MATH3411 INFORMATION, CODES & CIPHERS

Test 2 Session 2 2016 SOLUTIONS

Version A

Multiple choice: **e**, **b**, **a**, **d**, **b**
True/False: **F**, **T**, **T**, **T**, **F** .

1. **(e)**: 1. a, 2. b, 3. ba, 4. bab, 5. $baba$

2. **(b)**:

3. **(a)**:

4. **(d)**: $\phi(2016) = \phi(2^5)\phi(3^2)\phi(7) = (2^5 - 2^4)(3^2 - 3)6 = 576$, so by Euler's Theorem,
$$5^{1155} \equiv (5^{576})^2 \times 5^3 \equiv 1^2 \times 125 \equiv 125 \pmod{2016}.$$

5. **(b)** $\gcd(3, 121) = 1$ and $3^{15} \equiv 1 \pmod{121}$ (here, $121 = 2^3 * 15 + 1$).

6. (i) **False**: Encode the message $bb\bullet$:

	subinterval start	**width**
begin	0	1
b	0.3	0.4
b	$0.3 + 0.3 \times 0.4 = 0.42$	$0.4 \times 0.4 = 0.16$
$\bullet$	$0.42 + 0.7 \times 0.16 = 0.532$	$0.16 \times 0.3 = 0.048$

so the message encodes as a number in the interval $[0.532, 0.58)$.

(ii) **True**: The ternary entropy is approximately 0.966 .

(iii) **True**: $t = 37$ and $s = 6$, so $a = 31$ and $b = 43$.

(iv) **True**: The longest two codeword lengths are 7 and 8.

(v) **False**: There are $\phi(125 - 1) = 60$ primitive elements in GF(125).

7. (i) Here, we have that $\alpha^2 = \alpha + 1$:

$\alpha^1 = \alpha$	$\alpha^5 = 2\alpha$
$\alpha^2 = \alpha + 1$	$\alpha^6 = 2\alpha + 2$
$\alpha^3 = 2\alpha + 1$	$\alpha^7 = \alpha + 2$
$\alpha^4 = 2$	$\alpha^8 = 1$

(ii)

$$\left(\begin{array}{cc|c} \alpha^3 & \alpha^4 & \alpha^2 \\ \alpha & \alpha^6 & 1 \end{array}\right) \xrightarrow[R2 = \alpha^{-1}R2]{R1 = \alpha^5 R1} \left(\begin{array}{cc|c} 1 & \alpha & \alpha^7 \\ 1 & \alpha^5 & \alpha^7 \end{array}\right) \xrightarrow{R2 = R2 - R1} \left(\begin{array}{cc|c} 1 & \alpha & \alpha^7 \\ 0 & \alpha^5 - \alpha & 0 \end{array}\right) = \left(\begin{array}{cc|c} 1 & \alpha & \alpha^7 \\ 0 & \alpha & 0 \end{array}\right)$$
$$\xrightarrow{R1 = R1 - \alpha R2} \left(\begin{array}{cc|c} 1 & 0 & \alpha^7 \\ 0 & 1 & 0 \end{array}\right)$$

so $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha^7 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha + 2 \\ 0 \end{pmatrix}$.

(iii) $\{\alpha^5, \alpha^{15} = \alpha^7, \alpha^{21} = \alpha^5, \ldots\} = \{\alpha^5, \alpha^7\}$, so the minimal polynomial of α^5 is

$$\begin{aligned} (x - \alpha^5)(x - \alpha^7) &= x^2 - (\alpha^5 + \alpha^7)x + \alpha^5\alpha^7 \\ &= x^2 - (2\alpha + \alpha + 2)x + \alpha^4 \\ &= x^2 + x + 2\,. \end{aligned}$$

Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Version B

Multiple choice: **e**, **d**, **c**, **e**, **d**
True/False: **T**, **F**, **T**, **F**, **T** .

1. **(e)**: $1.a, \quad 2.b, \quad 3.ba, \quad 4.bb, \quad 5.bbb$

2. **(d)**:

symbol	code to use	encoded symbol
s_1	Huff_E	1
s_2	$\text{Huff}_{(1)}$	1
s_1	$\text{Huff}_{(2)}$	0
s_3	$\text{Huff}_{(1)}$	01
s_1	$\text{Huff}_{(3)}$	11

so this is encoded as $\;1100111$.

3. **(c)**:

4. **(e)**: $\phi(123) = \phi(3)\phi(41) = 2 \times 40 = 80$, so by Euler's Theorem,

$$2^{2016} \equiv (2^{80})^{25} \times 2^{16} \equiv 1^{25} \times (2^7)^2 \times 2^2 \equiv 128^2 \times 4 \equiv 5^2 \times 4 \equiv 100 \times 4 \pmod{2016}.$$

5. **(d)** $\gcd(7, 25) = 1$ and $7^{2^1 \times 3} \equiv -1 \pmod{25}$ (here $25 = 2^3 \times 3 + 1$).

Assignment Project Exam Help

6. (i) **True**: Encode the message $ab\bullet$:

	subinterval start	**width**
begin	0	1
b	0.4	0.4
a	0.4	$0.4 \times 0.4 = 0.16$
$\bullet$	$0.4 + 0.8 \times 0.16 = 0.528$	$0.2 \times 0.16 = 0.032$

https://powcoder.com

so the message encodes as a number in the interval $[0.528, 0.56)$.

(ii) **False**: The ternary entropy is approximately 0.921 .

Add WeChat powcoder

(iii) **True**: $t = 49$, $s = 12$, $a = 37$, $b = 61$.

(iv) **False**: 4

(v) **True**: $\gcd(3, 16) = 1$ and $5^3 \equiv 6 \pmod{17}$.

7. (i) Here, we have that $\alpha^2 = 2\alpha + 1$:

$$\boxed{\begin{array}{ll} \alpha^1 = \alpha & \alpha^5 = 2\alpha \\ \alpha^2 = 2\alpha + 1 & \alpha^6 = \alpha + 2 \\ \alpha^3 = 2\alpha + 2 & \alpha^7 = \alpha + 1 \\ \alpha^4 = 2 & \alpha^8 = 1 \end{array}}$$

(ii)

$$\left(\begin{array}{cc|c} \alpha^3 & \alpha^4 & \alpha^2 \\ \alpha^4 & \alpha^6 & \alpha^5 \end{array}\right) \xrightarrow[R2 = \alpha^4 R2]{R1 = \alpha^5 R1} \left(\begin{array}{cc|c} 1 & \alpha & \alpha^7 \\ 1 & \alpha^2 & \alpha \end{array}\right) \xrightarrow{R2 = R2 - R1} \left(\begin{array}{cc|c} 1 & \alpha & \alpha^7 \\ 0 & \alpha^2 - \alpha & \alpha - \alpha^7 \end{array}\right) = \left(\begin{array}{cc|c} 1 & \alpha & \alpha^7 \\ 0 & \alpha^7 & 2 \end{array}\right)$$

$$\xrightarrow{R2 = \alpha R2} \left(\begin{array}{cc|c} 1 & \alpha & \alpha^7 \\ 0 & 1 & 2\alpha \end{array}\right) \xrightarrow{R1 = R1 - \alpha R2} \left(\begin{array}{cc|c} 1 & 0 & \alpha^7 - 2\alpha^2 \\ 0 & 1 & 2\alpha \end{array}\right) = \left(\begin{array}{cc|c} 1 & 0 & 2 \\ 0 & 1 & 2\alpha \end{array}\right)$$

so $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ \alpha^5 \end{pmatrix} = \begin{pmatrix} 2 \\ 2\alpha \end{pmatrix}$.

(iii) $\{\alpha^2, \alpha^6, \alpha^{18} = \alpha^2, \dots\} = \{\alpha^2, \alpha^6\}$, so the minimal polynomial of α^5 is

$$\begin{aligned}(x - \alpha^2)(x - \alpha^6) &= x^2 - (\alpha^2 + \alpha^6)x + \alpha^8 \\ &= x^2 - (2\alpha + 1 + \alpha + 2)x + 1 \\ &= x^2 + 1\,.\end{aligned}$$