MATH3411 INFORMATION, CODES & CIPHERS

Test 2, Session 2 2012, SOLUTIONS

Version A

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

1. **(c)**: Word is $s_1 s_1 s_2$, or some permutation thereof, with probability $50/7^3 \approx 1/7$.

2. **(e)**: $I(A, B) = H(A) + H(B) - H(A, B)$.

3. **(b)**: $I(A, B) = H(B) - H(B \mid A) = H(0.2 + 0.7p) - (0.5p + 0.7)$, differentiating with respect to p gives the turning point at

$$0.7 \log_2\left((0.2 + 0.7p)^{-1} - 1\right) = 0.5,$$

or $(0.2 + 0.7p)^{-1} = 2^{5/7} + 1 \approx 2.64$. Solving for p gives $p \approx 0.26$.

4. **(d)**: $\phi(2012) = 1004$ so $3^{2011} = (3^{1004})^2 3^3 = 27$ in $\mathbb{Z}_{2012}$.

5. **(d)**: $3569 = 83 \times 43$.

6. (i) **True**: message encodes as $(0, a)(0, b)(1, a)(2, b)(3, a)$.
   (ii) **True**: binary entropy is 0.722 and by Shannon's theorem we can get arbitrarily close to this.
   (iii) **False**: $\gcd(22, 175) = 1$ so inverse exists.
   (iv) **True**: The powers of 5 in $\mathbb{Z}_{17}$ run 5, 8, 6,..., so $6 = 5^3$ in $\mathbb{Z}_{17}$ and $\gcd(3, \phi(17)) = \gcd(3, 16) = 1$, so 6 is primitive.
   (v) **True**: clearly $\gcd(7, 25) = 1$ in $\mathbb{Z}_{25}$, $7^2 = 49 = -1$ so $7^{24} = 1$.

7. (i)

$$\begin{aligned} \alpha^1 &= \alpha & \alpha^5 &= 2\alpha \\ \alpha^2 &= \alpha + 1 & \alpha^6 &= 2\alpha^2 = 2\alpha + 2 \\ \alpha^3 &= \alpha^2 + \alpha = 2\alpha + 1 & \alpha^7 &= 2\alpha^3 = \alpha + 2 \\ \alpha^4 &= 2\alpha^2 + \alpha = 2 & \alpha^8 &= 2\alpha^4 = 1 = \alpha^0 \end{aligned}$$

   (ii) Determinant of the coefficient matrix is $\alpha^{11} - \alpha^7 = (2\alpha + 1) - (\alpha + 2) = \alpha + 2 = \alpha^7$, so the solution is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \alpha^{-7} \begin{pmatrix} \alpha^7 & 2\alpha^5 \\ 2\alpha^2 & \alpha^4 \end{pmatrix} \begin{pmatrix} 2 \\ \alpha^3 \end{pmatrix} = \alpha \begin{pmatrix} 2\alpha^7 + 2\alpha^8 \\ \alpha^2 + \alpha^7 \end{pmatrix} = \begin{pmatrix} 2 + 2\alpha \\ \alpha^3 + 1 \end{pmatrix}$$

So $x = 2\alpha + 2 = \alpha^6$, $y = 2\alpha + 2 = \alpha^6$.

You can also use row reduction: your method for first year will work.

(iii) The other root of the minimal polynomial will be $\alpha^{21} = \alpha^5$, as $(\alpha^5)^3 = \alpha^{15} = \alpha^7$. So the polynomial is

$$(x-\alpha^7)(x-\alpha^5) = x^2-(\alpha^7+\alpha^5)x+\alpha^{12} = x^2-2x+2 = x^2+x+2.$$

Version B

Multiple Choice: b, c, e, d, a
True/False: F, T, T, F, T.

1. **(b)**: Word is $s_1 s_2 s_2$, or some permutation thereof, with probability $6/7^3 \approx 1/57$.

2. **(c)**: $H(A, B) = H(A) + H(B) - I(A, B)$

3. **(e)**: $I(A, B) = H(B) - H(B \mid A) = H(0.3 + 0.6p) - (0.5p + 0.9)$, differentiating with respect to p gives the turning point at

$$0.6 \log_2((0.3 + 0.6p)^{-1} - 1) = 0.5,$$

   or $(0.3 + 0.6p)^{-1} = 2^{5/6} + 1 \approx 2.78$. Solving for p gives $p \approx 0.10$.

4. **(d)**: $\phi(2012) = 1004$ so $5^{2011} = (5^{1004})^2 5^3 = 125$ in $\mathbb{Z}_{2012}$.

5. **(a)**: $5141 = 97 \times 53$.

6. (i) **False**: message encodes as $(0, a)(0, b)(2, a)(3, b)(2, b)$.

   (ii) **True**: binary entropy is 0.764 and by Shannon's theorem we can get arbitrarily close to this.

   (iii) **True**: $\gcd(21, 175) = 7$ so there is no inverse.

   (iv) **False**: The powers of 3 in $\mathbb{Z}_{17}$ run 3, 9, 10, 13, $\ldots$, so $13 = 3^4$ and $\gcd(4, \phi(17)) = \gcd(4, 16) \neq 1$, so 13 is not primitive.

   (v) **True**: clearly $\gcd(8, 21) = 1$ and in $\mathbb{Z}_{21}$, $8^2 = 64 = 1$ so $8^{20} = 1$.

7. (i)

$$\begin{aligned} \alpha^1 &= \alpha & \alpha^5 &= 2\alpha \\ \alpha^2 &= 2\alpha + 1 & \alpha^6 &= 2\alpha^2 = \alpha + 2 \\ \alpha^3 &= 2\alpha^2 + \alpha = 2\alpha + 2 & \alpha^7 &= 2\alpha^3 = \alpha + 1 \\ \alpha^4 &= 2\alpha^2 + 2\alpha = 2 & \alpha^8 &= 2\alpha^4 = 1 = \alpha^0 \end{aligned}$$

   (ii) Determinant of the coefficient matrix is $\alpha^7 - \alpha^5 = \alpha + 1 - (2\alpha) = 2\alpha + 1 = \alpha^2$, so the solution is

$$\begin{pmatrix} x \\ y \end{pmatrix} = \alpha^{-2} \begin{pmatrix} \alpha^5 & 2\alpha^4 \\ 2\alpha & \alpha^2 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha^2 \end{pmatrix} = \alpha^6 \begin{pmatrix} \alpha^5 + 2\alpha^6 \\ 2\alpha + \alpha^4 \end{pmatrix} = \begin{pmatrix} \alpha^3 + \alpha^8 \\ 2\alpha^7 + \alpha^2 \end{pmatrix}$$

   So $x = 2\alpha = \alpha^5$, $y = \alpha$.

   You can also use row reduction: your method for first year will work.

(iii) The other root of the minimal polynomial will be $\alpha^{21} = \alpha^5$, as $(\alpha^5)^3 = \alpha^{15} = \alpha^7$. So the polynomial is

$$(x-\alpha^7)(x-\alpha^5) = x^2-(\alpha^7+\alpha^5)x+\alpha^{12} = x^2-x+2 = x^2+2x+2.$$