This implies $0 \le \alpha - a_0 < 1$, so $a_0 = \lfloor \alpha \rfloor$ and thus, a_0 is unique. Therefore, $\alpha_1 = [a_1, a_2, \ldots]$ is also uniquely determined by α. Now, $a_1 = \lfloor \alpha_1 \rfloor$ so a_1 is also unique, etc. ☐

Definition 8.3. *Let α be an irrational number. If $\alpha = [a_0, a_1, a_2, \ldots]$, then we call this expression the expansion of α into* (infinite) simple continued fraction*; $\frac{p_i}{q_i} = [a_0, \ldots, a_i]$ is the i-th* convergent *of α, a_i is the i-th* partial quotient*, and $\alpha_i = [a_i, a_{i+1}, \ldots]$ is the i-th* complete quotient *of α. Here, the word "simple" (as with finite continued fractions) refers to continued fractions which satisfy the conditions $a_0 \in \mathbb{Z}$, $a_i \in \mathbb{N}$ for $i \ge 1$. Since we will mostly consider only such continued fractions, we will occasionally omit the word "simple".*

Example 8.3. Let $\alpha = [1, 1, 1, \ldots]$. Then, from $\alpha = 1 + \frac{1}{[1,1,1,\ldots]} = 1 + \frac{1}{\alpha}$, it follows that $\alpha^2 - \alpha - 1 = 0$, so since $\alpha \ge 1$, we have $\alpha = \frac{\sqrt{5}+1}{2}$.

The convergents $\frac{p_n}{q_n}$ satisfy the recurrences

$$\begin{aligned} p_n &= p_{n-1} + p_{n-2}, \quad p_0 = 1, \quad p_1 = 2, \\ q_n &= q_{n-1} + q_{n-2}, \quad q_0 = 1, \quad q_1 = 1. \end{aligned}$$

Therefore, $p_n = F_{n+2}$, $q_n = F_{n+1}$, where $(F_n)_n$ is the sequence of Fibonacci numbers.

8.4 Continued fraction and approximations to irrational numbers

Let α be an irrational number. By formula (8.12), each convergent of α satisfies the inequality

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2},$$

which provides an alternative (constructive) proof of Corollary 8.2.

Theorem 8.23 (Vahlen, 1895). *Let $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$ be two consecutive convergents of α. Then at least one of them satisfies the inequality*

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

Proof: Numbers $\alpha - \frac{p_n}{q_n}$, $\alpha - \frac{p_{n-1}}{q_{n-1}}$ have opposite signs, so

$$\left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| = \left|\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\right| = \frac{1}{q_n q_{n-1}} < \frac{1}{2q_n^2} + \frac{1}{2q_{n-1}^2}$$

(since $2ab < a^2 + b^2$ for $a \neq b$). Accordingly,

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{or} \quad \left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{2q_{n-1}^2}. \qquad \square$$

Theorem 8.24 (Borel, 1903). *Let $\frac{p_{n-2}}{q_{n-2}}, \frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}$ be three consecutive convergents of α. Then at least one of them satisfies the inequality*

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

Proof: Put $\alpha = [a_0, a_1, \dots]$, $\alpha_i = [a_i, a_{i+1}, \dots]$ and $\beta_i = \frac{q_{i-2}}{q_{i-1}}$ for $i \geq 1$. From Lemma 8.17, we have

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}. \tag{8.13}$$

To complete the proof, we have to show that there is no positive integer n such that for $i = n-1, n, n+1$ we have

$$\alpha_i + \beta_i \leq \sqrt{5}. \tag{8.14}$$

Assume that (8.14) is satisfied for $i = n-1, n$. Then from

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}, \qquad \frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = a_{n-1} + \beta_{n-1},$$

it follows that

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1} \leq \sqrt{5}.$$

Hence, $1 = \alpha_n \cdot \frac{1}{\alpha_n} \leq (\sqrt{5} - \beta_n)(\sqrt{5} - \frac{1}{\beta_n})$, which is equivalent to $\beta_n^2 - \sqrt{5}\beta_n + 1 \leq 0$. This implies that $\beta_n \geq \frac{\sqrt{5}-1}{2}$, and since β_n is rational, we get $\beta_n > \frac{\sqrt{5}-1}{2}$.

If (8.14) is also satisfied for $i = n, n+1$, then in the same way we get $\beta_{n+1} > \frac{\sqrt{5}-1}{2}$. Thus, we obtain

$$1 \leq a_n = \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}} = \frac{1}{\beta_{n+1}} - \beta_n < \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} = 1,$$

a contradiction. $\square$

Lemma 8.25. *Assume that α has a continued fraction expansion of the form*

$$\alpha = [a_0, a_1, \dots, a_N, 1, 1, 1, \dots].$$

Then $\lim_{n\to\infty} q_n^2 \left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{\sqrt{5}}.$

Proof: In the notation of Theorem 8.24, we have

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}.$$

Here, for n large enough, $\alpha_{n+1} = [1, 1, 1, \dots] = \frac{\sqrt{5}+1}{2}$ and, by Lemma 8.18,

$$\frac{1}{\beta_{n+1}} = \frac{q_n}{q_{n-1}} = [a_n, a_{n-1}, \dots, a_1] = [\underbrace{1, 1, \dots, 1}_{n-N}, a_N, \dots, a_1].$$

Since $[\underbrace{1, 1, \dots, 1}_{n-N-1}]$ and $[\underbrace{1, 1, \dots, 1}_{n-N}]$ are two consecutive convergents of $\frac{1}{\beta_{n+1}}$, we conclude that $\frac{1}{\beta_{n+1}}$ lies between them. Hence, $\lim_{n\to\infty} \frac{1}{\beta_{n+1}} = [1, 1, 1, \dots] = \frac{\sqrt{5}+1}{2}$. Therefore,

$$\lim_{n\to\infty} \beta_{n+1} = \left(\frac{\sqrt{5}+1}{2}\right)^{-1} = \frac{\sqrt{5}-1}{2} \quad \text{and} \quad \lim_{n\to\infty} (\alpha_{n+1} + \beta_{n+1}) = \sqrt{5}.$$

□

Theorem 8.26 (Legendre, 1798)**.** *Let p, q be integers such that $q \geq 1$ and*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}. \tag{8.15}$$

Then $\frac{p}{q}$ is a convergent of α.

Proof: We can assume that $\alpha \neq \frac{p}{q}$; otherwise, the statement is trivially satisfied. Then we can write $\alpha - \frac{p}{q} = \frac{\varepsilon\vartheta}{q^2}$, where $0 < \vartheta < \frac{1}{2}$ and $\varepsilon = \pm 1$. By Lemma 8.21, there is a continued fraction expansion of $\frac{p}{q}$,

$$\frac{p}{q} = [b_0, b_1, \dots, b_{n-1}],$$

where n is chosen such that $(-1)^{n-1} = \varepsilon$.

Let us define ω by

$$\alpha = \frac{\omega p_{n-1} + p_{n-2}}{\omega q_{n-1} + q_{n-2}}, \tag{8.16}$$

so that $\alpha = [b_0, b_1 \dots, b_{n-1}, \omega]$. Note that (8.16) is equivalent to

$$(\alpha q_{n-1} - p_{n-1})\omega = p_{n-2} - \alpha q_{n-2}.$$

We can assume that $\alpha q_{n-1} - p_{n-1} \neq 0$ because otherwise $\alpha = \frac{p_{n-1}}{q_{n-1}} = \frac{p}{q}$.

Now, from Lemma 8.17,

$$\frac{\varepsilon\vartheta}{q^2} = \alpha - \frac{p}{q} = \frac{1}{q_{n-1}}(\alpha q_{n-1} - p_{n-1}) = \frac{1}{q_{n-1}} \cdot \frac{(-1)^{n-1}}{\omega q_{n-1} + q_{n-2}},$$

so $\vartheta = \frac{q_{n-1}}{\omega q_{n-1} + q_{n-2}}$. By solving this equation for ω, we obtain $\omega = \frac{1}{\vartheta} - \frac{q_{n-2}}{q_{n-1}}$. This implies that $\omega > 2 - 1 = 1$. Let us expand ω in a (finite or infinite) simple continued fraction

$$\omega = [b_n, b_{n+1}, b_{n+2}, \dots].$$

Since $\omega > 1$, all b_j $(j = n, n+1, \dots)$ are positive integers. By Lemma 8.14 and taking the limit if necessary, we obtain

$$\begin{aligned} \alpha &= [b_0, b_1, \dots, b_{n-1}, [b_n, b_{n+1}, \dots]] \\ &= [b_0, b_1, \dots, b_{n-1}, b_n, b_{n+1}, \dots]. \end{aligned}$$

This is a simple continued fraction expansion of α and

$$\frac{p}{q} = \frac{p_{n-1}}{q_{n-1}} = [b_0, b_1, \dots, b_{n-1}]$$

is a convergent of α, which is the desired conclusion. □

The second proof of Hurwitz's theorem 8.9: The statement (i) follows directly from Theorem 8.24, while the statement (ii) follows from Lemma 8.25 and Theorem 8.26. Namely, if an irrational number α has the form from Lemma 8.25, then, by Theorem 8.26, all solutions of the inequality $\left|\alpha - \frac{p}{q}\right| < \frac{1}{Aq^2}$, where $A > \sqrt{5}$, are found among convergents of α, and according to Lemma 8.25, this inequality is satisfied by only finitely many convergents of α. □

Legendre's theorem 8.26 provides an elegant description of rational approximations which satisfy inequality (8.15). However, in application to Diophantine equation and in cryptanalysis, somewhat weaker inequalities often appear (a constant with q^{-2} on the right-hand side might be greater than $1/2$), and the question arises whether such weaker rational approximations can also be described in terms of continued fractions. The answer to this question is provided in the following theorem from [420], which we give in the formulation from [119].

Theorem 8.27 (Worley, 1981). *Let α be an arbitrary real number and c a positive real number. If the rational number $\frac{p}{q}$ satisfies the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}, \tag{8.17}$$

then

$$\frac{p}{q} = \frac{rp_{k+1} \pm sp_k}{rq_{k+1} \pm sq_k},$$

for some $k \geq -1$ and non-negative integers r, s such that $rs < 2c$ (and some choice of the sign).

Proof: We will suppose that $\alpha < \frac{p}{q}$. In the case $\alpha > \frac{p}{q}$, the proof is analogous. We will also assume that α is irrational (for α rational, a small modification of the proof is needed). Let k be the largest odd integer such that

$$\alpha < \frac{p}{q} \leq \frac{p_k}{q_k}.$$

(If $\frac{p}{q} > \frac{p_1}{q_1}$, then we take $k = -1$.) Let us define numbers r and s by

$$p = rp_{k+1} + sp_k,$$
$$q = rq_{k+1} + sq_k.$$

By Lemma 8.15, the determinant of this system is ± 1, so r, s are integers, and since $\frac{p_{k+1}}{q_{k+1}} < \frac{p}{q} \leq \frac{p_k}{q_k}$, we have $r \geq 0$ and $s > 0$.

Due to the maximality of k, we have

$$\left|\frac{p_{k+2}}{q_{k+2}} - \frac{p}{q}\right| < \left|\alpha - \frac{p}{q}\right| < \frac{c}{q^2}.$$

Furthermore,

$$\begin{aligned}\left|\frac{p_{k+2}}{q_{k+2}} - \frac{p}{q}\right| &= \frac{(a_{k+2}q_{k+1} + q_k)(rp_{k+1} + sp_k) - (a_{k+2}p_{k+1} + p_k)(rq_{k+1} + sq_k)}{qq_{k+2}} \\ &= \frac{sa_{k+2} - r}{qq_{k+2}}.\end{aligned}$$

Hence,

$$q(sa_{k+2} - r) < cq_{k+2} = \frac{c}{s}((sa_{k+2} - r)q_{k+1} + q),$$

i.e.

$$(sa_{k+2} - r)(q - \frac{c}{s}q_{k+1}) < \frac{c}{s}\,q.$$

Furthermore, we have

$$\frac{1}{sa_{k+2}-r} > \frac{q-\frac{c}{s}q_{k+1}}{\frac{c}{s}q} = \frac{s}{c} - \frac{1}{r+\frac{sq_k}{q_{k+1}}} \geq \frac{s}{c} - \frac{1}{r}.$$

Therefore, we obtained the inequality (quadratic inequality for r)

$$r^2 - sra_{k+2} + ca_{k+2} > 0. \tag{8.18}$$

We now distinguish two cases:

1) $s^2a_{k+2} \geq 4c$
   In this case, we have $s^4a_{k+2}^2 - 4cs^2a_{k+2} \geq (s^2a_{k+2}-4c)^2$, so the solutions of inequality (8.18) satisfy

$$r < \frac{1}{2s}\left(s^2a_{k+2} - \sqrt{s^4a_{k+2}^2 - 4cs^2a_{k+2}}\right) \leq \frac{2c}{s}$$

   or

$$r > \frac{1}{2s}\left(s^2a_{k+2} + \sqrt{s^4a_{k+2}^2 - 4cs^2a_{k+2}}\right) \geq \frac{1}{s}(s^2a_{k+2} - 2c).$$

   From the first possibility, it follows that $rs < 2c$. If the second possibility takes place, we introduce the substitution $t = sa_{k+2} - r$. The number t is a positive integer. Now we have

$$p = rp_{k+1} + sp_k = (sa_{k+2} - t)p_{k+1} + sp_k = sp_{k+2} - tp_{k+1},$$
$$q = sq_{k+2} - tq_{k+1}$$

   and $st = s^2a_{k+2} - rs < 2c$.

2) $s^2a_{k+2} < 4c$
   If $r < \frac{1}{2}sa_{k+2}$, then $rs < \frac{1}{2}s^2a_{k+2} < 2c$. If $\frac{1}{2}sa_{k+2} \leq r < sa_{k+2}$, then we again define $t = sa_{k+2} - r$ and we get $st \leq \frac{1}{2}s^2a_{k+2} < 2c$. □

If we substitute $c = 1$ in Theorem 8.27, we obtain the following result.

Corollary 8.28 (Fatou, 1904; Grace, 1918). *Let α be a real number and p, q integers such that $q \geq 1$ and*

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

Then there is $n \geq 0$ such that

$$\frac{p}{q} = \frac{p_n}{q_n} \quad \text{or} \quad \frac{p_n - p_{n-1}}{q_n - q_{n-1}} \quad \text{or} \quad \frac{p_n + p_{n-1}}{q_n + q_{n-1}}.$$

Theorem 8.29 (Lagrange, 1770)**.** *Let α be an irrational number and let $\frac{p_0}{q_0}$, $\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots$ be the convergents of α. Then*

(i) $|\alpha q_0 - p_0| > |\alpha q_1 - p_1| > |\alpha q_2 - p_2| > \cdots$

(ii) If $n \geq 1$, $1 \leq q \leq q_n$, and $(p, q) \neq (p_{n-1}, q_{n-1})$, (p_n, q_n), then $|\alpha q - p| > |\alpha q_{n-1} - p_{n-1}|$.

Proof: By Lemma 8.17, we have

$$\begin{aligned} |\alpha q_n - p_n| &= \frac{1}{\alpha_{n+1} q_n + q_{n-1}} < \frac{1}{q_n + q_{n-1}}, \\ |\alpha q_{n-1} - p_{n-1}| &= \frac{1}{\alpha_n q_{n-1} + q_{n-2}} > \frac{1}{(a_n + 1) q_{n-1} + q_{n-2}} = \frac{1}{q_{n-1} + q_n}, \end{aligned}$$

and the statement (i) follows.

In order to prove (ii), let us define numbers μ, ν by the equations

$$\begin{aligned} \mu p_n + \nu p_{n-1} &= p, \\ \mu q_n + \nu q_{n-1} &= q. \end{aligned}$$

The matrix of this system has determinant ± 1, so the numbers μ, ν are integers. If $\nu = 0$, then $p = \mu p_n$, $q = \mu q_n$, and this is impossible because $0 < q \leq q_n$ and $(p, q) \neq (p_n, q_n)$. If $\mu = 0$, then $p = \nu p_{n-1}$, $q = \nu q_{n-1}$. Since $(p, q) \neq (p_{n-1}, q_{n-1})$, we have $\nu \geq 2$, and hence

$$|\alpha q - p| \geq 2|\alpha q_{n-1} - p_{n-1}| > |\alpha q_{n-1} - p_{n-1}|.$$

If $\mu \neq 0$ and $\nu \neq 0$, then, due to $1 \leq q \leq q_n$, μ and ν have opposite signs and the numbers $\mu(\alpha q_n - p_n)$ and $\nu(\alpha q_{n-1} - p_{n-1})$ have equal signs. Thus,

$$|\alpha q - p| = |\mu(\alpha q_n - p_n)| + |\nu(\alpha q_{n-1} - p_{n-1})|,$$

so, since $\mu\nu \neq 0$, we get $|\alpha q - p| > |\alpha q_{n-1} - p_{n-1}|$. □

Definition 8.4. *Fractions of the form* $\dfrac{p_{n,r}}{q_{n,r}} = \dfrac{r p_{n+1} + p_n}{r q_{n+1} + q_n}$, $r = 1, \dots, a_{n+2} - 1$, $n \geq -1$, *are called* secondary convergents *(or* mediating fractions*) of the continued fraction* $[a_0, a_1, \dots]$.

Let us note that $\dfrac{p_{n,0}}{q_{n,0}} = \dfrac{p_n}{q_n}$, $\dfrac{p_{n,a_{n+2}}}{q_{n,a_{n+2}}} = \dfrac{p_{n+2}}{q_{n+2}}$.

Lemma 8.30. *For n even,*

$$\frac{p_n}{q_n} < \cdots < \frac{p_{n,r}}{q_{n,r}} < \frac{p_{n,r+1}}{q_{n,r+1}} < \cdots < \frac{p_{n+2}}{q_{n+2}},$$

while for n odd,

$$\frac{p_n}{q_n} > \cdots > \frac{p_{n,r}}{q_{n,r}} > \frac{p_{n,r+1}}{q_{n,r+1}} > \cdots > \frac{p_{n+2}}{q_{n+2}}.$$

Furthermore, for each positive integer n,

$$q_{n,r+1}p_{n,r} - p_{n,r+1}q_{n,r} = (-1)^{n+1}. \tag{8.19}$$

Proof: It is sufficient to prove formula (8.19). We have

$$\begin{aligned} &q_{n,r+1}p_{n,r} - p_{n,r+1}q_{n,r} \\ &\quad = ((r+1)q_{n+1} + q_n)(rp_{n+1} + p_n) - ((r+1)p_{n+1} + p_n)(rq_{n+1} + q_n) \\ &\quad = q_{n+1}p_n - p_{n+1}q_n = (-1)^{n+1}. \end{aligned}$$ □

We say that a rational number $\frac{a}{b}$, $b > 0$, is a *good approximation* of an irrational number α if

$$\left|\alpha - \frac{a}{b}\right| = \min\left\{\left|\alpha - \frac{x}{y}\right| \,:\, x, y \in \mathbb{Z},\, 0 < y \le b\right\}.$$

Theorem 8.31. *Any good approximation of α is either a convergent or a secondary convergent of α.*

Proof: Let $\frac{a}{b}$ be a good approximation of α which is neither a convergent nor secondary convergent of α. Without loss of generality, we can assume that $\frac{a}{b} > \alpha$. Then there are consecutive (ordinary or secondary) convergents $\frac{P}{Q}$ and $\frac{P'}{Q'}$ of α such that

$$\alpha < \frac{P}{Q} < \frac{a}{b} < \frac{P'}{Q'} \quad \text{and} \quad P'Q - PQ' = 1.$$

Now,

$$\frac{1}{Q'b} \le \frac{P'}{Q'} - \frac{a}{b} < \frac{P'}{Q'} - \frac{P}{Q} = \frac{1}{Q'Q}.$$

Thus, we obtain $Q < b$ and $\left|\alpha - \frac{P}{Q}\right| < \left|\alpha - \frac{a}{b}\right|$, a contradiction. □

Example 8.4. *Let us show that not every secondary convergent is a good approximation.*

Solution: Let $\alpha = [1, 2, 2, 2, \ldots]$. Then $\frac{1}{\alpha-1} = \alpha + 1$, so $\alpha = \sqrt{2}$. The convergents of α are: 1, $\frac{3}{2}$, $\frac{7}{5}$, $\frac{17}{12}, \ldots$, and the secondary convergents are: $\frac{4}{3}$, $\frac{10}{7}$, $\frac{24}{17}, \ldots$ However, $\left|\sqrt{2} - \frac{7}{5}\right| \approx 0.0142$ and $\left|\sqrt{2} - \frac{10}{7}\right| \approx 0.0144$, so $\frac{10}{7}$ is not a good approximation of $\sqrt{2}$. ♢

Definition 8.5. *We say that an irrational number α is* badly approximable *if there is a constant $c = c(\alpha) > 0$ such that*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}$$

for every rational number $\frac{p}{q}$. (From Hurwitz's theorem, it follows that the constant c has to satisfy $0 < c < \frac{1}{\sqrt{5}}$.)

Theorem 8.32. *An irrational number α is badly approximable if and only if the partial quotients in its simple continued fraction expansion are bounded.*

Proof: From Theorem 8.24 and Lemma 8.18, it follows that

$$\begin{aligned}\left|\alpha - \frac{p_n}{q_n}\right| &= \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})} \\ &= \frac{1}{q_n^2([a_{n+1}, a_{n+2}, \ldots] + [0, a_n, a_{n-1}, \ldots, a_1])}, \end{aligned} \tag{8.20}$$

so

$$\frac{1}{q_n^2(a_{n+1} + 2)} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2 a_{n+1}}. \tag{8.21}$$

If $\frac{p}{q}$ is not a convergent of α, then, by Theorem 8.26, $\left|\alpha - \frac{p}{q}\right| > \frac{1}{2q^2}$. If partial quotients of α are bounded, i.e. if there is $K > 0$ such that $a_n \leq K$ for each $n \geq 0$, then

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{q_n^2(K + 2)}.$$

Thus, for every rational number $\frac{p}{q}$, we have $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}$, where

$$c = \min\left(\frac{1}{K+2}, \frac{1}{2}\right) = \frac{1}{K+2},$$

which means that α is badly approximable.

Conversely, suppose that α is badly approximable. Then there is $c > 0$ such that $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}$ for every rational number $\frac{p}{q}$. Now, from (8.21), it follows that $a_{n+1} < \frac{1}{c}$ for $n \geq 0$, which means that the partial quotients of α are bounded. □

Corollary 8.33. *There are uncountably many badly approximable real numbers and uncountably many real numbers which are not badly approximable.*

Proof: By Theorem 8.32, all real numbers of the form $\alpha = [a_0, a_1, \ldots]$, where $a_n \in \{1, 2\}$ for $n \geq 0$, are badly approximable, and there are uncountably many such numbers.

All real numbers $\alpha = [a_0, a_1, \ldots]$, where $a_n = n + b_n$, $b_n \in \{0, 1\}$ for $n \geq 0$, are not badly approximable, and there are uncountably many such numbers. □

8.5 Equivalent numbers

Definition 8.6. *We say that irrational numbers α and γ are* equivalent *if there are integers a, b, c, d such that $ad - bc = \pm 1$ and*

$$\gamma = \frac{a\alpha + b}{c\alpha + d}\,.$$

It is easily verified that this is indeed an equivalence relation. The notation is $\alpha \cong \gamma$.

Theorem 8.34 (Serret, 1878)**.** *Let*

$$\alpha = [a_0, a_1, a_2, \ldots] \quad \textit{and} \quad \gamma = [c_0, c_1, c_2, \ldots]$$

be irrational numbers. Then α and γ are equivalent if and only if there are integers k and l such that $a_{k+n} = c_{l+n}$ for all $n \geq 0$.

Lemma 8.35. *Let a, b, c, d be integers and*

$$\gamma = \frac{a\alpha + b}{c\alpha + d}, \quad ad - bc = \pm 1, \quad \alpha > 1, \quad c > d > 0.$$

Then $\frac{b}{d}$ and $\frac{a}{c}$ are two consecutive convergents of γ, say $\frac{p_{n-2}}{q_{n-2}}$ and $\frac{p_{n-1}}{q_{n-1}}$, and $\alpha = \gamma_n$.

Proof: Let us express $\frac{a}{c}$ as a finite simple continued fraction

$$\frac{a}{c} = [a_0, a_1, \ldots, a_{n-1}] = \frac{p_{n-1}}{q_{n-1}}.$$

Since a and c are relatively prime, we have $a = p_{n-1}$, $c = q_{n-1}$. Choose n such that

$$p_{n-1}q_{n-2} - q_{n-1}p_{n-2} = \varepsilon,$$