Math 115, Summer 2012
Homework 3
Solution

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.

Solution: First we solve it mod 3. Plugging in 0,1,2 and reducing mod 3 gives 1,0,1, so the only root mod 3 is 1. First we check to see if this is nonsingular: if $f(x) = x^5 + x^4 + 1$,

$$f'(x) = 5x^4 + 4x^3 \equiv 2x^2 + x \mod 3,$$

so $f'(1) \equiv 0$ mod 3, and the root is singular. We saw in class that this means there may be no liftings, or many liftings. We write out the Taylor series to see which possibility occurs:

$$f(1+3t) = f(1) + 3tf'(1) + \ldots \equiv f(1) = 3 \not\equiv 0 \mod 9$$

so the only root 1 mod 3 DOES NOT lift to a root mod 9. Thus there are no solutions mod 9, and hence none mod 3^4

(2) Solve the congruence $x^3 + x + 57 \equiv 0 \mod 1125$.

Solution: $1125 = 3^2 \cdot 5^3$. First we solve it mod 3. $x^3 + x + 57 \equiv 2x \mod 3$, so the only root is 0. This is nonsingular since $f'(x) = 3x^2 + 1 \equiv 1 \mod 3$. So if $a = 1$, we have $f'(a) = f'(a)^{-1} = 1$. Set $a_1 = a = 1$, and lift

$$a_2 = a_1 - f(a_1)f'(a)^{-1} = 1 - 57 \cdot 1 \equiv -3 \equiv 6 \mod 9$$

So $a_2 = 6$ is our root mod 9.

Now we work mod 5. We have $x^3 + x + 57 \equiv x^3 + x + 2 \equiv 0 \mod 5$, and trial and error shows that $x = 4$ is the only root. It's nonsingular since $f'(4) = 3 \cdot 4^2 + 1 \equiv 4 \mod 5$, so $f'(a)^{-1} = 4 \mod 5$. Now set $a_1 = a = 4$ and lift:

$$a_2 = a_1 - f(a_1)f'(a)^{-1} = 4 - 25 \cdot 4 \equiv 4 \mod 25$$
$$a_3 = a_2 - f(a_2) \cdot f'(a)^{-1} = 4 - 125 \cdot 4 \equiv 4 \mod 125$$

So our root mod 125 is 4. Now we use the CRT. We want x such that

$$x \equiv 6 \mod 9$$
$$x \equiv 4 \mod 125$$

One way to solve this is to note that the second one says $x = 6 + 125k$ for some k. Substitute this into the first, giving

$$6 + 125k \equiv 6 \mod 9$$

which reduces to $4m \equiv 1 \mod 9$. Since $(4, 9) = 1$, we can find an inverse to 4 mod 9, namely 7, giving m=7 so $x = 4 + 125 \cdot 7 = 879$, which we can consider mod 1125.

(3) For each $n = 0, 1, 2, 3, 4$, give an example of a congruence which has exactly n solutions mod 5.

Solution: Consider the congruence

$$f(x) \equiv 0 \mod 5$$

Setting $f(x) = 1$, there are no solutions; with $f(x) = x$ there is one; with $f(x) \equiv x^2$ there are two, as we proved some time ago. Setting $f(x) = x(x-1)(x-2)$ gives three solutions, and $f(x) = x(x-1)(x-2)(x-3)$ gives four. It was not asked, but for five solutions, we have two options: the obvious $f(x) = 0$, and also the polynomial $f(x) = x^5 - x$ - every x mod 5 is a solution, by Fermat's Little Theorem.

(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)

Solution: It's enough by induction to prove that if a is a root mod p, then $(x-a) \mid f(x)$ mod p.

We write

$$f(x) = (x-a)q(x) + r(x),$$

where $r(x)$ is either identically zero mod p or else has degree less than that of $(x-a)$. In the latter case, we have $r(x) = c \not\equiv 0 \mod p$. Plugging in $x = a$ to the above equation then gives $0 \equiv c \mod p$, a contradiction, so $r(x)$ is the zero polynomial mod p, which means $(x-a)$ divides f mod p.

(5) How many primitive roots mod 101 are there?

Solution: By the formula from class, since 101 is prime, there are $\phi(p-1) = \phi(100) = 40$ primitive roots mod 101.

(6) (NZM 2.8.1) Find a primitive root mod p for each of the primes $p = 3, 5, 7, 11, 13$.

Solution: You only needed to find one primitive root for each modulus, but for completeness, I list all of them: 2 is a primitive root mod 3; 2 and 3 are primitive roots mod 5; 3 and 5 are primitive roots mod 7; 2,6,7, and 8 are primitive roots mod 11; and 2,6,7, and 11 are primitive roots mod 13.

(7) (NZM 2.8.4) Find the orders of 1,2,3,4,5, and 6 mod 7.

Solution: Note that in checking this, you know the order must divide $\phi(7) = 6$, so the only possible orders are 1,2,3, and 6. The answers are 1,3,6,3,6,2 respectively.

(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.

Solution: If a has order two, the $a^2 \equiv 1 \mod p$, and we proved in class that this implies $a \equiv \pm 1 \mod p$. But $a \not\equiv 1 \mod p$, for then it would have order 1. So $a \equiv -1$.

Conversely, assume $a \equiv -1 \mod p$. Then certainly $a^2 \equiv 1 \mod p$. So the order of a divides 2. It cannot be 1, since the only element with order 1 is 1 itself, and $1 \not\equiv -1 \mod p$, since p is odd, hence $p > 2$. Thus the order is actually 2.

(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.

Solution: Suppose for contradiction that a has order h, but $a^i \equiv a^j$ for some i, j with $1 \leq i < j \leq h$. Then cancelling a^i gives $1 \equiv a^{j-i}$, and since $j - i < h$, this contradicts the fact that a has order h.

(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.

Solution: Since a has order 3, we have $a^3 \equiv 1 \mod p$, hence $0 \equiv a^3 - 1 = (a-1)(a^a 2 + a + 1) \mod p$. Since p is prime (so there are no zerodivisors in $\mathbb{Z}/p$), either $a - 1 \equiv 0$ mod p or $a^2 + a + 1 \equiv 0 \mod p$. It can't be the case that $a - 1 \equiv 0 \mod p$, or else a would have order 1; thus $a^2 + a + 1 \equiv 0 \mod p$.

From the first part we have $1 + a \equiv -a^2 \equiv (-1) \cdot a^2 \mod p$. Now the order of a^2 is three since $(a^2)^3 = (a^3)^2 \equiv 1^2 \mod p$, and $a^2 \not\equiv 1$ since a has order 3, and $a^4 \not\equiv 1$ since the order of a would then divide 4. Meanwhile, the order of (-1) is 2, and since $-1 \equiv p - 1$ and a and $p - 1$ are relatively prime ($a \not\equiv p - 1 \equiv -1$ or else the order of a would be 2). This means that by a theorem from class, the order of their product is the product of their orders, namely 6.

(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, $5x^3 - x^2 + 2x + 1 \equiv 4x^2 + 7x - 9 \mod 5$.]

Solution:

(a) The first few terms of g are $x^{p-1} - (1 + 2 + \cdots + (p-1))x^{p-2} + \cdots$, so the leading term of $f - g$ is $(1 + 2 + \cdots + (p-1))x^{p-2}$.

(b) By Fermat's Little Theorem, $f(c) \equiv 1 - 1 = 0$, as long as $c \neq 0$. For any $0 < c < p$, g contains a factor $(x - c)$, so $g(c) = 0$. Hence $f(c) \equiv g(c) \equiv 0 \mod p$.

(c) The polynomial $f - g$ has degree $p-2$ as an *integer polynomial*. We want to show that it has no degree mod p. That is, when we reduce it mod p, we get the zero polynomial. If it has a degree mod p, that degree is at most $p - 2$. But in (b) we exhibited $p - 1$ distinct roots mod p. So if it has a degree, this contradicts the fact that the number of roots mod p is at most the degree mod p. Thus it has no degree, as desired, i.e., $f - g \equiv 0 \mod p$, so $f \equiv g \mod p$.

(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

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

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

Solution: By the previous result, the coefficients of each x^k of f and g are congruent mod p. The coefficients of x^{p-3} and x^{p-4} in f are 0 (note we're using $p \geq 5$ here). The coefficient of x^{p-3} in g is

$$(-1 \cdot -2) + (-1 \cdot -3) + \cdots + (-2 \cdot -3) + \cdots + (-(p-2)(-(p-1))) = \sum_{1 \leq i < j \leq p-1} ij.$$

Since this is congruent to the x^{p-3} coefficient of f, which is zero, that proves the first claim. The second congruence is similar, just noting that the sum is exactly the coefficient of x^{p-4} if you expand out the product defining g.