Mathematics 124 Fall 2003

HOMEWORK ASSIGNMENT # 5
DUE, Friday, October 31

Collaboration: On the homework sets, collaboration is not only allowed but encouraged. However, you must write up and understand your own individual homework solutions, and you may not share written solutions. If you learn how to solve a problem by talking to a classmate, CA, or looking it up in a book, you should cite the source in your homework write-up, just as you would reference your sources in a literature or history class.
Show all your working, and write up your solutions as neatly as possible.

1. (2 points) Find the smallest prime p such that
$$\left(\frac{-163}{p}\right) = 1.$$

2. It is a theorem of Dirichlet that for any coprime integers a and b, there exist infinitely many primes of the form $a + bn$. You may assume this theorem when solving the following problem.
   (a) (3 points) Let q be prime. Prove there exists infinitely many primes p such that q is not a quadratic residue modulo p.
   (b) (4 points) Let $m = q_1 q_2 \dots q_n$ be a product of distinct primes. Prove that there exists infinitely many primes p such that q_1 is not a quadratic residue modulo p, but $q_2, \dots q_n$ are quadratic residues modulo p. (Hint: Use the Chinese remainder theorem).
   (c) (1 point) Prove that any positive integer m can be written in the form $n^2 \cdot q_1 q_2 \dots q_n$, where q_i are distinct primes.
   (d) (1 point) Conclude that any integer positive m is either a quadratic non-residue modulo infinitely many prime numbers p, or that m is a perfect square.

3. Let p be an odd prime. Let q be a prime such that $q \equiv 1 \mod p$.
   (a) (1 point) Prove there exists an element ζ that, modulo q, has order exactly p.
   (b) (3 points) If $p = 3$, show that $(2\zeta + 1)^2 = -3 \mod q$.

4. (3 points) Let m be a positive integer. Prove that the number of solutions modulo m to the equation:
$$x^2 \equiv 1 \mod m.$$
is always a power of 2.

5. (2 points) Let $p \geq 5$ be prime. Prove that

$$\binom{2p}{p} \equiv 2 \mod p^3.$$