

## 18.781 Problem Set 4 - Fall 2009

Due Thursday, Oct. 15 at 2:30

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

- (Niven 2.5.3) If you are able to factor  $n = p_1 p_2$ , then it is easy to calculate  $\phi(n) = (p_1 - 1)(p_2 - 1)$ . Show that this also works in reverse: If you are given  $n = p_1 p_2$  and the value of  $\phi = (p_1 - 1)(p_2 - 1)$ , solve for  $p_1$  and  $p_2$ .
- (Niven 2.5.5) If  $m$  is not squarefree, show that there exist  $a_1, a_2$  such that  $a_1 \not\equiv a_2 \pmod{m}$ , but  $a_1^k \equiv a_2^k \pmod{m}$  for  $k \geq 2$ .
- (Niven 2.8.3) How many primitive roots does 13 have?
- (Niven 2.8.9 & 2.8.15)
  - Show that  $3^8 \equiv -1 \pmod{17}$ . Explain why this implies that 3 is a primitive root modulo 17.
  - Prove that if  $a$  has order  $h$  modulo  $p$ , and  $h$  is even, then  $a^{\frac{h}{2}} \equiv -1 \pmod{p}$ .
- (Niven 2.8.7) If  $p \geq 3$  is prime, how many solutions are there to  $x^{p-1} \equiv 1 \pmod{p}$ ? How many solutions are there to  $x^{p-1} \equiv 2 \pmod{p}$ ?
- (Niven 2.8.8) Determine how many solutions there are to:
  - $x^{12} \equiv 16 \pmod{17}$
  - $x^{48} \equiv 9 \pmod{17}$
  - $x^{20} \equiv 13 \pmod{17}$
  - $x^{18} \equiv 11 \pmod{23}$ .
- (Niven 2.8.14) Suppose that the order  $\pmod{p}$  of  $a$  is  $h$  and that  $\bar{a}$  satisfies  $a\bar{a} \equiv 1 \pmod{p}$ . Show that the order of  $\bar{a}$  is  $h$  as well. Furthermore, if  $a \equiv g^i \pmod{p}$  for some primitive root  $g$ , show that  $\bar{a} \equiv g^{p-1-i} \pmod{p}$ .
- (Niven 2.8.18) Show that if  $g$  and  $g'$  are both primitive roots modulo an odd prime  $p$ , then  $gg'$  is not a primitive root. (*Hint: Use the fact that  $p - 1$  is even.*)
- Check that 5 is a primitive root modulo 23. Which number(s) of the form  $5 + 23k$  (with  $0 \leq k \leq 22$ ) is *not* a primitive root modulo  $23^2$ ?
- (Niven 2.7.1) Solve the congruence  $x^2 + x + 7 \equiv 0 \pmod{81}$ .
- (Niven 2.7.4) Solve the congruence  $x^2 + 5x + 24 \equiv 0 \pmod{36}$ .
- (Niven 2.7.6) Solve the congruence  $x^3 + x^2 - 4 \equiv 0 \pmod{343}$ .
- (Niven 2.7.9) This problem explains how to lift solutions in the nonsingular case more quickly (using successive squaring).
  - 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  $f'(a) \pmod{p^j}$  rather than just  $\pmod{p}$ .*

- (b) If  $f(a_0) \equiv 0 \pmod{p}$ , explain how part (a) lets us find  $a_1, a_2, \dots$  such that  $f(a_i) \equiv 0 \pmod{p^{2^i}}$ .
- (c) Solve  $x^3 + x^2 + 4 \equiv 0 \pmod{3^8}$ .
14. 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)?
15. (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, and assume  $p \nmid a$ .
- (a) If  $p \mid D$ , show that  $f(x) \equiv 0 \pmod{p}$  has one solution  $x_0$ , and that  $f'(x_0) \equiv 0 \pmod{p}$ .
- (b) If  $p \nmid D$ , show that  $f(x) \equiv 0 \pmod{p}$  has zero or two solutions, and that  $f'(x') \not\equiv 0 \pmod{p}$  for any solution  $x'$ .
- (c) Prove that  $f(x) \equiv 0 \pmod{p^2}$  has 0, 1, 2,  $p$ , or  $p^2$  solutions.
16. (*Completing the cube*)
- (a) Suppose that  $f(x) = ax^3 + bx^2 + cx + d$  with  $p \nmid a$  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  $x^3 + 6x^2 - 6x - 18 \equiv 0 \pmod{23}$ .
17. 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.*