Math 210 — Homework Assignment 5

DUE DATE: FEB. 14, 2008

1. For the following relatively prime m_1 and m_2, find the reconstruction coefficients to reconstruct a number x mod $m_1 m_2$ from the numbers x_1 mod m_1 and x_2 mod m_2 (i.e., the coefficients c_1 and c_2 so that $x \equiv c_1 x_1 + c_2 x_2 \pmod{m_1 m_2}$).

(a) $m_1 = 8$, $m_2 = 21$.

(b) $m_1 = 7$, $m_2 = 19$.

2. Suppose that S is a set and that $\sim$ is an equivalence relation on S. For any a in S, define

$$S_a = \left\{ b \in S \mid b \sim a \right\}.$$

(a) Prove that the union $\displaystyle\bigcup_{a \in S} S_a = S$.

(b) Prove that for any two elements a_1, a_2 of S, either $S_{a_1} \cap S_{a_2} = \emptyset$ or $S_{a_1} = S_{a_2}$.

(c) Conclude that the elements of the set $P = \{S_a\}_{a \in S}$ form a partition of S.

REMINDER: In a set, duplicates don't count, e.g., $\{1, 2, 1, 3, 2\} = \{1, 2, 3\}$, and so in particular if $S_{a_1} = S_{a_2}$ then $\{S_{a_1}, S_{a_2}\} = \{S_{a_1}\}$.

3. To practice the idea that we can work with any field in the same way that we work with $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, let's do some linear algebra in $\mathbb{Z}/p\mathbb{Z}$ where p is a prime.

(a) Solve the system of equations $\begin{bmatrix} \bar{3} & \bar{4} \\ \bar{2} & \bar{1} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \bar{1} \\ \bar{4} \end{bmatrix}$ in $\mathbb{Z}/7\mathbb{Z}$.

(b) Solve the system of equations $\begin{bmatrix} \overline{11} & \bar{3} \\ \bar{9} & \bar{2} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \bar{5} \\ \overline{13} \end{bmatrix}$ in $\mathbb{Z}/19\mathbb{Z}$.

(c) Solve the system of equations $\begin{bmatrix} \overline{87} & \overline{60} \\ \bar{9} & \overline{78} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} \overline{43} \\ \overline{32} \end{bmatrix}$ in $\mathbb{Z}/133\mathbb{Z}$.

HINTS: (i) 133 is not a prime. (ii) Perhaps you don't need to solve the equations in (c) from scratch.

4. The purpose of this question is to prove that if p is a prime number and $p \equiv 3 \pmod 4$ then then the only solution to $x^2 + y^2 = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ is $x = \bar{0}$, $y = \bar{0}$.

Suppose that p is a prime, $p \geq 3$, and that z is a solution to $z^2 + \bar{1} = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ (i.e., to $z^2 = -\bar{1}$.)

(a) Explain why $z^k \cdot z^{4-k} = \bar{1}$ for $k = 0, 1, 2, 3$.

(b) Let S be the set of nonzero elements in $\mathbb{Z}/p\mathbb{Z}$. How many elements does S have?

(c) Show that the relation

$$a \sim b \text{ if and only if } \tfrac{a}{b} = z^k \text{ for some } k.$$

is an equivalence relation on the set S.

(d) Since $\sim$ is an equivalence relation it partitions S into disjoint subsets. Show that each subset must have exactly 4 elements.

(e) Combining (b) and (d) show that if $p \equiv 3 \pmod 4$ then the equation $z^2 + \bar{1} = \bar{0}$ has no solution in $\mathbb{Z}/p\mathbb{Z}$.

(f) Suppose that we have a solution to $x^2 + y^2 = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ and that $y \neq \bar{0}$. Explain why $z = x/y$ would be a solution to $z^2 + \bar{1} = \bar{0}$.

(g) Conclude that if p is a prime number and $p \equiv 3 \pmod 4$ then only solution to $x^2 + y^2 = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ is $x = \bar{0}$, $y = \bar{0}$.