Mathematics 124 Fall 2003

MIDTERM
DUE, Wednesday, November 5, 11:00 AM

Remarks: On the midterm no collaboration is allowed. Show all your working, and write up your solutions as neatly as possible. The points on the Exam total 105, although only the first 100 points will count. If you have any questions, don't hesitate to email me at `fcale@math.harvard.edu`.

1. (20 points) Find the general solution to the following simultaneous equations:

$$x \equiv 55 \mod 77, \qquad x \equiv 33 \mod 99, \qquad x \equiv 99 \mod 111.$$

   Show all your working.

2. (10 points) State the law of quadratic reciprocity, and use it to calculate which of the primes $p = 2$, 3, 5 and 7 are quadratic residues modulo 2003. You may assume that 2003 is prime.

3. (10 points) Let $p \geq 5$ be prime. Show that the sum of all the quadratic residues is 0 modulo p.

4. (a) (10 points) Find a prime p such that 2, 3, and 5 are all primitive roots modulo p.

   (b) (10 points) Prove that if 2 and 3 are primitive roots modulo p, then 6 is *not* a primitive root modulo p.

5. Let p be an odd prime.

   (a) (5 points) Suppose that $a \not\equiv 0 \mod p$. Find all solutions to the equation

$$x + \frac{1}{x} = a + \frac{1}{a} \mod p.$$

   (b) (5 points) Prove that exactly $(p+1)/2$ of the residues $0, 1, \ldots p-1$ modulo p can be written in the form $(a + 1/a)$ modulo p.

   (c) (7 points) Prove that m can be written in the form $(a + 1/a)$ modulo p if and only if $m^2 - 4$ is a quadratic residue modulo p.

   (d) (3 points) For what primes p can 1 be written in the form $a + 1/a$?

6. **A primality test for Fermat numbers**.

(a) (5 points) Suppose that $a^n \equiv 1 \mod m$. Prove that a has exact order n if and only if for each prime divisor q of n, one has

$$a^{n/q} \not\equiv 1 \mod m.$$

(b) (5 points) Suppose that a modulo m has order exactly $m-1$. Prove that m is prime. Hint: show that if m is composite, then $\varphi(m) < m-1$.

(c) (7 points) Let $k \geq 1$, and let $m = 2^{2^k} + 1$. Suppose that

$$3^{\frac{m-1}{2}} \equiv -1 \mod m.$$

Prove that 3 has exact order $m-1$, and that m is prime.

(d) (8 points) Let $k \geq 1$, and let $m = 2^{2^k} + 1$, and assume that m is prime. Prove that

$$3^{\frac{m-1}{2}} \equiv -1 \mod m.$$