MATH 304: HOMEWORK 5 (due 3/15)

Recall that the order of an element g in a group $(G, \cdot, 1)$ is the size of the subgroup it generates. If G is finite, so that g^n is the identity element 1 for some power n, then the order of g is the smallest value of n for which $g^n = 1$, since the subgroup generated by g is:

$$\langle g \rangle = \{g, g^2, g^3, \ldots, g^n = 1\}.$$

We are concerned with the group $(\mathbb{Z}/p\mathbb{Z})^\times$ of nonzero residue classes $a \pmod p$ under multiplication. In this case the notion of the order of the group element $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ in the group coincides with the notion of the order of $a \pmod p$ as defined in class and denoted by $e_p(a)$.

I asserted (and you may have used on a previous HW) the following in class:

Theorem (Order Divisibility Property)**.** *Suppose that* $a^n \equiv 1 \pmod p$. *Then the order* $e_p(a)$ *of* $a \pmod p$ *divides* n.

1. (a) Prove the order divisibility property. (I see two equally valid approaches: either prove the statement directly using the theory of congruences or prove a general statement about arbitrary finite groups G and then deduce the theorem as a special case.)

   (b) Prove that for a relatively prime to p, the congruence $a^m \equiv a^n \pmod p$ holds if and only if $m \equiv n \pmod{e_p(a)}$.

2. Let $f(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + a_0$ be a degree k monic polynomial whose coefficients a_i are integers. Let p be a prime number. Show that the congruence

   $$f(x) \equiv 0 \pmod p$$

   has at most k distinct solutions modulo p (i.e. at most k solutions x satisfying $0 \leq x < p$).

3. (a) Determine the number of solutions (modulo 11) to the congruence

   $$x^4 + 5x^3 + 4x^2 - 6x - 4 \equiv 0 \pmod{11}.$$

   (b) Determine the number of solutions (modulo 8) to the congruence

   $$x^2 - 1 \pmod 8.$$

   Since there are more than two solutions, is this a contradiction to problem 2?

4. In class, we proved that if n is a Carmichael number and p is a prime number dividing n, then $p - 1$ divides $n - 1$. Prove the stronger statement that $p - 1$ divides $\frac{n}{p} - 1$.

5. (a) Let $n = 1105$, so $n - 1 = 2^4 \cdot 69$. Use the Rabin-Miller test with $a = 2$ to conclude that n is composite.

   (b) Use the Rabin-Miller test with $a = 2$ to prove that $n = 294409$ is composite. Then find a factorization of n and use Korselt's criterion to show that n is a Carmichael number.

6. Find all of the primes less than 20 for which 3 is a primitive root.

7. (a) If k divides $p - 1$, show that the congruence $x^k \equiv 1 \pmod{p}$ has exactly k distinct solutions modulo p.

   (b) More generally, suppose that p does not divide a and consider the congruence

   $$x^k \equiv a \pmod{p}.$$

   Find a simple way to use the values of k, p and the index $I(a)$ to determine how many solutions this congruence has.