Problem Set 5.

1. Use the Minkowski lattice point theorem to prove that every prime congruent to 1 modulo 6 can be written in the form $x^2+3y^2$. Show similarly that all primes congruent to 1 modulo 8 are of the form $x^2+2y^2$. Hint: Consider a lattice in two–dimensional space where the first coordinate is congruent to a multiple of the second modulo p, with the multiple chosen to be a square root of -3 or -2 modulo p.

2. Prove the statements below to show that every positive integer is the sum of four integer squares.
   a) Show that if m and n are the sum of four integer squares, then so is mn, by studying the multiplication in the quaternions $\mathbf{H} = \mathbf{Q} + \mathbf{Q}\mathbf{i} + \mathbf{Q}\mathbf{j} + \mathbf{Q}\mathbf{k}$, where $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$. Show that the determinant of the linear map multiplication by $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ on the algebra of quaternions is the square of $a^2 + b^2 + c^2 + d^2$.
   b) Show by counting the number of squares in a finite field that the equation $au^2 + bv^2 = c$ is always solvable in a finite field if $a, b, c$ are elements of the field with $ab \neq 0$.
   c) Use the Minkowski lattice point theorem to prove that every prime is the sum of four integer squares, and hence that all positive integers are.

3. Show that the discriminant of the product of two polynomials is the product of their discriminants times the square of their resultant.

4. Let $K$ be a number field of degree at least 2 and $p$ a prime number. Consider the order $\mathcal{O} = \mathbf{Z} + p\mathcal{O}_K$. Show that $P = p\mathcal{O}_K$ is a noninvertible prime ideal of $\mathcal{O}$. Show that the ideal $p\mathcal{O}$ of the order $\mathcal{O}$ does not factor as a product of prime ideals of $\mathcal{O}$.