Test 1 for Spring/2010

11:10-13:00, April 23, 2010

1. **(a)** Find $x, y \in Z$ such that $17x + 257y = 1$ and **(b)** Solve $17x \equiv 1 \ mod \ 257$.

2. Decrypt the ciphertext *XZVIVKQKTUKIZEDIFCKOPIQ* which was encrypted by an affine cipher $y \equiv 9x + 10 \ mod \ 26$.

3. Decrypt ciphertext *cbxomkevj* encrypted by a Hill cipher

$$H = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 11 & 9 & 8 \end{bmatrix}$$

4. Solve $x^2 \equiv 133 \ (mod \ 143)$.

5. Find **(a)** the last two digits of 25^{244} and **(b)** the remainder of dividing 3^{12305} by 101.

6. Let $p = 7, 11, \ or \ 19$. Show that $a^{90} \equiv 1 \ (mod \ p)$ for all a with $gcd(a, p) = 1$.

7. A 3rd-order LFSR (linear feedback shift register) sequence starts 001110. Find the next four elements of the sequence.

8. Let $\phi(n)$ be the number of integers $1 \leq a \leq n$ such that $gcd(a, n) = 1$.

(a) Compute all of $\phi(d)$, where $d|10$, that is, $d = 1, 2, 5, 10$.

(b) Compute all of $\phi(d)$, where $d|12$.

(c) Find $\sum_{d|n} \phi(d)$ for $n = 10, 12, 15$.

(d) Show that $\sum_{d|n} \phi(d) = n, \ \forall \ n \in N = Z^+$.

9. Let a and $n > 1$ be integers with $gcd(a, n) = 1$. The *order* of a *mod* n is defined as the smallest integer $r \geq 1$ such that $a^r \equiv 1 \ (mod\ n)$, denoted as $r = ord_n(a)$.

(a) Compute $ord_{10}(3)$ and $ord_{11}(3)$.

(b) Show that $r \leq \phi(n)$.

(c) If $m \equiv 0 \ (mod\ r)$, then $a^m \equiv 1 \ (mod\ n)$.

(d) Suppose $a^t \equiv 1 \ (mod\ n)$ and $t = qr + s$ with $0 \leq s < r$, then $a^s \equiv 1 \ (mod\ n)$.

(e) Show that $a^t \equiv 1 \ (mod\ n)$ iff $ord_n(a)|t$.

(f) Show that $ord_n(a)|\phi(n)$.

10. Suppose $m_1, m_2, \cdots, m_k$ are integers such that $gcd(m_i, m_j) = 1$ whenever $i \neq j$. Let $a_1, a_2, \cdots, a_k$ be integers. The following *algorithm* is guaranteed to construct a general form of solution for the Chinese Remainder Theorem.

for $i = 1, 2, \cdots, k$

$z_i = m_1 \cdots m_{i-1} m_{i+1} \cdots m_k$

$y_i \equiv z_i^{-1} \ (mod\ m_i)$

endfor

Let $x = a_1 y_1 z_1 + a_2 y_2 z_2 + \cdots + a_k y_k z_k$.

(a) Show that $x \equiv a_i \ (mod\ m_i) \ for\ 1 \leq i \leq k$.

(b) Solve the following simultaneous congruence problem.

$$\begin{aligned} x &\equiv 2 \quad (mod\ 5) \\ x &\equiv 5 \quad (mod\ 7) \\ x &\equiv 8 \quad (mod\ 11) \end{aligned}$$