LINNIK’S ERGODIC METHOD AND
THE DISTRIBUTION OF INTEGER POINTS ON SPHERES

JORDAN S. ELLENBERG, PHILIPPE MICHEL AND AKSHAY VENKATESH

Abstract. We discuss the distribution of integral solutions to
\[ x^2 + y^2 + z^2 = d, \] as \( d \to \infty \).

In particular, we prove a refinement of Linnik’s theorem that the solutions
are uniformly distributed modulo \( q \). The paper is intended in large part as an
exposition of Linnik’s ideas.

Contents

1. Introduction 1
2. An overview of the ergodic method 9
3. Mixing 17

Part 2. Classical theory 19
4. The action of the class group on \( \tilde{R}_3(d) \) 19
5. Representations of binary quadratic forms by \( x^2 + y^2 + z^2 \). 23

Part 3. Adelization 25
6. Adelic actions on rational lattices 25
7. Adelic interpretation of \( R_3(d) \) 28
8. Adelic interpretation of \( R_3(d) \) 31
9. Adelic interpretation of \( \text{red}_q: R_3(d) \to R_3(d; q) \) 34
10. Some local analysis 35

Part 4. Graphs and Expanders 37
11. The graph structure on \( R_3(d; q) \) 37
12. Expander graphs and random walks 43
References 46

1. Introduction

Let \( d > 1 \) be an integer which, for simplicity of exposition, we assume to be squarefree, and let \( R_3(d) \) be the set of integer points on a 2-dimensional sphere of
radius \(d^{1/2}\):

\[
\mathcal{R}_3(d) := \{ \mathbf{x} = (x, y, z) \in \mathbb{Z}^3, \ x^2 + y^2 + z^2 = d \}.
\]

The study of \(\mathcal{R}_3(d)\) is a classical question of number theory. Surprisingly, there are interesting results about \(\mathcal{R}_3(d)\) that have been proved in the last two decades, and simply stated problems that remain unresolved. In increasing order of fineness, one may ask:

1. When is \(\mathcal{R}_3(d)\) nonempty?
2. If nonempty, how large is \(\mathcal{R}_3(d)\), and how can we generate points in \(\mathcal{R}_3(d)\)?
3. If \(\mathcal{R}_3(d)\) gets large, how is it distributed on the sphere of radius \(d^{1/2}\)?

1.1. **Existence.** The first question was studied by Legendre and the answer is:

**Theorem (Legendre/Gauss).** \(\mathcal{R}_3(d)\) is nonempty if, and only if, \(d\) is not of the form \(4^a(8b - 1)\) \((a, b \in \mathbb{N})\).

Put in different terms, this amount to say that the quadratic equation \(x^2 + y^2 + z^2 = d\) satisfies the Hasse principle. Legendre’s 1798 proof however was incomplete and the first complete proof was given by Gauss three years later in his *Disquisitiones arithmeticae* [Gau01]. An integer satisfying Legendre’s condition above will be called *admissible*.

1.2. **Size.** The second question is somewhat subtler and its resolution is the consequence of the work of several people and is stretched over more than a century. The initial and fundamental insight come from Gauss, who showed that \(\mathcal{R}_3(d)\) is closely connected with the set of classes of binary quadratic forms of discriminant \(-d\).

This relation amounts, in more modern terms, to the existence of a natural action on the quotient \(\mathrm{SO}_3(\mathbb{Z}) \setminus \mathcal{R}_3(d)\) of the ideal class group, \(\mathrm{Pic}(\mathcal{O}_K)\), of the ring of integers, \(\mathcal{O}_K\), of the quadratic field \(K = \mathbb{Q}(\sqrt{-d})\). This action is, in fact, transitive (at least if \(d\) is squarefree, which we assume here) and is faithful if and only if \(d \equiv 3\) modulo 8. In particular, whereas \(\mathrm{SO}_3(\mathbb{Z}) \setminus \mathcal{R}_3(d)\) does itself not have a natural group structure (what would the identity be?) the notion of “arithmetic progression” makes sense on \(\mathrm{SO}_3(\mathbb{Z}) \setminus \mathcal{R}_3(d)\). An exposition of these facts is given in [4].

An immediate consequence of the existence of this action is an exact formula relating \(|\mathcal{R}_3(d)|\) to the class number \(h_K = |\mathrm{Pic}(\mathcal{O}_K)|\) of \(K\). About 40 years after Gauss work (1838), Dirichlet’s class number formula provided an analytic expression for the class number:

**Theorem (Dirichlet).** The class number equals

\[
h_K = \frac{c}{2\pi} d^{1/2} \text{res}_{s=1} \zeta_K(s)
\]

with \(c = 2, 4, 6, 8\) or 12 and \(\zeta_K(s)\) is the Dedekind \(\zeta\)-function of \(K\).

An immediate consequence of this relation is the non-vanishing of the residue at 1 of \(\zeta_K\) (which we recall is a key step in the proof of Dirichlet’s prime number theorem). However, in order to get more precise information on its size, one had to wait another century and the work of Landau and Siegel (1936) culminating in

---

1Legendre assumed the existence of primes in arithmetic progressions which was only proven 40 years later by Dirichlet.
Theorem (Siegel).

\[ \text{res}_{s=1} \zeta_K(s) = d^{o(1)} \]

from which one concludes that

\[ |\mathcal{R}_3(d)| = d^{1/2 + o(1)}. \tag{1.1} \]

1.3. Distribution. The third question is the main focus of this paper; whereas it is not at first clear that is a worthy successor to the first two, its investigation has proved very rich. Progress on it has been entwined with the study of modular \(L\)-functions, as well as to the study of dynamics on homogeneous spaces. The first significant answer regarding this question are due to Y. V. Linnik who, in the late 50’s, proved – amongst other results – the following:

**Theorem 1.4 (Linnik).** As \( d \to +\infty \) amongst the admissible, squarefree, integers satisfying \( d \equiv \pm 1(5) \), the set \( \left\{ \frac{x}{\sqrt{d}}, x \in \mathcal{R}_3(d) \right\} \subset S_2 \) becomes equidistributed on the unit sphere \( S_2 \) with respect to the Lebesgue probability measure.

In explicit terms, that means that if \( \text{red}_\infty : \mathcal{R}_3(d) \to S_2 \) denotes the “scaling” map \( x \mapsto d^{-1/2}x \), then for any measurable subset \( \Omega \subset S_2 \) whose boundary has Lebesgue measure zero

\[ \frac{|\text{red}_\infty^{-1}(\Omega)|}{|\mathcal{R}_3(d)|} = \text{area}(\Omega)(1 + o(1)), \quad d \to +\infty; \tag{1.2} \]

(we take the normalization \( \text{area}(S_2) = 1 \)).

Linnik obtained this by an ingenious technique which he called the “ergodic method” which exploit the action of \( \text{Pic}(\mathcal{O}_K) \) on \( \text{SO}_3(\mathbb{Z}) \setminus \mathcal{R}_3(d) \). This method was generalized later (notably by Linnik’s student, Skubenko) to establish several remarkable results about the distribution of the representations of large integers by (integral) ternary quadratic forms \([\text{Lin68}]\). Until recently, Linnik's ergodic method remained surprisingly little-known, although simplified treatments were given by a number of authors \([\text{Tet83, Mal84}]\); one possible reason is that the method did not fit into ergodic theory as the term is now usually understood, i.e. dynamics of a measure-preserving transformation.

The aim of the present paper is to revisit and explain in a slightly different language Linnik’s original approach and to present further refinements which do not seem present in Linnik’s work and do not seem accessible to other approaches. For this, we will discuss in full detail the following discrete variant to Linnik’s equidistribution theorem.

1.5. The discrete sphere. Instead of looking at the position of \( \mathcal{R}_3(d) \) on the sphere (archimedean distribution), one could also look the congruence properties of points in \( \mathcal{R}_3(d) \) (\( q \)-adic distribution). For \( q \) an integer coprime with \( d \), let \( \mathcal{R}_3(d; q) \) denote the “sphere modulo \( q \)"

\[ \mathcal{R}_3(d; q) := \{ x = (\overline{x}, \overline{y}, \overline{z}) \in (\mathbb{Z}/q\mathbb{Z})^3, \overline{x}^2 + \overline{y}^2 + \overline{z}^2 \equiv d \mod q \}. \]

We have the following
Figure 1. $d^{-1/2}R_3(d) \subset S_2$ for $d = 101, 8011, 104851$
Theorem 1.6 (Linnik). Let \( q \) be a fixed integer, coprime with 30. As \( d \to +\infty \) amongst the admissible squarefree integers satisfying \( d \equiv \pm 1(5) \), \( (d,q) = 1 \), the multiset
\[
\{ \bar{x} \pmod{q}, \ x \in \mathcal{R}_3(d) \} \subset \mathcal{R}_3(d;q)
\]
denotes the reduction modulo \( q \) map, then, for any \( \bar{x} \in \mathcal{R}_3(d;q) \),
\begin{equation}
\frac{|\text{red}^{-1}_q(\bar{x})|}{|\mathcal{R}_3(d)|} = \frac{1}{|\mathcal{R}_3(d;q)|}(1 + o(1)),
\end{equation}
\subsection{1.7. A refinement of Theorem \ref{thm:1.4}}
We will focus our attention on proving a sharpened version of Theorem \ref{thm:1.6}. For any \( \bar{x} \in \mathcal{R}_3(d;q) \) define the deviation at \( \bar{x} \) to be
\[
\text{dev}_d(\bar{x}) = \frac{|\text{red}^{-1}_q(\bar{x})|}{|\mathcal{R}_3(d)|/|\mathcal{R}_3(d;q)|} - 1.
\]
Theorem \ref{thm:1.6} is then equivalent to
\[
\text{dev}_d(\bar{x}) \to 0, \text{ for any } \bar{x} \text{ as } d \to +\infty
\]
(amongst admissible squarefree \( d \equiv \pm 1(5) \)). We have
\[\text{Theorem 1.8.} \quad \text{Fix } \nu, \delta > 0 \text{ and suppose that } q^2 \leq d^{1/2-\nu} \text{ and } (q,30) = 1. \quad \text{The fraction of } \bar{x} \in \mathcal{R}_3(d;q) \text{ for which } |\text{dev}_d(\bar{x})| > \delta \text{ tends to zero as } d \to \infty \text{ with } d \equiv \pm 1(5) \text{ admissible.}\]
\subsection{1.9. An application to mixing}
\begin{itemize}
\item The method of proof of Theorem \ref{thm:1.8} has application regarding the mixing properties of the action of \( \text{Pic}(\mathcal{O}_K) \) on \( \mathcal{R}_3(d) \). Let \( [a] \) be the ideal class represented by some ideal \( a \in \mathcal{O}_K \). We would like to understand the distribution of the set of pairs
\[\{(x, [a], x), \ x \in \mathcal{R}_3(d) \} \subset \mathcal{R}_3(d) \times \mathcal{R}_3(d)\]
as \( d \to +\infty \) (this involve for each \( d \) the choice of an ideal class \([a]\)). Here we work in the context of the discrete sphere and consider the behaviour of the multiset
\[\{\text{red}_q(x, [a], x), \ x \in \mathcal{R}_3(d) \} \subset \mathcal{R}_3(d;q) \times \mathcal{R}_3(d;q)\].
\end{itemize}
For definiteness, we may and will assume that \( a \) is primitive\footnote{As we explain below the action on \( \text{SO}_3(\mathbb{Z})\backslash \mathcal{R}_3(d) \) can be lifted to an action on \( \mathcal{R}_3(d) \) of minimal norm in its \( \mathbb{Q}^\times \)-homothety class.} let \( N = \text{Nr}(a) \) be its norm. We also assume for simplicity that \( N \) is odd and coprime with 15d.
One has an inclusion
\[ \{ \text{red}_q(x, [a]x), \ x \in \mathcal{A}_3(d) \} \subset \mathcal{A}_3(d; q, N) \]
where \( \mathcal{A}_3(d; q, N) \) a specific multiset supported on \( \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \); this the graph the Hecke correspondence.

Let \( a \) be a primitive ideal of norm \( N \), then the multiset \( \{ \text{red}_q(x, [a]x), \ x \in \mathcal{A}_3(d) \} \subset \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \) becomes equidistributed on \( \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \) w.r.t. the uniform probability measure on \( \mathcal{A}_3(d; q, N) \).

When \( N \) is fixed, a variant of the proof of Theorem 1.6 gives the following

Let \( q, N \) be fixed integers, coprime and coprime with 30. As \( d \to +\infty \) amongst the admissible squarefree integers satisfying \( d \equiv \pm 1(5), (d, qN) = 1 \) and admitting a primitive ideal \( a \) of norm \( N \) exactly the multiset \( \{ \text{red}_q(x, [a]x), \ x \in \mathcal{A}_3(d) \} \) viewed as a multiset supported on \( \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \) becomes equidistributed with respect to the measure \( \mu_{d,q,N} \).

We will now consider the case of \( N \to \infty \). Then, \( \mathcal{A}_3(d; q, N) \) becomes equidistributed: more precisely the measure \( \mu_{d,q,N} \) converges to the uniform probability measure on \( \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \). In view of this and of the previous equidistribution result, it is natural to expect that the multiset \( \{ \text{red}_q(x, [a]x), \ x \in \mathcal{A}_3(d) \} \) become equidistributed as well. This is indeed true at least for \( N \) in a restricted range:

**Theorem 1.10.** Let \( q \) be a fixed integer coprime with 30 and \( \varepsilon > 0 \). For any \( d \) squarefree, admissible, satisfying \( (d, q) = 1 \) and \( d \equiv \pm 1(5) \) let \( a \) be a primitive \( \mathcal{O}_K \)-ideal of norm \( N = N_d \). Assume that \( N \to +\infty \) as \( d \to +\infty \) and that \( N \leq d^{1/2-\varepsilon} \), then the multiset
\[ \{ \text{red}_q(x, [a]x), \ x \in \mathcal{A}_3(d) \} \subset \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \]
becomes equidistributed on \( \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \) w.r.t. the uniform probability measure.

The idea of the proof is quite simple: a version of Theorem 1.8 (Thm. 3.1) shows that the multiset \( \{ \text{red}_q(x, [a]x), \ x \in \mathcal{A}_3(d) \} \) is almost equidistributed on \( \mathcal{A}_3(d; q, N) \) as long as \( q^2d_N \leq d^{1/2-\varepsilon} \); then because of the equidistribution of \( \mathcal{A}_3(d; q; N) \) on \( \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \) (Prop. 3.3) we can “push” the almost equidistribution on the varying space \( \mathcal{A}_3(d; q, N) \) to full equidistribution on the fixed space \( \mathcal{A}_3(d; q) \times \mathcal{A}_3(d; q) \). Since \( d_N = N^{1+\varepsilon(1)} \) this explain the constraint \( N \leq d^{1/2-\varepsilon} \).

The proof of Theorem 1.10 can be adapted to the archimedean setting to yield

**Theorem 1.11.** Given any \( \varepsilon > 0 \). For any \( d \) squarefree, admissible and \( d \equiv \pm 1(5) \) let \( a \) be a primitive \( \mathcal{O}_K \)-ideal of norm \( N = N_d \). Assume that \( N \to +\infty \) as \( d \to +\infty \) and that \( N \leq d^{1/2-\varepsilon} \), then the set
\[ \{ \text{red}_\infty(x, [a]x), \ x \in \mathcal{A}_3(d) \} \subset S^2 \times S^2 \]
becomes equidistributed on \( S^2 \times S^2 \) w.r.t. the product Lebesgue probability measure.

It is then natural to surmise the following

---

4 This holds if and only if every prime factor of \( N \) splits in \( K \)

5 In [MV07], a similar conjecture was made (in a slightly different context) and some applications of it were described.
**Conjecture** (Mixing conjecture). The above equidistribution results hold without the constraint \( N \leq d^{1/2-\varepsilon} \) and \( d \equiv \pm 1(5) \).

Notice that by Minkowski’s theorem, one has \( N \leq (4/\pi)d^{1/2} \) and by Siegel’s theorem the total number of primitive ideals equals \( d^{1/2 + o(1)} \) while the number of primitive ideals of norm \( \leq d^{1/2-\varepsilon} \) is bounded by \( \ll d^{1/2-\varepsilon/2} \) so, by comparison with the Mixing conjecture, Theorem 1.10 “misses” a lot of the possible primitive ideals; however, as we discuss below, Theorem 1.10 seem significantly stronger than what could be obtained by different methods, even on very strong hypotheses.

1.11.1. Representation of binary forms by quaternary quadratic forms. Theorem 1.10 has an interpretation in terms of representations of rank two quadratic forms by a fixed rank four quadratic form. Suppose \( d \equiv 1, 2(\text{mod} 4) \), then the (classes of) primitive quadratic forms of discriminant \(-4d = \text{disc}(\mathcal{O}_K)\) are given by the quadratic lattices \((a, \text{Nr}_{K/\mathbb{Q}})\) for \( a \) ranging over the primitive \( \mathcal{O}_K \)-ideals; moreover the various classes of embeddings of such a binary forms by the “four squares” quaternary quadratic form

\[
q_4(x, y, z, t) = x^2 + y^2 + z^2 + t^2
\]

are precisely described by the set of pairs

\[
\{(x, [a]x), \ x \in \mathcal{R}_3(d)\}.
\]

In particular, Theorem 1.10 and 1.11 translate to \( q \)-adic or archimedean equidistribution properties for the set of embeddings of some binary quadratic forms of large fundamental discriminant: those associated to a primitive ideal of norm \( N(a) \leq d^{1/2-\varepsilon} \) and the mixing conjecture would establish this equidistribution property for all of them.

These techniques and interpretation apply with little changes when \( q_4 \) is replaced by an integral anisotropic quaternary form; in particular, if the number of genus classes of this form is greater than 1 (eg. for definite forms), the appropriate analog of Theorem 1.10 or the corresponding mixing conjecture shows (in a way similar to [EV08]) that the Hasse principle holds of the corresponding binary forms when their discriminant gets sufficiently large. Alternatively this technique could be seen as providing non-trivial bound for some Fourier coefficients of Siegel modular forms of genus 2 (Yoshida lifts) and the mixing conjecture would provide such bounds with no restriction. Either of these interpretations should convey the opinion that the mixing conjecture is deep.

1.12. Another approach to Linnik’s problem: the works of Duke and Iwaniec. The condition \( d \equiv \pm 1(5) \) is stated merely for simplicity. In fact the conclusions of Theorems 1.4, 1.6, 1.8 or 1.10 continue to hold if the condition \( d \equiv \pm 1(5) \) is replaced by the more general one: given \( p > 2 \) some fixed prime,

**Linnik’s condition (at \( p \)).** The prime \( p \) splits in the quadratic field \( \mathbb{Q}(\sqrt{-d}) \).

As we will see, Linnik’s condition is genuine to the ergodic method and removing it was considered a major problem: it is only thirty years later that Duke [Duk88] resolved this problem along with other by using very different ideas and techniques (see also the independent work of Fomenko and Golubeva [FG87]). Since our main

---

\( a \) a representation of a rank \( m \) quadratic form \( (\mathbb{Z}^m, q_m) \) by a rank \( n \)-quadratic form \( (\mathbb{Z}^n, q_n) \), \( n \geq m \) is an isometric linear embedding \( \iota : \mathbb{Z}^m \rightarrow \mathbb{Z}^n \), ie. \( q_n(\iota(x)) = q_m(x) \), \( \forall x \in \mathbb{Z}^m \)
aim is to describe Linnik’s ergodic method, we will only give a brief account of Duke’s approach: for suitable test functions (harmonic homogeneous polynomials) the Weyl sums naturally associated with these equidistribution problems are Fourier coefficients of half-integral weight modular forms –this being a manifestation of the theta correspondence– and the decay of these sums is tantamount to providing non-trivial bound for these Fourier coefficients. Such bounds were proven by Iwaniec for holomorphic forms in a groundbreaking paper [Iwa87] and were generalized to general automorphic forms by Duke who applied them to solve various equidistribution problems linked to ternary definite or indefinite quadratic forms [Duk88, DSP90].

1.13. Connections to $L$-functions. One nice feature of Duke’s approach –in addition to removing Linnik’s condition entirely– is that is gives explicit (polynomial) control on the rates of equidistribution: there is an absolute constant $\eta > 0$ such that:

- the terms $o(1)$ in (1.2) (at least if $\Omega$ is sufficiently regular) and (1.3) take the shape $O(d^{-\eta/2})$;
- In the context of Theorem 1.8 if $d$ is large enough (depending on $\delta$), the number of $x \in \mathcal{B}_3(d; q)$ for which $|\text{dev}_d(x)| > \delta$ is zero, as long as $q^2 \leq d^{\eta/2}$.
- In Theorem 1.10, the multiset $\{\text{red}_q(x, [a|x], x \in \mathcal{B}_3(d))\}$ becomes equidistributed in $\mathcal{B}_3(d; q) \times \mathcal{B}_3(d; q)$ for $d \to +\infty$ as long as $N \leq d^{\eta/2}$.

The exponents $\eta$ can be explicit and, currently are relatively small.

Alternatively, it follows from the work of Waldspurger [Wal85, Wal91] that Duke’s approach is closely related to analytic properties of some $L$-functions and in particular to the subconvexity problem: the interested reader may consult [IS00, Mic07] for a general discussion of the subconvexity problem and [MV06] for its relation with Linnik’s equidistribution problem (this relation is to be discussed in much greater details in [MVb]); in addition [MV07] describes –in a slightly different context– an $L$-function approach to the mixing problem for Pic($O_K$). It turns out that the validity of the Generalized Riemann Hypothesis would solve the subconvexity problem in an optimal way, giving that any $\eta < 1/2$ is admissible.

1.14. Linnik’s ergodic method for other quadratic forms. The ergodic method applies to representation of integers by general ternary anisotropic quadratic forms. For definite forms, this shows in particular that the Hasse principle hold for sufficiently large, admissible, integers satisfying Linnik’s condition and possibly an additional natural technical assumption (coprimality with the discriminant of the form). The method will be presented in a general setting in [MV]. In the isotropic case, the method should work as well but at the price of extra complications linked to non-compactness: in that direction we can mention [ELMV09b] by M. Einsiedler, Ph. M. and A. V., which offers an ergodic theoretic proof of the distribution of the representations of large positive integers $d$ by the discriminant quadratic form $\text{disc}(a, b, c) = b^2 - 4ac$ (without Linnik’s type condition) again largely inspired by the ideas of Linnik and Skubenko.

1.15. Plan of the paper. In §2 we describe the main steps of the proof of Theorems 1.8 and 1.10. Each of these steps is then explained in detail in the remainder of the paper. The point of working with a discrete sphere $\mathcal{B}_3(d; q)$ rather than on the sphere $S_2$ is that it makes several technical details slightly simpler while
keeping intact the core of the arguments. We definitely hope that the interested reader will be able to use these ideas to shape his own proofs of Theorem 1.4 and of the corresponding analog of Theorem 1.10. Less motivated readers will find the proofs in [MV].

Part 2 concerns those parts of the proof that are most conveniently presented in classical language:
- In §4 we describe the natural action of the class group on the quotient \( \text{SO}_3(\mathbb{Z}) \backslash \mathcal{R}_3(d) \) and make it rather explicit. For that purpose, it is particularly useful to express everything in terms of quaternions. Presentations of similar material can be found in [Ven22, Ven29] and [She86]; our approach is slightly different.
- In §5 we establish the important “basic lemma” of Linnik.

Part 3 – comprised of §7 to §10 is concerned with transferring some of the key objects – \( \mathcal{R}_3(d) \), \( \mathcal{R}_3(d; q) \) – in terms of adelic quotients. This will be a key tool in proofs.

Part 4 is concerned with the part of the proof that is related to expanders.
- In §11 we prove that \( \mathcal{R}_3(d; q) \) – endowed with a graph structure that we shall describe – is an expander graph.
- In §12, we recall some basic facts from the theory of random walks on expander graphs. In particular we give a self-contained proof of a large deviation estimate (for non-backtracking paths) on such graphs.

1.16. Acknowledgements. The ideas of this paper are based on those of Linnik, and, indeed, this paper should be regarded in considerable part as an exposition of his work. This paper also draws on the ideas in the work of the latter two authors with M. Einsiedler and E. Lindenstrauss, as well as work of the first- and last- named author [ELMV09, ELMV07, ELMV09b, EV08]. The novel results of the paper were obtained in 2005; we apologize for the delay in bringing them to print.

We also thank P. Sarnak for encouragement of the project, R. Masri for reading an early version, E. Kowalski for reading a later one, J.-P. Serre and the referee for their comments and criticism; finally special thanks are due to G. Harcos who read very carefully the whole manuscript and made numerous corrections and comments on that occasion.

2. An overview of the ergodic method

We now present an overview of the proof of Theorem 1.8. We will try to isolate the main steps of the proof, each one of which contains some key results of a more general mathematical interest. In the present section, we treat each of these results as a black box; in the latter part of the paper, we “open the black boxes” one by one and provide complete proofs.

2.1. Assumptions and notations. We denote ”the sum of 3-squares” quadratic form and the associated inner product by

\[ q_3(x) = q_3(x, y, z) = x^2 + y^2 + z^2; \quad x \cdot x' = xx' + yy' + zz'; \]

Throughout the paper we shall make the following assumptions:

1. \( d \) will always denote a squarefree integer, not congruent to 7 modulo 8, and congruent to \( \pm 1 \) modulo 5.
2. \( q \) will always denote an integer prime to 30.
Remark. As pointed out in the introduction, one could replace 5 by an arbitrary fixed prime $p$ and the condition $d \equiv \pm 1$ modulo 5 by the Lindik’s condition at $p$, i.e. $p$ is split in $\mathbb{Q}(\sqrt{-d})$. The assumption that $q$ is prime to 30 is for convenience and could be removed entirely.

Write $K = \mathbb{Q}(\sqrt{-d})$; we denote by $\mathcal{O}_K$ the ring of integers of $K$, by $d_K$ its discriminant (equal to $-d$ or $-4d$) and by $\text{Pic}(\mathcal{O}_K)$ the ideal class group of $\mathcal{O}_K$. We also fix a square root of $-d$ in $K$, and denote it by $\sqrt{-d}$ without further commentary.

2.2. Some natural quotients. The problems considered in the introduction admit “obvious” symmetries owing to the evident action of $SO_3(\mathbb{Z})$ on $\mathcal{R}_3(d)$, $S_2$ or $\mathcal{R}_3(d; q)$. We denote the corresponding quotients by

\[ \tilde{\mathcal{R}}_3(d) = SO_3(\mathbb{Z})/\mathcal{R}_3(d), \quad \tilde{\mathcal{R}}_3(d; q) = SO_3(\mathbb{Z})/\mathcal{R}_3(d; q), \quad \tilde{S}_2 = SO_3(\mathbb{Z})/S_2. \]

and denote by $[x]$ the orbit $SO_3(\mathbb{Z})x$ of any element in the above sets.

For the purposes of our main theorems, there is no essential difference between working with $\mathcal{R}_3(d)$, $S_2$ or $\mathcal{R}_3(d; q)$ and working with $\tilde{\mathcal{R}}_3(d)$, $\tilde{S}_2$ or $\tilde{\mathcal{R}}_3(d; q)$ (since $SO_3(\mathbb{Z})$ is finite). It is conceptually clearer to consider the question of how $\tilde{\mathcal{R}}_3(d)$ becomes distributed in $\tilde{\mathcal{R}}_3(d; q)$ or $\tilde{S}_2$ than the similar question for $\mathcal{R}_3(d)$ and $S_2$ or $\mathcal{R}_3(d; q)$; this becomes clear when considering these problems for other ternary quadratic forms, especially indefinite ones. However, the latter formulation being slightly more classical, we will make the (slight) extra effort required to state theorems on $\mathcal{R}_3(d)$.

Recall that if $G$ is a group, a homogeneous space for $G$ is simply a set $X$ on which $G$ acts transitively (i.e. for any $x, x' \in X$, there is $g \in G$ such that $g.x = x'$). In such a case, the stabilizers of the elements of $X$ under this action are all conjugate.

**Proposition 2.3** ($\tilde{\mathcal{R}}_3(d)$ is a Pic($\mathcal{O}_K$)-homogeneous space). Let $d > 3$ be a square-free integer not congruent to 7 mod 8. Then there exists a natural action of Pic($\mathcal{O}_K$) on $\tilde{\mathcal{R}}_3(d)$, making $\tilde{\mathcal{R}}_3(d)$ into a homogeneous space for Pic($\mathcal{O}_K$). The stabilizer of any point is trivial if $d \equiv 3$ modulo 4, and the order 2 subgroup generated by a prime above 2 if $d \equiv 1, 2$ modulo 4. In particular,

\[ |\mathcal{R}_3(d)| = 24|\text{Pic}(\mathcal{O}_K)| \quad \text{when} \ d \equiv 3 \quad (8) \]

and

\[ |\mathcal{R}_3(d)| = 12|\text{Pic}(\mathcal{O}_K)| \quad \text{when} \ d \equiv 1, 2 \quad (4). \]

We discuss the precise version of this statement in [12] Proposition 4.7 and explain its adelic manifestation in [8,1].

Given $a \subset \mathcal{O}_K$ an ideal, we denote by $[a],[x]$ the action of its corresponding ideal class on some element $[x] \in \tilde{\mathcal{R}}_3(d)$.

2.4. The Pic($\mathcal{O}_K$)-action. The group Pic($\mathcal{O}_K$) is generated by the classes of primes above primes which are split or ramified in $\mathcal{O}_K$ so to describe the action on $\mathcal{R}_3(d)$ it is sufficient to describe the action of such classes. In fact we will only need the action of of ideals associated to split primes (ramified primes yields ideal classes of order two). Let $p > 2$ be a split prime (for instance for $d \equiv \pm 1(5)$, the prime 5 is split ) which is to say that the principal ideal $p\mathcal{O}_K$ factors into a product of two prime ideals

\[ p\mathcal{O}_K = p.p'. \]
We shall now realize explicitly the action of \([p]\) and the group it generates in terms of the action of \(\text{SO}_3\).

Let \(A_p\) be the set of elements of \(\text{SO}_3(\mathbb{Q})\) that have denominator \(p\) (i.e., so that \(p\delta\) is integral) and so that \(\delta \equiv 1 \mod 3\). The significance of the last condition is that it forces \(A_p\) to be a set of representatives for \(\text{SO}_3(\mathbb{Z})\)-cosets on matrices of denominator \(p\). We will see (§4.4) that \(|A_p| = p + 1\). Note that \(A_p\) is symmetric, i.e. \(\gamma \in A_p \implies \gamma^{-1} = \gamma^T \in A_p\).

**Proposition 2.5** (The action of a prime ideal). Suppose that \(p > 3\) splits in \(\mathbb{Q}(\sqrt{-d})\). For \(x \in \mathcal{R}_3(d)\), exactly two of

\[
\{\gamma \cdot x, \gamma \in A_p\}
\]

belong to \(\mathcal{R}_3(d)\). The classes of those two points in \(\tilde{\mathcal{R}}_3(d)\) are \([p] \cdot [x]\) and \([p'] \cdot [x] = [p]^{-1} \cdot [x]\).

As suggested by Proposition 2.5, the action of \([p]^2\) can be lifted from \(\tilde{\mathcal{R}}_3(d)\) to \(\mathcal{R}_3(d)\). This lifting is, in fact, rather less canonical than the \(\text{Pic}(\mathcal{O}_K)\)-action on \(\tilde{\mathcal{R}}_3(d)\).

2.5.1. Example: \(p = 5\). Here

\[
A_5 = \{A, A^{-1}, B, B^{-1}, C, C^{-1}\},
\]

where \(A, B, C\) are, respectively, rotations by angles \(\cos(-4/5)\) around the \(x, y, z\) axes. Explicitly,

\[
A = \frac{1}{5} \begin{pmatrix} 5 & 0 & 0 \\ 0 & -4 & 3 \\ 0 & -3 & -4 \end{pmatrix}, B = \frac{1}{5} \begin{pmatrix} -4 & 0 & 3 \\ 0 & 5 & 0 \\ -3 & 0 & -4 \end{pmatrix}, C = \frac{1}{5} \begin{pmatrix} -4 & -3 & 0 \\ 3 & -4 & 0 \\ 0 & 0 & 5 \end{pmatrix}.
\]

The first statement of the above proposition can be easily verified directly in this case. \(\square\)

2.6. Trajectories. We can use Proposition 2.5 to determine “distinguished trajectories” in \(\mathcal{R}_3(d)\).

To start with, pick any \(x \in \mathcal{R}_3(d)\); now by Lemma 2.5 there are precisely two matrices in \(A_p\) — say \(w_1, w_0\) — such that \(w_1 \cdot x = w_0 \cdot x\) both belong to \(\mathcal{R}_3(d)\). Denote \(w_1 \cdot x\) by \(x_1\), and \(w_0 \cdot x\) by \(x_{-1}\). Similarly, there is a unique choice of matrix \(w_2 \in A_5\) such that \(w_2 \neq (w_1)^{-1}\) and \(w_2 \cdot x_1\) belongs to \(\mathcal{R}_3(d)\); we denote \(w_2 \cdot x_1\) by \(x_2\). In this way, repeated application of Lemma 2.5 gives rise to a sequence \((x_i)_{i \in \mathbb{Z}}\) in \(\mathcal{R}_3(d)\) such that \(x_0 = x\) and for any \(i\),

\[
x_i \in \mathcal{R}_3(d), \ x_{i+1} \in \{\gamma \cdot x_i, \ \gamma \in A_p\} - \{x_{i-1}\}.
\]

Alternatively, this string can be represented by the data of \(x = x_0\) and an infinite (necessarily periodic) word \(W_x = (w_{x,i})_{i \in \mathbb{Z}}\) in the alphabet \(A_p\), satisfying

\[
(2.1) \quad w_{x,i+1} \neq (w_{x,i})^{-1}, \ x_i = w_{x,i} \cdot x_{i-1} \in \mathcal{R}_3(d).
\]

A word \((w_i)_{i}\) satisfying the condition \(w_{i+1} \neq (w_i)^{-1}\) is called reduced; it is easy to see that \(W_x\) is the unique reduced word satisfying (2.1), up to the “switch directions” transformation given by switching \(w_i\) and \(w_{i-1}\), or, equivalently, switching \(x_i\) and \(x_{-i}\). We refer to the sequence \((x_i)_{i \in \mathbb{Z}}\) as the trajectory of \(x\).

The equivalence of this trajectory to the one defined by the action of \([p]^2\) is explained in §4.6.
2.7. Example: $p = 5$ continued. Take $d = 101$. In this case, $|\mathcal{R}_3(d)| = 168$ and $|\text{Pic}(\mathcal{O}_K)| = 14$. The points of $|\mathcal{R}_3(d)|$, up to the action of $\text{SO}_3(\mathbb{Z})$, are:

$$(10, 1, 0), \pm(9, 4, 2), \pm(8, 6, 1), \pm(7, 6, 4)$$

The trajectory containing $(10, 1, 0)$ is:

$$(10, 1, 0) \xrightarrow{B} (-8, 1, -6) \xrightarrow{C^{-1}} (7, 4, -6) \xrightarrow{B^{-1}} (-2, 4, 9) \xrightarrow{C^{-1}}$$

$$(4, -2, 9) \xrightarrow{A} (4, 7, -6) \xrightarrow{C^{-1}} (1, -8, -6) \xrightarrow{A^{-1}} (1, 10, 0) \ldots$$

$W_{(10,1,0)} = \ldots B^* C^{-1} B^{-1} C^{-1} A C^{-1} A^{-1} \ldots$

with $B^* = w_1$.

We note that after seven steps (and thus, after any multiple of seven steps) the trajectory returns to the $\text{SO}_3(\mathbb{Z})$-orbit of $(10, 1, 0)$. This periodicity of order 7 reflects the fact that the class of a prime ideal above 5 has order 7 in the class group of $\mathbb{Q}(\sqrt{-101})$, which is cyclic of order 14.

2.8. The lengths of the trajectories. We should emphasize that it is certainly possible, and in some sense probably typical, for $[p]^\mathbb{Z}$ to be all or most of $\text{Pic}(\mathcal{O}_K)$.

What we know in this direction is rather minimal. On the one hand, it is easy to see that

$$|[p]^\mathbb{Z}| \gg \log(d):$$

suppose that $p^k$ is principal for some $k \geq 1$, writing $p^k = (a + \sqrt{-db})\mathcal{O}_K$ and taking norms one has

$$p^k = a^2 + b^2d \geq b^2d \geq d/4$$

since $b \neq 0$ and $b \in \mathbb{Z}/2$. While this lower bound goes to $\infty$ with $d$, it remains quite small compared with the size of $|\text{Pic}(\mathcal{O}_K)| = d^{1/2+o(1)}$. As far as we know, it is unknown whether there exist infinitely many squarefree $d \equiv 1(20)$ such that $|[p]^\mathbb{Z}|$ is greater than some positive power of $d$.

These considerations are, of course, related to the question:

for which $d$ does the process described in Proposition 2.7 traverse all points in $\mathcal{R}_3(d)$?

This condition on $d$ turns out to be equivalent to the condition that the prime ideal $p$ above $p$ and the 2-torsion ideal class above 2 generate the ideal class group $\mathbb{Q}(\sqrt{-d})$. The question of whether this happens for infinitely many $d$ is an interesting and seemingly difficult one; heuristically it is reasonable to suppose that this happens a positive fraction of the time. It is analogous to Gauss’s famous question:

do there exist infinitely many $d > 0$ for which $\mathbb{Q}(\sqrt{d})$ has class number 1?

The prime above $p$ plays the role in our situation that a real place does in Gauss’s problem; the period of the process above is analogous to the regulator of a real quadratic field.

2.9. Trajectories on the graph $\mathcal{R}_3(d; q)$. We shall now begin to examine solutions to $x^2 + y^2 + z^2 = d$ modulo a positive integer $q$, as in Theorem 1.6. We shall suppose, as in that theorem, that $q$ is relatively prime to $6p$.

Under this assumption, the matrices $A_p = \{\gamma_1, \ldots, \gamma_{p+1}\}$ define elements in $\text{SO}_3(\mathbb{Z}/q\mathbb{Z})$ and act on $\mathcal{R}_3(d; q)$; this endows $\mathcal{R}_3(d; q)$ with a structure of a $p + 1$-regular (undirected) graph by joining each $x \in \mathcal{R}_3(d; q)$ to

$$\gamma_1 x, \ldots, \gamma_{p+1} x.$$
By an abuse of notation we shall also refer to this graph as $R_3(d; q)$. More precisely, it is a *multigraph* – we allow multiple edges between pairs of vertices, and edges joining a vertex to itself.

Now to each point $x \in R_3(d; q)$, we may associate a well-defined marked walk on the graph $R_3(d; q)$ in the following way. To a given $x \in R_3(d)$, we constructed in §2.6 a word $W_x$ and a sequence $(x_i)_{i \in \mathbb{Z}}$ of points in $R_3(d; q)$, the trajectory of $x$, which is well-defined up to the substitution $x_i \mapsto x_{i-1}$. We denote by $\Gamma_x$ the reduction of this trajectory to $R_3(d; q)$; the data of $\Gamma_x$ consists in the sequence of vertices $(x_i)_{i \in \mathbb{Z}}$ of $R_3(d; q)$ ($x_i = \text{red}_q(x_i)$), together with a marked basepoint $x_0$ and a choice, for each $i$, of an edge joining $x_i$ to $x_{i+1}$. For any integer $\ell \geq 0$, we denote by $W_x^{(\ell)}$ and $\Gamma_x^{(\ell)}$ respectively the truncated word of length $2\ell$ and the truncated walk of length $2\ell$ centered respectively at $0$ and at $x$. In other words,

$$W_x^{(\ell)} = (w_{x_{-\ell+1}}, \ldots, w_{x_\ell}), \quad \Gamma_x^{(\ell)} = (x, w_{x_{-\ell+1}}, \ldots, w_{x_\ell}).$$

Note that the trajectories arising as $\Gamma_x$ are not completely arbitrary walk on $R_3(d; q)$; the condition $w_{i+1} \neq w_{i-1}$ from §2.6 implies that $\Gamma_x$ never traverses the same edge twice in succession. (This does not, of course, forbid $\Gamma_x$ from traveling from $\overline{x}$ to $\overline{y}$ and then back to $\overline{x}$; it just has to use two distinct edges joining $\overline{x}$ and $\overline{y}$.) A non-backtracking path in $R_3(d; q)$ is a (marked) path which never traverses the same edge twice in succession; equivalently, it can be defined by the data of a marked point $\overline{x}_0$, and a word $W_x = (w_i)_{i \in \mathbb{Z}}$ satisfying $w_{i+1} \neq w_{i-1}$; the vertices $\overline{x}_i$ can be determined inductively by the rule that $\overline{x}_{i+1}$ is the vertex arrived at by following the edge labeled $w_i$ from $\overline{x}_i$.

For instance, if $d = 101, q = 7, P = (7, 4, -6)$, we have (see §2.7)

$$\gamma_{P^{-2, 2}}: \cdots \to [(3, 1, 0)] \xrightarrow{B} [(-1, 1, 1)] \xrightarrow{C^{-1}} [(0, 4, 1)] \star \xrightarrow{B^{-1}} [(-2, 4, 2)] \xrightarrow{C^{-1}} [(4, -2, 2)] \cdots$$

Here * denotes the marked vertex, and we have used square brackets $[\ldots]$ to denote reduction modulo 7.
2.10. **Spacing properties of trajectories.** Our aim is to show that the integral points \( \mathcal{A}_3(d) \) and their associated trajectories \( \{ \Gamma_x, x \in \mathcal{A}_3(d) \} \) are well distributed, in some sense, on the graph \( \mathcal{A}_3(d; q) \). (In interpreting this statement, one should imagine that \( q \) is fixed, or not increasing too quickly, whereas \( d \to \infty \).) The first proposition develops a criterion to measure the “closeness” of two trajectories:

**Proposition 2.11** (Shadowing Lemma). The truncated words \( W_x(t) \) and \( W_{x'}(t) \) coincide if and only if \( x \equiv x'(\mod q) \) and the truncated walks \( \Gamma_x^{(t)} = \Gamma_{x'}^{(t)} \) coincide if and only if, in addition \( x \equiv x'(\mod q) \). Suppose this is the case; let \( x, x' \) denote the scalar product associated with the “sum of three squares” quadratic form, then

\[ x \cdot x' \equiv d(\mod q^2), \quad x \cdot x' \equiv \pm d(p^{2t}) \]

This proposition states roughly that if two points have parallel trajectories for a long time then these points have to be \( p \)-adically close. This proposition is named after the classical “shadowing lemma” in the theory of the geodesic flow.

**Proof.** The first part of Proposition 2.11 is proved in [11.6] using geometric properties of the Bruhat-Tits building of \( \text{SO}_3(\mathbb{Q}_p) \cong \text{PGL}_2(\mathbb{Q}_p) \). As for the second part, the equality of the two truncated trajectories it equivalent to \( x \equiv x'(\mod q) \) and \( x \equiv \pm x'(\mod p^t) \). This implies that \( (x - x'), (x - x') \equiv 0(\mod p^t) \) and \( (x - x'), (x - x') \equiv 0(\mod q^2) \) hence the two congruence above since \( x \cdot x = x' \cdot x' = d \) and \( pq \) is odd.

We shall use Proposition 2.11 in conjunction with:

**Proposition 2.12** (Linnik’s basic Lemma). Let \( e \in \mathbb{Z} \) such that \( |e| \neq d \). The number of pairs \( (x, x') \in \mathcal{A}_3(d)^2 \) with dot product \( x \cdot x' = e \) is \( \ll \varepsilon d^2 \).

Observe that, by Cauchy-Schwarz, the number of such pairs is zero if \( |e| > d \) and equal to \( |\mathcal{A}_3(d)| \) if \( |e| = d \) (since then \( x = x' \)).

This Lemma is proved in [11]. It corresponds to the “basic lemma” in Linnik’s ergodic method and is in a sense, a generalization of the well known bounds

\[ \tau(d) = \sum_{ab = d} 1 \ll \varepsilon d^2, \quad r_2(d) = \sum_{a^2 + b^2 = d} 1 \ll \varepsilon d^2. \]

Indeed, bounding the divisor function \( \tau(d) \), or the number of representations \( r_2(d) \) of \( d \) as the sum of two squares, amount to bounding the number of representations of the rank 1 form \( dX^2 \) by the binary quadratic forms \( Q(x, y) = xy \) and \( Q(x, y) = x^2 + y^2 \) respectively. By comparison, Proposition 2.12 concerns the number of ways to represent the rank two form \( dX^2 + 2eXY + dY^2 \) by the rank three form \( x^2 + y^2 + z^2 \).

As a consequence of these two results we obtain the following

**Corollary 2.13.** For any \( \varepsilon > 0 \), one has

\[ |\{(x, x') \in \mathcal{A}_3(d)^2, \quad \Gamma_x^{(t)} = \Gamma_{x'}^{(t)}\}| \ll \varepsilon |\mathcal{A}_3(d)| + d^{\varepsilon} \left( 1 + \frac{d}{q^2 p^{2t}} \right). \]

**Proof.** We arrange the pairs \( (x, x') \) according to the value of their inner product \( x \cdot x' = e \) by the Shadowing Lemma, \( |e| \leq d \) and \( e \equiv \pm d(\mod p^{2t}) \), \( e \equiv d(\mod q^2) \) hence by Linnik’s basic Lemma the total number of such pairs is bounded by

\[ |\mathcal{A}_3(d)| + \sum_{|e| < d, \quad e \equiv \pm d(\mod p^{2t})} d^{\varepsilon} \ll \varepsilon |\mathcal{A}_3(d)| + d^{\varepsilon} \left( 1 + \frac{d}{q^2 p^{2t}} \right). \]
Remark. The above estimate is optimal when the two terms on the right-hand side are roughly equal, that is for $\ell$ such that
\[ q^2 p^{2\ell} \asymp d^{1/2} \asymp |\mathcal{R}_3(d)|. \]
Now $q^2 p^{2\ell} \asymp |\mathcal{R}_3(d; q)|(p+1)p^{2\ell-1}$ is approximately the number of all non-backtracking walks of length $2\ell$ on $\mathcal{R}_3(d; q)$, so this Corollary may be interpreted by saying that for this choice of $\ell$, the map $x \mapsto \Gamma_x^{(\ell)}$ from $\mathcal{R}_3(d)$ to the set of such walks is essentially bijective.

2.14. Distribution properties of random walk. The previous section has shown that the deterministic walk $\{\Gamma_x, x \in \mathcal{R}_3(d)\}$ roughly behave like (non-back tracking) random walks on the graph $\mathcal{R}_3(d; q)$. Here we discuss the distribution of such random walks; these follow from the existence of a spectral gap:

Proposition 2.15 ($\mathcal{R}_3(d; q)$ is an expander). For any $q$ coprime with $6p$, the graph $\mathcal{R}_3(d; q)$ is connected and non-bipartite. If
\[ \lambda_0 = p + 1 \geq \lambda_1 \geq \ldots \lambda_{|\mathcal{R}_3(d; q)|-1} \geq -(p + 1) \]
denote the eigenvalues of its adjacency matrix $A(\mathcal{R}_3(d; q))$, then
\[ |\lambda_j| \leq 2\sqrt{p}, \ j \neq 0. \]

This is explained in Section 11.8 using the adelic description of $\mathcal{R}_3(d; q)$. Indeed, the graphs $\mathcal{R}_3(d; q)$ are closely related to the original Ramanujan graphs of Lubotzky-Phillips-Sarnak [LPS88]. The content of this assertion is equivalent to the (optimal) Ramanujan bound on the $p$-th Fourier coefficients of weight 2 holomorphic forms of level up to $18q^2$ (due to Deligne [Del74]). However, the existence of some spectral gap, which is what we need here, follows from any nontrivial bound for these Fourier coefficients — for instance, those given by Kloosterman or Rankin (2$\sqrt{p}$ replaced by $2p^{5/6}$ and $2p^{3/4}$ respectively).

The bound on the spectral gap in Proposition 2.15 says that the family of $p+1$-valent graphs $(\mathcal{R}_3(d; q))_{q, 2p=1}$ form a family of $1 - \frac{2\sqrt{p}}{p+1}$ expander (in fact Ramanujan) graphs as $q \to \infty$. We refer to [Lub94] for an extensive and motivated discussion of expander graphs, their properties, applications, and their construction via automorphic forms.

We shall use the fact that $\mathcal{R}_3(d; q)$ is an expander through:

Proposition 2.16 (Large deviation estimates). Fix $\eta, \varepsilon > 0$. For any subset $\mathcal{B} \subset \mathcal{R}_3(d; q)$ with $|\mathcal{B}| \geq \eta |\mathcal{R}_3(d; q)|$, the fraction of non-backtracking walks $\Gamma_\mathcal{B}$ of length $2\ell$ centered at any fixed point $\mathcal{X}$ of $\mathcal{R}_3(d; q)$ which satisfy:
\[ \left| \frac{|\Gamma_\mathcal{X} \cap \mathcal{B}|}{2\ell + 1} - \frac{|\mathcal{B}|}{|\mathcal{R}_3(d; q)|} \right| \geq \varepsilon \]
is bounded by $c_1 \exp(-c_2 \ell)$, where $c_1, c_2$ depend only on $\varepsilon, \eta$.

By $|\Gamma_\mathcal{X} \cap \mathcal{B}|$ we mean the number of $i \in [-\ell + 1, \ldots, \ell]$ such that the $i$-th vertex $\mathcal{X}_i$ of $\Gamma$ is contained in $\mathcal{B}$; in other words, the “amount of time” $\gamma$ spends in $\mathcal{B}$ if one imagines moving along the trajectory at a constant speed. It is then natural to compare the portion of time spent by a path in $\mathcal{B}$ (i.e. the ratio $|\Gamma_\mathcal{X} \cap \mathcal{B}|/(2\ell + 1)$) with the probability of being in $\mathcal{B}$ (i.e. $|\mathcal{B}|/|\mathcal{R}_3(d; q)|$). Large deviation estimates
show that with high probability, long paths spend the right amount of time in any large enough subset $|B|$. Such estimates, first proved by Chernoff for complete graphs, are a well-known and useful tool in different contexts; for instance it has been fruitfully applied in computer science (see [HLW06]). We were unable to find a reference in the existing literature for the particular version we need here (a large deviation estimate for non-backtracking walks), and so give a proof from first principles in §12.2 (Proposition 12.4).

2.17. Conclusion of the proof. We conclude this section by explaining how Propositions 2.11, 2.12 and 2.16 together imply Theorem 1.8.

Let $B_\delta$ be the set of $x \in R_3(d; q)$ such that

$$\text{dev}_d(x) = \frac{|\text{red}_q^{-1}(x)|}{|R_3(d)|/|R_3(d; q)|} - 1 > \delta. \tag{2.2}$$

Suppose that $|B_\delta| \geq \eta |R_3(d; q)|$. We will derive a contradiction for fixed $\delta, \eta$ and large enough $d$. A similar bound applies to the set of $x$ for which $\text{dev}_d(x) < -\delta$; taken together these yield Theorem 1.8.

Let $B$ be a subset of $R_3(d; q)$, since the action of any $[p]^i$ on $R_3(d)$ permutes $R_3(d)$, one has for $i \in [-\ell, \ell]$

$$|\text{red}_q^{-1}(B)| = \sum_x 1 = \sum_x 1 \text{ for } x \in B \text{ and } \text{red}_q([p]^i x) \in B \tag{2.3}$$

We shall take $B = B_\delta$ and choose $\ell$ according to the remark following Corollary 2.13:

$$\frac{1}{p} |R_3(d)| < q^\nu p^{2\ell} \leq p |R_3(d)|. \tag{2.4}$$

This is possible because of the hypothesis that $q^\nu \leq d^{1/2-\nu}$.

From (2.2) and (2.3), the average value of $\frac{|\Gamma^{(\ell)}_x \cap B_\delta|}{2\ell + 1}$ as $x$ ranges over $R_3(d)$ exceeds

$$\frac{|B_\delta|}{|R_3(d; q)|} (1 + \delta) \geq \frac{|B_\delta|}{|R_3(d; q)|} + \delta \eta. \tag{2.5}$$

Since $\frac{|\Gamma^{(\ell)}_x \cap B_\delta|}{2\ell + 1} \leq 1$ for every $x$, the number of $x \in R_3(d)$ for which

$$\frac{|\Gamma^{(\ell)}_x \cap B_\delta|}{2\ell + 1} > \frac{|B_\delta|}{|R_3(d; q)|} + \delta \eta/2$$

is at least

$$\frac{\delta \eta}{2} |R_3(d)| \geq \varepsilon \delta |R_3(d)|^{1/2-\varepsilon}$$

for any $\varepsilon > 0$ (the last bound following from (1.1)).

Let $M$ be the number of non-backtracking marked paths on $R_3(d; q)$ satisfying (2.5). Given that $\ell$ is chosen so that (2.4) is valid, we see from Corollary 2.13 that the number of pairs $(x, x')$ yielding the same trajectory $\Gamma^{(\ell)}_x$ on $R_3(d; q)$ is not much
larger than the number of diagonal pairs $|\mathcal{R}_3(d)|$: i.e. is bounded by $\ll_\varepsilon d^{1/2+\varepsilon}$. It follows that

$$M \gg_{\varepsilon, \delta, \eta} d^{1/2-\varepsilon}.$$  

for any $\varepsilon > 0$.

On the other hand, we also have an upper bound for $M$. The total number of non-backtracking marked paths of length $2\ell$ on $\mathcal{R}_3(d;q)$ is on order of $p^{2\ell}|\mathcal{R}_3(d;q)| \ll_\varepsilon d^{1/2+\varepsilon}$. Proposition 2.16 says that, of these, the proportion which satisfy (2.5) is at most $d^{-\tau}$ for some $\tau = \tau(\delta, \eta) > 0$; so

$$M \ll_{\varepsilon, \delta, \eta} d^{1/2-\tau}$$

which yields a contradiction for $d$ sufficiently large.

3. Mixing

In this section we prove Theorem 1.10 following the method of proof of Theorem 1.8. Let $d \equiv \pm 1 \pmod{5}$ and let $\mathfrak{a}$ be a primitive ideal. To simplify matters slightly we describe the proof when $\mathfrak{a} = \mathfrak{p}$ is a prime ideal of norm $N = p > 5$, in particular $p$ also splits in $K$. There $\mathcal{R}_3(d;q)$ admits two structures of regular (multi)graph: the 6-valent structure defined via $A_6$ and the $p+1$-valent structure defined via $A_p$. In the sequel, to differentiate between these two superposed structures, we will note $\gamma$’s and $w$’s elements in the alphabet $A_p$ and $A_5$ respectively.

Let $\mathcal{R}_3(d; q, p)$, be the set of walks of length 1 on $\mathcal{R}_3(d; q)$ (equivalently the set of oriented vertices), that is

$$\mathcal{R}_3(d; q, p) = \{ (\mathbf{x}, \gamma), \mathbf{x} \in \mathcal{R}_3(d; q), \gamma \in A_p \} = \mathcal{R}_3(d; q) \times A_p.$$  

The set $\mathcal{R}_3(d; q, p)$ project to the $\mathcal{R}_3(d; q) \times \mathcal{R}_3(d; q)$ via the map sending each walk to its extremities:

$$\pi : \mathcal{R}_3(d; q, p) \mapsto \mathcal{R}_3(d; q) \times \mathcal{R}_3(d; q) : (\mathbf{x}, \gamma) \mapsto (\mathbf{x}, \gamma, \mathbf{x});$$  

we denote by $\mu_{d, q, p}$ the push-forward of the uniform probability measure on $\mathcal{R}_3(d; q, p)$.

$\mathcal{R}_3(d; q, p)$ is evidently a (trivial) degree $p+1$ covering of $\mathcal{R}_3(d; q)$ (via the projection to the first coordinate) and in that way inherits the 6-valent graph structure of $\mathcal{R}_3(d; q)$: for $\gamma \in A_p$, the neighbors of $(\mathbf{x}, \gamma)$ are given by $(w, \mathbf{x}, \gamma)$ for $w$ varying over $A_5$.

For $\mathbf{x} \in \mathcal{R}_3(d)$, let $\gamma_{\mathbf{x}} \in A_p$ be the matrix such that $|\mathbf{p}| \mathbf{x} = \gamma_{\mathbf{x}} \mathbf{x}$ and define

$$\text{red}_{q, p} : \mathcal{R}_3(d) \mapsto \mathcal{R}_3(d; q, p) : \mathbf{x} \mapsto (\text{red}_q(\mathbf{x}), \gamma_{\mathbf{x}}).$$  

We then define for any $(\mathbf{x}, \gamma) \in \mathcal{R}_3(d; q, p)$ the deviation

$$\text{dev}_d(\mathbf{x}, \gamma) = \frac{|\text{red}_{q, p}^{-1}(\mathbf{x}, \gamma)|}{|\mathcal{R}_3(d)|/|\mathcal{R}_3(d; q, p)|} - 1.$$  

We have the following analog to Theorem 1.8

**Theorem 3.1.** Fix $\nu, \delta > 0$ and suppose that $pq^2 \leq d^{1/2-\nu}$ and $(q, 30p) = 1$. The proportion of $(\mathbf{x}, \gamma) \in \mathcal{R}_3(d; q, p)$ for which $|\text{dev}_d(\mathbf{x}, \gamma)| > \delta$ tends to zero as $d \to \infty$ with $d \equiv \pm 1(5)$ admissible.
Remark. If $p,q$ are fixed, this implies that the multiset $\{\text{red}_q(x), x \in \mathcal{B}_3(d)\}$ becomes equidistributed w.r.t the uniform measure and (by composing with $\pi$) that the multiset $\{(x, |p|x), x \in \mathcal{B}_3(d)\}$ is equidistributed on $\mathcal{B}_3(d; q) \times \mathcal{B}_3(d; q)$ w.r.t $\mu_{d,q,p}$.

Proof. The proof is simply an adaptation of the proof of Theorem 1.8 and we will use the Linnik flow at the prime 5: let

$$\Gamma_{x, \gamma_x}^{(f)} = ((x, \gamma_x), x^{-\ell_1-1}, \ldots, x^{-\ell}) \in \mathcal{B}_3(d; q, p) \times A_5^{(f)}$$

denote the truncated trajectory of $(\text{red}_q(x), \gamma_x)$ in $\mathcal{B}_3(d; q, p)$ associated with the action of $[p_5]^{2p}$. We have the following version of the shadowing lemma

**Proposition 3.2.** If the truncated walks $\Gamma_{x, \gamma_x}^{(f)} = \Gamma_{x', \gamma_{x'}}^{(f)}$ coincide then $x, x' \equiv \pm d (\text{mod } pq^2 5^{2\ell})$.

The congruence $x, x' \equiv \pm d (\text{mod } pq^2 5^{2\ell})$ has already been discussed and the congruence $x, x' \equiv \pm d (\text{mod } p)$ follows from the equality $\gamma_x = \gamma_{x'}$ and (11.7). From this we deduce exactly as for Corollary 2.13 that for any $\varepsilon > 0$, one has

$$\left| \left\{ (x, x') \in \mathcal{B}_3(d)^2, \Gamma_{x, \gamma_x}^{(f)} = \Gamma_{x', \gamma_{x'}}^{(f)} \right\} \right| \leq \varepsilon |\mathcal{B}_3(d)| + d^2 \left( 1 + \frac{d}{pq^2 5^{2\ell}} \right).$$

Since $pq^2 \leq d^{1/2-\varepsilon}$, for $d$ large enough, we may and do choose $\ell$ so that

$$\frac{1}{5} |\mathcal{B}_3(d)| < pq^2 5^{2\ell} \leq 5|\mathcal{B}_3(d)|$$

(compare with (2.4)). Noting that $|\mathcal{B}_3(d; q, p)| = (pq^2)^{1+o(1)}$, we conclude the proof of Theorem 3.1 by repeating the argument of the proof of Theorem 1.8. $\square$

We now deduce Theorem 1.10 for this, we need the following equidistribution result which is a direct consequence of the fact that the $p + 1$-graph $\mathcal{B}_3(d; q)$ has a uniform spectral gap when $p$ varies (Proposition 2.15), and of Lemma 12.1.1 (with $\ell = 1$ and $\|T_p\| \leq 2p^2$):

**Proposition 3.3** (Equidistribution of Hecke points). As $p \to \infty$ the measure $\mu_{q,p}$ converge to the uniform measure on $\mathcal{B}_3(d; q) \times \mathcal{B}_3(d; q)$: for any $(x, x') \in \mathcal{B}_3(d; q) \times \mathcal{B}_3(d; q)$

$$\frac{|\pi^{-1}(x, x')|}{|\mathcal{B}_3(d; q, p)|} \to \frac{1}{|\mathcal{B}_3(d; q)|^2}.$$
Under the assumptions of Theorem 3.1 for \( d \) large enough, one has by Theorem 3.1

\[
\left| \{ \gamma \in A, \gamma \cdot x_1 = x_2, \ \text{dev}_d(x_1, \gamma) > \varepsilon \} \right| \leq \varepsilon |\mathcal{R}_3(d; q, p)|
\]

so that

\[
\left| (\text{red}_{q,p} \circ \pi)^{-1}(x_1, x_2) \right| \geq (1 - \varepsilon) \left| \{ \gamma \in A, \gamma \cdot x_1 = x_2 \} \right| - \varepsilon
\]

\[
= (1 - \varepsilon) \mu_{d,q,p}(x_1, x_2) - \varepsilon \geq \frac{1}{|\mathcal{R}_3(d; q)|^2} - 3\varepsilon
\]

by Proposition 3.3, for any \( \varepsilon > 0 \) and \( d \) large enough. Using this lower bound for the points in the complementary set, one deduce for any \( \varepsilon > 0 \) and \( d \) large enough

\[
\left| (\text{red}_{q,p} \circ \pi)^{-1}(x_1, x_2) \right| \leq \frac{1}{|\mathcal{R}_3(d; q)|^2} + \varepsilon.
\]

\[\square\]

Part 2. Classical theory

4. The action of the class group on \( \tilde{\mathcal{R}}_3(d) \)

We present, in Proposition 4.1, a precise version of the homogeneous space structure on \( \tilde{\mathcal{R}}_3(d) \) discussed in Proposition 2.3. As we have remarked, the basic ideas here go back to Venkov [Ven22,Ven29] and in some sense to Gauss.

It will be convenient to modify, slightly, the definition of \( \tilde{\mathcal{R}}_3(d) \) in the case when \( d \equiv 3 \) modulo 4. Let SO\(_3\)(\( \mathbb{Z} \))\(^+\) be the index-2 subgroup of SO\(_3\)(\( \mathbb{Z} \)) consisting of matrices which act on the coordinate lines via even permutations. Set

\[
\tilde{\mathcal{R}}_3(d)^+ = \begin{cases} 
\text{SO}_3(\mathbb{Z})^+ \setminus \mathcal{R}_3(d), & \text{if } d \equiv 1, 2 \text{ mod } 4 \\
\text{SO}_3(\mathbb{Z}) \setminus \mathcal{R}_3(d), & \text{if } d \equiv 3 \text{ mod } 4
\end{cases}
\]

Thus, \( \tilde{\mathcal{R}}_3(d)^+ \) and \( \tilde{\mathcal{R}}_3(d) \) are equal when \( d \equiv 3 \) modulo 4; otherwise, the former is a double cover of the latter. We shall show the

**Proposition 4.1** (Torsor structure on \( \tilde{\mathcal{R}}_3(d)^+ \)). The set \( \tilde{\mathcal{R}}_3(d)^+ \) has the structure of a torsor for Pic(\( \mathcal{O}_K \)) (this structure is characterized by the properties given in Proposition 4.7). This action of Pic(\( \mathcal{O}_K \)) descends to \( \tilde{\mathcal{R}}_3(d) \) (obvious if \( d \equiv 3(\text{mod } 4) \)), and for \( d \equiv 1, 2(\text{mod } 4) \) the stabilizer of any point of \( \tilde{\mathcal{R}}_3(d) \) is the order 2 subgroup generated by the prime ideal above 2 (which is ramified).

Recall that, given a group \( G \), a \( G \)-torsor or a principal homogeneous space for \( G \) is a space \( X \) endowed with a transitive action of \( G \) and for which the stabilizer of some (hence any) point is trivial. Observe that fixing some \( x \in X \), the map

\[ g \in G \mapsto g.x \in X \]

provides an identification of \( G \) with \( X \) as \( G \)-spaces. However, there is a priori no canonical way of choosing \( x \); thus, one may think of a torsor as a set endowed with many different identifications with \( G \) but, in general, with no canonical one. For instance, the set of \( n \)th roots of 2 is a torsor for the group \( \mu_n \) of \( n \)th roots of unity.
4.2. Quaternions. We first recall the following classical facts.

Let $B$ be the $\mathbb{Q}$-algebra of Hamilton quaternions. For

$$x = u + a.i + b.j + b.k \in B,$$

the canonical involution is noted $\overline{x} = u - a.i - b.j - b.k$, the reduced trace $\text{tr}(x) = x + \overline{x} = 2u$ and the reduced norm $\text{Nr}(x) = x.\overline{x} = u^2 + a^2 + b^2 + c^2$. Let $B^{(0)}$ denote the space of trace-free quaternions (the kernel of $\text{tr}$) also called the pure quaternions. The space $B^{(0)}$ endowed with the reduced norm is a quadratic space and the map

$$(a, b, c) \mapsto a.i + b.j + b.k$$

is an isometry between the quadratic space $(\mathbb{Q}^3, a^2 + b^2 + c^2)$ and $(B^{(0)}, \text{Nr})$. In the sequel, we will freely identify $\mathbb{Q}^3$ with $B^{(0)}$, and, in particular, consider the elements of $\mathbb{H}_3(d)$ as trace-free quaternions.

We denote by $B^\times$, $B^{(1)}$ and $PB^\times = B^\times / \mathbb{Z}(B^\times)$ respectively, the group of units of $B$, the subgroup of units of reduced norm one, and the projective group of units; these define $\mathbb{Q}$-algebraic groups, and the action of $B^\times$ on $B^{(0)}$ by conjugation: given $x \in B^\times$

$$\gamma_x : B^{(0)} \rightarrow B^{(0)} \text{ with } z \mapsto \gamma_x(z) = xzx^{-1}$$

induces a covering and an isomorphism of $\mathbb{Q}$-algebraic groups $[\text{Vig80}, \text{Th. 3.3]}$:

$$(4.2) \quad Z(B^\times) \hookrightarrow B^\times \rightarrow PB^\times \cong \text{SO}(a^2 + b^2 + c^2).$$

4.3. Integral structures. Let $B(\mathbb{Z})$ denote the ring of Hurwitz quaternions,

$$B(\mathbb{Z}) = \mathbb{Z}[i, j, k, \frac{1 + i + j + k}{2}].$$

It is well known that the ring of Hurwitz quaternions, endowed with the reduced norm $\text{Nr}$, is euclidean: for any $y, q \in B(\mathbb{Z}) - \{0\}$, there is $x, r \in B(\mathbb{Z})$ such that $\text{Nr}(r) < \text{Nr}(q)$ and $y = qx + r$ ($[\text{Sam70}, \text{§5.7}]$). This implies that any left (or right) $B(\mathbb{Z})$-ideal is a principal ideal: any finitely generated left (resp. right) $B(\mathbb{Z})$-module $I \subset B(\mathbb{Q})$ is of the form $B(\mathbb{Z})q$ (resp. $qB(\mathbb{Z})$) for some $q \in B(\mathbb{Q})$; moreover any subring of $B(\mathbb{Q})$ which is finitely generated (as a $\mathbb{Z}$-module) is conjugate to a subring of $B(\mathbb{Z})$; in particular $B(\mathbb{Z})$ is a maximal order of $B(\mathbb{Q})$ and any maximal order in $B(\mathbb{Q})$ is $B(\mathbb{Q})^\times$-conjugate to it.

Finally, under $[\text{4.1}]$, the lattice $\mathbb{Z}^3 \subset \mathbb{Q}^3$ becomes identified with the trace free integral quaternions,

$$B^{(0)}(\mathbb{Z}) = B^{(0)}(\mathbb{Q}) \cap B(\mathbb{Z}).$$

Let $\text{PB}^\times(\mathbb{Z}) \simeq \text{SO}_3(\mathbb{Z})$ be the set of element in $\text{PB}^\times(\mathbb{Q})$ leaving $B^{(0)}(\mathbb{Z})$ invariant. Obviously the rotation associated to integral quaternions of norm 1 are in $\text{PB}^\times(\mathbb{Z})$: in other terms the obvious $B^\times \rightarrow \text{PB}^\times$ induces a map $B(\mathbb{Z})^\times \rightarrow \text{PB}^\times(\mathbb{Z}) \simeq \text{SO}_3(\mathbb{Z})$; that map however is not surjective: its image (ie. $B(\mathbb{Z})^\times / \pm 1$) is the index two subgroup $\text{SO}_3(\mathbb{Z})^+$ and the complementary coset is the coset of the rotations associated with the integral quaternions of norm 2 (for instance $1 + i$):

$$\text{SO}_3(\mathbb{Z}) = \text{SO}_3(\mathbb{Z})^+ \cup \gamma_{1+i}\text{SO}_3(\mathbb{Z})^+;$$

\footnote{Indeed, given $R$ such a subring, $RB(\mathbb{Z})$ is a right $B(\mathbb{Z})$ ideal, so of the form $RB(\mathbb{Z}) = qB(\mathbb{Z})$ and $q^{-1}Rq \subset q^{-1}RRB(\mathbb{Z}) = q^{-1}RB(\mathbb{Z}) = B(\mathbb{Z})$.}
similarly, for any prime $p$, we have a local map $B(\mathbb{Z}_p) \times \rightarrow SO_3(\mathbb{Z}_p)$ which is surjective unless $p = 2$; in that later case the image has index 2 in $SO_3(\mathbb{Z}_2)$ and its non-trivial coset is that of $\gamma_{1+i}$. Considered in terms of quaternion the quotient $\tilde{\mathcal{R}}_3(d)^+$ now appear more naturally:

$$\tilde{\mathcal{R}}_3(d)^+ = B(\mathbb{Z})^+ \mathcal{R}_3(d)$$

While our primary interest will be in the Hamilton quaternions and sums of three squares, the reader will observe that much of what we state here and below is valid for more general quaternion algebras endowed with a maximal order.

4.4. The set $\mathcal{A}_p$ in terms of quaternions. Recall that we have defined (for $p \neq 3$)

$$(4.3) \quad \mathcal{A}_p = \{\delta \in SO_3(\mathbb{Q}) : p\delta \in 1 + 3M_3(\mathbb{Z})\}.$$ 

Then $\mathcal{A}_p$ is a set of representatives for $SO_3(\mathbb{Z})$-cosets on $\{\delta \in SO_3(\mathbb{Q}) : p\delta \in M_3(\mathbb{Z})\}$: this is because the reduction modulo 3 map $SO_3(\mathbb{Z}) \mapsto SO_3(\mathbb{Z}/3\mathbb{Z})$ is an isomorphism.

Observe that one may find a set of representatives for $\mathcal{A}_p$ by taking the image, under $B(\mathbb{Z}) - \{0\} \rightarrow PB^\times(\mathbb{Z})$, of a set of representatives for Hurwitz-integral quaternions of norm $p$, under the action of units. In particular, since the number of Hurwitz-integral quaternions of norm $p$ is $24(p+1)$, and there are 24 units, it follows that $|\mathcal{A}_p| = p + 1$. (Note, however, that one cannot in general lift elements of $\mathcal{A}_p$ to quaternions of norm $p$; because of the constraint modulo 3, one can in general lift only to quaternions of norm $p$ or $2p$).

4.4.1. Example: $p = 5$. The set $\mathcal{A}_5$ is the associated with quaternions of norm 10:

The integral quaternions of norm 10 can all be expressed in the form $ru$, where $u \in B(\mathbb{Z}) \times$ and $r$ is an element of

$$(4.4) \quad \mathcal{A}_5 = \{1 \pm 3i, 1 \pm 3j, 1 \pm 3k\}.$$ 

Now a direct computation shows that the action of conjugation by the six elements of $\mathcal{A}_5$ yields precisely the action of the six matrices appearing in $\S 2.6$. For example, conjugation by $1 - 3i$ acts on $B(0)$ via the rule

$i \mapsto i,$

$$j \mapsto \frac{1}{10}(1 + 3i)j(1 - 3i) = -\frac{4}{5}j + \frac{3}{5}k,$$

$$k \mapsto \frac{1}{10}(1 + 3i)k(1 - 3i) = -\frac{3}{5}j - \frac{4}{5}k$$

which corresponds to the matrix $A$ in $\S 2.4$. Observe in particular that this matrix as well as the other elements of $\mathcal{A}_5$ satisfy the congruence $(??)$.

4.5. Construction of representations using ideal classes. As a first example of the usefulness of the quaternion, let us show how to deduce the Gauss-Legendre theorem from the Hasse-Minkowski local-global principle. If $d > 0$ is not of the form $4^a(8b - 1)$, then, for any prime $p$, $d$ is representable as a sum of three squares in $\mathbb{Z}_p^3$ and since $d$ is positive, $d$ is also representable over $\mathbb{R}$. By the Hasse-Minkowski theorem (cf. Ser73 Thm. 8, p. 41), there exists $x = (a,b,c) \in \mathbb{Q}^3$ such that $a^2 + b^2 + c^2 = d$. Let $x = ai + bj + ck$; then $x^2 = -d$ so the ring $\mathbb{Z}[x] = \mathbb{Z} + \mathbb{Z}x$
is finitely generated. By 
there is \( q \in B(\mathbb{Q}) \) such that \( q\mathbb{Z}[x]q^{-1} \in B(\mathbb{Z}) \) so that 
\[ y := qxq^{-1} \in B^{(0)}(\mathbb{Z}) \] is integral and satisfies \( y^2 = -d \).

More generally, the above scheme together with the group of \( \mathcal{O}_K \)-ideal classes makes it possible to generate plenty of \textit{new} integral representations from a given one.

Any element \( x \in \mathcal{A}_3(d) \) yields an embedding of \( \mathbb{Q}(\sqrt{-d}) \) into \( B(\mathbb{Q}) \): indeed \( x^2 = -d \) and thus \( \sqrt{-d} \mapsto x \) defines an embedding
\[ \iota_x : K \mapsto \mathbb{Q}[x] \subset B(\mathbb{Q}). \]
This embedding is \textit{integral} in the following sense: let
\[ \mathcal{O}_x = B(\mathbb{Z}) \cap \mathbb{Q}[x] \]
then \( \iota_x^{-1}(\mathcal{O}_x) = \mathcal{O}_K \) is the ring of integers\(^8\) of \( K \).

Now, given such an \( x \) and given an \( \mathcal{O}_K \)-ideal \( I \subset K \) (possibly fractional), we can also construct a new integral representation \( y \in \mathcal{A}_3(d) \) from \( x \) and \( I \): the finitely generated \( \mathbb{Z} \)-module \( B(\mathbb{Z})\iota_x(I) \) is a left \( B(\mathbb{Z}) \)-ideal, so of the form \( B(\mathbb{Z})q^{-1} \) and then
\[ y = q^{-1}xq \subset B(\mathbb{Z})\iota_x(I) \]
moreover if \( I \) is replaced by \( \lambda I, \lambda \in K^\times, q \) may be replaced by \( q' = \iota_x(\lambda^{-1})q \)
and \( q^{-1}x'q' = q^{-1}\iota_x(\lambda)x\iota_x(\lambda^{-1})q = y. \)
Notice that \( q \) is defined only up to multiplication on the right by an element of \( B^\times(\mathbb{Z}) \) this implies \( y \) is well defined up to \( B^\times(\mathbb{Z}) \)-conjugacy. Since \( B^\times(\mathbb{Z})/\pm 1 \simeq \text{SO}_3(\mathbb{Z})^+ \), we obtain for \( [x] \in \tilde{\mathcal{A}}_3(d)^+ \) fixed, a well defined map
\[ [x] : [I] \in \text{Pic}(\mathcal{O}_K) \mapsto [I],[x] \in \tilde{\mathcal{A}}_3(d)^+. \]

4.6. In \( \S 8 \) we will give a adelic/group theoretic interpretation of this map and show that it defines a \( \text{Pic}(\mathcal{O}_K) \)-torsor structure on \( \tilde{\mathcal{A}}_3(d)^+ \). In the present section we review this action in more algebraic terms.

For \( x, y, q, I \) as above, one has
\[ \mathbb{Q}[x]q = q\mathbb{Q}[y] = \{ \lambda \in B(\mathbb{Q}), x\lambda = y\lambda \} \]
is a 1-dimensional left \( \mathbb{Q}[x] \)-vector space (resp. right \( \mathbb{Q}[y] \)-vector space); \( \iota_x(I)q = q\iota_y(I) \) is a lattice in \( \mathbb{Q}[x]q \) and is clearly a left (resp. right) \( \mathcal{O}_x \) (resp. \( \mathcal{O}_y \))-module which is locally free of rank 1; moreover its class, \( [\iota_x(I)q] = [\iota_x(I)] \) in \( \text{Pic}(\mathcal{O}_x) \simeq \text{Pic}(\mathcal{O}_K) \) correspond to the class \([I]\).

Conversely, for each pair of elements \( x, y \in \mathcal{A}_3(d) \) we consider the abelian group
\[ \Lambda_{x \rightarrow y} = \{ \lambda \in B(\mathbb{Z}) : x\lambda = y\lambda \}; \]
in view of the isomorphism \( \text{SO}_3(\mathbb{Q}) \cong \text{PB}^\times(\mathbb{Q}) \) there exists (by Witt’s Theorem) a \( q \in B^\times(\mathbb{Q}) \) such that \( y = q^{-1}xq \) and therefore \( \Lambda_{x \rightarrow y} \) is a lattice in \( \mathbb{Q}[x]q \) and a locally free of rank 1 left \( \mathcal{O}_x \)-module (resp. right \( \mathcal{O}_y \)-module). Indeed
\[ \Lambda_{x \rightarrow y}q^{-1} \subset \mathbb{Q}[x] \] is an \( \mathcal{O}_x \)-ideal, say \( \iota_x(I) \subset \iota_x(K) \).

In this language a more precise version of Proposition \( 4.1 \) is the following

---

\(^8\)It is an order containing \( \mathbb{Z}[\sqrt{-d}] \), integrally closed at 2, because the local order \( B(\mathbb{Z}) \otimes \mathbb{Z} \mathbb{Z}_2 \) contains all elements of \( B \otimes \mathbb{Q} \mathbb{Q}_2 \) with norm in \( \mathbb{Z}_2 \).
Proposition 4.7 (Torsor structure on \(\widetilde{\mathfrak{R}}_3(d)^+\)). The set \(\widetilde{\mathfrak{R}}_3(d)^+\) has the structure of a torsor for Pic(\(\mathcal{O}_K\)) in which the unique element of Pic(\(\mathcal{O}_K\)) mapping \([x]\) to \([y]\) is given by the class \([\Lambda_{x\rightarrow y}]\).

More precisely, for any \(x, y, z \in \mathfrak{R}_3(d)\),

A. The map
\[
\Lambda_{x\rightarrow y} \otimes_{\mathcal{O}_K} \Lambda_{y\rightarrow z} \mapsto \Lambda_{x\rightarrow z}
\]

\(\lambda \otimes \mu \mapsto \lambda \mu\)
is an \((\mathcal{O}_x, \mathcal{O}_z)\)-bimodule isomorphism;

B. The class of \(\Lambda_{x\rightarrow y}\) is trivial if and only if \(x\) and \(y\) are identified in \(\widetilde{\mathfrak{R}}_3(d)^+\);

C. For every \(x\) and every \([I]\) \(\in\) Pic(\(\mathcal{O}_K\)), there exists a \(y\) such \([\Lambda_{x\rightarrow y}] = [r_x(I)]\).

D. If \(d \equiv 1, 2\) \ modulo \(4\), and \(x \neq y \in \widetilde{\mathfrak{R}}_3(d)^+\) project to the same element of \(\mathfrak{R}_3(d)\), then \([\Lambda_{x\rightarrow y}]\) is the ideal class of a prime above \(2\).

This proposition follows either from the adelic description given in [S] or could be proven directly using the local results of [10].

5. Representations of binary quadratic forms by \(x^2 + y^2 + z^2\).

We now discuss the proof of Proposition 2.12, “Linnik’s basic lemma.” We shall, in fact, discuss two approaches; the first (5.1) is simply quoting a result of G. Pall, the bound (5.2), which in turn rests on Siegel’s mass formula; the second approach, presented in (5.3) after a preliminary discussion, is based on ideas related to [B] and gives a proof of (5.2) at least when the discriminant of the binary form is fundamental. In the related paper [ELMV09], we present a self-contained proof of (5.2) for a general integral ternary quadratic form and without any square-freeness condition.

5.1. A result of Venkov and Pall. Let \((\mathbb{Z}^m, q), (\mathbb{Z}^n, r)\) be two non-degenerate integral quadratic forms with \(m \geq n\). One says that \(Q\) represents \(R\) if there exists a \(\mathbb{Z}\)-linear map \(\iota: \mathbb{Z}^n \rightarrow \mathbb{Z}^m\) such that, for any \(x \in \mathbb{Z}^n\), \(Q(\iota(x)) = R(x)\). It follows that \(\iota\) is an embedding.

In particular, given \(x_1, x_2 \in \mathfrak{R}_3(d)\) with \(x_1, x_2 = e\), the linear map
\[
\iota: \mathbb{Z}^2 \rightarrow \mathbb{Z}x_1 + \mathbb{Z}x_2
\]
defines a representation of the binary quadratic form \(R(x, y) = dx^2 + 2cxy + dy^2\) by the ternary form \(Q(x, y, z) = x^2 + y^2 + z^2\).

Therefore, counting the number of pairs \((x_1, x_2) \in \mathfrak{R}_3(d)^2\) with \(x_1, x_2 = e\) is essentially equivalent (up to the action of the finite group SO\(_3(\mathbb{Z})\)) to counting the number of representations of \(R\) by \(Q\).

The precise computation of the number of embeddings, \(r(a, b, c)\) say, of a binary quadratic form \(ax^2 + bxy + cy^2\) into the ternary quadratic \(x^2 + y^2 + z^2\) was carried out by Venkov [Ven70, p. 168] and (in a slightly more general setting) by Pall [Pal49, Theorem 4, page 359]. His theorem gives a formula
\[
r(a, b, c) = 24 \cdot 2^\nu \cdot \prod_{p \mid (b^2 - 4ac)} r_p(a, b, c)
\]
where it follows from Pall’s result that:

(1) \(\nu\) is the number of distinct odd primes dividing the discriminant \(b^2 - 4ac\);
(2) $r_p(a, b, c)$ is bounded by an absolute constant unless $p^2 | (a, b, c)$.

In particular, it follows that
\[
|r(a, b, c)| \ll \max(a, b, c)^2,
\]
when $(a, b, c)$ has no square factor.

One way to obtain a quantitative result like (5.2) is by use of Siegel’s mass formula, combined with a computation of local densities. We will sketch in the rest of this section an alternate approach. We must first revisit the material of §4 and describe a “different” (although closely related, as we shall see) connection between $\mathfrak{S}_3(d)$ and the class group.

5.2. The orthogonal complement construction. Consider the map
\[
x \in \mathfrak{S}_3(d) \mapsto (\mathbb{Z}x) \perp = \{ \lambda \in \mathbb{Z}^3, \ x \lambda = 0 \}
\]
which associate to $x$ the rank 2 lattice of integral vectors orthogonal to $x$: this is a rank 2-quadratic lattice (when equipped with the restriction of $q_3(\cdot)$) of discriminant $-4d$. Expressed in terms of quaternion (since $x \in \mathbb{B}^0(\mathbb{Z})$)
\[
(\mathbb{Z}x) \perp = \{ \lambda \in \mathbb{B}^0(\mathbb{Z}), \ \text{tr}(x \lambda) = -x \lambda + \lambda x = 0 \} = \Lambda_{x \rightarrow -x}.
\]
Thus we obtain a map
\[
\text{Perp} : \mathfrak{S}_3(d) \rightarrow \text{Pic}(\mathcal{O}_K)
\]
Both sides admit an action of Pic($\mathcal{O}_K$); the left-hand side by means of the torsor structure described in section §4.3 and the right-hand side by multiplication. But Perp is not equivariant for this action; indeed, for $x, y$ in $\mathfrak{S}_3(d)$, one has (noting that $[\Lambda_{y \rightarrow x}] = [\Lambda_{x \rightarrow y}]$)
\[
\text{Perp}(y) = \Lambda_{y \rightarrow -y} = [\Lambda_{x \rightarrow x}][\Lambda_{x \rightarrow -x}][\Lambda_{x \rightarrow -x}][\Lambda_{x \rightarrow x}] = [\Lambda_{x \rightarrow -x}]^2 \text{Perp}(x).
\]
So Perp intertwines the action of Pic($\mathcal{O}_K$) on the left with the square of this action on the right.

It follows that the image of Perp is precisely one coset of $2 \text{Pic}(\mathcal{O}_K)$ and the cardinality of a fiber of Perp is just the order of the 2-torsion subgroup of Pic($\mathcal{O}_K$).

Remark. We have seen that $\mathfrak{T}_3(d) \perp$ can be placed in bijection with the group Pic($\mathcal{O}_K$); but there is no natural group structure on $\mathfrak{T}_3(d) \perp$, for there is no natural choice of an identity element of $\mathfrak{T}_3(d) \perp$. In other words, the torsor structure is natural but admits no natural trivialization. What the orthogonal complement construction supplies is not a trivialization of the torsor $\mathfrak{T}_3(d) \perp$, but a trivialization of its square in the group of Pic($\mathcal{O}_K$)-torsors. The square is the torsor $T$ which can be described explicitly as the set of equivalence classes of pairs $(x, y)$ under the relation $(x, y) = (\alpha x, \alpha^{-1} y)$ for all $\alpha \in \text{Pic}(\mathcal{O}_K)$. The action of $\alpha \in \text{Pic}(\mathcal{O}_K)$ sends $(x, y)$ to $(\alpha x, y)$ (or to $(x, \alpha y)$, which is the same.) Then the map sending $(x, y)$ to $[\Lambda_{x \rightarrow -y}]$ is a canonical isomorphism between $T$ and Pic($\mathcal{O}_K$).\footnote{It is irresistible to ask which coset. A quadratic form $Ax^2 + Bxy + Cy^2$ of discriminant $d$ embeds, over $\mathbb{Q}$, into $\mathbb{Z}_5^2$ with the standard quadratic form only if $(A, d/A)_p = (d, d)_p$ for every $p$ dividing $2d$; here $(a, b)_p$ is the Hilbert symbol. This condition in fact defines a coset of squares, and so describes exactly the image of Perp.}

\footnote{The situation is similar to one familiar from geometry: If $X$ is a smooth cubic plane curve over a field $k$ with Jacobian $E$, then the points $X(k)$ form a torsor for the group $E(k)$. This}
5.3. Bounds for representations, revisited. We now sketch how the “orthogonal complement construction” leads us to another proof of Proposition 2.12.

For simplicity, we consider only the case where \( b^2 - 4ac \) is of the form \(-4d\), with \( d \) squarefree and \( d \equiv 1 \) modulo 4. Given an embedding 
\[
\iota: (\mathbb{Z}^2, ax^2 + bxy + cy^2) \longmapsto (\mathbb{Z}^3, x^2 + y^2 + z^2).
\]
consider the orthocomplement inside \( \mathbb{Z}^3 \) of \( \iota(\mathbb{Z}^2) \). It is generated by a single vector \( x \in \mathbb{Z}^3 \), unique up to sign. The quadratic lattice \( x^\perp \) is plainly the same as its sublattice \( \iota(\mathbb{Z}^2) \) after tensoring with \( \mathbb{Q} \); this means it must have discriminant either \(-d\) or \(-4d\), and because \( d \equiv 1 \) mod 4, it must be the latter, and the two lattices are identical. This implies that \( x\cdot x = d \).

The embedding \( \iota \) is determined up to at most 6 possibilities (6 being the maximal number of automorphisms of a positive definite form in rank two) by \( x \). It suffices, therefore, to count the number of \( x \in \mathcal{R}_3(d) \) so that the quadratic form induced on \( x^\perp \) is isomorphic to \( (\mathbb{Z}^2, ax^2 + bxy + cy^2) \). By [5.2] this is at most \( 24|\text{Pic}(\mathcal{O}_K)|[2] \), where \([2]\) denotes 2-torsion. By genus theory we have \( |\text{Pic}(\mathcal{O}_K)|[2] \ll d^\ell \), and the bound [5.2] follows.

Part 3. Adelization

In this part, we interpret, in adelic terms, the various classical arithmetic sets discussed so far – i.e. \( \mathcal{R}_3(d) \), \( \mathcal{R}_3(d) \), \( \text{Pic}(\mathcal{O}_K) \), \( \mathcal{R}_3(d; q) \), \( \mathcal{R}_3(d; q) \) – and the various maps between them. This interpretation provide a description of the results described in Part 2 and more importantly, will used for the proof of Proposition 2.13.

The principle of adelization goes as follows: firstly we interpret the various sets above in terms of a certain subset of the set of all rational 3-dimensional lattices (the \( \text{SO}_3 \)-genus of \( \mathbb{Z}^3 \)) equipped with additional “structures”; the reduction modulo \( q \) map \( \text{red}_q \) then corresponds to a forgetful map at the level of the structure. These sets of lattices + structures come with a natural action of groups of finite adelic points of \( \text{SO}_3 \) and suitable subgroups and therefore identified with suitable adelic quotients. We start by recalling how (finite) adèles arise quite naturally in the context of rational lattices.

6. Adelic actions on rational lattices

Given \( n \geq 1 \) an integer, let \( \mathcal{L}_n(\mathbb{Q}) \) denote the set of lattices in \( \mathbb{Q}^n \) (i.e. the finitely generated \( \mathbb{Z} \) (resp. \( \mathbb{Z}_p \))-modules in \( \mathbb{Q}^n \) (resp. \( \mathbb{Q}_p^n \)) of maximal rank) and, for any prime \( p \), let \( \mathcal{L}_n(\mathbb{Q}_p) \) denote the space of lattices in \( \mathbb{Q}_p^n \) (i.e. same as above with \( \mathbb{Q} \) and \( \mathbb{Z} \) replaced by \( \mathbb{Q}_p \) and \( \mathbb{Z}_p \)).

Given \( L \in \mathcal{L}_n(\mathbb{Q}) \) and \( p \) a prime, let \( L_p \) be the closure of \( L \) in \( \mathbb{Q}_p^n \) for the \( p \)-adic topology; then \( L_p = \mathbb{Z}_p^n \) for a.e. \( p \) and (essentially by the Chinese remainder theorem) the map 
\[
L \mapsto (L_p)_{p \in \mathbb{P}}
\]
is a bijection between \( \mathcal{L}_n(\mathbb{Q}) \) and the (restricted) product 
\[
\prod_p \mathcal{L}_n(\mathbb{Q}_p) := \{(L_p)_p, L_p \in \mathcal{L}_n(\mathbb{Q}_p), L_p = \mathbb{Z}_p^n \text{ for a.e. } p \},
\]
torsor has no canonical trivialization, but the embedding of \( X \) into the plane gives a canonical trivialization of the "cube" \( X \times E X \times E X \).
whose inverse is the map

\[(L_p)_p \mapsto \bigcap_p \mathbb{Q}^n \cap L_p.\]

In particular, for each \(p\), the natural action of the \(p\)-adic linear group \(GL_n(\mathbb{Q}_p)\) on \(L_n(\mathbb{Q}_p)\) induce, via this identification, an action of that group on \(L_n(\mathbb{Q})\). All these local actions eventually combine into an action of the restricted product of these groups

\[GL_n(\mathbb{A}_f) := \prod_p GL_n(\mathbb{Q}_p) = \{(g_p)_p, g_p \in GL_n(\mathbb{Q}_p), g_p \in GL_n(\mathbb{Z}_p) \text{ for a.e. } p\},\]

which is the group of finite adelic points of \(GL_n\). This action is given explicitly by

\[(g_p)_p.L = \text{the rational lattice corresponding to the sequence } (g_p.L_p)_p.\]

This action is easily seen to be transitive and the stabilizer of \(L_0 := \mathbb{Z}^n\) is the product

\[GL_n(\hat{\mathbb{Z}}) := \prod_p GL_n(\mathbb{Z}_p).\]

In the sequel, we denote by \(\mathbb{A}_f\) the ring of finite adèles of \(\mathbb{Q}\), i.e. the restricted product

\[\prod_p \mathbb{Q}_p = \{(x_p)_p \text{ prime}, x_p \in \mathbb{Q}_p, x_p \in \mathbb{Z}_p \text{ for a.e. } p\}\]

(with respect to the sequence of compact subrings \((\mathbb{Z}_p)_p \text{ prime}\)) and by \(\mathbb{A} = \mathbb{R} \times \mathbb{A}_f\) the full ring of adèles; the field of rationals \(\mathbb{Q}\) embed diagonally into \(\mathbb{A}_f\) and \(\mathbb{A}\) so these are in fact \(\mathbb{Q}\)-algebras. We also define the subring

\[\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \subset \mathbb{A}_f;\]

for the adelic (i.e. restricted product) topology \(\hat{\mathbb{Z}}\) is the maximal compact subring of \(\mathbb{A}_f\) (and the closure of \(\mathbb{Z}\) in \(\mathbb{A}_f\)).

Finally, given \(G\), a \(\mathbb{Q}\)-algebraic group realized as a Zariski-closed subgroup of \(GL_n,\mathbb{Q}\) — we denote by \(G(\mathbb{Q})\), \(G(\mathbb{A}_f)\), \(G(\mathbb{A})\), the groups of points of \(G\) in the corresponding rings; we also put \(G(\mathbb{Z}_p) = G(\mathbb{Q}_p) \cap GL_n(\mathbb{Z}_p)\) and \(G(\hat{\mathbb{Z}}) = \prod_p G(\mathbb{Z}_p)\).

The group of rational points \(G(\mathbb{Q})\) embeds diagonally into \(G(\mathbb{A}_f)\) and \(G(\mathbb{A})\) and in that way is considered a subgroup of these groups.

6.1. Genus. In the sequel, we will consider the restriction of this action on rational lattices to subgroups of \(G(\mathbb{A}_f) \subset GL_n(\mathbb{A}_f)\) for \(G\) suitable \(\mathbb{Q}\)-algebraic subgroups of \(GL_n\); especially for the orthogonal group \(G = SO_3 < GL_3\) and some subgroups of it. This triggers the following

**Definition 6.1.** For \(G < GL_n\) a \(\mathbb{Q}\)-algebraic subgroup and \(L\) a lattice, the \(G\)-genus of \(L\) is the orbit

\[\text{genus}_G(L) := G(\mathbb{A}_f).L \subset L_n(\mathbb{Q}).\]

The subgroup of rational points \(G(\mathbb{Q}) < G(\mathbb{A}_f)\) obviously acts on \(\text{genus}_G(L)\): the set of its orbits

\[\text{[genus}_G(L)] := G(\mathbb{Q}) \backslash \text{genus}_G(L)\]
is called the set of \( G \)-genus classes of \( L \) and its cardinality is the \textit{class number of \( G \) with respect to \( L \)} (and for \( L = \mathbb{Z}^n \), more simply, the set of genus classes and the the class number of \( G \)). In particular we have the identifications

\[
\text{genus}_G(\mathbb{Z}^n) \simeq G(A_f)/G(\hat{\mathbb{Z}}), \quad [\text{genus}_G(\mathbb{Z}^n)] := G(\mathbb{Q})\backslash G(A_f)/G(\hat{\mathbb{Z}}).
\]

We refer to [Kna97] for a more complete introduction to the adelic theory of algebraic groups (in relation with automorphic forms), and to [BM66, PR94] for more extensive treatments.

6.2. Summary. We begin by summarizing [7 to 9].

We set

\[
\mathcal{P} := \{(L, x), L \in \text{genus}_{SO_3}(\mathbb{Z}^3), \ x \in L, \ \langle x, x \rangle = d\}.
\]

\[
\mathcal{P}_{(q)} := \{(L, x), L \in \text{genus}_{SO_3}(\mathbb{Z}^3), \ x \in L/qL, \ \langle x, x \rangle = d(\text{mod} \ q)\}.
\]

For the sequel, we need to fix \textit{base points} \( x_0 \in \mathcal{R}_3(d) \) and \( \bar{x}_q \in \mathcal{R}_3(d; q) \); this being done, we define

\[
K_f[q] := \ker(SO_3(\hat{\mathbb{Z}}) \to SO_3(\mathbb{Z}/q\mathbb{Z}))
\]

\[
K_f'[q] := \{g \in SO_3(\hat{\mathbb{Z}}) : g \bar{x}_q = x_q\}
\]

and denote by \( SO_{x_0} \) the stabilizer of \( x_0 \) in \( SO_3 \). We will show in the following sections how to describe \( \mathcal{R}_3(d) \) and \( \mathcal{R}_3(d; q) \) adelically, by means of a commutative diagram

\[
\begin{array}{ccc}
\mathcal{R}_3(d) & \sim & SO_3(\mathbb{Q}) \backslash \mathcal{P} \sim \SO_{x_0}(\mathbb{Q}) \backslash \SO_{x_0}(A_f)/SO_{x_0}(\hat{\mathbb{Z}}) \\
\bar{\text{red}} & & \bar{\text{red}} \\
\mathcal{R}_3(d; q) & \sim & SO_3(\mathbb{Q}) \backslash \mathcal{P}_{(q)} \sim SO_3(\mathbb{Q}) \backslash SO_3(A_f)/K_f'[q].
\end{array}
\]

We will also explain how to describe \( \mathcal{R}_3(d) \) and \( \mathcal{R}_3(d; q) \) adelically, which is slightly more involved technically (though no different conceptually).

For this we define

\[
\mathcal{Q} = \{(L, x, \theta), L \in \text{genus}_{SO_3}(\mathbb{Z}^3), \ x \in L, \ \langle x, x \rangle = d, \ \theta : L/3L \simeq (\mathbb{Z}/3\mathbb{Z})^3\}.
\]

\[
\mathcal{P}_{(3,q)} := \{(L, x, \theta), L \in \text{genus}_{SO_3}(\mathbb{Z}^3), \ x \in L/qL, \ \langle x, x \rangle \equiv d(\text{mod} \ q), \ \theta : L/3L \simeq (\mathbb{Z}/3\mathbb{Z})^3\},
\]

and, for any integer \( a \),

\[
K_f[a, q] := K_f[a] \cap K_f'[q] \subset K_f'[q].
\]

Then we have the following diagram

\[
\begin{array}{ccc}
\mathcal{R}_3(d) & \sim & SO_3(\mathbb{Q}) \backslash \mathcal{Q} \sim \SO_{x_0}(\mathbb{Q}) \backslash \SO_{x_0}(A_f) \times SO_3(\hat{\mathbb{Z}}/3\hat{\mathbb{Z}})/SO_{x_0}(\hat{\mathbb{Z}}) \\
\bar{\text{red}} & & \bar{\text{red}} \\
\mathcal{R}_3(d; q) & \sim & SO_3(\mathbb{Q}) \backslash \mathcal{P}_{(3, q)} \sim SO_3(\mathbb{Q}) \backslash SO_3(A_f)/K_f[3, q] \\
\mathcal{R}_3(d; q) & \sim & SO_3(\mathbb{Q}) \backslash \mathcal{P}_{(q)} \sim SO_3(\mathbb{Q}) \backslash SO_3(A_f)/K_f'[q].
\end{array}
\]
where the vertical arrows at the bottom are the evident surjective maps. The horizontal arrows of these diagrams are described in [7] and [8] while the vertical arrows are discussed in [4].

6.3. Convention: orthogonal groups vs. unit group of quaternions. We have already noted in [4,2] that the quadratic spaces \((\mathbb{Q}^3, a^2 + b^2 + c^2)\), \((\mathbb{B}^0, \text{Nr})\) are isometric and that the action –by conjugation– of the units of Hamilton quaternions, \(\mathbb{B}^\times\), on \(\mathbb{B}^0\) induces and isomorphism of \(\mathbb{Q}\)-algebraic groups

\[
\mathbb{B}^\times \simeq \text{SO}_3
\]

with \(\mathbb{PB}^\times = Z(\mathbb{B}^\times)\mathbb{B}^\times\) the projective group of units. In particular the group of adele points \(\mathbb{PB}^\times(\mathbb{A})\) and \(\text{SO}_3(\mathbb{A})\) get naturally identified as are their various respective subgroups. In the sequel, we shall freely use this identification, moreover we will use the same notations for various subgroups \(\mathbb{K}_f[q]\), \(\mathbb{K}'_f[q]\) etc. to denote either some subgroup in \(\text{SO}_3(\mathbb{A})\) or its image in \(\mathbb{PB}^\times(\mathbb{A})\) under the above isomorphism.

7. Adelic interpretation of \(\mathcal{R}_3(d; q)\). Let \(L_0 := \mathbb{Z}^3\). In this section we identify \(\mathcal{R}_3(d; q)\) (as well as the sphere \(S_2\)), with an adelic quotient of \(\text{SO}_3\), verifying the second lines of [6.3] and [6.5].

7.1. The \(\text{SO}_3\)-genus of \(\mathbb{Z}^3\). An adelic consequence of the fact that the ring of Hurwitz quaternion is principal (cf. [4.3]) is the following:

**Proposition.** \(\mathbb{Z}^3\) has only one \(\text{SO}_3\)-genus class:

\[
(7.1) \quad \text{SO}_3(\mathbb{A}_f) = \text{SO}_3(\mathbb{Q})\text{SO}_3(\mathbb{Z}).
\]

**Proof.** Let \(L \in \text{genus}_{\text{SO}_3}(\mathbb{A}_f)\). In particular the covolume of \(L\) equals the covolume of \(L_0\) which is one. We identify \(L_0\) with the traceless integral quaternions \(\mathbb{B}^0(\mathbb{Z})\) and \(\text{SO}_3\) with \(\mathbb{PB}^\times\); in these terms, we need to show that there is \(q \in \mathbb{B}^\times(\mathbb{Q})\) such that \(qLq^{-1} = \mathbb{B}^0(\mathbb{Z})\). By definition, there is \(q_f \in \mathbb{B}^\times(\mathbb{A}_f)\) such that

\[
L = q_f \mathbb{B}^0(\mathbb{Z})q_f^{-1}
\]

and so \(\mathcal{O} := \mathbb{Z} + L = q_f(\mathbb{Z} + \mathbb{B}^0(\mathbb{Z}))q_f^{-1}\) is a lattice in \(\mathbb{B}(\mathbb{Q})\) containing the identity and stable by multiplication, i.e. an order; hence, by [4.3] there is \(q \in \mathbb{B}^\times(\mathbb{Q})\) such that \(q\mathcal{O}q^{-1} \subset \mathbb{B}(\mathbb{Z})\) and so \(qLq^{-1} \subset \mathbb{B}^0(\mathbb{Z})\); since \(qLq^{-1}\) and \(\mathbb{B}^0(\mathbb{Z})\) have the same covolume they are equal. \(\Box\)

If we replace \(\mathbb{Z}^3\) by another lattice or \(x^2 + y^2 + z^2\) by a different ternary quadratic form \(Q\), the number of classes in the genus will not, in general, be 1.

7.2. Level structure. By construction, the quadratic form \(x^2 + y^2 + z^2\) takes integral values on any lattice \(L \in \text{genus}_{\text{SO}_3}(L_0)\). In particular, given \(q \geq 1\) an integer, the quotient lattice \(L/qL \simeq (\mathbb{Z}/q\mathbb{Z})^3\) is naturally a quadratic space for the form \(x^2 + y^2 + z^2\). A \(q\)-level structure on such a lattice is an additional datum related to \(L/qL\). Here, we will consider two type of level \(q\)-structures:

- the principal \(q\)-structure: this is the datum of an isomorphism of quadratic spaces \(\theta : L/qL \simeq (\mathbb{Z}/q\mathbb{Z})^3\). We will use this only for \(q = 3\) and mainly for cosmetic purposes.

- a weak \(q\)-structure: this is the datum of a point \(\mathbf{x} \in L/qL\) such that \(\mathbf{x}\mathbf{x} \equiv d(\text{mod } q)\) when \((d,q) = 1\). This will be the main structure considered in the present paper.
Related to these level structures are the open compact subgroups of \( SO_3(\hat{\mathbb{Z}}) \),

\[
K_f[q], \; K_f'[q], \; K_f[3, q]
\]
defined by \((6.1), (6.2), (6.4)\) relative to the choice of some base point \( x_q \in \mathcal{R}_3(d; q) \).

### 7.3. \( \mathcal{R}_3(d; q) \) as an adelic quotient.

Let us consider first the set of pairs

\[
P\langle q \rangle := \{ (L, x), \; L \in \text{genus}_{SO_3}(L_0), \; x \in L/qL, \; x.a \equiv d(\text{mod } q) \}. \]

Since \( L/qL \simeq (L \otimes \hat{\mathbb{Z}})/(L \otimes \mathbb{Z}) \), the group \( SO_3(\mathbb{A}_f) \) (and its subgroup \( SO_3(\mathbb{Q}) \)) acts diagonally on \( P\langle q \rangle \).

We start with the action of \( SO_3(\mathbb{Q}) \): by \((7.1)\) any \( SO_3(\mathbb{Q}) \)-orbit in \( P\langle q \rangle \) contains a pair of the form \((L_0, x)\) with \( x \in \mathcal{R}_3(d; q) \). Moreover if two pairs \((L_0, x)\) and \((L_0, x')\) give rise to the same \( SO_3(\mathbb{Q}) \)-orbit then \( x \) and \( x' \) differ by an element of \( SO_3(\mathbb{Q}) \cap SO_3(\hat{\mathbb{Z}}) = SO_3(\mathbb{Z}) \). It follows that the map \( x \in \mathcal{R}_3(d; q) \rightarrow (L_0, x) \in P\langle q \rangle \) induces a bijection:

\[
SO_3(\mathbb{Z}) \backslash \mathcal{R}_3(d; q) \xrightarrow{\sim} SO_3(\mathbb{Q}) \backslash P\langle q \rangle.
\]

In the sequel, we will denote by \([L, x]_q\) the \( SO_3(\mathbb{Q}) \)-orbit of the pair \((L, x)\).

Regarding the action of \( SO_3(\mathbb{A}_f) \), one has

**Lemma.** The group \( SO_3(\mathbb{A}_f) \) acts transitively: for any \( x_q \in \mathcal{R}_3(d; q) \), we have

\[
P\langle q \rangle = SO_3(\mathbb{A}_f).(L_0, x_q) \simeq SO_3(\mathbb{A}_f)/K_f'[q].
\]

**Proof.** Indeed any \((L, x) \in P\langle q \rangle \) is in the orbit of a pair of the form \((L_0, x')\) for some \( x' \in \mathcal{R}_3(d; q) \). It follows from Lemma \((7.3.1)\) below that \( SO_3(\hat{\mathbb{Z}}) \) acts transitively on \( \mathcal{R}_3(d; q) \) (through its projection to \( SO_3(\mathbb{Z}/q\mathbb{Z}) \)). Taking \( k_{x'} \in SO_3(\hat{\mathbb{Z}}) \) such that \( k_{x'} x_q = x' \), we have \( k_{x'}^{-1}(L_0, x') = (L_0, x_q) \). \( \square \)

**Lemma 7.3.1.** For any prime \( p \), the group \( SO_3(\mathbb{Z}_p) \) acts transitively on \( \mathcal{R}_3(d; \mathbb{Z}_p) \) (defined in the evident way). Consequently, \( SO_3(\hat{\mathbb{Z}}) \) acts transitively on \( \mathcal{R}_3(d; \hat{\mathbb{Z}}) \).

**Proof.** This – which can be thought of as an analogue of Witt’s theorem over \( \mathbb{Z}_p \) – is immediate from Proposition \((10.1)\) using the first case if \( p = 2 \) and the second case if \( p \) is odd. \( \square \)

We thus have \( P\langle q \rangle \simeq SO_3(\mathbb{A}_f)/K_f'[q] \). From the above discussion, we deduce that

\[
\mathcal{R}_3(d; q) \xrightarrow{\sim} SO_3(\mathbb{Q}) \backslash P\langle q \rangle \xrightarrow{\sim} SO_3(\mathbb{Q}) \backslash SO_3(\mathbb{A}_f)/K_f'[q].
\]

### 7.3.2. Lifting to \( \mathcal{R}_3(d; q) \).

This adelic realization of \( \mathcal{R}_3(d; q) \) may, in fact, be lifted to an adelic realization of \( \mathcal{R}_3(d; q) \) itself, at least when \( q \) is coprime with 3. For this we add the additional data of the principal level 3-structure discussed in \((7.2)\).

This is a little bit artificial, relying on the special fact that the reduction modulo 3 maps yields an isomorphism

\[
SO_3(\mathbb{Z}) \simeq SO_3(\mathbb{Z}/3\mathbb{Z}).
\]

Consider the set of triples

\[
P_{(3, q)} := \{(L, x, \theta), \; L \in \text{genus}_{SO_3}(L_0), \; x \in L/qL, \; x.a \equiv d(q), \; \theta : L/3L \simeq (\mathbb{Z}/3\mathbb{Z})^3\}.\]
As above, \( \text{SO}_3(A_f) \) (hence its subgroup \( \text{SO}_3(\mathbb{Q}) \)) acts diagonally on \( \mathcal{P}_{(3,q)} \): explicitly for \( g \in \text{SO}_3(A_f) \), we have

\[
g.(L, \mathbf{x}, \theta) = (g.L, g.\mathbf{x}, \theta \circ g^{-1}).
\]

We consider first the \( \text{SO}_3(\mathbb{Q}) \)-orbits in \( \mathcal{P}_{(3,q)} \). From (7.1) any \( \text{SO}_3(\mathbb{Q}) \)-orbit contains a triple of the form \((L_0, \mathbf{x}, \theta)\). Moreover, since reduction modulo 3 is an isomorphism \( \text{SO}_3(\mathbb{Z}) \simeq \text{SO}_3(\mathbb{Z}/3\mathbb{Z}) \), the map \( \mathbf{x} \mapsto (\mathbf{x}, \text{Id}) \) yields a bijection between \( \mathcal{P}_3(d; q) \) and the set of \( \text{SO}_3(\mathbb{Z}) \)-orbits of pairs \( \{ (\mathbf{x}, \theta), \mathbf{x} \in \mathcal{P}_3(d; q), \theta : (\mathbb{Z}/3\mathbb{Z})^3 \simeq (\mathbb{Z}/3\mathbb{Z})^3 \} \). From this, we deduce that the map \( \mathbf{x} \in \mathcal{P}_3(d; q) \mapsto (L_0, \mathbf{x}, \text{Id}) \in \mathcal{P}_{(3,q)} \) induces a bijection:

\[
\mathcal{P}_3(d; q) \cong \text{SO}_3(\mathbb{Q}) \setminus \mathcal{P}_{(3,q)}.
\]

Returning to the action of the whole group \( \text{SO}_3(A_f) \), we have

**Lemma.** This action is transitive: fixing \( \mathbf{x}_q \in \mathcal{P}_3(d; q) \), we have

\[
\mathcal{P}_{(3,q)} = \text{SO}_3(\mathbb{A}_f). (L_0, \mathbf{x}_q, \text{Id}).
\]

**Proof:** The proof is exactly as above: any triple is in the orbit of a triple of the form \((L_0, \mathbf{x}, \theta)\). \( \mathbf{x} \in \mathcal{P}_3(d; q) \), \( \theta : (\mathbb{Z}/3\mathbb{Z})^3 \simeq (\mathbb{Z}/3\mathbb{Z})^3 \). This follows from the fact that \( \prod_{p \mid q} \text{SO}_3(\mathbb{Z}_p) \times \text{SO}_3(\mathbb{Z}_q) \) acts transitively on the set of pairs \((\mathbf{x}, \theta)\); recall (3.21) that we are assuming that \( q \) is prime to 3.

We have \( \mathcal{P}_{(3,q)} \simeq \text{SO}_3(\mathbb{A}_f)/K_f[3,q] \). (Recall the notation from [7.2].) From this and the above discussion, it follows that the map

\[
\mathbf{x} \in \mathcal{P}_3(d; q) \mapsto (L_0, \mathbf{x}, \text{Id}) \in \mathcal{P}_{(3,q)}
\]

induces a bijective map:

\[
(7.3) \quad \mathcal{P}_3(d; q) \cong \text{SO}_3(\mathbb{Q}) \setminus \mathcal{P}_{(3,q)} \cong \text{SO}_3(\mathbb{Q}) \setminus \text{SO}_3(\mathbb{A}_f)/K_f[3,q].
\]

To resume (7.3), the arrow going from the left to the right (7.3) is obtained as follows: for \( \mathbf{x}_q' \in \mathcal{P}_3(d; q) \), let \( \kappa' \in \text{SO}_3(\mathbb{Z}) \) be such that \( \kappa.\mathbf{x}_q' = \mathbf{x}_q \); the arrow is simply

\[
\mathbf{x}_q' \mapsto [\kappa]_{q,3}
\]

where

\[
[.]_{q,3} : g_f \in \text{SO}_3(\mathbb{A}_f) \mapsto \text{SO}_3(\mathbb{Q}) \setminus \text{SO}_3(\mathbb{A}_f)/K_f'[q,3]
\]

is the canonical projection.

**7.4. The sphere as an adelic quotient.** For completeness, we recall the interpretation of sphere \( S_2 \) as an adelic quotient: this will not be used there but it is the way to proceed in order to adapt the proof of Theorems 1.6 and 1.8 to obtain Theorems 1.10 and 1.11 or to obtain hybrid equidistribution theorems. Let \( \mathbb{A} = \mathbb{R} \times A_f \) denote the full ring of adèles and \( \text{SO}_3(\mathbb{A}) = \text{SO}_3(\mathbb{R}) \times \text{SO}_3(A_f) \); by (7.1), we have

\[
\text{SO}_3(\mathbb{Z}) \setminus \text{SO}_3(\mathbb{R}) \simeq \text{SO}_3(\mathbb{Q}) \setminus \text{SO}_3(\mathbb{A})/\text{SO}_3(\widehat{\mathbb{Z}}).
\]

Since \( \text{SO}_3(\mathbb{R}) \) acts transitively on \( S_2 \), we obtain – choosing some point \( \mathbf{x}_\infty \in S_2 \) and letting

\[
K_{\infty} = \text{SO}_{x_\infty}(\mathbb{R}) \simeq \text{SO}_2(\mathbb{R})
\]

– the identification

\[
(7.4) \quad \text{SO}_3(\mathbb{Z}) \setminus S_2 \simeq \text{SO}_3(\mathbb{Q}) \setminus \text{SO}_3(\mathbb{A})/K_{\infty} \cdot \text{SO}_3(\widehat{\mathbb{Z}}).
\]
As in the previous section, we may remove the quotient by $SO_3(\mathbb{R})$ by adding the principal 3-structure and obtain

$$SO_3(\mathbb{R}) \cong SO_3(\mathbb{Q}) \backslash SO_3(\mathbb{A}) / K_f[3].$$  
(7.5)  

$$S_2 \cong SO_3(\mathbb{Q}) \backslash SO_3(\mathbb{A}) / K_\infty.K_f[3].$$

8. Adelic interpretation of $\mathcal{A}_3(d)$. 

In this section, we describe the first line of the diagrams (6.3) and (6.5).

This will be a key tool in the proof of Proposition 2.11 and Proposition 2.15. Our presentation follows that in [EV08], but we emphasize that the material is in essence classical.

8.1. As before, let $\mathcal{P}$ be the set of pairs

$$\mathcal{P} = \{(L, x), \; x \cdot x = d, \; x \in L, \; L \in \text{genus}_{SO_3}(L_0)\}.$$  

By contrast with $\mathcal{P}_{(q)}$ or $\mathcal{P}_{(3,q)}$, the set $\mathcal{P}$ carries no natural action of $SO_3(\mathbb{A}_f)$; still, the group $SO_3(\mathbb{Q})$ acts on $\mathcal{P}$ diagonally; we will denote by $[\cdot]$ the projection $\mathcal{P} \to SO_3(\mathbb{Q})/\mathcal{P}$. By (7.1), every $SO_3(\mathbb{Q})$-orbit in $\mathcal{P}$ contains an element of the form $(L_0, x)$ (for some $x \in \mathcal{A}_3(d)$); two such pairs differ by the action of a unique element of $SO_3(\mathbb{Z})$. From this it follows that the map $x \in \mathcal{A}_3(d) \mapsto (L_0, x) \in \mathcal{P}$ induces a bijective map

$$\overline{\mathcal{A}_3(d)} \cong SO_3(\mathbb{Q}) \backslash \mathcal{P}.$$  

We will now realize $SO_3(\mathbb{Q}) \backslash \mathcal{P}$ as an adelic quotient by realizing it as (the projection of) an orbit of the adelic points of a subgroup of $SO_3$.

Choose an element $x_0 \in \mathcal{A}_3(d)$, so $(L_0, x_0) \in \mathcal{P}$ and let $SO_{x_0}$ be its stabilizer in $SO_3$. Since the quadratic space is 3-dimensional, $SO_{x_0}$ is the special orthogonal group of a quadratic plane (namely $\mathbb{Q}x_0^1$), and is in fact a 1-dimensional $\mathbb{Q}$-torus.

The group $SO_{x_0}(\mathbb{A}_f)$ acts (by multiplication on the first coordinate) on the subset of $\mathcal{P}$ consisting of pairs of the form $(L, x_0)$; in particular

$$(SO_{x_0}(\mathbb{A}_f).L_0, x_0) \subset \mathcal{P}.$$  

This subset is in fact rather big: we have

**Proposition 8.2.** The map

$$t \in SO_{x_0}(\mathbb{A}_f) \to [(t.L_0, x_0)] \in SO_3(\mathbb{Q}) \backslash \mathcal{P}$$

is surjective and induces an identification

$$SO_3(\mathbb{Q}) \backslash \mathcal{P} = [SO_{x_0}(\mathbb{A}_f)(L_0, x_0)] \cong SO_{x_0}(\mathbb{Q}) \backslash SO_{x_0}(\mathbb{A}_f)/SO_{x_0}(\mathbb{Z}).$$

**Proof.** By Witt’s theorem, every $SO_3(\mathbb{Q})$-orbit in $\mathcal{P}$ is of the form $[L, x_0]$, $L \in \text{genus}_{SO_3}(L_0)$ so it suffices to show that $L \in SO_{x_0}(\mathbb{A}_f).L_0$ Write $L = gL_0$ with $g \in SO_3(\mathbb{A}_f)$. Since $L \otimes \mathbb{Z}$ contains $x_0$, $L_0 \otimes \mathbb{Z}$ contains $g^{-1}x_0$; by Lemma 7.3.1 there is an element $k$ of $SO_3(\mathbb{Z})$ which sends $x_0$ to $g^{-1}x_0$. In particular, $gk = t$ lies in $SO_{x_0}(\mathbb{A}_f)$ and $t.L_0 = gk.L_0 = g.L_0 = L$. This show the first equality; The second bijection is induced by the map $t \in SO_{x_0}(\mathbb{A}_f) \mapsto (t.L_0, x_0)$ and follows easily from the equality $SO_{x_0}(\mathbb{Q}) = SO_3(\mathbb{Q}) \cap SO_{x_0}(\mathbb{A}_f)$ and the fact that the stabilizer of $L_0$ in $SO_{x_0}(\mathbb{A}_f)$ is $SO_{x_0}(\mathbb{Z}) = SO_{x_0}(\mathbb{A}_f) \cap SO_3(\mathbb{Z})$. \qed
Hence (8.1) extends to bijections
\[ \tilde{\mathcal{F}}_3(d) \cong \text{SO}_3(\mathbb{Q})/\mathcal{P} \cong \text{SO}_x_0(\mathbb{Q})/\text{SO}_x_0(\mathbb{A}_f)/\text{SO}_x_0(\widehat{\mathbb{Z}}). \]

8.3. **Relationship with the ideal class group.** What we have done so far is plainly sufficient to prove the equidistribution of \( \tilde{\mathcal{F}}_3(d) \). However, in our case a bit more is available: since \( \text{SO}_x_0(\mathbb{A}_f) \) is commutative (being an orthogonal group in two variables) it acts transitively by multiplication on the righthand side of (8.2) \( \text{SO}_x_0(\mathbb{A}_f) \) hence on \( \text{SO}_3(\mathbb{Q})/\mathcal{P} \cong \tilde{\mathcal{F}}_3(d) \).

On \( \text{SO}_3(\mathbb{Q})/\mathcal{P} \), the action is given as follows: for \( t \in \text{SO}_x_0(\mathbb{A}_f) \) and \( [L, x_0] \in \text{SO}_3(\mathbb{Q})/\mathcal{P} \),
\[ t.[L, x_0] := [tL, x_0]. \]
This is well defined since if \( [L, x_0] = [L', x_0] \) then \( L \) and \( L' \) differ by an element \( \tau \in \text{SO}_x_0(\mathbb{Q}) \) and because of the commutativity of \( \text{SO}_x_0 \),
\[ [t\tau L, x_0] = [\tau tL, x_0] = [tL, x_0]. \]

**Remark.** This action is very specific to the three dimensional case. For instance, if one studies the representations of an integer \( d \) by a quadratic form \( Q \) of higher rank, the quotient \( \text{SO}_Q(\mathbb{Z})/\tilde{\mathcal{F}}_3(d) \), when non-empty, can always be realized as a finite disjoint union of projections of adelic orbits of \( \text{SO}_x_0(\mathbb{A}_f) \): so \( \text{SO}_Q(\mathbb{Z})/\tilde{\mathcal{F}}_3(d) \) has a description in terms of double cosets of an adelic group but it will not carry a natural action of \( \text{SO}_x_0(\mathbb{A}_f) \).

We shall now identify \( \text{SO}_x_0(\mathbb{Q})/\text{SO}_x_0(\mathbb{A}_f)/\text{SO}_x_0(\widehat{\mathbb{Z}}) \) with a quotient of the commutative group \( \text{Pic}(\mathcal{O}_K) \). Therefore, the identification (8.2) may be considered as giving an action of \( \text{Pic}(\mathcal{O}_K) \) on \( \tilde{\mathcal{F}}_3(d) \).

For this purpose, it is again most convenient to phrase everything in terms of quaternion via the identifications \( Q^3 \cong B(0)(\mathbb{Q}) \) and \( SO_3(\mathbb{Q})/\mathcal{P} \cong \text{PB}^\times \). In particular we view \( x_0 \) as a trace-free quaternion. Now the stabilizer \( \text{SO}_x_0 \cong \text{PB}^\times x_0 \) is the multiplicative group generated by (conjugations by) invertible quaternions of the form \( a + bx_0 \). In the previous section, we have defined a transitive action of \( \text{SO}_x_0(\mathbb{A}_f) \cong \text{PB}^\times x_0(\mathbb{A}_f) \) on \( \tilde{\mathcal{F}}_3(d) \).

Now, the map \( a + bx\sqrt{-d} \mapsto a + bx_0 \) defines via conjugation an isomorphism of \( \mathbb{Q} \)-algebraic groups
\[ \text{Res}_{K/\mathbb{Q}} \mathcal{G}_m/\mathcal{G}_m \cong \text{PB}^\times x_0; \]
in particular, for any \( \mathbb{Q} \)-algebra \( A \), \( \text{PB}^\times x_0(A) \cong (A \otimes \mathbb{Q} K)^\times /A^\times \).

Thus, denoting by \( \mathbb{A}_{K,f}^\times = (\mathbb{A}_f \otimes K)^\times \) the group of finite idèles of \( K \) – equivalently, the \( \mathbb{A}_f \)-valued points of \( \text{Res}_{K/\mathbb{Q}} - \text{(8.3)} \) defines an action of \( \mathbb{A}_{K,f}^\times \) on \( \tilde{\mathcal{F}}_3(d) \).

The subgroups \( \mathbb{A}_{K,f}^\times = \mathcal{G}_m(\mathbb{A}_f) \) and \( K^\times \) act trivially, as does
\[ U = \prod_p U_p \subset \mathbb{A}_{K,f}^\times, \]
the preimage of \( \text{PB}^\times x_0(\widehat{\mathbb{Z}}) \) under (8.3), and we have
\[ \tilde{\mathcal{F}}_3(d) \cong K^\times /\mathbb{A}_{K,f}^\times /U. \]

Let
\[ \mathcal{O}_K^\times = (\mathcal{O}_K \otimes \overline{\mathbb{Z}})^\times = \prod_p \mathcal{O}_{K,p}^\times \subset \mathbb{A}_{K,f}^\times; \]
clearly $\tilde{\mathcal{O}}_K^\times \subset U$ and more precisely, we have for $p \neq 2$ (since $\text{PB}^\times(\mathbb{Z}_p) \simeq \text{PGL}_2(\mathbb{Z}_p)$)

$$U_p = \mathbb{Q}_p^\times \mathcal{O}_{K,p}^\times, \text{ while for } p = 2, U_2 = \left\{ \begin{array}{ll}
\mathbb{Q}_2^\times \mathcal{O}_{K,2}^\times, & \text{ if } d \equiv 1, 2 \mod 4
\mathbb{Q}_2^\times \pi_2^2 \mathcal{O}_{K,2}^\times, & \text{ if } d \equiv 3 \mod 4,
\end{array} \right.$$ 

where in the latter case, $\pi_2 = a + \sqrt{-db} \in \mathcal{O}_{K,2}$ is an uniformizer: let us recall that $\text{PB}^\times(\mathbb{Z}_2)$ is the image of $B(\mathbb{Z}_2)^\times \cup q_2 B(\mathbb{Z}_2)^\times$ in $\text{PB}^\times(\mathbb{Q}_2)$ for $q_2 \in B(\mathbb{Z}_2)$ any quaternion whose norm has 2-adic valuation 1.

To resume, we have

\begin{equation}
(8.4)
\mathbb{A}_f^\times \tilde{\mathcal{O}}_K^\times \subset U
\end{equation}

and in particular

$$\text{Pic}(\mathcal{O}_K) \simeq K^\times \mathbb{A}_K^\times / \mathbb{A}_f^\times \tilde{\mathcal{O}}_K^\times$$

acts transitively on $\tilde{\mathcal{A}}_3(d)$. If $d \equiv 1, 2(4)$, \((8.4)\) is an equality and $\tilde{\mathcal{A}}_3(d)$ is a $\text{Pic}(\mathcal{O}_K)$-torsor while for $d \equiv 3(4)$, the kernel has order 2 and is generated by (the image of) the element $\pi_2 \in \mathcal{O}_{K,2}$; reproducing what we did for $\tilde{\mathcal{A}}_3(d)$, we find in that case, that $\tilde{\mathcal{A}}_3(d)^+$ is naturally identified with $\text{Pic}(\mathcal{O}_K)$ and is in fact a torsor.

\textbf{A priori,} the action we have defined depends on $x_0$. We verify independence in \[8.6\]

4. Lifting the action to $\tilde{\mathcal{A}}_3(d)$. As before, by introducing an extra level 3-structure, we may replace $\tilde{\mathcal{A}}_3(d)$ by its covering $\mathcal{A}_3(d)$ and obtain a lift of the action of $\text{SO}_3(\mathbb{A}_f)$ and thus of $\mathbb{A}_f^\times$ on $\tilde{\mathcal{A}}_3(d)$ to an action on $\mathcal{A}_3(d)$. Notice that this latter action is, in general, not transitive; nor does it factor through the class group, but only through a certain ray class group.

Consider the set of triples

$$Q = \{ (L, x, \theta), \ L \in \text{genus}_{\text{SO}_3}(L_0), \ x \in L, \ x \cdot x = d, \theta: L/3L \simeq (\mathbb{Z}/3\mathbb{Z})^3 \}.$$ 

Using that the reduction mod 3 map from $\text{SO}_3(\mathbb{Z})$ to $\text{SO}_3(\mathbb{Z}/3\mathbb{Z})$ is an isomorphism, we may verify as above that the map

$$\mathcal{A}_3(d) \to \text{SO}_3(\mathbb{Q})/Q, \ x \mapsto [L_0, x, \text{Id}]/3$$

is bijective.

As above, the group $\text{SO}_3(\mathbb{A}_f)$ acts on the set of triples in $Q$ of the form $(L, x_0, \theta)$ by

\begin{equation}
(8.5)
t.(L, x_0, \theta) = (t.L, x_0, \theta \circ t^{-1}).
\end{equation}

\textbf{Proposition 8.5.} The set $\text{SO}_3(\mathbb{Q})/Q$ decomposes as a disjoint union of projection of $\text{SO}_3(\mathbb{A}_f)$ of the shape $[\text{SO}_3(\mathbb{A}_f), (L, x_0, \theta)]$ which is parametrized by the orbits of $\text{SO}_3(\mathbb{Z}/3\mathbb{Z}) \simeq \text{SO}_3(\mathbb{Z}/3\mathbb{Z})$ under the action of $\text{SO}_3(\mathbb{Z})$.

\textbf{Proof.} By Witt’s Theorem every $\text{SO}_3(\mathbb{Q})$-orbit in $Q$ is of the form $[L, x_0, \theta]$ and $\text{SO}_3(\mathbb{Q})/Q$ is covered by a union of subsets of the shape $[\text{SO}_3(\mathbb{A}_f), (L, x_0, \theta)]$. This union is disjoint: if $(L', x_0, \theta') \in [\text{SO}_3(\mathbb{A}_f), (L, x_0, \theta)]$, then $L'$ can be written $L' = s_Q s_f L$ with $s_f \in \text{SO}_3(\mathbb{A}_f)$ and $s_Q \in \text{SO}_3(\mathbb{Q})$ such that $s_Q x_0 = x_0$ and $s_Q \in \text{SO}_3(\mathbb{Q})$. Finally the proof of Proposition \[8.2\] gives that these sets correspond bijectively with the set of orbits of $\text{SO}_3(\mathbb{Z}/3\mathbb{Z})$-orbits of $\text{SO}_3(\mathbb{Z}/3\mathbb{Z})$.

As above, by commutativity, the $\text{SO}_3(\mathbb{A}_f)$-action \((8.5)\) descend to an action on $\text{SO}_3(\mathbb{Q})/Q$ given by

$$t.[L, x_0, \theta] = [t.L, x_0, \theta \circ t^{-1}],$$
whose orbits corresponds to the \(SO_{x_0}(\hat{\mathbb{Z}})\)-orbits of \(SO_3(\mathbb{Z}/3\mathbb{Z})\). In other words, we have a bijection

\[
R_3(d) \sim SO_3(\mathbb{Q}) \backslash SO_{x_0}(\hat{\mathbb{Q}}) \sim SO_{x_0}(\hat{\mathbb{A}_f}) \times SO_3(\mathbb{Z}/3\mathbb{Z})/SO_{x_0}(\hat{\mathbb{Z}}),
\]

where \(SO_{x_0}(\hat{\mathbb{Z}})\) acts diagonally on the product \(SO_{x_0}(\hat{\mathbb{A}_f}) \times SO_3(\mathbb{Z}/3\mathbb{Z})\). Under this identification, the action of \(t \in SO_{x_0}(\hat{\mathbb{A}_f})\) is the one induced by

\[
t.[t', \kappa] = [tt', \kappa], \quad (t', \kappa) \in SO_{x_0}(\hat{\mathbb{A}_f}) \times SO_3(\mathbb{Z}/3\mathbb{Z}).
\]

Thus \((8.6)\) gives us the desired way to lift the action of \(\hat{\mathbb{A}}_{K,f}^X\) to \(R_3(d)\).

### 8.6. Independence w.r.t. \(x_0\)

Let us see that the above defined actions of \(\hat{\mathbb{A}}_{K,f}^X\) on \(R_3(d)\), \(\hat{R}_3(d)\) do not depend on the choice of the base point \(x_0\).

Let \(x_0' \in R_3(d)\) be another point. By Witt’s theorem \(x_0' = \rho x_0\), for some \(\rho \in \text{PB}^X(\mathbb{Q})\). Then \(\text{PB}_{x_0'}^X = \rho \text{PB}_{x_0}^X \rho^{-1}\). Let \(u = a + b\sqrt{-d}\) be an element of \(\hat{\mathbb{A}}_K^X\) \((a, b \in \mathbb{A}_f)\), and let \(t_u\) (resp. \(t_u'\)) denote the corresponding element in \(\text{PB}_{x_0}^X(\mathbb{A}_f)\) (resp. in \(\text{PB}_{x_0'}^X(\mathbb{A}_f)\)): that is \(a + bx_0\) (resp. \(a + bx_0'\)) modulo scalars. Then \(t_u' = \rho t_u \rho^{-1}\). It will suffice to see that

\[
t_u [L_0, x_0, \text{Id}]_3 = t_u' [L_0, x_0, \text{Id}]_3;
\]

the latter expression equals

\[
t_u' [L_0, \rho^{-1} x_0', \text{Id}]_3 = t_u' [\rho L_0, x_0', \rho^{-1}]_3 = [t_u' \rho L_0, x_0', \rho^{-1} t_u^{-1} \rho^{-1}]_3
\]

\[
= [t_u t_u' \rho L_0, \rho^{-1} x_0', \rho^{-1} t_u^{-1} \rho^{-1}]_3
\]

\[
= [t_u L_0, x_0, t_u^{-1}]_3 = t_u [L_0, x_0, \text{Id}]_3.
\]

\[\square\]

### 9. Adelic Interpretation of \(\text{red}_{q}: \hat{R}_3(d) \rightarrow \hat{R}_3(d; q)\).

In this section, we interpret the reduction maps, \(\text{red}_{q}\) and \(\text{red}_{\infty}\) in terms of the adelic quotients from the previous sections.

Recall that, in \((7.4), (7.2), (8.2)\) (resp. \((7.5), (7.3), (8.6)\)) we have given adelic identifications of \(S_2, R_3(d; q)\) and \(\hat{R}_3(d)\), and of their finite coverings \(S_2, R_3(d; q)\) and \(R_3(d)\).

#### 9.1. First, let us recall the identifications

\[
\hat{R}_3(d) \simeq SO_3(\mathbb{Q})/\mathcal{P}, \quad \hat{R}_3(d; q) \simeq SO_3(\mathbb{Q})/\mathcal{P}(q)
\]

where

\[
SO_3(\mathbb{Q})/\mathcal{P} = \{[L, x], L \in SO_3(\mathbb{A}_f).L_0, \ x \in L, \ x.x = d\}
\]

\[
SO_3(\mathbb{Q})/\mathcal{P}(q) = \{[L, x]_q, L \in SO_3(\mathbb{A}_f).L_0, \ x \in L/qL, \ x.x \equiv d(q)\}.
\]

The map \(\text{red}_{q}: \hat{R}_3(d) \rightarrow \hat{R}_3(d; q)\) is induced by the natural map

\[
x \in L \mapsto \overline{x} \in L/qL
\]

which we also denote \(\text{red}_{q}\).

We now explain how to write \(\text{red}_{q}\) in the adelic language. Let \(t\) be an element of \(SO_{x_0}(\mathbb{A}_f)\) and \([t]\) its double coset in \(SO_{x_0}(\mathbb{Q})\). \(SO_{x_0}(\mathbb{A}_f)/SO_{x_0}(\hat{\mathbb{Z}})\). Recall that \(x_0\)
and \( \mathfrak{x}_q \) were basepoints in \( \mathcal{R}_3(d) \) and \( \tilde{\mathcal{R}}_3(d; q) \) respectively. We will demonstrate that the reduction map \( \text{red}_q \), thought of as a map
\[
\text{red}_q : \SO_{x_0}(\mathbb{Q})/\SO_{x_0}(\mathbb{A}_f)/\SO_{x_0}(\tilde{\mathbb{Z}}) \to \SO_3(\mathbb{Q})/\SO_3(\mathbb{A}_f)/K_f[q]
\]
is the one sending \([t] \) to \([t, k_{\mathfrak{x}_0}q] \), where \( k_{\mathfrak{x}_0} \in \SO_3(\tilde{\mathbb{Z}}) \) is a fixed element satisfying \( k_{\mathfrak{x}_0}x_q \equiv x_0(\mod q) \).

**Remark.** Since \( q \) is coprime with 3 we may assume that the component of \( k_{\mathfrak{x}_0} \) at 3 is trivial.

To see this, let \( t \in \SO_{x_0}(\mathbb{A}_f) \) be a representative for one of the double cosets in \( \SO_{x_0}(\mathbb{Q})/\SO_{x_0}(\mathbb{A}_f)/\SO_{x_0}(\tilde{\mathbb{Z}}) \). We may choose \( t \) to have integral coordinates at all primes dividing \( q \). Write \( \beta = \gamma k \), with \( \gamma \in \SO_3(\mathbb{Q}) \) and \( k \in \SO_3(\tilde{\mathbb{Z}}) \). Then by the definitions of \([\begin{smallmatrix} 2 & 1 \\ 1 & 1 \end{smallmatrix}] \) and \([\begin{smallmatrix} 3 \\ 1 \\ 1 \end{smallmatrix}] \), one finds that the element of \( \SO_3(\mathbb{Z})/\mathcal{R}_3(d) \) corresponding to \( t \) is \( \gamma x_0 \), while the element of \( \SO_3(\tilde{\mathbb{Z}})/\mathcal{R}_3(d; q) \) corresponding to \( tk_{\mathfrak{x}_0} \) is \( k\mathfrak{x}_0 \). But \( \gamma k \) fixes \( x_0 \) (whence also \( \mathfrak{x}_0 \)), so the reduction of \( \gamma^{-1}x_0 \) is precisely \( k\mathfrak{x}_0 \).

Again, we can lift the situation to \( \mathcal{R}_3(d) \): there is a natural map
\[
\SO_{x_0}(\mathbb{Q})/\SO_{x_0}(\mathbb{A}_f) \times \SO(\mathbb{Z}/3\mathbb{Z})/\SO_{x_0}(\tilde{\mathbb{Z}}) \to \SO_3(\mathbb{Q})/\SO_3(\mathbb{A}_f)/K_f[3, q]
\]
which corresponds to the reduction map \( \mathcal{R}_3(d) \to \mathcal{R}_3(d; q) \). Explicitly, choosing for base points the triples \((L_0, x_0, \text{Id})\), \((L_0, x_q, \text{Id})\) the map is given by
\[
[t, \kappa] \mapsto [tk_{\mathfrak{x}_0}, k_3]
\]
where \( k_3 \in \SO_3(\mathbb{Z}_3) \) is a lift of \( \kappa \in \SO_3(\mathbb{Z}/3\mathbb{Z}) \) and \( k_{\mathfrak{x}_0} \) is as above but such that its component at the place 3 is trivial.

**Remark.** Much in the same way the map
\[
\text{red}_\infty : \mathcal{R}_3(d) \to S_2
\]
correspond to the map
\[
[t, \kappa] \mapsto [tk_{\mathfrak{x}_0}, k_3] \in \SO_3(\mathbb{Q})/\SO_3(\mathbb{A})/K_\infty K_f[3]
\]
with \( k_{\mathfrak{x}_0} \in \SO_3(\mathbb{R}) \) such that \( k_{\mathfrak{x}_0}x_\infty = x_0/d^{1/2} \) and \( k_3 \in \SO_3(\mathbb{Z}_3) \) is as above.

10. SOME LOCAL ANALYSIS

This section is purely local. We obtain here an integral version of Witt’s theorem for integral representation of squarefree integers by ternary quadratic forms over \( \mathbb{Z}_p \). This is used to prove Lemma 7.3.1. Here it will prove convenient to work in terms of quaternions.

Let \( B \) be a quaternion algebra over \( \mathbb{Q}_p \), let \( \mathcal{O} \) be a maximal order of \( B \) and \( \mathcal{O}^{(0)} \subset B^{(0)} \) be the lattice of trace zero elements in \( \mathcal{O} \). As above, conjugation by element of \( B^\times \) induces a surjective map
\[
B^\times \to \SO(B^{(0)}, \text{Nr})
\]
under which \( \mathcal{O}^\times \) maps to \( \SO(\mathcal{O}^{(0)}, \text{Nr}) \). Let \( \mathcal{O}^{(1)} \subset \mathcal{O}^\times \) be the group of norm-1 units. Let \( d \in \mathbb{Z}_p \) be squarefree (that is, \( \text{ord}_p(d) \leq 1 \)) and let \( \mathcal{O}^{(0,d)} \subset \mathcal{O}^{(0)} \) be the set of elements of \( \mathcal{O} \) with trace 0 and norm \( d \); \( \mathcal{O}^{(0,d)} \) is obviously stable under the action of \( \mathcal{O}^\times \) by conjugation.
We fix an element $x$ of $\mathcal{O}^{(0,d)}$ and, as above, write $\Lambda_{x \rightarrow y}$ (or, when no confusion is likely, just $\Lambda$) for the set of $\lambda \in \mathcal{O}$ such that

\begin{equation}
(10.1) \quad x\lambda = \lambda y.
\end{equation}

The solutions to (10.1) in $B$ form a vector space of dimension 2, so $\Lambda$ is a free $\mathbb{Z}_p$-module of rank 2.

**Proposition 10.1.** The action of $\mathcal{O}^{(1)}$ and $\mathcal{O}^\times$ on $\mathcal{O}^{(0,d)}$ can be described as follows.

- Suppose $B$ is a division algebra. Then there are two orbits of $\mathcal{O}^{(1)}$ on $\mathcal{O}^{(0,d)}$, which are interchanged by conjugation by any element of $\mathcal{O}^\times$ whose norm is not in $\text{Nr}(\mathbb{Q}_p[x])$. In particular, the special orthogonal group of $\mathcal{O}^{(0)}$ acts transitively on $\mathcal{O}^{(0,d)}$.

- Suppose $B = M_2(\mathbb{Q}_p)$. Then:
  - If $p \neq 2$ and $p$ does not divide $d$, the action of $\mathcal{O}^{(1)}$ on $\mathcal{O}^{(0,d)}$ is transitive.
  - Otherwise, there are two orbits of $\mathcal{O}^{(1)}$ on $\mathcal{O}^{(0,d)}$; they are interchanged by $\mathcal{O}^\times$, unless $p = 2$ and $d \equiv 3 \mod 4$.

**Proof.** Suppose $B$ is a division algebra. Then $\mathcal{O}$ is the unique maximal order, and consists of all elements whose norm lies in $\mathbb{Z}_p$. Let $\lambda$ be a nonzero element of $\Lambda_{x \rightarrow y}$; then $y = \lambda^{-1}x\lambda$ so conjugation by $\lambda$ is an isometry of $\mathcal{O}^{(0,d)}$ relating $x$ to $y$. This show that $\mathcal{O}^\times$, hence $\text{SO}(\mathcal{O}^{(0)}; \text{Nr})$ acts transitively on $\mathcal{O}^{(0,d)}$.

Consider $\lambda$ as above; if there is element $\alpha \in \mathbb{Q}_p[x]$ with $\text{Nr}(\alpha) = \text{Nr}(\lambda)$, then $\alpha^{-1}\lambda$ has norm 1 and to $\Lambda$; conversely, any element of $\Lambda$ of norm 1 is $\alpha^{-1}\lambda$ for some $\alpha \in \mathbb{Q}_p[x]$ whose norm agrees with that of $\lambda$. This shows that the orbits of $\mathcal{O}^{(1)}$ on $\mathcal{O}^{(0,d)}$ are naturally identified with $\mathbb{Q}_p^\times/\text{Nr}(\mathbb{Q}_p[x]^\times)$. This quotient is a group of order 2.

Now suppose that $B = M_2(\mathbb{Q}_p)$, so that we can take $\mathcal{O}^\times = \text{GL}_2(\mathbb{Z}_p)$ and $\mathcal{O}^{(1)} = \text{SL}_2(\mathbb{Z}_p)$.

Let $x = \begin{bmatrix} b & a \\ c & -b \end{bmatrix}$ be an element of $\mathcal{O}^{(0,d)}$ (so that $b^2 + ac = -d$) and $y = \begin{bmatrix} 0 & 1 \\ -d & 0 \end{bmatrix}$; then

$$
\Lambda_{x \rightarrow y} = \mathbb{Z}_p \begin{bmatrix} b & 1 \\ c & 0 \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a & 0 \\ -b & 1 \end{bmatrix}
$$

and the elements of $\text{Nr}(\Lambda_{x \rightarrow y})$ are those elements of $\mathbb{Z}_p$ represented by the quadratic form $Q = aX^2 + 2bXY - cY^2$, which has discriminant $-4d$. Thus, $x$ and $y$ are in the same orbit of $\mathcal{O}^{(1)}$ if and only if $Q$ represents 1 over $\mathbb{Z}_p$.

For all facts used below about isomorphism classes of binary quadratic forms over $\mathbb{Z}_p$, see [Jon50, §31].

First, suppose $p$ is odd. If $p$ does not divide $d$, then $Q$ is equivalent to $X^2 + dY^2$, and in particular represents 1. So in this case, $\mathcal{O}^{(1)}$ acts transitively on $\mathcal{O}^{(0,d)}$. If $p$ divides $d$, then $Q$ is equivalent to either $X^2 + dY^2$ or $\varepsilon X^2 + \varepsilon^{-1}dY^2$, where $\varepsilon \in \mathbb{Z}_p^\times$ is a nonsquare. In the former case, $y$ is in the orbit of $x$; in the latter case, $Q$ does not represent 1 and

$$
y' = \begin{bmatrix} 0 & \varepsilon \\ -\varepsilon^{-1}d & 0 \end{bmatrix}
$$
is in the orbit of \(x\). So there are two orbits, as claimed. In both cases, \(Q\) represents an element of \(\mathbb{Z}_p^\times\), so \(\mathcal{O}_d^\times\) acts transitively on \(\mathcal{O}_d^{(0,d)}\).

Now take \(p = 2\). In this case, there are always exactly two equivalence classes of binary forms of discriminant \(4d\), one of which represents 1 over \(\mathbb{Z}_2\) and the other of which does not. A representative of the non-representing forms is given by:

- \(2X^2 + 2XY + (1/2)(d + 1)Y^2\) \((d = 3 \mod 4)\)
- \(\varepsilon X^2 + \varepsilon^{-1}dY^2\) \((d = 1, 2 \mod 4)\)

where, in the latter case, \(\varepsilon \in \mathbb{Z}_2^\times\) is an element which is not a norm from \(\mathbb{Q}_2(\sqrt{-d})^\times\).

In case \(d = 1\) or 2 mod 4, we again see that either \(y\) or \(y' = \begin{bmatrix} 0 & \varepsilon \\ -\varepsilon^{-1}d & 0 \end{bmatrix}\) lies in the orbit of \(x\), so there are two orbits of \(O(1)\) on \(O(0,d)\). And again \(Q\) represents an element of \(\mathbb{Z}_p^\times\), so some element of \(O(1)\) sends \(x\) to \(y\).

In case \(d = 3\) mod 4, take

\[y' = \begin{bmatrix} 1 & -2 \\ (1/2)(d + 1) & -1 \end{bmatrix}\]

A direct computation shows that the orbit of \(x\) under \(O(1)\) contains either \(y\) or \(y'\), so again there are two orbits. In this case, the two orbits are not interchanged by \(O^\times\).

\[\square\]

Part 4. Graphs and Expanders

11. The graph structure on \(\mathcal{R}_3(d; q)\)

Let \(p > 3\) be a prime, \((p, q) = 1\), we shall now replace the role of the finite adèles \(\mathbb{A}_f\) in the bijection (7.3) by the much smaller ring \(\mathbb{Q}_p\). More precisely, we will show the existence of a bijection:

\[(11.1) \mathcal{R}_3(d; q) \cong \Gamma(3,q)\backslash SO_3(\mathbb{Q}_p)/K_p,\]

where \(\Gamma(3,q) \subset SO_3(\mathbb{Q}_p)\) is a suitable lattice (i.e. a discrete cofinite subgroup) and \(K_p\) is the maximal compact subgroup \(SO_3(\mathbb{Z}_p)\). We have

\[SO_3(\mathbb{Q}_p) \simeq PB^\times(\mathbb{Q}_p) \simeq PGL_2(\mathbb{Q}_p)\]

(since \(B(\mathbb{Q}_p) \simeq M_2(\mathbb{Q}_p)\)), therefore the quotient \(SO_3(\mathbb{Q}_p)/K_p\) is identified with

\[PGL_2(\mathbb{Q}_p)/PGL_2(\mathbb{Z}_p) =: T_p\]

which has the structure of an infinite \(p + 1\)-valent tree (namely, the Bruhat-Tits tree of \(PGL_2(\mathbb{Q}_p)\), cf. [Ser03]).

The set \(\mathcal{R}_3(d; q)\) has thus a structure of a finite quotient of \(T_p\) and we will see that this graph structure coincides with that described in §2.9. In particular, the latter is connected.

From this viewpoint, it will be possible to prove Proposition 2.11 and Proposition 2.15 (i.e. the graph \(\mathcal{R}_3(d; q)\) is an expander). The latter relies on the theory of automorphic forms, especially the Jacquet-Langlands correspondence and the work of Eichler-Shimura.

Let us mention that a good part of this section is closely related to the book of Lubotzky [Lub94], especially Chapter 6 and the Appendix, in which the reader will find a motivated discussion of the passage between automorphic forms and expanders.
11.1. \( \mathcal{R}_3(d; q) \) as a quotient of a tree. If \( w \) is an element of \( \text{PB}^\times(\mathbb{Q}_p) \), we denote by \( [w]_p \) the element of \( \text{PB}^\times(\mathbb{A}_f) \) which projects to \( w \) at the \( p \)-adic place, and to the identity everywhere else. When no confusion is likely (as in the statement of the following lemma) we will identify \( \text{PB}^\times(\mathbb{Q}_p) \) with the subgroup \([\text{PB}^\times(\mathbb{Q}_p)]_p\) of \( \text{PB}^\times(\mathbb{A}_f) \).

Lemma. One has

\[
\text{PB}^\times(\mathbb{Q}) \cdot \text{PB}^\times(\mathbb{Q}_p) \cdot K_f[3, q] = \text{PB}^\times(\mathbb{A}_f).
\]

Consequently, the map \( g \in \text{PB}^\times(\mathbb{Q}_p) \to [g]_p \in \text{PB}^\times(\mathbb{A}_f) \) yields a bijective map

\[
\Gamma_{(3,q)} \cdot \text{PB}^\times(\mathbb{Q}_p)/K_p \xrightarrow{\sim} \text{PB}^\times(\mathbb{Q}) \backslash \text{PB}^\times(\mathbb{A}_f)/K_f[3, q] \xrightarrow{\sim} \mathcal{R}_3(d; q)
\]

where \( \Gamma_{(3,q)} \) is the lattice \( \text{PB}^\times(\mathbb{Q}) \cap \text{PB}^\times(\mathbb{Q}_p) . K_f[3, q] \).

Proof. This main ingredient of the proof is the so-called strong approximation property (for simply connected semi-simple algebraic groups): we will not discuss this property in any generality and refer to [PR94 Chap. 7] for a complete treatment. Alternatively, the reader may also refer to [Vig80, Chap. III] for a discussion of the strong approximation property in the context of quaternion algebras. For now, let us merely say that, if \( \text{PB}^\times \) satisfied the strong approximation property the assertion would follow immediately; unfortunately, \( \text{PB}^\times \) is not simply connected.

One remedies this problem by passing from the \( \mathbb{Q} \)-algebraic group \( \text{PB}^\times \) to its double cover \( B^{(1)} \) (cf. [4.2]). The group \( B^{(1)} \) is simply connected and semisimple. Moreover, \( B^{(1)}(\mathbb{Q}_p) \) is noncompact. Thus, it satisfies a strong approximation property: for any open compact \( \Omega \subset B^{(1)}(\mathbb{A}_f) \), we have

\[
B^{(1)}(\mathbb{Q}) \cdot B^{(1)}(\mathbb{Q}_p). \Omega = B^{(1)}(\mathbb{A}_f).
\]

It follows that \( \text{PB}^\times(\mathbb{Q}) \cdot \text{PB}^\times(\mathbb{Q}_p). K_f[3, q] \) contains the image

\[
\Theta = B^{(1)}(\mathbb{A}_f)/\{\pm 1\}
\]

of \( B^{(1)}(\mathbb{A}_f) \) in \( \text{PB}^\times(\mathbb{A}_f) \). It will suffice, then, to verify that

\[
\text{PB}^\times(\mathbb{Q}) \cdot \Theta \cdot K_f[3, q] = \text{PB}^\times(\mathbb{A}_f);
\]

this will follow from [7.1] if \( (\Theta \cap \text{PB}^\times(\mathbb{Z})). K_f[3, q] = \text{PB}^\times(\mathbb{Z}) \); equivalently, if \( \Theta \cap \text{PB}^\times(\mathbb{Z}) \) acts transitively on \( \text{PB}^\times(\mathbb{Z})/K_f[3, q] \simeq \mathcal{R}_3(d; q) \).

In turn, it is equivalent to show that \( \Theta_{p'} \cap \text{PB}^\times(\mathbb{Z}_{p'}) \) acts transitively on \( \mathcal{R}_3(d)(\mathbb{Z}_{p'}) \) for each \( p' \mid 3q \), where \( \Theta_{p'} \) is the image of \( B^{(1)}(\mathbb{Q}_{p'}) \) in \( \text{PB}^\times(\mathbb{Q}_{p'}) \).

Recall that \( \mathcal{R}_3(d)(\mathbb{Z}_{p'}) \) is identified with \( B^{(0,d)}(\mathbb{Z}_{p'}) \), the trace 0 quaternion of norm \( d \in \mathbb{Z}_{p'}^\times \); then \( \Theta_{p'} \cap \text{PB}^\times(\mathbb{Z}_{p'}) \) contains \( B^{(1)}(\mathbb{Z}_{p'})/\{\pm 1\} \) acting by conjugation. The transitivity of this action follows from the second part of Proposition 10.1 using the fact that \( (p', 2d) = 1 \). \( \square \)

11.2. The graph structure. We can describe the (Bruhat-Tits) graph structure on

\[
\text{SO}_3(\mathbb{Q}_p)/\text{SO}_3(\mathbb{Z}_p) \simeq \text{PB}^\times(\mathbb{Q}_p)/\text{PB}^\times(\mathbb{Z}_p)
\]

in at least two equivalent ways. We write \( K_p = \text{PB}^\times(\mathbb{Z}_p) \) in what follows.
11.2.1. Recall the definition of \( A_p \) from \[4.4\].

Let now \( [\gamma_p] \in PB^\times(Q_p) \) be the corresponding element considered in the \( p \)-adic group (alternatively take any element associated with a quaternion in \( B(Z_p) \) such that the \( p \)-adic valuation of its norm is 1); then

\[
K_p[\gamma_p]K_p = \bigsqcup_{\gamma \in A_p} [\gamma]_p K_p.
\]

we join any coset \( gK_p \) to the \( p + 1 \) cosets \( g[\gamma]_p K_p : \gamma \in A_p \). The resulting structure is independent of \( \gamma_p \).

11.2.2. More intrinsically, we may identify the quotient \( SO_{3}(Q_p)/SO_{3}(Z_p) \) with the sublattices of \( Q_p^3 \) in the orbit of \( SO_{3}(Q_p), Z_p^3 \). Given any such sublattice \( L \), the quadratic form takes values in \( Z_p \) on that lattice and the induced quadratic form on \( L/pL \cong (Z_p/pZ_p)^3 \) takes values in \( Z_p/pZ_p = \mathbb{F}_p \). Since \( p \) is odd, this later quadratic form is isotropic (represent 0 non-trivially over \( \mathbb{F}_p \)): there are precisely

\[
|\mathbb{F}_p^\times|/(x, y, z) \in \mathbb{F}_p^3, x^2 + y^2 + z^2 = 0| = p + 1 = (|\mathbb{F}_p|)
\]

isotropic lines. Given such a line, we choose \( \mathbf{v} \) a vector generating it and \( \mathbf{v} \in L \) a lifting of it. For any such isotropic vector \( \mathbf{v} \) we construct the new lattice:

\[
L_{\mathbf{v}} = \langle \mathbf{v}/p \rangle + \{ z \in L : \mathbf{v}.z \equiv 0 \mod p \}.
\]

Then \( L_{\mathbf{v}} \) depends only on \( \mathbf{v} \), and belongs to \( SO_{3}(Q_p), L = SO_{3}(Q_p), Z_p^3 \) also. In particular, we construct \( p + 1 \) such \( L_{\mathbf{v}} \), which we declare to be the neighbours of \( L \).

This defines a graph structure on \( SO_{3}(Q_p)/SO_{3}(Z_p) \) which is equivalent to the previous one: if \( L = gZ_p^3 \)

\[
\{ L_{\mathbf{v}}, \mathbf{v} \text{ isotropic} = \{ g[\gamma]_p Z_p^3, \gamma \in A_p \}.
\]

moreover

\[
(11.5) \text{ The resulting graph is a tree, i.e., is connected and has no cycles.}
\]

This later property is established using the following simple facts:

1. \( L \cap L_{\mathbf{v}} = \{ z \in L : \mathbf{v}.z \equiv 0 \mod p \} \) is the preimage under the projection \( L \mapsto L/pL \) of the plane \( \mathbf{v}^\perp \). In particular this is an index \( p \) sublattice of \( L \) and of \( L_{\mathbf{v}} \).

2. More precisely, for any \( \mathbf{v}, \mathbf{v}' \) generating distinct isotropic lines, let \( \mathbf{w} \) be a generator the (non-isotropic) line \( \langle \mathbf{v}, \mathbf{v}' \rangle^\perp \) and let \( \mathbf{w} \) be a lifting of \( \mathbf{w} \), then

\[
L = \mathbb{Z}_p \mathbf{v} + \mathbb{Z}_p \mathbf{v}' + \mathbb{Z}_p \mathbf{w}, \quad L_{\mathbf{v}} = \mathbb{Z}_p \mathbf{v}/p + \mathbb{Z}_p p \mathbf{v}' + \mathbb{Z}_p \mathbf{w},
\]

\[
L \cap L_{\mathbf{v}} = \mathbb{Z}_p \mathbf{v} + \mathbb{Z}_p p \mathbf{v}' + \mathbb{Z}_p \mathbf{w}.
\]

3. In particular for \( \mathbf{v} \neq \mathbf{v}' \)

\[
L_{\mathbf{v}} \cap L_{\mathbf{v}} = \{ z \in L : \mathbf{v}.z \equiv \mathbf{v}'.z \equiv 0 \mod p \} = \mathbb{Z}_p \mathbf{w} + pL
\]

is the preimage in \( L \) of the line \( \langle \mathbf{v}, \mathbf{v}' \rangle^\perp \).

4. Hence given three isotropic vectors \( \mathbf{v}, \mathbf{v}', \mathbf{v}'' \) generating distinct lines

\[
L_{\mathbf{v}} \cap L_{\mathbf{v}} \cap L_{\mathbf{v}''} = pL.
\]
The distance on that tree can be computed via Fact 1 above: the distance between $L, L' \in \text{SO}_3(\mathbb{Q}_p), \mathbb{Z}_p^3$ is given by

$$d(L, L') = p\text{-adic valuation of the index } [L : L \cap L'] = [L' : L \cap L'].$$

Using this one establishes the following generalization of Fact (3):

**Proposition 11.3.** Given $n \geq 1$, let $L, L', L''$ be three lattices such that $d(L, L') = d(L, L'') = n$, $d(L', L'') = 2n$; there exists $v$ some isotropic (mod $p^n$) vector $v \in L - pL$ (i.e. $v.v \equiv 0(p^n)$), and $w \in L$ with $w.w \not\equiv 0(p)$ and $v.w \equiv 0(p^n)$ so that

$$L \cap L' = \{x \in L, x.v \equiv 0(p^n)\} = \mathbb{Z}_p v + \mathbb{Z}_p w + p^n L$$

and

$$L' \cap L'' = \mathbb{Z}_p w + p^n L$$

is the preimage of a non-isotropic line, under the projection $L \mapsto L/p^n L$.

Using these remarks one can also establish the following

**Proposition 11.4.** Let $x \in L$ be such that $x.x$ is a square $\not\equiv 0(p)$, then there are exactly two distinct neighbors $L_v, L_{-v}$ of $L$ containing $x$. These are the intersection of the orbit $\text{SO}_x(\mathbb{Q}_p).L$ with the neighbors of $L$ and more generally

(i.e. an isometric embedding of $\mathbb{Z}$ in the tree w.r.t. the obvious metrics).

**Proof.** The fact that there are “at most two” neighboring lattices containing $x$ follows from Fact 1. Now $\text{SO}_x(\mathbb{Q}_p)$ is the set of rotations associated to the invertible quaternions in the quadratic algebra $\mathbb{Q}_p[x] = \mathbb{Q}_p + \mathbb{Q}_p x$. This quadratic algebra is split (i.e. $\simeq \mathbb{Q}_p \times \mathbb{Q}_p$) since $d$ is assumed to be square and in particular admits an element, $q_x \in \mathbb{Z}_p[x]$ whose norm has $p$-adic valuation 1. Let $t_x \in \text{SO}_x(\mathbb{Q}_p)$ be the associated rotation, then $t_x L$ and $t^{-1}_x L$ are the two neighboring lattices of $L$ containing $x$. One has $\mathbb{Q}_p[x]^{\times} = q^{\frac{1}{2}}_x \mathbb{Z}_p[x]^{\times}$ from which follows that

$$\text{SO}_x(\mathbb{Q}_p) = t^2_x \text{SO}_x(L)$$

($\text{SO}_x(L)$ the stabilizer of $L$ in $\text{SO}_x(\mathbb{Q}_p)$), hence

$$\text{SO}_x(\mathbb{Q}_p).L = t^2_x L$$

is an infinite geodesic in $\text{SO}_3(\mathbb{Q}_p).L$. \hfill \Box

**Remark 11.1.** If $d$ is not a square in $\mathbb{Z}_p^{\times}$, then $\mathbb{Q}_p[x]$ is a quadratic field with uniformizer $p$, then $\mathbb{Q}_p[x]^{\times} = p^2 \mathbb{Z}_p[x]^{\times}$ and $\text{SO}_x(\mathbb{Q}_p) \subset \text{SO}_3(L)$.

**Remark 11.2.** There is a further approach to study the tree structure on

$$\text{SO}_3(\mathbb{Q}_p)/\text{SO}_3(\mathbb{Z}_p) \simeq \text{PGL}_2(\mathbb{Q}_p)/\text{PGL}_2(\mathbb{Z}_p):$$

we interpret now this quotient as $[L_2(\mathbb{Q}_p)]$ the space of homothety classes of (rank 2) lattices in $\mathbb{Q}_p^2$ endowed with the natural transitive action of $\text{PGL}_2(\mathbb{Q}_p)$; this is the viewpoint taken in \cite{Ser03}. 


11.4.1. Let us now check that the neighbors of \( \mathbf{x} \in \mathfrak{R}_3(d; q) \) for the graph structure defined in \([2.9]\) correspond to the neighbors under \( T_p \) of the image of \( \mathbf{x} \) in \([7.3]\). Thus, the graph structure on \( \mathfrak{R}_3(d; q) \) coincides with the graph structure on \( \mathfrak{L}_3(q) \). In the notations of \([7.3.2]\), the neighbors of \( \mathbf{x} \) i.e. \( \{ \gamma \cdot \mathbf{x}, \gamma \in A_p \} \) correspond to the orbits of the triples

\[
\{ [L_0, \gamma \cdot \mathbf{x}, \text{Id}], \gamma \in A_p \} = \{ [\gamma^{-1} L_0, \mathbf{x}, \text{Id} \circ \gamma], \gamma \in A_p \};
\]

now for any \( p' \neq p \) and \( \gamma \in A_p, [\gamma]_{p'} \in K_{p'} \). Moreover, \( [\gamma]_3 \equiv \text{Id}(\text{mod } 3) \).

The action of \( A \) on \( \mathfrak{R}_3(d) \) is completely determined by the sequence \( \gamma \equiv \text{Id} \) (cf. \([11.2]\)) or more generally \([11.6]\)), therefore the above set equals \( \{ [\gamma^{-1}]_{p'}, [L_0, \mathbf{x}, \text{Id}], \gamma \in A_p \} \) which manifestly agrees with the graph structure introduced above.

11.5. The action of \([p]^z\). We focus now on the action of a prime ideal \( p \) above \( p \) on \( \mathfrak{R}_3(d) \). Fix \( \pi \) a uniformizer of \( K_p \), which we write in the form \( a + b\sqrt{-d} \in \mathbb{Z}_p[\sqrt{-d}] \). To any \( \mathbf{x} \in \mathfrak{R}_3(d) \) we associate the quaternion \( q_{\mathbf{x}} = a + b\mathbf{x} \) (the \( p \)-adic valuation of \( \text{Nr}(q_{\mathbf{x}}) \) equals 1) and the corresponding rotation \( t_{\mathbf{x}} \in \text{SO}_0(\mathbb{Q}_p) \) induced by conjugation by \( q_{\mathbf{x}} \); since \( K_p^* = \pi^\mathbb{Z} \mathcal{O}_K^* \), we have \( \text{SO}_0(\mathbb{Q}_p) = \pi^S \text{SO}_0(\mathbb{Z}_p) \).

The action of \( p \) can be interpreted in terms of our adelic viewpoint: We have seen in \([8.3]\) that the group \( \text{SO}_0(\mathbb{Q}_p) \) acts on \( \mathfrak{R}_3(d) \) with \( \text{SO}_0(\mathbb{Z}_p) \) acting trivially; by projection this also defines an action on \( \mathfrak{R}_3(d) \). Via the map \( \pi \mapsto q_{\mathbf{x}} \mapsto t_{\mathbf{x}} \) one obtains an action of the group \( \pi^\mathbb{Z} \) which in fact does not depend on the choice of \( \mathbf{x} \) \([8.6]\).

Let us also recall that if \( \mathbf{x} \in \mathfrak{R}_3(d) \) corresponds to the class \( [L_0, \mathbf{x}, \text{Id}] \in \text{SO}_0(\mathbb{Q}) \setminus \mathfrak{Q} \), the element \( \pi \cdot \mathbf{x} \in \mathfrak{R}_3(d) \) corresponds to the class \( t_{\mathbf{x}}[L_0, \mathbf{x}, \text{Id}] = [t_{\mathbf{x}} L_0, \mathbf{x}, \text{Id} \circ t_{\mathbf{x}}^{-1}] = [t_{\mathbf{x}} L_0, \mathbf{x}, \text{Id}] \), the final equality holding because the 3-component of \( t_{\mathbf{x}} \) is trivial. Therefore the trajectory \( \pi^z \cdot \mathbf{x} \) is described by the infinite sequence of lattices

\[
\ldots, L_{-2}, L_{-1}, L_0, L_1, L_2, \ldots, L_i = t_{\mathbf{x}} L_0.
\]

All the \( L_i \) contain \( \mathbf{x} \). Write \( L_{i,p'} = L_i \otimes \mathbb{Z}_{p'} \); then \( L_{i, p'} = L_{0, p'} \) for all \( i \) and all \( p' \neq p \), the \( p' \)-th component of \( t_{\mathbf{x}} \) being trivial. So the sequence of lattices \( (L_i) \) is completely determined by the sequence \( (L_{i,p}) \) of its \( p \)-adic components.

Since the rotation \( t_{\mathbf{x}} \) comes from a quaternion whose norm has \( p \)-adic valuation equal to 1, so \( t_{\mathbf{x}}^\pm L_{0, p} = L_{0, p} \), \( A_p \) are two neighbors of \( L_{0, p} \) in the tree hence of the form \( \gamma^\mp L_{0, p} \) for \( \gamma^\pm \in A_p \) two distinct elements; in particular the two elements \( \mathbf{x} \pm := \gamma^\mp \mathbf{x} \) belong to \( L_{0, p} \) and to all other \( L_{0, p'} \) as well so belong to \( \mathfrak{R}_3(d) \); in addition by proposition \([11.4]\) \( \gamma^\pm \) are the only two elements of \( A_p \) such that \( \mathbf{x} \in \gamma L_{0, p} \) so for \( \gamma' \in A_p \) not \( \{ \gamma^\pm \} \), \( \gamma'^{-1} \mathbf{x} \) is not \( p \)-integral; this proves Proposition \([2.5]\).

The sequence \( (L_{i,p})_{i \in \mathbb{Z}} \) describes an infinite geodesic passing through \( L_{0, p} \) in the tree (cf. \([11.2.1]\) or more generally \([11.6]\)),

\[
\text{SO}_3(\mathbb{Q}_p).L_{0, p} \simeq \text{SO}_3(\mathbb{Q}_p)/\text{SO}_3(\mathbb{Z}_p).
\]

Up to orientation, any such geodesic may be encoded by an infinite non-backtracking word in \( A_p \) where the \( i \)-th letter connects the \((i-1)\)-st element of the geodesic along an edge of the tree to the \( i \)-th element. In the present case, the word associated with the sequence \( (L_{i,p})_{i \in \mathbb{Z}} \) is the word \( (w_i^{-1})_{i \in \mathbb{Z}} \) in the alphabet \( A_p \) satisfying

\[
L_{i,p} = g_{i-1} w_{i-1}^{-1} L_{0,p}, \text{ for } g_{i-1} \text{ such that } L_{i-1,p} = g_{i-1} L_{0,p};
\]
equivalently, \((w_i)_{i \in \mathbb{Z}} \) is the word corresponding to the trajectory of \( \mathbf{x} \) defined in \([2.6]\).
11.6. Proof of Proposition 2.11. Suppose that two points $x, x' \in \mathcal{R}_3(d)$ give rise to the same truncated word of length $2\ell$:

$$W(\ell) : [-\ell + 1, \ell] \to \mathcal{A}_p.$$  

This means exactly that the geodesics $SO_x(\mathbb{Q}_p), L_{0,p}$ and $SO_{x'}(\mathbb{Q}_p), L_{0,p}$ in the Bruhat-Tits tree coincide “from times $-\ell$ to $\ell$” or in other terms

$$L_i,p = L_i', p, i = -\ell, \ldots, \ell.$$  

In particular $x' \in L_{\ell,p} \cap L_{-\ell,p}$. The last intersection is (Prop. 11.3) a sublattice of $L_{0,p}$ of index $p^{2\ell}$; more precisely, it is the preimage in $L_{0,p}$ of the line generated by $x(\mod p^\ell)$ in $L_{0,p}/p^\ell L_{0,p}$. Thus $x$ and $x'$ are linearly dependent in $L_{0,p}$, and since both vectors have norm $d$, we have $x \equiv \pm x'$ modulo $p^\ell$. This concludes the proof of Proposition 2.11.

11.7. Proof of Proposition 3.2. We suppose only that the first letters coincide

$$w_{x,1} = w_{x',1}$$

which means precisely that $x, x'$ are both contained in (Prop. 11.3)

$$L_{0,p} \cap L_{1,p} = \{ z \in \mathbb{Z}_p^3, z\nu \equiv 0(p) \},$$

for $\nu$ a non-zero isotropic vector in $\mathbb{Z}_p^3/p\mathbb{Z}_p^3$. Since $xx = d \neq 0(p)$, $\{\nu, x\}$ form a basis of $\nu^\perp$ and we can write $x' = \alpha x + \beta \nu$ with $\alpha \neq 0$, hence

$$xx' \equiv \alpha xx \equiv \alpha d(p),$$

by symetry

$$xx' \equiv x^{-1}x'x' \equiv x^{-1}d(p) \Rightarrow \alpha = \pm 1, xx' \equiv \pm d(p).$$

11.8. Proof of Proposition 2.15. We assume some familiarity with the theory of automorphic forms; in any case, we refer to Lubotzky’s book [Lub94, Chap. 6 & Appendix].

The space $L^2(\mathbb{P}^X(\mathbb{Q}) \backslash \mathbb{P}^X(\mathbb{A}_f)/K_f[3, q])$ admits an orthogonal decomposition into eigenspaces of the commutative algebra generated by Hecke operators. These eigenspaces are the set of $\mathbb{P}^X(\mathbb{R})K_f[3, q]$-invariant vectors of automorphic representations on $\mathbb{P}^X$. Such representations are of two types:

- one-dimensional representations;
- infinite dimensional representations.

The latter corresponds, via the Jacquet-Langlands correspondence [JL70] to automorphic representations of $GL_2$ with trivial central character, which are discrete series of weight 2, unramified outside 2, 3 and outside primes dividing $q$ (more precisely, their conductor divides $18q^2$). From the work of Deligne (or rather Eichler/Igusa/Shimura since this is weight 2), the eigenvalue of the standard $p$-th Hecke operator for such spaces is bounded in absolute value by $2\sqrt{p}$.

As for the former: each such is the representation of $\mathbb{P}^X(\mathbb{A})$ on the one-dimensional subspace generated by the function

$$g \in \mathbb{P}^X(\mathbb{Q}) \backslash \mathbb{P}^X(\mathbb{A}) \to \chi(Nr(g))$$

where $\chi : \mathbb{Q}^\times \to \{ \pm 1 \}$ is some quadratic character. The action of $\mathbb{P}^X(\mathbb{Q})$ on such a representation is trivial, as is the action of $K_f[3, q]$ (by definition); moreover since the elements of $\Theta$ come from quaternions of norm 1, the action of $\Theta$ is trivial as well; hence from (11.3), such representation has to be the trivial one. It follows
from this enumeration that \(-(p + 1)\) does not occur as an eigenvalue of the \(p\)-th Hecke operator so the graph, while connected (cf. above) is not bipartite.

**Remark.** The discussion above is also valid for \(\tilde{\mathcal{A}}_3(d; q)\): this follows immediately from the previous discussions by projection. In particular we have

\[
\Gamma_{(q)} \backslash \text{PB}^\times(\mathbb{Q}_p)/K_p \sim \text{PB}^\times(\mathbb{Q}) \backslash \text{PB}^\times(\mathbb{A}_f)/K_f[q] \sim \tilde{\mathcal{A}}_3(d; q)
\]

with \(\Gamma_{(q)} = \text{PB}^\times(\mathbb{Q}) \cap K_f'[q]\text{PB}^\times(\mathbb{Q}_p)\).

12. Expander graphs and random walks

The contents of this section follow lecture notes of Hoori, Linial and Wigderson [HLW06]. Our goal is to prove Proposition 2.16.

12.1. Let \(G = (V, E)\) be a (possibly directed) \(d\)-regular graph on \(|V| = n\) vertices, i.e. the number of incoming edges to each vertex is \(d\), and the number of outgoing edges is also \(d\). We assume \(d > 2\). The normalized adjacency matrix \(T\) of \(G\) acts on \(L^2(V)\) by

\[
Tf(x) = \frac{1}{d} \sum_{(x \to y) \in E} f(y)
\]

and defines a self-adjoint operator. By an abuse of notation, we will use \(L^2(G)\) and \(L^2(V)\) interchangeably. More generally, \(G\) may be allowed to have multiple edges and loops, in which case we modify the definition of \(T\) in the evident way.

Let \(\|T\|\) be the operator norm of \(T\) acting on the orthogonal complement of the constants in \(L^2(V)\). The graph \(G\) is said to be an \(\alpha\)-expander, for some \(\alpha < 1\), if \(\|T\| \leq 1 - \alpha\). In rough terms, the smaller \(\|T\|\) is, the more “strongly connected” the graph \(G\).

When we speak of a “random walk on \(G\),” we mean that we select a vertex uniformly and randomly from \(V\), and then proceed to walk along directed edges, at each stage choosing one of the adjacent edges one with each choice assigned probability \(1/d\).

**Lemma 12.1.1** (Equidistribution of random walks). Let \(x \in V\) be some given point and let \(Q\) be a subset of \(V\) with density \(\mu = |Q|/n\) then the probability that a random walk on \(G\), originating from \(x\), is in \(Q\) at step \(\ell\) equals

\[
\mu + O(\|T\|^\ell \sqrt{\mu|V|}),
\]

the implied constant being absolute.

**Proof.** Let \(1_x\) be the Dirac function at \(x\) and \(\chi_Q\) be the characteristic function of \(Q\), then the probability equal

\[
\langle T^\ell 1_x, \chi_Q \rangle = \mu + \langle 1_x, T^\ell (\chi_Q - \mu) \rangle
\]

and we conclude using \(\|T^\ell (\chi_Q - \mu)\| \leq \|T\|^\ell \|\chi_Q - \mu\|\). \qed

**Lemma 12.1.2.** Let \(Q_1, \ldots, Q_\ell\) be subsets of \(V\), with densities \(\mu_i := |Q_i|/n\). The probability that a random walk on \(G\) is in \(Q_j\) at step \(j\), for all \(1 \leq j \leq \ell\), is at most

\[
\prod_{i=1}^{\ell-1} \left(\sqrt{\mu_i \mu_{i+1}} + \|T\|\right).
\]
Proof. Let $\chi_{Q_i}$ be the characteristic function of $Q_i$, and $A_i$ be the endomorphism of $L^2(V)$ defined by $f \mapsto \chi_{Q_i} f$. Let $\Pi$ denote the projection onto the constants, so that $T\Pi = \Pi$. The endomorphism $A_i T A_{i+1}$ may be decomposed:

$$A_i T A_{i+1} = A_i \Pi A_{i+1} + A_i T (1 - \Pi) A_{i+1}.$$

The endomorphism $A_i \Pi A_{i+1}$ may be written as $f \mapsto \frac{\chi_i}{|V|} \langle f, \chi_{Q_i+1} \rangle$, and thus has operator norm $\mu_i^{1/2} \mu_{i+1}^{1/2}$. Since the operator norm of $A_i T (1 - \Pi) A_{i+1}$ is at most $\|T\|$, we conclude that the operator norm of $A_i T A_{i+1}$ is at most $(\mu_i \mu_{i+1})^{1/2}$.

The probability that a random walk visits $Q_i$ at step $i$ for every $i \in \{1, \ldots, \ell\}$ is given by

$$|V|^{-1} \langle 1_V, (A_1 T A_2) (A_2 T A_3) \cdots (A_{\ell-1} T A\ell) 1_V \rangle$$

and the result follows. \qed

Lemma 12.1.3. Let $Q$ be a subset of $V$, with $\mu := |Q|/n$, and let $\gamma$ be a random walk of length $\ell$. Then the probability that $|\gamma \cap Q| \geq (\mu + \epsilon)\ell$ is at most

$$c_1 \exp(-c_2 \ell)$$

for positive constants $c_1, c_2$ depending only on $d, \|T\|, \mu, \epsilon$.

In other words, the number of “bad” walks of length $\ell$, with respect to some fixed notion of “bad”, decays exponentially with $\ell$.

Proof. The constants $C_1, C_2, \ldots$ appearing in the proof are all understood to be positive constants depending only on $d, \|T\|, \mu, \epsilon$.

Let $S$ be a subset of $\{1, \ldots, \ell\}$ of size $k$. It follows from Lemma 12.1.2 that the probability that $\gamma_i \in Q$ for $i \in S$ and $\gamma_i \notin Q$ for $i \notin S$ is at most

$$C_1 \mu^k (1 - \mu)^{\ell-k} \left(1 + \frac{\|T\|}{\min(\mu, 1 - \mu)}\right)^\ell.$$

Summing over all choices of $S$ we have that the probability that $|\gamma \cap Q| = k$ is at most

$$C_1 \binom{\ell}{k} \mu^k (1 - \mu)^{\ell-k} \left(1 + \frac{\|T\|}{\min(\mu, 1 - \mu)}\right)^\ell.$$

On the other hand, the sum

$$\sum_{k \geq (\mu + \epsilon)\ell} \binom{\ell}{k} \mu^k (1 - \mu)^{\ell-k}$$

is at most $\exp(-C_2 \ell)$. Thus, we are done if $\|T\|$ is small enough that $(1 + \frac{\|T\|}{\min(\mu, 1 - \mu)}) < e^{C_2}$.

If this is not the case, we fix an integer $C_3 \geq 1$, and replace the graph $\mathcal{G}$ by the graph $\mathcal{G}(C_3)$ for which a directed edge from $x$ to $y$ corresponds to a directed path of length $C_3$ in the graph $\mathcal{G}$. (Note that $\mathcal{G}(C_3)$ may have multiple edges and loops.) This improves the spectral gap: if $T^{(C_3)}$ is the normalized adjacency matrix of $\mathcal{G}(C_3)$, we have $T^{(C_3)} = T^{C_3}$. Accordingly, $\|T^{(C_3)}\| = \|T\|^{C_3}$. Choosing $C_3$ large enough, the argument above shows that the probability that a random walk of length $\ell$ on the graph $\mathcal{G}(C_3)$ of remains within $Q$ for at least $(\mu + \epsilon)\ell$ steps is bounded above by $C_4 \exp(-C_5 \ell)$.

It follows immediately that the probability that a random walk on $\mathcal{G}$ of length $C_6 \ell$ spends time $\geq (\mu + \epsilon)C_3 \ell$ inside $Q$ is at most $C_4 \exp(-C_5 \ell)$.

This proves the desired claim. \qed
12.2. The arc graph. Lemma 12.1.3 tells us that an exponentially small proportion of random walks are poorly distributed in $G$, will not quite suffice for our purposes; what we need to know is that an exponentially small proportion of non-backtracking walks are poorly distributed in $G$. In this section we explain how to derive such a statement from Lemma 12.1.3.

We now assume $G$ to be symmetric; that is, $E$ is closed under reversal. For each edge $a \in E$, write $a^+$ for the target of $a$ and $a^-$ for the source of $a$. We denote the reversal of $a$ by $\bar{a}$. With these notations, define the arc graph $G'$ to be a directed graph whose vertices are the directed edges, or arcs, of $G$. There is an edge from the arc $a$ to the arc $b$ exactly when $a^+ = b^-$ and $a \neq \bar{b}$.

Thus, $G'$ is regular of degree $d - 1$. We denote by $T'$ the normalized adjacency matrix of $G'$:

$$T'F(a) = \frac{1}{d-1} \sum_{\substack{b^- = a^+ \\ b \neq \bar{a}}} F(b)$$

The key feature of the arc graph $G'$, for us, is that we have a natural bijection between non-backtracking paths of length $\ell$ on $G$, and paths of length $\ell - 1$ on $G'$.

12.3. Our goal will be to deduce a spectral gap for $T'$ from that for $T$. This is a simple analogue of Atkin-Lehner theory in the subject of modular forms: when $d = p + 1$ for some prime $p$, we can think of $G$ as a quotient of the Bruhat-Tits tree attached to $\text{PGL}_2(\mathbb{Q}_p)/\text{PGL}_2(\mathbb{Z}_p)$; then the arc graph of the Bruhat-Tits tree is obtained by replacing $\text{PGL}_2(\mathbb{Z}_p)$ with an Iwahori subgroup, so that the passage from graph to arc graph is much the same as the passage from the congruence subgroup $\Gamma_0(N)$ to the smaller subgroup $\Gamma_0(Np)$.

There are natural maps $B, E : L^2(G) \rightarrow L^2(G')$ ("beginning" and "end") defined via

$$Bf(a) = f(a^-), \quad Ef(a) = f(a^+).$$

Moreover, the orthogonal complement to $\text{Im}(B) \oplus \text{Im}(E)$ consists of those functions $F \in L^2(G')$ with the property that

$$\sum_{a^- = v} F(a) = \sum_{a^+ = v} F(a) = 0,$$

for all $v \in V_G$. On this orthogonal complement (the "new space"), the operator $T'$ acts via

$$(12.1) \quad F \mapsto -\frac{1}{d-1} \tilde{F},$$

where $\tilde{F}(a) = F(\bar{a})$. Moreover, one checks that

$$\langle Bf_1, Ef_2 \rangle = d \langle Tf_1, f_2 \rangle, \quad T' \circ B = E.$$

Thus, if $w \in L^2(G)$ is an eigenfunction for $T$ with eigenvalue $\lambda$, then the "old space" $\mathbb{C}(Bw) + \mathbb{C}(Ew)$ is stable under $T'$. From this we see that every eigenvalue of $T'$ on this space is also an eigenvalue of the matrix:

$$\left( \begin{array}{cc} 0 & \frac{1}{d-1} \\ \frac{-1}{(d-1)} & \frac{d\lambda}{(d-1)} \end{array} \right)$$

It is easily computed that the eigenvalues are bounded away from 1 if $\lambda$ is. By (12.1), the eigenvalues of $T'$ on the new space are bounded in absolute value by $1/(d - 1) < 1$. We conclude that $\|T'\|$ is bounded away from 1 if $\|T\|$ is.
Proposition 12.4. Let $\mathcal{G} = (V, E)$ be an undirected graph with $\|T\| < 1$, and let $Q$ be a subset of $V$, with $\mu := |Q|/n$. The probability that a random walk without backtracking of length $\ell$ spends more than $(\mu + \epsilon)\ell$ time in $Q$ is at most

$$c_1 \exp(-c_2\ell)$$

for constants $c_1, c_2 > 0$ depending only on $d, \|T\|, \mu, \epsilon$.

Proof. Let $Q' \subset V\mathcal{G}'$ be the subset of arcs whose initial vertex lies inside $Q$. Noting that $|Q'| = |Q|$ and $|V\mathcal{G}'| = |V|$, we apply Lemma 12.1.3 to $(\mathcal{G}', Q')$ taking into account that $\|T'\|$ is bounded away from 1 in terms of $\|T\|$.

\qed

References

[BM66] A. Borel and G. Mostow Edts., Proceedings of Symposia in Pure Mathematics. Vol. IX: Algebraic groups and discontinuous subgroups, Proceedings of the Symposium in Pure Mathematics of the American Mathematical Society held at the University of Colorado, Boulder, Colorado (July 5-August 6, vol. 1965, American Mathematical Society, Providence, R.I., 1966.

[Duk88] W. Duke, Hyperbolic distribution problems and half-integral weight Maass forms, Invent. Math. 92 (1988), no. 1, 73–90.

[DSP90] W. Duke and R. Schulze-Pillot, Representation of integers by positive ternary quadratic forms and equidistribution of lattice points on ellipsoids, Invent. Math. 99 (1990), no. 1, 49–57.

[Del74] P. Deligne, La conjecture de Weil. I, Inst. Hautes Études Sci. Publ. Math. 43 (1974), 273–307 (French).

[ELMV07] M. Einsiedler, E. Lindenstrauss, Ph. Michel, and A. Venkatesh, The distribution of periodic torus orbits on homogeneous spaces: Duke’s theorem for cubic fields, (to appear) (2007). http://arxiv.org/abs/0705.1113.

[ELMV09a] M. Einsiedler, E. Lindenstrauss, Ph. Michel, and A. Venkatesh, The distribution of periodic torus orbits on homogeneous spaces, Duke Math. Journal 148 (2009), no. 1, 119-174. http://arxiv.org/abs/math/0607815.

[ELMV09b] M. Einsiedler, E. Lindenstrauss, Ph. Michel, and A. Venkatesh, The distribution of periodic torus orbits on homogeneous spaces: Duke’s theorem for quadratic fields, Preprint (2009).

[EV08] J. S. Ellenberg and A. Venkatesh, Local-global principles for representations of quadratic forms, Invent. Math. 171 (2008), no. 2, 257–279.

[FG87] O. M. Fomenko and E. P. Golubeva, Asymptotic distribution of lattice points on the three-dimensional sphere, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 160 (1987), no. Anal. Teor. Chisel i Teor. Funktsii. 8, 54–71, 297 (Russian); English transl., J. Soviet Math. 52 (1990), no. 3, 3036–3048.

[Gau01] C. F. Gauss, Disquisitiones arithmeticae, Springer-Verlag, New York, 1801. Translated and with a preface by Arthur A. Clarke; Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.

[HLW06] S. Hoory, N. Linial, and A. Wigderson, Expander graphs and their applications, Bull. Amer. Math. Soc. (N.S.) 43 (2006), no. 4, 439–561 (electronic).

[Iwa87] H. Iwaniec, Fourier coefficients of modular forms of half-integral weight, Invent. Math. 87 (1987), no. 2, 385–401.

[IS00] H. Iwaniec and P. Sarnak, Perspectives on the analytic theory of $L$-functions, Geom. Funct. Anal. Special Volume (2000), 705–741. GAFA 2000 (Tel Aviv, 1999).

[JL70] J. Jacquet and R. P. Langlands, Automorphic forms on GL(2), Springer-Verlag, Berlin, 1970. Lecture Notes in Mathematics, Vol. 114.

[Jon50] B. W. Jones, The Arithmetic Theory of Quadratic Forms., Carus Monograph Series, vol. no. 10., The Mathematical Association of America, Buffalo, N. Y., 1950.

[Kna97] A. W. Knapp, Introduction to the Langlands program, Representation theory and automorphic forms (Edinburgh, 1996), Proc. Sympos. Pure Math., vol. 61, Amer. Math. Soc., Providence, RI, 1997, pp. 245–302.
Yu. V. Linnik, "Ergodic properties of algebraic fields," Translated from the Russian by M. S. Keane. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 45, Springer-Verlag New York Inc., New York, 1968.

A. Lubotzky, "Discrete groups, expanding graphs and invariant measures," Progress in Mathematics, vol. 125, Birkhäuser Verlag, Basel, 1994. With an appendix by Jonathan D. Rogawski.

A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," Combinatorica 8 (1988), no. 3, 261–277.

A. V. Malyshev, "Discrete ergodic method and its applications to the arithmetic of ternary quadratic forms," Topics in classical number theory, Vol. I, II (Budapest, 1981), Colloq. Math. Soc. János Bolyai, vol. 34, North-Holland, Amsterdam, 1984, pp. 1023–1049.

Ph. Michel, "Analytic number theory and families of automorphic L-functions, Automorphic forms and applications (Park City, UT, 2002), IAS/Park City Math. Ser., vol. 12, Amer. Math. Soc., Providence, RI, 2007, pp. 179-296.

Ph. Michel and A. Venkatesh, "Equidistribution, L-functions and ergodic theory: on some problems of Yu. Linnik," International Congress of Mathematicians. Vol. II, Eur. Math. Soc., Zürich, 2006, pp. 421–457.

Ph. Michel and A. Venkatesh, "Hegner points and non-vanishing of Rankin/Selberg L-functions," Analytic number theory, Clay Math. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 2007, pp. 169–183.

Ph. Michel and A. Venkatesh, "Lectures on Linnik's ergodic method," Expanded notes of lectures given in 2010 at the Tata Institute summer school and the CIMPA summer school in Weihai. in preparation.

Ph. Michel and A. Venkatesh, "Subconvexity, periods and equidistribution," Book in preparation; expanded version of notes from a 2009 Nachdiplom vorlesung given at ETH Zuerich.

G. Pall, "Representation by quadratic forms," Canadian J. Math. 1 (1949), 344–364.

V. Platonov and A. Rapinchuk, "Algebraic groups and number theory," Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994. Translated from the 1991 Russian original by Rachel Rowen.

P. Samuel, "Algebraic theory of numbers," Translated from the French by Allan J. Silberger, Houghton Mifflin Co., Boston, Mass., 1970.

J.-P. Serre, "A course in arithmetic," Springer-Verlag, New York, 1973. Translated from the French; Graduate Texts in Mathematics, No. 7.

J.-P. Serre, "Trees," Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003. Translated from the French original by John Stillwell; Corrected 2nd printing of the 1980 English translation.

T. R. Shemanske, "Representations of ternary quadratic forms and the class number of imaginary quadratic fields," Pacific J. Math. 122 (1986), no. 1, 223–250.

Yu. G. Teterin, "Representation of algebraic integers by ternary quadratic forms," Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) 121 (1983), 157–168 (Russian). Studies in number theory, 8.

B. A. Venkov, "On the arithmetic of quaternion algebras. Izv. Akad. Nauk (1922), 205–241.

B. A. Venkov, "On the arithmetic of quaternion algebras., Izv. Akad. Nauk (1929), 489–509, 532–562, 607–622.

B. A. Venkov, "Elementary number theory," Translated from the Russian and edited by Helen Alderson, Wolters-Noordhoff Publishing, Groningen, 1970.

M.-F. Vignéras, "Arithmétique des algèbres de quaternions," Lecture Notes in Mathematics, vol. 800, Springer, Berlin, 1980 (French).

J.-L. Waldspurger, "Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie," Compositio Math. 54 (1985), no. 2, 173–242 (French).

J.-L. Waldspurger, "Correspondances de Shimura et quaternions," Forum Math. 3 (1991), no. 3, 219–307, DOI 10.1515/form.1991.3.219 (French).