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*

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

Proof. By the Theorem,

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

□

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 $x, y \in \mathbb{Z}$.

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

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

Since

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

it follows that

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

Hence

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

Thus

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

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

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

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

Since

$$(m - n\sqrt{d})(M - N\sqrt{d}) = (mM + dnN) - (mN + nM)\sqrt{d}.$$

it follows (on taking norms) that

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

So if we set

$$u = \frac{mM + dnN}{t},\ v = \frac{mN + nM}{t}$$

then

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

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

$$mM - dnN \equiv m^2 - dn^2 = t \equiv 0 \bmod T,$$

and similarly

$$mN - nM \equiv mn - nm \equiv 0 \bmod T.$$

Thus

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

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 with $(x, y) \neq (\pm 1, 0)$.

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. *For any $C > 1$, there are only a finite number of units within the range $1 < \eta \leq C$,*

Proof. Suppose

$$\eta = x + y\sqrt{d} \in (1, C)$$

is a unit. Then

$$\bar{\eta} = x - y\sqrt{d} = \pm\eta^{-1}.$$

Hence

$$-1 \leq x + y\sqrt{d} \leq 1,$$

and so

$$0 < x < C + 1.$$

Since

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

it follows that

$$y^2 < x^2 + 1 < (C+1)^2 + 1.$$

The result follows, since x and y have denominator 1 or 2. □

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

This unit is unique; for if there were a second unit $X + Y\sqrt{d} = x + y\sqrt{d}$ then both have the same norm 1, so

$$\begin{aligned} X^2 - dY^2 = x^2 - dy^2 &\implies (X - Y\sqrt{d}(X + Y\sqrt{d}) = (x - y\sqrt{d})(x + y\sqrt{d}) \\ &\implies X - Y\sqrt{d} = x - y\sqrt{d}(x + y\sqrt{d}) \\ &\implies X = x,\ Y = y. \end{aligned}$$

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

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

□