Homework Set Five (ungraded)

Question 1. Recall that the Chinese Remainder Theorem (as proved in class) states that given relatively prime integers $m, n \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$ there exists $x \in \mathbb{Z}$ such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. (In fact, x is well defined modulo mn.) Prove by induction that given $a_1, \ldots a_r \in \mathbb{Z}$ and mutually coprime (meaning any distinct pair is relatively prime) integers $n_1, \ldots, n_r$ there exists $x \in \mathbb{Z}$ such that $x \equiv a_i \pmod{n_i}$ for each $1 \leq i \leq r$.

Question 2. The following is the oldest known instance of the Chinese Remainder Theorem, from the late third or early fourth century.

"We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"
–*Sun Tzu Ching* (Master Sun's Mathematical Manuel)
Circa AD 300, volume 3, problem 26.

Solve this 1700 year old problem.

Question 3. Let $p \in \mathbb{N}$ be prime.

(a) Prove that if $\overline{c} \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$ then there exists $\overline{b} \in \mathbb{Z}/p\mathbb{Z}$ such that $\overline{c}\overline{b} = \overline{1}$. (Since $\mathbb{Z}/p\mathbb{Z}$ is a commutative ring, this implies that it is in fact a field.) Hint: Euclidean Algorithm.

(b) Prove that if $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ satisfies $\overline{a}^2 = \overline{1}$, then $a \equiv \pm 1 \pmod{p}$.

(c) Use the previous parts to prove

$$(p-1)! \equiv -1 \pmod{p}.$$

(Hint: Place the units in pairs.)

Question 4. Consider the field $\mathbb{F}_2$ and the irreducible polynomial $f = x^3 + x + 1 \in \mathbb{F}_2[x]$. Let $k = \mathbb{F}_2[x]/\sim$, where if $g, h \in \mathbb{F}_2[x]$ we have $g \sim h$ when $f \mid g - h$. Give a complete multiplication table for the multiplicative group $k^\times$.

Question 5. Suppose a and b are integers such that $\gcd(a, b) = 1$ and $p > 2$ is a prime. If $p \mid a^2 + b^2$, show that $p \equiv 1 \pmod{4}$.