Math 115, Summer 2012
Homework 3
Due Thursday, July 12th

NZM a.b.c refers to a problem in our text, 5th edition - these may differ slightly from the problems appearing in other editions, so use the version printed here to be safe).

(1) (NZM 2.6.2) Solve the congruence $x^5 + x^4 + 1 \equiv 0 \mod 3^4$, if possible.
(2) Solve the congruence $x^3 + x + 57 \equiv 0 \mod 1125$.
(3) For each $n = 0, 1, 2, 3, 4$, give an example of a congruence which has exactly n solutions mod 5.
(4) (NZM 2.7.4) Prove that if $f(x) \equiv 0 \mod p$ has j solutions $x \equiv a_1$, $x \equiv a_2, \ldots,$ $x \equiv a_j$, then there is a polynomial $q(x)$ such that $f(x) \equiv (x - a_1)(x - a_2) \cdots (x - a_j)q(x) \mod p$. (the textbook has a hint)
(5) How many primitive roots mod 101 are there?
(6) (NZM 2.8.1) Find a primitive root mod p for each of the primes $p = 3, 5, 7, 11, 13$.
(7) (NZM 2.8.4) Find the orders of 1,2,3,4,5, and 6 mod 7.
(8) (NZM 2.8.5) Let p be an odd prime. Prove that a has order 2 mod p if and only if $a \equiv -1$ mod p.
(9) (NZM 2.8.6) If a has order h mod m, prove that no two of the numbers $a, a^2, \ldots, a^h$ are congruent mod m.
(10) Prove that if a has order 3 mod p, then $a^2 + a + 1 \equiv 0 \mod p$, and $1 + a$ has order 6 mod p.
(11) Let p be an odd prime, and set

$$f(x) = x^{p-1} - 1, \quad g(x) = (x - 1)(x - 2) \cdots (x - (p - 1))$$

Prove the following:
(a) The degree of the polynomial $f(x) - g(x)$ is $p - 2$.
(b) If c is any integer $0 < c < p$, then $f(c) \equiv g(c) \equiv 0 \mod p$.
(c)

$$f(x) \equiv g(x) \mod p$$

[Recall that we say two polynomials are congruent mod p if each of their coefficients are congruent mod p. For example, $5x^3 - x^2 + 2x + 1 \equiv 4x^2 + 7x - 9 \mod 5$.]

(12) Use the previous exercise to prove that for every prime $p > 3$,

$$\sum_{1 \leq i < j \leq p-1} ij \equiv 0 \mod p$$

and

$$\sum_{1 \leq i < j < k \leq p-1} ijk \equiv 0 \mod p$$

For example, if $p = 5$, the first one says that

$$1 \cdot 2 + 1 \cdot 3 + 1 \cdot 4 + 2 \cdot 3 + 2 \cdot 4 + 3 \cdot 4 \equiv 0 \mod 5$$

Of course, you have to prove it for general p, not just $p = 5$.