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.

   (b) Determine the order of 9 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 $x^2 + x + 7 \equiv 0 \pmod{81}$.

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

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

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.*

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

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

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)?

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) $x^2 + x - 1 \equiv 0 \pmod{13}$.

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 $f'(x_0) \equiv 0 \pmod p$.

   (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'.

   (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 $g(x) = Ax^3 + Cx + D$.

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

10. (Niven 3.2.5)

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

    (b) Find the solutions to $x^2 \equiv a \pmod{11}$ for $a = 1, 3, 4, 5, 9$.

    (c) Find the solutions to $x^2 \equiv a \pmod{121}$ for $a = 1, 3, 4, 5, 9$.

11. (Niven 3.2.6a & 3.2.11)

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

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

(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.*