FINAL EXAM 2013 – MA 1301
SOLUTIONS

- **Problem 1:**

(a) Compute $\gcd(217, 161)$.

$$\begin{aligned} 217 &= 161 + 56 \\ 161 &= 56 \cdot 2 + 49 \\ 56 &= 49 + 7 \\ 7 &= 7 \cdot 1. \end{aligned}$$

Therefore, we have that $\gcd(217, 161) = 7$.

(b) c has to be a multiple of 7.

(c) By (a) we get

$$7 = 217 \cdot 3 - 4 \cdot 161.$$

Consequently, $217 \cdot 6 - 161 \cdot 8 = 14$ and so $x_0 = 6$ and $y_0 = -8$. All other solutions are given by $x = 6 + 31t$ and $y = -8 - 23t$ for t an integer.

- **Problem 2:**

(•) $n = 273$, $N_1 = 91$, $N_2 = 39$ and $N_3 = 21$.

(•) $91x \equiv 1 \mod 3$ gives $x_1 = 1$; $39x \equiv 1 \mod 7$ gives $x_2 \equiv 2 \mod 7$ and $21x \equiv 1 \mod 13$ provides $x_3 = 5$.

(•) The solution of the system of congruence equations is given by $\overline{x} = 1 \cdot 91 \cdot 2 + 2 \cdot 39 \cdot 12 + 5 \cdot 21 \cdot 20 \equiv 3218 \mod 273$ so that gives $\overline{x} = 215 \mod 273$.

- **Problem 3:**

(a) For a with $\gcd(a, n) = 1$: (i) the order of a modulo n is the least integer k such that $a^k \equiv 1 \mod n$; (ii) a primitive root of n is an integer r of order $\varphi(n)$, i.e. $r^{\varphi(n)} \equiv 1 \mod n$.

(b) ($\bullet$) 1 has order 1.

($\bullet$) $2 \equiv 2 \mod 7$, $2^2 \equiv 4 \mod 7$, $2^3 \equiv 1 \mod 7$ gives that 2 has order 3.

($\bullet$) $3 \equiv 3 \mod 7$, $3^2 \equiv 2 \mod 7$, $3^3 \equiv 6 \mod 7$, $3^4 \equiv 4 \mod 7$, $3^5 \equiv 5 \mod 7$, $3^6 \equiv 1 \mod 7$ gives that 3 has order 6 and is a primitive root of 7.

($\bullet$) $4 \equiv 4 \mod 7$, $4^2 \equiv 2 \mod 7$ and $4^3 \equiv 1 \mod 7$ yields that 4 is of order 3 modulo 7.

($\bullet$) $5 \equiv 5 \mod 7$, $5^2 \equiv 4 \mod 7$, $5^3 \equiv 6 \mod 7$, $5^4 \equiv 2 \mod 7$, $5^5 \equiv 3 \mod 7$ and $5^6 \equiv 1 \mod 7$ shows that 5 is a primitive root of 7.

($\bullet$) The integer 6 is of order 2 modulo 7: $6 \equiv 6 \mod 7$ and $6^2 \equiv 1 \mod 7$.

- **Problem 4:**

(a) Suppose p is an odd prime and a such that $\gcd(a, p) = 1$. (i) a is a quadratic residue if the congruence $x^2 \equiv a \mod p$ has a solution; (ii) a is a quadratic non-residue if the congruence $x^2 \equiv a \mod p$ has no solution; (iii) the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be $+1$ if a is a quadratic residue and is -1 if a is a quadratic non-residue.

(b) Since $\gcd(a, p) = 1$, Lagrange's Theorem on polynomial congruences implies that $x^2 \equiv a \mod p$ has at most 2 solutions. If x_0 is a solution of $x^2 \equiv a \mod p$, then $(p - x_0)^2 = p^2 - 2px_0 + x_0^2 \equiv x_0^2 \equiv a \mod p$. Therefore, x_0 and $p - x_0$ are all solutions, and since $p \neq 2$ they are different.

(c) For two distinct primes p and q we have that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$.

(d) Compute the Legendre symbol $\left(\frac{281}{397}\right)$.

$281 = 4 \cdot 70 + 1$ and $397 = 4 \cdot 99 + 1$

$$\begin{array}{rcl}
\left(\frac{281}{397}\right) & = & \left(\frac{397}{281}\right) \text{ Quadratic Reciprocity} \\
\left(\frac{397}{281}\right) & = & \left(\frac{116}{281}\right) \ 397 = 281 + 116 \\
\left(\frac{116}{281}\right) & = & \left(\frac{4 \cdot 29}{281}\right) \\
\left(\frac{2 \cdot 2 \cdot 29}{281}\right) & = & \left(\frac{2}{281}\right)^2 \left(\frac{29}{281}\right) \text{ Multiplictativity} \\
\left(\frac{29}{281}\right) & = & \left(\frac{281}{29}\right) \text{ Quadratic Reciprocity} \\
\left(\frac{281}{29}\right) & = & \left(\frac{20}{29}\right) \ 281 = 29 \cdot 9 + 20 \\
\left(\frac{20}{29}\right) & = & \left(\frac{2}{29}\right)\left(\frac{10}{29}\right) \text{ Multiplictativity} \\
\left(\frac{2}{29}\right)\left(\frac{10}{29}\right) & = & \left(\frac{2}{29}\right)^2 \left(\frac{5}{29}\right) \text{ Multiplictativity} \\
\left(\frac{5}{29}\right) & = & \left(\frac{29}{5}\right) \text{ Quadratic Reciprocity} \\
\left(\frac{29}{5}\right) & = & \left(\frac{4}{5}\right) \ 29 = 5 \cdot 5 + 4 \\
\left(\frac{4}{5}\right) & = & +1. \text{ Computation}
\end{array}$$

- **Problem 5:**

(a) An arithemtic function f is multiplicative if $f(mn) = f(m)f(n)$ for all integers m, n with $\gcd(m, n) = 1$.

(b) Euler's φ-function, $\varphi(n)$, for a positive integer n is defined as the number of integers in $\{1, ..., n\}$ that are relatively prime to n. Equivalently, $\varphi(n)$ is the number of integers in $\{1, ..., n\}$ that have a multiplicative inverse modulo n.

$$\begin{array}{rcl}
\varphi(p_1^{k_1} p_2^{k_2} p_3^{k_3}) & = & (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})(p_3^{k_3} - p_3^{k_3-1}) \\
& = & n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\Big(1 - \frac{1}{p_3}\Big).
\end{array}$$

(c) $\varphi(60) = \varphi(2^2 \cdot 3 \cdot 5) = 16$

- **Problem 6:**
  (a) $n = 55 = 5 \cdot 11$, we have $\varphi(55) = 40$. Therefore, $3d \equiv 1 \mod 40$ yields $d = 27$. Secret key is $\{55, 27\}$.
  (b) Encrypted message m is $E(m) = m^3 \mod 55$. For $m = 18$ we get $E(18) = 18^3 = 5832 \equiv 2 \mod 55$, i.e. one sends 2.