University of Ruhuna

B.Sc.(General) Degree

Level III (Semester II) Examination - December 2016

Subject: Applied/ Industrial Mathematics
Course Unit: IMT321β **(Applied Algebra - Coding Theory)**
Time: Two (02) Hours

Answer 04 Questions only. Calculators will be provided.

---

1. a) State the Little Fermat's theorem.
Using the above theorem, find $4^{532} \mod 11$.

b) Explain the terms

(i) Encryption

(ii) Decryption

used in cryptosystems.

c) In a Caesar cipher, the encryption and decryption functions are given by

$$c = e_k(m) \quad \text{and} \quad m = d_k(c) = d_k(e_k(m)),$$

respectively, where m is the plaintext message, c is the resulting ciphertext, e is the encryption function, d is the decryption function and k is the key.
Let us consider the English alphabet with letters represented as
$A = 0, B = 1, \cdots, Z = 25$.

(i) Write down the encryption function $c = e_k(m)$ and decryption function $m = d_k(c)$ explicitly.

(ii) Suppose that the following ciphertext encrypted using Caesar cipher with $k = 11$ has been received by you.

OPALCEXPYE ZQ XLESPXLETND

Decrypt the above ciphertext to obtain the original message ignoring the spaces.

---

2. a) In the RSA public key cryptosystem, explain

(i) key generation

(ii) the encryption algorithm

(iii) the decryption algorithm

b) (i) Let the primes p and q be 7 and 13 respectively. Choosing the encryption key, e as 5, find the decryption key d.

(ii) Encrypt the message $m = 10$. Decrypt the ciphertext you obtained.

Continued.

3. a) Find $Q(x)$ and $R(x)$ such that $f(x) = Q(x)g(x) + R(x)$, where $\deg(R(x)) < \deg(g(x))$, if

(i) $f(x) = x^3 + x + 1$ and $g(x) = x^2 + x + 1$ in $\mathbb{F}_2[x]$,

(ii) $f(x) = x^6 + x^4 + x + 1$ and $g(x) = 2x^3 + x + 3$ in $\mathbb{F}_5[x]$.

b) Find the greatest common divisor (gcd) of $f(x) = x^5 + x^3 + x + 1$ and $g(x) = x^4 + x^2 + x + 1$ in $\mathbb{F}_2[x]$ using the Euclidean algorithm.

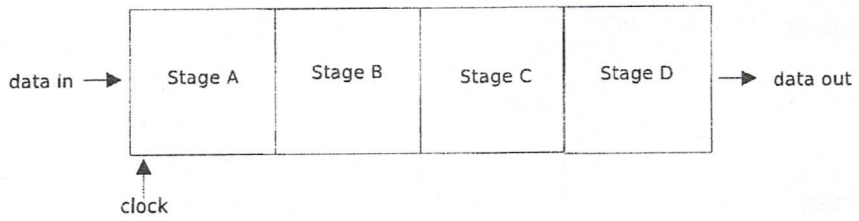
c) (i) Define "an irreducible polynomial" over a field.

(ii) Consider the irreducible polynomial $x^2 + x + 1$ in $\mathbb{F}_2[x]$. Find the residue classes of $\dfrac{\mathbb{F}_2[x]}{x^2 + x + 1}$.

(iii) Construct the addition and multiplication tables for $\dfrac{\mathbb{F}_2[x]}{x^2 + x + 1}$.

---

4. a) Explain the process of data transfering inside the following Serial-in Serial-out shift register with 4 stages.



b) (i) Find the recurrence relation for the function $t^2 + t + 1$ in $\mathbb{F}_3[t]$.

(ii) Write down all possible pairs of initial conditions in $\mathbb{F}_3$ for the recurrence relation in part(i) above, and find the first 10 terms corresponding to each pair. Hence determine the periods.

(iii) For each of the period find the corresponding minimal polynomial.

---

5. a) (i) Define ISBN code in the usual notation.

(ii) What is the minimum distance of the ISBN code?

(iii) Is the following string is a valid ISBN? Justify your answer.

$$0 - 1316 - 5332 - 6$$

b) Define the following terms.

(i) Hamming distance $d(x_1, x_2)$ between two codewords x_1 and x_2.

(ii) Minimum (Hamming) distance $d(A)$ of a code A.

(iii) Hamming weight $w(x)$ of a codeword x.

Continued.

Let $A = \{x_1, x_2, x_3\}$ be the following code over $\mathbb{F}_2$.

$$x_1 = (0000), \quad x_2 = (0111), \quad x_3 = (1010)$$

(α) Find the hamming distance between each pair.

(β) Find the minimum(hamming) distance of the code A.

(γ) Express the code A in the form $[n, k, d]$.

c) What do you mean by the following phrases?

(i) C is a $t-$error detecting code,

(ii) C is a $t-$error correcting code.

The Mariner 9 used the binary (32,64,16) code to transmit pictures from Mars to earth. Determine how many errors it can correct.

d) (i) State the Sphere-packing and Singleton bounds for a $t-$error correcting $q-$ary $[n, k]$ linear code.

(ii) What are perfect codes and Maximum Distance Seperable (MDS) codes?

(iii) Is the binary $[11, 8, 5]$ code both perfect and MDS? Justify your answer.

---

6. a) Let C be a (5,2) binary code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

(i) Write down the code C.

(ii) Find the cosets of C.

(iii) Obtain the parity check matrix H associated with G.

(iv) Construct the Slepian standard array for this problem.

(v) Extend the standard array in part(iv) by listing the syndromes of each coset leader in an extra column on the right.

(vi) Hence, decode the following received codewords.

(α) 11111

(β) 01011

b) What is the meaning of even parity and odd parity?
Explain each term by giving an example.

Last Page

රුහුණ විශ්වවිද්‍යාලය

සාමාන්‍ය විද්‍යා උපාධි

තෙවන ස්ථලය (දෙවන සමාසික) පරීක්ෂණය - 2016 දෙසැම්බර්

විෂයය: ව්‍යාවහාරික/ කාර්මික ගණිතය
පාඨමාලා ඒකකය: IMT321β (ව්‍යාවහාරික වීජය - කේතකරණ වාදය)
කාලය: පැය දෙකයි (02)

ප්‍රශ්න 04 කට පමණක් පිළිතුරු සපයන්න. ගණක යන්ත්‍ර සපයනු ලැබේ.

---

1. අ) Little Fermat ගේ ප්‍රමේයය ප්‍රකාශ කරන්න.
ඉහත ප්‍රමේයය භාවිතයෙන් $4^{532} \mod 11$ සොයන්න.

ආ) cryptosystems හි භාවිතා වන
(i) Encryption
(ii) Dedryption
යන පද පැහැදිලි කරන්න.

ඇ) Caesar cipher හි encryption සහ decryption ශ්‍රිත පිළිවෙලින්

$$c = e_k(m) \quad \text{සහ} \quad m = d_k(c) = d_k(e_k(m))$$

මෙහින් දෙනු ලබන අතර මෙහි m යනු plaintext පණිවිඩයද, c යනු ciphertext ද, e යනු encryption ශ්‍රිතයද, d යනු decryption ශ්‍රිතයද, k යනු යතුර (key) ද වේ.
අකුරු $A = 0, B = 1, \cdots, Z = 25$ ලෙස දැක්වූ ඉංග්‍රීසි හෝඩිය (English alphabet) සලකමු.
(i) encryption ශ්‍රිතය $c = e_k(m)$ සහ decryption ශ්‍රිතය $m = d_k(c)$ ප්‍රකාශිත ලෙස ලියා දක්වන්න.
(ii) $k = 11$ සහිත Caesar cipher භාවිතයෙන් encrypt කළ පහත දැක්වෙන ciphertext ඔබට ලැබී ඇතැයි සිතන්න.

OPALCEXPYE ZQ XLESPXLETND

හිස් අවකාශ නොසලකා හරිමින් මුල් පණිවිඩය ලබා ගැනීම සඳහා ඉහත ciphertext decrypt කරන්න.

---

2. අ) RSA public key cryptosystem හි එන
(i) යතුරු ජනනය (key generation)
(ii) කේතකරණ ඇල්ගොරිතමය (the encryption algorithm)
(iii) විකේතකරණ ඇල්ගොරිතමය (the decryption algorithm)
පැහැදිලි කරන්න.

සම්බන්ධිතයි.

ආ) (i) p සහ q ප්‍රථමක සංඛ්‍යා පිළිවෙළින් 7 සහ 13 ලෙස ගනිමු. encryption යතුර e යන්න 5 ලෙස ගෙන decryption යතුර d සොයන්න.

(ii) $m = 10$ encrypt කරන්න. ඔබ ලබාගත් ciphertext decrypt කරන්න.

---

3. අ) (i) $\mathbb{F}_2[x]$ තුළ $f(x) = x^3 + x + 1$ සහ $g(x) = x^2 + x + 1$,

(ii) $\mathbb{F}_5[x]$ තුළ $f(x) = x^6 + x^4 + x + 1$ සහ $g(x) = 2x^3 + x + 3$

නම් $f(x) = Q(x)g(x) + R(x)$ වන පරිදි $Q(x)$ සහ $R(x)$ සොයන්න.

මෙහි $\deg(R(x)) < \deg(g(x))$ වේ.

ආ) Euclidean ඇල්ගොරිතමය භාවිතයෙන් $\mathbb{F}_2[x]$ තුළ $f(x) = x^5 + x^3 + x + 1$ සහ $g(x) = x^4 + x^2 + x + 1$ හි මහා පොදු භාජකය (greatest common divisor(gcd)) සොයන්න.

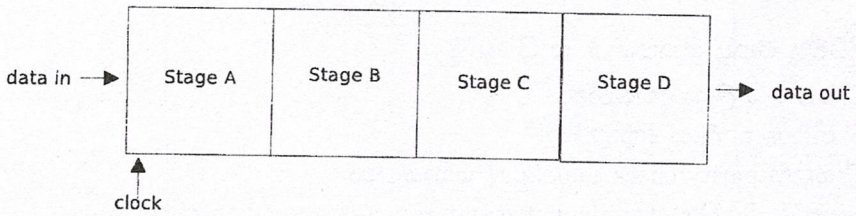
ඇ) (i) ක්ෂේත්‍රයක් පිරිවසා අනූනනීය බහුපදයක් (irreducible polynomial) අර්ථ දක්වන්න.

(ii) $\mathbb{F}_2$ පිරිවසා $x^2 + x + 1$ අනූනනීය බහුපදය (irreducible polynomial) සලකන්න. $\dfrac{\mathbb{F}_2[x]}{x^2 + x + 1}$ හි අවශිෂ්ඨ පන්ති (residue classes) සොයන්න.

(iii) $\dfrac{\mathbb{F}_2[x]}{x^2 + x + 1}$ සඳහා ආකලන සහ ගුණන වගු ගොඩනගන්න.

---

4. අ) පහත දක්වා ඇති අවස්ථා 4 කින් සමන්විත ශ්‍රේණිගත ඇතුලුවීම (serial-in) සහ ශ්‍රේණිගත පිටවීම (serial-out) සහිත shift regisetrs හි දත්ත හුවමාරු වීමේ ක්‍රියාවලිය පැහැදිලි කරන්න.



ආ) (i) $\mathbb{F}_3[t]$ තුළ $t^2 + t + 1$ ශ්‍රිතය සඳහා පුනරාවර්ත සම්බන්ධතාවය (recurrence relation) සොයන්න.

(ii) ඉහත (i) කොටසෙහි ඇති පුනරාවර්ත සම්බන්ධතාවයේ, $\mathbb{F}_3$ තුළ ඇති සියලුම වියහැකි ආරම්භක අවශ්‍යයතා යුගල ලියා දක්වා, එක් එක් යුගලට අනුරූප පළමු පද 10 සොයන්න.
එමඟින් ආවර්තයන් නිර්ණය කරන්න.

(iii) ලබාගත් එක් එක් ආවර්තය සඳහා අනුරූප minimal polynomials සොයන්න.

---

5. අ) (i) සුපුරුදු අංකනයෙන් ISBN කේතය අර්ථ දක්වන්න.

(ii) ISBN කේතයේ අවම දුර කුමක්ද?

(iii) $0 - 1316 - 5332 - 6$ වලංගු ISBN කේතයක්ද? ඔබගේ පිළිතුර පැහැදිලි කරන්න.

ආ) පහත දැක්වෙන පද අර්ථ දක්වන්න.

(i) x_1 සහ x_2 කේතවචන දෙක අතර හැමිං දුර (Hamming distance), $d(x_1, x_2)$.

(ii) A කේතයක අවම (හැමිං) දුර (Minimum (Hamming) distance), $d(A)$.

(iii) x කේතවචනයක හැමිං බර (Hamming weight) $w(x)$.

සම්බන්ධිතයි.

$\mathbb{F}_2$ පිරිවසා $A = \{x_1, x_2, x_3\}$ යනු පහත දැක්වන කේතයන් යැයි ගනිමු.

$$x_1 = (0000) \quad x_2 = (0111) \quad x_3 = (1010)$$

(α) එක් එක් යුගල් අතර ඇති හැමිං දුර (Hamming distance) සොයන්න.

(β) A කේතයෙහි අවම (හැමිං) දුර (Minimum (Hamming) distance) සොයන්න.

(γ) A කේතය $[n, k, d]$ ආකාරයෙන් ප්‍රකාශ කරන්න.

ඇ) පහත දැක්වෙන phrases මඟින් ඔබ අදහස් කරන්නේ කුමක්ද?

(i) C යනු $t-$error detecting කේතයක් වේ

(ii) C යනු $t-$error correcting කේතයක් වේ.

අභාහරු සිට පෘථිවියට ඡායාරූප සම්ප්‍රේෂණය සඳහා Mariner 9 යානය විසින් (32,64,16) ද්විමය කේතයක් භාවිතා කරන ලදී. එම කේතයට දෝෂ කොපමණ සංඛ්‍යාවක් නිවැරදි කළ හැකිදැයි නිර්ණය කරන්න.

ඈ) (i) $t-$error correcting $q-$ary $[n, k]$ ඒකජ කේතයක් සඳහා සුපුරුදු අංකනයෙන් Sphere packing සහ Singleton පරියන්ත ප්‍රකාශ කරන්න.

(ii) perfect සහ Maximum Distance Seperable (MDS) කේත යනු මොනවාද?

(iii) $[11, 8, 5]$ ද්විමය කේතය perfect සහ MDS වේද? ඔබේ පිළිතුර සනාථ කරන්න.

---

6. අ) C යනු ජනන න්‍යාසය

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

වන ද්විමය ඒකජ කේතයක් යැයි ගනිමු.

(i) C කේතය ලියා දක්වන්න.

(ii) C හි cosets ලියා දක්වන්න.

(iii) C සඳහා parity check matrix H සොයන්න.

(iv) මෙම ගැටලුව සඳහා Slepian standard array ගොඩනගන්න.

(v) සෑම coset leader එකකම සින්ඩ්‍රෝමය (syndrome) දකුණු පස වෙනම තීරයක ලැයිස්තුගත කරමින් ඉහත (iv) කොටසෙහි Slepian standard array විස්තීර්ණය කරන්න.

(vi) එමඟින් පහත දැක්වෙන සම්ප්‍රේෂණය වූ කේත වචන (codewords) decode කරන්න.

(α) 11111

(β) 01011

ආ) even parity සහ odd parity මඟින් කුමක් අදහස් කරයිද? උදාහරණය බැගින් දෙමින් ඔබේ පිළිතුර පැහැදිලි කරන්න.

අවසාන පිටුව.