(a) Welke van de volgende matrices kan gebruikt worden als een key in zo'n Hill cipher: $Key1 = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}$ of $Key2 = \begin{pmatrix} 2 & 17 \\ 8 & 3 \end{pmatrix}$? Leg uit waarom. (5p)

(b) Stel dat de plaintext "twente" is ge-encrypt tot de ciphertext "xzcdjx". Vind de key door gebruik te maken van een known plaintext attack en verifieer deze. (8p)

Probleem 2:

6. Ga uit van een RSA encryption schema met priemgetallen $p = 11$, $q = 23$ en public exponent $e = 3$.

   (a) Bereken de corresponderende private key d. Kan $e = 11$ gebruikt worden als een public exponent? Leg uit waarom. (5p)

   (b) Demonstreer het RSA encryption schema door de string 11100 (in binaire vorm) te encrypten en decrypt de resulterende ciphertext. (7p)

   (c) Demonstreer het RSA signature schema (zonder hash function) door de string 111000 (in binaire vorm) te signen en verifieer de signature. (7p)

Puntenverdeling:

1		2		3							4		5		
a	b	a	b	a	b	c	d	e	f	g	a	b	a	b	c
9	9	8	8	5	4	3	3	3	3	3	5	8	5	7	7

Voor een voldoende dient het puntentotaal voor de vragen 1-3 minimaal 22 en voor de vragen 4-5 minimaal 14 te zijn.
Als aan deze voorwaarde voldaan is dan wordt het tentamencijfer:
Cijfer: $1 + 9\frac{\text{punten}}{80}$