Math 160a - Fall 2002
Lloyd Kilford

Homework set 1
Due: 10th October 2002

1. Let p be an odd prime. Prove that the number of solutions to $x^2 \equiv a \mod p$ is $1 + \left(\frac{a}{p}\right)$, and hence show that there are two solutions to

$$x^2 + 4x + 11 \equiv 0 \mod 37.$$

2. Find all primes p such that 5 is a square modulo p.

3. Compute $\left(\frac{372}{307}\right)$ and $\left(\frac{475}{401}\right)$. You may assume that 307 and 401 are both prime.

4. Is 3 a generator modulo 211? You may assume that 211 is prime.

5. Let K be a finite field of size q. What is the group of cubes in K? What is the group of n^{th} powers?

6. Find a quadratic form of the form $\alpha x^2 + \beta y^2$ defined over $\mathbf{F}_7$ which represents all elements of $\mathbf{F}_7^*$, but does not nontrivially represent 0. Comment on why this form does not represent 0. (Think about the Legendre symbol).

7. Let p be a Fermat prime (in other words, $p = 2^{2^i} + 1$ for some i). What is the value of $\left(\frac{2}{p}\right)$?