MATH 42-NUMBER THEORY
PROBLEM SET #6
DUE THURSDAY, MARCH 24, 2011

2. Give a characterization of the squares in terms of a generator. That is, which powers of a generator are squares?

Solution: Even powers of generators are squares.

3. Prove the following properties of the Legendre symbol.

(a) $\left(\frac{1}{p}\right) = 1$
(b) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$
(c) $\left(\frac{a^2}{p}\right) = 1$

Solution:

(a) $\left(\frac{1}{p}\right) = 1$ since for any p, $1 \equiv 1^2 \mod p$.
(b) We can use Euler's criterion.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} \equiv a^{(p-1)/2} b^{(p-1)/2} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.$$

Alternately, we could have proved this by proving that a square times a square is a square, a non-square times a non-square is a square, and a non-square times a square is a non-square. The easiest way to do this is to use the characterization of squares in terms of generators.
(c) $\left(\frac{a^2}{p}\right) = 1$ since a^2 is clearly always a square mod p.

7. Prove that -1 is a square mod p if and only if $p \equiv 1 \mod 4$. (That is, prove that if $p \equiv 1 \mod 4$, then -1 is a square, and also prove that if -1 is a square mod p, then $p \equiv 1 \mod 4$.)

Solution: If $p \equiv 1 \mod 4$, then $p = 4k + 1$ for some $k \in \mathbb{N}$. Euler's criterion tells us that $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \mod p$, so we get

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = (-1)^{2k} = 1 \mod p.$$

Thus, if $p \equiv 1 \mod p$, $\left(\frac{-1}{p}\right) = 1$.

On the other hand, we know that if $\left(\frac{-1}{p}\right) = 1$, then $(-1)^{(p-1)/2} \equiv 1 \mod p$, so $(p-1)/2$ must be even. In other words, $(p-1)/2 = 2k$ for some integer k, and $p = 4k + 1$. That is, $p \equiv 1 \mod 4$.

9. Prove that if a and b are natural numbers that can be written as the sum of two squares, then ab can also be written as the sum of two squares.

Solution: If a and b can be written as the sum of two squares, we have $a = m^2 + n^2$ and $b = s^2 + t^2$ for integers m, n, s, t. Then $ab = m^2s^2 + m^2t^2 + n^2s^2n^2t^2$. We notice that this is $ab = (ms + nt)^2 + (mt - ns)^2$, so ab is a sum of two squares also.

10. Is it true that if a and b are natural numbers that cannot be written as the sum of two squares, then ab cannot be written as the sum of two squares?

Solution: No, it's not true. For example, 6 can't be written as the sum of two squares and 3 can't be written as the sum of two squares. However, $18 = 3^2 + 3^2$.