18.781 Problem Set 7 - Fall 2008

Due Tuesday, Oct. 28 at 1:00

Throughout this assignment, $f(x)$ always denotes a polynomial with integer coefficients.

1. (a) Show that $e_{32}(3) = 8$, and write down a list of powers demonstrating that any odd number n satisfies $n \equiv \pm 3^j \pmod{32}$ for some j.

   The successive powers of 3 mod 32 are

   $$3, 9, 27, 17, 19, 25, 11, 1.$$

   This shows both that $e_{32}(3) = 8$ and, since 31 is not listed and thus no powers of 3 are additive inverses mod 32, all 16 odd congruence classes mod 32 can be written as either one of the above numbers or its negative.

   (b) Determine the order of 9 modulo 64.

   By the above list of powers, 9 has order 4 modulo 32. So lifting to 64, 9 has order divisible by 4. In fact, $9^4 \equiv 33 \pmod{64}$, and since $33^2 \equiv 1 \pmod{64}$, 9 has order 8 modulo 64.

(Bonus) Prove that $e_{2^k}(g) = 2^{k-2}$ if and only if $g \equiv 3$ or $5 \pmod 8$.

2. (Niven 2.7.1) Solve the congruence $x^2 + x + 7 \equiv 0 \pmod{81}$.

   We solve this congruence by solving modulo successive powers of 3. For the modulus 3, we just have $x^2 + x + 1 \equiv 0$ which has the double root 1. Because this is a double root, it is a *singular* root, so all possible lifts of the number give the same number mod 9, so either they are all roots or none is. Then mod 9 we have to check 1, which clearly satisfies the equation, so they all $(1, 4, 7)$ satisfy the equation. So now we lift to 27 and get the solutions that we need to check are $1, 4, 7$. We find that 4 satisfies the equation but not the other two, so $4, 13, 22$ are all solutions (once again, using singularity) to the equation mod 27. Finally, lifting to 81 we get that the equation must be checked at $4, 13$, and 22. Since none of these satisfy the equation, it has no solutions mod 81.

3. (Niven 2.7.4) Solve the congruence $x^2 + 5x + 24 \equiv 0 \pmod{36}$.

   Here we see that our modulus factors as $36 = 2^2 \cdot 3^2$. We solve each prime power separately and then combine them using CRT. Mod 4 is small enough that we can just check it by hand, the solutions are 0 and 3. For the second prime power, mod 9 we can first get that 0 and 1 are solutions mod 3. Then by the nonsingularity, each of these lifts uniquely to mod 9, we can quickly see that 0 lifts to 6 and 1 lifts to 7, so our solutions are 6 and 7 mod 9.

   Now we combine our solutions mod 4 and mod 9 into solutions mod 36 by taking pairs and using the Chinese Remainder Theorem.

$\pmod 4$	$\pmod 9$		$\pmod{36}$
$x \equiv 0$	$x \equiv 6$	$\Rightarrow$	$x \equiv 24$
$x \equiv 0$	$x \equiv 7$	$\Rightarrow$	$x \equiv 16$
$x \equiv 3$	$x \equiv 6$	$\Rightarrow$	$x \equiv 15$
$x \equiv 3$	$x \equiv 7$	$\Rightarrow$	$x \equiv 7.$

So the solutions mod 36 are $7, 15, 16$, and 24.

4. (Niven 2.7.6) Solve the congruence $x^3 + x^2 - 4 \equiv 0 \pmod{343}$.

   This equation is easiest; when we begin by checking the seven congruences classes mod 7, we get no solutions. So there cannot be any solutions mod $7^3 = 343$.

5. (Niven 2.7.9) This problem explains how to lift solutions in the nonsingular case more quickly (using successive squaring).

   (a) Suppose that $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$. Let x be an integer such that $f'(a)x \equiv 1 \pmod{p^j}$, and set $b := a - f(a)x$. Prove that $f(b) \equiv 0 \pmod{p^{2j}}$.
   Remark. *The key difference from before is that x is now the inverse of $f'(a)$ mod p^j rather than just mod p.*

   So we can lift our solutions more quickly here. To prove the result, we use our Taylor expansion of the polynomial f at a. We know that

   $$f(a + tp^j) = f(a) + tp^j f'(a) + t^2 p^{2j} f''(a)/2! + \cdots \equiv f(a) + tp^j f'(a) \pmod{p^{2j}}.$$

   So to lift a to the modulus p^{2j}, we want to find t so that

   $$0 \equiv f(a) + tp^j f'(a) \pmod{p^2 j},$$

   or, we want

   $$t \equiv -\frac{f(a)}{p^j} \cdot x \pmod{p^j},$$

   where x is the inverse of $f'(a)$ mod p^j, as it is defined above. Note that we know the fraction in the congruence makes sense because we know a is a root mod p^j, so we can divide this in the integers. So we have that this t gives us the proper lifted root, so plugging this t in to $a + tp^j$, we get that $a - f(a)x$ is our lifted root mod p^{2j}. Since this is the exact form of b, we are done.

   (b) If $f(a_0) \equiv 0 \pmod{p}$, explain how part (a) lets us find $a_1, a_2, \ldots$ such that $f(a_i) \equiv 0 \pmod{p^{2^i}}$.

   This is just Newton's method applied to modular arithmetic! Given a polynomial f with a nonsingular root a mod p, we know $f'(a)$ is coprime to p, and thus is invertible in every modulus that is a power of p. So, from some a_i the solution mod p^{2^i}, let $a_{i+1} = a_i - x_i f(a_i)$ for x_i the inverse of $f'(a)$ mod p^{2^i}, and by the above proof this a_{i+1} is a solution mod $p^{2^{i+1}}$.

   (c) Solve $x^3 + x^2 + 4 \equiv 0 \pmod{3^8}$.

   We are clearly supposed to use the above method with this equivalence. First we solve it mod 3 to find that it has the unique solution 1, and this solution is nonsingular, since $f'(x) = 3x^2 + 2x$. So we know this unique solution will lift to a unique solution for all powers of 3.

   Now we begin to use the method above with $a_0 = 1$. $f'(a_0) = 5$ which has inverse 2 mod 3, so we know $a_1 = a_0 - f(a_0) \cdot x_0 = 1 - 6 \cdot 2 = -11 \equiv 7 \pmod{9}$. So $a_1 = 7$. Now looking mod 9, the inverse of $f'(7) = 161$ is 8, so $x_1 = 8$. Then

   $$a_2 = a_1 - f(a_1) \cdot x_1 = 7 - 396 \cdot 8 \equiv 79 \pmod{81}.$$

Calculating x_2, we get that the inverse of $f'(79) = 18881 \equiv 8 \pmod{81}$ is 71. So

$$a_3 = a_2 - f(a_2)x_2 = 79 - 499284 \cdot 71 = -35449085 \equiv 6559 \pmod{6561 = 3^8}.$$

So we are done. But note that this can be solved much more easily by noting that there is a unique solution for all powers of 3 and then noting that -2 is a solution in the integers, so is a solution for all powers of 3.

6. Suppose that $f(a) \equiv 0 \pmod{p}$. Is it possible that $f(a) \equiv 0 \pmod{p^j}$ for all j (i.e., the solution can be lifted unchanged)?

   If $f(a) \equiv 0 \pmod{p^j}$ for all j, then that means that arbitrarily large powers of p divide the integer $f(a)$. The only integer that this could possibly hold for is 0, since otherwise we can find a j for which $p^j > |f(a)|$, and so if $f(a) \neq 0$, clearly we cannot have $p^j | f(a)$. But if $f(a) = 0$, then it is true that the solution a lifts for all j, just as the solution -2 lifted in the previous problem.

7. (Niven 2.9.1abd) Rewrite the following congruences in the form $(x - r)^2 \equiv k \pmod{p}$.

   (a) $4x^2 + 2x + 1 \equiv 0 \pmod{5}$
   (b) $3x^2 - x + 5 \equiv 0 \pmod{7}$
   (c) $x^2 + x - 1 \equiv 0 \pmod{13}$.

   (a)
   $$4x^2 + 2x + 1 \equiv 4(x + 3x + 4) \equiv 4((x + 4)^2 + 3) \equiv 0 \pmod{5}.$$
   So the congruence is equivalent to $(x - 1)^2 \equiv 2 \pmod{5}$.

   (b)
   $$3x^2 - x + 5 \equiv 3(x^2 + 2x + 4) \equiv 3((x + 1)^2 + 3) \equiv 0 \pmod{7}.$$
   So we get $(x - 6)^2 \equiv 4 \pmod{7}$.

   (c)
   $$x^2 + x - 1 \equiv (x + 7)^2 - 11 \equiv 0 \pmod{13}.$$
   So $(x - 6)^2 \equiv 11 \pmod{13}$.

8. (Niven 2.9.2 & 2.9.3) Suppose $f(x) = ax^2 + bx + c$, with discriminant $D = b^2 - 4ac$. Let p be an odd prime.

   (a) If $p \nmid a$ and $p \mid D$, show that $f(x) \equiv 0 \pmod{p}$ has one solution x_0, and that $f'(x_0) \equiv 0 \pmod{p}$.
   Here we have that $D \equiv 0 \pmod{p}$, so we have exactly one square root of D, 0. Now, since we showed in class that $ax^2 + bx + c \equiv 0$ if and only if $(2ax + b)^2 \equiv D \pmod{p}$, we thus have that the only solution mod p when $2ax + b \equiv 0$, which is determined uniquely by the inverse of $2a$, which exists since p is prime and $p \nmid a$, times $-b$.
   For this solution, we find that $f'(x) = 2ax + b \equiv 0 \pmod{p}$.

   (b) If $p \nmid a$ and $p \nmid D$, show that $f(x) \equiv 0 \pmod{p}$ has zero or two solutions, and that $f'(x') \not\equiv 0 \pmod{p}$ for a solution x'.
   Here we have to solve $(2ax + b)^2 \equiv D \pmod{p}$ with $D \not\equiv 0$. Here, we know we have either two square roots, when D is a QR, or zero square roots, when D is

a QNR. In the first case, each square root corresponds to a unique root to the equation, so we have two solutions, and since we know the square roots are not zero, we get that $f'(a) = 2ax' + b \not\equiv 0 \pmod{p}$ for a solution x'.

(Bonus) Prove that $f(x) \equiv 0 \pmod{p^2}$ has $0, 1, 2, p$, or p^2 solutions.

9. (*Completing the cube*)

   (a) Suppose that $f(x) = ax^3 + bx^2 + cx + d$ and that $p \geq 5$. Prove that the congruence $f(x) \equiv 0 \pmod{p}$ is equivalent to some congruence $g(x) \equiv 0 \pmod{p}$ where $g(x) = Ax^3 + Cx + D$.

   Here we can complete the cube the same way we completed the square for any odd prime. First, multiply the equation through by $27a^2$, which can be done because 3 is invertible, since $p \geq 5$. We get

   $$27a^3x^3 + 27a^2bx^2 + 27a^2cx + 27a^2d \equiv 0 \pmod{p}.$$

   Then our leftmost term is a cube, and the next term is the next term of the binomial expansion of $(3ax + b)^3$. So we get

   $$(3ax + b)^3 + (27a^2c - 9ab^2)x + (27a^2d - b^3) \equiv 0 \pmod{p}.$$

   Now, we write the other terms in the form $(3ax + b)$:

   $$(3ax + b)^3 + (9ac - 3b^2)(3ax + b) + (27a^2d - 9abc + 2b^3) \equiv 0 \pmod{p}.$$

   So letting $y = 3ax + b$, we get the equivalent congruence

   $$y^3 + (9ac - 3b^2)y + (27a^2d - 9abc + 2b^3) \equiv 0 \pmod{p}.$$

   (b) Solve $x^3 + 6x^2 - 6x - 18 \equiv 0 \pmod{23}$.

   So here we carry out the above simplification with $a = 1, b = 6, c = -6$, and $d = -18 \bmod 23$. So $y = 3x + 6$ and we get

   $$y^3 + (-162)y + (270) \equiv y^3 - y + 17 \equiv 0 \pmod{23}.$$

   This makes the calculation a bit easier, but by plugging in all of the residues mod 23, $\{-11, -10, \ldots, 10, 11\}$, shows that this has no solution, and so the original congruence had no solution.

10. (Niven 3.2.5)

   (a) Prove that the quadratic residues mod 11 are $1, 3, 4, 5$, and 9.

   This can be found by squaring the numbers 1 to $\frac{11-1}{2} = 5$ and reducing mod 11. We get $1, 4, 9, 5$, and 3. Rearranged, these are the ones listed.

   (b) Find the solutions to $x^2 \equiv a \pmod{11}$ for $a = 1, 3, 4, 5, 9$. The solutions for each of the congruences are just the plus and minus of the number squared to get the residue. Using our list above, we can see that the answers to the 5 conguences are, respectively, $\pm 1, \pm 5, \pm 2, \pm 4$, and ± 3, all mod 11.

(c) Find the solutions to $x^2 \equiv a \pmod{121}$ for $a = 1, 3, 4, 5, 9$. The polynomial is easily seen to be nonsingular in all cases, so every solution lifts to exactly one solution mod 121.

We can lift a solution x by setting the new solution equal to $x + 11t$, and then the equivalence $a \equiv (x + 11t)^2 \equiv x^2 + 2 \cdot x \cdot (11t) \pmod{121}$ gives that we can find t to be

$$t \equiv \frac{a - x^2}{11} \cdot \frac{1}{2x} \pmod{11},$$

where the first fraction is calculated as an integer, since $x^2 \equiv a \pmod{11}$, and the second fraction just means multiplying by the inverse of $2x$ mod 11. Using this formula, we find the following:

For $a = 1$, $x = \pm 1$, $t = 0$ so the new solutions are just ± 1.

For $a = 3$, $x = \pm 5$, $t = \pm 2$ so the new solutions are ± 27.

For $a = 4$, it's easy to see you'll get ± 2 since they work in the integers.

For $a = 5$, $x = \pm 4$, $t = \pm 4$, so the new solutions are ± 48.

Finally, for $a = 9$, you must get ± 3, since it holds in the integers.

11. (Niven 3.2.6a & 3.2.11)

(a) Write down the quadratic residues for $p = 7, 13, 17$, and 29.

From a bit of calculation, we find the quadratic residues in the table below:

p	QR's
7	1,2,4
13	1,3,4,9,10,12
17	1,2,4,8,9,13,15,16
29	1,4,5,6,7,9,13,16,20,22,23,24,25,28

(b) Prove that if p is an odd prime, then there are equally many quadratic residues and nonresidues mod p.

In class, we saw that for an odd prime, the QR's are exactly the even powers of a primitive root. Since there are an equal number of even and odd powers of the generator, there are an equal number of QR's and QNR's.

A second way to prove this is to consider the map of multiplication by a QNR. We know this map takes QR's to QNR's and QNR's to QR's. Since this map is a bijection on the residues mod p (because it is invertible), it shows that the set of QR's is equal to the set of QNR's.

(Bonus) Suppose that $q \equiv 1 \pmod{4}$ is prime, and that $p = 2q + 1$ is also prime. Prove that 2 is a primitive root modulo p.

Remark. *Such a p is known as a "Sophie Germain" prime; it is believed that there are infinitely many, but this is not known.*