Chapter 14

Pell's Equation

14.1 Kronecker's Theorem

Diophantine approximation concerns the approximation of real numbers by rationals. Kronecker's Theorem is a major result in this subject, and a very nice application of the Pigeon Hole Principle.

Theorem 14.1. *Suppose $\theta \in \mathbb{R}$; and suppose $N \in \mathbb{N}$, $N \neq 0$. Then there exists $m, n \in \mathbb{Z}$ with $0 < n \leq N$ such that*

$$|n\theta - m| < \frac{1}{N}.$$

Proof. If $x \in \mathbb{R}$ we write $\{x\}$ for the fractional part of x, so that

$$x = [x] + \{x\}.$$

Consider then $N + 1$ fractional parts

$$0, \{\theta\}, \{2\theta\}, \ldots \{N\theta\};$$

and consider the partition of $[0, 1)$ into N equal parts;

$$[0, 1/N), [1/N, 2/N), \ldots, [(N-1)/N, 1).$$

By the pigeon-hole principal, two of the fractional parts must lie in the same partition, say

$$\{i\theta\}, \{j\theta\} \in [t/N, (t+1)/N],$$

where $0 \leq i < j < N$. Setting

$$[i\theta] = r, \ [j\theta] = s,$$

we can write this as

$$i\theta - r, \ j\theta - s \in [t/N, (t+1)/N).$$

Hence

$$|(j\theta - s) - (i\theta - r)| < 1/N,$$

ie

$$|n\theta - m| < 1/N,$$

where $n = j - i,\ m = r - s$ with $0 < n \leq N$. □

Corollary 14.1. *If $\theta \in \mathbb{R}$ is irrational then there are an infinity of rational numbers m/n such that*

$$|\theta - \frac{m}{n}| < \frac{1}{n^2}.$$

Proof. By the Theorem,

$$\begin{aligned} |\theta - \frac{m}{n}| &< \frac{1}{nN} \\ &\leq \frac{1}{n^2}. \end{aligned}$$

□

14.2 Pell's Equation

We use Kronecker's Theorem to solve a classic Diophantine equation.

Theorem 14.2. *Suppose the number $d \in \mathbb{N}$ is not a perfect square. Then the equation*

$$x^2 - dy^2 = 1$$

has an infinity of solutions with $x, y \in \mathbb{Z}$.

Remark: Before we prove the theorem, it may help to bring out the connection with quadratic number fields.

Note first that although d may not be square-free, we can write

$$d = a^2 d',$$

where d' is square-free (and $d' \neq 1$). Pell's equation can then be written

$$x^2 - d'(ay)^2 = 1,$$

which in turn gives

$$\mathcal{N}(z) = 1,$$

where

$$z = x + ay\sqrt{d'}.$$

Thus z is a unit in the quadratic number field $\mathbb{Q}(\sqrt{d'}$.

Let us denote the group of units in this number field by U. Every unit $\epsilon \in U$ is not necessarily of this form. Firstly the coefficient of $\sqrt{d'}$ must be divisible by a; and secondly, if $d' \equiv 1 \bmod 4$ then we are omitting the units of the form $(m + n\sqrt{d'})/2$.

But it is not difficult to see that these units form a subgroup $U' \subset U$ of finite index in U. It follows that U' is infinite if and only if U is infinite.

However, we shall not pursue this line of enquiry, since it is just as easy to work with these numbers in the form

$$z = x + y\sqrt{d}.$$

In particular, if

$$z = m + n\sqrt{d},\ w = M + N\sqrt{d}$$

then

$$zw = (mM + dnN) + (mN + nM)\sqrt{d};$$

and on taking norms (ie multiplying each side by its conjugate),

$$(m^2 - dn^2)(M^2 - dN^2) = (mM + dnN)^2 - d(mN + nM)^2$$

Similarly,

$$\begin{aligned} \frac{z}{w} &= \frac{(m + n\sqrt{d})(M - N\sqrt{d})}{M^2 - dN^2} \\ &= \frac{(mM + dnN) - (mN - nM)\sqrt{d}}{M^2 - dN^2}. \end{aligned}$$

On taking norms,

$$\frac{m^2 - dn^2}{M^2 - dN^2} = u^2 - dv^2,$$

where

$$u = \frac{mM + dnN}{M^2 - dN^2},\ \frac{mN - nM}{M^2 - dN^2}.$$

Now to the proof.

Proof. By the Corollary to Kronecker's Theorem there exist an infinity of $m, n \in \mathbb{Z}$ such that

$$|\sqrt{d} - \frac{m}{n}| < \frac{1}{n^2}.$$

Since

$$\sqrt{d} + \frac{m}{n} = 2\sqrt{d} - (\sqrt{d} - \frac{m}{n})$$

it follows that

$$|\sqrt{d} + \frac{m}{n}| < 2\sqrt{d} + 1.$$

Hence

$$\begin{aligned} |d - \frac{m^2}{n^2}| &= |\sqrt{d} - \frac{m}{n}| \cdot |\sqrt{d} + \frac{m}{n}| \\ &< \frac{2\sqrt{d} + 1}{n^2}. \end{aligned}$$

Thus

$$|m^2 - dn^2| < 2\sqrt{d} + 1.$$

It follows that there must be an infinity of m, n satisfying

$$m^2 - dn^2 = t$$

for some integer t with $|t| < 2\sqrt{d} + 1$.

Let (m, n), (M, N) be two such solutions (with $(m, n) \neq \pm(M, N)$.

Note that since

$$m^2 - dn^2 = t = M^2 - dN^2$$

we have

$$u^2 - dv^2 = 1.$$

Of course u, v will not in general be integers, so this does not solve the problem. However, we shall see that by a suitable choice of m, n, M, N we can ensure that $u, v \in \mathbb{Z}$.

Let $T = |t|$; and consider $(m, n) \bmod T = (m \bmod T, n \bmod T)$. There are just T^2 choices for the residues $(m, n) \bmod T$. Since there are an infinity of solutions m, n there must be some residue pair $(r, s) \bmod T$ with the property that there are an infinity of solutions (m, n) with $m \equiv r \bmod T, n \equiv s \bmod T$.

Actually, all we need is two such solutions $(m, n), (M, N)$, so that

$$m \equiv M \bmod T, \ n \equiv N \bmod T.$$

For then

$$\begin{aligned} mM - dnN &\equiv m^2 - dn^2 = t \bmod T \\ &\equiv 0 \bmod T \end{aligned}$$

(since $t = \pm T$); and similarly

$$\begin{aligned} mN - nM &\equiv mn - nm \bmod T \\ &\equiv 0 \bmod T. \end{aligned}$$

Thus

$$T \mid mM - dnN, \ mN - nM$$

and so

$$u, v \in \mathbb{Z}.$$

□

14.3 Units II: Real quadratic fields

Theorem 14.3. *Suppose $d > 1$ is square-free. Then there exists a unique unit $\epsilon > 1$ in $\mathbb{Q}(\sqrt{d})$ such that the units in this field are*

$$\pm\epsilon^n$$

for $n \in \mathbb{Z}$.

Proof. We know that the equation

$$x^2 - dy^2 = 1$$

has an infinity of solutions. In particular it has a solution $(x, y) \neq (\pm 1, 0)$.

Let

$$\eta = x + y\sqrt{d}.$$

Then

$$\mathcal{N}(\eta) = 1;$$

so η is a unit $\neq \pm 1$.

We may suppose that $\eta > 1$; for of the 4 units $\pm\eta, \pm\eta^{-1}$ just one appears in each of the intervals $(-\infty, -1),\ (-1, 0),\ (0, 1),\ (1, \infty)$.

Lemma 14.1. *There are only a finite number of units in $(1, C)$, for any $C > 1$.*

Proof. Suppose

$$\epsilon = \frac{m + n\sqrt{d}}{2} \in (1, C)$$

is a unit. Then

$$\bar{\epsilon} = \frac{m - n\sqrt{d}}{2} = \pm\epsilon^{-1}.$$

Thus

$$-1 \leq \frac{m - n\sqrt{d}}{2} \leq 1.$$

Hence

$$0 < m < C + 1.$$

Since

$$m^2 - dn^2 = \pm 4$$

it follows that

$$n^2 < m^2 + 4 < (C + 1)^2 + 4.$$

□

We have seen that there is a unit $\eta > 1$. Since there are only a finite number of units in $(1, \eta]$ there is a least such unit ϵ.

Now suppose $\eta > 1$ is a unit. Since $\epsilon > 1$,

$$\epsilon^n \to \infty \text{ as } n \to \infty.$$

Hence we can find $n \geq 0$ such that

$$\epsilon^n \leq \eta < \epsilon^{n+1}.$$

Then

$$1 \leq \epsilon^{-n}\eta < \epsilon.$$

Since $\epsilon^{-n}\eta$ is a unit, it follows from the minimality of ϵ that

$$\epsilon^{-n}\eta = 1,$$

ie

$$\eta = \epsilon^n.$$

□