

## HW ASSIGNMENT #6 (DUE THURSDAY, MARCH 13)

1. If  $(a, n) = 1$ , prove that  $a^i \equiv a^j \pmod{n}$  if and only if  $i \equiv j \pmod{e_n(a)}$ .
2. If  $(a, n) = 1$  and  $e_n(a) = st$ , show that  $e_n(a^s) = t$ .
3. If  $(a, n) = (b, n) = (e_n(a), e_n(b)) = 1$ , prove that  $e_n(ab) = e_n(a) \cdot e_n(b)$ .
4. If  $m = a^n - 1$ , prove that  $n \mid \phi(m)$ . [**Hint:** First prove that  $e_m(a) = n$ .]
5. Let  $p$  be a prime number. For any positive integer  $k$ , prove that

$$1^k + 2^k + 3^k + \cdots + (p-1)^k \equiv \begin{cases} 0 \pmod{p} & \text{if } p-1 \nmid k \\ -1 \pmod{p} & \text{if } p-1 \mid k \end{cases}$$

6. If  $p$  is a prime and  $p \equiv 1 \pmod{4}$ , prove that there is an integer  $x$  such that  $x^2 \equiv -1 \pmod{p}$ . [**Hint:** Use the fact, shown during the proof of Theorem 21.2, that if  $d \mid p-1$  there are exactly  $\phi(d)$  distinct integers  $a \pmod{p}$  with  $e_p(a) = d$ .]
7. If  $p$  and  $q = 2p+1$  are both prime, prove that 2 is a primitive root modulo  $q$  if and only if  $2^p \equiv -1 \pmod{q}$ .
8. If  $p$  and  $q$  are distinct odd primes, show that  $pq$  is a pseudoprime to the base 2 if and only if  $e_q(2) \mid (p-1)$  and  $e_p(2) \mid (q-1)$ .
9. Let  $n \geq 2$  be a positive integer.
  - a. If  $n$  is divisible by two distinct odd primes  $p$  and  $q$ , prove that there are no primitive roots modulo  $n$ .
  - b. If  $n$  is divisible by  $4p$ , where  $p$  is an odd prime, prove that there are no primitive roots modulo  $n$ .
  - c. If  $n = 2^k$  with  $k \geq 3$ , prove that there are no primitive roots modulo  $n$ . [**Hint:** Use induction on  $k$  to prove that if  $a$  is any odd integer, then  $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ .]
  - d. Conclude from parts (a)-(c) that if  $n$  has a primitive root, then either  $n = 2$ ,  $n = 4$ ,  $n = p^k$ , or  $n = 2p^k$  for some odd prime number  $p$  and some integer  $k \geq 1$ . (It is a difficult theorem due to Gauss that the converse of this statement holds as well.)