

## Math 25 Final Exam

December 7, 2009

**Instructions:** You should show all of your work and reasons for your computations with the exception that you may solve simple congruences by inspection.

1. Show that 3 is a primitive root modulo 34; then use index arithmetic to find all solutions to  $x^{12} \equiv 13 \pmod{34}$ . **Note:** You do not need to simplify your final answer, and you may assume that  $3^4 \equiv 13 \pmod{34}$ .

2. Describe the congruences which characterize all the odd primes  $p$  for which 7 is a quadratic residue modulo  $p$ . **Note:** Your final answer should have the form  $p \equiv a_1, \dots, a_r \pmod{n}$  for appropriate  $a_i$  and  $n$ .

3. Show that no prime  $p \equiv 7 \pmod{8}$  can be written as the sum of three squares in  $\mathbb{Z}$ .

4. Prove directly (don't quote a general result) that 7 is a Gaussian prime.

5. Suppose that  $F$  and  $g$  are arithmetic functions, and that  $F(n) = \sum_{d|n} g(d)$ , and that  $g(1) = 1$ ,  $g(3) = 4$ ,  $F(2) = 3$ ,  $F(4) = 5$ ,  $F(6) = 7$  and  $F(12) = 11$ .

(a) What is  $g(12)$ ?

(b) Is  $F$  multiplicative? Completely multiplicative?

6. Suppose that  $f$  and  $g$  are multiplicative arithmetic functions.

(a) Show that the product  $(fg)(n) = f(n)g(n)$  is multiplicative.

(b) Suppose that  $f$  is multiplicative and  $\mu$  is the Möbius function. If  $n = p_1^{e_1} \cdots p_r^{e_r}$  with the  $e_i \geq 1$ , show that

$$\sum_{d|n} \mu(d)f(d) = (1 - f(p_1))(1 - f(p_2)) \cdots (1 - f(p_r)).$$

7. Define  $\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, p \text{ a prime, } k \geq 1 \\ 0 & \text{otherwise.} \end{cases}$

You may assume without proof that  $\sum_{d|n} \Lambda(d) = \log(n)$ . Use Möbius inversion to show

that  $\Lambda(n) = - \sum_{d|n} \mu(d) \log(d)$

8. Define  $\sigma_{-1}(n) = \sum_{d|n} d^{-1} = \sum_{d|n} \frac{1}{d}$ . Suppose that  $n$  is a perfect number. Show that  $\sigma_{-1}(n) = 2$ . *Hint:* Expand  $n\sigma_{-1}(n)$ .

9. Let  $k$  and  $n$  be positive integers, and suppose that  $\gcd(k, \phi(n)) = 1$ , where  $\phi$  is the Euler phi function. Show that the congruence  $x^k \equiv a \pmod{n}$  is solvable for all  $a \in U_n$ .  
*Hint:* What would Bezout say? While you can solve this without further constraint, you may assume if you like that there is a primitive root modulo  $n$ .

10. Let  $p_1, \dots, p_r$  be distinct odd primes, and let  $\varepsilon_1, \dots, \varepsilon_r \in \{\pm 1\}$  (i.e., for each  $i$ , fix  $\varepsilon_i = 1$  or  $-1$ ). Show that there exist infinitely many integers  $a$  so that  $\left(\frac{a}{p_i}\right) = \varepsilon_i$  for all  $i$  (simultaneously).

11. Short answer/True-False. Answer the questions below with only a brief explanation.

(a) For an odd prime  $p$ ,  $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) =$

(b) (True/False) If  $n$  is a positive integer, and for all integers  $a$  with  $\gcd(a, n) = 1$ , we have  $a^{n-1} \equiv 1 \pmod{n}$ , then  $n$  is prime.

(c) How many primitive roots are there modulo the prime  $p = 257$ .

(d) Suppose that  $g$  is a primitive root modulo the odd prime  $p$ . Can one determine the value of the Legendre symbol  $\left(\frac{g}{p}\right)$ ? If so, what is it? If not, why not?

(e) Compute  $\gcd(7469, 2464)$ .

(f) Compute  $5^{2009} \pmod{11}$ .

(g) Can the integer  $5^3 11^2$  be expressed as the sum of two squares in  $\mathbb{Z}$ ?

(h) Are there infinitely many primes  $p$  such that  $\left(\frac{p}{7}\right) = 1$ ? You may quote any theorem you like to answer this one way or the other.

(i) Find all incongruent solutions modulo 168 (if any) to the system:  $7x \equiv 3 \pmod{12}$  and  $10x \equiv 6 \pmod{14}$ .

(j) Compute the value of the Legendre symbol  $\left(\frac{117}{1151}\right)$ , noting that 1151 is a prime.