Algebraic Number Theory

Problem sheet 0

For the first class, I would like to discuss some warm-up examples of Diophantine equations and try to explain some motivations of algebraic number theory. The theory of Diophantine equations is an important branch of number theory which deals with the solutions of polynomial equations in either integers or rational numbers. For simplicity, we only consider the plane algebraic curve defined by $F(x, y)$ where $F(x, y) \in \mathbb{Q}[x, y]$.

The following are basic question about the equation $F(x, y) = 0$ we want to ask:
Q1:Does there exist a rational(or integer) solution?
Q2:If there exists a solution, is it true that the set of rational(or integer) solution is finite?
Q3:Can we find all of ratinoal(or integer) solution?

1. First we consider the degree one case: $ax + by = c$, where $a, b, c \in \mathbb{Q}$ and a, b not all zero.
   (a) Show that the equation admits infinitely many rational solutions and find all of them.
   (b) Assume $a, b, c \in \mathbb{Z}$, prove that the equation has integer solution if and only if $\gcd(a, b)|c$. In this case, find all integer solutions
2. Next we turn to case of degree two.
   (a) Find all rational and integer solutions of equation $x^2 + y^2 = 1$.
   (b) More generally, let $F(x, y)$ be a "general"(or irreducible) quadratic polynomial over $\mathbb{Q}$, show that either $F(x, y) = 0$ has no rational solution or it admits infinitely many rational solutions.
   (c) Give an example of quadratic polynomial defind over $\mathbb{Q}$ such that it has no rational solution.

   Remark. In particular, for quadratic curves, it is remained to consider the integer solutions and we will deal with this in the following several exercises.
3. We shall discuss the family of equations $x^2 + y^2 = r$ at the same time, where r runs through the set of rational numbers.
   (a) show that $\mathbb{Z}[\sqrt{-1}]$ is euclidean.
   (b) show that $\alpha \in \mathbb{Z}[\sqrt{-1}]$ is a unit if and only if $N(\alpha) = 1$ where $N(a + b\sqrt{-1}) := a^2 + b^2$. Hence find all units of this ring.
   (c) Let $r = p$ be a prime number, show that TFAE(the following are equivalent):
      i. $x^2 + y^2 = p$ has integer solution

ii. $p = 2$ or $p \equiv 1 \mod 4$.

iii. p is not a prime element in $\mathbb{Z}[\sqrt{-1}]$

Further, determine the number of integer solutions in this case.

(d) Let $r = n$ be a positive integer, determine when the associated equation has integer solution. In this case, determine the number of integer solutions.

(e) Finally let's consider the general case, namely when r is a rational number. Determine when the equation has a **rational** solution and in this case try to find the number of rational solutions

4. (a) show that the equation $x^2+2y^2 = 1$ has finitely many integer solutions and deduce that $\mathbb{Z}[\sqrt{-2}]$ has finitely many units.(what are they?)

(b) show that $\mathbb{Z}[\sqrt{2}]$ is euclidean.

(c) Find a nontrivial integer solution of $x^2 - 2y^2 = 1$. Show that the equation has infinitely many integer solution and show that the ring $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.

5. (a) show that the equation $x^2+3y^2 = 1$ has finitely many integer solutions and deduce that $\mathbb{Z}[\sqrt{-3}]$ has finitely many units.(what are they?)

(b) show that $\mathbb{Z}[\sqrt{3}]$ is euclidean.

(c) Find a nontrivial integer solution of $x^2 - 3y^2 = 1$. Show that the equation has infinitely many integer solution and show that the ring $\mathbb{Z}[\sqrt{3}]$ has infinitely many units.

6. Finally let us see some examples of cubic curves. Let us study the family of elliptic curves $x^3 + y^3 = r$, $r \in \mathbb{Q}$

(a) Let $r = p$ be a prime, prove that the associated equation has integer solution if and only if $p = 2$ or $p = 1 + 3n + 3n^2$ for some integer n.

(b) For every $0 \neq r \in \mathbb{Q}$ show that the equation $x^3 + y^3 = r$ has only finitely many integer solutions.

Remark. i. The finiteness of integer solutions holds for every elliptic curves, which is so-called Siegel's Theorem.

ii. The set of rational solution of an elliptic curve is an important object in number theory. It turns out that (if the set is not empty) the set has a natural group structure and Mordell Theorem tells us that the group is a finitely generated abelian group. Mazur shows that the torsion part of the group is very restrictive. Hence it suffices to study the torsion-free part, that is its rank, which, by BSD conjecture, is expected to be equal to some value of the associated L function.

iii. The case of higher degree is easy in some sense. In fact, Faltings proves that for "smooth" curve of higher degree(or higher genus if you are familiar with Algebraic Geometry), there are only finitely many rational solutions.

7. Show that Fermat equation $x^3 + y^3 = 1$ has no nontrivial rational solution, which is a special case of Fermat's Last Theorem.