M4/5P14 - DIOPHANTINE EQUATIONS

0.1. **Thue's Theorem.**

Theorem 0.1 (Thue's Theorem)**.** *Let*

$$f(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n$$

be a polynomial of degree $n \geq 3$ with $a_0, \ldots, a_n \in \mathbb{Z}$. Assume that f is irreducible and let m be a non-zero integer.
Then the equation

$$f(x,y) = m$$

admits at most finitely many solutions.

Recall that a polynomial f is irreducible if for any polynomials g and h with rational coefficients such that

$$f = g \cdot h$$

we have that either g or h is constant.

We will use the following generalisation of Dirichlet Theorem (we will omit the proof):

Theorem 0.2 (Siegel Theorem)**.** *Let α be an algebraic number of degree $n \geq 3$ and let $\varepsilon > 0$.*
Then there exist at most finitely many rational numbers x/y such that

$$|\alpha - \frac{x}{y}| < \frac{\varepsilon}{|y|^n}.$$

Proof of Theorem 0.1.
Note that by assumption $a_0 \neq 0$.
Suppose that

$$f(x,y) = m$$

admits infinitely many solutions $x_k, y_k \in \mathbb{Z}$, with $k \in \mathbb{N}$. Since $f(x,0) = m$ admits at most two solutions with $x \in \mathbb{Z}$, we may assume that $y_k \neq 0$ for all k.
Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be the solutions of $f(z,1) = 0$. Since f is irreducible, the α_i are all distinct. Then

$$|m| = |f(x_k, y_k)| = |y_k^n f(x_k/y_k, 1)|. \tag{1}$$

Note that if $\alpha_i \notin \mathbb{R}$ for all i, then there exists $c > 0$ such that

$$|f(z,1)| > c$$

for all $z \in \mathbb{R}$. Thus, $|y_k|^n < |m|/c$, which immediately implies a contradiction.

We now consider the general case. By (1), we have

$$\begin{aligned}|m| =&|a_0 y_k^n \prod_{i=1}^{n}(\alpha_i - \frac{x_k}{y_k})|\\ \geq&|y_k^n \prod_{i=1}^{n}(\alpha_i - \frac{x_k}{y_k})|.\end{aligned}$$

Let

$$A = \min_{i\neq j} \frac{|\alpha_i - \alpha_j|}{2}.$$

If k is sufficiently large then

$$|y_k| > |m|^{1/n}/A.$$

Thus,

$$|\prod_{i=1}^{n}(\alpha_i - \frac{x_k}{y_k})| < A^n.$$

In particular, there exists $i \in \{1, \ldots, n\}$ (depending on k) such that

$$|\alpha_i - \frac{x_k}{y_k}| < A.$$

We may assume that for infinitely many values of k, the index i is constant. By the definition of A, we also have

$$|\alpha_j - \frac{x_k}{y_k}| \geq |\alpha_j - \alpha_i| - |\alpha_i - \frac{x_k}{y_k}| > 2A - A = A$$

for all $j \neq i$. It follows that

$$|\alpha_i - \frac{x_k}{y_k}| < \frac{|m|}{A^{n-1}|y_k^n|}$$

for infinitely many k.
Let $a, b \in \mathbb{R}$, such that $\alpha_i = a + bi$. Then if $b \neq 0$ we have

$$|b| < \frac{|m|}{A^{n-1}|y_k^n|}$$

which implies

$$|y_k^n| < \frac{|m|}{A^{n-1}|b|}$$

for infinitely many k, a contradiction. Thus, we may assume that α_i is real. Note that α_i is algebraic of degree n which admits infinitely many rational numbers x_k/y_k such that

$$|\alpha_i - \frac{x_k}{y_k}| < \frac{\epsilon}{|y_k|^n}$$

where $\epsilon = |m|/A^{n-1}$, contradicting Theorem 0.2. □

0.2. **Binary Forms.**
A **binary integral form** f is an integral homogeneous polynomial in two variables, i.e.

$$f(x.y) = \sum_{i=0}^{d} a_i x^i y^{d-i},$$

where $a_0, \ldots, a_d \in \mathbb{Z}$. d is called the degree of f.
If $f(1,0) \neq 1$, we define the **discriminant** of f as

$$D_f = a_d^{2d-2} \cdot \prod_{i<j} (\alpha_i - \alpha_j)^2$$

where $\alpha_1, \ldots, \alpha_d$ are the zeroes of $f(x,1)$.

Example 0.3. *Let $f(x,y) = ax^2 + 2bxy + y^2$ be a quadratic form. Then the discriminant of f is*

$$D_f = 4(b^2 - ac).$$

Let $f(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ be a cubic form. Then the discriminant is

$$D_f = 27(-a^2d^2 + 6abcd + 3b^2c^2 - 4ac^3 - 4db^3).$$

Let f, g be binary forms. Then f, g are **equivalent** if there exists

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with $a, b, c, d \in \mathbb{Z}$ such that $\det A = 1$ and

$$|g(x,y)| = |f(ax + by, cx + dy)|.$$

If f and g are equivalent then $D_f = D_g$. In addition, if

$$f(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3,$$

then we can define

$$H^f(x,y) = \frac{-1}{36} \det \begin{pmatrix} f_{x,x} & f_{x,y} \\ f_{y,x} & f_{y,y} \end{pmatrix}$$

and

$$G^f(x,y) = \frac{1}{3} \det \begin{pmatrix} f_x & f_y \\ H_x^f & H_y^f \end{pmatrix}.$$

We will use the following basic result in the theory of binary forms (we will omit the proofs).

Theorem 0.4. *If f and g are equivalent cubics then $H^f = H^g$ and $G^f = G^g$.*

Lemma 0.5. *Let $f(x,y)$ be a binary cubic and let $H = H^f$, $G = G^f$ and $D_1 = \frac{1}{27} D_f$. Then*

$$G^2 + D_1 f^2 = 4H^3.$$

Theorem 0.6. *The number of equivalence classes of binary integral forms of given degree and given discriminant is finite.*

0.3. **Mordell's equation.**

Theorem 0.7 (Mordell's Theorem)**.** *Let d be a non-zero integer. Then the equation*

$$y^2 + d = x^3 \tag{2}$$

admits at most finitely many solutions $x, y \in \mathbb{Z}$.

Let $f(x, y)$ be a cubic form with $D_f = 108d$ and assume that $f(x, y) = 1$ admits a solution $x_0, y_0 \in \mathbb{Z}$. Let

$$x = H(x_0, y_0) \qquad \text{and} \qquad y = G(x_0, y_0)/2.$$

Then Lemma 0.5 implies that x, y are solutions of (2).

Proof. Let us assume that p, q is a solution of (2) and let

$$f(x, y) = x^3 - 3pxy^2 + 2qy^3.$$

We have $f(1, 0) = 1$,

$$H^f(x, y) = \frac{-1}{36} \det \begin{pmatrix} 6x & 6py \\ 6py & 12qy - 6px \end{pmatrix}$$

$$= px^2 - 2qxy + p^2y^2$$

and

$$G^f(x, y) = \frac{1}{3} \det \begin{pmatrix} 3x^2 - 3py^2 & -6pxy + 6qy^2 \\ 2px - 2qy & -2qx + 2p^2y \end{pmatrix}$$

$$= 2(-qx^3 + 3p^2x^2y - 3pqxy^2 + (-p^3 + 2q^2)y^3).$$

In particular,

$$D_f = 108d \qquad p = H^f(1, 0) \qquad \text{and} \qquad q = \frac{-G^f(1, 0)}{2}.$$

Since by Theorem 0.4, H^f and G^f are invariants of the cubic, in order to determine p and q, it is enough to consider equivalence classes of f at any point (x_0, y_0) such that $f(x_0, y_0) = 1$. By Theorem 0.6, there are only finitely many equivalence classes of cubic forms with discriminant equal to $108d$.
For each such form, we solve the equation

$$f(x, y) = 1$$

and Theorem 0.1 implies that there are only finitely many solutions. Thus, the claim follows. □