MATH3411 INFORMATION, CODES & CIPHERS

Test 2 Session 2 2014 SOLUTIONS

Version A

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

1. **(e)**:

code number rescaled	in interval	decoded symbol
0.69	$[0.4, 0.9)$	s_2
$(0.69 - 0.4)/.5 = 0.58$	$[0.4, 0.9)$	s_2
$(0.58 - 0.4)/.5 = 0.36$	$[0, 0.4)$	s_1
$0.36/.4 = 0.90$	$[0.9, 1)$	$\bullet$

The decoded message is then $s_2 s_2 s_1 \bullet$.

2. **(d)**: $M_H = \dfrac{8}{13} H(0.75) + \dfrac{5}{13} H(0.4) \approx 0.873.$

3. **(c)**

4. **(e)**: $\phi(2014) = \phi(2 \times 19 \times 53) = \phi(2)\phi(19)\phi(53) = 1 \times 18 \times 52 = 936,$
so by Euler's Theorem,

$$3^{940} \equiv 3^{936} \times 3^4 \equiv 1^{936} \times 81 \equiv 81 \pmod{2014}.$$

5. **(c)** $\gcd(4, 15) = 1$ and $4^{14} \equiv 1 \pmod{15}$.

6. (i) **True**
   (ii) **False**: The binary entropy is approximately 1.38 .
   (iii) **False**: $a = 61$ and $b = 103$, so $2a + b = 267$.
   (iv) **True**: The codewords are 0, 10, 110, 1110 .
   (v) **False**: There are $\phi(26) = 12$ primitive elements in GF(27).

7. (i) Here, we have that $\alpha^3 = \alpha + 1$.

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

   (ii) $\alpha^{3k} = (\alpha + 1)^k = \alpha^2 + \alpha + 1 = \alpha^5 = \alpha^{12}$, so $3k \equiv 12 \pmod 7$; hence, $k = 4$.
   (iii) $\{\alpha^3, \alpha^6, \alpha^{12} = \alpha^5, \alpha^{10} = \alpha^3, \ldots\} = \{\alpha^3, \alpha^5, \alpha^6\}$,
   so the minimal polynomial of α^3 is

$$\begin{aligned} & (x - \alpha^3)(x - \alpha^5)(x - \alpha^6) \\ &= x^3 - (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha^3\alpha^5 + \alpha^3\alpha^6 + \alpha^5\alpha^6)x - \alpha^3\alpha^5\alpha^6 \\ &= x^3 + (\alpha + 1 + \alpha^2 + \alpha + 1 + \alpha^2 + 1)x^2 + (\alpha + \alpha^2 + \alpha^4)x + 1 \\ &= x^3 + x^2 + (\alpha + \alpha^2 + \alpha^2 + \alpha)x + 1 \\ &= x^3 + x^2 + 1\,. \end{aligned}$$

Version B

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

1. **(a)**:

code number rescaled	in interval	decoded symbol
0.35	$[0, 0.4)$	s_1
$0.35/.4 = 0.875$	$[0.4, 0.9)$	s_2
$(0.875 - 0.4)/.5 = 0.95$	$[0.9, 1)$	$\bullet$

2. **(b)**: $M_H = \dfrac{2}{5}H(0.7) + \dfrac{3}{5}H(0.2) \approx 0.786.$

3. **(a)**

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

$$2^{2014} = (2^{80})^{25} \times 2^{14} \equiv 1^{25} \times (2^7)^2 \equiv 128^2 \equiv 5^2 \equiv 25 \pmod{123}\,.$$

5. **(b)** $3^3 = 10$ and $3^5 = 5$ in $\mathbb{Z}_{17}$ and $\gcd(3, 16) = \gcd(5, 16) = 1$.

6. (i) **True**
   (ii) **True**: The binary entropy is approximately 1.495 and by Shannon's Theorem, we can get arbitrarily close to this.

   (iii) **False**: $a = 61$ and $b = 103$, so $2a + b = 225$.
   (iv) **True**: The codewords are 0, 100, 101, 1100 .
   (v) **False**: The numbers x_i generated are 1,7,2,9,6,0,5,15 .

7. (i) Here, we have that $\alpha^3 = \alpha^2 + 1$.

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

   (ii) $\dfrac{\alpha^2 + 1}{\alpha^3 + \alpha^4} = \dfrac{\alpha^3}{\alpha^2 + 1 + \alpha^2 + \alpha + 1} = \dfrac{\alpha^3}{\alpha} = \alpha^2$

   (iii) $\{\alpha^5, \alpha^{10} = \alpha^3, \alpha^6, \alpha^{12} = \alpha^5, \ldots\} = \{\alpha^3, \alpha^5, \alpha^6\}$,
   so the minimal polynomial of α^5 is

$$\begin{aligned} &(x - \alpha^3)(x - \alpha^5)(x - \alpha^6) \\ &= x^3 - (\alpha^3 + \alpha^5 + \alpha^6)x^2 + (\alpha^3\alpha^5 + \alpha^3\alpha^6 + \alpha^5\alpha^6)x - \alpha^3\alpha^5\alpha^6 \\ &= x^3 + (\alpha^2 + 1 + \alpha + 1 + \alpha^2 + \alpha)x^2 + (\alpha + \alpha^2 + \alpha^2 + \alpha + 1)x + 1 \\ &= x^3 + x + 1\,. \end{aligned}$$