LECTURE 12: DIOPHANTINE APPROXIMATION

1. Dirichlet Theorem

Many important ideas in Number Theory stem from notions of Diophantine approximation, which is to say rational approximations to real numbers with prescribed properties.

Theorem 1.1 (Dirichlet)**.** *Let $\theta \in \mathbb{R}$ and let Q be a real number exceeding* 1*. Then there exist integers p and q with $1 \leqslant q < Q$ and $(p, q) = 1$ such that $|q\theta - p| \leqslant 1/Q$.*

Proof. We apply the Box Principle. Write $N = \lceil Q \rceil$, and consider the $N + 1$ real numbers

$$0,\ 1,\ \{\theta\},\ \{2\theta\},\ \ldots,\ \{(N-1)\theta\},$$

where here, and throughout, we write $\{x\}$ for $x - \lfloor x \rfloor$. These $N + 1$ real numbers all lie in the interval $[0, 1]$. But if we divide this unit interval into N disjoint intervals of length $1/N$, it follows that there must be two numbers from the above set which necessarily lie in the same interval. The difference between these two numbers has the shape $q\theta - p$, where p and q are integers with $0 < q < N$. Thus we deduce that there exist integers p and q with $1 \leqslant q < Q$ and $|q\theta - p| \leqslant 1/Q$. The coprimality condition is obtained easily by dividing through by (p, q). □

Corollary 1.2. *Whenever θ is irrational, there exist infinitely many distinct pairs $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $(p, q) = 1$ and $|\theta - p/q| < 1/q^2$.*

Proof. Let $Q > 1$. Then by Dirichlet's theorem on Diophantine approximation, there exist $p \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $(p, q) = 1$, $q < Q$ and $0 < |\theta - p/q| \leqslant 1/(qQ) < 1/q^2$. Let Q' be any real number exceeding $|\theta - p/q|^{-1}$. A second application of Dirichlet's theorem shows that there exist $p' \in \mathbb{Z}$ and $q' \in \mathbb{N}$ with $(p', q') = 1$, $1 \leqslant q' < Q'$ and

$$\left|\theta - \frac{p'}{q'}\right| \leqslant \frac{1}{q'Q'} < \frac{|\theta - p/q|}{q'} \leqslant \left|\theta - \frac{p}{q}\right|.$$

Thus, necessarily, one has $p'/q' \neq p/q$. Furthermore, $|\theta - p'/q'| < 1/(q')^2$. By iterating this process, we obtain a sequence $(p_n/q_n)_{n=1}^{\infty}$ of distinct rational numbers with

$$0 < \left|\theta - \frac{p_n}{q_n}\right| < \left|\theta - \frac{p_{n-1}}{q_{n-1}}\right| < \cdots < \left|\theta - \frac{p_1}{q_1}\right|,$$

and $|\theta - p_i/q_i| < 1/q_i^2$, and hence infinitely many approximations p/q with $(p, q) = 1$ and $|\theta - p/q| < 1/q^2$. □

2. Continued fractions

Given a rational fraction $\frac{u_0}{u_1}$ with $u_0 \in \mathbb{Z}$ and $u_1 \in \mathbb{N}$, we apply the Euclid algorithm to obtain

$$\begin{aligned} u_0 &= a_0 u_1 + u_2, \quad 0 < u_2 < u_1, \\ u_1 &= a_1 u_2 + u_3, \quad 0 < u_3 < u_2, \\ &\vdots \\ u_{n-1} &= a_{n-1} u_n + u_{n+1}, \quad 0 < u_{n+1} < u_n, \\ u_n &= a_n u_{n+1} \end{aligned}$$

If we set $\theta_i = \frac{u_i}{u_{i+1}}$, then we obtain the relation

$$\theta_i = a_i + \frac{1}{\theta_{i+1}}, \quad i = 0 \ldots, n-1, \qquad \theta_n = a_n.$$

This gives the expansion

$$\frac{u_0}{u_1} = \theta_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}}.$$

For the above expansion, it is usually more convenient to write

$$[a_0; a_1, \ldots, a_n].$$

Example 2.1. Write 57/32 as a continued fraction.
Put $\theta = 57/32$. Then $a_0 = \lfloor \theta \rfloor = 1$, and

$$\theta_1 = \frac{1}{\frac{57}{32} - 1} = \frac{32}{25}.$$

Then $a_1 = \lfloor \theta_1 \rfloor = 1$, and

$$\theta_2 = \frac{1}{\frac{32}{25} - 1} = \frac{25}{7}.$$

Then $a_2 = \lfloor \theta_2 \rfloor = 3$, and

$$\theta_3 = \frac{1}{\frac{25}{7} - 3} = \frac{7}{4}.$$

Then $a_3 = \lfloor \theta_3 \rfloor = 1$, and

$$\theta_4 = \frac{1}{\frac{7}{4} - 1} = \frac{4}{3}.$$

Then $a_4 = \lfloor \theta_4 \rfloor = 1$, and

$$\theta_5 = \frac{1}{\frac{4}{3} - 1} = 3.$$

Then $a_5 = 3$ and $\theta_5 = a_5$, so stop.

In this way we find that $57/32 = [1; 1, 3, 1, 1, 3]$.

Now we generalise this expansion to irrational numbers.

The continued fraction algorithm:
Given $\theta \in \mathbb{R}\backslash\mathbb{Q}$, we define the integers $a_0 \in \mathbb{Z}$, $a_j \geqslant 1$, $j \geqslant 1$, as follows:

- Let $a_0 = \lfloor \theta \rfloor \in \mathbb{Z}$ and define θ_1 by $\theta = a_0 + 1/\theta_1$, so that $\theta_1 > 1$.
- $a_1 = \lfloor \theta_1 \rfloor \geqslant 1$ and define θ_2 by $\theta_1 = a_1 + 1/\theta_2$, so that $\theta_2 > 1$.

$$\vdots$$

- Let $a_n = \lfloor \theta_n \rfloor \geqslant 1$ and define θ_{n+1} by
$$\theta_n = a_n + 1/\theta_{n+1}, \tag{2.1}$$
so that $\theta_{n+1} > 1$.

$$\vdots$$

We consider the sequence of fractions

$$C_n = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots + \cfrac{1}{a_n}}}} = [a_0; a_1, \dots, a_n]. \tag{2.2}$$

As we shall show below the sequence C_n always converges so that we also use the notation

$$[a_0; a_1, a_2, \dots] = \lim_{n\to\infty} [a_0; a_1, \dots, a_n].$$

We shall justify existence of this limit below.

Example 2.2. Write $\sqrt{3}$ as a continued fraction.
Put $\theta = \sqrt{3}$. Then $a_0 = \lfloor \sqrt{3} \rfloor = 1$, and

$$\theta_1 = \frac{1}{\sqrt{3} - 1} = \tfrac{1}{2}(\sqrt{3} + 1).$$

Then $a_1 = \lfloor \theta_1 \rfloor = 1$, and

$$\theta_2 = \frac{1}{\frac{1}{2}(\sqrt{3} - 1)} = \sqrt{3} + 1.$$

Then $a_2 = \lfloor \theta_2 \rfloor = 2$, and

$$\theta_3 = \frac{1}{\sqrt{3} - 1} = \tfrac{1}{2}(\sqrt{3} + 1) = \theta_1,$$

and the sequence repeats.

In this way we find that $\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, \dots]$, a periodic continued fraction that, by convention, we write as $[1; \overline{1, 2}]$.

Example 2.3. Find the continued fraction expansion of $\frac{1}{2}(10-\sqrt{7})$.
Put $\theta = \frac{1}{2}(10-\sqrt{7})$. Then $a_0 = \left[\frac{1}{2}(10-\sqrt{7})\right] = 3$, and

$$\theta_1 = \frac{1}{\frac{1}{2}(10-\sqrt{7})-3} = \frac{2(4+\sqrt{7})}{16-7} = \tfrac{1}{9}(8+2\sqrt{7}).$$

Then $a_1 = \lfloor \theta_1 \rfloor = 1$, and

$$\theta_2 = \frac{1}{\frac{1}{9}(8+2\sqrt{7})-1} = \frac{9(-1-2\sqrt{7})}{1-28} = \tfrac{1}{3}(1+2\sqrt{7}).$$

Then $a_2 = \lfloor \theta_2 \rfloor = 2$, and

$$\theta_3 = \frac{1}{\frac{1}{3}(1+2\sqrt{7})-2} = \frac{3(-5-2\sqrt{7})}{25-28} = 5+2\sqrt{7}.$$

Then $a_3 = \lfloor \theta_3 \rfloor = 10$, and

$$\theta_4 = \frac{1}{(5+2\sqrt{7})-10} = \frac{-5-2\sqrt{7}}{25-28} = \tfrac{1}{3}(5+2\sqrt{7}).$$

Then $a_4 = \lfloor \theta_4 \rfloor = 3$, and

$$\theta_5 = \frac{1}{\frac{1}{3}(5+2\sqrt{7})-3} = \frac{3(-4-2\sqrt{7})}{16-28} = \tfrac{1}{2}(2+\sqrt{7}).$$

Then $a_5 = \lfloor \theta_5 \rfloor = 2$, and

$$\theta_6 = \frac{1}{\frac{1}{2}(2+\sqrt{7})-2} = \frac{2(-2-\sqrt{7})}{4-7} = \tfrac{1}{3}(4+2\sqrt{7}).$$

Then $a_6 = \lfloor \theta_6 \rfloor = 3$, and

$$\theta_7 = \frac{1}{\frac{1}{3}(4+2\sqrt{7})-3} = \frac{3(-5-2\sqrt{7})}{25-28} = 5+2\sqrt{7} = \theta_3,$$

and the sequence repeats.

In this way we find that

$$\tfrac{1}{2}(10-\sqrt{7}) = [3;1,2,10,3,2,3,10,3,2,3,\ldots] = [3;1,2,\overline{10,3,2,3}].$$

Definition 2.4. In the above description of the continued fraction algorithm, and the resulting continued fraction expansion of a real number θ,

- the integers a_i are known as the **partial quotients** of θ,
- the real numbers θ_n are known as the **complete quotients** of θ,
- the rational numbers

  $$C_n = [a_0; a_1, \ldots, a_n],$$

  are known as the **convergents** to θ.

Our next goal is to investigate the behaviour of the convergents C_n.

More generally, let us fix $a_0 \in \mathbb{Z}$ and real numbers $a_i \geqslant 1$, $i \geqslant 1$, and consider the sequence $C_n = [a_0; a_1, \ldots, a_n]$.

Lemma 2.5. *Define the integers p_n and q_n by the recurrence relations*

$$p_0 = a_0, \quad q_0 = 1, \quad p_1 = a_0a_1 + 1, \quad q_1 = a_1,$$

and for $n \geqslant 2$,

$$p_n = a_np_{n-1} + p_{n-2}, \quad q_n = a_nq_{n-1} + q_{n-2}. \tag{2.3}$$

Then

$$C_n = [a_0; a_1, \dots, a_n] = \frac{p_n}{q_n}.$$

Remark 2.6. The recurrence relations can be also written in the matrix form:

$$\begin{pmatrix} p_{n-1} & q_{n-1} \\ p_n & q_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} \begin{pmatrix} p_{n-2} & q_{n-2} \\ p_{n-1} & q_{n-1} \end{pmatrix}$$

Proof. The proof simply goes by induction on n. The cases $n = 0$ and $n = 1$ are straightforward. Suppose that the lemma is true for n. Then

$$\begin{aligned}[a_0; a_1, \dots, a_{n+1}] &= [a_0; a_1, \dots, a_{n-1}, a_n + 1/a_{n+1}] \\ &= \frac{(a_n + 1/a_{n+1})p_{n-1} + p_{n-2}}{(a_n + 1/a_{n+1})q_{n-1} + q_{n-2}} = \frac{(a_np_{n-1} + p_{n-2}) + p_{n-1}/a_{n+1}}{(a_nq_{n-1} + q_{n-2}) + q_{n-1}/a_{n+1}} \\ &= \frac{p_n + p_{n-1}/a_{n+1}}{q_n + q_{n-1}/a_{n+1}} = \frac{a_{n+1}p_n + p_{n-1}}{q_na_{n+1} + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}.\end{aligned}$$

This proves the result. □

Lemma 2.7. *With notation as in Lemma 2.5,*

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1} \quad \textit{and} \quad p_nq_{n-2} - p_{n-2}q_n = (-1)^{n-2}a_n,$$

so that

$$C_n - C_{n-1} = \frac{(-1)^{n-1}}{q_{n-1}q_n} \quad \textit{and} \quad C_n - C_{n-2} = \frac{(-1)^{n-2}a_{n-2}}{q_{n-2}q_n}. \tag{2.4}$$

Proof. Using the recursive formula (2.3), we obtain

$$\begin{aligned}p_nq_{n-1} - p_{n-1}q_n &= (a_np_{n-1} + p_{n-2})q_{n-1} - p_{n-1}(a_nq_{n-1} + q_{n-2}) \\ &= -(p_{n-1}q_{n-2} - p_{n-2}q_{n-2}).\end{aligned}$$

Hence, the proof of the first formula follows by induction.

The proof of the second formula is similar. □

Theorem 2.8. *The sequence $C_n = [a_0; a_1, \dots, a_n]$ converges, and it satisfies*

$$C_1 > C_3 > \cdots > C_{2i+1} > \cdots > \lim_{n\to\infty} C_n > \cdots > C_{2i} > \cdots > C_4 > C_2.$$

Proof. It follows from (2.4) that $C_{2n+1} > C_{2n}$ for all n, $C_{n-2} > C_n$ if n is odd, and $C_n > C_{n-2}$ if n is even. This implies the inequalities

$$C_1 > C_3 > \cdots > C_{2i+1} > \cdots > C_{2i} > \cdots > C_4 > C_2.$$

The sequences C_{2i} and C_{2i+1} are convergent as bounded monotone sequences. It follows from the relation $q_n = a_nq_{n-1} + q_{n-2}$ that $q_n \geqslant q_{n-1} + q_{n-2}$ for $n \geqslant 2$, whence $q_n \to \infty$ as $n \to \infty$. Since $C_n - C_{n-1} = \frac{(-1)^{n-1}}{q_{n-1}q_n} \to 0$, we deduce that these sequences have the same limit. □

Corollary 2.9. *Let $C_n = \frac{p_n}{q_n}$ be the convergents for a real number θ. Then*

$$|\theta - C_n| \leqslant \frac{1}{q_n q_{n+1}},$$

In particular, if θ is irrational, then

$$\theta = \lim_{n\to\infty} C_n.$$

Proof. It follows from (2.1) that

$$\theta = [a_0, \theta_1] = [a_0, a_1, \theta_2] = \cdots = [a_0, a_1, \dots, a_n, \theta_{n+1}].$$

So by Lemma 2.5,

$$\theta = \frac{p_n\theta_{n+1} + p_{n-1}}{q_n\theta_{n+1} + q_{n-1}},$$

and by Lemma 2.7,

$$\begin{aligned}|\theta - C_n| &= |[a_0, a_1, \dots, a_n, \theta_{n+1}] - [a_0, a_1, \dots, a_n]| \\ &= \frac{1}{q_n(q_n\theta_{n+1} + q_{n-1})} \leqslant \frac{1}{q_n(q_n a_{n+1} + q_{n-1})} = \frac{1}{q_n q_{n+1}}.\end{aligned}$$

When θ is irrational, $a_n \geqslant 1$ for all n, and $q_n = a_n q_{n-1} + q_{n-2} \geqslant q_{n-1} + q_{n-2}$ for $n \geqslant 2$, whence $q_n \to \infty$ as $n \to \infty$. This implies the second part of the corollary. □

Remark 2.10. If θ is irrational, we have $a_{n+1} = \lfloor\theta_{n+1}\rfloor < \theta_{n+1}$, so that in the above proof we obtain

$$\left|\theta - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

This provides a constructive way to generate the rational apporoximations whose existence was shown in Corollary 1.2.