

## 18.781 Problem Set 5 - Fall 2009

Due Thursday, Oct. 22 at 2:30

1. (a) Show that the order of 3 (mod 32) is 8 ( $e_{32}(3) = 8$ ), 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.  
(c) Prove that the order of  $g \pmod{2^k}$  is  $2^{k-2}$  ( $e_{2^k}(g) = 2^{k-2}$ ) if and only if  $g \equiv 3$  or  $5 \pmod{8}$ .
2. (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  $a = 1, 3, 4, 5, 9$ .
3. (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  $p$ .
4. Prove that if  $p \mid (n^2 - 5)$  for some integer  $n$ , then  $p \equiv 1$  or  $4 \pmod{5}$ .
5. (Niven 2.4.10 & 2.4.11)
  - (a) Suppose that  $m \not\equiv \pm 1 \pmod{n}$  and  $m^2 \equiv 1 \pmod{n}$ . Prove that at least one of  $(n, m + 1)$  and  $(n, m - 1)$  is a nontrivial divisor of  $n$ .
  - (b) Show that 341 is a pseudoprime for the base 2, but is not a strong pseudoprime. In particular,  $2^{85} \equiv m \not\equiv \pm 1 \pmod{341}$ , but  $2^{170} \equiv 1 \pmod{341}$ . Find a nontrivial divisor of 341.
6. Suppose that  $n$  is squarefree. Prove that  $n$  is a probable prime to base  $a$  for all  $a$  if and only if  $(p - 1) \mid (n - 1)$  for every prime divisor  $p \mid n$ .
7. (Niven 2.4.4)
  - (a) Show that 561 is probable prime to any base.
  - (b) Show that it is composite by showing that it is not a strong probable prime for base 2.
8. (Niven 2.8.33,34,35)
  - (a) Let  $a, k$  be positive integers,  $a > 1$ . Show that  $k \mid \phi(a^k - 1)$ .
  - (b) Show that if  $p \mid \phi(m)$  and  $p \nmid m$ , then there is at least one prime  $q$  such that  $q \mid m$  and  $q \equiv 1 \pmod{p}$ .
  - (c) Prove that for any prime number  $p$ , there are infinitely many primes  $q$  such that  $q \equiv 1 \pmod{p}$ .
9. Let  $m$  be an odd positive integer and let  $n$  be any positive integer. Show that  $(2^m - 1, 2^n + 1) = 1$