Problem Set 3

Due: Monday, September 26

Reading Assignment: Sections 4.0-4.3, 4.5, 4.6

Problem 1. [18 points]

(a) [4 pts] Use the Pulverizer to find integer values of x, y that satisfy $71x + 50y = 1$. What is the inverse of 71 modulo 50 (Write the inverse as a number in the set $\{1, 2, \ldots, 49\}$?

(b) [4 pts] Use the Pulverizer to find integer values of x, y that satisfy $43x + 64y = 1$. What is the inverse of 64 modulo 43 (Write the inverse as a number in the set $\{1, 2, \ldots, 42\}$?

(c) [4 pts] Prove that $2 \mid (n)(n+1)$ for all integers n.

(d) [6 pts] Prove that $3! \mid (n)(n+1)(n+2)$ for all integers n.

Although we won't ask you to prove it, this formula from parts c, d actually generalizes to $k! \mid (n)(n+1) \cdot \ldots \cdot (n+k-1)$. As an extra challenge, see if you can prove it yourself.

Problem 2. [20 points] Prove the following statements about divisibility.

(a) [4 pts] If $a \mid b$, then $\forall c$, $a \mid bc$

(b) [4 pts] If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$.

(c) [4 pts] $\forall c$, $a \mid b \Leftrightarrow ca \mid cb$

(d) [4 pts] $\gcd(ka, kb) = k \gcd(a, b)$

(e) [4 pts] Prove that for integers a, b, c, d and $n \geq 1$, $a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ implies $ac \equiv bd \pmod{n}$.

Problem 3. [22 points] In this problem, we are going to walk through a proof of Wilson's theorem, which states the following:

Theorem 1 (Wilson's Theorem)**.** *If p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.*

(a) [2 pts] Verify that Wilson's theorem holds for $p = 2, 3$.

(b) [6 pts] Prove the following theorem about the existence and uniqueness of modular inverses for prime modulos.

Theorem 2. *If p is a prime, show that for all a, if gcd$(a,\ p) = 1$, then there exists some unique b such that $ab \equiv 1$ (mod p) and $b \in \{1, 2, \ldots p-1\}$.*

There are two components to this proof (1) to show that such a b exists and (2) that there is a unique b.

Hint: To show that b exists, consider that since $\gcd(a,\ p) = 1$, there exist integers b, c such that $ab + pc = 1$. What happens if you consider this equation modulo p?

(c) [6 pts] Let p be a prime number. Prove that for integer a, $a^2 \equiv 1 \pmod{p}$ if and only if $a \equiv \pm 1 \pmod{p}$.

Hint: Consider $a^2 - 1 = (a+1)(a-1)$.

(d) [8 pts] Prove Wilson's theorem using the above parts.

Hint: Use theorem 2 to pair up the integers in the expansion of $(p-1)!$ with their inverses. Based on part c, which integers don't get paired?

Problem 4. [20 points] The following parts can be solved using Fermat's little theorem, which states that for integers a, p such that $\gcd(a, p) = 1$, $a^{p-1} \equiv 1 \pmod{p}$.

(a) [2 pts] Find $3^{31} \pmod{7}$.

(b) [4 pts] Prove that $7 \mid n^6 - 1$ for all integers n such that $\gcd(n, 7) = 1$.

(c) [6 pts] Prove that $42 \mid n^7 - n$ for all integers n.

(d) [8 pts] Prove that $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ is an integer $\forall n \in \mathbb{Z}$.

Problem 5. [20 points]

Prove that the greatest common divisor of three integers a, b, and c is equal to their smallest positive linear combination; that is, the smallest positive value of $sa + tb + uc$, where s, t, and u are integers.

Problem 6. [20 points] In this problem, we will investigate numbers which are squares modulo a prime number p. These numbers are referred to quadratic residues of p.

(a) [5 pts] An integer n is a quadratic residue of p if there exists another integer x such that $n \equiv x^2 \pmod{p}$. Prove that $x^2 \equiv y^2 \pmod{p}$ if and only if $x \equiv y \pmod{p}$ or $x \equiv -y \pmod{p}$. (*Hint: This is similar to problem 3c*)

(b) [5 pts] The following is a simple test we can perform to see if a number $n \not\equiv 0 \pmod{p}$ is a quadratic residue of p for odd primes p.

Theorem 3 (Euler's Criterion)**.** *:*

1. *n is a quadratic residue of p if and only if* $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
2. *n is quadratic non-residue p if and only if* $n^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

This can be proved completely using Wilson's theorem and part a of this problem. However for this part prove the following: If n is a quadratic residue of p, then $n^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

(c) [10 pts] Assume that $p \equiv 3 \pmod{4}$ and $n \equiv x^2 \pmod{p}$. Find one possible value for x, expressed as a function of n and p. (*Hint: Write p as $p = 4k + 3$ and use Euler's Criterion. You might have to multiply two sides of an equation by n at one point.*)