Math 4351 Exam #1

SOLUTIONS

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

$$\left.\begin{array}{l} p \mid b \\ \text{and} \\ p \mid b^2+c^2 \end{array}\right\} \Longrightarrow \left.\begin{array}{l} p \mid b^2 \\ \text{and} \\ p \mid b^2+c^2 \end{array}\right\} \Longrightarrow p \mid c^2 \underset{p \text{ prime}}{\Longrightarrow} p \mid c$$

(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:

		3	8
53	17	2	1
1	0	1	-8
0	1	-3	25

$\Longrightarrow 25 \cdot 17 - 8 \cdot 53 = 1$

$\Longrightarrow 25 \cdot 17 \underset{(53)}{\equiv} 1$

$\Longrightarrow$ 25 is the inverse.

(3) [6 pts] Compute 5^{113} (mod 23), stating any results you use.

Little Farmat : $(a, 23) = 1 \implies a^{22} \underset{(23)}{\equiv} 1$.

So $5^{22} \underset{(23)}{\equiv} 1 \implies 5^{\overbrace{22\cdot 5}^{110}} \underset{(23)}{\equiv} 1 \implies 5^{113} = \cancel{5^{110}}\cdot 5^3$

1

$= 25\cdot 5 \underset{(23)}{\equiv} 2\cdot 5$

$= 10$.

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

mod 5 : $x^2 - 1 \underset{(5)}{\equiv} 0 \implies x \underset{(5)}{\equiv} 1, 4$

mod 7 : $x^2 + x + 1 \underset{(7)}{\equiv} 0 \implies x \underset{(7)}{\equiv} 2, 4$

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

$$4 \longmapsto (4, 4)$$
$$11 \longmapsto (1, 4)$$
$$9 \longmapsto (4, 2)$$
$$16 \longmapsto (1, 2)$$

↳ 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 $1 \cdot x = x = x \cdot 1$ $(\forall x)$ and $(\forall x) \exists y$ 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)

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

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)

$$\underset{\text{CRT}}{\cong} (\mathbb{Z}/5\mathbb{Z})^* \times (\mathbb{Z}/7\mathbb{Z})^*$$

$$\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \quad (\text{under } +)$$

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,

$$a^q \underset{(m)}{\not\equiv} 1 \text{ and } a^{2^i q} \underset{(m)}{\not\equiv} -1, \; i=0,1,\dots,k-1,$$

then m is composite.

This works because were m prime, we would have $a^{m-1} \underset{(m)}{\equiv} 1$, hence either $a^{2^i q} \underset{(m)}{\equiv} 1$ $(i=0,1,\dots,k-1)$ or one of them $\underset{(m)}{\equiv} -1$ (since at some point you have a square root of 1 and ± 1 are the only possibilities).

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

$$\left(\frac{41}{97}\right) \underset{41 \underset{(4)}{\equiv} 1}{\overset{QR2}{=}} \left(\frac{97}{41}\right) = \left(\frac{97-2\cdot 41}{41}\right) = \left(\frac{15}{41}\right) = \left(\frac{5}{41}\right)\cdot\left(\frac{3}{41}\right)$$

$$\underset{QR2}{=} \left(\frac{41}{5}\right)\cdot\left(\frac{41}{3}\right) = \left(\frac{1}{5}\right)\cdot\left(\frac{2}{3}\right) = 1\cdot(-1) = -1.$$

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