Math 4351 Exam #1

(1) [4 pts] Show or disprove, for $p$ prime: if $p \mid b$ and $p \mid b^2 + c^2$, then $p \mid c$.

\[ p \mid b \quad \text{and} \quad p \mid b^2 + c^2 \Rightarrow p \mid c \]

(2) [6 pts] Find the inverse of 17 (mod 53). [Hint: there is a method to do this. Trial and error will not receive full credit.]

Use the Euclidean Algorithm:

\[
\begin{array}{c|ccc|c}
53 & 17 & 2 & 1 & 3 \\
\hline
1 & 0 & 1 & -8 & 8 \\
0 & 1 & -3 & 25 & \end{array}
\]

\[ 25 \cdot 17 - 8 \cdot 53 = 1 \Rightarrow 25 \text{ is the inverse.} \]
(3) [6 pts] Compute $5^{113} \pmod{23}$, stating any results you use.

$\text{Little Fermat: } \phi(23) = 22 \Rightarrow 5^{22} \equiv 1 \pmod{23}$.

So $5^{22} \equiv 1 \Rightarrow 5^{110} \equiv 1 \Rightarrow 5^{113} = 5^{10 \cdot 5^2} \equiv 25 \cdot 5 \equiv 1 \pmod{23}$

$= 10$.

(4) [8 pts] Use the Chinese Remainder Theorem to find all solutions of the congruence $x^2 + 15x + 29 \equiv 0 \pmod{35}$.

$\text{mod 5: } x^2 - 1 \equiv 0 \Rightarrow x \equiv 1, 4 \pmod{5}$

$\text{mod 7: } x^2 + x + 1 \equiv 0 \Rightarrow x \equiv 2, 4 \pmod{7}$

Under $\mathbb{Z}/35\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$,

$\begin{align*}
4 & \rightarrow (4, 4) \\
11 & \rightarrow (1, 4) \\
9 & \rightarrow (4, 2) \\
16 & \rightarrow (1, 2)
\end{align*}$

(5) the 4 solutions $(\mod 35)$.
(5) (a) [3 pts] What is a group?

A set with associative binary operation and "identity element" 1 such that

1 \cdot x = x = x \cdot 1 \quad (\forall x) \quad and \quad (\forall x) \exists y \text{ s.t. } xy = yx = 1.

Identify each of the following groups as a (specific) cyclic group or product of (specific) cyclic groups of the form \((\mathbb{Z}/n\mathbb{Z}, +)\). Does a primitive root (i.e. generator) exist? If not, why not? If so, write one down and say how many there are.

(b) [5 pts] \(G = (\mathbb{Z}/27\mathbb{Z})^*\) (under multiplication)

\[\equiv (\mathbb{Z}/18\mathbb{Z}, +) \quad \text{since} \quad (\mathbb{Z}/p^k\mathbb{Z})^* \quad (p = \text{odd prime}) \quad \text{is cyclic of order} \quad \phi(p^k) = p^k - 1 \quad \text{[in this case,} \quad \phi(3^3) = 3^2 \cdot 2 = 18]\]

Yes, a primitive root is 2.

There are \(\phi(18) = \phi(2) \cdot \phi(3^2) = 1 \cdot (3 \cdot 2) = 6\) primitive roots.

(c) [5 pts] \(G = (\mathbb{Z}/35\mathbb{Z})^*\) (under multiplication)

\[\equiv (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^* \quad \text{CRT}\]

\[\equiv \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \quad \text{(under +)}\]

The largest order of an element in this group is the lcm \([4, 6] = 12\), not 24 (= the group order).

Therefore, it is not cyclic, and there is no primitive root.
(6) [6 pts] State the Miller-Rabin test and explain why it works.

Given \( m > 2 \) odd with \( m-1 = 2^k q \), \( q \) odd. If for some \( a \) coprime to \( m \),

\[ a^q \not\equiv 1 \pmod{m} \quad \text{and} \quad a^{2^i q} \not\equiv -1, \quad i = 0, 1, \ldots, k-1, \]

then \( m \) is composite.

This works because if \( m \) were prime, we would have

\[ a^{m-1} \equiv 1 \pmod{m} \]

hence either \( a^{2^i q} \equiv 1 \pmod{m} \) (for some \( i \)) or one of them \( \equiv -1 \) (since at some point you have a square root of 1 and \( \pm 1 \) are the only possibilities).

(7) [7 pts] Use quadratic reciprocity to compute the Legendre symbol \((\frac{41}{97})\). Then state your result in terms of solvability or unsolvability of a congruence.

\[
\left( \frac{41}{97} \right) \overset{\text{QR}}{=} \left( \frac{97}{41} \right) = \left( \frac{97 - 2 \cdot 41}{41} \right) = \left( \frac{15}{41} \right) = \left( \frac{15}{3} \cdot \frac{5}{41} \right) = \left( \frac{1}{5} \right) \cdot \left( \frac{3}{41} \right) = 1 \cdot \left( \frac{3}{41} \right) = -1. 
\]

So the congruence \( x^2 \equiv 41 \pmod{97} \) has no solution.