MATH3411 INFORMATION, CODES & CIPHERS

Test 3 Session 2 2018 SOLUTIONS

Version A

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

1. **(d)**: $H_M = \frac{8}{13}H(0.75) + \frac{8}{13}H(0.4) \approx 0.904$
2. **(d)**: The second least likely codewords have probability $\frac{4}{125}$ and length $\lceil \log_2 \frac{125}{4} \rceil = 5$.
3. **(c)**: $H(B|A) = \sum_i P(a_i)H(B|a_i) = \frac{3}{7}H(\frac{4}{5}) + \frac{4}{7}H(\frac{5}{8}) = \frac{3}{7}H(\frac{1}{5}) + \frac{4}{7}H(\frac{3}{8})$.
4. **(e)**: You can use Euler's Theorem but it's easier just to note that $10^3 \equiv -1 \pmod{1001}$:
$$10^{1001} \equiv \left(10^3\right)^{333} \times 10^2 \equiv (-1)^{333} \times 100 \equiv -100 \equiv 901 \pmod{1001}.$$
5. **(b)** Neither 12 nor 18 are coprime to 28, unlike 3 and 9.
Consider $a = 3$: Since $3^3 \equiv -1 \pmod{28}$,
$$3^{27} \equiv \left(3^3\right)^9 \equiv (-1)^9 \equiv -1 \not\equiv 1 \pmod{28}.$$
We see that $n = 28$ is not pseudo-prime to base 3.
Consider $a = 9$:
$$9^{27} \equiv \left(3^3\right)^{18} \equiv (-1)^{18} \equiv 1 \equiv 1 \pmod{28}.$$
We see that $n = 28$ is pseudo-prime to base 9.
6. (i) **False**: $\phi(22) = \phi(2)\phi(11) = 10$.
(ii) **True**: $x^3 + x + 1$ has no roots in $\mathbb{Z}_2$ so it has no linear factor.
Since its degree is 3, it is irreducible. Therefore, $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ is a field.
(iii) **True**: $\gcd(3, 17) = 1$, $3^{16} \equiv 1 \pmod{17}$ and $3^{\frac{16}{2}} \equiv -1 \not\equiv 1 \pmod{17}$
(iv) **True**: $11 = 5^5 \pmod{18}$ and $\gcd(5, \phi(18)) = 1$ (here $\phi(18) = 5$).
(v) **False**: There are $\phi(\phi(125)) = \phi(100) = 40$ primitive elements in $\mathbb{U}_{125}$.
7. (i) Here, $\alpha^2 = -\alpha - 2 = 2\alpha + 1$:

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

(ii) $\dfrac{\alpha^2 + 1}{\alpha^3 + \alpha^4} = \dfrac{2\alpha + 2}{2\alpha + 1} = \dfrac{\alpha^3}{\alpha^2} = \alpha$
(iii) $m_2(x) = (x - \alpha^2)(x - \alpha^6) = x^2 - (\alpha^2 + \alpha^6)x + 1 = x^2 + 1$

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

Version B

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

1. **(e)**: $H_M = \frac{2}{5}H(0.7) + \frac{3}{5}H(0.2) \approx 0.786$
2. **(c)**: $H(A,B) = H(A) + H(B) - I(A,B) = 0.93 + 0.76 - 0.56 = 1.13$
3. **(c)**: By Euler's Theorem, $5^{\phi(2018)} \equiv 5^{1008} \equiv 1 \pmod{2018}$, so
$$5^{2018} \equiv \left(5^{1008}\right)^2 \times 5^2 \equiv 1^2 \times 25 \equiv 25 \pmod{2018}.$$
4. **(d)** $6 \equiv 5^3 \pmod{17}$ and $\gcd(3,16) = 1$; also, $10 \equiv 5^7 \pmod{17}$ and $\gcd(7,16) = 1$. Therefore, both 6 and 10 are primitive elements in $\mathbb{Z}_{17}$.
5. **(a)**: The second most likely codewords have probability $\frac{50}{343}$ and length $\lceil \log_3 \frac{343}{50} \rceil = 2$.
6. (i) **False**: $\phi(48) = \phi(3)\phi(2^4) = 16$.
   (ii) **True**: $x^3 + x^2 + 1$ has no roots in $\mathbb{Z}_2$ so it has no linear factor. Since its degree is 3, it is irreducible.
   (iii) **True**: There are $\phi(\phi(31)) = \phi(30) = 8$ primitive elements in $\mathbb{U}_{31}$.
   (iv) **False**: $\gcd(5,65) \neq 1$
   (v) **False**: $\gcd(2,61) = 1$ and $2^{60} \equiv 1 \pmod{61}$; however, for the prime powers $p = 3, 5$ of $n - 1 = 60$, $2^{\frac{60}{p}} \equiv 1 \pmod{31}$.
7. (i) Here, $\alpha^2 = -2\alpha - 2 = \alpha + 1$.

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

   (ii)
$$\left(\begin{array}{cc|c} \alpha^4 & \alpha^5 & 2 \\ \alpha^2 & \alpha^7 & \alpha^3 \end{array}\right) \xrightarrow[R2 = \alpha^6 R2]{R1 = \alpha^4 R1} \left(\begin{array}{cc|c} 1 & \alpha & 1 \\ 1 & \alpha^5 & \alpha \end{array}\right) \xrightarrow{R2=R2-R1} \left(\begin{array}{cc|c} 1 & \alpha & 1 \\ 0 & \alpha & \alpha - 1 \end{array}\right)$$
$$\xrightarrow{R1=R1-R2} \left(\begin{array}{cc|c} 1 & 0 & 2\alpha + 2 \\ 0 & \alpha & \alpha^7 \end{array}\right) \xrightarrow{R2=\alpha^{-1}R2} \left(\begin{array}{cc|c} 1 & 0 & \alpha^6 \\ 0 & 1 & \alpha^6 \end{array}\right)$$
   so $x = y = \alpha^6 = 2\alpha + 2$.
   (iv) $m_5(x) = (x - \alpha^5)(x - \alpha^7) = x^2 - (\alpha^7 + \alpha^5)x + \alpha^7\alpha^5 = x^2 - 2x + 2 = x^2 + x + 2$

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