PRACTICE PROBLEMS FOR THE FIRST MIDTERM

1. Give the definition of:

(i) a representation as a sum of two squares.
(ii) a primitive representation.
(iii) $p_2(n)$.
(iv) an involution.
(v) the conjugate of a Gaussian integer.
(vi) the norm of a Gaussian integer.
(vii) $r_2(n)$.
(viii) a curve of genus zero.

2. If a is not divisible by m and $1 < \lambda < m$ then show that we can find $1 \leq x < \lambda$ and $1 \leq |y| \leq m/\lambda$ such that $ax \equiv y \mod m$.
3. Suppose that $n > 1$ is an integer of which -1 is a quadratic residue. Exhibit a correspondence between solutions of the equation $u^2 \equiv -1 \mod n$ and pairs of integers x and y such that

$$n = x^2 + y^2 \qquad x > 0 \qquad y > 0 \qquad (x, y) = 1 \qquad \text{and} \qquad y \equiv ux \mod n.$$

4. Show that every positive prime of which -2 is a quadratic residue can represented in the form $x^2 + 2y^2$.
5. Show that every prime congruent to 1 or 3 modulo 8 is a sum of three squares.
6. Factor

$$1{,}000{,}009 = 972^2 + 235^2.$$