Problem Set 3.

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 $\mathbb{H} = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, where $i^2 = j^2 = k^2 = -1$. Show that the determinant of the linear map multiplication by $a + bi + cj + dk$ 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. (a) Let $\alpha_1, \ldots, \alpha_{n-1}$ be real numbers, and let $t > 0$ be a positive real number. By considering the lattice in $\mathbb{R}^n$ spanned by $(t, 0, \ldots, 0), (0, t, 0, \ldots, 0), \ldots, (0, 0, \ldots, t, 0)$ and $(-\alpha_1 t, -\alpha_2 t, \ldots, -\alpha_{n-1} t, 1/t^{n-1})$ and the region $P = \{(x_1, \ldots, x_n) ||x_i|| \leq 1\}$ show that the real numbers $\alpha_i$ can be simultaneously approximated by rationals in the sense that there exists integers $q \leq tn^{-1}, p_i$ such that $|q\alpha_i - p_i| < 1/t$. Remark: This can also be proved by the Dirichlet box principle applied to fractional parts of vectors $k(\alpha_1, \alpha_2, \ldots)$ as $k$ varies from 1 to $q^{n-1}$.

   (b) Use Minkowski’s Theorem to show that if coins of radius $r$ are placed at all nonzero points of the integer lattice in the plane, then the length of a radial segment from the origin which misses all coins is at most $1/r$. How about the similar problem with marbles of radius $r$ at nonzero integer lattice points in 3–space?

   (c) Show that if $\alpha$ is real irrational, there are infinitely many rational numbers $p/q$ such that $|\alpha - p/q| \leq 1/q^2$. It is a major Diophantine approximation result of Roth that there are only finitely many rational numbers approximating an real algebraic $\alpha$ with exponent greater than 2, that is if $\alpha$ is a real algebraic irrational, $\epsilon > 0$ there are only a finite number of rationals $p/q$ with $|\alpha - p/q| \leq 1/q^{2+\epsilon}$. Bombieri has shown that versions of the ABC conjecture imply even stronger versions of Roth’s theorem.