ASYMPTOTICS FOR THE NUMBER OF SIMPLE \((4a+1)\)-KNOTS OF GENUS 1

ALISON BETH MILLER

Abstract. We investigate the asymptotics of the total number of simple \(4a+1\)-knots with Alexander polynomial of the form \(mt^2 + (1 - 2m)t + m\) for some \(m \in [-X, X]\). Using Kearton and Levine’s classification of simple knots, we give equivalent algebraic and arithmetic formulations of this counting question. In particular, this count is the same as the total number of \(\mathbb{Z}[1/m]\)-equivalence classes of binary quadratic forms of discriminant \(1 - 4m\), for \(m\) running through the same range. Our heuristics, based on the Cohen-Lenstra heuristics, suggest that this total is asymptotic to \(X^{3/2}/\log X\), and the largest contribution comes from the values of \(m\) that are positive primes. Using sieve methods, we prove that the contribution to the total coming from \(m\) prime is bounded above by \(O(X^{3/2}/\log X)\), and that the total itself is \(o(X^{3/2})\).

1. Introduction

In this paper we will count simple \(4a+1\)-knots by way of invariants with arithmetic structure. Informally, an \(n\)-knot is a knotted copy of \(S^n\) in \(S^{n+2}\); for a formal definition see Section 2.1. For \(n \geq 5\), it is impossible to classify all \(n\)-knots, but there is a restricted family, the simple \(n\)-knots, which have been completely classified by classical algebraic invariants. In this paper we will look at the case \(n = 1\pmod{4}\) and \(n > 1\). The case where \(n = 3\pmod{4}\) has many similarities, but also a few differences and would be an interesting subject for further research.

There is a natural definition of the genus for \(4a+1\)-knots. For \(a \geq 1\) this definition has the property that the degree of the Alexander polynomial of a genus \(g\) simple knot is precisely \(2g\).

1.1. Questions and Heuristics. We are interested in the general question: for a given positive integer \(g\), what are the asymptotics of the number of distinct \(4a+1\) knots with squarefree Alexander polynomial of degree \(2g\) and coefficients of “size” bounded by \(X\)? It is known by results of Bayer and Michel [1] that this number is always finite. In this paper we address the case \(g = 1\). In this case, the only possible Alexander polynomials are of the form \(\Delta_m = mt^2 + (1 - 2m)t + m\) for \(m \in \mathbb{Z}\) and the question becomes:

**Question** (Counting question, knot version). Fix \(a \geq 1\). Asymptotically, what is the total number of equivalence classes of simple \(4a+1\) knots of genus 1 with Alexander polynomial of the form \(\Delta_m\) for \(|m| \leq X\)?

Perhaps surprisingly, the answer to this question does not depend on the value of \(a\), but is uniform for all \(a > 1\). This follows from the classification of simple knots in terms of their Alexander module and Blanchfield pairing [2]. Using this classification, we can transform our counting question into an equivalent entirely algebraic question:

**Question** (Counting question, equivalent Alexander/Blanchfield version). Fix \(a \geq 0\). Asymptotically, what is the total number of isomorphism classes of simple \(4a+1\) knots with Alexander polynomial of the form \(\Delta_m\) for \(|m| \leq X\)?

Note that this question has a uniform answer for all \(a \geq 0\).

We will show that the question of counting knots is also equivalent to the following statement in number theory

**Question** (Counting question, equivalent quadratic form version). Asymptotically, what is the total, over all \(m\) with \(|m| \leq X\), of the number of \(\text{SL}_2(\mathbb{Z}[1/m])\)-equivalence classes of binary quadratic forms over \(\mathbb{Z}[1/m]\) having discriminant \(1 - 4m\)?

Asymptotics of binary quadratic forms are a very-well studied question in number theory, going back to Gauss. The difficulty in Question 1 comes from inverting the varying integer \(m\). We observe that there is a clear split in behavior between the cases where the constant term of the Alexander polynomial is prime
and the cases where it is composite. Using the theory of binary quadratic forms, we propose the following heuristics. In Section 2.4 we justify these heuristics using the Cohen-Lenstra-Hooley heuristics for binary quadratic forms plus some additional reasonable assumptions.

**Heuristic 1.** The total number of distinct Alexander modules (with pairing) having Alexander polynomial equal to $\Delta_p$ for some prime $p$ in the range $[1, X]$ is asymptotic to a constant times $X^{3/2}/\log X$.

**Heuristic 2.** The total number of distinct Alexander modules (with pairing) having Alexander polynomial equal to $\Delta_{-p}$ for some prime $p$ in the range $[1, X]$ is asymptotic to a constant times $X \log X$.

**Heuristic 3.** The total number of distinct Alexander modules (with pairing) having Alexander polynomial equal to $mt^2 + (1 - 2m)t + m$ for $m$ running over all integers in the range $[-X, X]$ with $|m|$ not prime is asymptotic to a constant times $X \log X$.

1.2. **Results.** The difficulty in proving these heuristics is that we are in general counting quadratic forms over rings with infinite unit group. However, the total contribution from $m$ prime and positive can be bounded above using Rosser’s sieve.

Theorem 1.1. The total number of isotopy classes of simple $4a+1$-knots having Alexander polynomial equal to $pt^2 + (1 - 2p)t + p$ for $p$ running over all primes in the range $[1, X]$ is (unconditionally) bounded above by $O(X^{3/2}/\log X)$.

Sieve methods are not powerful enough to give a lower bound, so instead we apply the Brauer-Siegel theorem to obtain

Theorem 1.2. The total number of isotopy classes of simple $4a+1$-knots having Alexander polynomial equal to $\Delta_p$ for $0 \leq p \leq X$ is $\gg (X^{3/2-\epsilon})$ for all $\epsilon > 0$.

Like the Brauer-Siegel theorem, this result is ineffective.

**Remark.** Both of these results should generalize to $g > 1$. To prove the upper bound, we will need to replace Gauss’s asymptotics for binary quadratic forms with asymptotics for $\text{Sp}_{2g}$-orbits on $2g$-ary quadratic forms. In a forthcoming paper [14], the author obtains such bounds on $\text{Sp}_{2g}$-orbits, and she hopes to apply these bounds to knot theory in future work.

For the lower bound, it should be possible to replace the Brauer-Siegel with a relative Brauer-Siegel theorem for CM extensions. However there may be technical issues regarding the cases of non-maximal orders.

For the other cases, it is much harder to obtain sharp results. For instance, in the case of $m = -p$ Theorem 1.1 remains true with exactly the same proof, but Heuristic 2 suggests a strictly lower order of growth.

However, we will show the following weak upper bound on the total:

Theorem 1.3. The total number of distinct Alexander modules (with pairing) having Alexander polynomial equal to $mt^2 + (1 - 2m)t + m$ for $m$ running over all integers in the range $[-X, X]$ is bounded above by $O(X^{3/2})$.

1.3. **Acknowledgments.** The author would like to thank Manjul Bhargava for leading me to explore this problem, and for his guidance and support throughout the process. She would also like to thank Barry Mazur for helpful advice on the organization of this paper. She would also like to thank Arul Shankar and Lenny Ng for comments on previous versions of this paper. Much of this paper was originally part of the author’s Ph.D. thesis at Princeton, where she was supported by an NSF Graduate Fellowship and an NDSEG Fellowship.

2. **Proofs**

2.1. **Preliminaries on knots.** There are multiple different ways to formalize the notion of an $n$-knot. The following two definitions are both commonly used:

Definition. (i) An $n$-knot $K$ is a PL embedded copy of $S^n$ in $S^{n+2}$ that is locally flat (locally homeomorphic to $\mathbb{R}^n \subset \mathbb{R}^{n+2}$). Equivalence is given by ambient isotopy.
(ii) An $n$-knot is a smoothly embedded submanifold $K$ of $S^{n+2}$ that is homeomorphic to $S^n$ (but not necessarily diffeomorphic; $K$ might be an exotic sphere). Equivalence is induced by orientation-preserving diffeomorphism of the $S^{n+2}$.

In both cases, we will consider both $S^n$ and $S^{n+2}$ as oriented manifolds, so that reversing the orientation of either or both may give an inequivalent knot.

Although it is far from obvious, classification results we use will give the same answer regardless of which of the two definitions above is used. I will talk about knots and equivalence with the understanding that all statements hold using either formulation.

**Definition.** The knot $K$ is called simple if $\pi_i(S^{n+2} - K) = \pi_i(S^1)$ for all $i \leq (n - 1)/2$.

We now introduce the related concept of a Seifert hypersurface.

**Definition.** A Seifert hypersurface in $S^{n+2}$ is a compact oriented $(n + 1)$-manifold $V$ with boundary such that $K = \partial V$ is homeomorphic to $S^n$. We say that $V$ is a Seifert hypersurface for the knot $K$.

(We again have the choice of working in either the PL category or the smooth category, and again all results we use hold uniformly in both cases.)

**Definition.** A simple Seifert hypersurface in $S^{n+2}$ is said to be simple if $V$ is $\frac{n-1}{2}$-connected.

It is known that the simple knots are exactly those with simple Seifert hypersurfaces.

**Theorem 2.1.** If $V$ is a simple Seifert hypersurface in $S^{n+2}$, then $\partial V$ is a simple $(n-1)$-knot. Conversely, any simple $n$-knot $K$ has a (non-unique) simple Seifert hypersurface.

**Proof.** Farber states this as Theorem 0.5 in [5], where he deduces it from results of Levine [10, 13] and Trotter [16].

We now specialize to $n = 4a+1$. If $V$ is a simple Seifert hypersurface in $S^{4a+3}$ it follows from the Hurewicz theorem and Poincare duality that $H_i(V, \mathbb{Z})$ is trivial for all $i$ except $i = 2a + 1$, and $H_{2a+1}(V, \mathbb{Z})$ is a free $\mathbb{Z}$-module of even rank.

**Definition.** If $V$ is a simple Seifert surface in $S^{4a+3}$, we define the genus of $V$ to be half the rank of $H_{2a+1}(V, \mathbb{Z})$.

The genus of a $4a + 1$-knot $K$ is the minimum genus of any Seifert surface for $K$.

In the classical case $a = 0$, the genus is a subtle geometric invariant of knots. However for $a > 1$, the genus of a simple knot $K$ is easily computable from the Alexander polynomial of $K$, defined.

**Theorem 2.2.** [11] If $V$ is any simple Seifert surface for $K$, and $P$ is a Seifert matrix for $V$, then

$$\Delta_K = t^{-\dim \ker P} (\det tP - P^t)$$

is the normalized Alexander polynomial of $K$, and in particular is independent of $V$.

**Corollary 2.3.** If $K$ is any simple knot, then the genus of $K$ is equal to $\frac{1}{2} \deg \Delta_K$.

**Proof.** This follows from Theorem 2.2 and the result that any simple knot has a Seifert surface with nondegenerate Seifert pairing (itself a consequence of Theorem 3 and Proposition 1 in [12]).

2.2. Relationship between knots, ideal classes, and quadratic forms. We now use the classification of simple knots to show that the various forms of Question 1 stated in the introduction are equivalent.

**Theorem 2.4** (Classification of simple knots). [12, 13, 17, 9, 5] The following are in bijection with each other:

(i) equivalence classes of simple $4a + 1$ knots of genus $\leq g$
(ii) $S$-equivalence classes of $2g \times 2g$ Seifert matrices $P$
(iii) Alexander modules of genus $\leq g$ equipped with Blanchfield pairing
(iv) $R$-equivalence classes of $\mathbb{Z}[x]$-modules with isometric structures

For each of these objects, there is a natural way of defining an Alexander polynomial, and these bijections preserve the Alexander polynomial.
For \( g = 1 \), we can add two more items to the list. First define

\[
R_m = \mathbb{Z} \left[ \frac{t, t^{-1}}{\Delta(t)} \right] / \mathbb{Z} \left[ \frac{1}{m}, \frac{1 + \sqrt{1 - 4m}}{2} \right].
\]

(Note that this ring is called \( \mathcal{O}_m \) in the author’s Ph.D thesis [15].)

Inspired by [2] we define

**Definition.** An oriented ideal class of \( R_m \) is a homothety class of fractional ideals \( I \) of \( R_m \) equipped with an isomorphism \( \phi : \wedge^2 I \cong \mathbb{Z}[\frac{1}{m}] \) of \( \mathbb{Z}[\frac{1}{m}] \)-modules.

The set of oriented ideal classes of \( R_m \) is often called the narrow class group of \( R_m \), though that term is used as well for other distinct but related groups.

Any such \( \phi \) can be written in the form

\[
\phi(\alpha, \beta) = \text{tr} \left( \frac{\alpha \beta}{\kappa \sqrt{1 - 4m}} \right)
\]

for a unique \( \kappa \in \mathbb{Z}[\frac{1}{m}] \). Such a \( \phi \) maps \( \wedge^2 I \) isomorphically to \( \mathbb{Z}[\frac{1}{m}] \) if and only if \( \kappa \) is a generator of the fractional ideal \( NI \) of \( \mathbb{Z}[\frac{1}{m}] \).

Hence we can also describe oriented ideal classes of \( R_m \) as equivalence \( [I, \kappa] \) of pairs where \( I \) is a fractional ideal of \( R_m \) and \( \kappa \in \mathbb{Z}[\frac{1}{m}] \) is a generator of \( NI \), modulo the equivalence relation \( (I, \kappa) \sim (\alpha I, N\alpha \kappa) \) for every \( \alpha \in \text{Frac}(R_m) = \mathbb{Q}(\sqrt{1 - 4m}) \).

In this paper we will write our narrow ideal classes as \([I, \kappa] \). We’ll use the same notation for imaginary quadratic rings.

**Remark.** In my Ph.D. thesis [15] I defined conjugate self-balanced modules/ideal classes, which generalize the definition of oriented ideal class above to the case of \( g > 1 \). They can be thought of as relative ideal classes for a quadratic extension of rings.

**Corollary 2.5.** When \( g = 1 \) we can add the following two items to the list in Theorem 2.4:

(v) pairs \((m, [I, \kappa])\) where \( m \) is an integer and \([I, \kappa] \) is an oriented ideal class of the ring \( R_m = \mathbb{Z}[\frac{1}{m}, \frac{1 + \sqrt{1 - 4m}}{2}] \).

(vi) pairs \((m, [Q])\) where \( m \) is an integer and \([Q] \) is an \( \text{SL}_2[\mathbb{Z}[\frac{1}{m}]] \)-equivalence class of binary quadratic forms over \( \mathbb{Z}[\frac{1}{m}] \) with \( \text{Disc} \ Q = 1 - 4m \).

In both cases, the corresponding Alexander polynomial is

\[
\Delta_m = mt^2 + (1 - 2m)t + m.
\]

**Proof.** First of all, the bijection between (v) and (vi) is a generalization of the standard bijection between binary quadratic forms and ideal classes in quadratic rings. Given an oriented ideal class \((I, \phi) \) of \( R_m \), choose any \( \mathbb{Z}[\frac{1}{m}] \) basis \( u_1, u_2 \) of \( I \) with \( \phi(u_1 \wedge u_2) = 1 \). The function \( \phi((\sqrt{1 - 4m})a \wedge b) \) is a symmetric bilinear form on the rank 2 \( \mathbb{Z}[\frac{1}{m}] \)-module \( I \). If we write \( \phi \) out in the basis \( u_1, u_2 \) we obtain a binary quadratic form \( Q \) of discriminant \( \sqrt{1 - 4m} \).

To finish, it’s easiest to either biject Alexander modules with oriented ideal classes, or Seifert matrices with binary quadratic forms. The former bijection is easier to prove, the latter easier to describe. We prove the former:

If \( M \) is an Alexander module with Alexander polynomial \( \Delta_m \), we can view \( M \) as a module over the quotient ring \( R_m = \mathbb{Z}[t, t^{-1}] / \Delta_m \). Because \( \Delta_m \) is squarefree, we have \( M \otimes \mathbb{Z} Q \cong R_m \otimes \mathbb{Z} Q \) as \( R_m \otimes \mathbb{Z} Q = \mathbb{Q}[t, t^{-1}] / \Delta(t) \)-modules. Hence \( M \) is isomorphic as \( R_m \)-module to some fractional ideal \( I \) of \( R_m \). Choose such an \( I \) and an isomorphism \( \phi : I \to M \).

To put an orientation on \( I \), we use the Blanchfield pairing. The isomorphism \( \phi \) lets us transfer the Blanchfield pairing on \( M \) to a \( R_m \)-hermitian perfect pairing

\[
\langle \cdot, \cdot \rangle : I \times I \to \frac{1}{\Delta(t)} \mathbb{Z}[t, t^{-1}] / \mathbb{Z}[t, t^{-1}].
\]

To obtain an orientation, we compose with the map \( T : \frac{1}{\Delta(t)} \mathbb{Z}[t, t^{-1}] / \mathbb{Z}[t, t^{-1}] \to \mathbb{Q} \) sending \([f] \mapsto f'(0) \). The map \( T \) is a special case of “Trotter’s trace function” in knot theory. It’s determined \( \mathbb{Z}[\frac{1}{m}] \)-linearly from the values \( T(\frac{1}{\Delta(t)}) = 0, T(\frac{t}{\Delta(t)}) = \frac{1}{m} \).
By standard arguments, the pairing $T((a, b)) : I \times I \to \mathbb{Z}[\frac{1}{m}]$ is skew-symmetric with determinant a unit in $\mathbb{Z}[\frac{1}{m}]$. Moreover we can recover the pairing $\langle \cdot \rangle$ from the pairing $T((a, b))$. □

We can now apply the formulas for the Alexander module and Blanchfield pairing in terms of the Seifert matrix original given by Levine in [13] and reproved by Friedl and Powell in [6]. When one works out the details, it turns out that the composite map from Seifert matrices to binary quadratic forms sends a Seifert matrix $P$ to the quadratic form with matrix $\frac{P + PT}{2}$. (This is not an integer matrix, but still gives an integer quadratic form.)

We then obtain the following corollary.

Corollary 2.6. Two $2 \times 2$ Seifert matrices $P_1$ and $P_2$ with the same Alexander polynomial $\Delta_m$ (equivalently, with the same determinant $m$) are $S$-equivalent if and only if there exists $X \in \text{SL}_2(\mathbb{Z}[\frac{1}{m}])$ with $P_1 = X P_2 X^T$.

This is a special case of 4.15 in Trotter [16]. For larger Seifert matrices Trotter also shows that $S$-equivalence implies $\text{Sp}_{2\nu}(\mathbb{Z}[\frac{1}{m}])$-equivalent, but the converse is not generally the case.

Another corollary (which can also be proved directly):

Corollary 2.7. Any binary quadratic form over $\mathbb{Z}[\frac{1}{m}]$ of discriminant $1 - 4m$ is $\text{SL}_2(\mathbb{Z}[\frac{1}{m}])$-equivalent to a form defined over $\mathbb{Z}$.

2.3. The map from oriented ideal classes of $\mathbb{Z}[\gamma_m]$ to oriented ideal classes of $\text{Cl}^+(R_m)$. Corollary 2.7 can also be interpreted as a statement about narrow class groups. Let $\gamma_m = \frac{1 + \sqrt{1 - 4m}}{2}$, so that $\mathbb{Z}[\gamma_m]$ is the ring of integers in $\mathbb{Q}(\sqrt{1 - 4m})$.

The inclusion $\iota : \mathbb{Z}[\gamma_m] \to R_m$ induces a map $\iota_* : \text{Cl}^+(\mathbb{Z}[\gamma_m]) \to \text{Cl}^+(R_m)$. More generally, if $(I, \kappa)$ is a (possibly non-invertible) ideal class of $\mathbb{Z}[\gamma_m]$, then we can map it to the ideal class $(IR_m, \kappa)$ of $R_m$.

Corollary 2.8. The map $\iota_* : \text{Cl}^+(\mathbb{Z}[\gamma_m]) \to \text{Cl}^+(R_m)$ is surjective.

The kernel of $\iota_*$ can also be described explicitly:

Proposition 2.9. The kernel $\ker \iota^*$ is generated by the classes

$$(p, \gamma_m, p)\langle (p, 1 - \gamma_m), p \rangle^{-1} = \langle (p, \gamma_m), p \rangle^2$$

where $p$ runs through the set of all prime factors of $1 + 4m$.

Proof. First, observe that $R_m = \mathbb{Z}[\gamma_m, \frac{1}{m}]$, and that $m$ factors in $R_m$ as

$$m = \prod_{p|\nu} (p, \gamma_m)(p, 1 - \gamma_m).$$

Let $[I, \kappa]$ be an arbitrary element of $\ker \iota*$ since we are in the kernel we can rescale so that $I \cdot R_m = R_m$ and $\kappa = 1$. Then $I$ is a fractional ideal of $\mathbb{Z}[\gamma_m]$ which becomes trivial when we invert the element $m$, so we can factor $I$ as

$$I = \prod_{p|\nu} (p, \gamma_m)^{a_p} (p, 1 - \gamma_m)^{b_p}.$$

In order to have $NI = (1)$ we must have $a_p = -b_p$ for all $p$. The result follows. □

Note that not all oriented ideal classes of $\mathbb{Z}[\gamma_m]$ are invertible. However:

Proposition 2.10. Two (possibly non-invertible) oriented ideal classes $[I, \kappa]$ and $[I', \kappa']$ of $\mathbb{Z}[\gamma_m]$ become equivalent in $R_m$ if and only if there exists $[J, \lambda] \in \ker \iota*$ with

$$[I, \kappa] = [J, \lambda][I', \kappa'].$$

Proof. As before, can reduce to the case $\kappa = \kappa'$. For each $p$ let

$$a_p = v_p(I) - v_p(I')$$

where $p$ is the ideal $(p, \gamma_m)$ and let

$$J = \prod_p \langle (p, \gamma_m), p \rangle^{a_p} \langle (p, 1 - \gamma_m)^{-a_p}, p \rangle^{-1}.$$

One can then check locally that $I = J I'$.
2.4. Consequences for the heuristics. In the case when \( m = \pm p \) is prime, we have a consequence that

**Proposition 2.11.** If \( m \) is prime (possibly negative) then the map \( \iota_* : \text{Cl}^+ (\mathbb{Z}[\gamma_m]) \to \text{Cl}^+ (R_m) \) is an isomorphism. More generally, oriented ideal classes of \( \mathbb{Z}[\gamma_m] \) are in bijection with oriented ideal classes of \( R_m \) via \( [I, \kappa] \mapsto [IR_m, \kappa] \).

Translating back into the language of quadratic forms, we also have the important corollary:

**Corollary 2.12.** Two quadratic forms over \( \mathbb{Z} \) of determinant \( 1 - 4p \) are \( \text{SL}_2(\mathbb{Z}[\frac{1}{m}]) \)-equivalent if and only if they are \( \text{SL}_2(\mathbb{Z}) \)-equivalent.

This corollary is also implied by Trotter’s work in [10].

We can now easily prove Theorem 1.2:

**Proof of Theorem 1.2.** We show the equivalent statement, that the total is \( \gg X^{3/2-\epsilon}/\log X \) for any \( \epsilon > 0 \).

Choose any \( \epsilon > 0 \). By the Brauer-Siegel theorem plus the formula for class number of non-maximal orders, there exists some constant \( c_\epsilon \) such that the size

\[
|\text{Cl}^+ (\mathbb{Z}[\gamma_m])| \geq c_\epsilon X^{1/2-\epsilon}
\]

for every \( m \in [0, X] \). We have just seen that \( |\text{Cl}^+ (\mathbb{Z}[\gamma_m])| = |\text{Cl}^+ (R_m)| \) when \( m \) is prime. Hence the total contribution of the \( \sim X/\log X \) primes in \( [0, X] \) is \( \gg X^{3/2-\epsilon}/\log X \). \( \square \)

When \( m \) is not prime, for any \( p \) dividing \( m \) the ideals \((p, \gamma_m)\) and \((p, 1 - \gamma_m)\) represent two nontrivial distinct ideal classes, as can be checked with reduction theory. Hence the class \([(p, \gamma_m), p][p, 1 - \gamma_m], p]^{-1} = [(p, \gamma_m), p]^2 \) is always a nontrivial element of \( \text{Cl}^+ (\mathbb{Z}[\gamma_m]^2) \). Note that these ideals satisfy one relation, coming from the identity

\[
\prod_{p|m} (p, \gamma_m)^{v_p(m)} = (\gamma_m).
\]

This motivates the following heuristics

**Heuristic 4.** When \( m \) runs through all positive integers of the form \( p_1^{n_1} \cdots p_k^{n_k} \), the distribution of the finite abelian groups \( \text{Cl}^+ (R_m) \) agrees with the distribution of \( G/(g_1, \ldots, g_k) \), where \( G \) is a finite abelian group selected from the Cohen-Lenstra distribution for narrow class groups of imaginary quadratic fields [3] and \( g_1, \ldots, g_k \) are randomly chosen elements of \( G^2 \) subject to the constraint that \( \prod g_k^{n_k} = 1 \). When \( m \) runs through all positive integers of the form \( p_1^{n_1} \cdots p_k^{n_k} \), the distribution of the finite abelian groups \( \text{Cl}^+ (R_m) \) agrees with the distribution of \( G/(g_1, \ldots, g_k) \), where \( G \) is a finite abelian group selected from the Cohen-Lenstra distribution for narrow class groups of real quadratic fields [3] and \( g_1, \ldots, g_k \) are randomly chosen elements of \( G^2 \) subject to the constraint that \( \prod g_k^{n_k} = 1 \).

These heuristics are fairly naive and it is worth investigating them further for accuracy, but I conjecture that they at least give the correct order of magnitude for the average sizes of these groups. An important special case: if \( m = p_1 p_2 \), this is essentially the Cohen-Lenstra distribution for narrow class groups of real quadratic fields, and we should expect similar behavior, namely that on average the class group should have size about \( (\log m)^2 \), and the total contribution of all \( m = p_1 p_2 \leq X \) will be \( O(X \log X) \).

We now consider the case of general \( m \). By Erdős-Kac, most integers \( \leq X \) have on the order of \( \log \log X \) prime factors. On the other hand, Cohen-Lenstra distribution is heavily biased towards groups \( G \) where \( G^2 \) is generated by a small number of elements: for every \( n \), the probability of \( G^2 \) being generated by \( \leq n \) elements is positive, and goes to 1 rapidly as \( n \to \infty \).

Hence we expect that, for a density 1 subset of \( m \), we have

\[
\text{Cl}^+ (R_m) \cong \text{Cl}^+ (\mathbb{Z}[\gamma]) / \text{Cl}^+ (\mathbb{Z}[\gamma])^2.
\]

(By genus theory for binary quadratic forms, this implies that two quadratic forms of discriminant \( 1 - 4m \) are \( \mathbb{Z}[\frac{1}{m}] \)-equivalent if and only if they are \( \mathbb{Z} \)-equivalent.)
2.5. Proof of Theorem 1.1 by Sieving. By Corollaries 2.7 and 2.12, it’s enough to show

**Proposition 2.13.** The total number of $\text{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms $ax^2 + bxy + cy^2$ with prime discriminant of the form $p = 1 - 4m$ for $m \in [0, X]$ is bounded above by $O(\frac{X^{3/2}}{\log X})$.

We’ll actually show that the total for $m \in [X, 2X]$ is also $O(\frac{X^{3/2}}{\log X})$, and the proposition will follow by summing. As well, we will only count the positive definite quadratic forms, as the count of negative definite forms is the same.

We follow the approach of Rosser’s sieve [2], modifying the terminology to suit our approach. We introduce an auxiliary parameter $Z \leq X$ whose value will be chosen later, and let $P(Z)$ denote the product of all primes up to $Z$. Let

$$\mathcal{F} = \{(\alpha, \beta, \gamma \in \mathbb{R}^3 \mid ||\beta|| \leq \gamma \leq \alpha\}$$

be the standard fundamental domain for $\text{SL}_2(\mathbb{Z})$ acting on positive definite binary quadratic forms.

Then the total we wish to bound is at most:

$$S(X, Z) := \sum_{X \leq m \leq 2X} \sum_{(m, P(Z)) = 1} \#\{(a, b, c) \in \mathbb{Z}^3 \cap \mathcal{F} : b^2 - 4ac = 1 - 4m\}$$

Note here that $b^2 - 4ac = 1 - 4m$ implies $b$ odd: we write $b = 2b' + 1$ and let $\mathcal{F}'$ be the preimage of $\mathcal{F}$ under the affine transformation $(\alpha, \beta, \gamma) \mapsto (\alpha, 2\beta + 1, \gamma)$. Using this change of variables

$$S(X, Z) = \sum_{X \leq m \leq 2X} \sum_{(m, P(Z)) = 1} \#\{(a, b', c) \in \mathbb{Z}^3 \cap \mathcal{F}' : ac - b'(b' + 1) = m\}$$

To apply the sieve, we need estimates on the following quantities for all squarefree $d \leq X$:

\begin{equation}
S_d(X) := \sum_{m \leq [X/2]} \#\{(a, b', c) \in \mathbb{Z}^3 \cap \mathcal{F}' : ac - b'(b' + 1) = m\}.
\end{equation}

**Lemma 2.14.** For a positive integer $s$, let $\rho(s) = \prod_{p \mid s} \frac{p+1}{p}$. If $d$ is a squarefree positive integer $\leq X$, there exist explicit real constants $c_1, c_2$ such that

\begin{equation}
S_d(X) = c_1 \rho(d) X^{3/2} + R_d(X),
\end{equation}

and the error term $R_d(X)$ is bounded by

\begin{equation}
|R_d(X)| \leq c_2 X \rho(d)(\max(d, \log X)).
\end{equation}

**Proof.** We observe that for all squarefree $d$, $S_d(X)$ counts the number of points in the intersection of the region

$$\mathcal{R}_X = \{(\alpha, \beta', \gamma) \in \mathcal{F}' \mid |\alpha \gamma - \beta'(b' + 1)| \leq X\}$$

with the union of the cosets of $(d\mathbb{Z})^3$ on which the function $ac - b(b + 1)$ vanishes modulo $d$.

We wish to apply:

**Lemma 2.15** (Davenport). Let $R$ be a bounded semi-algebraic region in $\mathbb{R}^n$, defined by $k$ polynomial inequalities of degree at most $\ell$. Then the number of points $(a, b, c) \in \mathbb{Z}^n \cap R$ can be asymptotically expressed as

$$\text{vol}(R) + \epsilon(R)$$

with the error term $\epsilon(R)$ bounded in size by $\epsilon(R) < \kappa \max(\text{vol}(\overline{R}), 1)$ where $\overline{R}$ runs over all projections of $R$ onto subspaces of $\mathbb{R}^n$ spanned by coordinate axes, and $\kappa = \kappa(n, m, k, \ell)$ is some explicit constant depending only on $n, m, k, \ell$.

We cannot apply Davenport’s lemma directly because $\mathcal{R}_X$ goes off to infinity. Instead, we truncate the cusp: for a positive real parameter $\tau$, define

$$\mathcal{R}_{X, \tau} = \{(x, y, z) \in \mathcal{R}_X \mid z < \tau\}.$$ 

We observe that any lattice point $(a, b, c) \in \mathcal{R}_X$ has $c \leq 2X$, so also belongs to $R_{X, 2X}$.
One can calculate that the largest 1-dimensional projection of \( R_{X,2X} \) has length \( 2X \), while the largest 2-dimensional projection of \( R_{X,2X} \) has area \( c_3 X \log X \) for an explicit constant \( c_3 \).

Now let \( L_1, \ldots, L_n \) be the cosets of \( (d\mathbb{Z})^3 \) for which \( ac - b'(b' + 1) \equiv 0 \mod d \) for all \( (a,b',c) \in L_i \).

The number \( n \) is equal to the number of solutions to \( ac - b'(b' + 1) = 0 \) in \( (\mathbb{Z}/d\mathbb{Z})^3 \); a calculation with the Chinese remainder theorem gives \( n = \rho(d)d^3 \).

Applying Davenport’s lemma to \( R_{X,t} \) rescaled by \( d^{-1} \) and translated appropriately, we obtain that there exists a real number \( \kappa \) such that for each \( i \)

\[
\#(R_{X,2X} \cap L_i) - c_1 d^{-3/2} X^{3/2} \leq \kappa (\max(d^{-2}X \log X, d^{-1}X, 1)) = \kappa d^{-2} X \max(\log X, d)
\]

where the last step uses \( d \leq X \).

Summing over all \( \rho(d)d^3 \) values of \( i \) and applying the triangle inequality, we obtain

\[
S_d(X) - \rho(d)c_1 d^{-3/2} X^{3/2} = \sum_i \#(R_{X,2X} \cap L_i) - c_1 d^{-3} X^{3/2} \leq \rho(d)\kappa d^{-2} X \max(\log X, d)
\]

as desired. \( \square \)

We are now ready to prove Proposition 2.13.

**Proof.** We apply Rosser’s sieve. First we calculate the “sieving density,” also known as the “dimension.” The following inequality is analogous to (1.3) in [7]: for all \( Z > W \geq 2 \) we have

\[
\prod_{W < p < Z} (1 - \rho(p))^{-1} \leq \left( \frac{\log Z}{\log W} \right)^{\kappa} \left( 1 + \frac{K}{\log W} \right).
\]

where \( \kappa = 1 \) and \( K \) is a sufficiently large constant. This is true by comparing to the product \( \prod_{W < p < Z} (1 - 1/p) \) and applying Mertens’ formula for the asymptotic growth of the latter.

Therefore we may apply (the first half of) Theorem 1.4 of [7] with \( y = Z \) (so that \( s = 1 \)) to obtain

\[
S(X, Z) < X^{3/2} \prod_{p < Z} (1 - \rho(p)) \left( F(1) + e^{\sqrt{K}} Q(1)(\log Z)^{-1/3} \right) + \sum_{d < Z \text{ squarefree}} |R_d(X)|
\]

where \( F(s) \), \( Q(s) \) are specific functions defined in [7]; we will not need any properties of them, just that \( F(1) \) and \( Q(1) \) are explicit constants.

Using our previous result that \( \prod p < Z (1 - \rho(p)) \sim 1/(\log Z) \), we see that the first term is \( O(X^{3/2}/\log Z) \).

Applying (3) to the second term gives

\[
\sum_{d < Z \text{ squarefree}} |R_d(X)| \leq c_1 X \sum_{d < Z \text{ squarefree}} \rho(d)d(\max(d, \log X)).
\]
We estimate $\rho(d)$. Since $d$ is squarefree, we can write $d$ as a product of distinct primes: $d = \prod_{i=1}^{n_d} p_i$. Then we make the crude bound
\[
\rho(d) = \prod_{i=1}^{n_d} \frac{p_i + 1}{p_i} = \frac{1}{d} \prod_{i=1}^{n_d} \left(1 + \frac{1}{p_i}\right) = \frac{1}{d} \sum_{d'|d} \frac{1}{d'} \leq \frac{1}{d} \sum_{1 \leq d' \leq Z} \frac{1}{d'} \leq \frac{\log Z + 1}{d}.
\]

Plugging (8) into the sum in (7), we obtain
\[
\sum_{d < Z \text{ squarefree}} |R_d(X)| \leq c_3 1 \sum_{d < Z} \max(d, \log x) \leq c_1 (\log Z + 1) \sum_{d < Z} (d + \log X) \leq c_1 X (\log Z + 1) (Z^2 + Z \log X) \leq c_1 X (\alpha \log X + 1) (X^{2\alpha} + X^\alpha \log X).
\]

In the last line we have set $z = X^\alpha$.

We deduce the following asymptotics for our error term, where we have fixed $\alpha$ and allow $X$ to vary
\[
\sum_{d < z \text{ squarefree}} |R_d(X, z)| = O(X^{1+2\alpha} \log X).
\]

This will be $o(X^{3/2}/\log X)$ for any $\alpha < 1$.

We conclude that if we set $Z = X^\alpha$ for a fixed $\alpha < 1$, the main term in (9) is $O(X^{3/2}/\log X)$ and the error term is $o(X^{3/2}/\log X)$, giving the desired asymptotic.

2.6. Proof of Theorem 1.3. We now prove Theorem 1.3. We will prove it in the equivalent form

**Theorem 2.16.** If $T(X)$ is the number of $\text{SL}_2(\mathbb{Z}[\frac{1}{m}])$-equivalence classes of binary quadratic forms of discriminant $1 - 4m$ as $m$ runs through all integers in the range $[-X, X]$, then
\[
\lim_{X \to \infty} \frac{T(X)}{X^{3/2}} = 0.
\]

Gauss’s bound for the total number of $\text{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms with discriminant in this range is $O(X^{3/2})$, so this theorem says that strengthening the equivalence relation to $\text{SL}_2(\mathbb{Z}[\frac{1}{m}])$-equivalence decreases the order of growth.

We can instead think of our total $T(X)$ as counting $\text{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms weighted as follows:

**Definition.** The weight $w(Q)$ of a binary quadratic form $Q$ of discriminant $1 - 4m$ is equal to $\frac{1}{n}$ where $n$ is the number of distinct $\text{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms comprising the $\text{SL}_2(\mathbb{Z}[\frac{1}{m}])$-equivalence class of $Q$.

Then
\[
T(X) = \sum_{\text{SL}_2(\mathbb{Z})\text{-equivalence classes } [Q]} w(Q)
\]

where $\text{disc}[Q] = 1 - 4m$ with $m \in [-X, X]$. 

Recall that the content of a binary quadratic form \( ax^2 + bxy + cy^2 \) is defined to be \( \text{content}(Q) = \gcd(a, b, c) \). In order to bound our weighted count we will first need to divide up by content.

**Definition.** Let \( T_d(X) \) be the number of \( \text{SL}_2(\mathbb{Z}[\frac{1}{d}]) \)-equivalence classes of binary quadratic forms \( ax^2 + bxy + cy^2 \) of content \( d \) with discriminant \( 1 - 4m \) as \( m \) runs through all integers in the range \([-X,X]\).

As before, we have

\[
T_d(X) = \sum_{\text{SL}_2(\mathbb{Z})\text{-equivalence classes } [Q] \text{ with } \text{disc}[Q]=1-4m \text{ and } m \in [-X,X]} \frac{1}{w(Q)}.
\]

(11)

The key result we need here is that

**Lemma 2.17.** If \( Q \) is a binary quadratic form with content \( d \) and discriminant \( 1 - 4m \), then we have an upper bound

\[
w(Q) \leq \epsilon_d(\omega(m))
\]

where \( \epsilon_d(n) = d^{-2}2^{1-n} \) and \( \omega(m) \) denotes the number of distinct prime factors of \( m \).

**Proof.** We translate this question over to the language of oriented ideal classes. Our hypothesis becomes: if \([I, \alpha]\) is an oriented ideal class of \( \mathbb{Z}[\gamma_m] \), and the endomorphism ring of the ideal \( I \)

\[
O_I = \{ \lambda \in \mathbb{Z}[\gamma_m] \mid \lambda I \subset I \},
\]
equals \( \mathbb{Z}[\frac{1+\sqrt{m/d}}{2}] \), or equivalently, \( \mathbb{Z}[\gamma_m] = \mathbb{Z} + dO_I \). We must show that there are at least \( \epsilon_d(n) \) distinct ideal classes \([I', \alpha']\) of \( O_I \) such that the \([I'R_f, \alpha']\) and \([IR_f, \alpha]\) are equivalent oriented ideal classes of \( R_f \).

We first do the case \( d = 1 \).

Let \([I_Q, \kappa_Q]\) be the oriented ideal class of \( \mathbb{Z}[\gamma_m] \) corresponding to the quadratic form \( Q \). Because \( d = 1 \), the ideal class \( I_Q \) is invertible. Hence if \([J, \lambda]\) runs through the elements of \( \ker \epsilon_* \), the ideal classes \([JI_Q, \lambda\kappa_Q]\) are all distinct but becomes equivalent classes of \( \lambda \).

So it suffices for \( f = 1 \) to show that \( |\ker \epsilon_*| \geq 2^{\omega(m)-1} \). For this, note that if we let \( s \) run through the divisors of \( m \) with \( s > \sqrt{m} \), the CM points \( \mathbb{Z} = \frac{1+\sqrt{m}}{2} \) all lie in the fundamental domain of the upper-half plane. Hence the ideal classes \((m, \gamma)\) are all distinct, and they also all lie in \( \ker \epsilon_* \). We conclude that

\[
|\ker \epsilon_*| \geq \left[ \frac{d(m)}{2} \right] \geq 2^{\omega(m)-1}.
\]

We can use the same argument for \( d > 1 \). However, here \( I_Q \) is no longer invertible, so the map \([J, \lambda] \mapsto [JI_Q, \lambda\kappa_Q]\) is no longer injective. Indeed, by the theory of ideals in quadratic orders, the fibers of this map are the same as the fibers of the homomorphism

\[
\phi : \text{Cl}^+(\mathbb{Z}[\gamma_m]) \to \text{Cl}^+(O_I).
\]

If we show \( |\ker(\phi)| \leq d^2 \) we will then get the desired bound.

Note that \( \mathbb{Z}[\gamma_m] \) has index \( d \) in \( O_I \), so \( \mathbb{Z}[\gamma_m] = O_I + dO_I \). Then there is a surjective homomorphism \( (O_I/dO_I)^\times \to \ker \phi \).

When \( \mathbb{Z}[\gamma_m] \) is a maximal order, this is (exercise in Cox). Explicitly this is given by: for a class \([\alpha] \in (O_I/dO_I)^\times \), choose a representative \( \alpha \in O_I \) with \( \alpha \overline{\alpha} > 0 \) and \( \alpha \) relatively prime to \( 1 - 4m \). Then we map \([\alpha]\) to the narrow ideal class

\[
[\alpha O_I \cap \mathbb{Z}[\gamma_m], \alpha \overline{\alpha}].
\]

Hence

\[
|\ker(\phi)| \leq |(O_I/dO_I)^\times| < d^2
\]
as desired. (In fact, one can do better using the precise formulas for class numbers of orders.) \( \square \)

**Proof of Theorem 2.10.** We divide up our count of quadratic forms according to the content. Note that

\[
X^{-3/2}T_d(X) = \sum_{d \geq 1} X^{-3/2}T_d(X).
\]

We claim that the series \( \sum_{d \geq 1} X^{-3/2}T_d(X) \) satisfies the conditions of the dominated convergence theorem. Indeed, for every \( d \), \( T_d(X) \) is at most the number of \( \text{SL}_2 \)-equivalence classes of primitive binary quadratic forms with odd discriminant in the range \([-d^{-2}X, d^{-2}X] \). By Gauss’s count of binary quadratic forms, the
latter is bounded above by \( cd^{-3}X^{3/2} \) for some uniform constant \( c \). Hence \( X^{-3/2}\mathbb{T}_d(X) \leq cd^{-3} \) for all \( X \), and so the series \( \sum_{d \geq 1} X^{-3/2}\mathbb{T}_d(X) \) is dominated by the convergent series \( \sum_{d \geq 1} cd^{-3} \).

So it suffices to prove \( \lim_{X \to \infty} X^{-3/2}\mathbb{T}_d(X) = 0 \) for any fixed \( d \). We’ll show that \( \lim_{X \to \infty} X^{-3/2}\mathbb{T}_d(X) < \epsilon \) for any \( \epsilon > 0 \).

We give an upper bound for \( \mathbb{T}_d(X) \) using equation (11).

Let

\[ S = \{ (\alpha, \beta', \gamma) \in \mathbb{R}^3 \mid |2\beta' + 1| \leq |\gamma| \leq |\alpha| \}. \]

By reduction theory of binary quadratic forms, every \( \text{SL}_2(\mathbb{Z}) \)-orbit of binary quadratic forms has at least one representative of the form \( ax^2 + (2b' + 1)xy + cy^2 \) with \((a, b', c) \in S \) (possibly more than one if the form is indefinite or if one of the representatives lies on the boundary of \( S \)).

Using this and Lemma 2.17 we bound the right hand side of (11) as

\[
\mathbb{T}_d(X) \leq \sum_{Q = ax^2 + (2b' + 1)xy + cy^2} w(Q) \sum_{(a, b', c) \in S \cap \mathbb{Z}^3} \sum_{m = b'(b' + 1) - ac \in [-X, X]} \max(1, d^{2(21 - \omega(b'(b' + 1) - ac))})
\]

Now, we choose a parameter \( N \), and split the sum into the contribution from triples \((a, b', c)\) with

\[ \omega(b'(b' + 1) - ac) \geq N \]

and those triples with

\[ \omega(b'(b' + 1) - ac) < N. \]

The total contribution of the triples with

\[ \omega(b'(b' + 1) - ac) \geq N \]

is at most

\[
d^{21 - N} \{ (a, b', c) \in S \cap \mathbb{Z}^3 \mid \gcd(a, 2b' + 1, c) = d, b'(b' + 1) - ac \in [-X, X] \} \leq 2^{1 - N} \kappa_1(d)X^{3/2}
\]

for some real constant \( \kappa_1(d) \) depending on \( d \), by the same Davenport’s Lemma argument used in the proof of (11).

On the other hand, since all weights are \( \leq 1 \), the contribution of the triples \((a, b', c)\) such that

\[ \omega(b'(b' + 1) - ac) < N \]

is at most

\[
\{ (a, b', c) \in S \cap \mathbb{Z}^3 \mid \gcd(a, 2b' + 1, c) = d, b'(b' + 1) - ac \in [-X, X] \text{ has at most } r \text{ prime factors} \}
\]

However, a naïve sieving argument shows that the triples \((a, b', c)\) with

\[ \omega(b'(b' + 1) - ac) \geq N \]

have density 0 in \( S \cap \mathbb{Z}^3 \). To be more precise, if we pick a real parameter \( r \), then the set

\[ A(N, r) = \{ (a, b', c) \in S \cap \mathbb{Z}^3 \mid b'(b' + 1) - ac \in [-X, X] \text{ has } < N \text{ prime factors } \leq r \}
\]

is a union of sublattices of \( \mathbb{Z}^3 \). By a standard sieving argument, the density \( \rho(N, r) \) of \( A(N, r) \) in \( \mathbb{Z}^3 \) goes to 0 as \( r \to \infty \) for fixed \( N \).

Applying Davenport’s lemma to this union of sublattices, we obtain

\[
\{ (a, b', c) \in S \cap \mathbb{Z}^3 \mid \gcd(a, 2b' + 1, c) = d, b'(b' + 1) - ac \in [-X, X] \text{ has at most } r \text{ prime factors} \}
\]

(13)

\[
\leq \{ (a, b', c) \in S \cap A(N, r) \mid b'(b' + 1) - ac \in [-X, X] \}
\]

\[ = \rho(N, r)X^{3/2} + \epsilon_{N, r}(X) \]

where the error term \( \epsilon_{N, r}(X) \) is \( O(X \log X) \) for fixed \( N \) and \( r \).
Combining equations (12) and (13) we get

\[ T_d(X) \leq 2^{1-N} \kappa_1(d) X^{3/2} + \rho(N, r) \kappa_2 X^{3/2} + \epsilon_{N, r}(X) \]

so

\[ \lim_{X \to \infty} X^{-3/2} T_d(X) \leq 2^{1-N} \kappa_1(d) + \rho(N, r) \kappa_2. \]

But we can make the right hand side arbitrarily small by first choosing \( N \) arbitrarily large and then choosing \( r \) arbitrarily large depending on \( N \).

Hence \( \lim_{X \to \infty} X^{-3/2} T_d(X) = 0 \) as desired.

\[ \square \]

References

[1] E. Bayer and F. Michel. Finitude du nombre des classes d’isomorphisme des structures isométriques entières. Comment. Math. Helv., 54(3):378–396, 1979.
[2] M. Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. Ann. of Math. (2), 159(1):217–250, 2004.
[3] H. Cohen and H. W. Lenstra, Jr. Heuristics on class groups of number fields. In Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), volume 1068 of Lecture Notes in Math., pages 33–62. Springer, Berlin, 1984.
[4] H. Davenport. On a principle of Lipschitz. J. London Math. Soc., 26:179–183, 1951.
[5] M. Farber. Classification of simple knots. Uspekhi Mat. Nauk, 38(5(233)):59–106, 1983.
[6] Stefan Friedl and Mark Powell. A calculation of Blanchfield pairings of 3-manifolds and knots. Mosc. Math. J., 17(1):59–77, 2017.
[7] H. Iwaniec. Rosser’s sieve. Acta Arith., 36(2):171–202, 1980.
[8] C. Kearton. Classification of simple knots by Blanchfield duality. Bull. Amer. Math. Soc., 79:952–955, 1973.
[9] C. Kearton. Blanchfield duality and simple knots. Trans. Amer. Math. Soc., 202:141–160, 1975.
[10] J. Levine. Unknotting spheres in codimension two. Topology, 4:9–16, 1965.
[11] J. Levine. Polynomial invariants of knots of codimension two. Ann. of Math. (2), 84:537–554, 1966.
[12] J. Levine. An algebraic classification of some knots of codimension two. Comment. Math. Helv., 45:185–198, 1970.
[13] J. Levine. Knot modules. I. Trans. Amer. Math. Soc., 229:1–50, 1977.
[14] A. B. Miller. Asymptotics for Sp\(_2\)-orbits on quadratic forms.
[15] A. B. Miller. Counting simple knots via arithmetic invariant theory. Princeton Ph.D. Thesis, 2014.
[16] H. Trotter. On S-equivalence of Seifert matrices. Invent. Math., 20:173–207, 1973.
[17] H. Trotter. Knot modules and Seifert matrices. In Knot theory (Proc. Sem., Plans-sur-Bex, 1977), volume 685 of Lecture Notes in Math., pages 291–299. Springer, Berlin, 1978.