# Introduction

Diophantine approximation may be roughly described as the branch of number theory concerned with approximations by rational numbers; or rather, this constituted the original motivation.

That such questions have attracted continued attention is undoubtedly substantially due to their relevance for another, more ancient, topic: the theory of Diophantine equations, namely those whose solutions have to be found in integers or rationals, possibly in a finite extension of $\mathbb{Q}$. The connections between the subjects, which had already been observed by Lagrange and Legendre, were explicitly pointed out by the Norwegian A. Thue; in 1909 he proved a finiteness theorem for Diophantine equations which for the first time included whole families of equations, of arbitrarily large degree. At that time they could be treated only occasionally, and merely with *ad hoc* methods, albeit ingenious ones. Thue's theorem relied solely on a result which limited the accuracy of the rational approximations to algebraic numbers (a previous result had been obtained by Liouville, but it was too weak for applications to equations).

Thue's method was extended and refined by such authors as C. L. Siegel, A. O. Gelfond, and F. Dyson; in 1955 K. F. Roth proved a best-possible result in this direction. However, other related questions remained open, like the simultaneous approximations to several numbers; for them, Roth's techniques gave only partial answers. Around 1970 W. M. Schmidt combined the known methods with new ideas and resolved the whole subject, proving a multidimensional version of Roth's result, which became known as the *subspace theorem*.

Schmidt himself discovered remarkable applications to Diophantine equations generalizing in several variables those considered by Thue. Later, the theorem was extended by H.-P. Schlickewei to cover number fields and several absolute values. These versions soon suggested new applications, for instance to the so-called *S-unit equations* (which had already appeared in Siegel's work). More recently, still further applications have been found, to Diophantine equations with recurrence sequences of semi-exponential type, and also to the problem of integral points on varieties.

The present book will cover some of these results.

In Chapter 1 we shall briefly review a few classical facts, from Pell's equation to Thue's and Roth's theorems. We shall also recall some modern versions with several absolute values (after Ridout, Mahler, and Lang) and some applications.

In Chapter 2 we shall state a few versions, by Schmidt and Schlickewei, of the subspace theorem. Then we shall apply this to the treatment of the equation $x_1 + \cdots + x_n = 1$ in $S$-units $x_i$ and, in general, of $S$-unit points on algebraic varieties. Finally, as an application, we shall present a fairly simple proof of one of Schmidt's theorems on norm-form equations.

Chapter 3 will be devoted to integral points on algebraic curves and on certain varieties of higher dimension. After some definitions and examples, we shall sketch a modern version of Siegel's original proof of his celebrated theorem; then we shall present a new argument depending on the subspace theorem; here we shall also mention how this method may be extended to cover the case of certain surfaces (and more generally of varieties) with sufficiently many components at infinity. As an application, we treat the question of quadratic-integral points on algebraic curves. In this chapter we consider also the Hilbert property for the set of rational points on an algebaric variety originating from Hilbert's irreducibility theorem, and compare it with the Chevalley–Weil theorem.

Chapter 4 will concern linear recurrence sequences. After surveying a number of basic facts and the classical results on zeros, we shall concentrate on the so-called *quotient problem* (concerning the integrality of the values $u_n/v_n$) and the *dth-root problem* (concerning the equations $y^d = u_n$). A related question treated in this chapter concerns estimates of the greatest common divisor of pairs of numbers of the form $(a^n - 1, b^n - 1)$. We shall present several applications of these estimates, to seemingly unrelated fields.

Finally, the last chapter contains applications of Diophantine estimates arising from the subspace theorem to transcendental number theory.

# 1

# Diophantine Approximation and Diophantine Equations

## 1.1 The Origins

As mentioned in the introduction, Diophantine approximation stems from the study of the *good* rational approximations to a given real number. The term "Diophantine" comes from the mathematician Diophantus of Alexandria (about 250 AD) who wrote a treatise on mathematical problems corresponding to equations in which solutions in integers or rational numbers were required).[1]

Naturally, every real number admits rational approximations with arbitrarily small error; however, the really "good" ones are those whose accuracy is high *compared* with the complexity of the rational fraction. In other words, we try to approach our number by means of "simple" rational fractions; that is, ones with a "small" denominator (or numerator). The issue is that, once the target has been specified, not all denominators happen to be equally effective. For instance, using the denominator 100, we can approximate $\sqrt{2}$ at best with an accuracy of about $1/250$ (with the fraction $141/100$), while the denominator 70 yields an accuracy superior to $1/13,000$ (with the fraction $99/70$).

These questions go back to ancient times; as remarked by Tijdeman (see his paper in [EE]), the inequalities $233/71 < \pi < 22/7$ obtained by Archimedes may be considered primordial results in this direction.

However, apart from the great intrinsic interest of this topic, here we want to emphasize its applications to the theory of Diophantine equations, those to be solved in integers (of $\mathbb{Z}$) or rational numbers (in $\mathbb{Q}$ or more generally in a number field); reciprocally, Diophantine equations have often represented a source of motivations for Diophantine approximation.

We shall briefly review a few fundamental steps of this interplay, focusing later with more detail on certain aspects (see also Tijdeman's paper mentioned above).

[1] This consisted of several books, of which only a part has survived to our time.

### 1.1.1 Linear Equations

The simplest Diophantine equations, the linear ones, were considered by Euclid, who in practice answered all the most natural questions about them.

We start with the simplest case of a line passing through the origin, of equation $aX = bY$. Here $a, b$ can be supposed to be coprime integers. Owing to the uniqueness of factorization in the ring $\mathbb{Z}$ of integers, all the integral points are of the form $(x, y) = (nb, na)$, for $n \in \mathbb{Z}$.

Our second example is a line of equation $aY - bX = 1$ ($a, b > 0$ integers); it is particularly illustrative, and the general theory of linear equations boils down to this case. Euclid's algorithm shows that there exist integer solutions if and only if $a$ and $b$ are coprime.

This simple equation already embodies a principle of Diophantine approximation. In fact, for an integer solution $(p, q)$ (with $q > 0$) we have

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{1}{qb}. \tag{1.1}$$

Hence the fraction $p/q$ is remarkably close to $a/b$. In fact, if $p', q' > 0$ are any integers with $p'/q' \neq a/b$, the difference $(a/b) - (p'/q')$ has the form $d/bq'$, where $d$ $(= q'a - p'b)$ is a *non-zero* integer; therefore the absolute value $|d| \geq 1$, whence $|(a/b) - (p'/q')| \geq 1/q'b$. This shows that the integral point $(p, q)$ on our line produces a rational approximation $p/q$ for the (rational) number $a/b$ which is in a way *optimal*; for its accuracy is superior to that of any other fraction $p'/q'$ whose denominator $q'$ is $< q$ (with the obvious possible exception of the *trivial* approximation $p'/q' = a/b$).

This argument may be reversed, and the search for good rational approximations to $a/b$ leads to solutions for the above Diophantine equation. Indeed, an algorithm for finding solutions to (1.1) comes from the continued fraction for $a/b$; we review in brief the fundamental facts about this.

**Remark 1.1** (Euclid's algorithm and continued fractions) We just recall briefly and without proofs these issues. We start with Euclid's algorithm for solving $ax + by = \gcd(a, b)$ for integers $a, b$. Assuming $b > 0$, we divide $a$ by $b$, obtaining $a = q_1 b + r_1$ with $0 \leq r_1 < b$. If $r_1 > 0$ we continue as follows: $b = q_2 r_1 + r_2$, $0 \leq r_2 < r_1$ and so on, $r_i = q_{i+2} r_{i+1} + r_{i+2}$, $0 \leq r_{i+2} < r_{i+1}$ until we obtain a zero remainder, which will certainly happen sooner or later; at that point the algorithm stops. It is easy to check that the last non-zero remainder is the $\gcd(a, b)$ and, using the equations in reverse order, we easily obtain the sought solution. (The same algorithm holds in $k[X]$, for any field $k$.)

This kind of algorithm can be rephrased in terms of the *continued fraction* *expansion* of the (positive) rational number $a/b$ in the sense that we may write

$$\frac{a}{b} = a_1 + \frac{r_1}{b} = a_1 + \frac{1}{a_2 + r^2/r^1} = \cdots = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_m}}}.$$

This expansion is essentially unique (except that, if $a_m > 1$, we may replace $a_m$ by $(a_m - 1) + 1$). A solution to Euclid's equation is obtained by computing the truncated continued fraction at the penultimate term.

This algorithm works for any real number $\xi$ in the following way. We start by writing $\xi = a_1 + \theta_1$, where $a_1 = [\xi]$ is the integral part and $0 \le \theta_1 < 1$. If $\theta_1 \neq 0$ (which is certainly the case if $\xi$ is irrational), we write $\theta_1 = 1/\xi_1$ with $\xi_1 > 1$, and we continue with $\xi_1 = a_2 + \theta_2$, where $0 \le \theta_2 < 1$.

If $\xi$ is rational, the procedure ends after finitely many steps and amounts to Euclid's algorithm, as illustrated above. If $\xi$ is irrational, the procedure continues indefinitely and we write

$$\xi = a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}} = a_1 + \frac{1}{a_2+}\,\frac{1}{a_3+} = \cdots = [a_1, a_2, \ldots],$$

where the last two expressions are the customary abbreviations. The integers $a_i$ are called *partial quotients*, a terminology which is motivated by the link with Euclid's algorithm. They are all strictly positive, with the possible exception of the first one. We have written this equality meaning that the finite truncations to such infinite continued fractions converge to $\xi$, as can be proved. Actually much more is true: on defining $p_m/q_m = [a_1, a_2, \ldots, a_m]$, $q_m > 0$, as the reduced expression for the truncated continued fraction, called the *convergent* to $\xi$, we have

$$\left|\xi - \frac{p_m}{q_m}\right| < \frac{1}{q_m q_{m+1}} \le \frac{1}{a_{m+1} q_m^2}. \tag{1.2}$$

This may be re-written as $|q_m \xi - p_m| < 1/a_{m+1} q_m$. The approximations are "the best" in the sense that for every integer $q < q_{m+1}$ and every $p$ we have $|q_m \xi - p_m| \le |q\xi - p|$ with equality only for $q = q_m$, $p = p_m$. (In particular, $|\xi - p_m/q_m| < |\xi - p/q|$ for all integers $p$ and $0 < q < q_m$.) The last property essentially holds also for a rational $\xi$.

On putting $p_0 = 1, q_0 = 0$, the sequences $p_m$ and $q_m$ satisfy the recurrences

$$p_{m+2} = a_{m+2} p_{m+1} + p_m, \qquad q_{m+2} = a_{m+2} q_{m+1} + q_m,$$

which are sometimes expressed in rather convenient matrix form as

$$\begin{pmatrix} p_m & p_{m-1} \\ q_m & q_{m-1} \end{pmatrix} = \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_{m+1} & 1 \\ 1 & 0 \end{pmatrix}.$$

By induction, or taking determinants, these yield that

$$p_n q_{n+1} - p_{n+1} q_n = (-1)^n.$$

It is to be noted that, viewing $a_1, a_2, \ldots$ as independent variables, the above formula provides infinitely many polynomial parametrizations with integral coefficient for $\mathrm{SL}_2$.

As we have remarked, the continued fraction is effectively computable for every given rational number; for quadratic irrationals it has been known from as far back as Lagrange and Galois that the continued fraction is pre-periodic and conversely, that the anti-period and period are effectively computable. On the other hand, very little is known for more general classes of numbers, with a few exceptions; for instance, for no algebraic number of degree $> 2$ do we know whether the partial quotients are bounded (one would conjecture that they are not). Only for a "few" transcendental numbers do we have explicit formulae, for instance $e = [2,1,2,1,1,4,1,1,6,1,1,\ldots]$.

We refer to [C1], [L2], and [S1] for the basic theory and proofs of the stated facts.

**Exercise 1.2** Prove that the different parametrizations of $\mathrm{SL}_2$ described above cannot be obtained from one another by polynomial composition.

**Exercise 1.3** Prove that for coprime $a, b$ Euclid's algorithm leads to an integral solution $(m,n)$ of $aX + bY = 1$ after at most constant $\cdot \log \min(|a|,|b|) + 1$ steps. (Also, find a "best-possible" constant and show that it is attained with consecutive Fibonacci numbers.)

**Exercise 1.4** Prove that, if $a, b$ are coprime positive integers, for all sufficiently large integers $r$ there exists a solution of $aX + bY = r$ in non-negative integers. (Also, prove that the largest $r$ for which there are not such solutions is $(a-1)(b-1)-1$.)

**Exercise 1.5** Compute the anti-period and period of the continued fraction for $\sqrt{7}$.

**Exercise 1.6** Let $A$ be an $r \times n$ matrix with entries in $\mathbb{Z}$ and let $\mathbf{v} \in \mathbb{Z}^r$. Prove that the equation $A\mathbf{x} = \mathbf{v}$ has a solution $\mathbf{x} \in \mathbb{Z}^n$ if and only if the congruence $A\mathbf{x} \equiv \mathbf{v} \mod m$ has a solution for all positive integers $m$. (Hint: the image $A(\mathbb{Z}^n)$ is a subgroup of $\mathbb{Z}^r$. Use the theorem of elementary divisors to find a basis $\mathbf{b_i}$ of $\mathbb{Z}^r$ such that some integral multiples $\delta_i \mathbf{b_i}$ generate the subgroup ...).

### 1.1.2 Binary Quadratic Equations

Let us now consider quadratic Diophantine equations, which historically represented the next step after the linear case. Again, let us concentrate on the case of two variables, supposed to take integer values; our problem then corresponds to the search for integral points on an affine conic, which can be assumed irreducible (otherwise we fall back to the case of lines).

If the conic is an ellipse, the integral points naturally form a finite set, due to compactness.[2]

If the conic is a parabola, then easy linear substitutions (with integral coefficients together with their inverses) put its equation in the shape

$$dY = aX^2 + bX + c, \qquad a,b,c,d \in \mathbb{Z}, \qquad ad \neq 0, \tag{1.3}$$

and the search for integral points reduces to the solution of the congruence $aX^2 + bX + c \equiv 0 \pmod{d}$.

We are left with the hyperbola, the most interesting case. It turns out (as observed by Lagrange and Gauss) that the whole theory depends on the equation

$$X^2 - \Delta Y^2 = 1, \tag{1.4}$$

where $\Delta$ is a positive integer, assumed not to be a perfect square (for otherwise the factorization $X^2 - \Delta Y^2 = (X + \sqrt{\Delta}Y)(X - \sqrt{\Delta}Y)$ shows that the only integral solutions are $(\pm 1, 0)$).

This equation, which can be traced back to ancient times,[3] was explicitly proposed in the seventeenth century by P. Fermat, the famous judge who was a great mathematician as a hobby. However, Euler erroneously attributed it to J. Pell, and even today the denomination *Pell's equation* is commonly used.

It was Lagrange who first proved (for this proof see Remark 1.10(ii) below) that, *if $\Delta$ is a positive integer, not a perfect square, the equation always admits non-trivial integral solutions*, namely solutions $(p,q) \in \mathbb{Z}^2$ such that $q \neq 0$. Observe that such a solution generates an infinity of them on putting, for any integer $n \in \mathbb{Z}$, $p_n \pm q_n\sqrt{\Delta} = (p \pm q\sqrt{\Delta})^n$, or, equivalently,

$$p_n = \frac{(p+q\sqrt{\Delta})^n + (p-q\sqrt{\Delta})^n}{2}, \qquad q_n = \frac{(p+q\sqrt{\Delta})^n - (p-q\sqrt{\Delta})^n}{2\sqrt{\Delta}}.$$

In fact, one may check that the $(p_n, q_n)$ are pairwise distinct integral points satisfying $p_n^2 - \Delta q_n^2 = 1$, i.e. lying on the hyperbola defined by Pell's equation.

Lagrange's result is quite remarkable, for several reasons. For instance, it

[2] This is, however, no longer true over an arbitrary number field; in fact, over a suitable quadratic field, affine ellipses and hyperbolas become isomorphic curves.
[3] For instance it appears in Indian mathematics of the seventh century – see [W].

easily yields the structure of the invertible elements in the quadratic ring $\mathbb{Z}[\sqrt{\Delta}]$: *they form a group isomorphic to* $\mathbb{Z}/(2)\oplus\mathbb{Z}$ (a special case of a result by Dirichlet), where the pair $0\oplus 1$ is obtained just from the "minimal" non-trivial solution of Pell's equation. Moreover, as alluded to above, a solution of (1.4) is relevant also in the treatment of general quadratic equations (like e.g. $X^2-\Delta Y^2=c$).

From our point of view, the equation is linked with the "good" rational approximations for the irrational number $\sqrt{\Delta}$. In fact, for a solution $(p,q)$ in positive integers, it is easily verified that

$$\left|\sqrt{\Delta}-\frac{p}{q}\right|\leq(2\sqrt{\Delta})^{-1}\frac{1}{q^2}. \tag{1.5}$$

We see that, even forgetting the factor $(2\sqrt{\Delta})^{-1}<1$, the right-hand side is dominated by $q^{-2}$; on the other hand, a random choice for the denominator $q$, and the consequent optimization for $p$, would yield an accuracy comparable to $q^{-1}$ for the approximation to $\sqrt{\Delta}$. In particular, the error coming from a solution of Pell's equation is negligible compared with that which may arise from a fraction with a "generic" denominator of similar magnitude.

The exponent "2" assigned to $q$ on the right-hand side of (1.5) is not unique to the case of the numbers $\sqrt{\Delta}$. Actually, it comes from the *double freedom* in choosing $p,q$ and in fact every irrational number admits an infinity of rational approximations of such an accuracy. This result will be an easy consequence of the following well-known lemma, which is as simple as it is useful and elegant.

**Theorem 1.7** (Dirichlet's lemma) *Let $\xi\in\mathbb{R}$ and let $Q>0$ be a positive integer. Then there exist $p,q\in\mathbb{Z}$, such that $(p,q)=1$ and*

$$0<q\leq Q,\qquad |q\xi-p|<\frac{1}{Q+1}. \tag{1.6}$$

*Proof* For a proof, consider the sequence of $Q+1$ numbers (not necessarily distinct) $0,\{\xi\},\{2\xi\},\ldots,\{Q\xi\}\in[0,1)$, where the symbol $\{x\}$ denotes the *fractional part* of the real number $x$, i.e. $\{x\}:=x-[x]$, where $[x]=\max\{n\in\mathbb{Z}\colon n\leq x\}$.

If we now split $[0,1)$ as a disjoint union of the $Q+1$ intervals $I_n=[n/(Q+1),(n+1)/(Q+1))$, for $n=0,1,\ldots,Q$, there are two possible cases.

(i) Each interval contains precisely one number of the sequence. If so, simply let $\{q\xi\}$ be the element of the sequence contained in the last interval.

(ii) All the elements of the sequence belong to only $Q$ of the $Q+1$ intervals; then the so-called *(Dirichlet) box principle* yields two numbers within the same interval, i.e. integers $r,s$, where $0\leq r<s\leq Q$, and an integer $n$ such that

$\{r\xi\}, \{s\xi\} \in I_n$. Therefore,

$$(Q+1)^{-1} > |\{r\xi\} - \{s\xi\}| = |(s-r)\xi - ([s\xi] - [r\xi])|,$$

and, on putting $p = [s\xi] - [r\xi]$, $q = s - r$, we obtain the desired conclusion. □

**Remark 1.8** A slightly simpler argument is sometimes presented: it considers $Q$ intervals $[n/Q, (n+1)/Q)$, and only the second case. This yields the weaker estimate in which the right-hand side is replaced by $1/Q$, an almost equally useful result.

**Corollary 1.9** *Let $\xi \in \mathbb{R} \setminus \mathbb{Q}$. Then there exist infinitely many $p, q \in \mathbb{Z}$, $q > 0$, such that $(p,q) = 1$ and*

$$|q\xi - p| < q^{-1}. \tag{1.7}$$

*Proof* In fact, it suffices to apply the previous result, on choosing successively $Q = 1, 2, \ldots$. The fractions $p/q$ yielded in turn by the conclusion certainly satisfy the inequality of the corollary, since $q \le Q$ and hence $|\xi - (p/q)| < (qQ)^{-1} \le q^{-2}$. Moreover, such rational fractions $p/q$ constitute an infinite set, since for $Q \to \infty$ their sequence converges to $\xi$, which is irrational. □

**Remark 1.10** (i) The above discussion on the integer points on a line shows that the corollary is false for $\xi \in \mathbb{Q}$.

(ii) In the special case $\xi = \sqrt{\Delta}$, the existence of non-trivial solutions for Pell's equation yields another proof of the corollary (through (1.4)), strengthened in fact by a factor $1/(2\sqrt{\Delta})$. Conversely, applying the corollary to $\xi = \sqrt{\Delta}$ easily shows the existence of infinitely many solutions for at least one equation of the type $X^2 - \Delta Y^2 = m$ (where $|m| \le 2\sqrt{\Delta} + 1$). Looking then at pairs of positive solutions $(p,q) \ne (p^*, q^*)$, distinct but congruent modulo $m$, one finds (see Exercise 1.23 below) non-trivial solutions of Pell's equation, given by $m^{-1}(pp^* - \Delta qq^*, pq^* - p^*q)$.

(iii) It is easily shown (see Exercise 1.15 below) that *for almost all real numbers* $\xi$ (in the sense of Lebesgue measure) *the exponent* $-1$ *in Corollary 1.9 is the best-possible value*, i.e. the approximations $|\xi - (p/q)| < q^{-2-\varepsilon}$ are finite in number as soon as we fix $\varepsilon > 0$ (see [C1], Chapter VIII]). Intuitively, this result appears natural; in fact, for integers $q$ having $N$ (decimal) digits, such an approximation yields roughly $(2+\varepsilon)N$ digits of $\xi$. But in the choice for $p, q$ we dispose of $2N$ digits only, yielding a *gain of information*, which is but rarely possible. (For more precise results, due e.g. to Kintchine, see [C1], [S3].)

(iv) An efficient algorithm to find the *optimal* rational approximations comes from the expansion of $\xi$ as a *continued fraction*; we have sketched this procedure in Remark 1.1 above (see also [C1], [O], [S2]). Such a procedure coincides with Euclid's algorithm for $\xi \in \mathbb{Q}$ and for $\xi = \sqrt{\Delta}$ also leads to the solutions of Pell's equations.

For later reference, we give a multi-dimensional analogue of Dirichlet's lemma.

**Theorem 1.11** *Let $\xi_1, \ldots, \xi_r$ be real numbers and let $Q$ be a given positive integer; then there exist a positive integer $q \leq Q^r$ and integers $p_1, \ldots, p_r$ such that $|q\xi_i - p_i| < Q^{-1}$.*

Note that for $r = 1$ we recover *almost* the previous lemma.

*Sketch of proof* Consider the $Q^r + 1$ points $(\{t\xi_1\}, \ldots, \{t\xi_r\})$ in the unit cube, for $0 \leq t \leq Q^r$. Subdividing the unit cube into $Q^r$ small cubes of side $1/Q$ yields two points within the same small cube, corresponding to two different integers $0 \leq t_1 < t_2 \leq Q^r$. On taking their difference, putting $q = t_1 - t_2$, we obtain the desired inequality. □

**Exercise 1.12** Let $a_1 < a_2 < \cdots$ be the sequence of integers of the form $2^r 3^s$, arranged in increasing order. Prove that the ratio $a_{n+1}/a_n$ tends to 1 as $n \to \infty$.

**Exercise 1.13** Let $\xi \in \mathbb{R}$. Suppose that $w > 0$ is such that for every integer $Q \geq 1$ there exist integers $p, q$ with $|p|, |q| \leq Q$ and $0 < |q\xi - p| \leq Q^{-w}$. Prove that $w \leq 1$. (Hint: fix a large $Q$ and find coprime $p, q$ with the said property. Then define $X \geq Q$ by $|q\xi - p| = X^{-w}$. Choose now $t, u$ with the property for $[2X]$ in place of $Q$. Finally, eliminate $\xi$ to estimate $|pu - qt|$.) Actually the argument proves that in Dirichlet's lemma we cannot replace the term $(Q+1)$ by $c(Q+1)$ for any $c > 2$.

**Exercise 1.14** Prove that there exists $\xi \in \mathbb{R}$ such that for every real number $w$ and infinitely many pairs $(p, q)$ of positive integers we have $0 < |q\xi - p| < q^{-w}$. (Compare this case with the previous exercise. Hint: define $\xi$ by a series of rational numbers, with suitably rapid convergence.)

**Exercise 1.15** Prove that the set of real numbers $\xi$ for which there exists a number $\mu > 1$ and infinitely many integers $p, q$ such that $|q\xi - p| < q^{-\mu}$ has Lebesgue measure zero.

**Remark 1.16** **Approximations in function fields.** As we have pointed out, the "exponent" 2 attributed to $q^{-1}$ in the approximations $|\xi - (p/q)| \leq q^{-2}$ comes from the *double freedom* in choosing $p, q$. One may see clearly this principle even more by looking at a function field version of the Dirichlet lemma