MATH 4023 **Name** _____

Exam 3 **July 23, 2010** **Score:** KEY

Instructions: This is a closed book, closed notes exam. Please read all instructions carefully and complete all problems. Be sure to show your work in order to receive full credit, an answer with no supporting work will receive no credit.

1. This problem concerns arithmetic modulo 20 (in $\mathbb{Z}_{20}$). All answers should only involve expressions of the form $\overline{a}$ with a an integer satisfying $0 \leq a < 20$.

   (a) Compute $\overline{8} + \overline{17}$.

   $\overline{8}+\overline{17} = \overline{25} = \overline{5}$

   (b) Compute $\overline{8}\ \overline{17}$.

   $\overline{80}+\overline{56} = \overline{16}$.

   (c) Compute $\overline{7}^{-1}$.

   $\overline{7}\cdot\overline{3} = \overline{21} = \overline{1}$ mod 20

   $\overline{7}^{-1} = \boxed{\overline{3}}$

   (d) Find all zero divisors of $\mathbb{Z}_{20}$.

   $\overline{2}, \overline{4}, \overline{5}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{15}, \overline{16}, \overline{18}$

2. Find the last 2 digits of 15^{101}.

3. This problem makes use of the following equation:

$$1 = 15 \cdot 27 - 4 \cdot 101.$$

Using this equation (not necessary to prove it!) answer the following.

(a) Compute the multiplicative inverse of 15 in $\mathbb{Z}_{101}$.

$\overline{1} = \overline{15} \cdot \overline{27} \Rightarrow \overline{27}$ is the inverse of $\overline{15}$.

(b) Compute 15^{101} mod 101.

$GCD(15,101) = 1 \Rightarrow$ By Fermat's Theorem

$15^{101} = 15 \pmod{101}$

(c) Solve the equation $15x = 8$ mod 101.

Part (a), $\overline{15}^{-1} = \overline{27}$ so

Since $GCD(15,101)=1 \Rightarrow x = \overline{27}\ \overline{8} = \overline{14} = 14 \pmod{101}$

(d) Solve the simultaneous linear congruences:

$$x \equiv 7 \mod 101$$
$$x \equiv 3 \mod 27$$

By Chinese Remainder theorem, there is a unique Soln mod (2727)

$x = 3 + 27k$, for some k.

But $3 + 27k = 7 \pmod{101}$

$\Rightarrow 27k = 4 \pmod{101}$

$\Rightarrow k = (15)(4) \pmod{101}$, $\overline{15}^{-1} = 27$

$\Rightarrow k = 60 + 101r$, for some r.

$\Rightarrow x = 3 + 27(60) \pmod{2727}$

$\Rightarrow x = 1623 \pmod{2727}$

4. Assume that for an RSA cryptosystem $n = 143$ and the enciphering exponent is $e = 103$, where $n = 143 = 11 \times 13$.

(a) Compute the deciphering exponent d.

$\phi(n) = \phi(143) = 10 \times 12 = 120$

$GCD(103, 120) = 1$, and

$1 = 7 \cdot 103 - 6 \cdot 120$ [use Euclidean Algorithm to get this]

$\Rightarrow \overline{103}^{-1} = \overline{7} \pmod{120}$.

$d = \overline{7}$.

(b) Assume that the following letter to number translation table is used:

$$J = 1, Q = 2, R = 3, L = 4, D = 5, A = 6, S = 7, Y = 8, T = 9, O = 0$$

Encrypt the message " SO".

$SO \longrightarrow 70$

So compute $(70)^{103} \pmod{143}$

$70^2 = 38 \pmod{143}$

$70^4 = 14 \pmod{143}$

$70^8 = 53 \pmod{143}$

$70^{16} = 92 \pmod{143}$

$70^{32} = 27 \pmod{143}$

$70^{64} = 14 \pmod{143}$.

(c) Assume that a message has been grouped into blocks of two letters, enciphered and send out as 10 03. Decipher the message.

$(10)^7 = 10 \pmod{143}$

$(03)^7 = 42 \pmod{143}$

So the message is $1042 \longleftrightarrow JOLQ$.

5. Let C be a binary code with generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

(a) Find the Partity check matrix of C.

$$H = [A^t \mid I] = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(b) Find all of the codewords of C

000, 001, 010, 100, 011, 101, 110, 111

Codewords $\{000000, 001011, 010101, 100110, 011110, 101101, 110011, 111000\}$

(c) How many redundant digits are there in a codeword?

3

(d) What is the minimum distance d of C?

weights, 3, 3, 3, 4, 4, 4, 3

$d(c) = 3$.

(e) How many errors can it detect? How many errors can it correct?

detect 2 errors; $[d \geq t+1]$

Corrects 1-error. $[d \geq 2t+1]$

(f) Use this coding to encode 101.

101101.