7

Further Topics

We explained at the beginning of this book that we would restrict our focus on a certain special type of results in probabilistic number theory: convergence in law of arithmetically defined sequences of random variables. In this chapter, we will quickly survey (with some references) some important and beautiful results that either do not exactly fit our precise setting, or require rather deeper tools than we wished to assume, or could develop from scratch.

7.1 Equidistribution Modulo 1

We have begun this book with the motivating "founding" example of the Erdős–Kac Theorem, which is usually interpreted as the first result in probabilistic number theory. However, one could arguably say that at the time when this was first proved, there already existed a substantial theory that is really part of probabilistic number theory in our sense, namely, the theory of *equidistribution modulo* 1, due especially to Weyl [120]. Indeed, this concerns originally the study of the fractional parts of various sequences $(x_n)_{n\geqslant 1}$ of real numbers, and the fact that in many cases, including many when x_n has some arithmetic meaning, the fractional parts become *equidistributed* in $[0,1]$ with respect to the Lebesgue measure.

We now make this more precise in probabilistic terms. For a real number x, we will denote (as in Chapter 3) by $\langle x\rangle$ the fractional part of x, namely, the unique real number in $[0,1[$ such that $x-\langle x\rangle \in \mathbf{Z}$. We can identify this value with the point $e(x)=e^{2i\pi x}$ on the unit circle, or with its image in $\mathbf{R}/\mathbf{Z}$, either of which might be more convenient. Given a sequence $(x_n)_{n\geqslant 1}$ of real numbers, we define random variables S_{N} on $\Omega_{\mathrm{N}}=\{1,\ldots,\mathrm{N}\}$ (with uniform probability measure) by

$$\mathsf{S}_{\mathrm{N}}(n)=\langle x_n\rangle.$$

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

Then the sequence $(x_n)_{n\geqslant 1}$ is said to be *equidistributed modulo* 1 if the random variables S_N converge in law to the uniform probability measure dx on $[0,1]$, as $N \to +\infty$.

Among other things, Weyl proved the following results:

Theorem 7.1.1 (1) *Let* $P \in \mathbf{R}[X]$ *be a polynomial of degree* $d \geqslant 1$ *with leading term* ξX^d *where* $\xi \notin \mathbf{Q}$. *Then the sequence* $(P(n))_{n\geqslant 1}$ *is equidistributed modulo* 1.

(2) *Let* $k \geqslant 1$ *be an integer, and let* $\xi = (\xi_1, \dots, \xi_d) \in (\mathbf{R}/\mathbf{Z})^d$. *The closure* T *of the set* $\{n\xi \mid n \in \mathbf{Z}\} \subset (\mathbf{R}/\mathbf{Z})^d$ *is a compact subgroup of* $(\mathbf{R}/\mathbf{Z})^d$ *and the* T*-valued random variables on* Ω_N *defined by*

$$\mathsf{K}_N(n) = n\xi$$

converge in law as $N \to +\infty$ *to the probability Haar measure on* T.

The second part of this theorem is the same as Theorem B.6.5, (1). We sketch partial proofs of the first property, which is surprisingly elementary, given the Weyl Criterion (Theorem B.6.3).

We proceed by induction on the degree $d \geqslant 1$ of the polynomial $P \in \mathbf{R}[X]$, using a rather clever trick for this purpose. We may assume that $P(0) = 0$ (as the reader should check). If $d = 1$, then $P = \xi X$ for some real numbers ξ and $P(n) = n\xi$; the assumption is that ξ is irrational, and the result then follows from the 1-dimensional case of the second part, as explained in Example B.6.6.

Suppose that $d = \deg(P) \geqslant 2$ and that the statement is known for polynomials of smaller degree. We use the following:

Lemma 7.1.2 *Let* $(x_n)_{n\geqslant 1}$ *be a sequence of real numbers. Suppose that for any integer* $h \neq 0$, *the sequence* $(x_{n+h} - x_n)_n$ *is equidistributed modulo* 1. *Then* (x_n) *is equidistributed modulo* 1.

Sketch of the proof We leave this as an exercise to the reader; the key step is to use the following very useful inequality of van der Corput: for any integer $N \geqslant 1$, for any family $(a_n)_{1\leqslant n\leqslant N}$ of complex numbers, and for any integer $H \geqslant 1$, we have

$$\Bigl|\sum_{n=1}^{N} a_n\Bigr|^2 \leqslant \Bigl(1 + \frac{N+1}{H}\Bigr) \sum_{|h|<H} \Bigl(1 - \frac{|h|}{H}\Bigr) \sum_{\substack{1\leqslant n\leqslant N\\ 1\leqslant n+h\leqslant N}} a_{n+h}\bar{a}_n.$$

We also leave the proof of this inequality as an exercise... □

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

In the special case of $\mathsf{K}_{\mathrm{N}}(n) = \langle \mathrm{P}(n)\rangle$, this means that we have to consider auxiliary sequences $\mathsf{K}'_{\mathrm{N}}(n) = \langle \mathrm{P}(n+h) - \mathrm{P}(n)\rangle$, which corresponds to the same problem for the polynomials

$$\mathrm{P}(\mathrm{X}+h) - \mathrm{P}(\mathrm{X}) = \xi(\mathrm{X}+h)^d - \xi \mathrm{X}^d + \cdots = d\xi \mathrm{X}^{d-1} + \cdots.$$

Since these polynomials have degree $d-1$, and leading coefficient $d\xi \notin \mathbf{Q}$, the induction hypothesis applies to prove that the random variables K'_{N} converge to the Lebesgue measure. By the lemma, so does K_{N}.

Remark 7.1.3 The reader might ask what happens in Theorem B.6.3 if we replace the integers $n \leqslant \mathrm{N}$ by primes taken uniformly from those that are $\leqslant \mathrm{N}$. The answer is that the same properties hold – for both assertions, we have the same limit in law, under the same conditions on the polynomial for the first one. The proofs are quite a bit more involved however, and depend on Vinogradov's fundamental insight on the "bilinear" nature of the prime numbers. We refer to [59, 13.5, 21.2] for an introduction.

Exercise 7.1.4 Suppose that $0 < \alpha < 1$. Prove that the sequence $(\langle n^{\alpha}\rangle)_{n\geqslant 1}$ is equidistributed modulo 1.

Even in situations where equidistribution modulo 1 holds, there remain many fascinating and widely open questions when one attempts to go "beyond" equidistribution to understand fluctuations and variations that lie deeper. One of the best known problem in this area is that of the distribution of the *gaps* in a sequence that is equidistributed modulo 1.

Thus let $(x_n)_{n\geqslant 1}$ be a sequence in $\mathbf{R}/\mathbf{Z}$ that is equidistributed modulo 1. For $\mathrm{N} \geqslant 1$, consider the set of the N first values

$$\{x_1, \ldots, x_{\mathrm{N}}\}$$

of the sequence. The complement in $\mathbf{R}/\mathbf{Z}$ of these points is a disjoint union of "intervals" (in $[0,1[$, all but one of them are literally subintervals, and the last one "wraps-around"). The number of these intervals is $\leqslant \mathrm{N}$ (there might indeed be less than N, since some of the values x_i might coincide). The question that arises is: what is the distribution of the lengths of these gaps? Stated in a different way, the intervals in question are the connected components of $\mathbf{R}/\mathbf{Z} - \{x_1, \ldots, x_{\mathrm{N}}\}$, and we are interested in the Lebesgue measure of these connected components.

Let Ω_{N} be the set of the intervals in $\mathbf{R}/\mathbf{Z} - \{x_1, \ldots, x_{\mathrm{N}}\}$, with uniform probability measure. We define random variables by

$$\mathsf{G}_{\mathrm{N}}(\mathrm{I}) = \mathrm{N}\,\mathrm{length}(\mathrm{I})$$

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

for $\mathrm{I} \in \Omega_{\mathrm{N}}$. Note that the average gap is going to be about $1/\mathrm{N}$, so that the multiplication by N leads to a natural normalization where the average of G_{N} is about 1.

In the case of purely random points located in $\mathbf{S}^1$ independently at random, a classical probabilistic result is that the analogue random variables converge in law to an *exponential random variable* E on $[0, +\infty[$, that is, a random variable such that

$$\mathbf{P}(a < \mathrm{E} < b) = \int_a^b e^{-x} dx$$

for any nonnegative real numbers $a < b$. This is also called the "Poisson" behavior. For any (deterministic, for instance, arithmetic) sequence (x_n) that is equidistributed modulo 1, one can then ask whether a similar distribution will arise.

Already the special case of the sequence $(\langle n\xi \rangle)$, for a fixed irrational number ξ, leads to a particularly nice and remarkable answer, the "Three Gaps Theorem" (conjectured by Steinhaus and first proved by Sós [113]). This says that there are *at most three* distinct gaps between the fractional parts $\langle n\xi \rangle$ for $1 \leqslant n \leqslant \mathrm{N}$, independently of N and $\xi \notin \mathbf{Q}$.

Although this is in some sense unrelated to our main interests (there is no probabilistic limit theorem here!) we will indicate in Exercise 7.1.5 the steps that lead to a recent proof due to Marklof and Strömbergsson [86]. It is rather modern in spirit, as it depends on the use of lattices in $\mathbf{R}^2$, and especially on the space of lattices.

Very little is known in other cases, but numerical experiments are often easy to perform and lead at least to various conjectural statements. For instance, let $0 < \alpha < 1$ be fixed and put $x_n = \langle n^\alpha \rangle$. By Exercise 7.1.4, the sequence $(x_n)_{n \geqslant 1}$ is equidistributed modulo 1. In this case, it is expected that G_{N} should have the exponential limiting behavior for all α *except* for $\alpha = \frac{1}{2}$. Remarkably, this exceptional case is the only one where the answer is known! This is a result of Elkies and McMullen that we will discuss below in Section 7.5.

Exercise 7.1.5 Throughout this exercise, we fix an irrational number $\xi \notin \mathbf{Q}$.

(1) For $g \in \mathrm{SL}_2(\mathbf{R})$ and $0 \leqslant t < 1$, show that

$$\varphi(g,t) = \inf\{y > 0 \mid \text{there exists } x \text{ such that } -t < x \leqslant 1 - t \text{ and } (x,y) \in \mathbf{Z}^2 g\}$$

exists. Show that the function φ that it defines satisfies $\varphi(\gamma g, t) = \varphi(g,t)$ for all $\gamma \in \mathrm{SL}_2(\mathbf{Z})$.

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

(2) Let $\mathrm{N} \geqslant 1$ and $1 \leqslant n \leqslant \mathrm{N}$. Prove that the gap between $\langle n\xi\rangle$ and the "next" element of the set

$$\{\, \langle \xi\rangle, \dots, \langle \mathrm{N}\xi\rangle \,\}$$

(i.e., the next one in "clockwise order") is equal to

$$\frac{1}{\mathrm{N}}\varphi\left(g_{\mathrm{N}}, \frac{n}{\mathrm{N}}\right),$$

where

$$g_{\mathrm{N}} = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \mathrm{N}^{-1} & 0 \\ 0 & \mathrm{N} \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R}).$$

(3) Let $g \in \mathrm{SL}_2(\mathbf{R})$ be fixed. Consider the set

$$\mathrm{A}_g = g\mathbf{Z}^2 \cap \Big( ]-1,1[\times]0, +\infty[\Big).$$

Show that there exists $a = (x_1, y_1) \in \mathrm{A}_g$ with $y_1 > 0$ minimal.

(4) Show that either there exists $b = (x_2, y_2) \in \mathrm{A}_g$, not proportional to a, with y_2 minimal, or $\varphi(g,t) = y_1$ for all t.

(5) Assume that $y_2 > y_1$. Show that (a,b) is a basis of the lattice $g\mathbf{Z}^2 \subset \mathbf{R}^2$, and that x_1 and x_2 have opposite signs. Let

$$\mathrm{I}_1 =]0,1] \cap]-x_1, 1-x_1] \quad \text{and} \quad \mathrm{I}_2 =]0,1] \cap]-x_2, 1-x_2]\,.$$

Prove that

$$\varphi(g,t) = \begin{cases} y_2 & \text{if } t \in \mathrm{I}_1, \\ y_1 & \text{if } t \in \mathrm{I}_2,\ t \notin \mathrm{I}_1, \\ y_1 + y_2 & \text{otherwise.} \end{cases}$$

(6) If $y_2 = y_1$, show that $t \mapsto \varphi(g,t)$ takes at most three values by considering similarly $a' = (x_1', y_1') \in \mathrm{A}_g$ with $x_1' \geqslant 0$ minimal, and $b' = (x_2', y_2')$ with $x_2' < 0$ maximal.

7.2 Roots of Polynomial Congruences and the Chinese Remainder Theorem

One case of equidistribution modulo 1 deserves mention since it involves some interesting philosophical points, and has been the subject of a number of important works.

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

Let f be a fixed integral monic polynomial of degree $d \geqslant 1$. For any integer $q \geqslant 1$, the number $\varrho_f(q)$ of roots of f modulo q is finite, and the function ϱ_f is multiplicative (by the Chinese Remainder Theorem); moreover it is elementary that the set M_f of integers $q \geqslant 1$ such that $\varrho_f(q) \geqslant 1$ is infinite. On the other hand, we always have $\varrho_f(p) \leqslant d$ for p prime, so $\varrho_f(q) \leqslant d^{\omega(q)}$ at least when q is squarefree.

Exercise 7.2.1 Prove that M_f is infinite. [**Hint**: It suffices to check that the set of primes p such that $\varrho_f(p) \geqslant 1$ is infinite; assuming that it is not, show that the set of values $f(n)$ for $n \geqslant 1$ would be "too small."]

The question is then: is it true that the fractional parts $\langle a/q\rangle$ of the roots $a \in \mathbf{Z}/q\mathbf{Z}$ of f modulo q, when $\varrho_f(q) \geqslant 1$, become equidistributed modulo 1?

This problem admits a number of variants, and the deepest is undoubtedly the case of equidistribution of $\langle a/p\rangle$ when the modulus p is restricted to be a prime number. Indeed, it is only when $d = 2$ and f is irreducible that the equidistribution of roots modulo primes has been proven, first by Duke–Friedlander–Iwaniec [29] for quadratic polynomials with negative discriminant, and by Toth [118] for quadratic polynomials with positive discriminant, that is, with two real roots.

When all moduli q are taken into account, on the other hand, one can prove equidistribution for any irreducible polynomial, as was first done by Hooley [57]. However, although one might think that this provides evidence for the stronger statement modulo primes, it turns out that this result has in fact almost nothing to do with roots of polynomials!

More precisely, Kowalski and Soundararajan [80] show that equidistribution holds for the fractional parts of elements of sets modulo q obtained by the Chinese Remainder Theorem, starting from subsets A_{p^ν} of $\mathbf{Z}/p^\nu\mathbf{Z}$, under the sole condition that A_p should have at least two elements for a positive proportion of the primes.

In other words, for p prime and $\nu \geqslant 1$, let $\mathrm{A}_{p^\nu} \subset \mathbf{Z}/p^\nu\mathbf{Z}$ be an arbitrary subset of residue classes, and for $q \geqslant 1$, define $\mathrm{A}_q \subset \mathbf{Z}/q\mathbf{Z}$ to be the set of $x \pmod q$ such that, for all primes p dividing q, with exact exponent ν, we have $x \pmod{p^\nu} \in \mathrm{A}_{p^\nu}$. Define $\varrho(q) = |\mathrm{A}_q|$, which is a multiplicative function, and let Ω be the set of all $q \geqslant 1$ such that A_q is not empty. For any $q \in \Omega$, let Δ_q be the probability measure on $\mathbf{R}/\mathbf{Z}$ given by

$$\Delta_q = \frac{1}{\varrho(q)} \sum_{x \in \mathrm{A}_q} \delta_{\langle \frac{a}{q}\rangle},$$

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

where δ_x denotes a Dirac mass at x (the measure Δ_q is the image of the uniform probability measure on A_q by the map $a \mapsto \langle \frac{a}{q} \rangle$). Then [80, Th. 1.1] implies the following:

Theorem 7.2.2 *Suppose that there exists* $\alpha > 0$ *such that*

$$\sum_{\substack{p \leqslant \mathrm{Q} \\ \varrho(p) \geqslant 2}} 1 \geqslant \alpha \pi(\mathrm{Q})$$

for all Q *large enough. Let* N(Q) *be the number of* $q \leqslant \mathrm{Q}$ *such that* A_q *is not empty. Then the probability measures*

$$\frac{1}{\mathrm{N}(\mathrm{Q})} \sum_{\substack{q \leqslant \mathrm{Q} \\ q \in \Omega}} \Delta_q$$

converge to the Lebesgue measure on $\mathbf{R}/\mathbf{Z}$.

Example 7.2.3 Let $f \in \mathbf{Z}[\mathrm{X}]$ be monic and without repeated roots. If $\deg(f) \geqslant 2$, then this theorem applies to the case where A_{p^ν} is the set of roots of f modulo p^ν, because a basic theorem of algebraic number theory (the Chebotarev Density Theorem; see, for instance, [91, Th. 13.4]) implies that there is a positive proportion of primes p for which f has $\deg(f) \geqslant 2$ distinct roots in $\mathbf{Z}/p\mathbf{Z}$. However, the theorem shows that we can replace A_{p^ν} by any other subset A'_{p^ν} of $\mathbf{Z}/p^\nu\mathbf{Z}$ with the same cardinality, without changing the conclusion concerning the fractional parts modulo all q, whereas (of course) we could select A'_p in such a way that there is no equidistribution modulo primes, in the sense that the measures

$$\frac{1}{\mathrm{P}(\mathrm{Q})} \sum_{\substack{p \leqslant \mathrm{Q} \\ p \in \Omega}} \Delta_p,$$

where P(Q) is the number of primes $p \leqslant \mathrm{Q}$ in Ω, do not converge to the Lebesgue measure.

Remark 7.2.4 Theorem 7.2.2 does not correspond exactly to the setting considered in [57], which concerns (implicitly) the slightly different probability measures

$$\frac{1}{\mathrm{M}(\mathrm{Q})} \sum_{\substack{q \leqslant \mathrm{Q} \\ q \in \Omega}} \varrho(q) \Delta_q, \tag{7.1}$$

where

$$\mathrm{M}(\mathrm{Q}) = \sum_{q \leqslant \mathrm{Q}} \varrho(q).$$

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

Interestingly, these two ways of making precise the idea of equidistribution modulo q are *not* equivalent: it is shown in [80, Prop. 2.8] that there exist choices of subsets (A_p) to which Theorem 7.2.2 applies, but for which the measures (7.1) *do not* converge to the uniform measure.

7.3 Gaps between Primes

The Prime Number Theorem

$$\pi(x) \sim \frac{x}{\log x}$$

indicates that the average gap between successive prime numbers of size x is about $\log x$. A natural problem, especially in view of the many conjectures that exist concerning the distribution of primes (such as the Twin Prime conjecture), is to understand the distribution of these gaps.

One way to do this, which is consistent with our general framework, is the following. For any integer $\mathrm{N} \geqslant 1$, we define the probability space Ω_{N} to be the set of integers n such that $1 \leqslant n \leqslant \mathrm{N}$ (as in Chapter 2), with the uniform probability measure. Fix $\lambda > 0$. We then define the random variables

$$\mathsf{G}_{\lambda,\mathrm{N}}(n) = \pi(n + \lambda \log n) - \pi(n),$$

which measures how many primes exist in the interval starting at n of length equal to λ times the average gap.

A precise conjecture exists concerning the limiting behavior of $\mathsf{G}_{\lambda,\mathrm{N}}$ as $\mathrm{N} \to +\infty$:

Conjecture 7.3.1 *The sequence $(\mathsf{G}_{\lambda,\mathrm{N}})_{\mathrm{N}}$ converges in law as $\mathrm{N} \to +\infty$ to a Poisson random variable with parameter λ, that is, for any integer $r \geqslant 0$, we have*

$$\mathbf{P}_{\mathrm{N}}(\mathsf{G}_{\lambda,\mathrm{N}} = r) \to e^{-\lambda}\frac{\lambda^r}{r!}.$$

To the author's knowledge, this conjecture first appears in the work of Gallagher [45], who in fact proved that it would follow from a suitably uniform version of the famous Hardy-Littlewood k-tuple conjecture. (Interestingly, the same assumption would imply also a generalization of Conjecture 7.3.1 where one considers suitably normalized gaps between simultaneous prime values of a family of polynomials, e.g., between twin primes; see [73], where Gallagher's argument is presented in a probabilistic manner very much in the style of this book.)

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

Part of the interest of Conjecture 7.3.1 is that the distribution obtained for the gaps is exactly what one expects from "purely random" sets (see the discussion by Feller in [37, I.3, I.4]).

7.4 Cohen–Lenstra Heuristics

In this section, we will assume some basic knowledge concerning algebraic number theory. We refer, for instance, to the book [58] of Ireland and Rosen for an elementary introduction to this subject, in particular to [58, Ch. 12], and to the book [91] of Neukirch for a complete account.

Beginning with a famous paper of Cohen and Lenstra [25], there is by now an impressive body of work concerning the limiting behavior of certain arithmetic measures of a rather different nature than all those we have described up to now. For these, the underlying arithmetic objects are families of number fields of certain kinds, and the random variables of interest are given by the *ideal class groups* of the number fields, or some invariants of the ideal class groups, such as their p-primary subgroups (recall that, as a finite abelian group, the ideal class group C of a number field K can be represented as a direct product of groups of order a power of p, which are zero for all but finitely many p).

The basic idea of Cohen and Lenstra is that the ideal class groups, in suitable families, should behave (in general) in such a way that a given finite abelian group C appears as an ideal class group with "probability" proportional to the inverse $1/\operatorname{Aut}(\mathrm{C})$ of the order of the automorphism group of C, so that, for instance, obtaining a group of order p^2 of the form $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z}$, with automorphism group of size about p^4, is much more unlikely than obtaining the cyclic group $\mathbf{Z}/p^2\mathbf{Z}$, which has automorphism group of size $p^2 - p$.

Imaginary quadratic fields provide a first basic (and still very open!) special case. Using our way of presenting probabilistic number theory, one could define the finite probability spaces Ω_{D} of negative "fundamental discriminants" $-d$ (that is, either $-d$ is a squarefree integer congruent to 3 modulo 4, or $-d = 4\delta$ where δ is squarefree and congruent to 1 or 2 modulo 4) with $1 \leqslant d \leqslant \mathrm{D}$ and the uniform probability measure, and one would define for each D and each prime p a random variable $\mathsf{P}_{p,\mathrm{D}}$ taking values in the set A_p of isomorphism classes of finite abelian groups of order a power of p, such that $\mathsf{P}_{p,\mathrm{D}}(-d)$ is the p-part of the class group of $\mathbf{Q}(\sqrt{-d})$. One of the conjectures ("heuristics") of Cohen and Lenstra is that if $p \geqslant 3$, then $\mathsf{P}_{p,\mathrm{D}}$ should converge in law as $\mathrm{D} \to +\infty$ to the probability measure μ_p on A_p such that

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

$$\mu_p(\mathrm{A}) = \frac{1}{\mathrm{Z}_p} \frac{1}{|\operatorname{Aut}(\mathrm{A})|}$$

for any group $\mathrm{A} \in \mathrm{A}_p$, where Z_p is the constant required to make the measure thus defined a probability measure (the existence of this measure – in other words, the convergence of the series defining Z_p – is something that of course requires a proof).

Very few unconditional results are known toward these conjectures, and progress often requires significant ideas. There has however been striking advances by Ellenberg, Venkatesh and Westerland [32] in some analogue problems for quadratic extensions of polynomial rings over finite fields, where geometric methods make the problem more accessible, and in fact allow the use of essentially topological ideas (see the Bourbaki report [98] of O. Randal-Williams).

7.5 Ratner Theory

Although all the results that we have described up to now are beautiful and important, maybe the most remarkably versatile tool that can be considered to lie within our chosen context is *Ratner theory*, named after the fundamental work of M. Ratner [99]. We lack the expertise to present anything more than a few selected statements of applications of this theory; we refer to the survey of É. Ghys [47] and to the book of Morris [89] for an introduction (Section 1.4 of that book lists more applications of Ratner Theory), and to that of Einsiedler and Ward [30] for background results on ergodic theory and dynamical systems (some of which also have remarkable applications in number theory).

We illustrate the remarkable power of this theory with the beautiful result of Elkies and McMullen [31] which was already mentioned in Section 7.1. We consider the sequence of fractional parts of $\sqrt{n}$ for $n \geqslant 1$ (viewed as elements of $\mathbf{R}/\mathbf{Z}$). As in the previous section, for any integer $\mathrm{N} \geqslant 1$, we define the space Ω_{N} to be the set of connected components of $\mathbf{R}/\mathbf{Z} - \{\langle 1\rangle, \dots, \langle\sqrt{\mathrm{N}}\rangle\}$, with uniform probability measure, and we define random variables on Ω_{N} by

$$\mathsf{G}_{\mathrm{N}}(\mathrm{I}) = \mathrm{N}\,\mathrm{length}(\mathrm{I}).$$

Elkies and McMullen found the limiting distribution of G_{N} as $\mathrm{N} \to +\infty$. It is a very nongeneric probability measure on $\mathbf{R}$!

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

Theorem 7.5.1 (Elkies–McMullen) *As* $\mathrm{N} \to +\infty$*, the random variables* G_{N} *converge in law to a random variable on* $[0, +\infty[$ *with probability law* $\mu_{\mathrm{EM}} = \frac{6}{\pi^2} f(x)dx$*, where* f *is continuous, analytic on the intervals* $[0, 1/2]$*,* $[1/2, 2]$ *and* $[2, +\infty[$*, is not of class* C^3*, and satisfies* $f(x) = 1$ *if* $0 \leqslant x \leqslant 1/2$*.*

This is [31, Th. 1.1]. The restriction of the density f to the two intervals $[1/2, 2]$ and $[2, +\infty[$ can be written down explicitly and it is an "elementary" function. For instance, if $1/2 \leqslant x \leqslant 2$, then let $r = \frac{1}{2}x^{-1}$ and

$$\psi(r) = \arctan\left(\frac{2r-1}{\sqrt{4r-1}}\right) - \arctan\left(\frac{1}{\sqrt{4r-1}}\right);$$

we then have

$$f(x) = \frac{2}{3}(4r-1)^{3/2}\psi(r) + (1-6r)\log r + 2r - 1$$

(see [31, (3.53)]).

We give the barest outline of the proof, in order to simply point out what kind of results are meant by Ratner Theory. The paper of Elkies and McMullen also gives a detailed and highly readable introduction to this area.

The proof studies the gap distribution by means of the function L_{N} defined for $x \in \mathbf{R}/\mathbf{Z}$ so that $\mathrm{L}_{\mathrm{N}}(x)$ is the measure of the gap interval containing x (with $\mathrm{L}_{\mathrm{N}}(x) = 0$ if x is one of the boundary points of the gap intervals for $\langle\sqrt{1}\rangle, \ldots, \langle\sqrt{\mathrm{N}}\rangle$). We can then check that for $t \in \mathbf{R}$, the total measure in $\mathbf{R}/\mathbf{Z}$ of the points lying in a gap interval of length $< t$, which is equal to the Lebesgue measure

$$\mu(\{x \in \mathbf{R}/\mathbf{Z} \mid \mathrm{L}_{\mathrm{N}}(x) < t\}),$$

is given by

$$\int_0^t td(\mathbf{P}_{\mathrm{N}}(\mathsf{G}_{\mathrm{N}} < t)) = t\,\mathbf{P}_{\mathrm{N}}(\mathsf{G}_{\mathrm{N}} < t) - \int_0^t \mathbf{P}_{\mathrm{N}}(\mathsf{G}_{\mathrm{N}} < t)dt.$$

Concretely, this means that it is enough to understand the limiting behavior of L_{N} in order to understand the limit gap distribution. Note that there is nothing special about the specific sequence considered in that part of the argument.

Fix $t \geqslant 0$. The key insight that leads to questions involving Ratner theory is that if N is a square of an integer, then the probability

$$\mu(\{x \in \mathbf{R}/\mathbf{Z} \mid \mathrm{L}_{\mathrm{N}}(x) < t\})$$

can be shown (asymptotically as $\mathrm{N} \to +\infty$) to be very close to the probability that a certain affine lattice $\Lambda_{\mathrm{N},x}$ in $\mathbf{R}^2$ intersects the triangle Δ_t with vertices

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

$(0,0)$, $(1,0)$ and $(0,2t)$ (with area t). The lattice has the form $\Lambda_{\mathrm{N},x} = g_{\mathrm{N},x} \cdot \mathbf{Z}^2$ for some (fairly explicit) affine transformation $g_{\mathrm{N},t}$.

Let $\mathrm{ASL}_2(\mathbf{R})$ be the group of affine transformations

$$z \mapsto z_0 + g(z)$$

of $\mathbf{R}^2$ whose linear part $g \in \mathrm{GL}_2(\mathbf{R})$ has determinant 1, and $\mathrm{ASL}_2(\mathbf{Z})$ the subgroup of those affine transformations of determinant 1 where both the translation term z_0 and the linear part have coefficients in $\mathbf{Z}$. Then the lattices $\Lambda_{\mathrm{N},x}$ can be interpreted as elements of the quotient space

$$\mathrm{M} = \mathrm{ASL}_2(\mathbf{Z})\backslash \mathrm{ASL}_2(\mathbf{R}),$$

which parameterizes affine lattices $\Lambda \subset \mathbf{R}^2$ with $\mathbf{R}^2/\Lambda$ of area 1. This space admits a unique probability measure $\widetilde{\mu}$ that is invariant under the right action of $\mathrm{ASL}_2(\mathbf{R})$ by multiplication.

Now we have, for each $\mathrm{N} \geqslant 1$, a probability measure μ_{N} on M, namely, the law of the random variable $\mathbf{R}/\mathbf{Z} \to \mathrm{M}$ defined by $x \mapsto \Lambda_{\mathrm{N},x}$. What Ratner Theory provides is a very powerful set of tools to prove that certain probability measures on M (or on similar spaces constructed with groups more general than $\mathrm{ASL}_2(\mathbf{R})$ and suitable quotients) are equal to the canonical measure $\widetilde{\mu}$. This is applied, essentially, to all possible limits of subsequences of (μ_{N}), to show that these must coincide with $\widetilde{\mu}$, which leads to the conclusion that the whole sequence converges in law to $\widetilde{\mu}$. It then follows that

$$\mu(\{x \in \mathbf{R}/\mathbf{Z} \mid \mathrm{L}_{\mathrm{N}}(x) < t\}) \to \widetilde{\mu}(\{\Lambda \in \mathrm{M} \mid \mathrm{M} \cap \Delta_t \neq \emptyset\}).$$

This gives, in principle, an explicit form of the gap distribution. To compute it exactly is an "exercise" in euclidean geometry – which is by no means easy!

7.6 And Even More ...

And there are even more interactions between probability theory and number theory than what our point of view considers... Here are some examples, which we order, roughly speaking, in terms of how close they are from the perspective of this book:

- Applications of limit theorems for arithmetic probability measures to other problems of analytic number theory: we have given a few examples in exercises (see Exercises 2.3.5 or 3.3.4), but there are many more of course.

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press

- Using probabilistic ideas to *model* arithmetic objects, and make conjectures or prove theorems concerning those; in contrast with our point of view, it is not always expected in such cases that there should exist actual limit theorems comparing the model with the actual arithmetic phenomena.
  A typical example is the so-called “Cramér model” for the distribution of primes, which is known to lead to wrong conclusions in some cases, but is often close enough to the truth to be used to suggest how certain problems might behave (see, for instance, the survey of Pintz [94]).
- Using number-theoretic ideas to *derandomize* certain constructions or algorithms. There are indeed a number of very interesting results that use the “randomness” of specific arithmetic objects to give deterministic constructions, or deterministic proofs of existence, for mathematical objects that might have first been shown to exist using probabilistic ideas.
  Examples include the construction of expander graphs by Margulis (see, e.g., [74, §4.4]), or of Ramanujan graphs by Lubotzky, Phillips and Sarnak [84], or in a different vein, the construction of explicit “ultraflat” trigonometric polynomials (in the sense of Kahane) by Bombieri and Bourgain [13], or the construction of explicit functions modulo a prime with smallest possible Gowers norms by Fouvry, Kowalski and Michel [42].

https://doi.org/10.1017/9781108888226.008 Published online by Cambridge University Press