LECTURE 13: DIOPHANTINE APPROXIMATION AND ALGEBRAIC NUMBERS

1. Pell's equation

We investigate the solubility of the equation

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

for a fixed integer d that is not a perfect square, in integers x and y. We note that the equation $x^2 - dy^2 = 1$ always has the (trivial) solutions $(x, y) = \pm(1, 0)$, so the relevant problem is of determining whether there are additional solutions.

We observe that it is natural to look for non-trivial solutions among integers (x, y) such that $|x - \sqrt{d}y|$ is small. Thus, it is natural to expect that this topic is connected with the problem of Diophantine approximation of $\sqrt{d}$.

Theorem 1.1. *Suppose that $d > 0$ is not a perfect square. Then the Diophantine equation $x^2 - dy^2 = 1$ has a non-trivial solution.*

Proof. Since $\sqrt{d}$ is irrational, we know that there are infinitely many pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}$ with $(p, q) = 1$ such that

$$|p - q\sqrt{d}| < 1/q.$$

For those pairs, we also have

$$|p + q\sqrt{d}| \leqslant |p - q\sqrt{d}| + 2q\sqrt{d} < 1/q + 2q\sqrt{d},$$

and

$$|p^2 - dq^2| = |(p - q\sqrt{d})(p + q\sqrt{d})| < 1 + 2\sqrt{d}.$$

Hence, there are infinitely many pairs (p, q) for which $p^2 - dq^2$ takes the same fixed value. Suppose then that $p^2 - dq^2 = r$ has infinitely many integral solutions. Then we may select two positive solutions, say $(p, q) \neq (u, v)$, satisfying

$$p^2 - dq^2 = u^2 - dv^2 = r \quad \text{and} \quad p \equiv u \pmod{r} \text{ and } q \equiv v \pmod{r}.$$

To construct a solution, we consider

$$\frac{p + \sqrt{d}q}{u + \sqrt{d}v} = \frac{pu - dqv}{r} + \frac{-pv + qu}{r}\sqrt{d}.$$

Then

$$pu - dqv \equiv p^2 - dq^2 \equiv 0 \pmod{r} \quad \text{and} \quad -pv + qu \equiv 0 \pmod{r},$$

so that

$$x = (pu - dqv)/r \quad \text{and} \quad y = (-pv + uq)/r$$

are integers. Moreover,

$$\begin{aligned}(pu-dqv)^2-d(-pv+uq)^2&=(pu)^2+d^2(qv)^2-d(pv)^2-d(uq)^2\\&=(p^2-dq^2)(u^2-dv^2)=r^2.\end{aligned}$$

Hence, (x,y) gives a solution of the Pell equation. If $y=0$, then $pv=qu$. Since $(p,q)=1$ and $(u,v)=1$, it follows that $(p,q)=(u,v)$. Hence, (x,y) gives a non-trivial solution. □

Remark 1.2. Given this single non-trivial solution (x,y) of $x^2-dy^2=1$, we generate infinitely many others by noting that whenever (u,v) is any one solution, then

$$(u^2+dv^2)^2-d(2uv)^2=(u^2-dv^2)^2=1,$$

whence $(u^2+dv^2,2uv)$ is a second solution with larger x-coordinate. By iterating this process we plainly obtain infinitely many distinct non-trivial solutions.

A non-trivial solution of Pell's equation can be found by computing the continued fraction expansion of $\sqrt{d}$.

Example 1.3. We compute $\sqrt{3}=[1;\overline{1,2}]$. We consider convergents p_n/q_n to $\sqrt{3}$, and the corresponding values of $p_n^2-3q_n^2$. It is useful in this context to recall that when $\theta=[a_0;a_1,\dots]$, then the convergents p_n/q_n to θ satisfy the relations

$$\begin{gathered}p_0=a_0,\quad q_0=1,\quad p_1=a_0a_1+1,\quad q_1=a_1,\\p_n=a_np_{n-1}+p_{n-2},\quad q_n=a_nq_{n-1}+q_{n-2}.\end{gathered}$$

In the case at hand, we obtain

$$\begin{gathered}p_0=1\text{ and }q_0=1\Rightarrow p_0^2-3q_0^2=-2,\\p_1=1\cdot 1+1=2\text{ and }q_1=1\Rightarrow p_1^2-3q_1^2=4-3=1,\\p_2=2p_1+p_0=5\text{ and }q_2=2q_1+q_0=3\Rightarrow p_2^2-3q_2^2=25-3\cdot 9=-2,\\p_3=p_2+p_1=7\text{ and }q_3=q_2+q_1=4\Rightarrow p_3^2-3q_3^2=49-3\cdot 16=1,\end{gathered}$$

and so on. One can check that for each natural number n, the pair $(x,y)=(p_{2n-1},q_{2n-1})$ provides a solution of the equation $x^2-3y^2=1$.

2. Liouville's Theorem

We now discuss rational approximations to algebraic numbers.

Definition 2.1. We say that the real number θ is **algebraic** and has **degree** d if there exists a polynomial $f\in\mathbb{Z}[t]$ such that (i) $\deg(f)=d$, (ii) f is irreducible over $\mathbb{Q}$, and (iii) one has $f(\theta)=0$.

Note that the degree d of θ is unique, for if f and g are polynomials for which $f(\theta)=g(\theta)=0$, then by the division algorithm for polynomials, there is some greatest common divisor h of f and g for which $h(\theta)=0$. If f and g are both irreducible then they must be scalar multiples of h, and hence they have the same degree.

In fact, this argument shows more: if we restrict our attention to polynomials whose coefficients have no common factor and for which the leading coefficient is positive, then the choice is unique. This unique polynomial $f \in \mathbb{Z}[t]$ is known as the **minimal polynomial** of θ.

Definition 2.2. We say that the real number θ is **transcendental** if θ is **not** algebraic of any degree.

An argument based on countability shows that not all real numbers are algebraic, and indeed that almost all real numbers are transcendental. However, it was not until 1844 that any explicit transcendental number was exhibited—or indeed that transcendental numbers were known to exist at all.

Theorem 2.3 (Liouville, 1844)**.** *Suppose that $\theta \in \mathbb{R}$ is an algebraic number of degree $d > 1$. Then there exists a positive constant $c = c(\theta)$ such that whenever $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, one has*

$$|\theta - p/q| \geqslant c/q^d.$$

Proof. Write f for the minimal polynomial of θ, so that $f \in \mathbb{Z}[t]$ has degree n. Then by the Mean Value Theorem, given $p \in \mathbb{Z}$ and $q \in \mathbb{N}$, there exists a real number x with x lying between θ and p/q, such that

$$f(\theta) - f(p/q) = (\theta - p/q) f'(x).$$

But by hypothesis, f is an irreducible polynomial of degree $d > 1$, and so $f(p/q) \neq 0$. Therefore, $q^d f(p/q)$ is a non-zero integer, whence

$$|q^d f(p/q)| \geqslant 1.$$

Moreover, since without loss of generality we may suppose that $|\theta - p/q| \leqslant 1$, we find that $|x| \leqslant |\theta| + 1$, and hence

$$|f'(x)| \leqslant \sup_{|z| \leqslant |\theta|+1} |f'(z)|.$$

Writing $c(\theta)^{-1}$ for the latter supremum, we conclude that

$$1/q^d \leqslant |f(p/q)| = |f(\theta) - f(p/q)| = |\theta - p/q| \cdot |f'(x)| \leqslant c(\theta)^{-1} |\theta - p/q|,$$

whence

$$|\theta - p/q| \geqslant c(\theta)/q^d.$$

□

It is worthwhile noting a simple enhancement of Liouville's theorem that is of utility in applications.

Theorem 2.4. *Suppose that θ is a non-zero algebraic number of degree $d \geqslant 1$. Then there exists a positive constant $c = c(\theta)$ such that whenever $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ satisfy $(p, q) = 1$, and q is sufficiently large, one has*

$$|\theta - p/q| \geqslant c/q^d.$$

Proof. When θ is algebraic of degree exceeding 1, the desired conclusion is immediate from Liouville's theorem. It remains only to consider the case in which θ is rational, say $\theta = r/s$ for some $r \in \mathbb{Z}$ and $s \in \mathbb{N}$ with $(r, s) = 1$. But then, whenever $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ satisfy $(p, q) = 1$, and q is larger than s, one has $r/s \neq p/q$, and so

$$\left|\theta - \frac{p}{q}\right| = \left|\frac{r}{s} - \frac{p}{q}\right| = \left|\frac{qr - ps}{qs}\right| \geqslant \frac{1}{qs}.$$

Thus, when the degree of θ is 1, the desired conclusion holds with $c(\theta) = 1/s$. □

Corollary 2.5. *The number*

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}$$

is irrational.

Proof. Suppose that e is rational. Then by Theorem 2.4, there are positive constants c and q_0 such that

$$|e - p/q| \geqslant \frac{c}{q}$$

whenever $p, q \in \mathbb{N}$ satisfy $(p, q) = 1$ and $q \geqslant q_0$.

Let j be a natural number, and set $Q_j = j!$, $P_j = \sum_{n=0}^{j} \frac{j!}{n!}$. Then $P_j \equiv 1 \pmod{j}$, while $Q_j \equiv 0 \pmod{j}$. Hence, writing $P_j/Q_j = p_j/q_j$ in lowest terms, we have that $j \mid q_j \mid Q_j$, whence $j \leqslant q_j \leqslant j!$. Now,

$$|e - p_j/q_j| = \sum_{n=j+1}^{\infty} \frac{1}{n!} < \frac{1}{j!} \sum_{h=1}^{\infty} \frac{1}{(j+1)^h} = \frac{1}{j \cdot j!} \leqslant \frac{1}{jq_j}.$$

Choosing $j > \max(1/c, q_0)$ results in a contradiction. Hence, e must be irrational. □

Corollary 2.6. *Let $\theta = \sum_{n=0}^{\infty} 2^{-n!}$. Then θ is transcendental.*

Proof. Suppose that θ is algebraic of some degree $d \geqslant 1$. Then by Theorem 2.4 there exists a constant $c = c(\theta) > 0$ such that whenever $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ are coprime and q is sufficiently large, then

$$|\theta - p/q| \geqslant c(\theta)/q^d.$$

For each natural number j, write

$$p_j = 2^{j!} \sum_{n=0}^{j} 2^{-n!} \quad \text{and} \quad q_j = 2^{j!}.$$

Then $(p_j, q_j) = 1$ since p_j is odd and 2 is the only prime factor of q_j. We have

$$|\theta - p_j/q_j| = \sum_{n=j+1}^{\infty} 2^{-n!} < 2^{1-(j+1)!} \leqslant 2^{-j \cdot j!} = q_j^{-j}.$$

Thus there exist infinitely many $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $(p,q) = 1$ and satisfying the property that $|\theta - p/q| < q^{-(d+1)}$ (just take $j > d$), contradicting the above when $q > 1/c(\theta)$. Thus, θ cannot be algebraic, and consequently is transcendental. □

Aside: In fact one can show that whenever $a \geqslant 2$ and $b \geqslant 3$ are integers, then the number $\sum_{n=1}^{\infty} a^{-b^n}$ is transcendental (though do not try quoting this in your homework!). It is also known that π is transcendental (Lindemann, 1882), and that e is transcendental (Hermite, 1873). Indeed, Lindemann proved that whenever $\alpha_1, \ldots, \alpha_n$ are distinct algebraic numbers, and $\beta_1, \ldots, \beta_n$ are non-zero algebraic numbers, then $\beta_1 e^{\alpha_1} + \cdots + \beta_n e^{\alpha_n} \neq 0$. Since $e^{i\pi} + 1 = 0$, it follows that π cannot be algebraic.

We note also the theorem of Gelfond–Schneider (1934) that resolved Hilbert's 7th problem: whenever $\alpha \neq 0, 1$ is algebraic, and β is algebraic and irrational, the number α^β is transcendental. Thus, for example, one sees that $2^{\sqrt{2}}$ and $e^\pi = (-1)^{-i}$ are both transcendental.

Open Problem: Is it true that e and π are algebraically independent? That is to say, is it true that there is **no** non-trivial polynomial $F(x,y) \in \mathbb{Z}[x,y]$ with the property that $F(e,\pi) = 0$?