Diophantine approximation over the real line

1 "Good" approximants

The main goal of classical Diophantine approximation is to estimate the number of *"good" approximants* of the type $\frac{r}{s} \in \mathbb{Q}$, where r and s are coprime integers[1], of a given number $\alpha \in \mathbb{R}$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$, it is obviously possible to choose $r, s \in \mathbb{Z}$ in a way that the error term $|\alpha - \frac{r}{s}|$ is arbitrarily small, therefore we have to explain what it means for an approximant to be "good" in this theory. First of all we observe that the size of the error $|\alpha - \frac{r}{s}|$ can be controlled by the denominator s in the following way: choose any integer s, then the set $\frac{1}{|s|}\mathbb{Z}$ subdivides the real line into consecutive intervals of length $\frac{1}{|s|}$. The real number α is contained in one of such intervals that we denote by I_α, so the distance between α and the closest extremum of I_α is at most $\frac{1}{2|s|}$. This reasoning shows that for any choice of s we can always find an approximant $\frac{r}{s}$ such that $|\alpha - \frac{r}{s}| \leq \frac{1}{2|s|} < \frac{1}{|s|}$.

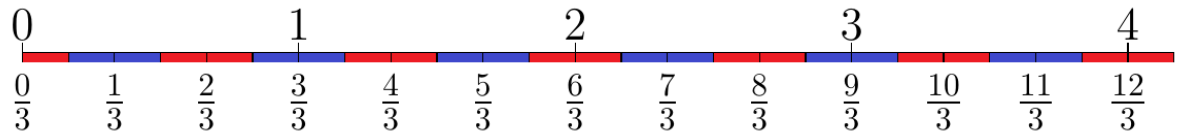

Figure 1: Partition of the real line by $\frac{1}{3}\mathbb{Z}$.

Notice that in the above naive (and non-effective) process, the error term is bounded by a linear expression in $|s|^{-1}$. Roughly speaking a "good" approximant of α will be a rational that improves such a trivial error/denominator relation and hence satisfies the fundamental inequality:

$$\left|\alpha - \frac{r}{s}\right| < |s|^{-t} \tag{1}$$

with $t \in \mathbb{R}_{>1}$. Clearly the value of exponent t tells us how good is the rational approximation, in fact a big value of t means that we are able to shrink the error term by using a relatively small denominator (i.e. a simpler number). For instance π can be approximated by the value $\frac{22}{7}$ and notice that $\frac{22}{7} - \pi < 7^{-3}$, so we are in presence of a "good" approximant. The fundamental question of the whole theory is the following: is the existence of good approximants of α just a result of chance or it depends on the nature of α? Consider for instance the case of π, is $\frac{22}{7}$ just a "lucky" approximant? Intuitively, if for a fixed positive real number t Equation (1) has *infinitely many* solutions $\frac{r}{s} \in \mathbb{Q}$, this is a sign that the approximation of α with exponent t is not just a matter of luck. We will see that the algebraic properties (in terms of Galois theory) of α heavily control the quality of the rational approximations of α i.e. the metric properties of rationals around α.

Moreover we want to stress that the theory of Diophantine approximation is deeply connected to the problem of determining the finiteness for the solutions of Diophantine equations.

[1] Classically a rational approximant is denoted with the symbol $\frac{p}{q}$ but here we adopt a different choice of letters since we want to keep p and q for prime numbers

2 Approximation exponent

An intrinsic measure of the "approximability" of a real number α is formalised in the following definition:

Definition 2.1. Let $\alpha \in \mathbb{R}$ and put:

$$T_\alpha := \left\{ t \in \mathbb{R} \colon \exists \text{ infinitely many coprime couples } (r,s) \in \mathbb{Z}^2 \text{ such that } 0 < \left| \alpha - \frac{r}{s} \right| < |s|^{-t} \right\} .$$

The *approximation exponent* of $\alpha \in \mathbb{R}$ is:

$$\tau(\alpha) := \sup T_\alpha .$$

Notice that $\tau(\alpha)$ may as well be $+\infty$, and this case will be explained soon. But assume for a moment that $\tau(\alpha) \in \mathbb{R}$, then Definition 2.1 says that for any $\varepsilon > 0$ the real number α has infinitely many rational approximations that satisfy Equation (1) with an exponent t strictly bigger than $\tau(\alpha) - \varepsilon$.

Proposition 2.2. *Fix $\alpha \in \mathbb{R}$ and $C \in \mathbb{R}$, then the following statements are equivalent:*

(*i*) $\tau(\alpha) \leq C$.

(*ii*) *For any $\varepsilon > 0$ the inequality*

$$0 < \left| \alpha - \frac{r}{s} \right| < |s|^{-C-\varepsilon} \tag{2}$$

is satisfied by at most finitely many distinct couples $(r,s) \in \mathbb{Z}^2$ of coprime integers.

(*iii*) *For all $\varepsilon > 0$ there exists $\delta := \delta(\alpha, \varepsilon) \in \mathbb{R}$ such that*

$$\left| \alpha - \frac{r}{s} \right| \geq \frac{\delta}{|s|^{C+\varepsilon}}$$

for every couple $(r,s) \in \mathbb{Z}^2$ of coprime integers such that $\alpha \neq \frac{r}{s}$.

Proof. (*i*) and (*ii*) are equivalent essentially by definition. Let's show by contradiction that (*iii*) implies (*ii*): assume that there exists ε_0 such that

$$0 < \left| \alpha - \frac{r}{s} \right| < |s|^{-C-\varepsilon_0}$$

has infinitely many solutions. Then we can apply (*iii*) with $\varepsilon = \frac{\varepsilon_0}{2}$ and obtain that there are infinitely many coprime couples (r,s) satisfying:

$$\frac{\delta}{|s|^{C+\frac{\varepsilon_0}{2}}} \leq \left| \alpha - \frac{r}{s} \right| < |s|^{-C-\varepsilon_0} .$$

This implies that $\delta \leq |s|^{-\frac{\varepsilon_0}{2}}$ for infinitely many s, Which means $\delta = 0$. This is a contradiction. Let's now show that (*ii*) implies (*iii*). Let $(r_1, s_1), \ldots, (r_k, s_k)$ be all the distinct solutions of Equation (2). Then consider

$$m = m(\alpha, \varepsilon) = \min_{j=1,\ldots,k} \left| \alpha - \frac{r_j}{s_j} \right| .$$

Now it is enough to choose any $\delta = \delta(\alpha, \varepsilon) \in]0, 1]$ such that $\frac{\delta}{|s|^{C+\varepsilon}} \leq m$.

□

The naive argument explained in the introduction of this chapter about partitioning the real line into consecutive intervals of length $|s|^{-1}$ says that $1 \in T_\alpha$ for any $\alpha \in \mathbb{R}$. Therefore $\tau(\alpha) \geq 1$ for any $\alpha \in \mathbb{R}$. As one can expect, rational numbers are badly approximable by rationals:

Proposition 2.3. *If $\alpha \in \mathbb{Q}$ then $\tau(\alpha) = 1$.*

Proof. We want to prove that if $\alpha \in \mathbb{Z}$ then $\tau(\alpha) \leq 1$ so it is enough to show that for any $\varepsilon > 0$ the coprime couples $(r,s) \in \mathbb{Z}^2$ satisfying:

$$0 < \left| \alpha - \frac{r}{s} \right| < |s|^{-1-\varepsilon} \tag{3}$$

are finitely many. We can assume that $\left|\alpha - \frac{r}{s}\right| < 1$ because otherwise the inequality is not satisfied. In other words we are in the following situation

$$s(\alpha - 1) < r < s(\alpha + 1) \tag{4}$$

Let's write $\alpha = \frac{a}{b}$, then since $\frac{a}{b} \neq \frac{r}{s}$ we can write:

$$\left|\alpha - \frac{r}{s}\right| = \left|\frac{a}{b} - \frac{r}{s}\right| = \frac{|as - rb|}{|bs|} \geq \frac{1}{|b||s|} \tag{5}$$

We point out that the last inequality of Equation (5) follows from the fact that $|as - rb|$ is a strictly positive integer, so it must be at least 1. By comparing Equation (3) with Equation (5) we find $|s| < |b|^{\frac{1}{\varepsilon}}$. This means that there are finitely many solutions for the denominators s. Moreover by Equation (4) for any such denominator we have only finitely possibilities for the numerators r. □

The general study of $\tau(\alpha)$ for $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ is very complicated since it turns out that this value depends on the nature of α. We start with the study some classical bounds for $\tau(\alpha)$.

Lemma 2.4 (Dirichlet, 1840)**.** *Let $\alpha \in \mathbb{R}$ and let $Q \in \mathbb{N}_{>0}$. Then there exists two coprime integers r, s with $0 < s \leq Q$ such that*

$$\left|\alpha - \frac{r}{s}\right| \leq \frac{1}{s(Q+1)}$$

Proof. We find two integers r and s, not necessarily coprime, that satisfy the lemma; one clearly gets claim after simplifying the common factors.

For any number $x \in \mathbb{R}$ we denote by $\{x\}$ the fractional part of x, i.e. $\{x\} := x - \lfloor x \rfloor$. Consider the $Q+1$ numbers $0, \{\alpha\}, \{2\alpha\}, \ldots, \{Q\alpha\} \in [0,1[$ and moreover divide $[0,1[$ into $Q+1$ disjoint intervals $I_j = \left[\frac{j}{Q+1}, \frac{j+1}{Q+1}\right[$ for $j = 0, \ldots, Q$. At this point one of the following mutually exclusive conditions is verified:

(*i*) Any interval I_j contains exactly one number $\{k\alpha\}$ for $j, k = 0, \ldots Q$, so in particular there exists an integer $0 < s \leq Q$ such that

$$\frac{Q}{Q+1} \leq \{s\alpha\} < 1 \tag{6}$$

which is equivalent to

$$-1 < \lfloor s\alpha \rfloor - s\alpha \leq -\frac{Q}{Q+1}$$

By adding 1 we get

$$0 < 1 + \lfloor s\alpha \rfloor - s\alpha \leq \frac{1}{Q+1}$$

which implies the thesis if we put $r := 1 + \lfloor s\alpha \rfloor$.

(*ii*) There exist two integers a, b satisfying $0 \leq a < b \leq Q$ and $|\{b\alpha\} - \{a\alpha\}| < \frac{1}{Q+1}$. But the latter inequality is equivalent to

$$|(b-a)\alpha - (\lfloor b\alpha \rfloor - \lfloor a\alpha \rfloor)| < \frac{1}{Q+1}$$

Which the claim we wanted for $s := b - a$ and $r := \lfloor b\alpha \rfloor - \lfloor a\alpha \rfloor$. □

Remark 2.5. Note that the proof of Dirichlet lemma is nothing more than a clever application of the pigeonhole principle.

Proposition 2.6. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then $2 \in T_\alpha$. So in particular $\tau(\alpha) \geq 2$.*

Proof. Assume by contradiction that all the (distinct) solutions of the inequality

$$0 < \left|\alpha - \frac{r}{s}\right| < |s|^{-2} \tag{7}$$

are the coprime couples $(r_1, s_1), \ldots, (r_n, s_n)$. Put $\delta := \min_i |s_i\alpha - r_i| > 0$. Choose any integer $Q > \frac{1}{\delta}$, then by Lemma 2.4 we can find two coprime integers r, s with $0 < s \leq Q$ such that:

$$0 < \left|\alpha - \frac{r}{s}\right| \leq \frac{1}{s(Q+1)} < \frac{1}{sQ} \leq \frac{1}{s^2}\,.$$

Notice that $0 < \left|\alpha - \frac{r}{s}\right|$ since $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. We have found a solution (r, s) of Equation (7) that also satisfies $|s\alpha - r| < \frac{1}{Q} < \delta$. But by the definition of δ this implies that (r, s) is different from any of the (r_i, s_i). □

We shall now see how the approximation exponent can be bounded from above for algebraic numbers.

Theorem 2.7 (Liouville, 1844)**.** *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree d over $\mathbb{Q}$, then there exists a real number $c := c(\alpha) > 0$ such that for any $r, s \in \mathbb{Z}$ with $s > 0$ and $\alpha \neq \frac{r}{s}$ it holds that*

$$\left|\alpha - \frac{r}{s}\right| \geq \frac{c}{s^d}$$

Proof. If $\left|\alpha - \frac{r}{s}\right| > 1$ then the theorem holds for $c = 1$, therefore from now on we can safely assume that $\left|\alpha - \frac{r}{s}\right| \leq 1$. Let $f(X) = a_0 + a_1 X + \ldots + a_d X^d \in \mathbb{Z}[X]$ be a minimal polynomial of α. Since $f(X)$ is irreducible over $\mathbb{Q}$ it cannot have rational roots, in particular $f\left(\frac{r}{s}\right) \neq 0$. Then:

$$\left|f\left(\frac{r}{s}\right)\right| = \frac{\left|a_0 s^d + a_1 r s^{d-1} + \ldots + a_d r^d\right|}{s^d} \geq \frac{1}{s^d} \tag{8}$$

where the last inequality follows from the fact that the numerator is a strictly positive integer. By the mean value theorem we have that:

$$\left|f\left(\frac{r}{s}\right)\right| = \left|f(\alpha) - f\left(\frac{r}{s}\right)\right| = |f'(\beta)|\left|\alpha - \frac{r}{s}\right|, \quad \text{for } \beta \in \mathbb{R} \text{ such that } |\alpha - \beta| < \left|\alpha - \frac{r}{s}\right| \leq 1$$

But clearly $|f'(\beta)|$ is bounded from above by the number

$$M := \max\{|f'(x)| \colon x \in [\alpha - 1, \alpha + 1]\}$$

so by Equation (8) we obtain

$$M\left|\alpha - \frac{r}{s}\right| \geq \left|f\left(\frac{r}{s}\right)\right| \geq \frac{1}{s^d}$$

Therefore the theorem is proved after setting $c := \min\{1, \frac{1}{M}\}$. □

Remark 2.8. The whole proof of Liouville's theorem is based on the following very simple fact: since f is a polynomial with coefficients in $\mathbb{Z}$, when $\frac{r}{s}$ is close to α (but not equal) then $f\left(\frac{r}{s}\right)$ cannot be "too close" to $0 = f(\alpha)$. Indeed the distance between $f\left(\frac{r}{s}\right)$ and 0 is bounded from below by $\frac{1}{s^d}$.

Proposition 2.9. *Let $\alpha \in \mathbb{R}$ be an algebraic number of degree d over $\mathbb{Q}$, then $\tau(\alpha) \leq d$.*

Proof. It follows immediately from Proposition 2.2 if we choose $\delta(\alpha, \varepsilon)$ to be the constant $c(\alpha)$ of Liouville's theorem. □

Thanks to Liouville's theorem it is possible to explicitly construct transcendental numbers, in fact it is enough to find some $\alpha \in \mathbb{R}$ such that $\tau(\alpha) = +\infty$. Such a problem is discussed below:

Definition 2.10. A *Liouville number* is a real number α such that for any $m \in \mathbb{N}_{>0}$ there exists a pair of coprime integers $(r, s) \in \mathbb{Z}^2$ with $s > 1$ such that:

$$\left|\alpha - \frac{r}{s}\right| < s^{-m} \tag{9}$$

It is immediate to see that a Liouville number cannot be rational, because if it was $\alpha = \frac{a}{b}$ then for any approximant we would have a lower bound like in Equation (5) that compared with Equation (9) gives $s < |b|^{m-1}$ for any $m \in \mathbb{N}_{>0}$, so in particular $s < 1$, i.e. a contradiction. We now show that Liouviulle numbers are exactly those reals having infinite approximation exponent.

Proposition 2.11. *$\alpha \in \mathbb{R}$ is a Liouville number if and only if $\tau(\alpha) = +\infty$.*

Proof. If $\tau(\alpha) = +\infty$ then obviously α is a Lioville number. Viceversa assume by contradiction that α is a Liouville number such that $\tau(\alpha) < +\infty$ and consider $\sigma := \lceil \tau(\alpha) \rceil + 1$. The inequality

$$\left|\alpha - \frac{r}{s}\right| < |s|^{-\sigma} \tag{10}$$

has finitely many coprime solutions (r, s) and the set of solutions is actually nonempty since

$$\left|\alpha - \frac{\lfloor \alpha \rfloor}{1}\right| < 1 = 1^{-\sigma}.$$

Therefore, amongst all solutions of Equation (10) we consider the one with biggest denominator s. On the other hand, since α is a Liouville number we have a sequence of coprime couples $\{(r_n, s_n)\}$ such that

$$\left|\alpha - \frac{r_n}{s_n}\right| < \frac{1}{s_n^n}$$

In the next step we want to show that $s_n \to +\infty$. Assume by contradiction that $\{s_n\}$ is bounded by $M > 0$, then

$$\left|M!\,\alpha - \frac{M!\,r_n}{s_n}\right| \geq \min\{M!\,\alpha - \lfloor M!\,\alpha\rfloor, \lceil M!\,\alpha\rceil - M!\,\alpha\} > 0$$

since $\frac{M!\,r_n}{s_n} \in \mathbb{Z}$ (note that s_n is a factor of $M!$ because $s_n \leq M$) and $\alpha \notin \mathbb{Z}$. But on the other hand since $s > 1$:

$$0 \leq \lim_{n\to+\infty} \frac{1}{s_n^n} \leq \lim_{n\to+\infty} \frac{1}{2^n} = 0\,.$$

We get the contradiction when we take the limit for $n \to +\infty$ of $\left|M!\,\alpha - \frac{M!\,r_n}{s_n}\right|$. Hence, there exists some $N > \sigma$ such that $s_N > s$. But

$$\left|\xi - \frac{r_N}{s_N}\right| < \frac{1}{s_N^N} < \frac{1}{s^N} < \frac{1}{s^\sigma}$$

Contradicting the maximality of the denominator s. □

It is relatively easy to construct Liouville numbers. Fix an integer $b \geq 2$ and a sequence of integers $\{a_k\}_{k\geq 1}$ with $a_k \in \{0, \ldots, b-1\}$ and $a_k \neq 0$ for infinitely many k. We are going to show that the number

$$\ell = \sum_{k=1}^{\infty} \frac{a_k}{b^{k!}}$$

is a Liouville number. First of all notice that we have the following representation for ℓ in base b

$$\ell = 0.a_1a_2000a_3...$$

where the $k!$-th term of the expansion is a_k, and the remaining terms are 0. Since the sequence $\{a_k\}$ is not eventually 0, it follows that ℓ is not rational. Moreover for any $m \in \mathbb{N}_{>0}$ define $s_m := b^{m!}$ and $r_m := s_m \sum_{k=1}^{m} \frac{a_k}{b^{k!}}$, then

$$0 < \left|\ell - \frac{r_n}{s_n}\right| < \left|\ell - \sum_{k=1}^{m} \frac{a_k}{b^{k!}}\right| = \sum_{m+1}^{\infty} \frac{a_k}{b^{(k!)}} \leq \sum_{k=m+1}^{\infty} \frac{b-1}{b^{k!}} < \sum_{k=(m+1)!}^{\infty} \frac{b-1}{b^k} = \frac{b-1}{b^{(m+1)!}} \sum_{k=0}^{\infty} \frac{1}{b^k} =$$

$$= \frac{b-1}{b^{(m+1)!}} \frac{b}{b-1} < \frac{b^{m!}}{b^{(m+1)!}} = \frac{1}{b^{(m+1)!-m!}} = \frac{1}{b^{(m!)m}} = \frac{1}{s_m^m}$$

From the above described construction it is also easy to deduce that the set of Liouville numbers is uncountable.

The improvement of the upper bound of Proposition 2.9 has been object of a massive quest for several years. Here a list of the successive sharpenings:

- Thue: $\tau(\alpha) \leq 1 + \frac{d}{2}$
- Siegel: $\tau(\alpha) \leq 2\sqrt{d}$
- Gelfond-Dyson: $\tau(\alpha) \leq \sqrt{2d}$

The definitive answer for the approximation exponent of an algebraic number was given in 1955 by Roth, who was awarded the Fields medal because of it.

Theorem 2.12 (Roth)**.** *Let $\alpha \in \mathbb{R}$ an algebraic number, then $\tau(\alpha) = 2$*

Proof. See [Rot55]. □

An obviously equivalent, but more useful, formulation of Roth's theorem is the following:

Theorem 2.13. *Let $\alpha \in \mathbb{R}$ be an algebraic number and let $\varepsilon > 0$ be a real number. Then there exists a real constant $C(\alpha, \varepsilon) > 0$ such that for every pair of coprime integers (r, s) with $s > C(\alpha, \varepsilon)$, it holds that:*

$$\left|\alpha - \frac{r}{s}\right| > s^{-2-\varepsilon}$$

The following table summarizes the properties of the approximation exponent that we have so far unveiled. It is now clear why the approximation exponent is often called *irrationality measure*

Type of α	**Appr. exp.**
Rational	$\tau(\alpha) = 1$
Algebraic	$\tau(\alpha) = 2$
Transcendental	$\tau(\alpha) \geq 2$
Liouville	$\tau(\alpha) = +\infty$

What happens to the irrationality measure of transcendental numbers can be quite wild, but in [Bug08, Theorem 2] it is shown that for any $\lambda \in]2, +\infty[$ there exists a real number β such that $\tau(\beta) = \lambda$. Moreover, from a set theoretic point of view it is not difficult to show that the subset of reals made of all the numbers having approximation exponent > 2 has Lebeasgue measure equal to 0 (this result follows from Cantelli's lemma, see for instance [Bug12, Theorem E.3]). The exact value of the approximation exponent of some specific transcendental numbers is an active area of research; for instance it is well known that $\tau(e) = 2$ whereas for π the most accurate currently available bound is $\tau(\pi) \leq 7,103205334137\ldots$ (see [ZZ20]).

Remark 2.14. In this brief section we have studied Diophantine approximations based on Equation (1), i.e. we compared the error with the powers of the approximants' denominators. One can ask similar questions but using more general functions $\Psi(s)$ (of the denominators), instead of $\Psi(s) = s^{-t}$ (see for instance [Bug04]).

3 A baby example: Pell's equation over $\mathbb{Q}$

Diophantine approximation is deeply linked to the problem of finding solution of Diophantine equations. Here we highlight this relationship in the nontrivial case of Pell's equation:

$$X^2 - dY^2 = 1\,, \quad \text{for } d \in \mathbb{N}_{>0}\,. \tag{11}$$

Note that if d is a perfect square, i.e. $d = m^2$ for $m \in \mathbb{N}_{>0}$, then the solutions $(x, y) \in \mathbb{Z}^2$ of the equation $1 = X^2 - dY^2 = (X + mY)(X - mY)$ are obviously just $(\pm 1, 0)$. The couples $(\pm 1, 0)$ are in any case solutions of Equation (11) for any $d \in \mathbb{N}_{>0}$, and they will be called *trivial solutions (of the Pell's equation)*. So, assume that d is not a perfect square; first of all it is useful to see Equation (11) in the field $\mathbb{Q}(\sqrt{d})$, so that we can write it as

$$1 = \left(X + Y\sqrt{d}\right)\left(X - Y\sqrt{d}\right)\,. \tag{12}$$

If a non-trivial solution exists, then there exists also a solution with positive components; therefore assume that (x, y) is a solution with $x, y > 0$. Then $x = \sqrt{1 + dy^2} > y\sqrt{d}$ and by Equation (12) we obtain

$$\left|x - y\sqrt{d}\right| = \frac{1}{x + y\sqrt{d}} < \frac{1}{2y\sqrt{d}}\,,$$

namely

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2\sqrt{d}} < \frac{1}{y^2} \tag{13}$$

In other words, a non-trivial solution of Pell's equation (seen as a rational number) turns out to be a good approximant of $\sqrt{d}$. The above argument shows how to get good approximants from some solutions of a Diophantine equation, but the process can be reversed (in a non-effective way). In fact, in the next theorem we will see that the existence of infinitely many good approximants of $\sqrt{d}$ plays in a crucial role in the proof that Pell's equation has infinitely many integral solutions:

Theorem 3.1. *If $d \in \mathbb{N}_{>0}$ is not a perfect square then Equation (11) has infinitely many solutions $(x, y) \in \mathbb{Z}^2$.*

Proof. By Proposition 2.6 there are infinitely many rationals $\frac{x}{y}$ with $y > 0$ that satisfy Equation (13). For them we have $\left|x - y\sqrt{d}\right| < y^{-1} < 1$, so $x < 1 + y\sqrt{d}$. From these two inequalities we get:

$$\left|x^2 - dy^2\right| < \frac{\left|x + y\sqrt{d}\right|}{y} < \frac{2y\sqrt{d} + 1}{y} \leq 2\sqrt{d} + 1 \tag{14}$$

Since d is not a perfect square $x^2 - dy^2$ is a nonzero integer, therefore from Equation (14) and the pigeonhole principle we conclude that there is a nonzero integer $M \in]-2\sqrt{d} - 1, 2\sqrt{d} + 1[$ such that the equation

$$X^2 - dY^2 = M$$

has infinitely many solutions $(x, y) \in \mathbb{Z}^2$ with $y > 0$. So far we have proved that a modification of Pell's equation (with M instead of 1) has infinitely many integral solutions.

$(\mathbb{Z}/M\mathbb{Z})^2$ is a finite, so again by the pigeonhole principle there exist two elements $x_i + y_i\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ for $i = 1, 2$, such that the following conditions are all verified:

$$\begin{cases} y_1 \neq y_2\,, \\ x_i, y_i > 0\,, \\ (x_i + y_i\sqrt{d})(x_i - y_i\sqrt{d}) = M\,, \\ x_1 \equiv x_2 \pmod{M}\,, \\ y_1 \equiv y_2 \pmod{M}\,. \end{cases} \tag{15}$$

We can also assume that $\frac{x_1}{y_1} \neq \frac{x_2}{y_2}$ otherwise from the identity $M = X^2 - dY^2 = Y^2\left(\frac{X^2}{Y^2} - d\right)$ we would get $y_1 = y_2$. Let's now write

$$(x_1 + y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = A + B\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$$

with $A = x_1x_2 - dy_1y_2$, $B = x_2y_1 - x_1y_2$. By the modular conditions of Equation (15) we get $A \equiv 0 \pmod{M}$ and $B \equiv 0 \pmod{M}$, i.e. $A = MA_1$ and $B = MB_1$ for $A_1, B_1 \in \mathbb{Z}$. Moreover

$$A_1^2 - dB_1^2 = \frac{1}{M^2}\left(A^2 - dB^2\right) = 1\,,$$

so (A_1, B_1) is an integral solution of Pell's equation. It is actually a nontrivial solution, in fact if $B' = 0$, then $B = 0$ i.e. $\frac{x_1}{y_1} = \frac{x_2}{y_2}$.

So far we proved that Pell's equation admits a nontrivial integral solution; by simplicity let's denote it by (x, y). We now show that we can modify such solution to get infinitely many (distinct) integral solutions (x_n, y_n) for $n \in \mathbb{N}_{>0}$. Let's define x_n and y_n via the following formula:

$$x_n + y_n\sqrt{d} = \left(x + y\sqrt{d}\right)^n\,.$$

After applying the automorphism of $\mathbb{Z}[\sqrt{d}]$ induced by $\sqrt{d} \mapsto -\sqrt{d}$ we get also

$$x_n - y_n\sqrt{d} = \left(x - y\sqrt{d}\right)^n\,.$$

Therefore:

$$x_n^2 - dy_n^2 = \left(x + y\sqrt{d}\right)^n\left(x - y\sqrt{d}\right)^n = \left(x^2 - dy^2\right)^n = 1$$

The couples (x_n, y_n) are pairwise distinct, because otherwise $x + y\sqrt{d}$ would be a root of unity in $\mathbb{Z}[\sqrt{d}]$ i.e. $x + y\sqrt{d} = \pm 1$. But this is impossible since (x, y) is a nontrivial solution of Pell's equation. □

Remark 3.2. The proof of Theorem 3.1 is divided in three steps: first one uses the fact that $2 \in T_{\sqrt{d}}$ and the pigeon principle to show that the modified Pell's equation $X^2 - dY^2 = M$ has infinitely many integral solutions. Then, again by the pigeonhole principle one shows the existence of an integral nontrivial solution of Pell's equation. Finally, from such solution one generates a sequence of distinct integral solutions.

Remark 3.3. We didn't provide an explicit description for the integral solutions of Pell's equation, but this is actually well known for any number field K. Let $d \in O_K - \{0\}$, then the set of solutions $(x, y) \in O_K^2$ of the equation $X^2 - dY^2 = 1$ is completely described in [Sch06].

References

[Bug04] Y. Bugeaud. *Approximation by algebraic numbers*, volume 160 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2004.

[Bug08] Y. Bugeaud. Diophantine approximation and Cantor sets. *Math. Ann.*, 341(3):677–684, 2008.

[Bug12] Y. Bugeaud. *Distribution modulo one and Diophantine approximation*, volume 193 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2012.

[Rot55] K. F. Roth. Rational approximations to algebraic numbers. *Matematika*, 2(3), 1955.

[Sch06] W. A. Schmid. On the set of integral solutions of the Pell equation in number fields. *Aequationes Math.*, 71(1-2):109–114, 2006.

[ZZ20] D. Zeilberger and W. Zudilin. The irrationality measure of π is at most 7.103205334137.... *Mosc. J. Comb. Number Theory*, 9(4):407–419, 2020.