8. Dirichlet's Theorem and Farey Fractions

We are concerned here with the approximation of real numbers by rational numbers, generalizations of this concept and various applications to problems in number theory.

A property of the integers which we frequently use is that if $|h| < 1$, then $h = 0$, alternatively that if $h \neq 0$, then $|h| \geq 1$. The rationals are dense in $\mathbb{R}$ but two rationals with small denominators cannot be too close together. Thus when a/q and b/r are two different rational numbers we have

$$\frac{a}{q} - \frac{b}{r} = \frac{ar - bq}{qr}$$

and since they are unequal the numerator is non-zero. Thus

$$\left| \frac{a}{q} - \frac{b}{r} \right| \geq \frac{1}{qr} \tag{1}$$

There is a very simple, and useful, theorem due to Dirichlet which tells us how well a real number can be approximated by a rational number a/q in terms of the denominator q.

Theorem 8.1 (Dirichlet). *For any real number α and any integer $Q \geq 1$ there exist integers a and q with $1 \leq q \leq Q$ such that*

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{q(Q+1)}.$$

As an immediate consequence of casting out all common factors of a and q in a/q we have

Corollary 8.2. *The conclusion holds with the additional condition $(a, q) = 1$.*

Proof of Theorem 8.1. Let I_n denote the interval $\left[\frac{n-1}{Q+1}, \frac{n}{Q+1}\right)$ and consider the Q numbers $\{\alpha\}$, $\{2\alpha\}$, ..., $\{Q\alpha\}$. (Here we use $\{*\} = * - \lfloor * \rfloor$ to denote the "fractional" part). If one of these numbers, say $\{q\alpha\}$, lies in I_1, then we are done. We take $a = \lfloor q\alpha \rfloor$ and then $0 \leq \alpha - a < \frac{1}{Q+1}$. Similarly when one of the numbers lies in I_{Q+1}, then $1 - \frac{1}{Q+1} \leq q\alpha - \lfloor q\alpha \rfloor < 1$, whence $-\frac{1}{Q+1} \leq q\alpha - (\lfloor q\alpha \rfloor + 1) < 0$ and we can take $a = \lfloor q\alpha \rfloor + 1$. When neither of these situations occurs the Q numbers must lie in the $Q - 1$ intervals $I_2, \dots, I_Q$, so there must be at least one interval which contains at least two of the the numbers (the *pigeon hole principle*, or *box argument*, or *Schubfachprinzip*). Thus there are q_1, q_2 with $q_1 < q_2$ such that $|(\alpha q_2 - \lfloor \alpha q_2 \rfloor) - (\alpha q_1 - \lfloor \alpha q_1 \rfloor)| < \frac{1}{Q+1}$. We put $q = (q_2 - q_1)$, $a = (\lfloor \alpha q_2 \rfloor - \lfloor \alpha q_1 \rfloor)$.

This turns out to be a very powerful theorem and in many applications it is all that one needs to know about the approximation of reals by rationals. It is obviously best possible. Take $b = 1$, $r = Q + 1$ in (1) above.

Theorem 8.3. *Suppose that α is irrational. Then there exist infinitely many rational numbers a/q with $(a,q)=1$ such that $|\alpha - a/q| < q^{-2}$. In particular there are arbitrarily large q for which this inequality holds.*

Proof. Choose Q_1 to be an integer > 1 and choose a_1, q_1 in accordance with Corollary 1. Then $|\alpha - a_1/q_1| \le \frac{1}{q_1(Q_1+1)} < q_1^{-2}$. Now, given $a_1/q_1, \dots, a_n/q_n$ with $(a_m, q_m) = 1$ and $|\alpha - a_m/q_m| < q_m^{-2}$ we obtain a_{n+1}, q_{n+1} as follows. Since α is irrational we have $\alpha \ne a_m/q_m$ $(m = 1, \dots, n)$. Choose

$$Q_{n+1} > \max\left\{|\alpha - a_1/q_1|^{-1}, \dots, |\alpha - a_n/q_n|^{-1}\right\}$$

and then choose a_{n+1}, q_{n+1} in accordance with Corrollary 1. Obviously

$$|\alpha - a_{n+1}/q_{n+1}| \le \frac{1}{q_{n+1}(Q_{n+1}+1)} < q_{n+1}^{-2}$$

and

$$|\alpha - a_{n+1}/q_{n+1}| < \min\{|\alpha - a_1/q_1|, \dots, |\alpha - a_n/q_n|\}$$

so we must have a_{n+1}/q_{n+1} distinct from any of $a_1/q_1, \dots, a_n/q_n$. Moreover it is clear that for any q_m the a_m is uniquely defined by the inequality

$$|\alpha - a_m/q_m| \le \frac{1}{q_m(Q_m+1)}.$$

Thus the q_m are distinct and so there are arbitrarily large q_m.

When α is rational, say $\alpha = a_0/q_0$, then the inequality $|\alpha - a/q$ has only a finite number of solutions in a, q with $(a,q)=1$ since, by (1), we have $|\alpha - a/q| \ge \frac{1}{q_0 q}$ when $a/q \ne a_0/q_0$. Indeed the inequality $|\alpha - a/q| < \frac{1}{q_0 q}$ has the unique solution $a/q = a_0/q_0$.

Theorem 8.4. *The real number α is irrational if and only if for every $\varepsilon > 0$ there are $a \in \mathbb{Z}$, $q \in \mathbb{N}$ such that $0 < |q\alpha - a| < \varepsilon$*

Proof. If $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, then choose $Q = \lfloor 1/\varepsilon \rfloor$. Then by Theorem 1, there are a, q such that $|q\alpha - a| \le \frac{1}{Q+1} < \varepsilon$. Moreover, $q\alpha \ne a$. If $\alpha \in \mathbb{Q}$, then there are $b \in \mathbb{Z}$ and $r \in \mathbb{N}$ such that $(b,r)=1$ and $\alpha = b/r$. Choose $\varepsilon = \frac{1}{2r}$ and suppose that there are $a \in \mathbb{Z}$, $q \in \mathbb{N}$ such that $|q\alpha - a| < \varepsilon$. Then $|\alpha - a/q| < \frac{1}{2rq}$ and $\alpha - a/q = b/r - a/q = \frac{bq-ar}{rq}$. Thus $|bq - ar| < \frac{1}{2}$. Hence $bq = ar$, whence $q\alpha - a = 0$.

Example $e = \sum_0^\infty \frac{1}{k!}$ is irrational. To prove this let $q = K!$, $a = K! \sum_{k=0}^{K} \frac{1}{k!}$. Then $0 < \sum_{k=K+1}^\infty \frac{K!}{k!} = qe - a$ and

$$\sum_{k=K+1}^\infty \frac{K!}{k!} = \frac{1}{K+1} \sum_{k=K+1}^\infty \frac{1}{(k-K-1)!\binom{k}{K+1}} \le \frac{e}{K+1} < \varepsilon$$

if K is large enough.

There is a useful generalisation of this.

Theorem 8.5 (Liouville). *Suppose that α is an algebraic number of degree n (≥ 1). Then there is a positive constant $c = c(\alpha)$ such that*

$$\left|\alpha - \frac{a}{q}\right| > cq^{-n}$$

whenever $a \in \mathbb{Z}$, $q \in \mathbb{N}$ and $a/q \neq \alpha$ (this latter condition can be omitted when $n \geq 2$).

Proof. By "algebraic of degree n" we mean that α is a root of a non-constant polynomial with integer coefficients and the degree n corresponds to the minimal degree amongst all such polynomials. It is not hard to see that we may suppose that there is a unique polynomial

$$P(\lambda) = a_0\lambda^n + a_1\lambda^{n-1} + \cdots + a_n$$

such that
(i) $a_j \in \mathbb{Z}$ for $0 \leq j \leq n$,
(ii) $a_0 > 0$,
(iii) $(a_0, a_1, \dots, a_n) = 1$,
(iv) $P(\alpha) = 0$,
(v) n minimal.
Firstly a polynomial satisfying (i) and (iv) must exist by definition of α. Taking one of minimal degree ensures (v). By multiplying through by ±1 we can ensure (ii) and by taking out common factors we can ensure (iii). Moreover if there were two distinct such polynomials P and P^*, then by (ii) and (iii) the one cannot be a multiple of the other so we could obtain, by considering $a_0^*P(\lambda) - a_0P(\lambda)$, one of lower degree satisfying (i) and (iv) and then repeat the above process to obtain (ii) and (iii) and so contradict (v).

It suffices to show that there is a $c(\alpha)$ such that if $|\alpha - a/q| \leq 1$, then $|\alpha - a/q| > c(\alpha)q^{-n}$ for then we can replace $c(\alpha)$ by $\min\big(1, c(\alpha)\big)$ and so the conclusion follows also when $|\alpha - a/q| \geq 1$.

Since the a_j are integers we have

$$q^n P\left(\frac{a}{q}\right) \in \mathbb{Z}.$$

Moreover $P(a/q) \neq 0$, for otherwise we could factor out $\lambda - a/q$ and obtain a polynomial of lower degree $Q(\lambda) = P(\lambda)/(\lambda - a/q)$ which satisfies $Q(\alpha) = 0$. Although in the first instance this could be guaranteed only to have rational coefficients by multiplying through by a suitably integer we could recover a polynomial Q^* of degree $n-1$ with integer coefficients and satisfying $Q^*(\alpha) = 0$. Hence

$$q^n \left|P\left(\frac{a}{q}\right)\right| \geq 1.$$

On the other hand, by the mean value theorem of the differential calculus

$$-P(a/q) = P(\alpha) - P(a/q) = (\alpha - a/q)P'(\beta)$$

where β lies between α and a/q. Since we are supposing that $|\alpha - a/q| \le 1$ it follows that

$$|P'(\beta)| \le \max\{|P'(\lambda) : \lambda \in \lfloor \alpha - 1, \alpha + 1 \rfloor\} = c(\alpha).$$

Hence

$$1 \le q^n |P(a/q)| \le |\alpha - a/q| c(\alpha).$$

Example The number

$$\theta = \sum_{k=0}^{\infty} \frac{1}{2^{k!}}$$

is transcendental, i.e. is not algebraic. To see this suppose on the contrary that it is algebraic and let n be its degree. Let $q = q_K = 2^{K!}$, $a = a_K = \sum_{k=0}^{K} 2^{K!-k!}$. Then $0 < \theta - a/q = \sum_{k=K+1}^{\infty} \frac{1}{2^{k!}} \le \frac{1}{2^{(K+1)!}} \sum_{l=0}^{\infty} \frac{1}{2^l} = \frac{2}{q^{K+1}}$, and so if K is sufficiently large we have

$$0 < |\theta - a_K/q_K| < \frac{c(\theta)}{q_K^n}$$

which contradicts Liouville's theorem.

In the quadratic case we know the α which give rise to the largest $c(\alpha)$.

Theorem 8.6. *Let $\alpha = \frac{1+\sqrt{5}}{2}$ and suppose that $c < \frac{1}{\sqrt{5}}$. Then the inequality $|\alpha - a/q| < cq^{-2}$ has only finitely many solutions.*

Proof. The irrational number α is a root of the polynomial $P(x) = x^2 - x - 1$. Moreover the other root of $P(x)$ is $\frac{1-\sqrt{5}}{2}$. Thus $P(a/q)$ is non-zero and $q^2 P(a/q) \in \mathbb{Z}$. Hence $|P(a/q)| \ge q^{-2}$. The polynomial $P(x)$ has an expansion

$$P(x) = \sqrt{5}(x - \alpha) + (x - \alpha)^2$$

about the point α. If $|\alpha - a/q| < cq^{-2}$, then the right hand side has absolute value

$$< \frac{\sqrt{5}c}{q^2} + \frac{c^2}{q^4}$$

when $x = a/q$. Hence

$$1 - \sqrt{5}c < c^2 q^{-2}$$

and this only holds for

$$q < \frac{c}{\sqrt{1 - c\sqrt{5}}}.$$

The box principle has many useful generalizations and applications, mostly in combinatorics, but there are several famous ones in number theory. Of course it is an immediate consequence of the principle of induction that if n sets partition a set of $n+1$ objects then one of them contains two objects. More generally when n sets partition a set of $kn+1$ objects one of them must contain $k+1$ objects, and consequently if a finite number of sets partition an infinite set, then one of them is also infinite.

We can use Dirichlet's theorem to treat Pell's equation, $x^2 - dy^2 = 1$. When d is a perfect square the solubility of the equation is boringly trivial. By factorising the left hand side and equating each factor to ±1 we see that the only solutions are $x = \pm 1$, $y = 0$ in that case. Therefore we henceforward suppose that d is not a perfect square. In particular $\sqrt{d}$ is irrational.

Let $\alpha = \sqrt{d}$ in Dirichlet's theorem. Since $\sqrt{d}$ is irrational, by the method of proof of Theorem 1.2 we can obtain an infinite sequence of triples of integers a_1, q_1, Q_1; a_2, q_2, Q_2; a_3, q_3, Q_3;... with

$$\left|\sqrt{d} - \frac{a_n}{q_n}\right| < \frac{1}{q_n(Q_n+1)}, \quad Q_{n+1} > \left|\sqrt{d} - \frac{a_n}{q_n}\right|^{-1}.$$

Thus

$$\begin{aligned}|a_n^2 - dq_n^2| &= \left|a_n - q_n\sqrt{d}\right| \left|a_n + q_n\sqrt{d}\right| \\ &\le \frac{1}{Q_n+1}\left|a_n - q_n\sqrt{d} + 2q_n\sqrt{d}\right| \\ &\le \frac{1}{Q_n+1}\left(\frac{1}{Q_n+1} + 2Q_n\sqrt{d}\right) \\ &< 2\sqrt{d}.\end{aligned}$$

Thus we have found infinitely many solutions to the inequality

$$|x^2 - dy^2| < 2\sqrt{d}.$$

Hence, by the box principle, there exists an integer t with $0 < |t| < 2\sqrt{d}$ such that there are infinitely many pairs x, y with

$$x^2 - dy^2 = t. \tag{2}$$

Again by the box principle, there are infinitely many pairs x and y so that not only (2) holds but x is in a fixed residue class modulo $|t|$ and y is in a fixed residue class modulo $|t|$.

Let x_0, y_0 be a given such pair and let x, y be another with x and y large (obviously if one is, then so is the other). Then

$$x \sim y\sqrt{d}.$$

Choose

$$u = \frac{|xx_0 - dyy_0|}{|t|}, \; v = \frac{|yx_0 - xy_0|}{|t|}.$$

Then $v \sim y|x_o - y_0\sqrt{d}||t|^{-1} \to \infty$ with y since $\sqrt{d}$ is irrational. Moreover

$$\begin{aligned}u^2 - dv^2 &= t^{-2}\left((xx_0 - dyy_0)^2 - d(yx_0 - xy_0)^2\right) \\ &= t^{-2}(x^2x_0^2 - dy^2x_0^2 - dx^2y_0^2 + d^2y^2y_0^2) \\ &= t^{-2}(x^2 - dy^2)(x_0^2 - dy_0^2) \\ &= 1.\end{aligned}$$

Thus we have produced infinitely many solutions to Pell's equation. It is, at least theoretically, possible to calculate solutions, for a given d, by this method, but this is very inefficient and there is a much faster way *via* the theory of continued fractions. However, it is now possible to obtain the structure of the complete solution set to Pell's equation. Let x_0, y_0 be the solution with $x_0 > 0$, $y_0 > 0$, $x_0 + y_0\sqrt{d}$ minimal. Then, by the binomial theorem there are $x_k > 0$, $y_k > 0$ such that

$$x_k \pm y_k\sqrt{d} = (x_0 \pm y_0\sqrt{d})^k$$

and it is easily verified that

$$x_k^2 - dy_k^2 = 1.$$

Suppose that there is another solution

$$X^2 - dY^2 = 1$$

with $X > 0$, $Y > 0$ and not in this list. Then for some $k \geq 0$

$$x_k + y_k\sqrt{d} < X + Y\sqrt{d} < x_{k+1} + y_{k+1}\sqrt{d}.$$

Hence

$$1 < (X + Y\sqrt{d})(x_0 - y_0\sqrt{d})^k < x_0 + y_0\sqrt{d}$$

and again by the binomial theorem for some non-zero integers X', Y' we have

$$1 < X' + Y'\sqrt{d} = (X + Y\sqrt{d})(x_0 - y_0\sqrt{d})^k$$

and $X'^2 - dY'^2 = 1$. Clearly X' and Y' cannot both be negative and if X' is positive and Y' is negative, then we would have

$$X' + Y'\sqrt{d} = 1/(X' - Y'\sqrt{d}) < 1$$

and if X' is negative and Y' is positive, then the above formula shows that $X' + Y'\sqrt{d}$ is negative. Hence both X' and Y' are positive which would contradict the minimality of $x_0 + y_0\sqrt{d}$. Therefore the "complete" solution to Pell's equation (2) is given by $x + y\sqrt{d} = (x_0 + y_0\sqrt{d})^m$, $m = 1, 2, \ldots$ where x_0, y_0 is the "least" solution. Of course this argument gives no easy way of finding the least solution.

The set

$$\mathcal{F}_n = \left\{ \frac{a}{q} : 0 \leq a \leq q \leq n,\ (a,q) = 1 \right\}$$

is the *Farey series of order* n. Thus $\mathcal{F}_5$ is

$$\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}.$$

An analysis of $\mathcal{F}_n$ gives an alternative line of approach to questions of diophantine approximation.

Theorem 8.7.
(i) If $\frac{a}{q}$ and $\frac{b}{r}$ are successive terms of $\mathcal{F}_n$, then $qb - ar = 1$.
(ii) If $\frac{a}{q}$, $\frac{c}{s}$ and $\frac{b}{r}$ are three successive terms of $\mathcal{F}_n$, then

$$\frac{c}{s} = \frac{a+b}{q+r}.$$

Proof. (i) Since $(a, q) = 1$ we can solve the congruence $ay \equiv -1 \pmod{q}$ with $n - q < y \le n$. Let $x = (ay + 1)/q$, so that $qx - ay = 1$. Clearly $(x, y) = 1$. Thus $x/y \in \mathcal{F}_n$. Also $\frac{x}{y} = \frac{a}{q} + \frac{1}{qy}$, so that $\frac{x}{y}$ comes later in the series. If it is not b/r, then

$$\frac{x}{y} - \frac{b}{r} = \frac{xr - by}{yr} \ge \frac{1}{yr}$$

and

$$\frac{b}{r} - \frac{a}{q} = \frac{bq - ar}{rq} \ge \frac{1}{rq}.$$

Hence

$$\frac{1}{yq} = \frac{x}{y} - \frac{a}{q} \ge \frac{1}{yr} + \frac{1}{rq} = \frac{y+q}{yrq} > \frac{n}{yrq} \ge \frac{1}{yq}$$

which is absurd.

(ii) By (i), $qc - as = 1$ and $sb - cr = 1$. Solving for c and s gives

$$c(qb - ar) = b + a, \; s(bq - ar) = q + r.$$

and (ii) follows.

As defined, the elements of $\mathcal{F}_n$ lie in $[0, 1]$, but we could just as well take

$$\mathcal{F}_n^* = \left\{ \frac{a}{q} : 1 \le q \le n, \; (a, q) = 1 \right\}$$

and quite clearly the above theorem holds for $\mathcal{F}_n^*$ in place of $\mathcal{F}_n$.

Suppose that $\frac{a_-}{q_-}$, $\frac{a}{q}$, $\frac{a_+}{q_+}$ are three successive terms of $\mathcal{F}_n^*$. Clearly

$$\frac{a_-}{q_-} < \frac{a_- + a}{q_- + q} < \frac{a}{q} < \frac{a + a_+}{q + q_+} < \frac{a_+}{q_+}.$$

Thus we can partition $\mathbb{R}$ into intervals $I(a/q)$ of the form

$$\left[\frac{a_- + a}{q_- + q}, \frac{a + a_+}{q + q_+} \right).$$

Moreover

$$(a + a_\pm)q - a(q + q_\pm) = a_\pm q - a q_\pm = \pm 1,$$

so that $(a + a_\pm, q + q_\pm) = 1$ and

$$\frac{a + a_\pm}{q + q_\pm} - \frac{a}{q} = \frac{\pm 1}{(q + q_\pm)q}.$$

Since the $\frac{a+a_\pm}{q+q_\pm}$ are not in $\mathcal{F}_n$ we must have $q + q_\pm \ge n + 1$. Hence each interval $I(a/q)$ is of the form

$$\left[\frac{a}{q} - \frac{\theta_-}{q(n+1)}, \frac{a}{q} + \frac{\theta_+}{q(n+1)} \right)$$

with $0 \le \theta_\pm \le 1$. Since the $I(a/q)$ partition $\mathbb{R}$ we have another proof of Dirichlet's theorem.