Name: .... Student ID: ....

UNSW SCHOOL OF MATHEMATICS AND STATISTICS

MATH3411 INFORMATION CODES AND CIPHERS

2013 S2 **TEST 2** **VERSION A**

- Time Allowed: **45 minutes**

For the multiple choice questions, **circle the correct answer**;
each multiple choice question is worth **1 mark**.
For the true/false and written answer questions, use extra paper.
Staple everything together at the end.

1. Using the LZ78 algorithm a message is encoded as $(0, a)(1, a)(1, b)(2, a)(3, b)(4, a)$. What is the last dictionary entry after decoding?

(a) *aaaa* (b) *aaab* (c) *abba* (d) *baaa* (e) *bbba*

2. A 2-symbol Markov source has transition matrix $M = \begin{pmatrix} 0.8 & 0.4 \\ 0.2 & 0.6 \end{pmatrix}$ and equilibrium distribution $\mathbf{p} = \frac{1}{3}\begin{pmatrix} 2 \\ 1 \end{pmatrix}$. The (binary) Markov entropy H_M is approximately

(a) 0.791 (b) 0.918 (c) 0.846 (d) 0.888 (e) 0.805

3. Let $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$, so that $H'(x) = \log_2(x^{-1} - 1)$. An asymmetric binary channel with input $A = \{a_1, a_2\}$ and output $B = \{b_1, b_2\}$ has noise entropy $H(B \mid A) = 0.4p + 0.6$ in bits, output entropy $H(B) = H(0.3 + 0.5p)$ in bits and $p = P(a_1)$. The channel capacity is achieved when p has the value approximately

(a) 0.13 (b) 0.26 (c) 0.31 (d) 0.36 (e) 0.43

4. Using Euler's Theorem or otherwise, calculate $2^{1203} \pmod{2013}$
(NB: 2013 is not prime). The answer is

(a) 1 (b) 2 (c) 4 (d) 8 (e) 16

5. For which of the following numbers a is $n = 14$ a pseudoprime to base a?

(a) 2 (b) 3 (c) 4 (d) 5 (e) none of these

6. **[5 marks]** For each of the following, say whether the statement is true or false, giving a brief reason or showing your working. You will get $\frac{1}{2}$ **mark** for a correct true/false answer, and if your true/false answer is correct, then you will get $\frac{1}{2}$ **mark** for a good reason.

Begin each answer with the word "True" or "False".

i) If arithmetic coding with source symbols a, b and stop symbol $\bullet$ corresponding to the intervals $[0, 0.3)$, $[0.3, 0.7)$ and $[0.7, 1)$ is used, then the message 0.55 decodes as $bb\bullet$.

ii) For a 2-symbol source $S = \{s_1, s_2\}$ with probabilities $p_1 = 1/5$, $p_2 = 4/5$ it is possible to find a binary encoding of some extension S^n with average word length per original source symbol less than 0.8.

iii) When using Fermat factorisation to factor $n = 1333$ as a product $n = ab$ where $2 \le a < b$, the sum $a + b$ equals 71.

iv) For a source $S = \{a, b\}$ with probabilities $P(a) = \frac{1}{5}$ and $P(b) = \frac{4}{5}$, the second longest codewords in the binary Shannon-Fano code for the third extension S^3 have length 5.

v) The number 5 is one of the pseudo-random numbers generated by the linear congruential $x_{i+1} \equiv 4x_i + 2 \pmod{11}$, seeded with $x_0 = 1$.

7. **[5 marks]** Let $\mathbb{F} = \mathbb{Z}_3(\alpha)$ where α is a root of the polynomial $x^2 + 1 \in \mathbb{Z}_3[x]$.

(i) Express all nonzero elements of $\mathbb{F}$ as a power of $\gamma = \alpha + 1$ and as a linear combination over $\mathbb{Z}_3$ of 1 and α.

(ii) Find the primitive elements of $\mathbb{F}$.

(iii) Find the inverse of α in $\mathbb{F}$.

(iv) Simplify $\dfrac{\gamma^7 + \alpha}{\gamma^4 + \gamma}$, giving your answer as a linear combination of 1 and α. Show your working.

Name: .... Student ID: ....

UNSW SCHOOL OF MATHEMATICS AND STATISTICS

MATH3411 INFORMATION CODES AND CIPHERS

2013 S2 **TEST 2** **VERSION B**

- Time Allowed: **45 minutes**

> For the multiple choice questions, **circle the correct answer**;
> each multiple choice question is worth **1 mark**.
> For the true/false and written answer questions, use extra paper.
> Staple everything together at the end.

1. Using the LZ78 algorithm a message is encoded as $(0,a)(1,a)(1,b)(2,a)(3,b)(5,a)$. What is the last dictionary entry after decoding?

(a) $aaaa$ (b) $aaab$ (c) $abba$ (d) $baaa$ (e) $bbba$

2. A 2-symbol Markov source has transition matrix $M = \begin{pmatrix} 0.2 & 0.4 \\ 0.8 & 0.6 \end{pmatrix}$ and equilibrium distribution $\mathbf{p} = \frac{1}{3}\begin{pmatrix} 1 \\ 2 \end{pmatrix}$. The (binary) Markov entropy H_M is approximately

(a) 0.791 (b) 0.918 (c) 0.846 (d) 0.888 (e) 0.805

3. Let $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$, so that $H'(x) = \log_2(x^{-1} - 1)$. An asymmetric binary channel with input $A = \{a_1, a_2\}$ and output $B = \{b_1, b_2\}$ has noise entropy $H(B\,|\,A) = 0.4p + 0.7$ in bits, output entropy $H(B) = H(0.2 + 0.7p)$ in bits and $p = P(a_1)$. The channel capacity is achieved when p has the value approximately

(a) 0.29 (b) 0.33 (c) 0.37 (d) 0.40 (e) 0.43

4. Using Euler's Theorem or otherwise, calculate $5^{1203} \pmod{2013}$.
(NB: 2013 is not prime). The answer is

(a) 1 (b) 5 (c) 25 (d) 125 (d) 625

5. For which of the following numbers a is $n = 15$ a pseudoprime to base a?

(a) 2 (b) 3 (c) 4 (d) 5 (e) none of these

6. [**5 marks**] For each of the following, say whether the statement is true or false, giving a brief reason or showing your working. You will get $\frac{1}{2}$ **mark** for a correct true/false answer, and if your true/false answer is correct, then you will get $\frac{1}{2}$ **mark** for a good reason.

Begin each answer with the word “True” or “False”.

i) If arithmetic coding with source symbols a, b and stop symbol $\bullet$ corresponding to the intervals $[0, 0.3)$, $[0.3, 0.7)$ and $[0.7, 1)$ is used, then the message 0.55 decodes as $b\bullet$.

ii) For a 2-symbol source $S = \{s_1, s_2\}$ with probabilities $p_1 = 1/4$, $p_2 = 3/4$ it is possible to find a binary encoding of some extension S^n with average word length per original source symbol less than 0.8.

iii) When using Fermat factorisation to factor $n = 1333$ as a product $n = ab$ where $2 \leq a < b$, the sum $a + b$ equals 74.

iv) For a source $S = \{a, b\}$ with probabilities $P(a) = \frac{1}{5}$ and $P(b) = \frac{4}{5}$, the second shortest codewords in the binary Shannon-Fano code for the third extension S^3 have length 3.

v) The number 7 is one of the pseudo-random numbers generated by the linear congruential $x_{i+1} \equiv 4x_i + 2 \pmod{11}$, seeded with $x_0 = 1$.

7. [**5 marks**] Let $\mathbb{F} = \mathbb{Z}_3(\alpha)$ where α is a root of the polynomial $x^2 + x + 2 \in \mathbb{Z}_3[x]$.

(i) Express all nonzero elements of $\mathbb{F}$ as a power of α and as a linear combination over $\mathbb{Z}_3$ of 1 and α.

(ii) Find the primitive elements of $\mathbb{F}$.

(iii) Find the inverse of $2\alpha + 1$ in $\mathbb{F}$.

(iv) Simplify $\dfrac{\alpha^2 + 1}{\alpha^3 + \alpha^4}$, giving your answer as a linear combination of 1 and α. Show your working.