

Updated: May 25, 2010

Diophantine approximation, irrationality and transcendence

Michel Waldschmidt

Course N°11, May 24, 2010

These are informal notes of my course given in April – June 2010 at IMPA (*Instituto Nacional de Matematica Pura e Aplicada*), Rio de Janeiro, Brazil.

Recall Hurwitz's Theorem, which is the implication (i) \implies (vi) of Proposition 4.

Lemma 112. *Let ϑ be a real number. The following conditions are equivalent:*

- (i) ϑ is irrational.
- (ii) There exist infinitely many $p/q \in \mathbf{Q}$ such that

$$0 < \left| \vartheta - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}.$$

We proved it by using continued fractions, as a consequence of Borel's Lemma 110: *among three consecutive convergents of the continued fraction of an irrational number ϑ , one at least satisfies property (ii) of Lemma 112.*

We give two further proofs of Lemma 112: the first one rests on Farey's series, the last one does not involve continued fractions nor Farey series (but the ideas are very similar). The last proof yields a new irrationality criterion (Lemma 120).

6.5 Farey series

6.5.1 Definition and properties

For $n \geq 1$, the *Farey series* \mathcal{F}_n of order n is the finite increasing sequence of rational numbers in the range $[0, 1]$ having denominators $\leq n$. Each of them starts with 0 and ends with 1. Here are the first ones

$$\mathcal{F}_1 = \{0, 1\}$$

$$\begin{aligned}
\mathcal{F}_2 &= \left\{ 0, \frac{1}{2}, 1 \right\} \\
\mathcal{F}_3 &= \left\{ 0, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, 1 \right\} \\
\mathcal{F}_4 &= \left\{ 0, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1 \right\} \\
\mathcal{F}_5 &= \left\{ 0, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, 1 \right\} \\
\mathcal{F}_6 &= \left\{ 0, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, 1 \right\} \\
\mathcal{F}_7 &= \left\{ 0, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{5}{6}, \frac{6}{7}, 1 \right\} \\
\mathcal{F}_8 &= \left\{ 0, \frac{1}{8}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{3}{8}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{5}{8}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{5}{6}, \frac{6}{7}, \frac{7}{8}, 1 \right\}
\end{aligned}$$

The number of elements in \mathcal{F}_n is given by the inductive relation

$$|\mathcal{F}_n| = |\mathcal{F}_{n-1}| + \varphi(n),$$

with $|\mathcal{F}_1| = 2$, where $\varphi(n)$ is Euler's function ($\varphi(n)$ is the number of integers in the range $1, \dots, n$ which are relatively prime to n). Hence

$$|\mathcal{F}_n| = 1 + \sum_{m=1}^n \varphi(m).$$

One can deduce the estimate

$$|\mathcal{F}_n| \sim \frac{3n^2}{\pi^2}.$$

Proposition 113. *If $h/k < h'/k'$ are successive terms in a Farey series \mathcal{F}_n , then $h'k - hk' = 1$.*

For the proof, we follow § I.2 of [2]. Other proofs are given in [1], Chap. 3.

Lemma 114. *Let $x = (x_1, x_2)$ and $y = (y_1, y_2)$ be two elements of \mathbf{Z}^2 . The following conditions are equivalent:*

- (i) (x, y) is a basis of \mathbf{Z}^2 over \mathbf{Z} .
- (ii) $x_1y_2 - x_2y_1 = \pm 1$.

(iii) x and y are linearly independent over \mathbf{R} , and the closed parallelogram

$$\mathcal{P} = \{\lambda x + \mu y ; \lambda \in \mathbf{R}, \mu \in \mathbf{R}, 0 \leq \lambda \leq 1, 0 \leq \mu \leq 1\}$$

with vertices $0, x, y$ and $x + y$ does not contain integer points in \mathbf{Z}^2 but its vertices.

(iv) x and y are linearly independent over \mathbf{R} , and the closed triangle

$$\mathcal{T} = \{\lambda x + \mu y ; \lambda \in \mathbf{R}_{\geq 0}, \mu \in \mathbf{R}_{\geq 0}, \lambda + \mu \leq 1\}$$

with vertices $0, x$ and y , does not contain integer points in \mathbf{Z}^2 but its vertices.

Proof. A change of basis for \mathbf{Z}^2 has an invertible matrix with determinant a unit in \mathbf{Z} , hence (i) \iff (ii).

Assume (i). Any element z in \mathbf{Z}^2 can be written in a unique way as $\lambda x + \mu y$ with λ and μ in \mathbf{R} , and these numbers λ and μ are in \mathbf{Z} . Hence, when $z \in \mathcal{P}$, we have $0 \leq \lambda \leq 1, 0 \leq \mu \leq 1$, and therefore each of λ, μ is 0 or 1. This proves (iii).

Conversely, assume (iii). Let $u \in \mathbf{Z}^2$. Since (x, y) is a basis of \mathbf{R}^2 over \mathbf{R} , we can write $u = tx + t'y$ with t and t' in \mathbf{R} . Define two integers a and a' by $a = \lfloor t \rfloor$ and $a' = \lfloor t' \rfloor$. From $0 \leq t - a < 1$ and $0 \leq t' - a' < 1$ we deduce $u - ax - a'y \in \mathbf{Z}^2 \cap \mathcal{P}$ with $u - ax - a'y \notin \{x, y\}$, hence $u = ax + a'y$. This proves (i).

Since \mathcal{P} contains \mathcal{T} , (iii) implies (iv).

Finally, assume (iv). If $z \in \mathcal{P} \cap \mathbf{Z}^2$ is distinct from $0, x$ and y , then $z \notin \mathcal{T}$, from which we deduce that $x + y - z \in \mathcal{T} \cap \mathbf{Z}^2$. From $z \neq x$ and $z \neq y$ we deduce $x + y - z = 0$, hence $z = x + y$. Therefore $\mathcal{P} \cap \mathbf{Z}^2 = \{0, x, y, x + y\}$, which is (iii). □

Proof of Proposition 113. Let $h/k < h'/k'$ be successive terms in the Farey series \mathcal{F}_n . From $(h, k) \neq (h', k')$ and $\gcd(h, k) = \gcd(h', k') = 1$, we deduce that the two vectors (h, k) and (h', k') of \mathbf{R}^2 are linearly independent. Since $h'k - hk' > 0$, using Lemma 114, it suffices to check that the triangle \mathcal{T} with vertices $0, x$ and y does not contain any element of \mathbf{Z}^2 but the vertices. Assume $z = (h'', k'') \in \mathcal{T} \cap \mathbf{Z}^2$ with $z \notin \{0, x, y\}$. We have $z = \lambda x + \mu y$ with $\lambda \geq 0, \mu \geq 0, 0 < \lambda + \mu \leq 1, (\lambda, \mu) \notin \{(0, 1); (1, 0)\}$. Then $k'' = \lambda k + \mu k' \leq n$ and $h/k < h''/k'' < h'/k'$, which contradicts the assumption that there is no element between h/k and h'/k' in \mathcal{F}_n . □

Corollary 115. *if $h/k < h''/k'' < h'/k'$ are successive elements in a Farey series \mathcal{F}_n , then*

$$\frac{h''}{k''} = \frac{h + h'}{k + k'}.$$

Proof. From Proposition 113 we deduce $h''k - hk'' = 1$, $h'k'' - h''k' = 1$, hence $h''(k + k') = k''(h + h')$. \square

Examples in \mathcal{F}_5 of \mathcal{F}_6 are $1/3 < 2/5 < 1/2 < 2/5$: the fraction $(h + h')/(k + k')$ may or may not be in reduced form.

Here is our second proof of Lemma 112.

Proposition 116. *Let $h/k < h'/k'$ be successive elements in a Farey series \mathcal{F}_n . Define $h'' = h + h'$, $k'' = k + k'$. Then h''/k'' is in reduced form, and for any α in the interval $h/k \leq \alpha \leq h'/k'$, at least one of the following inequalities hold:*

$$\alpha - \frac{h}{k} < \frac{1}{\sqrt{5}k^2}, \quad \left| \alpha - \frac{h''}{k''} \right| < \frac{1}{\sqrt{5}k''^2}, \quad \frac{h'}{k'} - \alpha < \frac{1}{\sqrt{5}k'^2}.$$

Proof. From $h(k + k') - (h + h')k = 1$, we deduce that $k + k'$ and $h + h'$ are relatively prime.

By symmetry we may assume $h''/k'' < \alpha < h'/k'$. If none of the inequalities hold, then

$$\alpha - \frac{h}{k} \geq \frac{1}{\sqrt{5}k^2}, \quad \alpha - \frac{h''}{k''} \geq \frac{1}{\sqrt{5}k''^2}, \quad \frac{h'}{k'} - \alpha \geq \frac{1}{\sqrt{5}k'^2}.$$

Using $h'k - hk' = 1$ and $h'k'' - h''k' = 1$, we deduce

$$\frac{1}{kk'} \geq \frac{1}{\sqrt{5}} \left(\frac{1}{k^2} + \frac{1}{k'^2} \right)$$

and

$$\frac{1}{k'k''} \geq \frac{1}{\sqrt{5}} \left(\frac{1}{k'^2} + \frac{1}{k''^2} \right).$$

We deduce

$$\sqrt{5}kk' \geq k^2 + k'^2 \quad \text{and} \quad \sqrt{5}k'k'' \geq k'^2 + k''^2,$$

which means that the numbers $x = k/k'$ and $y = k'/k''$ satisfy

$$x^2 - \sqrt{5}x + 1 \leq 0 \quad \text{and} \quad y^2 - \sqrt{5}y + 1 \leq 0.$$

Since the roots of $X^2 - \sqrt{5}X + 1$ are Φ and $1/\Phi$, it follows that x and y lie in the interval $(1/\Phi, \Phi)$. From $k'' = k + k'$ we deduce $1/y = x + 1$, hence:

$$\frac{1}{\Phi} + 1 \leq x + 1 = \frac{1}{y} \leq \Phi.$$

Since x and y are rational numbers, this is not compatible with the irrationality of Φ . \square

Notice that the end of the proof is the same as the proof of Borel's Lemma 110.

We conclude this section by some further remark on Farey sequences, which we do not plan to use, but which may be interesting to know.

The converse of Corollary 115 is true: *If h, k, h', k' are positive integers with $0 < h/k < h'/k' < 1$ which satisfy $h'k - kh' = 1$, then h/k and h'/k' are consecutive elements in the Farey series \mathcal{F}_n with $n = \max\{k, k'\}$.*

Here is the proof. Suppose first $k \geq k'$. Denote by h''/k'' the successor of h/k in \mathcal{F}_k . Then $h''k - k''h = 1$ and $1 \leq k'' \leq k$, hence $(h'' - h')k = (k'' - k')h$, which shows that k' and k'' are congruent modulo k . Since they both lie in the interval $[1, k]$, we deduce $k' = k''$, hence $h' = h''$.

Similarly, if $k < k'$, we denote by h''/k'' the predecessor of h'/k' in $\mathcal{F}_{k'}$. The same argument gives $h/k = h''/k''$. \square

It follows that *if $h/k < h'/k'$ are consecutive in the Farey series \mathcal{F}_n , then the smallest $m > n$ such that there is an element h''/k'' of \mathcal{F}_m in the interval $h/k < h''/k'' < h'/k'$ is $m = k + k'$, this element h''/k'' is unique and $h'' = h + h', k'' = k + k' = m$.*

Indeed, by definition of m , we have $m = k''$. From the inequalities

$$\frac{h}{k} < \frac{h + h'}{k + k'} < \frac{h'}{k'},$$

it follows that $m \leq k + k'$. The unicity of an element of \mathcal{F}_m in this interval follows from the fact that two distinct rational numbers with denominator m are at distance $\geq 1/m$, while Proposition 113 yields

$$\frac{h'}{k'} - \frac{h}{k} = \frac{1}{kk'} < \frac{1}{m}.$$

We have seen in Proposition 116 that $(h + h')/(k + k')$ is in reduced form. Finally Corollary 115 shows that $h''/k'' = (h + h')/(k + k')$, hence $k'' = k + k'$.

Here is a connection with continued fractions: *let p/q be an irreducible fraction with $q \geq 2$; write the continued fraction of p/q which ends with*

$a_n \geq 2$ as $p/q = [0, a_1, \dots, a_n]$. Then the predecessors and successors of p/q in the Farey series \mathcal{F}_q have continued fractions $[0, a_1, \dots, a_n - 1]$ and $[0, a_1, \dots, a_{n-1}]$:

$$[0, a_1, \dots, a_{n-1}] < \frac{p}{q} = [0, a_1, \dots, a_n] < [0, a_1, \dots, a_n - 1] \quad \text{if } n \text{ is odd,}$$

$$[0, a_1, \dots, a_n - 1] < \frac{p}{q} = [0, a_1, \dots, a_n] < [0, a_1, \dots, a_{n-1}] \quad \text{if } n \text{ is even.}$$

Indeed, using the other continued fraction $p/q = [0, a_1, \dots, a_n - 1, 1] = p_{n+1}/q_{n+1}$, we write as in (64)

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

where $p_n/q_n = [0, a_1, \dots, a_n - 1]$ and $p_{n-1}/q_{n-1} = [0, a_1, \dots, a_{n-1}]$, and we have $q_{n-1} < q_n < q$, $pq_n - p_nq = (-1)^n$, $pq_{n-1} - p_{n-1}q = (-1)^{n-1}$ (recall Lemma 68 with n replaced by $n+1$ and $a_{n+1} = 1$). Hence the result follows from the previous remarks.

6.5.2 Hurwitz Theorem

Here is the third proof of Hurwitz's Lemma 112.

We start with the next auxiliary result, which also follows from the results we proved on continued fractions (take for p/q and r/s two consecutive convergents of ϑ) or on Farey series (take two consecutive elements of a Farey series such that ϑ is in their interval).

Lemma 117. *Let ϑ be a real irrational number. Then there exist infinitely many pairs $(p/q, r/s)$ of irreducible fractions such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \text{and} \quad qr - ps = 1.$$

In this statement and the next ones, it is sufficient to prove inequalities \leq in place of $<$: this follows from the irrationality of ϑ .

Proof. Let H be a positive integer. Among the irreducible rational fractions a/b with $1 \leq b \leq H$, select one for which $|\vartheta - a/b|$ is minimal. If $a/b < \vartheta$ rename a/b as p/q , while if $a/b > \vartheta$, then rename a/b as r/s .

First consider the case where $a/b < \vartheta$, hence $a/b = p/q$. Since $\gcd(p, q) = 1$, using Euclidean's algorithm, one deduces (Bézout's Theorem) that there

exist $(r, s) \in \mathbf{Z}^2$ such that $qr - sp = 1$ with $1 \leq s < q$ and $|r| < |p|$. Since $1 \leq s < q \leq H$, from the choice of a/b it follows that

$$\left| \vartheta - \frac{p}{q} \right| \leq \left| \vartheta - \frac{r}{s} \right|$$

hence r/s does not belong to the interval $[p/q, \vartheta]$. Since $qr - sp > 0$ we also have $p/q < r/s$, hence $\vartheta < r/s$.

In the second case where $a/b > \vartheta$ and $r/s = a/b$ we solve $qr - sp = 1$ by Euclidean algorithm with $1 \leq q < s$ and $|p| < r$, and the argument is similar.

We now complete the proof of the existence of infinitely many such pairs. Once we have a finite set of such pairs $(p/q, r/s)$, we use the fact that there is a rational number m/n closer to ϑ than any of these rational fractions. We use the previous argument with $H \geq n$. This way we produce a new pair $(p/q, r/s)$ of rational numbers which is none of the previous ones (because one at least of the two rational numbers $p/q, r/s$ is a better approximation than the previous ones). Hence this construction yields infinitely many pairs, as claimed. □

Lemma 118. *Let ϑ be a real irrational number. Assume $(p/q, r/s)$ are irreducible fractions such that*

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \text{and} \quad qr - ps = 1.$$

Then

$$\min \left\{ q^2 \left(\vartheta - \frac{p}{q} \right), s^2 \left(\frac{r}{s} - \vartheta \right) \right\} < \frac{1}{2}.$$

Proof. Define

$$\delta = \min \left\{ q^2 \left(\vartheta - \frac{p}{q} \right), s^2 \left(\frac{r}{s} - \vartheta \right) \right\}.$$

From

$$\frac{\delta}{q^2} \leq \vartheta - \frac{p}{q} \quad \text{and} \quad \frac{\delta}{s^2} \leq \frac{r}{s} - \vartheta$$

with $qr - ps = 1$ one deduces that the number $t = s/q$ satisfies

$$t + \frac{1}{t} \leq \frac{1}{\delta}.$$

Since the minimum of the function $t \mapsto t + 1/t$ is 2 and since $t \neq 1$, we deduce $\delta < 1/2$. □

Remark. The inequality $t + (1/t) \geq 2$ for all $t > 0$ with equality if and only if $t = 1$ is equivalent to the arithmetico-geometric inequality

$$\sqrt{xy} \leq \frac{x+y}{2},$$

when x and y are positive real numbers, with equality if and only if $x = y$. The correspondance between both estimates is $t = \sqrt{x/y}$.

From Lemmas 117 and 118 it follows that for $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$, there exist infinitely many $p/q \in \mathbf{Q}$ such that

$$0 < \left| \vartheta - \frac{p}{q} \right| < \frac{1}{2q^2}.$$

A further step is required in order to complete the proof of Lemma 112.

Lemma 119. Let ϑ be a real irrational number. Assume $(p/q, r/s)$ are irreducible fractions such that

$$\frac{p}{q} < \vartheta < \frac{r}{s} \quad \text{and} \quad qr - ps = 1.$$

Define $u = p + r$ and $v = q + s$. Then

$$\min \left\{ q^2 \left(\vartheta - \frac{p}{q} \right), s^2 \left(\frac{r}{s} - \vartheta \right), v^2 \left| \vartheta - \frac{u}{v} \right| \right\} < \frac{1}{\sqrt{5}}.$$

Proof. First notice that $qu - pv = 1$ and $rv - su = 1$. Hence

$$\frac{p}{q} < \frac{u}{v} < \frac{r}{s}.$$

We repeat the proof of lemma 118 ; we distinguish two cases according to whether u/v is larger or smaller than ϑ . Since both cases are quite similar, let us assume $\vartheta < u/v$. The proof of lemma 118 shows that

$$\frac{s}{q} + \frac{q}{s} \leq \frac{1}{\delta} \quad \text{and} \quad \frac{v}{q} + \frac{q}{v} \leq \frac{1}{\delta}.$$

Hence each of the four numbers $s/q, q/s, v/q, q/v$ satisfies $t+1/t \leq 1/\delta$. Now the function $t \mapsto t+1/t$ is decreasing on the interval $(0, 1)$ and increasing on the interval $(1, +\infty)$. It follows that our four numbers all lie in the interval $(1/x, x)$, where x is the root > 1 of the equation $x + 1/x = 1/\delta$. The two roots x and $1/x$ of the quadratic polynomial $X^2 - (1/\delta)X + 1$ are at a mutual

distance equal to the square root of the discriminant $\Delta = (1/\delta)^2 - 4$ of this polynomial. Now

$$\frac{v}{q} - \frac{s}{q} = 1,$$

hence the length $\sqrt{\Delta}$ of the interval $(1/x, x)$ is ≥ 1 and therefore $\delta \leq 1/\sqrt{5}$. This completes the proof of Lemma 119. \square

Remark. In the three proofs of Hurwitz's Theorem, the number $\sqrt{5}$ occurs as follows: for any $x > 1$,

$$\max \left\{ x + \frac{1}{x}, \frac{1+x}{x} + \frac{x}{1+x} \right\} \geq \sqrt{5},$$

with equality if and only if $x = \Phi$ (the Golden ratio). Indeed, for $x > 1$ we have

$$x + \frac{1}{x} > \sqrt{5} \iff x > \Phi$$

and, with $t = (x+1)/x$,

$$t + \frac{1}{t} > \sqrt{5} \iff t > \Phi \iff x + \frac{1}{x} > \sqrt{5} \iff x < \Phi.$$

6.5.3 A further irrationality criterion

Lemma 120. *Let ϑ be a real number. The following conditions are equivalent:*

- (i) ϑ is irrational.
- (ii) For any $\epsilon > 0$ there exists p/q and r/s in \mathbf{Q} such that

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q\vartheta - p; r - s\vartheta\} < \epsilon.$$

- (iii) There exist infinitely many pairs $(p/q, r/s)$ of rational numbers such that

$$\frac{p}{q} < \vartheta < \frac{r}{s}, \quad qr - ps = 1$$

and

$$\max\{q(q\vartheta - p); s(r - s\vartheta)\} < 1.$$

Proof. The implications (iii) \implies (ii) \implies (i) are easy. For (i) \implies (iii) we are going to combine the arguments in the proof of Lemma 117 with results from the theory of continued fractions.

Since ϑ is irrational, there are infinitely many p/q such that

$$\left| \vartheta - \frac{p}{q} \right| < \frac{1}{2q^2}.$$

This is a weak form of Hurwitz Lemma 112. According to Legendre's Lemma 111, such a p/q is a convergent of ϑ . The best approximation property of the convergents (Lemma 105) implies that for any $a/b \in \mathbf{Q}$ with $1 \leq b \leq q$ and $a/b \neq p/q$, we have

$$\left| \vartheta - \frac{a}{b} \right| > \left| \vartheta - \frac{p}{q} \right|.$$

Assume first $p/q < \vartheta$. Let r/s be defined by $qr - ps = 1$ and $1 \leq s < q$, $|r| < |p|$. We have

$$0 < \frac{r}{s} - \vartheta < \frac{r}{s} - \frac{p}{q} = \frac{1}{qs} \leq \frac{1}{s^2}.$$

Next assume $p/q > \vartheta$. In this case rename it r/s and define p/q by $qr - ps = 1$ and $1 \leq q < s$, $|p| < |r|$.

Finally, repeat the argument in the proof of Lemma 117 to get an infinite set of approximations. Lemma 120 follows. \square

References

- [1] G. H. HARDY AND E. M. WRIGHT, *An introduction to the theory of numbers*, Oxford University Press, Oxford, sixth ed., 2008. Revised by D. R. Heath-Brown and J. H. Silverman.
- [2] W. M. SCHMIDT, *Diophantine approximation*, vol. **785**, Lecture Notes in Mathematics. Berlin-Heidelberg-New York: Springer-Verlag, 1980, new ed. 2001.