MATH 3070
Assignment # 3
Due Thursday, October 2, 2008

1. For any $m \in \mathbb{N}$, prove that the set of invertible elements mod m is closed under multiplication. That is, the product of any pair of invertible elements is also invertible.

   This, combined with the fact that 1 is invertible and inverses are invertible, makes the set of invertible elements mod m a *group*. This set of elements is usually denoted $\mathbb{Z}_m^*$, the multiplicative group mod m.

2. Prove that the congruence $x^2 \equiv 244714 \pmod{1256636}$ has no solutions.

3. Let $(a, m) = 1$. Prove that the set $\{ax \pmod{m} : 0 \leq x \leq m-1\}$ is a complete residue system mod m. Thus multiplying by an integer relatively prime to the modulus simply rearranges the residues mod m.

4. Solve the following systems of congruences or prove that there is no solution.

   (a) $3x \equiv 4 \pmod{7}$, $5x \equiv 3 \pmod{8}$, $12x \equiv 17 \pmod{29}$.

   (b) $5x \equiv 3 \pmod{12}$, $3x \equiv 7 \pmod{8}$, $x \equiv 12 \pmod{25}$.

5. Solving quadratics mod m.

   (a) Give an example to show that it is possible for $x^2 \equiv a \pmod{m}$ to have more than two solutions mod m.

   (b) Prove that in the case $m = p^2$, where p is an odd prime, the maximum number of solutions is still two unless $a \equiv 0 \pmod{p^2}$.

   (c) Prove that the maximum number of solutions is four when $m = p_1 p_2$, a product of two distinct primes.

6. Prove that for all $n \in \mathbb{Z}$ the polynomial $n^{35} - 4n^{24} + 5n^{16} + 21n^8 - n^3 + 2$ is never divisible by 17.

7. Prove the converse of Wilson's Theorem: if n is composite then $(n-1)! \not\equiv -1 \pmod{n}$. In fact, prove the stronger statement that $(n-1)! \equiv 0 \pmod{n}$ for $n > 4$ and composite.