Quadratic Forms Over Hasse Domains:

Finiteness of the Hermite Constant

by

Jacob Hicks

(Under the Direction of Pete L. Clark)

Abstract

This document describes three previous papers that proved representation theorems for binary and quaternary quadratic forms using Geometry of Numbers tools and a computational approach. It then goes on to generalize the some of the Geometry of Numbers tools used to S-integer rings of global fields.

Index words: Geometry of Numbers, Hermite Constant, Quadratic Forms, Lattice, Universality

Quadratic Forms Over Hasse Domains:
Finiteness of the Hermite Constant

by

Jacob Hicks

B.S. Mathematical Sciences, Clemson University, 2005

B.S. Computer Science, Clemson University, 2005

M.A. Mathematics, University of Georgia, 2012

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2016

Quadratic Forms Over Hasse Domains:

Finiteness of the Hermite Constant

by

Jacob Hicks

Approved:

Major Professor: Pete L. Clark

Committee: Daniel Krashen
Robert Rumely
Robert Varley

Electronic Version Approved:

Suzanne Barbour
Dean of the Graduate School
The University of Georgia
May 2016

Quadratic Forms Over Hasse Domains:

Finiteness of the Hermite Constant

Jacob Hicks

April 29, 2016

Acknowledgments

I first acknowledge Pete Clark, Hans Parshall, Kate Thompson, and Nathan Walters who were my coauthors on the works appearing in this document. I cannot begin to express the depth of my appreciation for my parents whose love and support helped me through both the brightest and darkest times of graduate school. I would like to thank Pete for being compassionate and helpful, and for being willing to work with me to discover what it would take for me to have a successful graduate career.

Brian and Cristina have been my best friends throughout my graduate school experience and a reliable refuge of fun, laughter, and rest. My thanks to Kate motivated me by her example and encouraged me by her friendship, sarcasm, and food. I would also like to thank Laura and the rest of the staff in the math department for being so eager to help, encouraging, and great to talk with for all the graduate students.

My church family has been a constant reminder to keep things in an eternal perspective. My Bible study with its ever changing makeup has always been a place to find people who both understand the rigors of graduate school and that there is a life outside of it. Most of all, I want to thank my God. Even though I was often not aware of it at the time, looking back His love was always there leading, guiding, and comforting me.

Contents

List of Tables

Chapter 1

Introduction

This thesis presents work done on bounding the Hermite constant and proving representation theorems of quadratic forms using a mixture of Geometry of numbers and computational tools. It begins with work done on binary quadratic forms jointly conducted with Hans Parshall, Pete L. Clark, and Katherine Thompson. This work was published in the journal Integers [8]. The main result of the work was:

Theorem 4.3. *Let $q = \langle A, B, C \rangle$ be one of the 2779 primitive, positive definite integral binary quadratic forms in Table A.1, and let $\Delta = B^2 - 4AC$ be the discriminant of q. For a prime $p \nmid 2\Delta$, the following are equivalent:*

1. *The form q integrally represents p: there are $x, y \in \mathbb{Z}$ with $q(x, y) = p$.*
2. *All of the following conditions hold:*
   - *(a)* $\left(\frac{\Delta}{p}\right) = 1$.
   - *(b) For each odd prime $m \mid \Delta$, if $m \nmid A$, then $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right)$, and if $m \nmid C$, then $\left(\frac{p}{m}\right) = \left(\frac{C}{m}\right)$.*
   - *(c) If $16 \mid \Delta$ and $2 \nmid A$, then $p \equiv A \pmod 4$. If $16 \mid \Delta$ and $2 \nmid C$, then $p \equiv C \pmod 4$.*
   - *(d) If $32 \mid \Delta$ and $2 \nmid A$, then $p \equiv A \pmod 8$. If $32 \mid \Delta$ and $2 \nmid C$, then $p \equiv C \pmod 8$.*

Following the work on binary forms, we consider quaternary quadratic forms. This work was jointly conducted with Pete L. Clark, Katherine Thompson, and Nathan Walters that was also published in Integers [9]. We produced proofs of the universality of nine diagonal quadratic forms of square discriminant. All but one of these was done using by hand computations. Then the study of quaternary forms continues in work conducted with Katherine Thompson on non-diagonal quadratic forms culminating in:

Theorem 6.1. *The 105 integral, positive definite, quaternary quadratic forms appearing in Tables A.2 and A.3 of the Appendix are universal.*

After considering forms over the integers, our attention turned to the case of totally real number fields. The value of the Hermite constant is know exactly in the case of integers in dimension two and four that we studied. In the case of totally real number fields, the exact value of the Hermite constant is not yet known. A paper of Icaza [28] had bounded the Hermite constant over number fields and an insight gained from a paper of Deutsch [14] led to an improvement in her bound for totally real number fields given by

Theorem 7.6. *Let $K/\mathbb{Q}$ be a totally real number field of degree d, let $d(K)$ be the discriminate of the number field, and let B_N be the unit ball. For all $N \in \mathbb{Z}^+$ we have*

$$\gamma_N^+(\mathbb{Z}_K) \le d^{-2d} 4^d \left(\frac{(dN)!}{(N!)^d}\right)^{\frac{2}{N}} |d(K)| \left(\mathrm{Vol}\, B_N\right)^{\frac{-2d}{N}}$$

Finally the idea of extending the Hermite constant to other classes of fields and rings led to the following

Theorem 8.7. *$\gamma_N(R)$ is finite for all global fields K with characteristic not equal to 2 and all S-integer rings of K for all dimensions N.*

Chapter 2

Quadratic Forms

2.1 Quadratic forms over a ring

Let R be a commutative ring, and let $N \in \mathbb{Z}^+$. An *N-ary quadratic form over R* is a homogeneous quadratic polynomial

$$q(v) = q(x_1, \ldots, x_N) = \sum_{1 \le i \le j \le N} a_{ij} x_i x_j \in R[x_1, \ldots, x_N], a_{ij} \in R. \tag{2.1}$$

Two quadratic forms $q(v) = q(x_1, \ldots, x_N)$, $q'(v) = q'(x_1, \ldots, x_N)$ over R are *equivalent over R* if there is $A \in \mathrm{GL}_N(R)$ such that $q(Av) = q'(v)$. We write $q \cong q'$.

Let $q(v)$ be an n-ary quadratic form over R, and let $d \in R$. We say that q *R-represents d* if there exists $v \in R^n$ such that $q(v) = d$. We say that q is *isotropic* over R if there exists $v \in R^n$, $v \neq (0, \ldots, 0)$ such that $q(v) = 0$; otherwise q is *anisotropic*. We say q is *universal* over R if q R-represents every element of R.

Base change: Let S be another commutative ring, and let $\varphi : R \to S$ be a ring homomorphism. Given an n-ary quadratic form q over R and such a map φ, we may associate an n-ary quadratic form $q_{/S}$ in the evident way: namely

$$q_{/S}(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} \varphi(a_{ij})x_jx_j \in S[x_1,\ldots,x_n].$$

Base change is useful for showing that q *does not* represent $d \in R$: if q R-represents d, then for all homomorphisms $\varphi : R \to S$, $q_{/S}$ S-represents $\varphi(d)$: indeed, if $q(x_1,\ldots,x_n) = d$, then $q_{/S}(\varphi(x_1),\ldots,\varphi(x_n)) = \varphi(d)$. For succinctness we will say that q S-represents d. For instance, let $R = \mathbb{Z}$ and $q = x^2 + y^2$. Then q does not $\mathbb{Z}$-represent any negative integers. The formal justification of this is that in the ordered field $\mathbb{R}$ any sum of squares is non-negative, so q does not even $\mathbb{R}$-represent any negative integers. Moreover, q does not represent any $n \equiv 3 \pmod 4$: taking the map $\varphi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, by enumeration of cases one sees that $x^2 + y^2 = 3$ has no solution in $\mathbb{Z}/4\mathbb{Z}$.

Suppose that R is a domain of characteristic different from 2 and with fraction field K. For the n-ary quadratic form $q(v)$ of (2.1), let $M_q = (m_{ij}) \in M_n(K)$ be the matrix with $m_{ii} = a_{ii}$ for all i and $m_{ij} = \frac{a_{ij}}{2}$ for all $i \neq j$. Then, putting $v = (x_1,\ldots,x_n)^t$, we have

$$q(v) = v^t M_q v. \tag{2.2}$$

The form q is *classical* if $M_q \in M_n(R)$, or equivalently, $a_{ij} \in 2R$ for all $i \neq j$. Diagonal forms are classical. Two n-ary forms q and q' are equivalent over R iff there exists $A \in \mathrm{GL}_n(R)$ with $M_{q'} = AM_qA^t$. Then $\det M_{q'} = (\det A)^2 \det M_q$, which shows that the class $\operatorname{disc} q$ of $\det M_q$ modulo $(R^\times)^2$ is an invariant of the equivalence class of q, called the *discriminant* of q. When $R = \mathbb{Z}$, $(\mathbb{Z}^\times)^2 = \{1\}$, so $\operatorname{disc} q$ is a well-defined integer. In general we say q is *nondegenerate* if $\operatorname{disc} q \neq 0$.

Let $q_1(x_1,\ldots,x_m)$ be an m-ary quadratic form over R and $q_2(y_1,\ldots,y_n)$ be an n-ary quadratic form over R. We define their *direct sum* $q_1 \oplus q_2$ to be the $(m+n)$-ary form $q(x_1,\ldots,x_m,y_1,\ldots,y_n) =$

$q_1(x_1, \ldots, x_m) + q_2(y_1, \ldots, y_n)$.

2.2 Quadratic forms over a field of characteristic not equal to 2

The theory of quadratic forms is considerably simpler when $R = K$ is a field of characteristic different from 2. The results that we need are from Chapter 1 of the theory of quadratic forms over fields [31, Ch. I].

Fact 2.1. *[31, Cor. I.2.4]: Every form q over K is K-equivalent to a diagonal form $(a_1, \ldots, a_n) := a_1x_1^2 + \ldots + a_nx_n^2$. In other words, there is $A \in \mathrm{GL}_n(K)$ such that $AM_qA^t = D(a_1, \ldots, a_n)$, where $D(a_1, \ldots, a_n)$ is diagonal with (i, i) entry a_i.*

The binary form $\mathbb{H} = (1, -1)$ plays a distinguished role in the theory.

Fact 2.2. *[31, Thm. 1.3.2]: For a nondegenerate binary form $q(x, y)$ over K, the following are equivalent:*

1. *q is K-equivalent to $\mathbb{H}$.*
2. $\operatorname{disc} q = -1$.
3. *q is isotropic.*

Fact 2.3. *[31, Thm. 1.3.4(2)]: For a nondegenerate quadratic form q over K, the following are equivalent:*

1. *q is isotropic.*
2. *There exists a quadratic form q' such that $q \cong q' \oplus \mathbb{H}$.*

A quadratic form is *hyperbolic* if it is isomorphic to $\bigoplus_{i=1}^{r} \mathbb{H}$ for some $r \in \mathbb{N}$.

2.3 Totally isotropic subspaces

We may view an n-ary quadratic form q as a map $q : K^n \to K$. A K-subspace W of K^n is called *totally isotropic* for q if $q|_W \equiv 0$.

Fact 2.4. *[31, Thm. 1.3.4(1)]: Let $q : K^n \to K$ be a nondegenerate quadratic form, and let $W \subset K^n$ be a totally isotropic subspace of dimension r. Then $q \cong \mathbb{H}^r \oplus q'$.*

Proposition 2.5. *Let q be a nondegenerate, isotropic quaternary quadratic form over a field K of characteristic different from 2. The following are equivalent:*

(i) q is hyperbolic.

(ii) $\operatorname{disc} q = 1$.

(iii) q admits a two-dimensional totally isotropic subspace.

Proof. (i) $\implies$ (ii): A quaternary hyperbolic form q is equivalent to the diagonal form $(1, -1, 1, -1)$, which has discriminant 1.

(ii) $\implies$ (i): Since q is isotropic, by Fact 2.3, $q \cong \mathbb{H} \oplus q'$, with q' binary. We have

$$1 = \operatorname{disc} q = (\operatorname{disc} \mathbb{H}) \cdot (\operatorname{disc} q') = -\operatorname{disc} q',$$

so $\operatorname{disc} q' = -1$. By Fact 2.2, $q' \cong \mathbb{H}$, so $q \cong \mathbb{H} \oplus \mathbb{H}$.

(i) $\implies$ (iii): We may assume $q = \mathbb{H} \oplus \mathbb{H} = (1, -1, 1, -1)$, in which case $W = \langle e_1 - e_2, e_3 - e_4 \rangle$ is a 2-dimensional totally isotropic subspace.

(iii) $\implies$ (i): This follows immediately from Fact 2.4. □

Chapter 3

Classical Geometry of Numbers

3.1 Lattices

We begin with a treatment of integral lattices. Fix some positive integer N. We can endow $\mathbb{R}^N$ with the structure of a locally compact topological group under addition. We can take a *lattice* in $\mathbb{R}^N$ to be discrete subgroup which is free of rank N. Thus we have that a lattice can be given by the $\mathbb{Z}$-span of an $\mathbb{R}$-basis for $\mathbb{R}^N$. This basis is not unique for a given lattice. Any invertible $\mathbb{Z}$-linear transformation with determinant ± 1 will give another basis. For the remainder of the chapter we will take $a_1, a_2, \ldots, a_N$ to be a basis for a lattice Λ.

If we view the basis vectors as the columns of a matrix find that $\det(a_1, a_2, \ldots, a_N)$ is an invariant of the lattice up to multiplication by ± 1. Hence if we take $|\det(a_1, a_2, \ldots, a_N)|$ we have an invariant of the lattice. In a more abstract setting, let a group G act on a space X. A *fundamental region* is a subset $R \subset X$ that contains exactly one element from every G orbit on X. For any lattice, Λ we can let Λ act on $\mathbb{R}^N$ by translation. Viewing this as in the more abstract setting yields a fundamental region that is the *fundamental parallelepiped*. This parallelepiped tiles the space with its translates. The volume of this fundamental parallelepiped is independent of the chosen basis and is known as the *covolume* of the lattice which will be denoted $\mathrm{Covol}(\Lambda)$. This covolume is also the determinant of the lattice. In particular since the basis vectors must be linearly independent, the covolume must be positive.

A lattice is a group under addition. If we have another lattice Γ such that $\Gamma \subset \Lambda$, then this lattice is called a sublattice of Λ and is in addition a subgroup. The index of the lattice is the sublattice is $D = \frac{\operatorname{Covol}\Gamma}{\operatorname{Covol}\Lambda}$. The index is independent of the choice of basis.

3.2 Minkowski's Convex Body Theorem

As Cassels says in his Introduction to the Geometry of Numbers, the whole of the geometry of Numbers may be said to have sprung from Minkowski's convex body theorem[4, p.64]. The statement of the theorem is straightforward:

Theorem 3.1 (Minkowski's Convex Body Theorem)**.** *If a set of point in Euclidean N-space is symmetric about the origin (contains $-x$ whenever it contains x) and convex [ie contains the whole line segment*

$$\lambda x + (1 - \lambda)y, 0 \leq \lambda \leq 1$$

when it contains x and y] and has volume $V > 2^N$, then it always contains a $\mathbb{Z}$-lattice point other than the origin.

It is clear that this is the best possible bound for such a theorem because we can take the open hypercube surrounding the origin and containing no other lattice points except on its open boundary. This shape has volume $V = 2^N$, is symmetric about the origin, and is convex yet contains no integral points except the origin.

Minkowski's convex body theorem is immediately generalized to the case of lattice points by: If Λ is a lattice and a set of point in Euclidean N-space space is symmetric about the origin and convex and has volume $V > 2^N \operatorname{Covol}\Lambda$, then it always contains an lattice point other than the origin. This theorem shows a relationship between the geometric properties of volume, convexity, and symmetry and the arithmetical property of containing lattice points [4].

3.3 Minkowski's Linear Forms Theorem

Theorem 3.2 (Minkowski's Linear Forms Theorem)**.** *is given by: Let $\Lambda \subset \mathbb{R}^N$ be a lattice. Let $C = (c_{ij}) \in M_N(\mathbb{R})$ be a matrix. Consider the associated system of linear forms.*

$$L_i(x) = L_i(x_1, \ldots, x_N) = \sum_{j=1}^{N} c_{ij}x_j, 1 \leq i \leq n$$

Let $\epsilon_1, \ldots, \epsilon_N$ be positive real numbers such that

$$|\det(C)| \operatorname{Covol} \Lambda \leq \prod_{i=1}^{N} \epsilon_i$$

Then there is an $x \in \Lambda^{\bullet}$, with $|L_i(x)| \leq \epsilon_i$ for all $1 \leq i \leq N$.

For proof see [4, p.73]

3.4 Hermite Constant

The Hermite constant is an invariant of N-dimensional lattices. Colloquially, it determines how short an element of a lattice in Euclidean space can be. More formally, γ_N for fixed $N > 0$ is defined to be: For a lattice $\Lambda \subset \mathbb{R}^N$ with unit covolume, let $\lambda(\Lambda)$ denote the least length of a nonzero element of L. Then $\sqrt{\gamma_N}$ is the maximum $\lambda(L)$ over all such lattices. This is also tied to knowing the densest sphere packing in a given dimension N [3].

This can be viewed as a specific case in which we fix a quadratic form, the square of the standard Euclidean distance formula and allow the lattice to vary. If we instead allow the quadratic form to be arbitrary and restrict the lattice, we arrive at the same constant. Let $\mathbb{Z}^N \subset \mathbb{R}^N$ be our lattice under consideration and let Q be the set of positive definite quadratic forms over $\mathbb{R}$ then

$$\gamma_N = \sup_{q \in Q} \inf_{x \in \mathbb{Z}^N} \frac{q(x)}{\operatorname{disc} q}$$

The bound in the 1 dimensional case is trivially 1. In the two dimensional case, Lagrange proved the constant is $\gamma_2 = \frac{2}{\sqrt{3}}$ [32]. Gauss proved the case of $N = 3$ to be $2^{\frac{1}{3}}$ [20]. Korkine-Zolotarev found that $\gamma_4 = \sqrt{2}$ [30]. The value is known for N up to 8 and for 24. A simple bound given by Hermite for all N is

$$\gamma_N \leq \left(\frac{4}{3}\right)^{\frac{N-1}{2}}.$$

This shows that the Hermite constant is finite for all N.

Chapter 4

Binary Quadratic Forms

This work in this chapter was done in the context of a VIGRE Research Group at the University of Georgia throughout the 2011-2012 academic year. The results given below appear in [8]. Co-first authors on this paper were Pete L. Clark, Hans Parshall, and Katherine Thompson.

We list 2779 regular primitive positive definite integral binary quadratic forms, and show that, conditional on the Generalized Riemann Hypothesis, this is the complete list of *regular*, positive definite binary integral quadratic forms (up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence). For each of these 2779 forms we determine the primes that they represent by elementary combinatorial methods, avoiding Gauss's genus theory. The key intermediate result is a *Small Multiple Theorem* for representations of primes by integral binary forms. This result and some computations lead to the main theorem:

Theorem 4.3. *Let $q = \langle A, B, C\rangle$ be one of the 2779 primitive, positive definite integral binary quadratic forms in Table A.1, and let $\Delta = B^2 - 4AC$ be the discriminant of q. For a prime $p \nmid 2\Delta$, the following are equivalent:*

1. *The form q integrally represents p: there are $x, y \in \mathbb{Z}$ with $q(x, y) = p$.*

2. *All of the following conditions hold:*

   (a) $\left(\frac{\Delta}{p}\right) = 1$.

(b) For each odd prime $m \mid \Delta$, if $m \nmid A$, then $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right)$, and if $m \nmid C$, then $\left(\frac{p}{m}\right) = \left(\frac{C}{m}\right)$.

(c) If $16 \mid \Delta$ and $2 \nmid A$, then $p \equiv A \pmod 4$. If $16 \mid \Delta$ and $2 \nmid C$, then $p \equiv C \pmod 4$.

(d) If $32 \mid \Delta$ and $2 \nmid A$, then $p \equiv A \pmod 8$. If $32 \mid \Delta$ and $2 \nmid C$, then $p \equiv C \pmod 8$.

4.1 Background

An *imaginary quadratic discriminant* is a negative integer Δ which is 0 or 1 modulo 4. For a given imaginary quadratic discriminant Δ, let $C(\Delta)$ be the set of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of primitive positive definite integral binary quadratic forms of discriminant Δ. Then $C(\Delta)$ is a finite set [12, Thm. 2.13] which, when endowed with Gauss's composition law, becomes a finite abelian group, the *class group of discriminant* Δ [12, Thm. 3.9].

Thus a form q of discriminant Δ determines an element $[q] \in C(\Delta)$. A quadratic form q is *ambiguous* if $[q]^2 = 1$. For a $q = \langle A, B, C\rangle$, the form $\overline{q} = \langle A, -B, C\rangle$ represents the inverse of $[q]$ in $C(\Delta)$ [12, Thm. 3.9]. Note that q and $\overline{q}$ are $\mathrm{GL}_2(\mathbb{Z})$-equivalent: $\overline{q}(x, y) = q(x, -y)$, so q and $\overline{q}$ represent the same integers.

A discriminant Δ is *idoneal* if every $q \in C(\Delta)$ is ambiguous; this holds if and only if $C(\Delta) \cong (\mathbb{Z}/2\mathbb{Z})^r$ for some $r \in \mathbb{N}$. A quadratic form is *idoneal* if its discriminant is idoneal. A discriminant Δ is *bi-idoneal* if $C(\Delta) \cong (\mathbb{Z}/4\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z})^r$ for some $r \in \mathbb{N}$. A quadratic form q is *bi-idoneal* if Δ is bi-idoneal and q is *not* ambiguous.

A *full congruence class of primes* is the set of all primes $p \nmid 2\Delta$ with $p \equiv n \pmod N$ for fixed coprime positive integers n and N. We say q is *regular* if the set of primes $p \nmid 2\Delta$ represented by q is a union of full congruence classes.

Theorem 4.1 (Fermat's Two Squares Theorem)**.** *An odd prime p is of the form $x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$.*

To rephrase in this terminology the form $q(x, y) = x^2 + y^2$ is regular. Much classical work on quadratic forms can be phrased as showing that certain specific binary quadratic forms represent full congruence classes of primes, or are regular. Among primitive, positive definite, integral binary quadratic forms, one could ask many questions. How many are regular? How many represent full congruence classes of primes? Remarkably, this problem has recently been solved (conditionally on GRH) but the answer did not appear explicitly in the literature until [8]. Here it is:

Theorem 4.2. *Let q be a primitive, positive definite integral binary quadratic form.*

1. *The following are equivalent:*

   (a) q is regular.

   (b) q represents a full congruence class of primes.

   (c) q is either idoneal or bi-idoneal.

2. *There are at least* 425 *and at most* 432 *imaginary quadratic discriminants which are either idoneal or bi-idoneal. These* 425 *known discriminants give rise to precisely* 2779 $\mathrm{SL}_2(\mathbb{Z})$-*equivalence classes of regular forms: see Table A.1.*

3. *The list of idoneal and bi-idoneal discriminants of part b) is complete among all imaginary quadratic discriminants* Δ *with* $|\Delta| \leq 80604484$. *Assuming the Riemann Hypothesis for Dedekind zeta functions of imaginary quadratic fields, there are precisely* 425 *imaginary discriminants which are idoneal or bi-idoneal.*

For these 2779 regular forms, it is natural to ask for explicit congruence conditions. The following result accomplishes this.

Theorem 4.3. *Let* $q = \langle A, B, C\rangle$ *be one of the* 2779 *primitive, positive definite integral binary quadratic forms in Table A.1, and let* $\Delta = B^2 - 4AC$ *be the discriminant of q. For a prime* $p \nmid 2\Delta$*, the following are equivalent:*

1. *The form q integrally represents p: there are* $x, y \in \mathbb{Z}$ *with* $q(x, y) = p$.

2. *All of the following conditions hold:*

   (a) $\left(\frac{\Delta}{p}\right) = 1$.

   (b) *For each odd prime* $m \mid \Delta$*, if* $m \nmid A$*, then* $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right)$*, and if* $m \nmid C$*, then* $\left(\frac{p}{m}\right) = \left(\frac{C}{m}\right)$.

   (c) *If* $16 \mid \Delta$ *and* $2 \nmid A$*, then* $p \equiv A \pmod 4$*. If* $16 \mid \Delta$ *and* $2 \nmid C$*, then* $p \equiv C \pmod 4$.

   (d) *If* $32 \mid \Delta$ *and* $2 \nmid A$*, then* $p \equiv A \pmod 8$*. If* $32 \mid \Delta$ *and* $2 \nmid C$*, then* $p \equiv C \pmod 8$.

Our main goal is to offer a new proof of Theorem 4.3 using none of Gauss's genus theory but instead using elementary ideas from the *Geometry of Numbers*. Our methods build on the classical proof of the Two Squares Theorem via Minkowski's Convex Body Theorem and its recent generalization to the 65 principal idoneal forms $x^2 + Dy^2$ of T. Hagedorn [21], although we find it simpler to use (sharp) bounds on minima of binary quadratic forms going back to Lagrange and Legendre.

We may compare the two methods as follows: let q be a binary form of discriminant Δ, and let $p \nmid 2\Delta$ be a prime. To analyze the question of whether q represents p, genus theory begins with the observation that $\left(\frac{\Delta}{p}\right) = 1$ if and only if some $q' \in C(\Delta)$ represents p and attempts to rule out the representation of p by all forms $q' \neq q$. Our method begins with a *small multiple theorem*: if $\left(\frac{\Delta}{p}\right) = 1$, then q represents some multiple kp of p with k bounded in terms of Δ and via a combination of *elimination* and *reduction* attempts to show that we may take $k = 1$. Our method is more computational – at present it is more a technique than a theory – and the reasons for its success in all 2779 cases are rather mysterious!

4.2 A Small Multiple Theorem

Let $q = \langle A, B, C \rangle$ be a real binary quadratic form with discriminant $\Delta \neq 0$. Recall:

• If $\Delta > 0$, then q is **indefinite**: it assumes both positive and negative values.

• If $\Delta < 0$ and $A, C > 0$, then q is **positive definite**: it assumes only positive values except at

$(x, y) = (0, 0)$.

• If $\Delta < 0$ and $A, C < 0$, then q is **negative definite**: it assumes only negative values except at $(x, y) = (0, 0)$. Since q is negative definite if and only if $-q$ is positive definite, negative definite forms do not require separate consideration.

Theorem 4.4. *Let $q = \langle A, B, C\rangle$ be a binary form over $\mathbb{R}$ with discriminant Δ.*
a) If $\Delta < 0$, there are integers x and y, not both zero, such that $|q(x, y)| \leq \sqrt{\frac{|\Delta|}{3}}$.
b) If $\Delta > 0$, there are integers x and y, not both zero, such that $|q(x, y)| \leq \sqrt{\frac{\Delta}{5}}$.

Proof. The core of the proof is the following "reduction lemma": if x_0, y_0 are coprime integers with $q(x_0, y_0) = M \neq 0$, then there are $b, c \in \mathbb{R}$ such that q is $\mathrm{SL}_2(\mathbb{Z})$-equivalent to $Mx^2 + bxy + cy^2$ with $-|M| < b \leq |M|$. For the details, see e.g. [23, Thm. 453, Thm. 454]. □

Proposition 4.5. *Let $q = \langle A, B, C\rangle$ be an integral form of discriminant Δ. Let p be an odd prime with $\left(\frac{\Delta}{p}\right) = 1$. Then there is an index p sublattice $\Lambda_p \subset \mathbb{Z}^2$ such that for all $(x, y) \in \Lambda_p$, we have $q(x, y) \equiv 0 \pmod{p}$.*

Proof. If $p \mid A$, take $M_p = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$ and $\Lambda_p = M_p\mathbb{Z}^2$. If $p \nmid A$, by the quadratic formula in $\mathbb{Z}/p\mathbb{Z}$, there is $r \in \mathbb{Z}$ with $Ar^2 + Br + C \equiv 0 \pmod{p}$; set $M_p = \begin{bmatrix} p & r \\ 0 & 1 \end{bmatrix}$ and $\Lambda_p = M_p\mathbb{Z}^2$. In either case, $q(x, y) \equiv 0 \pmod{p}$ for all $(x, y) \in \Lambda_p$. □

Theorem 4.6. *Let $q = \langle A, B, C\rangle$ be an integral form of discriminant Δ. Let p be an odd prime with $\left(\frac{\Delta}{p}\right) = 1$.*
a) If q is positive definite, there are $x, y, k \in \mathbb{Z}$ with $q(x, y) = kp$ and $1 \leq k \leq \sqrt{\frac{|\Delta|}{3}}$.
b) If q is indefinite, there are $x, y, k \in \mathbb{Z}$ with $q(x, y) = kp$ and $1 \leq |k| \leq \sqrt{\frac{\Delta}{5}}$.

Proof. By Proposition 4.5, there is an index p sublattice $\Lambda_p = M_p\mathbb{Z}^2 \subset \mathbb{Z}^2$ with $q(x, y) \equiv 0 \pmod{p}$ for all $(x, y) \in \Lambda_p$. Thus the quadratic form $q'(x, y) = q(M_p(x, y))$ has discriminant

$(\det M_p)^2\Delta = p^2\Delta$ and is such that $q'(x,y) \equiv 0 \pmod{p}$ for all $(x,y) \in \mathbb{Z}^2$. Apply Theorem 4.4 to q': if q is positive definite, there are integers x and y, not both zero, such that $|q(M_p(x,y)| = |q'(x,y)| \leq \left(\sqrt{\frac{|\Delta|}{3}}\right)p$. Thus $q(x,y) = kp$ with $1 \leq |k| \leq \sqrt{\frac{|\Delta|}{3}}$; since q is positive definite, $k > 0$. If $\Delta > 0$, there are integers x and y, not both zero, such that $|q(M_p(x,y)| = |q'(x,y)| \leq \left(\sqrt{\frac{\Delta}{5}}\right)p$, so $q(x,y) = kp$ with $1 \leq |k| \leq \sqrt{\frac{\Delta}{5}}$. □

Remark 4.7. *: Taking $q = \langle 1,1,1\rangle$ (resp. $\langle 1,1,-1\rangle$) shows that the bound in Theorem 4.6a) (resp. Theorem 4.6b) is sharp.*

Remark 4.8. *Let $q = \langle A,B,C\rangle$ be positive definite with $|\Delta| < 12$. Then $\sqrt{\frac{|\Delta|}{3}} < 2$, and Theorem 4.6 takes the form: every odd prime p with $\left(\frac{\Delta}{p}\right) = 1$ is $\mathbb{Z}$-represented by q. It is easy to see that these are the only odd primes $p \nmid 2\Delta$ which are represented by q (c.f. Proposition 4.9), so this proves Theorem 4.3 for these forms, namely for $\langle 1,1,1\rangle$, $\langle 1,0,1\rangle$, $\langle 1,1,2\rangle$, $\langle 1,0,2\rangle$, and $\langle 1,1,3\rangle$.*

4.3 2779 Regular Forms

In this section we will use Theorem 4.6 to prove Theorem 4.3.

In this chapter we will take "forms" to be primitive, positive definite integral binary quadratic forms.

4.3.1 Necessity

Proposition 4.9. *Let $q = \langle A,B,C\rangle$ be a form with discriminant Δ. Let p be an odd prime not dividing Δ. Suppose there exist $x,y \in \mathbb{Z}$ with $q(x,y) = p$. Then p satisfies conditions (i) - (iv) from Theorem 4.3.*

Proof. Via the discriminant-preserving transformation $\langle A,B,C\rangle \mapsto \langle C,B,A\rangle$ we may assume in $m \nmid A$ in part (ii) and $2 \nmid A$ in parts (iii) and (iv); otherwise, q would not be primitive.

(i) If both x and y were divisible by p, this would imply $p^2 \mid q(x,y) = p$, a contradiction. If $p \nmid y$, then we have $A(xy^{-1})^2 + B(xy^{-1}) + C \equiv 0 \pmod{p}$. Let $r \in \mathbb{Z}$ with $r \equiv xy^{-1} \pmod{p}$. Then

$$(2Ar + B)^2 = 4A(Ar^2 + Br + C) + B^2 - 4AC \equiv \Delta \pmod{p}$$

As $p \nmid \Delta$, we conclude $\left(\frac{\Delta}{p}\right) = 1$. The case $p \nmid x$ follows similarly.

(ii) Let m be an odd prime such that $m \mid \Delta$ and $m \nmid A$. Via a change of variables we can diagonalize q over $\mathbb{Z}/m\mathbb{Z}$ as $\langle A, 0, C - B^2(4A)^{-1}\rangle$, so there are $w, z \in \mathbb{Z}$ with

$$p = q(x,y) \equiv Aw^2 + (C - B^2(4A)^{-1})z^2 \pmod{m}.$$

Multiplying by $4A$ gives $4Ap \equiv 4A^2w^2 \pmod{m}$. Hence $p \equiv Aw^2 \pmod{m}$. It follows that $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right)$.

(iii) Suppose $2 \nmid A$ and $\Delta \equiv 0 \pmod{16}$. We have $B^2 \equiv 4AC \pmod{16}$, so $B = 2B_0$ for some $B_0 \in \mathbb{Z}$. Then $4(B_0^2 - AC) \equiv 0 \pmod{16}$, so $B_0^2 - AC \equiv 0 \pmod{4}$.

Case 1: B_0 is odd. Then $A \equiv C \equiv \pm 1 \pmod{4}$. Now, $Ax^2 + 2B_0xy + Cy^2 = p$, so $x^2 + y^2 \equiv p \equiv 1 \pmod{2}$, and $x \not\equiv y \pmod{2}$. If $y \equiv 0 \pmod{2}$, $p \equiv A \pmod{4}$ as claimed. Similarly if $x \equiv 0 \pmod{2}$, $p \equiv C \pmod{4}$. But since $A \equiv C \pmod{4}$, $p \equiv A \pmod{4}$ as claimed.

Case 2: B_0 is even. Then $AC \equiv 0 \pmod{4}$. As $2 \nmid A$, $C \equiv 0 \pmod{4}$. Hence, $Ax^2 \equiv p \pmod{4}$, and so $p \equiv A \pmod{4}$ as claimed.

(iv) Suppose $2 \nmid A$ and $\Delta \equiv 0 \pmod{32}$. Put $B = 2B_0$, so $B_0^2 - AC \equiv 0 \pmod{8}$.

Case 1: B_0 is odd, Then $A \equiv C \pmod{2}$ and in fact $A \equiv C \pmod{8}$. Thus $x^2 + y^2 \equiv p \equiv 1 \pmod{2}$, so $x \not\equiv y \pmod{2}$. If $y \equiv 0 \pmod{2}$, set $y = 2y_0$. Then $Ax^2 + 4y_0(B_0x + Cy_0) = p$. If y_0 is even, then $Ax^2 \equiv A \equiv p \pmod{8}$. If instead y_0 is odd, then since B_0, x, and C are odd, $B_0x + Cy_0$ is even and $Ax^2 \equiv A \equiv p \pmod{8}$. Similarly if $x \equiv 0 \pmod{2}$, then $p \equiv C \equiv A \pmod{8}$.

Case 2: B_0 is even. Put $B_0 = 2B_1$ and $C = 4C_0$, so $B_1^2 \equiv AC_0 \pmod 2$ and

$$p = Ax^2 + Bxy + Cy^2 = Ax^2 + 4y(B_1x + C_0y).$$

Thus x is odd and $x^2 \equiv 1 \pmod 8$. If y is even, then $p \equiv Ax^2 \equiv A \pmod 8$. If y is odd then either $B_1 \equiv C_0 \equiv 0 \pmod 2$ so $p \equiv Ax^2 \equiv A \pmod 8$ or $B_1 \equiv C_0 \equiv 1 \pmod 2$, so $B_1x + C_0y$ is even and once again $p \equiv Ax^2 \equiv A \pmod 8$. □

4.3.2 Sufficiency

Our proof that (b) implies (a) in Theorem 4.3 is handled individually for each of the 2779 forms. For each form, we apply a three step process. First, we use Theorem 4.6 to demonstrate that our form represents a small multiple of a prime. In the second step, we *eliminate* certain multiples from consideration. In the final step, we *reduce* the remaining multiples to find a representation of p.

Example 4.10. *Consider $q = \langle 3, 3, 5 \rangle$ with $\Delta = -51$. Let p be an odd prime not dividing Δ that satisfies conditions (i) - (iv) of Theorem 4.3.*

Step 1: From condition (i) of Theorem 4.3, $\left(\frac{\Delta}{p}\right) = 1$. Apply Theorem 4.6: there are $x, y, k \in \mathbb{Z}$ with $q(x, y) = kp$ and $1 \le k \le \sqrt{\frac{51}{3}} = 4.123\ldots$.

Step 2 (Elimination): We will show that the cases $k = 2$ and $k = 3$ cannot occur.

• *Suppose $q(x, y) = 2p$. Then x and y are both even, so $q(x, y) = 2p \equiv 0 \pmod 4$, contradicting the fact that p is odd.*

• *Suppose $q(x, y) = 3p$. Then $q(x, y) \equiv 5y^2 \equiv 0 \pmod 3$, so $3 \mid y$. Hence, $q(x, y) \equiv 3x^2 \equiv 3p \pmod 9$, so $\left(\frac{p}{3}\right) = 1$. As $3 \mid \Delta$, from condition (ii) of Theorem 4.3, $\left(\frac{p}{3}\right) = \left(\frac{5}{3}\right) = -1$: contradiction.*

Step 3 (Reduction): We cannot hope to eliminate the possibility of $k = 4$: we want to show that *there are $x, y \in \mathbb{Z}$ such that $q(x, y) = p$, and then necessarily $q(2x, 2y) = 4p$. (A similar argument will be needed for any value of k which is a perfect square). We must instead argue that a representation of $4p$ by q implies a representation of p by q. In this case, this is easy: suppose $q(x, y) = 4p$. Then as above x and y are both even, so $q(\frac{x}{2}, \frac{y}{2}) = p$.*

In Lemmas 4.11 and 4.12, we collect a number of congruence restrictions that apply assuming a form q represents kp. In particular, for our 2779 forms, we use Lemma 4.11 in the elimination step and Lemma 4.12 in the reduction step.

Lemma 4.11 (Elimination)**.** *Let $q = \langle A, B, C\rangle$ be a form of discriminant Δ. Let $p \nmid 2\Delta$ be a prime. Suppose there are $x, y, k \in \mathbb{Z}$, $k \geq 1$, with $q(x, y) = kp$.*
a) Let $a \in \mathbb{Z}$, $a > 1$. Suppose $2^{a+2} \mid \Delta$ and $2^a \mid B$. If $p \equiv A \pmod{2^a}$, then k is a square modulo 2^a.
b) If k is even, A, C are odd, $B \equiv 0 \pmod 4$ and $A + C \not\equiv 2 \pmod 4$, then $4 \mid k$.
c) Let m be an odd prime dividing Δ. If $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right)$, then k is a square modulo m.
d) Let m be an odd prime dividing k. If $\left(\frac{\Delta}{m}\right) = -1$ or $m^2 \mid \Delta$, then $m^2 \mid k$.
e) Let m be an odd prime dividing $\gcd(\Delta, k)$ such that $m^2 \nmid k$. If $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right)$ then $\left(\frac{k/m}{m}\right) = \left(\frac{-\Delta/m}{m}\right)$.

Proof. a) Since $\Delta \equiv B^2 \equiv 0 \left(\operatorname{mod} 2^{a+2}\right)$, and A is odd, $2^a \mid C$. Then $kp \equiv Ax^2 \equiv px^2 \pmod{2^a}$, and since p is odd, this implies $k \equiv x^2 \pmod{2^a}$.
b) We have $q(x, y) \equiv Ax^2 + Cy^2 \equiv A(x^2 - y^2) \equiv kp \pmod 4$. Since k is even, $x \equiv y \pmod 2$ and thus $kp \equiv A(x^2 - y^2) \equiv 0 \pmod 4$. Since p is odd, $4 \mid k$.
c) Via a change of variables we can diagonalize q over $\mathbb{Z}/m\mathbb{Z}$ as $\langle A, 0, C - B^2(4A)^{-1}\rangle$, so there are $w, z \in \mathbb{Z}$ with

$$kp = q(x, y) \equiv Aw^2 + (C - B^2(4A)^{-1})z^2 \pmod m .$$

Thus $4Akp \equiv 4A^2w^2 \pmod m$, implying $kp \equiv Aw^2 \pmod m$. As $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right) \neq 0$, k is a square modulo m.
d) Suppose first that $\left(\frac{\Delta}{m}\right) = -1$. We have $q(x, y) \equiv 0 \pmod m$. If $m \nmid y$, then $q(xy^{-1}, 1) \equiv 0 \pmod m$, so Δ is a square modulo m: contradiction. So $m \mid y$. Then $Ax^2 \equiv 0 \pmod m$, and

$m \nmid A$, since otherwise $\Delta \equiv B^2 \pmod{m}$. Hence $m \mid x$. Then $m^2 \mid q(x, y) = kp$, and since $\left(\frac{\Delta}{p}\right) = 1$, we have $p \neq m$ and $m^2 \mid k$.

Next suppose $m^2 \mid \Delta$. If $m \mid \gcd(A, C)$, since $m \mid \Delta$ we would also have $m \mid B$, contradicting the primitivity of q. We may assume without loss of generality that $m \nmid A$. As $B^2 - 4AC \equiv 0 \pmod{m}$, $C \equiv B^2(4A)^{-1} \pmod{m}$. Hence, $Ax^2 + Bxy + B^2(4A)^{-1}y^2 \equiv 0 \pmod{m}$, so by multiplying through by $4A$,

$$4A^2x^2 + 4ABxy + B^2y^2 \equiv (2Ax + By)^2 \equiv 0 \pmod{m}.$$

Since m is prime, $2Ax + By \equiv 0 \pmod{m}$, so $4A^2x^2 + 4ABxy + B^2y^2 \equiv 0 \pmod{m^2}$. As $B^2 - 4AC \equiv 0 \pmod{m^2}$, we have $B^2(4A)^{-1} \equiv C \pmod{m^2}$. Then

$$4Akp \equiv 4A^2x^2 + 4ABxy + B^2y^2 \equiv 0 \pmod{m^2}.$$

Since $p \nmid \Delta$, $m \neq p$. Then m does not divide $4Ap$, so $m^2 \mid k$.

e) Since $m \mid \Delta$ and $p \nmid \Delta$, $m \neq p$. We may write $\Delta = m\Delta_0$ and $k = mk_0$ with $\Delta_0, k_0 \in \mathbb{Z}$ and $m \nmid k_0$. Then

$$Ax^2 + Bxy + Cy^2 \equiv mk_0p \pmod{m^2}.$$

As in part d),

$$Ax^2 + Bxy + (B^2(4A)^{-1})y^2 \equiv 0 \pmod{m^2}.$$

Subtracting gives

$$(C - B^2(4A^{-1}))y^2 \equiv mk_0p \pmod{m^2}.$$

Since $\gcd(m, k_0p) = 1$, it follows that $m \nmid y$. Multiplying through by $4A$, we get

$$-m\Delta_0y^2 \equiv (4AC - B^2)y^2 \equiv 4Amk_0p \pmod{m^2}.$$

Then $(4Ak_0p + \Delta_0y^2)m \equiv 0 \pmod{m^2}$, so $4Apk_0 \equiv -\Delta_0y^2 \pmod{m}$. It follows that $\left(\frac{-\Delta_0}{m}\right) = \left(\frac{-\Delta_0y^2}{m}\right) =$

$\left(\frac{4Apk_0}{m}\right) \equiv \left(\frac{A}{m}\right)\left(\frac{p}{m}\right)\left(\frac{k_0}{m}\right) = \left(\frac{k_0}{m}\right)$. □

Lemma 4.12 (Reduction)**.** *Let $q = \langle A, B, C\rangle$ have discriminant Δ. Let p be an odd prime not dividing Δ. Suppose there exist $x, y, k \in \mathbb{Z}$ with $q(x, y) = kp$ and $k \geq 1$.*

a) Let $a \in \mathbb{Z}$ with $a \geq 1$. If $p \equiv A \pmod{2^a}$, then $q(x, y) \equiv Ak \pmod{2^a k}$.

b) Let $a \in \mathbb{Z}$ with $a \geq 0$, and let $m \mid \Delta$ be an odd prime. If $m^{2a} \mid k$, $m^{2a+1} \nmid k$, and $\left(\frac{p}{m}\right) = \left(\frac{A}{m}\right)$, then we have $\left(\frac{q(x,y)/m^{2a}}{m}\right) = \left(\frac{Ak/m^{2a}}{m}\right)$.

Proof. a) Write $p = 2^a\ell + A$. Then $q(x, y) \equiv k(2^a\ell + A) \equiv Ak \pmod{2^a k}$.

b) Write $k = m^{2a}k_0$. Then $\left(\frac{q(x,y)/m^{2a}}{m}\right) = \left(\frac{k_0 p}{m}\right) = \left(\frac{Ak_0}{m}\right)$. □

4.3.3 Proof of Theorem 4.3

(a) $\implies$ (b): This is Proposition 4.9.

(b) $\implies$ (a): Let $q = \langle A, B, C\rangle$ be one of the 2779 regular forms, and let $p \nmid 2\Delta$ be a prime satisfying conditions (i) - (iv) from Theorem 4.3.

Step 1: Using condition (i), Theorem 4.6 implies there exist $x, y, k \in \mathbb{Z}$ such that $q(x, y) = kp$ with $1 \leq k \leq \sqrt{\frac{|\Delta|}{3}}$.

Step 2 (Elimination): For each $k \in \{2, \ldots, \lfloor\sqrt{\frac{|\Delta|}{3}}\rfloor\}$, assume $q(x, y) = kp$. If k does not satisfy the conditions imposed on it by Lemma 1, we have a contradiction. We similarly have a contradiction if k does not satisfy the conditions imposed on it by applying Lemma 1 to the equivalent forms $q(y, x) = \langle C, B, A\rangle$ and $q(x + y, x + 2y) = \langle A + B + C, 2A + 3B + 4C, A + 2B + 4C\rangle$ representing kp. We eliminate these k from consideration.

Step 3 (Reduction): For each $k \in \{2, \ldots, \lfloor\sqrt{\frac{|\Delta|}{3}}\rfloor\}$ that was not eliminated in Step 2, assume $q(x, y) = kp$. Using a computer, we have verified that this assumption leads to a representation of p by q in every case. Our algorithm is as follows. First, we construct the finite set of matrices

$$\mathcal{M} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(\mathbb{Z}) \;\middle|\; a \geq 0,\; q(a,c) = kA \text{ and } q(b,d) = kC \right\}$$

by enumerating the representations of kA and kC by q. Given $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathcal{M}$,

$$q(M(x,y)) = kAx^2 + (2abA + (ad+bc)B + 2cdC)xy + kCy^2.$$

In particular, $q(M(x,y)) = kq(x,y)$ whenever $2abA + (ad+bc)B + 2cdC = kB$. By iterating over $\mathcal{M}$ and checking this condition, we verify that there exists some $M \in \mathcal{M}$ such that $q(M(x,y)) = kq(x,y)$. Fixing such an M, we further check whether for each $(x,y) \in \mathbb{Z}^2$ with $q(x,y) \equiv 0 \pmod{k}$ that also satisfies the congruence restrictions imposed by Lemma 4.12, the pair $(x_0, y_0) = M(x,y)$ satisfies $x_0 \equiv y_0 \equiv 0 \pmod{k}$. It suffices to check this condition modulo $k\Delta$ by an exhaustive search. In every case we've considered, this search successfully produces such an $M \in \mathcal{M}$. Once such an M has been found, we can set $x_0 = kw$ and $y_0 = kz$. Then $q(M(x,y)) = q(kw, kz) = k^2 p$, so $q(w,z) = p$. Therefore, we've shown that q represents p.

Example 4.13. *: Consider $q = \langle 2, 1, 7 \rangle$ with $\Delta = -55$. Let p be an odd prime not dividing Δ that satisfies conditions (i) - (iv) of Theorem 4.3.*

Step 1: From condition (i) of Theorem 4.3, $\left(\frac{\Delta}{p}\right) = 1$. Thus, applying Theorem 4.6 yields $x, y, k \in \mathbb{Z}$ with $q(x,y) = kp$ and $1 \leq k \leq \sqrt{\frac{55}{3}} = 4.28\ldots$.

Step 2 (Elimination): By Lemma 4.11(c), k is a square modulo 5. As $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$, $k \in \{1, 4\}$.

Step 3 (Reduction): Suppose $q(x,y) = 4p$. One might try to argue, as in Example 4.1, that both x and y are even. However, this need not be the case: e.g. q represents 7 and $q(3,1) = 4 \cdot 7$. Applying *the algorithm described above we obtain*

$$\mathcal{M} = \left\{ \begin{bmatrix} 1 & -3 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & -2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ -1 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ -1 & -2 \end{bmatrix}, \begin{bmatrix} 1 & 3 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} 2 & -3 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 2 & -1 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}, \begin{bmatrix} 2 & 1 \\ 0 & -2 \end{bmatrix}, \begin{bmatrix} 2 & 3 \\ 0 & 1 \end{bmatrix} \right\}.$$

Set $M = \begin{bmatrix} 1 & -3 \\ -1 & -1 \end{bmatrix}$. *Set* $(x_0, y_0) = M(x, y) = (x - 3y, -x - y)$ *and note* $q(x_0, y_0) = 4q(x, y) = 16p$. *If we knew* $x_0 \equiv y_0 \equiv 0 \pmod 4$*, then we could divide through by 4 to obtain an integer representation of* p*. Certainly we need only consider* $(x, y) \in \mathbb{Z}^2$ *with* $q(x, y) \equiv 0 \pmod 4$*. Further, since we're assuming* $\left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$ *and* $\left(\frac{p}{11}\right) = \left(\frac{2}{11}\right) = -1$*, condition (ii) of Theorem 4.3 implies we need only consider* $(x, y) \in \mathbb{Z}^2$ *with* $\left(\frac{q(x,y)}{5}\right) = \left(\frac{4p}{5}\right) = -1$ *and* $\left(\frac{q(x,y)}{11}\right) = \left(\frac{4p}{11}\right) = -1$*. By an exhaustive search modulo* 220*, we verify the only such* $(x, y) \in \mathbb{Z}^2$ *yield* $x_0 \equiv y_0 \equiv 0 \pmod 4$*. Setting* $x_0 = 4w$ *and* $y_0 = 4z$*, we have* $q(x_0, y_0) = 32w^2 + 16wz + 224z^2 = 16p$*. Dividing through by 16, we see* $q(w, z) = 2w^2 + wz + 7z^2 = p$*. Therefore, we've shown that* q *represents* p*.*

Chapter 5

Diagonal Quaternary Quadratic Forms

This work in this chapter was done in the context of a VIGRE Research Group at the University of Georgia throughout the 2011-2012 academic year. The results given below appear in [9]. Co-first authors were Pete Clark, Katherine Thompson, and Nathan Walters.

In [25], Hermite applied GoN methods to give a striking new proof that every positive integer is a sum of four squares (Lagrange's Theorem), many years before Minkowski's foundational work in GoN [36]. It is thus remarkable that a systematic study of the application of GoN methods to universality theorems for quadratic forms seems not to have been undertaken until [9]. The closest precedent in the literature is a late paper of L.J. Mordell [37]. Mordell proves in particular a *small multiple theorem* for certain diagonal quaternary forms of square discriminant. Especially, his results apply to the *multiplicative forms*

$$q_{a,b} = x^2 + ay^2 + bz^2 + abw^2$$

for $a, b \in \mathbb{Z}^+$. We generalize this to all forms of square discriminant (Theorem 5.6).

Although our methods apply to many nondiagonal forms of square discriminant [26] which will be discussed in the next chapter, in the remainder of this chapter we concentrate on the diagonal case. Work of Ramanujan [39] and Dickson [15] shows that there are precisely nine universal diagonal positive definite quaternary integral quadratic forms of square discriminant. Here we give GoN proofs of the universality of all nine of these forms.

Of these nine forms, seven are multiplicative,

$$q_{1,1},\ q_{1,2},\ q_{1,3},\ q_{2,2},\ q_{2,3},\ q_{2,4},\ q_{2,5},$$

and the universality of the two remaining forms can be rather easily deduced from these (Theorems 5.16 and 5.17). Mordell gives GoN proofs of the universality of $q_{1,1}$, $q_{1,2}$, $q_{1,3}$ and also alludes to Liouville's reduction of $q_{2,3}$ to $q_{1,1}$ (Theorem 5.14). Similar methods can be applied to show universality of the forms $q_{2,2}$ and $q_{2,4}$ (Theorems 5.13 and 5.15), as Mordell likely knew. Because of the work of the previous chapter we possess certain analogous results for representations of primes by binary quadratic forms, and we make use of them in the proofs (though in the next chapter we prove them without these). In [33], [34], Liouville states how to give elementary (non-GoN) proofs of the universality of these six multiplicative forms.

This leaves $q_{2,5}$. This form stymied Liouville, who says he can only prove that it represents all positive *even* integers [34]. The universality of $q_{2,5}$ was first proven by Ramanujan and Dickson, using (non-elementary) representation theorems for certain ternary subforms. Mordell does not mention that there are seven universal multiplicative forms, and the form $q_{2,5}$ does not appear in [37].

In [27], Hurwitz gave an elementary proof of Lagrange's Theorem using quaternion arithmetic. Recently Deutsch [13] gave Hurwitz-style universality proofs for eight of the nine diagonal universal forms of square discriminant, but not for $q_{2,5}$. This lack of success is somewhat puzzling because the relevant quaternion algebra $\left(\frac{-2,-5}{\mathbb{Q}}\right)$ still carries a Euclidean quaternion order, as was shown by Fitzgerald [17]. Using quaternionic methods Fitzgerald showed $q_{2,5}$ represents $16n$ for all $n \in \mathbb{Z}^+$.

Thus it seems that the literature contained no elementary proof of the universality of $q_{2,5}$. David B. Leep has found a different elementary proof of the universality of $q_{2,5}$. The main result of the present section, Theorem 5.18, gives an elementary – though computational – proof of the universality of $q_{2,5}$. Moreover, in a key step of the argument we show that if $q_{2,5}$ represents $2n$ then it also represents n. This step does not use GoN methods and thus could be used to complete the elementary universality proofs of Liouville and Fitzgerald.

Most of the universality proofs for the first eight forms make use of well-chosen linear changes of variable. This is one of the oldest tricks of the trade, going back at least to Euler [16, 141: July 26, 1749]. However, in the proofs of the first eight theorems (and in the classical literature) the relevant changes of variable are written down without any systematic justification. (In [37] Mordell exhibits relations between these changes of variable and the multiplicative structure of the forms $q_{a,b}$ via (5.1), but this is not a complete explanation.) In order to prove the universality of $q_{2,5}$, we needed to devise and implement an algorithm to search for these changes of variable, of which some thousands were required. Our algorithm can be used on the other eight forms as well, and it forms the basis of the universality proofs of the nondiagonal forms explored in the next section.

5.1 A multiplicative identity

Lemma 5.1. *(Lagrange [32]) Let R be a commutative ring, and let $a, b, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4$ be elements of R. Then:*

$$(x_1^2 + ax_2^2 + bx_3^2 + abx_4^2)(y_1^2 + ay_2^2 + by_3^2 + aby_4^2) = (x_1y_1 - ax_2y_2 - bx_3y_3 - abx_4y_4)^2$$

$$+a(x_1y_2 + x_2y_1 + bx_3y_4 - bx_4y_3)^2 + b(x_1y_3 - ax_2y_4 + x_3y_1 + ax_4y_2)^2$$

$$+ab(x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)^2.$$

Proof. The proof is a direct application of Littlewood's Principle: all purely algebraic identities are trivial to prove (though not necessarily trivial to discover). ∎

Corollary 5.2. *Let R be any commutative ring, let $a, b \in R$, and let $q_{a,b}$ be the diagonal quadratic form $(1, a, b, ab)$. Then the set of elements of R which are R-represented by $q_{a,b}$ is multiplicatively closed.*

In view of Corollary 5.2 we call a quadratic form $q_{a,b}$ *multiplicative*.

5.2 An application of geometry of numbers

Lemma 5.3. *Let p be an odd prime, and let $q(v)$ be an n-ary quadratic form over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. If $n \geq 3$, then q is isotropic.*

Proof. This is a special case of the Chevalley-Warning Theorem [29, Thm. 10.2.1]. For the convenience of the reader, we give a (yet) more elementary proof.

Step 1: We show that any nondegenerate binary quadratic form $q(x, y)$ over $\mathbb{F}_p$ is universal. By Fact 1 above, we may assume q is diagonal, say $q(x, y) = ax^2 + by^2$, with $ab \in \mathbb{F}_p^\times$. Let $d \in \mathbb{F}_p$. We may rewrite the equation $q(x, y) = d$ as

$$x^2 = \frac{d - by^2}{a}.$$

Then as x and y range over all elements of $\mathbb{Z}/p\mathbb{Z}$, both the left and right hand sides take on $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ distinct values. Since $p < \frac{p+1}{2} + \frac{p+1}{2}$, these values sets cannot be disjoint, which leads to a solution (x, y).

Step 2: It is enough to show every ternary form over $\mathbb{F}_p$ is isotropic; since degenerate forms are isotropic, we may assume $q(x, y, z) = ax^2 + by^2 + cz^2$ with $abc \in \mathbb{F}_p^\times$. By Step 1, there are $x_0, y_0 \in \mathbb{F}_p$ such that $q(x_0, y_0) = -c$, and then $q(x_0, y_0, 1) = 0$. ∎

Theorem 5.4. *Let $q(v)$ be a nondegenerate quaternary integral quadratic form of square discriminant. For each squarefree positive integer n prime to* $2 \operatorname{disc} q$*, there is an index n^2 subgroup $\Lambda_n \subset \mathbb{Z}^4$ such that for all $v \in \Lambda_n$, $q(v) \equiv 0 \pmod{n}$.*

Proof. Step 1: Let $n = p_1 \cdots p_r$, with $p_1, \ldots, p_r$ distinct odd primes. Suppose that for all $1 \leq i \leq r$ there exists a subgroup Λ_i of $\mathbb{Z}^4$ of index p_i^2 such that for all $v \in \Lambda_i$, $q(v) \equiv 0 \pmod{p_i}$. Then taking $\Lambda_n = \bigcap_{i=1}^r \Lambda_i$, an easy Chinese Remainder Theorem argument gives $[\mathbb{Z}^4 : \Lambda_n] = n^2$ and for all $v \in \Lambda_n$, $q(v) \equiv 0 \pmod{n}$.

Step 2: We are reduced to considering the case $n = p$ for $p \nmid 2\operatorname{disc}(q)$ and $a \in \mathbb{Z}^+$. Let $\overline{q}$ be the reduction of q modulo p. Since $p \nmid \operatorname{disc}(q)$, $\operatorname{disc} \overline{q} = 1 \pmod{(\mathbb{F}_p^\times)^2}$: in particular $\overline{q}$ is nondegenerate. By Proposition 1, $\overline{q}$ admits a 2-dimensional totally isotropic subspace $W \subset \mathbb{F}_p^4$. Now reduction modulo p induces an isomorphism of commutative groups $\mathbb{Z}^4/(p\mathbb{Z}^4) \xrightarrow{\sim} \mathbb{F}_p^4$. Taking $\Lambda_p = \varphi^{-1}(W)$ gives an index p^2 subgroup of $\mathbb{Z}^4$ such that for all $v \in \Lambda_p$, $q(v) \equiv 0 \pmod{p}$. □

Theorem 5.5. *(Korkine-Zolotarev) Let $q(v)$ be a positive definite real quaternary quadratic form, and let $\Lambda \subset \mathbb{Z}^4$ be a finite index subgroup. Then there exists $0 \neq v \in \Lambda$ such that*

$$q(v) \leq (4 \operatorname{disc} q)^{\frac{1}{4}} \sqrt{[\mathbb{Z}^4 : \Lambda]}.$$

Proof. In [4, § X.3.2] the result is stated with $\Lambda = \mathbb{Z}^4$. Our version follows: if $\Lambda = A\mathbb{Z}^4$, replace $q(v)$ with $q(Av)$, of discriminant $(\det A)^2 \operatorname{disc} q = [\mathbb{Z}^4 : \Lambda]^2 \operatorname{disc} q$. □

For a positive definite real quaternary quadratic form q, put

$$\mathrm{KZ}(q) = (4 \operatorname{disc} q)^{\frac{1}{4}},$$

$$M(q) = \left(\frac{4\sqrt{2}}{\pi}\right)(\operatorname{disc} q)^{\frac{1}{4}} = \left(\frac{4}{\pi}\right)\mathrm{KZ}(q).$$

Theorem 5.6. *Let $q(x, y, z, w)$ be a positive definite integral quadratic form of square discriminant. Let $n \in \mathbb{Z}^+$ be squarefree and prime to $2 \operatorname{disc} q$. Then there exist $x, y, z, w, k \in \mathbb{Z}$ such that*

$$q(x, y, z, w) = kn$$

and

$$1 \le k \le \lfloor (4 \operatorname{disc} q)^{\frac{1}{4}} \rfloor = \lfloor \mathrm{KZ}(q) \rfloor.$$

Proof. Applying Theorem 5.5 to Λ_n from Theorem 5.4, we get $v \in \mathbb{Z}^4$ such that

$$q(v) \equiv 0 \pmod{n}$$

and

$$0 < q(v) \le (4 \operatorname{disc} q)^{\frac{1}{4}} \sqrt{[\mathbb{Z}^4 : \Lambda]} = \mathrm{KZ}(q) \cdot n. \tag{5.1}$$

□

Theorem 5.5 is classical, but not so easy. One gets a version of Theorem 5.5 with a slightly worse constant more easily by applying Minkowski's Convex Body Theorem to the ellipsoids $\Omega_R = q(x, y, z, w) \le R^2$: there is a nonzero element $v \in \Lambda$ with

$$q(v) \le \frac{4\sqrt{2}}{\pi} (\operatorname{disc} q)^{\frac{1}{4}} \sqrt{[\mathbb{Z}^4 : \Lambda]}$$

and thus a version of Theorem 5.6 with (5.1) replaced by

$$1 \le k \le \left\lfloor \frac{4\sqrt{2}}{\pi} (\operatorname{disc} q)^{\frac{1}{4}} \right\rfloor = \lfloor M(q) \rfloor = \left\lfloor \frac{4}{\pi} \mathrm{KZ}(q) \right\rfloor. \tag{5.2}$$

In all the cases considered in this section we can make do with $M(q)$ instead of $\mathrm{KZ}(q)$.

5.3 Nine Universality Theorems

For the remainder of this section, all quadratic forms considered will be positive definite quadratic forms over $\mathbb{Z}$, so we make the convention that "form" means "positive definite quadratic form over $\mathbb{Z}$", a representation of n means a $\mathbb{Z}$-representation of the integer n, and "universal" means "positive universal", i.e., the form q integrally represents every positive integer.

5.4 Some history of universal forms

Recall the following theorem, a high water mark of classical number theory.

Theorem 5.7. *(Lagrange [32]) Every positive integer is the sum of four squares.*

Proof. Apply Corollary 5.2 with $a = b = 1$: we get the set of integers $\mathbb{Z}$-represented by $q = (1, 1, 1, 1)$ is multiplicatively closed. Since $1 = 1^2 + 0^2 + 0^2 + 0^2$ and $2 = 1^2 + 1^2 + 0^2 + 0^2$ are represented by q, it's enough to show q $\mathbb{Z}$-represents every odd prime p. Apply Theorem 5.6 with $n = p$: there are $x, y, z, w, k \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^2 + w^2 = kp,$$

with

$$1 \leq k \leq \lfloor (4 \operatorname{disc} q)^{\frac{1}{4}} \rfloor = \lfloor \sqrt{2} \rfloor = 1.$$

Thus $k = 1$ and every odd prime is a sum of four squares: done! □

Thus Lagrange's Theorem is the assertion that $(1, 1, 1, 1)$ is universal. Which other forms are universal? As we have already mentioned, Liouville proved several further universality theorems [33], [34]. The following result surveys more recent work. (When we enumerate forms, we really mean integral equivalence classes of forms.)

Theorem 5.8. *a) There is no universal form in fewer than four variables.*

b) For every $n \geq 5$, there are infinitely many universal forms.

c) (Ramanujan-Dickson) There are precisely 54 diagonal *universal quaternary forms.*

d) (Halmos) A diagonal quaternary form is universal iff it represents 1 *through* 15*.*

e) (Conway-Schneeberger, Bhargava) A classical form is universal iff it represents 1 *through* 15*. Moreover there are precisely* 204 *such forms.*

f) (Bhargava-Hanke) A form is universal iff it represents 1 *through* 290*. Moreover there are, up to equivalence, precisely* 6436 *such quaternary forms.*

Proof. a) See e.g. [10, p. 142]. b) Since $q_{1,1}$ is universal, for all $n \geq 4$ and all $d \in \mathbb{Z}^+$ so is $(1, \ldots, 1$ (n times$), d)$. This exhibits infinitely many pairwise nonisomorphic universal $(n+1)$-ary forms for all $n \geq 4$. c) See [39] and [15]. d) See [22]. This follows directly from the proof of part c), but P.R. Halmos seems to have been the first to have explicitly noticed this. e) See [11] and [1]. f) See [2]. □

Parts b) through f) of Theorem 5.8 rely heavily on the theory of *ternary forms* as well as the local theory over $\mathbb{Q}_p$ and $\mathbb{Z}_p$. Thus these proofs are not elementary in our sense, but we hope to apply GoN methods to ternary forms in the near future. Parts b) through e) are still relatively elementary in the sense of not requiring high technology: especially, Bhargava's proof of the "15 Theorem" is a triumph of insight over hard computations or deep theory. In contrast, the proof of the "290 Theorem" uses both lengthy computer calculations and sophisticated modular forms theory.

What about GoN methods? Our GoN proof Theorem 5.7 is far from the first. Rather Hermite was first [25]. Another GoN proof was given by J.H. Grace [18].

The results of §3 bring GoN methods to bear on all quaternary forms of square discriminant. The work of Bhargava-Hanke shows that there are 112 such universal forms – a sizable number –

so it makes sense to concentrate first on diagonal forms. Of the 54 universal diagonal forms, nine have square discriminant:

$$(1,1,1,1),\ (1,1,2,2),\ (1,1,3,3),\ (1,2,2,4),\ (1,2,3,6), (1,2,4,8),\ (1,2,5,10), \qquad (5.3)$$

$$(1,1,1,4),\ (1,1,2,8). \qquad (5.4)$$

Remark 4.1: It is an easy exercise to write down a list of 54 forms such that any universal quaternary form is integrally equivalent to *at most one* form in the list. In particular, it is elementary to see that there can be no diagonal universal forms of square discriminant other than the nine listed in (5.3) and (5.4).

The seven forms of (5.3) are multiplicative forms $q_{a,b} = (1, a, b, ab)$ – whereas the two forms of (5.4) are not, although $(1, 1, 1, 4)$ is closely related to $q_{1,1}$ and $(1, 1, 2, 8)$ is closely related to $q_{1,2}$.

We will show that all of these forms are universal. First observe:

Lemma 5.9. *A form representing all squarefree positive integers is universal.*

Proof. Every positive integer n may be written uniquely in the form A^2b with b squarefree. If $q(x_1, \ldots, x_n) = b$, then $q(Ax_1, \ldots, Ax_n) = A^2b = n$. □

5.5 Binary subforms

Theorem 5.10. *a) A prime $p > 2$ is represented by $x^2 + y^2$ iff $p \equiv 1 \pmod 4$.*
b) A prime $p > 2$ is represented by $x^2 + 2y^2$ iff $p \equiv 1, 3 \pmod 8$.
c) A prime $p > 3$ is represented by $x^2 + 3y^2$ iff $p \equiv 1 \pmod 3$.

d) A prime $p > 2$ *is represented by* $x^2 + 4y^2$ *iff* $p \equiv 1 \pmod 4$.

e) A prime $p > 5$ *is represented by* $x^2 + 5y^2$ *iff* $p \equiv 1, 9 \pmod{20}$.

f) A prime $p > 5$ *is represented by* $2x^2 + 5y^2$ *iff* $p \equiv 7, 13, 23, 27 \pmod{40}$.

Proof. See the previous chapter. □

5.6 Six multiplicative forms

Let $q = q_{a,b}$ be one of the forms of (5.3). One checks that q represents all primes $p \leq \operatorname{disc} q$. By Lemma 5.1, to establish universality it suffices to show q represents every $p > \operatorname{disc} q$. By Theorem 5.6, for any such p there are $x, y, z, w, k \in \mathbb{Z}$ such that

$$q(x, y, z, w) = kp,\ 1 \leq k \leq M(q) = \left\lfloor \frac{4\sqrt{2}}{\pi} (\operatorname{disc} q)^{\frac{1}{4}} \right\rfloor.$$

Theorem 5.11. *The form* $q_{1,2} = x^2 + y^2 + 2z^2 + 2w^2$ *is universal.*

Proof. By Theorem 5.10a), it suffices to show that $q_{1,2}$ represents every prime $p \equiv 3 \pmod 4$; fix such a p. We have $M(q_{1,2}) = 2$, so there are $k, x, y, z, w \in \mathbb{Z}$ with

$$x^2 + y^2 + 2z^2 + 2w^2 = kp,\ k \in \{1, 2\}.$$

If $k = 1$, we're done, so suppose $x^2 + y^2 + 2z^2 + 2w^2 = 2p$. Then $x \equiv y \pmod 2$.
Case 1: x and y are both even. So we may take $x = 2X$, $y = 2Y$ to get

$$2X^2 + 2Y^2 + z^2 + w^2 = p.$$

Case 2: x and y are both odd. Then

$$p = \frac{1}{2}(x^2 + y^2) + z^2 + w^2 = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + z^2 + w^2 = X^2 + Y^2 + z^2 + w^2.$$

Since $p \equiv 3 \pmod 4$, exactly 3 of X, Y, z, w are odd: without loss of generality suppose z and w are odd. Then

$$p = X^2 + Y^2 + 2\left(\frac{z+w}{2}\right)^2 + 2\left(\frac{z-w}{2}\right)^2 = X^2 + Y^2 + 2Z^2 + 2W^2.$$

□

Theorem 5.12. *The form $q_{1,3} = x^2 + y^2 + 3z^2 + 3w^2$ is universal.*

Proof. Here $M(q_{1,3}) = 3$, so for all $p > 3$, there are $k, x, y, z, w \in \mathbb{Z}$ with

$$x^2 + y^2 + 3z^2 + 3w^2 = kp, \ k \in \{1, 2, 3\}.$$

Case 1: Suppose $k = 2$. Then $x + y$ and $z + w$ have the same parity.

Case 1a): Suppose $x + y$, $z + w$ are both even. Then $\frac{x \pm y}{2}, \frac{z \pm w}{2} \in \mathbb{Z}$, so

$$\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + 3\left(\frac{z+w}{2}\right)^2 + 3\left(\frac{z-w}{2}\right)^2 = \frac{2p}{2} = p.$$

Case 1b): $x + y$ and $z + w$ are both odd. Without loss of generality x and z are odd and y and w are even, so

$$2p \equiv x^2 + y^2 + 3z^2 + 3w^2 \equiv 1 + 3 \equiv 0 \pmod 4,$$

so p is even, contradiction.

Case 2: Suppose $k = 3$, i.e., $x^2 + y^2 + 3z^2 + 3w^2 = 3p$. Then $3 \mid x^2 + y^2$, so x and y are both divisible by 3. Substituting $x = 3X$, $y = 3Y$ and simplifying gives

$$z^2 + w^2 + 3X^2 + 3Y^2 = p.$$

□

Theorem 5.13. *The form* $q_{2,2} = x^2 + 2y^2 + 2z^2 + 4w^2$ *is universal.*

Proof. It suffices to show that $q_{2,2}$ represents every prime $p > 2$. Taking $z = w = 0$ and applying Theorem 5.10b), we see q represents all $p \equiv 1, 3 \pmod 8$; taking $y = z = 0$ and applying Theorem 5.10d), we see $q_{2,2}$ represents all $p \equiv 1 \pmod 4$, so we may assume $p \equiv 7 \pmod 8$. By Theorem 5.7, there are $x, y, z, w \in \mathbb{Z}$ such that

$$x^2 + y^2 + z^2 + w^2 = p. \tag{5.5}$$

Up to order, the only way to write 7 as a sum of three squares in $\mathbb{Z}/8\mathbb{Z}$ is $7 = 1 + 1 + 1 + 4$, so we may assume that in (5.5) we have y, z odd and w even, and thus

$$x^2 + y^2 + z^2 + w^2 = x^2 + 2\left(\frac{y-z}{2}\right)^2 + 2\left(\frac{y+z}{2}\right)^2 + 4\left(\frac{w}{2}\right)^2 = p.$$

□

Theorem 5.14. *The form* $q_{2,3} = x^2 + 2y^2 + 3z^2 + 6w^2$ *is universal.*

Proof. (Liouville [33]) Let $n \in \mathbb{Z}^+$. By Theorem 5.7, there are $x, y, z, w \in \mathbb{Z}$ with $n = x^2+y^2+z^2+w^2$. After replacing some of x, y, z, w by their negatives and reordering, we may assume $3 \mid y + z + w$; further, two of y, z, w must have the same parity, so after reordering them we may assume $y \equiv z \pmod 2$. Then $Z = \frac{y+z+w}{3}$, $W = \frac{y+z-2w}{2}$, $Y = \frac{y-z}{2}$ are all integers, and, as one readily checks,

$$n = x^2 + y^2 + z^2 + w^2 = x^2 + 2Y^2 + 3Z^2 + 6W^2.$$

□

Theorem 5.15. *The form* $q_{2,4} = x^2 + 2y^2 + 4z^2 + 8w^2$ *is universal.*

Proof. It suffices to show that q represents each $p > 2$. By Theorem 5.10d), every $p \equiv 1 \pmod 4$ is represented by x^2+4z^2, so we may assume $p \equiv 3 \pmod 4$. By Theorem 5.13 there are $x, y, z, w \in \mathbb{Z}$

such that

$$p = x^2 + 2y^2 + 2z^2 + 4w^2. \tag{5.6}$$

If y is even, put $y = 2Y$ to get $p = x^2 + 2z^2 + 4w^2 + 8Y^2$; and similarly if z is even. So suppose y and z are both odd. Also x is odd, so reducing (5.6) modulo 4 gives

$$p \equiv x^2 + 2y^2 + 2z^2 + 4w^2 \equiv 1 + 2 + 2 \equiv 1 \pmod 4.$$

□

5.7 Two non-multiplicative forms

Theorem 5.16. *The form $q = x^2 + y^2 + z^2 + 4w^2$ is universal.*

Proof. Let $n \in \mathbb{Z}^+$ be squarefree, so in particular $4 \nmid n$. By Theorem 5.7 there are $x, y, z, w \in \mathbb{Z}$ such that $n = x^2 + y^2 + z^2 + w^2$. Since $4 \nmid n$, x, y, z, w cannot all be odd. Without loss of generality, $w = 2W$ for $W \in \mathbb{Z}$ and thus

$$n = x^2 + y^2 + z^2 + (2W)^2 = x^2 + y^2 + z^2 + 4W^2.$$

□

Theorem 5.17. *The form $q = x^2 + y^2 + 2z^2 + 8w^2$ is universal.*

Proof. Step 1: We claim q represents every $n \equiv 3 \pmod 4$. By Theorem 5.11 there are $x, y, z, w \in \mathbb{Z}$ such that

$$n = x^2 + y^2 + 2z^2 + 2w^2. \tag{5.7}$$

If w is even, we may substitute $w = 2W$ to get

$$n = x^2 + y^2 + 2z^2 + 8W^2,$$

and similarly if z is even. Thus we may assume z, w are both odd. Reducing (5.7) modulo 4 gives $n \equiv x^2 + y^2 \pmod 4$, so $n \not\equiv 3 \pmod 4$.

Step 2: Suppose n_1 and n_2 are odd positive integers both represented by q. We claim that $n_1 n_2$ is also represented by q. If

$$n_1 = x_1^2 + x_2^2 + 2x_3^2 + 2(2x_4)^2,\ n_2 = y_1^2 + y_2^2 + 2y_3^2 + 2(2y_4)^2,$$

then by Lemma 5.1 we have

$$n_1 n_2 = z_1^2 + z_2^2 + 2z_3^2 + 2(2x_1y_4 + x_2y_3 - x_3y_2 + 2x_4y_1)^2. \tag{5.8}$$

with $z_1, z_2, z_3 \in \mathbb{Z}$. Equation (5.8) exhibits n_1n_2 in the form $q(v)$ iff $x_2y_3 - x_3y_2$ is even. Since n_1 is odd, then $x_1^2 + x_2^2$ is odd and thus exactly one of x_1, x_2 is even. By interchanging x_1 and x_2 if necessary, we may assume that x_2 is even. In exactly the same way we may assume that y_2 is even and thus that $x_2y_3 - x_3y_2$ is even.

Step 3: Every odd $n \in \mathbb{Z}^+$ is represented by q. By Step 2 it is enough to show that every odd prime number p is represented by q. If $p \equiv 1 \pmod 4$, then by Theorem 5.10a) $p = x_1^2 + x_2^2$, whereas if $p \equiv 3 \pmod 4$ then q represents p by Step 1.

Step 4: Suppose $n = 2n' \equiv 2 \pmod 4$. Since n' is odd, by Step 3, there are integers y_1, y_2, y_3, y_4, with $y_2 = 2Y_2$, such that $n' = y_1^2 + y_2^2 + 2y_3^2 + 2(2y_4)^2$. Then

$$n = 2 \cdot n' = (0^2 + 0^2 + 2 \cdot 1^2 + 2(2 \cdot 0)^2)(y_1^2 + y_2^2 + 2y_3^2 + 2(2y_4)^2)$$

$$= z_1^2 + z_2^2 + z_3^2 + 2(-y_2)^2 = z_1^2 + z_2^2 + z_3^2 + 8Y_2^2.$$

□

5.8 The form $q_{2,5} = (1, 2, 5, 10)$

Theorem 5.18. *The form $q_{2,5} = x^2 + 2y^2 + 5z^2 + 10w^2$ is universal.*

To prove Theorem 5.18 we need to clarify and systematize the rather *ad hoc* methods used for the other universality proofs, so we begin by laying out a general strategy.

Let $q(v)$ be an n-ary integral quadratic form, and let $d \in \mathbb{Z}$. We wish to show that q represents d, and say we know that it integrally represents kd for some "small" positive integer k, i.e., there exists $x \in \mathbb{Z}^n$ such that $q(x) = kd$.

Suppose first that we can find $A \in M_n(\mathbb{Z})$ such that we have an identity of quadratic forms $q(Av) = kq(v)$. Then $q(Ax) = kq(x) = k^2 d$, and thus

$$q(A\left(\frac{x}{k}\right)) = d.$$

This gives an integral representation of d by q *provided* $Ax \in (k\mathbb{Z})^n$, a condition which depends only the classes of $x_1, \ldots, x_n \pmod{k}$. Since $q(x) = kd$, we need only consider admissible n-tuples, i.e., $(x_1, \ldots, x_n) \in (\mathbb{Z}/k\mathbb{Z})^n$ such that $q(x_1, \ldots, x_n) \equiv 0 \pmod{k}$. And we do not need the same matrix A to work for each admissible n-tuple: we only need that for each admissible n-tuple $x \in (\mathbb{Z}/k\mathbb{Z})^n$ there is *some* $A_x \in M_n(\mathbb{Z})$ such that $q(Av) = kq(v)$ and $A_x x \equiv 0 \pmod{k}$.

However, in most cases this is asking too much.

Lemma 5.19. *For all $k \in \mathbb{Z}^+$, $\{A \in M_n(\mathbb{Z}) \mid q(Av) = kq(v)\}$ is finite.*

Proof. $M_n(\mathbb{R})$ is an n^2-dimensional Euclidean space in which $M_n(\mathbb{Z})$ sits as a discrete subgroup. Since q is positive definite, the set of $A \in M_n(\mathbb{R})$ with $q(Av) = kq(v)$ for all $v \in \mathbb{R}^n$ is bounded, so its intersection with $M_n(\mathbb{Z})$ is finite.

However, for our applications we want an algorithmic enumeration of $O_q(k)$. This can be achieved by revisiting the above argument more quantitatively.

Step 1: Suppose $q = q_0 = x_1^2 + \ldots + x_n^2$, so

$$O_q(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid q(Av) = q(v)\}$$

is the standard real orthogonal group $O_n(\mathbb{R})$. $M_n(\mathbb{R})$ endowed with the *Frobenius norm* $A = (a_{ij}) \mapsto |A| = \sqrt{\sum_{1 \le i,j \le n} a_{ij}^2}$ is a Banach algebra: for all $A, B \in M_n(\mathbb{R})$, $|AB| \le |A||B|$ (this amounts to the Cauchy-Schwarz inequality). Let $q_0 = x_1^2 + \ldots + x_n^2$. Then $O_{q_0}(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid q_0(Av) = q(v)\}$ is the standard orthogonal group $O_n(\mathbb{R})$, and thus for all $A \in O_{q_0}(\mathbb{R})$, $|A| = \sqrt{n}$. All positive definite n-ary forms are $\mathbb{R}$-equivalent, so choose $P \in \mathrm{GL}_n(\mathbb{R})$ such that $q(v) = q_0(Pv)$. Then $O_q(\mathbb{R}) = P^{-1}O_{q_0}(\mathbb{R})P$: if $A \in O_{q_0}(\mathbb{R})$, then $q(P^{-1}APv) = q_0(APv) = q_0(Pv) = q(v)$, and conversely. So for $A \in O_q(\mathbb{R})$,

$$|A| = |P^{-1}PAP^{-1}P| \le |P^{-1}||PAP^{-1}||P| \le \sqrt{n}|P||P^{-1}|.$$

Step 2: For $A \in M_n(\mathbb{R})$, $k \in \mathbb{R}^{>0}$, $q(Av) = kq(v)$ iff $q(\frac{A}{\sqrt{k}}v) = q(v) \iff \frac{A}{\sqrt{k}} \in O_q(\mathbb{R})$. Thus if $A \in M_n(\mathbb{R})$ and $q(Av) = kq(v)$,

$$|A| \le \sqrt{kn}|P||P^{-1}|.$$

So we may compute $O_q(k)$ by running through $\{A \in M_n(\mathbb{Z}) \mid |A| \le \sqrt{kn}|P||P^{-1}|\}$ and testing to see whether $q(Av) = kq(v)$ holds. □

Remark 4.2: The algorithm given above was chosen because it is (we hope) easily understood by a wide audience. We do not claim any particular efficiency.

However, we may also consider matrices with denominators. For $k, r \in \mathbb{Z}^+$, put

$$O_q(k, r) = \{A \in M_n(\mathbb{Z}) \mid q\left(\frac{A}{r}v\right) = kq(v)\} = \{A \in M_n(\mathbb{Z}) \mid q(Av) = kr^2q(v)\}.$$

By Lemma 5.19, $O_q(k, r)$, is finite *for each fixed k and r*, but for fixed k the sets $O_q(k, r)$ tend to grow in size with r.This improves our chances of success: we say a tuple $x \in (\mathbb{Z}/kr\mathbb{Z})^n$ is *admissible* if $q(x) \equiv 0 \pmod{k}$. Let $A_q(k,r)$ denote the set of all admissible tuples. We say that $O_q(k,r)$ *covers* $A_q(k,r)$ if for each $x \in A_q(k,r)$, there exists $A_x \in O_q(k,r)$ such that $A_x x \equiv 0 \pmod{kr}$. If for some $r \in \mathbb{Z}^+$ we have that $O_q(k,r)$ covers $A_q(k,r)$, then for all $d \in \mathbb{Z}^+$, if there exists $x \in \mathbb{Z}^n$ such that $q(x) = kd$, then $A_x\left(\frac{x}{kr}\right) \in \mathbb{Z}^n$ and $q(A_x\left(\frac{x}{kr}\right)) = d$.

We now turn to the proof of Theorem 5.18. As usual, we apply Theorem 5.6: since $\lfloor M(q) \rfloor = 5$, for any prime $p > 5$ there exists $(x,y,z,w) \in \mathbb{Z}^4$ with $x^2 + 2y^2 + 5z^2 + 10w^2 = kp$ with $k \in \{1,2,3,4,5\}$. So to complete the proof, it suffices to find, for each $k \in \{2,3,4,5\}$, a positive integer r such that $O_q(k,r)$ covers $A_q(k,r)$.

Theorem 5.20. *Let $q = q_{2,5} = x^2 + 2y^2 + 5z^2 + 10w^2$. Then:*
a) The 26768 elements of $O_q(2,8)$ cover all $\#A_q(2,8) = 32768$ admissible tuples, and thus for all $d \in \mathbb{Z}^+$, if q represents $2d$ then it also represents d.
b) For no $r < 8$ does $O_q(2,r)$ cover $A_q(2,r)$.
c) The 83072 elements of $O_q(3,8)$ cover all $\#A_q(3,8) = 135168$ admissible tuples, and thus for all $d \in \mathbb{Z}^+$, if q represents $3d$ then it also represents d.
d) For no $r < 8$ does $O_q(3,r)$ cover $A_q(3,r)$.
e) The 10384 elements of $O_q(4,4)$ cover all $\#A_q(4,4) = 16384$ admissible tuples.
f) For no $r < 4$ does $O_q(4,r)$ cover $A_q(4,r)$.
g) The 16 elements of $O_q(5,1)$ cover all $\#A_q(5,1) = 25$ admissible tuples, and thus for all $d \in \mathbb{Z}^+$, if q represents $5d$ then it also represents d.

Proof. A computer calculation. The C++ code used for this may be found at
`http://www.math.uga.edu/~pete/MinimalCode.cpp.` □

This completes the proof of Theorem 5.18.

Remark 4.3: Notice that – without any GoN input – Theorem 5.20a) yields:

Theorem 5.21. *For all* $d \in \mathbb{Z}^+$*, if* $q_{2,5}$ *represents* $2d$*, then it also represents* d*.*

As described in the introduction, Theorem 5.21 completes a quaternionic proof of the universality of $(1, 2, 5, 10)$ initiated by Deutsch and continued by Fitzgerald.

Remark 4.4: The case $k = 5$ is easy enough to be treated by hand. If $x^2 + 2y^2 + 5z^2 + 10w^2 = 5p$, then $5 \mid x^2 + 2y^2$, so x and y are both divisible by 5. Putting $x = 5X$, $y = 5Y$ and simplifying gives $z^2 + 2w^2 + 5X^2 + 10Y^2 = p$.

Chapter 6

Nondiagonal Quaternary Quadratic Forms

This work in this chapter was done in the context of a VIGRE Research Group at the University of Georgia throughout the 2011-2012 academic year. The results given below appear in [8]. Co-first authors on this paper was Katherine Thompson.

In this chapter, we again use GoN methods to provide proofs of universality of positive definite quaternary integral quadratic forms. Now, however, we only require that the forms have square discriminant. The work of Conway [10] and Bhargava-Hanke [2] shows there are 112 such forms (a list of all 6436 universal quaternary integral quadratic forms is available at [35]). Of the 112 candidates, 105 have lent themselves to our methods and GoN universality proofs can be given. In light of the nine forms discussed in [9], this paper adds 96 universality statements and proves the universality of the previous forms without using binary subforms. Of these 96 forms only 11 are classically integral.

We wish to emphasize that the primary of interest of this work is not the universality theorems themselves but the way in which they are proved. To prove the 290 Theorem, Bhargava-Hanke must analyze the universality of more than 6000 individual forms, and they do so by considering the associated theta series and applying deep and sophisticated techniques from the theory of modular forms. To analyze the Fourier coefficients of the theta-series, Siegel's work on local densities is used to bound the Eisenstein coefficients, and the theory of newforms and Deligne's bounds on Hecke eigenvalues (i.e., the Ramanujan-Petersson Conjecture) are used to bound the cusp coefficients. In constrast, the present method is almost entirely self-contained. The only GoN result which does not receive a full proof here or in [9] is Korkine-Zolotarev's computation of the 4-dimensional Hermite constant γ_4 [30]. In fact, for all 105 forms treated here, the upper bound on γ_4 coming from Minkowski's Convex Body Theorem is sufficient. That state-of-the-art universality theorems can be proved by such elementary methods seems truly remarkable...and also somewhat mysterious.

Our techniques prove universality of 78 forms of class number greater than one. To the best of our knowledge all previous applications of GoN methods to representation theorems for integral quadratic forms (including [8] and [9]) treat only class number one forms. One might have guessed that such elementary methods were inherently limited to the class number one case. The present paper shows that the range of applicability of GoN methods is considerably larger. It would be interesting to probe this range more thoroughly, and we hope to do so in the future.

6.1 Proving Universality

Theorem 6.1. *The 105 integral, positive definite, quaternary quadratic forms appearing in Tables A.2 and A.3 of the Appendix are universal.*

Proof. Let $q = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j = x^t A_q x$ be a form in Table A.2 and A.3. Suppose we can show:

(a) For all squarefree $n \in \mathbb{Z}^+$ with $\gcd(n, 2\Delta_q) = 1$, q represents n.

(b) If q represents $n \in \mathbb{Z}^+$ and $p \mid 2\Delta_q$, then q represents pn.

Then q represents every squarefree positive integer and is thus universal: write $n \in \mathbb{Z}^+$ as ts^2 with t squarefree. There is $\vec{v} \in \mathbb{Z}^4$ with $q(\vec{v}) = t$, so $q(s\vec{v}) = ts^2 = n$.

We now explain how to establish (a) and (b) for q: the method includes computer computation, and an example is provided in the following section.

Establishing (a): By the Small Multiple Theorem (Theorem 4.6), for all $n \in \mathbb{Z}^+$ there is $\vec{v} \in \mathbb{Z}^4$ such that $q(\vec{v}) = kn$ for some $k \in \{1, 2, ..., \lfloor (4\Delta_q)^{1/4} \rfloor\}$.

If $q(\vec{v}) = kn$, suppose we can find a matrix $A \in M_4(\mathbb{Z})$ such that $q(Ax) = kq(x)$: an identity of quadratic forms. Then $q(A\vec{v}) = kq(\vec{v}) = k^2 n$. If, however, we could show $A\vec{v} \in (k\mathbb{Z})^4$, allowing $\vec{w} = (A\vec{v})/k \in \mathbb{Z}^4$, we would have $q(\vec{w}) = \frac{1}{k^2} q(A\vec{v}) = n$.

The strategy is to use a computer to create a set of such matrices. Since the $A\vec{v} \in (k\mathbb{Z})^4$ condition can be checked modulo k, we have a finite set of vectors to consider. If for each vector we can find a matrix, we will have shown (a). Consider the set of such matrices:

$$O_q(k) = \{A \in M_4(\mathbb{Z}) : q(A\vec{v}) = kq(\vec{v})\}.$$

By the previous chapter, $O_q(k)$ is finite. Here is another algorithm to compute $O_q(k)$:

We create the set of vectors $V_i = \{\vec{v} \in \mathbb{Z}^4 : q(\vec{v}) = ka_{ii}\}$ for $i \in \{1, 2, 3, 4\}$. By positivity of q, the finite set V_i can be enumerated by evaluating $q(\vec{v})$ at all vectors inside a bounded ellipsoid. Let $M = [v_1|v_2|v_3|v_4] \in M_4(\mathbb{Q})$. Then $M \in O_q(k)$ if and only if:

- For all $1 \leq i \leq 4$, $v_i \in V_i$, and
- For all $1 \leq i < j \leq 4$, $v_i^t A_q v_j = ka_{ij}$.

The problem has been reduced to a computer search to find a d such that $O_q(k,d)$ covers $A_q(k,d)$. For all the forms in Tables I and II, the computer search was successful.

Establishing (b): fix a prime p such that $p \mid 2\Delta_q$ and a vector $\vec{v} \in \mathbb{Z}^4$. This time we wish to find a matrix $A \in M_4(\mathbb{Z})$ such that $q(A\vec{v}) = pq(\vec{v})$. We again consider matrices in $O_q(p,d)$. Now all vectors in $(\mathbb{Z}/pd\mathbb{Z})^4$ are admissible. We say a matrix $A \in O_q(p,d)$ *multiplies* a vector $\vec{v} \in (\mathbb{Z}/pd\mathbb{Z})^4$ if $A\vec{v} \in (d\mathbb{Z})^4$, which then gives $\vec{x} = A\frac{\vec{v}}{d} \in \mathbb{Z}^4$ and $q(\vec{x}) = q\left(A\frac{\vec{v}}{d}\right) = \frac{1}{d^2}q(A\vec{v}) = pq(\vec{v})$.

We are again reduced to a computer search, and upon finding a d for all (q,p) pairs required, we have shown that if q represents n then q represents pn. This search was successful for all the forms in Tables I and II.

This completes the proof. □

Remark 6.2. *For* 104 *of the* 105 *forms of Theorem 6.1, using the first assertion of the Small Multiple Theorem – coming from the Minkowski bound – either does not change the computations at all or does not significantly lengthen them. However for*

$$q = x_1^2 + 2x_2^2 + x_2x_3 + 4x_3^2 + 31x_4^2,$$

the last form in Table II, using the first assertion of the Small Multiple Theorem requires consideration of $k = 7$, and our computation has not terminated for this value. If we use the second assertion of the Small Multiple Theorem – coming from the Korkine-Zolotarev bound – then $k = 7$ does not need to be considered.

6.2 An Example

We will now illustrate all steps of the algorithm with a particular form:

$$q(x) = x_1^2 + x_1x_2 + 2x_2^2 + 3x_3^2 + 3x_3x_4 + 6x_4^2.$$

This form is not classically integral, has class number 3 and discriminant $\frac{441}{16}$. Applying the Small Multiple Theorem for n satisfying $(n, 42) = 1$, we obtain $k \leq 3$. For the cases $q(\vec{v}) = 3n$ or $q(\vec{v}) = 2n$, we must prove the existence of a reduction to a representation of n by q.

For $k = 3$ (i.e., assuming $q(\vec{v}) = 3n$), using a computer search we find that a denominator of 1 that all that is required. That is, we only need to consider vectors $\vec{v} \in (\mathbb{Z}/3\mathbb{Z})^4$. Moreover, setting

$$M = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

one quickly observes that $qM(x) = 3q(x)$. Noting that M reduces all admissible vectors $v \in$

$A_q(1,3)$:

$$M\,(0,\ 0,\ 0,\ 0)^t = (0,\ 0,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 0,\ 1)^t = (0,\ 3,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 0,\ 2)^t = (0,\ 6,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 1,\ 0)^t = (3,\ 0,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 1,\ 1)^t = (3,\ 3,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 1,\ 2)^t = (3,\ 6,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 2,\ 0)^t = (6,\ 0,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 2,\ 1)^t = (6,\ 3,\ 0,\ 0)^t$$

$$M\,(0,\ 0,\ 2,\ 2)^t = (6,\ 6,\ 0,\ 0)^t$$

we see that a representation of $3n$ by q can be reduced.

Next we address the case where $q(\vec{x}) = 2n$. This time a denominator of 2 suffices. There are 160 admissible vectors and we need to consider vectors in $(\mathbb{Z}/4\mathbb{Z})^4$.

$$O_q(2,2) = \left\{ M_1 = \begin{pmatrix} 0 & -2 & 0 & -6 \\ 1 & 1 & -3 & 0 \\ 0 & -2 & 0 & 2 \\ 1 & 1 & 1 & 0 \end{pmatrix}, M_2 = \begin{pmatrix} 0 & -4 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 2 & 0 \end{pmatrix}, M_3 = \begin{pmatrix} 0 & -4 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 0 & 0 & -1 & -3 \end{pmatrix}, \right.$$

$$\left. M_4 = \begin{pmatrix} 0 & -4 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 0 & 2 & -2 \\ 0 & 0 & -2 & -2 \end{pmatrix}, M_5 = \begin{pmatrix} 0 & 4 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 2 & 0 \end{pmatrix}, M_6 = \begin{pmatrix} 0 & -2 & 0 & 6 \\ 1 & 1 & 3 & 0 \\ 0 & -2 & 0 & -2 \\ 1 & 1 & -1 & 0 \end{pmatrix} \right\}.$$

For all $M_i \in O_q(2,2)$, we have $q(M_i x) = 8q(x)$. For each of the six matrices we provide an example of an admissible vector that it covers:

$$M_0(0,0,0,2)^t = (-12,0,4,0)^t$$
$$M_1(0,0,0,1)^t = (0,0,4,0)^t$$
$$M_2(0,0,1,1)^t = (0,0,4,-4)^t$$
$$M_3(0,0,1,3)^t = (0,0,-4,-8)^t$$
$$M_4(0,1,0,0)^t = (4,0,0,0)^t$$
$$M_5(0,1,1,1)^t = (4,4,-4,0)^t.$$

Similarly all other 154 admissible tuples are covered by one of the six matrices above.

Now it remains to show that if q represents a positive integer n then it represents $2n$, $3n$, and $7n$. In each case there is an integer matrix that allows multiplication. Specifically:

$$P_2 = \begin{pmatrix} 0 & 2 & 0 & 0 \\ -1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & -1 & -1 \end{pmatrix}, P_3 = \begin{pmatrix} 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, P_7 = \begin{pmatrix} 1 & -2 & -3 & -3 \\ 0 & 2 & 0 & -3 \\ 0 & -1 & 2 & -1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Note that for each i, $P_i \in M_4(\mathbb{Z})$, and hence for all $\vec{v} \in \mathbb{Z}^4$, $P_i\vec{v} \in \mathbb{Z}^4$. Moreover, for each i, $q(P_i x) = i \cdot q(x)$. This completes the proof of the universality of q.

6.3 Local Success of the Method

In this section we will discuss the success of the method. At every level $d \in \mathbb{Z}^+$, we say that the method succeeds if the finite set $A_q(k, d)$ of admissible vectors is covered by the finite set $O_q(k, d)$ of matrices: i.e., if every $\vec{v} \in A_q(k, d)$ is reduced by at least one $A \in O_q(k, d)$. If not, then we move on to $A_q(k, d')$ for a larger value of d' (up to the limits of our computational power). We show here that the method necessarily *succeeds locally* in the following sense: given any $\vec{v} \in A_q(k, d')$, there is a lift $\tilde{\vec{v}}$ of $\vec{v}$ to $A_q(k, dd')$ such that $\tilde{\vec{v}}$ is reduced by some $\tilde{A} \in A_q(k, dd')$.

Although the above statement in terms of congruence classes is a natural one when analyzing the method of proof of Theorem 6.1, we will actually prove a stronger result concerning integer vectors. In turn, by clearing denominators, this integral result follows quickly from a result about rational quadratic forms. The result for rational forms uses one of the key facts in the basic theory of algebraic quadratic forms: the isometry group of a nondegenerate quadratic form acts transitively on the set of vectors on which the quadratic form takes any fixed nonzero value. To make a short, clean proof of a slightly more general result, we have decided to make use of a basic property of Pfister forms (see [31] for details).

Theorem 6.3. *Let K be a field of characteristic different from 2, and let $q_{/K}$ be a nondegenerate n-ary Pfister form of square discriminant. For $k, p \in K^\times$, suppose q represents p and kp. Then for* *all* $\vec{v}, \vec{w} \in K^n$ *with* $q(\vec{v}) = p$ *and* $q(\vec{w}) = kp$*, there is* $M \in \mathrm{GL}_n(K)$ *with* $M\vec{w} = k\vec{v}$ *and* $q(Mx) = kq(x)$*.*

Proof. Putting

$$O_q(k) = \{M \in GL_n(K) \mid q(Mx) = kq(x)\},$$

we must show that there is $M \in O_q(k)$ such that $M\vec{w} = k\vec{v}$. Since q is a Pfister form, by [31, Thm. X.1.8] q is a *round form*: if we define

$$D(q)^\bullet := \{q(x) \mid x \in K^n\} \setminus \{0\}$$

and

$$G(q) := \{c \in K^\times \mid cq \cong q\},$$

then $D(q)^\bullet = G(q)$. Thus $D(q)^\bullet$ is a subgroup of $K^\times$, so $p, kp \in D(q)^\bullet \implies k \in D(q)^\bullet = G(q)$: there is $M_1 \in GL_n(K)$ such that $q(M_1 x) = kq(x)$ for all x. Taking $x = \vec{v}$, we get

$$q(M_1\vec{v}) = kq(\vec{v}) = kp = q(\vec{w}).$$

By [31, Prop. I.4.7], there is $M_2 \in O(q) = O_q(1)$ with $M_2 M_1 \vec{v} = \vec{w}$. Put $M = M_2 M_1$. Then

$$M\vec{v} = \vec{w}$$

and

$$q(Mx) = q(M_2 M_1 x) = q(M_1 x) = kq(x),$$

so $M \in O_k(q)$. □

Corollary 6.4. *Let* q_Z *be a positive quaternary quadratic form with square discriminant.*

a) For $k, p \in \mathbb{Z} \setminus \{0\}$*, suppose* q *integrally represents* $1, p, kp$*. Then for all* $\vec{v}, \vec{w} \in \mathbb{Z}^4$ *with* $q(\vec{v}) = p$ *and* $q(\vec{w}) = kp$*, there is* $M \in M_4(\mathbb{Q})$ *such that* $M\vec{w} = k\vec{v}$ *and* $q(M\vec{x}) = kq(\vec{x})$*.*

b) If q is positive universal, reduction always succeeds locally: for all $k, p \in \mathbb{Z} \setminus \{0\}$ and $\vec{w} \in \mathbb{Z}^4$ with $q(\vec{w}) = kp$, there is $d \in \mathbb{Z}^+$ and $A \in O_q(k, d)$ with $A\vec{w} \in (kd\mathbb{Z})^4$.
(Thus if $\vec{v} = \frac{\vec{w}}{kd}$, then $\vec{v} \in \mathbb{Z}^4$ and $q(\vec{v}) = p$.)

Proof. a) A nondegenerate quaternary quadratic form over a field of characteristic different from 2 is a Pfister form if and only if it has a diagonal representation $\langle 1, a, b, ab\rangle$ if and only if it represents 1 and has square discriminant. Thus Theorem 6.3 applies to $q_{/\mathbb{Q}}$: there is $M \in M_4(\mathbb{Q})$ such that $M\vec{w} = k\vec{v}$.

b) Since q is positive universal, there is $\vec{v} \in \mathbb{Z}^4$ with $q(\vec{v}) = p$. Applying part a), we get $M \in M_4(\mathbb{Q})$ with $q(Mx) = kq(x)$ and $M\vec{w} = k\vec{v}$. Let d be the greatest common denominator of the entries of M, and put

$$A = dM,\ \vec{u} = \frac{A\vec{w}}{kd}.$$

Then $A \in M_4(\mathbb{Z})$ and

$$q(Ax) = q(dMx) = d^2 q(Mx) = kd^2 q(x),$$

so $A \in O_q(k, d)$, and finally

$$A\vec{w} = dM\vec{w} = kd\vec{v} \in (kd\mathbb{Z})^4. \qquad \square$$

Chapter 7

Totally Real Number Fields

A *totally real number field*, K, is a finite extension of $\mathbb{Q}$ such that the image of each embedding of K into $\mathbb{C}$ lies in $\mathbb{R}$. A *totally positive quadratic from* over a totally real number field K is a quadratic form, $q = \sum_{1<i\leq j<Nj} a_{ij}x_ix_j \in K[x_1, \ldots, x_N]$ such that for each embedding, $\sigma_n : K \to \mathbb{R}$, $\sigma(q) = \sum_{1<i\leq j<N} \sigma(a_{ij})x_ix_j$ is a positive definite quadratic form.

Icaza, in her work on Hermite constants [28] for totally positive quadratic forms over totally real number fields produced a bound using the Cartesian product of ellipsoids called polyellipsoids. Inspired by Deutsch [14], I replaced the polyellispoids used by Icaza with a more complicated shape that yields a better bound. The bulk of this result comes down to computing the volume of this body. Using these techniques leads to

Theorem 7.6. *Let $K/\mathbb{Q}$ be a totally real number field of degree d. Let B_N be the unit N-ball. For all $N \in \mathbb{Z}^+$.*

$$\gamma_N^+(\mathbb{Z}_K) \leq d^{-2d}4^d \left(\frac{(dN)!}{(N!)^d}\right)^{\frac{2}{N}} |d(K)| \operatorname{Vol}(B_N)^{\frac{-2d}{N}}$$

$\gamma_N^+(Z_K)$ is the positive Hermite constant which is restricted to considering only totally positive quadratic form.

7.1 Works of Deutsch and Icaza

Icaza defines the Hermite constant for number fields as follows: $\gamma_{N,K}$. Let q be a positive definite quadratic form over K. Define

$$\mu(q) := \min_{x \in (\mathbb{Z}_K^n)^\bullet} \{\|q(x)\|\}$$

$$d(f) := \|\det(q)\|$$

where $\|\cdot\|$ denotes the absolute value of the field norm. Then put $\gamma(q) := \mu(q)/d(q)^{1/n}$. Finally define $\gamma_{N,K} := \sup_q\{\gamma(q)\}$ where q runs over all totally positive definite quadratic forms defined over K.

Using this definition Icaza derives a bound on the Hermite Constant for all number fields. For the purposes of this chapter, I am restricting Icaza's results to totally real number fields. In this case Icaza'a bound is given by $\gamma^+_{N,K} \leq 4^d B_N \|D\|$, where d is the degree of K, B_N is the volume of the N-sphere, and D is the discriminant of K. This is obtained by looking at an ellipsoid around each embedding of the form into the real numbers, taking the Cartesian product, and applying Minkowski's convex body theorem.

Proof of Icaza's result [28]. Let $\sigma_1, \ldots, \sigma_d \to \mathbb{R}$ be the real embeddings. Let $q = \sum_{1<i\leq j<N j} a_{ij} x_i x_j \in K[x_1, \ldots, x_N]$ be totally positive. We define for each embedding $q_i = \sigma_i(q) \in \mathbb{R}[x_1, \ldots, x_N]$. As defined each of these forms is positive definite. Then for all $t \in K^N$ and $x_i = \sigma_i(t)$

$$\|q(t)\| = \prod_{i=1}^{d} |q_i(x_i)| = \prod_{i=1}^{d} q_i(x_i)$$

and in the same vein

$$\|\operatorname{disc} q\| = \prod_{i=1}^{d} \operatorname{disc} q_i,$$

so we can take

$$\gamma(q) = \inf_{x \in (\mathbb{Z}_K^N)^\bullet} \prod_{i=1}^{d} \frac{q_i(x_i)}{(\operatorname{disc} q_i)^{\frac{1}{N}}}.$$

Since each q_i is a positive definite real quadratic form, we can define function with level sets

$$\Omega(q_i, R) = \{x \in \mathbb{R}^N \mid q_i(x) \leq R^2\}$$

These are ellispoids. Take $y_1, \ldots, y_d \in \mathbb{R}^N$ and define

$$Q : \mathbb{R}^{dN} \to \mathbb{R}, Q(y_1, \ldots, y_d) = \max_{1 \leq i \leq d} q_i(y_i)$$

The level sets of this function form polyellipsoids, which are the Cartesian product of ellipsoids.

$$\Omega(Q, R) = \{x \in \mathbb{R}^N \mid Q \leq R^2\} = \prod_{i=1}^{d} \Omega(q_i, R)$$

The volume of this figure can be computed using this decomposition into its embeddings

$$\operatorname{Vol}\Omega(Q, R) = \prod_{i=1}^{d} \operatorname{Vol}\Omega(q_i, R) = \prod_{i=1}^{d} \frac{\operatorname{Vol}(B_N)}{\sqrt{\operatorname{disc} q_i}} R^N = \frac{\operatorname{Vol}(B_N)^d R^{dN}}{\sqrt{\|\operatorname{disc} q\|}}$$

Set $\Lambda = \mathbb{Z}_K^N \subset \mathbb{R}^{dN}$; Λ is the Cartesian product of N copies of the usual lattice $\mathbb{Z}_K$ in $\mathbb{R}^d$, Thus we have that the Covol $\Lambda = \sqrt{|d(K)|}^N$. We can then choose an R such that

$$\frac{\operatorname{Vol}(B_N)^d R^{dN}}{\sqrt{\operatorname{disc} q}} = \operatorname{Vol}\Omega(Q, R) = 2^{dN} \operatorname{Covol}\Lambda = 2^{dN} |d(K)|^{N/2}$$

This R is

$$R = 2\, |d(K)|^{\frac{1}{2d}}\, \|\operatorname{disc} q\|^{\frac{1}{2dN}} \operatorname{Vol}(B_N)^{\frac{-1}{N}}$$

Then we apply Minkowski's Convex Body Theorem to see that there is a $v \in \Omega(Q, R) \cap \Lambda^\bullet$. Then $q_i(v) \leq R^2$ for all i, so

$$|q(v)| = \prod_{i=1}^{d} q_i(v) \leq R^{2d} = 4^d\, |d(K)|\, \|\operatorname{disc} q\|^{\frac{1}{N}} \operatorname{Vol}(B_N)^{\frac{-2d}{N}}$$

an therefore

$$\gamma(q) \leq \frac{|q(v)|}{|\operatorname{disc} q|^{\frac{1}{N}}} \leq 4^d \operatorname{Vol}(B_N)^{\frac{-2d}{N}} |d(K)|$$

□

Deutsch in his paper on Götsky's four squares theorem [14] he first proves the two squares theorem over $\mathbb{Q}\left(\sqrt{5}\right)$ using a polyellipsoid in the same manner as Icaza. He then uses a refined technique for proving the sum of four squares is universal over the same field. Instead of taking the Cartesian product of ellipsoids, he takes the sum of the distance formula defining the individual spheres to get a smaller convex body. After some calculations to determine the volume of this body, he uses it to get a better bound on the in the particular case of the sum of four squares.

The plan for remainder of this chapter is to use Deutsch's idea of using the sum of sphere equations and take the sum of ellipsoids equations to get a bound on arbitrary degree totally real number fields.

7.2 Improved bound on Hermite constant

We will be treating $\mathbb{R}^{Nd}$ as d copies of $\mathbb{R}^N$ and hence will use the notation $x_{i,j} = x_{(i-1)n+j}$ to visually simply the statements.

Definition 7.1. *Let q be a totally positive n-ary quadratic form over a totally real number field K with $[K : \mathbb{Q}] = d$. Let $\sigma_1, \ldots, \sigma_d$ be the embeddings from $K \hookrightarrow \mathbb{R}$. Then we define the region $\Omega_q(R) = \left\{x \in \mathbb{R}^{Nd} \mid \sum_{i=1}^{d} \sqrt{\sigma_i(q)\left(x_{i,1}, \ldots, x_{i,N}\right)} < R\right\}$.*

Theorem 7.2. $\operatorname{Vol}(\Omega_q(R)) = \frac{(n!)^d}{(dN)!} \frac{(V_N)^d}{\sqrt{\|\operatorname{disc} q\|}} R^{Nd}$.

We will first prove several lemmas that will be used in the proof of this theorem. We will see that the volume of this region differs from the polyellipsoid used by Icaza by a factor of $\frac{(n!)^d}{(dn)!}$.

Lemma 7.3. *Let q be a positive definite n-ary real quadratic form. Let $B_q(R)$ be the closed ellipsoid defined by $\sqrt{q(x_1,\ldots,x_n)} \leq R$ in $\mathbb{R}^n$. Let $S_q(R)$ be the surface area of $B_q(R)$. Let S_n be the surface area of the unit n ball. Let $r = \sqrt{q(x_1,\ldots,x_n)}$. Let g be a continuous function of a single variable. Then*

$$\int_{B_q(R)} g(r) = \int_0^R g(r)S_q(r)dr = \frac{S_n}{\sqrt{\operatorname{disc} q}} \int_0^R g(r)r^{n-1}dr$$

Proof of Lemma 7.3. We begin by integrating over the entire ellipsoid, since the function is taken to be constant over level sets of the ellipsoid we can instead integrate over the surface at each level set.

$$\int_{B_q(R)} g(q) = \int_0^R g(r)S_q(r)dr$$

and $S_q(r) = S_q(1)r^{n-1} = \frac{S_n}{\sqrt{\operatorname{disc} q}} r^{n-1}$.

$$\int_0^R g(r)S_n r^{n-1}dr = \frac{S_n}{\sqrt{\operatorname{disc} q}} \int_0^R g(r)r^{n-1}dr$$

□

We will need a combinatorial identity to simplify a later integral.

Lemma 7.4. *For $m \in \mathbb{Z}^{>0}$*

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{m}{m+k} = \binom{m+n}{n}^{-1}$$

Proof. We begin with a base case that $n = 1$.

$$\begin{aligned}
\sum_{k=0}^{1} (-1)^k \binom{1}{k} \frac{m}{m+k} &= (-1)^0 \binom{1}{0} \frac{m}{m+0} + (-1)^1 \binom{1}{1} \frac{m}{m+1} \\
&= 1 \cdot 1 \cdot \frac{m}{m+0} - 1 \cdot 1 \cdot \frac{m}{m+1} \\
&= \frac{1}{m+1}
\end{aligned}$$

and

$$\binom{m+1}{1}^{-1} = (m+1)^{-1} = \frac{1}{m+1}$$

So the base case is verified.

We will define a recursive relationship between b_n and b_{n-1}.

$$\begin{aligned}
b_n &= \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{m}{m+k} \\
&= 1 + \sum_{k=1}^{n-1} (-1)^k \binom{n}{k} \frac{m}{m+k} + (-1)^n \frac{m}{m+n} \\
&= 1 + \sum_{k=1}^{n-1} (-1)^k \left[\binom{n-1}{k} + \binom{n-1}{k-1} \right] \frac{m}{m+k} + (-1)^n \frac{m}{m+n} \\
&= 1 + \sum_{k=1}^{n-1} (-1)^k \binom{n-1}{k} \frac{m}{m+k} + \sum_{k=1}^{n-1} (-1)^k \binom{n-1}{k-1} \frac{m}{m+k} + (-1)^n \frac{m}{m+n} \\
&= \sum_{k=0}^{n-1} (-1)^k \binom{n-1}{k} \frac{m}{m+k} + \sum_{k=1}^{n-1} (-1)^k \binom{n-1}{k-1} \frac{m}{m+k} + (-1)^n \frac{m}{m+n} \\
&= b_{n-1} + \sum_{k=1}^{n-1} (-1)^k \binom{n-1}{k-1} \frac{m}{m+k} + (-1)^n \frac{m}{m+n} \\
&= b_{n-1} + \sum_{k=1}^{n} (-1)^k \binom{n-1}{k-1} \frac{m}{m+k} \\
&= b_{n-1} + \frac{m}{n} \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{k}{m+k} \\
&= b_{n-1} + \frac{m}{n} \left[\sum_{k=0}^{n} (-1)^k \binom{n}{k} - \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{m}{m+k} \right] \\
&= b_{n-1} + \frac{m}{n} \left[- \sum_{k=0}^{n} (-1)^k \binom{n}{k} \frac{m}{m+k} \right] \\
&= b_{n-1} - \frac{m}{n} b_n
\end{aligned}$$

$$b_n = b_{n-1} - \frac{m}{n} b_n \implies \frac{m+n}{n} b_n = b_{n-1} \implies b_n = \frac{n}{m+n} b_{n-1}$$

Which when used with the base case gives us

$$b_n = \frac{n}{m+n} b_{n-1} = \frac{n(n+1)}{(m+n)(m+n-1)} b_{n-2} = \frac{n!m!}{(n+m)!} b_0 = \binom{m+n}{n}^{-1} b_0 = \binom{m+n}{n}^{-1}$$

□

We define a quantity, $\Omega_q(k, R)$, that we will use to establish this formula recursively. The definition here depends on the ordering given to the real embeddings of the field.

Lemma 7.5. *Define* $\Omega_q(k, R) = \left\{ x \in \mathbb{R}^{nk} \mid \sum_{i=1}^{k} \sqrt{\sigma_i(q)\left(x_{(i-1)n+1}, \ldots, x_{(i-1)n+n}\right)} < R \right\}$ *for* q *a totally real quadratic form,* $k \in \mathbb{Z}^{>0}$*, and* $R \in R^{\geq 0}$*. Let* V_n *be the volume* B_n*. If* $1 \leq k < d$ *then*

$$\mathrm{Vol}\left(\Omega_q(k+1, R)\right) = \frac{V_n(R)}{\binom{(k+1)n}{n} \sqrt{\mathrm{disc}\, \sigma_{k+1}(q)}} \mathrm{Vol}\left(\Omega_q(k, R)\right)$$

Proof of Lemma 7.5. We will use Lemma 7.3 with $g(r) = \mathrm{Vol}(\Omega_q(k, R-r)$.

$$
\begin{aligned}
\int_{B_{\sigma_{k+1}}(R)} g(r) &= \frac{S_n}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\int_0^R g(r) r^{n-1} \\
&= \frac{S_n}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\int_0^R \mathrm{Vol}(\Omega_q(k, R-r)) r^{n-1} \\
&= \frac{S_n}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\int_0^R \mathrm{Vol}(\Omega_q(k,1))(R-r)^{kn} r^{n-1} \\
&= \frac{S_n \mathrm{Vol}(\Omega_q(k,1))}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\int_0^R (R-r)^{kn} r^{n-1} \\
&= \frac{S_n \mathrm{Vol}(\Omega_q(k,1))}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\int_0^R \sum_{i=0}^{kn}\binom{kn}{i}(-1)^i R^{kn-i} r^{n+i-1} \\
&= \frac{S_n \mathrm{Vol}(\Omega_q(k,1))}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\sum_{i=0}^{kn}\binom{kn}{i}(-1)^i R^{kn-i}\left.\frac{r^{n+i}}{n+i}\right|_0^R \\
&= \frac{S_n \mathrm{Vol}(\Omega_q(k,1))}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\sum_{i=0}^{kn}\binom{kn}{i}(-1)^i \frac{R^{k(n+1)}}{n+i} \\
&= \frac{S_n \mathrm{Vol}(\Omega_q(k,1))R^{k(n+1)}}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\sum_{i=0}^{kn}\binom{kn}{i}(-1)^i \frac{1}{n+i} \\
&= \frac{S_n \mathrm{Vol}(\Omega_q(k,1))R^{k(n+1)}}{n\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\sum_{i=0}^{kn}\binom{kn}{i}(-1)^i \frac{n}{n+i} \\
&= \left(\frac{S_n R^n}{n\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\right)\left(\mathrm{Vol}(\Omega_q(k,1))R^{kn}\right)\left(\sum_{i=0}^{kn}\binom{kn}{i}(-1)^i \frac{n}{n+i}\right) \\
&= \left(\frac{V_n(R)}{\sqrt{\operatorname{disc}\sigma_{k+1}(q)}}\right)\left(\mathrm{Vol}(\Omega_q(k,R))\right)\binom{kn}{n}^{-1}
\end{aligned}
$$

□

Proof of Theorem 7.2. First we start with $\Omega_q(1,R) = \Omega_{\sigma_1(q)}(R)$. Then $\mathrm{Vol}(\Omega_{\sigma_1(q)}(R)) = \frac{V_n}{\sqrt{\operatorname{disc}\sigma_1(q)}}R^n$.

And $\Omega_q(R) = \Omega_q(d, R)$.

$$\begin{aligned}
\mathrm{Vol}(\Omega_q(R)) &= \mathrm{Vol}(\Omega_q(d,R)) \\
&= \frac{V_n(R)}{\binom{dn}{n}\sqrt{\mathrm{disc}\,\sigma_d(q)}}\,\mathrm{Vol}(\Omega_q(d-1,R)) \\
&= \frac{V_n(R)}{\binom{dn}{n}\sqrt{\mathrm{disc}\,\sigma_d(q)}}\frac{V_n(R)}{\binom{(d-1)n}{n}\sqrt{\mathrm{disc}\,\sigma_{d-1}(q)}}\,\mathrm{Vol}(\Omega_q(d-2,R)) \\
&= \prod_{k=1}^{d} V_n(R)\frac{1}{\prod_{k=1}^{d}\binom{kn}{n}}\frac{1}{\prod_{k=1}^{d}\sqrt{\mathrm{disc}\,\sigma_k(q)}} \\
&= (V_n(R))^d\frac{(n!)^d}{(dn)!}\frac{1}{\sqrt{\|\mathrm{disc}\,q\|}}
\end{aligned}$$

□

So now we use the convex body to obtain a bound on the Hermite Constant.

Theorem 7.6. *Let $K/\mathbb{Q}$ be a totally real number field of degree d. For all $N \in \mathbb{Z}^+$.*

$$\gamma_N^+(\mathbb{Z}_K) \leq d^{-2d}4^d\left(\frac{(dN)!}{(N!)^d}\right)^{\frac{2}{N}} |d(K)|\,\mathrm{Vol}(B_N)^{\frac{-2d}{N}}$$

Proof. Let $\Lambda = \mathbb{Z}_K^N \subset \mathbb{R}^{dN}$. Then we have that $\mathrm{Covol}\,\Lambda = \sqrt{|d(K)|}^N$ [40]. We can choose a value for R such that it satisfies

$$\frac{(n!)^d}{(dn)!}\frac{(V_n)^d}{\sqrt{\|\mathrm{disc}\,q\|}}R^{nd} = \mathrm{Vol}(\Omega_q(R)) = 2^{dN}\,\mathrm{Covol}\,\Lambda = 2^{dN}\,|d(K)|^{\frac{N}{2}}$$

.

We find that

$$R = 2\left(\frac{(dn)!}{(n!)^d}\right)^{\frac{1}{dn}} |d(K)|^{\frac{1}{2d}}\,|\mathrm{disc}\,q|^{\frac{1}{2dN}}\,V_n^{\frac{-1}{N}}$$

Now we can apply the Minkowski's Convex Body Theorem to find a vector $v \in \Omega_q(R) \cap \Lambda^\bullet$.

Thus $\sum_{i=1}^{d} \sqrt{\sigma_i(q(v))} \leq R$

We can apply the arithmetic-geometry mean inequality to find that

$$d\left(\prod_{i=1}^{d} \sqrt{\sigma_i(q(v))}\right)^{1/d} \leq \sum_{i=1}^{d} \sqrt{\sigma_i(q(v))}$$

Since $|q(v)| = \prod_{i=1}^{d} \sigma_i(q(v))$, we can then see that $d\,|q(v)|^{\frac{1}{2d}} \leq R$

So

$$\begin{aligned} |q(v)| &\leq d^{-2d}R^{2d} \\ &= d^{-2d}\left(2\left(\frac{(dn)!}{(n!)^d}\right)^{\frac{1}{dn}} |d(K)|^{\frac{1}{2d}}\,|\text{disc}\,q|^{\frac{1}{2dn}}\,V_n^{\frac{-1}{N}}\right)^{2d} \\ &= d^{-2d}2^{2d}\left(\frac{(dn)!}{(n!)^d}\right)^{\frac{2}{n}} |d(K)|\,|\text{disc}\,q|^{\frac{1}{n}}\,V_n^{\frac{-2d}{n}} \end{aligned}$$

Which finally gives

$$\gamma_n^+(K) \leq \frac{|q(v)|}{|\text{disc}\,q|^{1/n}} \leq d^{-2d}2^{2d}\left(\frac{(dn)!}{(n!)^d}\right)^{\frac{2}{n}} |d(K)|\,V_n^{\frac{-2d}{n}}$$

□

It is not readily apparent if this new bound is an improvement or not. It differs from the bound found by Icaza by exactly a factor of $d^{-2d}\left(\frac{(dn)!}{(n!)^d}\right)^{\frac{2}{n}}$. This quantity can be shown to always be less than one for values of d and n greater than 1.

Theorem 7.7. *Let n, d be positive integers such that $n, d > 1$.*

$$d^{-2d}\left(\frac{(dn)!}{(n!)^d}\right)^{\frac{2}{n}} < 1$$

Proof. We manipulate the expression slightly.

$$d^{-2d}\left(\frac{(dn)!}{(n!)^d}\right)^{\frac{2}{n}} = \left(\frac{(dn)!}{d^{nd}(n!)^d}\right)^{\frac{2}{n}}$$

In the denominator we can think of it as an array with n columns and d rows all multiplied together. Since we have a term of d^{nd} we can distribute a d to every entry in our array and have

$$\left.\begin{array}{c} n! = \overbrace{n(n-1)(n-2)\cdots 1}^{n} \\ n! = n(n-1)(n-2)\cdots 1 \\ \vdots \\ n! = n(n-1)(n-2)\cdots 1 \end{array}\right\} d \qquad \left.\begin{array}{c} \overbrace{dn\ d(n-1)\ d(n-2)\cdots d}^{n} \\ dn\ d(n-1)\ d(n-2)\cdots d \\ \vdots \\ dn\ d(n-1)\ d(n-2)\cdots d \end{array}\right\} d$$

Now consider the d leading terms of the numerator paired with the first column of the array.

$$\frac{dn}{dn}, \frac{dn-1}{dn}, \ldots, \frac{dn-d+1}{dn} = \frac{d(n-1)+1}{dn}$$

Similarly the $k+1$–st block of d terms of the numerator will be paired with the $k+1$–st column of the array

$$\frac{d(n-kd)}{d(n-kd)}, \frac{d(n-kd)-1}{d(n-kd)}, \ldots, \frac{d(n-kd)-d+1}{d(n-kd)} = \frac{d(n-(k+1)d)+1}{d(n-kd)}$$

So in each block of terms the numerator is smaller than the denominator. Therefore the bound is an improvement. □

Chapter 8

Abstract Geometry of Numbers

In the previous chapter the definition of the Hermite constant was extended to the case of totally positive quadratic forms over the ring of integers in a totally real field. We now seek to extend the definition to the case of S-integer rings also called Hasse domains within a global field. The principal result of this section is showing the finiteness of this extended constant.

Theorem 8.7. *The Hermite constant for S-integer rings of global fields of characteristic not equal to 2 is finite.*

The choice of language, notation, and introduction for this section are taken from [6].

8.1 Hasse Domains

A *norm* on a ring R is a function $|\cdot| : R \to \mathbb{R}^{\geq 0}$ such that

1. $|x| = 0 \iff x = 0$,
2. $|x| \geq 1$ for all $x \in R^{\bullet}$; $|x| = 1 \iff x \in R^{\times}$,
3. $\forall x, y \in R$, $|xy| = |x||y|$.

Let $|\cdot|$ be a norm on a ring R.

$$A(R) = \inf\{C \in \mathbb{R}^{>0} \mid \forall x, y \in R,\ |x + y| \leq C \max(|x|, |y|)\}.$$

If there is no such C, then $A(R) = \inf \varnothing = \infty$. If $A(R) < \infty$ we say that the norm is *almost metric* and call $A(R)$ the *Artin constant*. It follows that for all $x, y \in K$, $|x+y| \leq A(R) \max(|x|, |y|)$, and thus $|\cdot|$ is an absolute value on K in the sense of E. Artin.

When $A(R) = 1$ we say the norm is *non-Archimedean* or *ultrametric*.

Lemma 8.1. *Let R be a domain with fraction field K, and let $|\cdot|$ be an almost metric norm on R with Artin constant $A(R)$. Then we have*

a) $A(R) = \max(|1|, |2|)$.

b) For $\alpha \in \mathbb{R}^{>0}$, $A(R, |\cdot|^{\alpha}) = A(R)^{\alpha}$.

c) The map $(x, y) \mapsto |x - y|$ *is a metric on K iff* $A(R) \leq 2$.

d) For $x_1, \ldots, x_n \in K$, $|x_1 + \ldots + x_n| \leq |n| \max_i |x_i|$.

See [6] for proof.

Let K be a global field. A *place* on K is an equivalence class of almost metric norms on K. We denote by Σ_K the set of all places of K. Let S be a finite, nonempty subset of Σ_K containing all the Archimedean places. We define $\mathbb{Z}_{K,S}$ as the set of all elements $x \in K$ such that $|x|_v \leq 1$ for every ultrametric place $|\cdot|_v \in \Sigma_K \setminus S$. Following O'Meara [38] we call such a ring a *Hasse domain*. Every Hasse domain is a residually finite Dedekind domain hence comes equipped with the canonical ideal norm $|I| = \#R/I$.

Next we recall some facts.

• Suppose $K \cong \mathbb{Q}[t]/(f)$ is a number field. Then the set of Archimedean places of K is finite and nonempty. More precisely, if f has r real roots and s conjugate pairs of complex roots, then K has r real places – i.e., such that the corresponding completion is isomorphic to the normed field $\mathbb{R}$ – and s complex places – i.e., such that the corresponding completion is isomorphic to the normed

field $\mathbb{C}$. We write out the infinite places as $\infty_1, \ldots, \infty_{r+s}$. The finite places correspond to maximal ideals of $\mathbb{Z}_K$, the integral closure of $\mathbb{Z}$ in K, which is the unique minimal Hasse domain with fraction field K: any other Hasse domain $\mathbb{Z}_{K,S}$ with fraction field K is an overring of R, obtained as $\bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} R \setminus S_f} R_{\mathfrak{p}}$ where S_f is a finite set of maximal ideals corresponding to a finite set of places.
• Suppose K has characteristic $p > 0$. Then there is a prime power $q = p^f$ such that $K/\mathbb{F}_q(t)$ is a regular extension – separable, with constant field $\mathbb{F}_q$. There is a unique smooth, projective geometrically integral curve $C_{/\mathbb{F}_q}$ such that $K = \mathbb{F}_q(C)$ is the field of rational functions on C. The places of K are all non-Archimedean and correspond bijectively to closed points on C, or equivalently to complete $\mathfrak{g}_{\mathbb{F}_q} = \operatorname{Aut}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbits of $\overline{\mathbb{F}_q}$-valued points of C. Thus the Hasse domains with fraction field K correspond to finite unions of complete $\mathfrak{g}_{\mathbb{F}_q}$-orbits of $\overline{\mathbb{F}_q}$-points of C, and any such R is the ring of rational functions which are regular away from the support of D, a finite set of points. There is no unique minimal Hasse domain in this case, because we cannot take $D = \emptyset$: the ring of functions which are regular on all of C is just $\mathbb{F}_q$.

The norm $|\cdot|$ on R need not be almost metric but is *multimetric*: a finite product of almost metric norms. Note in particular that the canonical norms on every Hasse domain and affine domain are multimetric.

For $1 \leq j \leq m$ we put $\mathcal{N}_j = |K^\times|_j$.

The norm $|\cdot|$ is of *q-type* iff there is $q > 0$ such that $\mathcal{N}_j \subset q^{\mathbb{Z}}$ for all j: this is the situation for affine domains. We emphasize that more than one choice of q is always possible but that such a choice will always be given as part of the structure. As in the $m = 1$ case we put $\deg_j = \log_q |\cdot|_j$. When each $-\deg j$ is a discrete valuation, we say the norm is *totally ultrametric*.

The norm is *totally dense* if $\mathcal{N}_j$ is dense for each j. If each $|\cdot|_j$ is metric, this is equivalent to each $|\cdot|_j$ being Archimedean, and we use the terminology *totally Archimedean*. The canonical norm on $R = \mathbb{Z}_K$, K a number field, is totally Archimedean. The norm is of *mixed type* if some $\mathcal{N}_j$ is dense and some $\mathcal{N}_{j'}$ is not. The canonical norm on $R = \mathbb{Z}_{K,S}$ when $S \neq \varnothing$ is of mixed multimetric type.

We say an ideal normed Dedekind domain $(R, |\cdot|)$ is *multinormed* if there are elementwise norms $|\cdot|_1, \ldots, |\cdot|_m$ on R such that $|x| = \prod_{j=1}^m |x|_j$ for all $1 \leq j \leq m$. We say that $(R, |\cdot|)$ is **multimetric** if each norm $|\cdot|_j$ is almost metric.

A multimetric ideal normed Dedekind domain R is of *multinormed linear type* if for all $n \in \mathbb{Z}^+$ there is $C \in \overline{\mathcal{N}}$ such that: given $M = (m_{ij}) \in \mathrm{GL}_n(K)$, an R-lattice $\Lambda \subset K^n$ and for all $1 \leq j \leq m$ constants $\epsilon_{1j}, \ldots, \epsilon_{nj} \in \overline{\mathcal{N}_j}$ such that

$$|\det M| \operatorname{Covol} \Lambda \leq C \prod_{i,j} \epsilon_{ij}, \tag{8.1}$$

there is $x = (x_1, \ldots, x_n) \in \Lambda^\bullet$ such that

$$\forall i, j, \ \left| \sum_{k=1}^n m_{ik} x_k \right|_j \leq \epsilon_{ij}.$$

When R is of multinormed linear type, we let $C_M(R, n)$ be the supremum over all $C \in \overline{\mathcal{N}}$ such that (8.1) holds. We call the $C_M(R, n)$'s the *multinormed linear constants* of R.

8.2 Linear Forms Constants

First we consider *Real Minkowski functionals*. Let $N \in \mathbb{Z}^+$. For $x = (x_1, \ldots, x_N) \in \mathbb{R}^N$, put $||x|| = \max_i |x_i|$. Let $I_N = \{x \in \mathbb{R}^N \mid ||x|| = 1\}$, i.e., the boundary of the unit ball in the ℓ^∞-metric.

Consider the following axioms for a function $f : \mathbb{R}^N \to \mathbb{R}^{\geq 0}$:

MF0 $\forall x \in \mathbb{R}^N$, $f(x) = 0 \implies x = 0$. (definiteness)

MF1 $\forall \alpha \in \mathbb{R}^{\geq 0}$, $\forall x \in \mathbb{R}^N$, $f(\alpha x) = \alpha f(x)$. (positive homogeneity)

MF2 $\forall x \in \mathbb{R}^N$, $f(-x) = f(x)$. (symmetry)

MF3 $\forall x, y \in \mathbb{R}^N$, $f(x + y) \leq f(x) + f(y)$. (subadditivity)

MF4 f is continuous. (continuity)

MF4' $\sup(f|_{I_N}) < \infty$. (boundedness)

MF4" f is continuous at 0.

Lemma 8.2. *Let $f : \mathbb{R}^N \to \mathbb{R}^{\geq 0}$ satisfy (MF1). Then (MF4) $\implies$ (MF4′) $\iff$ (MF4″), and the first implication cannot be reversed.*

Proof can be found in [6].

A *Minkowski distance function* is a function $f : \mathbb{R}^N \to \mathbb{R}^{\geq 0}$ satisfying (MF0) through (MF3). These are precisely the norm functions on the finite-dimensional $\mathbb{R}$-vector space $\mathbb{R}^N$. We recall the very standard facts that $\|\cdot\| : x \mapsto \|x\|$ is a Minkowski Distance Function ("Minkowski's Inequality") and that if f is any Minkowski distance function then there are constants $0 < C_1 < C_2 < \infty$ such that

$$\forall x \in \mathbb{R}^N,\ C_1 \|x\| \leq f(x) \leq C_2 \|x\|.$$

Thus in the presence of (MF0) through (MF2), (MF3) $\implies$ (MF4).

Classical geometry of numbers also includes the study of functions which merely satisfy (MF1) and (MF4): the level sets $f^{-1}([0, R])$ of such functions are *star bodies*, and conversely to any star body we can associate a function $f : \mathbb{R}^N \to \mathbb{R}$ satisfying (MF1) and (MF4). The portion of the classical geometry of numbers that we wish to generalize requires only the weaker (MF4′), so we define a *Minkowski functional* as a function $f : \mathbb{R}^N \to \mathbb{R}^{\geq 0}$ which satisfies (MF1) and (MF4′).

Let f be a Minkowski functional. A lattice Λ is *f-admissible* if $\inf(f|_{\Lambda^\bullet}) \geq 1$. We define the *lattice constant of f* as

$$\Delta(f) = \inf\{\operatorname{Covol} \Lambda \mid \Lambda \text{ is } f\text{-admissible}\}.$$

Thus $\Delta(f) = \infty$ iff there are no f-admissible lattices (e.g. when $f \equiv 0$). When $\Delta(f) < \infty$ we say f is *of finite type*.

Lemma 8.3. *For any Minkowski functional $f : \mathbb{R}^N \to \mathbb{R}^{\geq 0}$ and any $\alpha \in \mathbb{R}^{\geq 0}$, αf is also a Minkowski functional, and*

$$\Delta(\alpha f) = \alpha^{-N} \Delta(f).$$

8.3 Mahler-Minkowski Functionals

Let R be a Hasse domain. Thus K is a global field, $S \subset \Sigma_K$ is a finite set of places containing all the infinite places, and $R = \mathbb{Z}_{K,S}$ is the ring of functions which have non-negative valuation at every $v \in \Sigma_K \setminus S$. For each $v \in S$, let $|\cdot|_v$ be the corresponding almost metric norm: precisely, if $K_v \cong \mathbb{R}$ then it is the usual Euclidean absolute value; if $K_v \cong \mathbb{C}$ we take the square of the standard Euclidean absolute value; if v is ultrametric and the residue cardinality is q then for a uniformizer π_v we have $|\pi_v|_v = q^{-1}$. We put

$$\mathcal{K} = \prod_{v \in S} K_v$$

and define $|\cdot| : \mathcal{K} \to \mathbb{R}^{\geq 0}$ by $|x| = \prod_{v \in S} |x|_v$. The map $x \mapsto |x|$ is a norm: we have $|x| \geq 1$ for all $x \in R^\bullet$, with equality iff $x \in R^\times$. Moreover we have

$$\forall x \in R^\bullet, \ \#R/(x) = \prod_{v \in S} |x|_v.$$

The additive group $(R, +)$ is discrete in $\mathcal{K}$ with compact fundamental domain. Thus there is a unique Haar measure Vol on $(\mathcal{K}, +)$ such that $\mathrm{Covol}(R) = 1$. Further, for every nonzero ideal I of R, we have $\mathrm{Covol}\, I = \#R/I$ and thus by [6, Prop. 1.8] $I \mapsto \mathrm{Covol}\, I$ is an ideal norm on R.

Let $N \in \mathbb{Z}^+$. For $x = (x_1, \ldots, x_N) \in \mathcal{K}^N$, we put $||x|| = \max_{1 \leq i \leq N} |x_i|$. Let $e_1, \ldots, e_N$ be the standard basis vectors of $\mathcal{K}^N$. Let

$$I_N = \{x = (x_1, \ldots, x_N) \in \mathcal{K}^N \mid \forall 1 \leq i \leq N, \forall v \in S, \ |x_i|_v \leq 1\}.$$

A *Mahler-Minkowski functional* is a function $f : \mathcal{K}^n \to \mathbb{R}^{\geq 0}$ satisfying

MF1 (Homogeneity) $\forall \alpha \in \mathcal{K},\ \forall x \in \mathcal{K}^N,\ f(\alpha x) = |\alpha| f(x)$, and

MF4′ (Linear Majorization) The *cube constant* $C(f) = \sup(f|_{I_N})$ is finite.

Remark 8.4. *Since I_N is compact, as above* continuity *of f implies (MF4′).*

We define an R-lattice in $\mathcal{K}$ to be a finitely generated *free* R-submodule $\Lambda \subset \mathcal{K}^N$ such that $\langle \Lambda \rangle_{\mathcal{K}} = \mathcal{K}^N$.

We give $(\mathcal{K}^N, +)$ the product Haar measure, so that the *standard R-lattice* $\Lambda_0 = R^N$ has covolume 1. Then any R-lattice Λ has a covolume $\operatorname{Covol} \Lambda \in (0, \infty)$. More explicitly, if Λ is a free R-lattice then we may write $\Lambda = g\Lambda_0$ for some $g \in \mathrm{GL}_N(\mathcal{K})$ and then $\operatorname{Covol} \Lambda = |\det g|$. Let $f : \mathcal{K}^n \to \mathbb{R}^{\geq 0}$ be a Mahler-Minkowski functional. An R-lattice $\Lambda \subset \mathcal{K}^N$ is **f-admissible** if $\inf(f|\Lambda^\bullet) > 1$. We define the *lattice constant of f* as

$$\Delta(f) = \inf\{\operatorname{Covol} \Lambda \mid \Lambda \text{ is } f\text{-admissible}\}.$$

The definition of $C(R, N)$ is the largest number C such that: if $M \in \mathrm{GL}_N(K)$, $\Lambda \subset K^N$ is an R-lattice and $\{\epsilon_i\}_{1 \leq i \leq N}$ are positive constants with each ϵ_i in the closure of $|K^\times|$ and such that

$$|\det M| \operatorname{Covol} \Lambda \leq C \prod_i \epsilon_i,$$

then there is $x = (x_1, \ldots, x_N) \in \Lambda^\bullet$ such that

$$\forall 1 \leq i \leq N,\ \left| \sum_{k=1}^N m_{ik} x_k \right| \leq \epsilon_i.$$

Taking M to be the identity matrix and each $\epsilon_i = 1$ we get that if $\operatorname{Covol} \Lambda \leq C(R, N)$ then there is $x \in \Lambda^\bullet$ with $\|x\| \leq 1$, so $\inf(\|\cdot\|, \Lambda^\bullet) \leq 1$ and Λ is not $\|\cdot\|$-admissible.

Theorem 8.5. *We have*

$$\Delta(\|\cdot\|) \geq C(R, N) > 0$$

Proof. Let $\Lambda \subset \mathcal{K}$ be a lattice, we can take an R-basis, $e_1, \ldots, e_N$. We have that K is dense in $\mathcal{K}$ hence we can apply weak approximation. Thus we can construct a sequence $\{e_{i,n}\}_{n=1}^{\infty} \subset K^N$ so that each $e_{i,n} \to e_i$. We can then use these points to construct a sequence of lattices $\Lambda_n = \langle e_{1,n}, \ldots, e_{N,n} \rangle_R$.

We can assume that these are all linearly independent vectors and hence for a lattice lattices because it is only required that the matrix formed by the vectors have full rank. Since we are working over a finite product of fields and $GL_N(\mathcal{K}) = \prod GL_N(K_v)$ this will hold if the determinant is nonzero. Since the original lattice Λ had nonzero covolume and the determinant is a continuous function of its entries and $\operatorname{Covol} \Lambda_n \to \operatorname{Covol} \Lambda$, eventually the determinant must be nonzero for all $n > M$ for some M. Hence we by renumbering our sequence so that it starts at M and have every $e_{i,n}$ define a full rank lattice.

If any of our constructed lattices are such that $\operatorname{Covol} \Lambda_n \leq \operatorname{Covol}$, we can apply a scaling factor so that it will.

Each $\Lambda_n \subset K^N$ is a rational lattice. We use the definition of $C(R, N)$ with the identity matrix and $\epsilon_{i,v} = 1$ for all i and v gives $\Lambda_n^\bullet \cap I_N \neq \emptyset$. Specifically there exists some $x_n \in \Lambda_n^\bullet \cap I_N$.

Since our lattices are discrete and I_N is compact, this intersection must be finite for each n. Suppose for the sake of contradiction that $\Lambda^\bullet \cap I_N = \emptyset$. Then for each $z = (z_1, \ldots, z_N) \in (R^N)^\bullet$, the set of $n \in \mathbb{Z}^+$ with $\sum_{i=1}^N z_i e_{i,n} \in I_N$ must be finite, otherwise there would be a limit point to this sequence in I_N giving a contradiction.

So there must be infinitely many $z \in (R^N)^\bullet$ such that for some $n \in \mathbb{Z}^+$, $\sum_{i=1^N} z_i e_{i,n} \in I_N$. Then there must be at least one $1 \leq i \leq N$ such that for each $M > 0$ for at least one $v \in S$, there is $z \in (R^N)^\bullet$ which for some absolute value $|\cdot|_v$ with $|z_i|_v \geq M$ and $n \in \mathbb{Z}^+$ such that $\sum_{i=1}^N e_i z_{i,n} \in I_N$. We can them consider the projection map from $\mathcal{K}^N \to \mathcal{K}$ which projects to the coefficient of e_i. This map will produce a sequence of points that generate a contradiction. □

For Mahler-Minkowski functionals $f, g : \mathcal{K}^N \to \mathbb{R}^{\geq 0}$, g *majorizes* f if $f(x) \leq g(x)$ for all $x \in K^N$. If so, every f-admissible lattice is also g-admissible, hence $\Delta(f) \geq \Delta(g)$. We now deduce the main result of this section.

Theorem 8.6. *For any Mahler-Minkowski functional $f : \mathcal{K}^N \to \mathbb{R}^{\geq 0}$, we have*

$$\Delta(f) \geq C(f)^{-N} C_M(R, N) > 0. \tag{8.2}$$

Proof. The functional f is majorized by $C(f)\|\cdot\|$. Apply Theorem 8.5. □

8.4 Finiteness of Hermite Constant in the Global Field Case

In this section we extend the definition of Hermite Constant to the context of global fields and S-integer rings as follows. Let $R_{K,S}$ be the S-integer ring of the global field K and let Q be the set of non-degenerate quadratic forms.

$$\gamma_N(R_{K,S}) = \sup_{q \in Q} \inf_{x \in (R_{K,S}^N)^\bullet} \frac{|q(x)|}{|\mathrm{disc}\, q|^{\frac{1}{N}}}.$$

Theorem 8.7. *The Hermite constant for S-Integer rings of global fields of characteristic not equal to 2 is finite.*

Let q_0 be a quadratic form over an S-integer ring $\mathbb{Z}_{K,S}$ and let Q be the set of quadratic forms which are $GL_N(\mathcal{K})$ equivalent to q. Then we define the *Hermite invariant* of q to be $\gamma_N(R, q) = \sup_{q \in Q} \inf_{x \in (R_{K,S}^N)^\bullet} \frac{|q(x)|}{|\mathrm{disc}\, q|^{\frac{1}{N}}}$. We will first provide a proof of the finiteness of the Hermite invariant for an arbitrary class of quadratic forms in the number and function field cases separately and then use those theorems to prove this main theorem.

Theorem 8.8. *Let K be a number field, let S be a finite set of places including all the infinite places, $\mathbb{Z}_{K,S}$ its ring of S-integers, N a positive integer, and $\mathcal{K} = \prod_{p \in S} K_p$. For any non-degenerate $GL_N(\mathcal{K})$ equivalence class of quadratic forms of $q \in \mathcal{K}[x_1, \ldots, x_N]$, we have*

$$\gamma_N(\mathbb{Z}_{K,S}, q) \leq \frac{\Delta_K(q)^{\frac{-2}{N}}}{|\mathrm{disc}\, q|^{\frac{1}{N}}}$$

Proof. First we pick an equivalence class of quadratic forms, Q_0, that are $\mathcal{K}$-equivalent to a particular non-degenerate representative q_0.

$$\gamma_{N,0} = \sup_{q \in Q_0} \inf_{x \in (\mathbb{Z}_{K,S}^N)^\bullet} \frac{|q(x)|}{|\mathrm{disc}\, q|^{\frac{1}{N}}}.$$

We can rewrite this expression varying over matrices instead of forms.

$$\begin{aligned}
\gamma_{N,0} &= \sup_{M \in GL_N(\mathcal{K})} \inf_{x \in (\mathbb{Z}_{K,S}^N)^\bullet} \frac{|q_0(Mx)|}{|\mathrm{disc}\, M^T q_0 M|^{\frac{1}{N}}}. \\
&= \sup_{M \in GL_N(\mathcal{K})} \inf_{x \in (\mathbb{Z}_{K,S}^N)^\bullet} \frac{|q_0(Mx)|}{|\mathrm{disc}\, q_0|^{\frac{1}{N}}\, |\det M|^{2/N}}.
\end{aligned}$$

If we replace M with αM where $\alpha \in \mathcal{K}^\times$

$$\begin{aligned}
\sup_{M \in GL_N(\mathcal{K})} \inf_{x \in (\mathbb{Z}_{K,S}^N)^\bullet} \frac{|q_0(\alpha M x)|}{|\mathrm{disc}\, q_0|^{\frac{1}{N}}\, |\det \alpha M|^{2/N}} &= \sup_{M \in GL_N(\mathcal{K})} \inf_{x \in (\mathbb{Z}_{K,S}^N)^\bullet} \frac{|\alpha|^2\, |q_0(Mx)|}{|\mathrm{disc}\, q_0|^{\frac{1}{N}}\, |\alpha|^2\, |\det M|^{2/N}} \\
&= \sup_{M \in GL_N(\mathcal{K})} \inf_{x \in (\mathbb{Z}_{K,S}^N)^\bullet} \frac{|q_0(Mx)|}{|\mathrm{disc}\, q_0|^{\frac{1}{N}}\, |\det M|^{2/N}} \\
&= \gamma_{N,0}
\end{aligned}$$

Hence we can freely scale by squares in the value group without changing the value of the fractions. Therefore we can either choose to scale each matrix so that the inf $|q_0(Mx)|$ is one or p, or if the quadratic form is isotropic its value is zero and it can be safely ignored in the supremum. We construct the set $GL'_N(\mathcal{K})$ to be the representatives of each class of matrix under scaling that gives 1.

We can scale $\inf |q_0(Mx)|$ so that it equals 1. In this case the term drops out of the equation leaving simply:

$$\gamma_{N,0} = \sup_{M \in GL'_N(\mathcal{K})} \frac{1}{|\operatorname{disc} q_s|^{\frac{1}{N}} \, |\det M|^{2/N}}$$

On the other side of the equation.

$$\frac{\Delta_N^{-2/N}}{|\operatorname{disc} q_0|^{1/N}} = \frac{\left(\inf_{\Lambda} \left\{\operatorname{Covol} \Lambda \mid \Lambda \text{ is } \sqrt{|q_0|}\text{-admissible}\right\}\right)^{-2/N}}{|\operatorname{disc} q_0|^{1/N}}$$

And being $\sqrt{|q_0|}$-admissible means that for all $x \in (\mathbb{Z}^N)^\bullet$ $\sqrt{|q_0(x)|} > 1$.

Just as before we change from varying over lattices to varying over matrices.

$$\frac{\Delta_N^{-2/N}}{|\operatorname{disc} q_0|^{1/N}} = \frac{\left(\inf_{M \in GL_N(\mathcal{K})} \left\{\operatorname{Covol} M\mathbb{Z}_{K,S}^N \mid \forall x \in M\mathbb{Z}_{K,S}^N, q_0(x) > 1\right\}\right)^{-2/N}}{|\operatorname{disc} q_0|^{\frac{1}{N}}}$$

But the covolume of this is simply the determinant of the matrix M.

$$\frac{\Delta_N^{-2/N}}{|\operatorname{disc} q_0|^{1/N}} = \frac{\left(\inf_{M \in GL_N(\mathcal{K})} \left\{|\det M| \mid \forall x \in M\mathbb{Z}_{K,S}^N, q_0(x) > 1\right\}\right)^{-2/N}}{|\operatorname{disc} q_0|^{\frac{1}{N}}}$$

For each matrix we can select a representative of the coset given by scaling as above such that the infimum of the absolute value of the quadratic form on the lattice is 1. This is the same set of matrices as before. We introduce the α parameter that varies over scalars to allow us to cover the full range of matrices.

$$
\begin{aligned}
\frac{\Delta_N^{-2/N}}{|\mathrm{disc}\, q_0|^{1/N}} &= \frac{\left(\inf_{M\in GL'_N(\mathcal{K})} \inf_{\alpha\in\mathcal{K}^\times} \left\{|\det \alpha M| \mid \forall x \in \mathbb{Z}_{K,S}^N, q_0(\alpha M x) > 1\right\}\right)^{-2/N}}{|\mathrm{disc}\, q_s|^{\frac{1}{N}}} \\
&= \frac{\left(\inf_{M\in GL'_N(\mathcal{K})} \inf_{\alpha\in\mathcal{K}^\times} \left\{|\alpha|^N |\det M| \mid \forall x \in \mathbb{Z}_{K,S}^N, q_0(\alpha M x) > 1\right\}\right)^{-2/N}}{|\mathrm{disc}\, q_0|^{\frac{1}{N}}}
\end{aligned}
$$

We have $\inf |q_0(Mx)| = 1$ and there exists a sequence of $\alpha \in \mathcal{K}^\times$ that approaches 1 from above without becoming constant.

Then we can use that sequence to see that the α will drop out of our equation.

$$
\begin{aligned}
\frac{\Delta_N^{-2/N}}{|\mathrm{disc}\, q_0|^{1/N}} &= \frac{\left(\inf_{M\in GL'_N(\mathcal{K})} \inf_{\alpha\in\mathcal{K}^\times} \{|\det M| \mid \forall x \in \mathbb{Z}_{K,S}^N, q_0(\alpha M x) > 1\}\right)^{-2/N}}{|\mathrm{disc}\, q_0|^{\frac{1}{N}}} \\
&= \frac{\left(\inf_{M\in GL'_N(\mathcal{K})} |\det M|\right)^{-2/N}}{|\mathrm{disc}\, q_0|^{\frac{1}{N}}}
\end{aligned}
$$

We can take apply the negative from the exponent to take the reciprocal switching the infimum to a supremum.

$$
\begin{aligned}
\frac{\Delta_N^{-2/N}}{|\mathrm{disc}\, q_0|^{1/N}} &= \sup_{M\in GL'_N(\mathcal{K})} \frac{1}{|\det M|^{2/N} |\mathrm{disc}\, q_0|^{\frac{1}{N}}} \\
&= \sup_{M\in GL'_N(\mathcal{K})} \frac{1}{|\det M|^{2/N} |\mathrm{disc}\, q_0|^{\frac{1}{N}}} \\
&= \gamma_{N,0}
\end{aligned}
$$

Therefore we can see that the two sides of the equation are in fact equal.

□

Theorem 8.9. *Let K be a function field of characteristic not equal to 2, let S be a finite set of places, $\mathbb{Z}_{K,S}$ its ring of S-integers, N a positive integer, and $\mathcal{K} = \prod_{p \in S} K_p$. For any non-degenerate $GL_N(\mathcal{K})$ equivalence class of quadratic forms of $q \in \mathcal{K}[x_1, \ldots, x_N]$, we have*

$$\gamma_N(\mathbb{Z}_{K,S}, q) \leq \frac{l^2 \Delta_K(q)^{\frac{-2}{N}}}{|\operatorname{disc} q|^{\frac{1}{N}}}$$

The proof of this theorem mirrors the proof in the number field case. The changes need to be made because we can not necessarily reduce the infimum of every quadratic forms value to the same square class as one and because there may not be a sequence approaching approaching 1 that is non-constant. In both of these cases it introduces factors of l cardinality of the constant field. The equality still holds with some power of l introduced.

Proof of Theorem 8.7. There are a finite number of square classes in any of our local fields and hence we can apply the appropriate one of the two theorems in each case. Further since we present a lower bound on the lattice constant, this produces a bound on each of the classes of quadratic forms. Hence we have the desired upper bound showing finiteness. □

Bibliography

[1] M. Bhargava, *On the Conway-Schneeberger fifteen theorem*. Quadratic forms and their applications (Dublin, 1999), 27–37, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.

[2] M. Bhargava and J.P. Hanke, *Universal quadratic forms and the 290-theorem*, preprint.

[3] Blichfeldt, H. F. (1929). "The minimum value of quadratic forms, and the closest packing of spheres". Math. Ann. 101: 605–608.

[4] J.W.S. Cassels, *An introduction to the geometry of numbers*. Corrected reprint of the 1971 edition. Classics in Mathematics. Springer-Verlag, Berlin, 1997.

[5] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press, 1978.

[6] P.L. Clark, *Abstract GoN: Linear Forms*. Preprint, `math.uga.edu/~pete/GoN_Linear_Forms.pdf`.

[7] P.L. Clark, *Geometry of Numbers With Applications to Number Theory*, `math.uga.edu/~pete/geometryofnumbers.pdf`.

[8] P.L. Clark, J. Hicks, H. Parshall and K.Thompson, *GoNI: Primes represented by binary quadratic forms*, INTEGERS 13 (2013), A37, 18 pp.

[9] P.L. Clark, J. Hicks, K. Thompson and N. Walters, *GoNII: Universal quaternary quadratic forms*, INTEGERS 12 (2012), A50.

[10] J. H. Conway, *The sensual (quadratic) form*, Carus Mathematical Monographs 26, MAA, 1997.

[11] J.H. Conway, *Universal quadratic forms and the fifteen theorem*. Quadratic forms and their applications (Dublin, 1999), 23–26, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000.

[12] D.A. Cox, *Primes of the Form* $x^2 + ny^2$, John Wiley & Sons Inc., 1989.

[13] J.I. Deutsch, *A quaternionic proof of the universality of some quadratic forms*. Integers 8 (2008), no. 2, A3, 23 pp.

[14] J.I. Deutsch, *Geometry of numbers proof of Götzky's four squares theorem*. Journal of Number Theory 96 (2002), 417–431.

[15] L.E. Dickson, *Integers represented by positive ternary quadratic forms*. Bull. Amer. Math. Soc. 33 (1927), 63–70.

[16] L. Euler, *Opera Omnia IV.A-4. The Correspondence Euler - Goldbach* F. Lemmermeyer, M. Mattmüller, eds., Basel 2011.

[17] R.W. Fitzgerald, *Norm Euclidean quaternionic orders*. Integers 11 (2011), A58, 12 pp.

[18] J.H. Grace, *The Four Square Theorem*. J. London Math. Soc. 2 (1927), 3–8.

[19] C.F. Gauss, *Disquisitiones Arithmeticae (English Edition)*, trans. A.A. Clarke, Springer-Verlag, 1986.

[20] C.F. Gauss, *Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen von Ludwing August Seeber* m J. Reine. Agnew. Math. 20 (1840), 312-320.

[21] T.R. Hagedorn, *Primes of the Form $x^2 + ny^2$ and the Geometry of (Convenient) Numbers*, preprint.

[22] P.R. Halmos, *Note on almost-universal forms*. Bull. Amer. Math. Soc. 44 (1938), 141–144.

[23] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*. Sixth edition. Revised by D. R. Heath-Brown and J. H. Silverman. Oxford, 2008.

[24] F. Halter-Koch, *Representation of prime powers in arithmetical progressions by binary quadratic forms*. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[25] C. Hermite, *Sur la théorie des formes quadratiques, II.* J. Reine Angew. Math. 47 (1854), 343–368.

[26] J. Hicks and K. Thompson, *GoNIII: More universal quaternary forms*, Integers (accepted).

[27] A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*. Berlin, 1919.

[28] M.I. Icaza. *Hermite constant and extreme forms for algebraic number fields*. J. London Math. Soc. (2), 55(1):11–22, 1997.

[29] K. Ireland and M. Rosen, *A classical introduction to modern number theory*. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[30] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives quaternaires*. Math. Ann. 5 (1872), 581–583.

[31] T.Y. Lam, *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[32] J.L. Lagrange, *Démonstration d'un Théorème D'Arithmétique*, Nouv. Mém. Acad. Roy. Sc. de Berlin, année 1770, Berlin, 1772, 123–133, Oeuvres, 3, 1869, 189–201.

[33] J. Liouville, *Sur Les Deux Formes* $x^2 + y^2 + z^2 + t^2$, $x^2 + 2y^2 + 3z^2 + 6t^2$. Jour. de Math., (1) 10, (1845), 169–170.

[34] J. Liouville, *Sur La Représentation Des Nombres Par La Forme Quadratique* $x^2 + ay^2 + bz^2 + abt^2$. Jour. de Math., (2) 1, (1856), 230.

[35] Mimura, Y., `http://www.kobepharma-u.ac.jp/~math/notes/uqf.html`

[36] H. Minkowski, *Geometrie der Zahlen*, Leipzig and Berlin, 1910.

[37] L.J. Mordell, *The representation of numbers by some quaternary quadratic forms*. Acta Arith. 12 (1966/1967), 47–54.

[38] O.T. O'Meara. *On the finite generation of linear groups over Hasse domains.* Journal für die reine und angewandte Mathematik 217 (1965): 79-108.

[39] Ramanujan, *On the expression of a number in the form* $ax^2 + by^2 + cz^2 + du^2$, Proceedings of the Cambridge Philosophical Society 19 (1917), 11–21.

[40] P. Samuel, *Théorie algébrique des nombres*. Hermann,

[41] W. A. Stein et al., *Sage Mathematics Software (Version 4.7.1)*, The Sage Development Team, 2011, `http://www.sagemath.org`

[42] P.J. Weinberger, *Exponents of the class groups of complex quadratic fields*. Acta Arith. 22 (1973), 117-124.

Appendix A

Appendix

Table A.1: Representatives for 2779 $SL_2(\mathbb{Z})$-equivalence Classes of Regular Binary Forms

$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$
3	$\langle 1, 1, 1\rangle$	4	$\langle 1, 0, 1\rangle$	7	$\langle 1, 1, 2\rangle$	8	$\langle 1, 0, 2\rangle$
11	$\langle 1, 1, 3\rangle$	12	$\langle 1, 0, 3\rangle$	15	$\langle 1, 1, 4\rangle$	15	$\langle 2, 1, 2\rangle$
16	$\langle 1, 0, 4\rangle$	19	$\langle 1, 1, 5\rangle$	20	$\langle 1, 0, 5\rangle$	20	$\langle 2, 2, 3\rangle$
24	$\langle 1, 0, 6\rangle$	24	$\langle 2, 0, 3\rangle$	27	$\langle 1, 1, 7\rangle$	28	$\langle 1, 0, 7\rangle$
32	$\langle 1, 0, 8\rangle$	32	$\langle 3, 2, 3\rangle$	35	$\langle 1, 1, 9\rangle$	35	$\langle 3, 1, 3\rangle$
36	$\langle 1, 0, 9\rangle$	36	$\langle 2, 2, 5\rangle$	39	$\langle 2, \pm 1, 5\rangle$	40	$\langle 1, 0, 10\rangle$
40	$\langle 2, 0, 5\rangle$	43	$\langle 1, 1, 11\rangle$	48	$\langle 1, 0, 12\rangle$	48	$\langle 3, 0, 4\rangle$
51	$\langle 1, 1, 13\rangle$	51	$\langle 3, 3, 5\rangle$	52	$\langle 1, 0, 13\rangle$	52	$\langle 2, 2, 7\rangle$
55	$\langle 2, \pm 1, 7\rangle$	56	$\langle 3, \pm 2, 5\rangle$	60	$\langle 1, 0, 15\rangle$	60	$\langle 3, 0, 5\rangle$
63	$\langle 2, \pm 1, 8\rangle$	64	$\langle 1, 0, 16\rangle$	64	$\langle 4, 4, 5\rangle$	67	$\langle 1, 1, 17\rangle$
68	$\langle 3, \pm 2, 6\rangle$	72	$\langle 1, 0, 18\rangle$	72	$\langle 2, 0, 9\rangle$	75	$\langle 1, 1, 19\rangle$
75	$\langle 3, 3, 7\rangle$	80	$\langle 3, \pm 2, 7\rangle$	84	$\langle 1, 0, 21\rangle$	84	$\langle 2, 2, 11\rangle$
84	$\langle 3, 0, 7\rangle$	84	$\langle 5, 4, 5\rangle$	88	$\langle 1, 0, 22\rangle$	88	$\langle 2, 0, 11\rangle$
91	$\langle 1, 1, 23\rangle$	91	$\langle 5, 3, 5\rangle$	96	$\langle 1, 0, 24\rangle$	96	$\langle 3, 0, 8\rangle$
96	$\langle 4, 4, 7\rangle$	96	$\langle 5, 2, 5\rangle$	99	$\langle 1, 1, 25\rangle$	99	$\langle 5, 1, 5\rangle$
100	$\langle 1, 0, 25\rangle$	100	$\langle 2, 2, 13\rangle$	112	$\langle 1, 0, 28\rangle$	112	$\langle 4, 0, 7\rangle$
115	$\langle 1, 1, 29\rangle$	115	$\langle 5, 5, 7\rangle$	120	$\langle 1, 0, 30\rangle$	120	$\langle 2, 0, 15\rangle$
120	$\langle 3, 0, 10\rangle$	120	$\langle 5, 0, 6\rangle$	123	$\langle 1, 1, 31\rangle$	123	$\langle 3, 3, 11\rangle$
128	$\langle 3, \pm 2, 11\rangle$	132	$\langle 1, 0, 33\rangle$	132	$\langle 2, 2, 17\rangle$	132	$\langle 3, 0, 11\rangle$
132	$\langle 6, 6, 7\rangle$	136	$\langle 5, \pm 2, 7\rangle$	144	$\langle 5, \pm 4, 8\rangle$	147	$\langle 1, 1, 37\rangle$
147	$\langle 3, 3, 13\rangle$	148	$\langle 1, 0, 37\rangle$	148	$\langle 2, 2, 19\rangle$	155	$\langle 3, \pm 1, 13\rangle$
156	$\langle 5, \pm 2, 8\rangle$	160	$\langle 1, 0, 40\rangle$	160	$\langle 4, 4, 11\rangle$	160	$\langle 5, 0, 8\rangle$
160	$\langle 7, 6, 7\rangle$	163	$\langle 1, 1, 41\rangle$	168	$\langle 1, 0, 42\rangle$	168	$\langle 2, 0, 21\rangle$
168	$\langle 3, 0, 14\rangle$	168	$\langle 6, 0, 7\rangle$	171	$\langle 5, \pm 3, 9\rangle$	180	$\langle 1, 0, 45\rangle$
180	$\langle 2, 2, 23\rangle$	180	$\langle 5, 0, 9\rangle$	180	$\langle 7, 4, 7\rangle$	184	$\langle 5, \pm 4, 10\rangle$
187	$\langle 1, 1, 47\rangle$	187	$\langle 7, 3, 7\rangle$	192	$\langle 1, 0, 48\rangle$	192	$\langle 3, 0, 16\rangle$
192	$\langle 4, 4, 13\rangle$	192	$\langle 7, 2, 7\rangle$	195	$\langle 1, 1, 49\rangle$	195	$\langle 3, 3, 17\rangle$
195	$\langle 5, 5, 11\rangle$	195	$\langle 7, 1, 7\rangle$	196	$\langle 5, \pm 2, 10\rangle$	203	$\langle 3, \pm 1, 17\rangle$
208	$\langle 7, \pm 4, 8\rangle$	219	$\langle 5, \pm 1, 11\rangle$	220	$\langle 7, \pm 2, 8\rangle$	224	$\langle 3, \pm 2, 19\rangle$
224	$\langle 5, \pm 4, 12\rangle$	228	$\langle 1, 0, 57\rangle$	228	$\langle 2, 2, 29\rangle$	228	$\langle 3, 0, 19\rangle$
228	$\langle 6, 6, 11\rangle$	232	$\langle 1, 0, 58\rangle$	232	$\langle 2, 0, 29\rangle$	235	$\langle 1, 1, 59\rangle$
235	$\langle 5, 5, 13\rangle$	240	$\langle 1, 0, 60\rangle$	240	$\langle 3, 0, 20\rangle$	240	$\langle 4, 0, 15\rangle$
240	$\langle 5, 0, 12\rangle$	252	$\langle 8, \pm 6, 9\rangle$	256	$\langle 5, \pm 2, 13\rangle$	259	$\langle 5, \pm 1, 13\rangle$
260	$\langle 3, \pm 2, 22\rangle$	260	$\langle 6, \pm 2, 11\rangle$	264	$\langle 5, \pm 4, 14\rangle$	264	$\langle 7, \pm 4, 10\rangle$
267	$\langle 1, 1, 67\rangle$	267	$\langle 3, 3, 23\rangle$	275	$\langle 3, \pm 1, 23\rangle$	276	$\langle 5, \pm 2, 14\rangle$
276	$\langle 7, \pm 2, 10\rangle$	280	$\langle 1, 0, 70\rangle$	280	$\langle 2, 0, 35\rangle$	280	$\langle 5, 0, 14\rangle$

$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$
280	⟨7, 0, 10⟩	288	⟨1, 0, 72⟩	288	⟨4, 4, 19⟩	288	⟨8, 0, 9⟩
288	⟨8, 8, 11⟩	291	⟨5, ±3, 15⟩	292	⟨7, ±4, 11⟩	308	⟨3, ±2, 26⟩
308	⟨6, ±2, 13⟩	312	⟨1, 0, 78⟩	312	⟨2, 0, 39⟩	312	⟨3, 0, 26⟩
312	⟨6, 0, 13⟩	315	⟨1, 1, 79⟩	315	⟨5, 5, 17⟩	315	⟨7, 7, 13⟩
315	⟨9, 9, 11⟩	320	⟨3, ±2, 27⟩	320	⟨7, ±4, 12⟩	323	⟨3, ±1, 27⟩
328	⟨7, ±6, 13⟩	336	⟨5, ±2, 17⟩	336	⟨8, ±4, 11⟩	340	⟨1, 0, 85⟩
340	⟨2, 2, 43⟩	340	⟨5, 0, 17⟩	340	⟨10, 10, 11⟩	352	⟨1, 0, 88⟩
352	⟨4, 4, 23⟩	352	⟨8, 0, 11⟩	352	⟨8, 8, 13⟩	355	⟨7, ±3, 13⟩
360	⟨7, ±2, 13⟩	360	⟨9, ±6, 11⟩	363	⟨7, ±1, 13⟩	372	⟨1, 0, 93⟩
372	⟨2, 2, 47⟩	372	⟨3, 0, 31⟩	372	⟨6, 6, 17⟩	384	⟨5, ±4, 20⟩
384	⟨7, ±6, 15⟩	387	⟨9, ±3, 11⟩	388	⟨7, ±2, 14⟩	400	⟨8, ±4, 13⟩
403	⟨1, 1, 101⟩	403	⟨11, 9, 11⟩	408	⟨1, 0, 102⟩	408	⟨2, 0, 51⟩
408	⟨3, 0, 34⟩	408	⟨6, 0, 17⟩	420	⟨1, 0, 105⟩	420	⟨2, 2, 53⟩
420	⟨3, 0, 35⟩	420	⟨5, 0, 21⟩	420	⟨6, 6, 19⟩	420	⟨7, 0, 15⟩
420	⟨10, 10, 13⟩	420	⟨11, 8, 11⟩	427	⟨1, 1, 107⟩	427	⟨7, 7, 17⟩
435	⟨1, 1, 109⟩	435	⟨3, 3, 37⟩	435	⟨5, 5, 23⟩	435	⟨11, 7, 11⟩
448	⟨1, 0, 112⟩	448	⟨4, 4, 29⟩	448	⟨7, 0, 16⟩	448	⟨11, 6, 11⟩
456	⟨5, ±2, 23⟩	456	⟨10, ±8, 13⟩	468	⟨7, ±6, 18⟩	468	⟨9, ±6, 14⟩
475	⟨7, ±1, 17⟩	480	⟨1, 0, 120⟩	480	⟨3, 0, 40⟩	480	⟨4, 4, 31⟩
480	⟨5, 0, 24⟩	480	⟨8, 0, 15⟩	480	⟨8, 8, 17⟩	480	⟨11, 2, 11⟩
480	⟨12, 12, 13⟩	483	⟨1, 1, 121⟩	483	⟨3, 3, 41⟩	483	⟨7, 7, 19⟩
483	⟨11, 1, 11⟩	504	⟨5, ±4, 26⟩	504	⟨10, ±4, 13⟩	507	⟨7, ±5, 19⟩
520	⟨1, 0, 130⟩	520	⟨2, 0, 65⟩	520	⟨5, 0, 26⟩	520	⟨10, 0, 13⟩
528	⟨7, ±2, 19⟩	528	⟨8, ±4, 17⟩	532	⟨1, 0, 133⟩	532	⟨2, 2, 67⟩
532	⟨7, 0, 19⟩	532	⟨13, 12, 13⟩	544	⟨5, ±4, 28⟩	544	⟨7, ±4, 20⟩
552	⟨7, ±6, 21⟩	552	⟨11, ±8, 14⟩	555	⟨1, 1, 139⟩	555	⟨3, 3, 47⟩
555	⟨5, 5, 29⟩	555	⟨13, 11, 13⟩	564	⟨5, ±4, 29⟩	564	⟨10, ±6, 15⟩
568	⟨11, ±2, 13⟩	576	⟨5, ±2, 29⟩	576	⟨9, ±6, 17⟩	580	⟨7, ±6, 22⟩
580	⟨11, ±6, 14⟩	592	⟨8, ±4, 19⟩	595	⟨1, 1, 149⟩	595	⟨5, 5, 31⟩
595	⟨7, 7, 23⟩	595	⟨13, 9, 13⟩	600	⟨7, ±4, 22⟩	600	⟨11, ±4, 14⟩
603	⟨9, ±3, 17⟩	612	⟨7, ±2, 22⟩	612	⟨11, ±2, 14⟩	616	⟨5, ±2, 31⟩
616	⟨10, ±8, 17⟩	624	⟨5, ±4, 32⟩	624	⟨11, ±6, 15⟩	627	⟨1, 1, 157⟩
627	⟨3, 3, 53⟩	627	⟨11, 11, 17⟩	627	⟨13, 7, 13⟩	640	⟨7, ±2, 23⟩
640	⟨11, ±8, 16⟩	651	⟨5, ±3, 33⟩	651	⟨11, ±3, 15⟩	660	⟨1, 0, 165⟩
660	⟨2, 2, 83⟩	660	⟨3, 0, 55⟩	660	⟨5, 0, 33⟩	660	⟨6, 6, 29⟩
660	⟨10, 10, 19⟩	660	⟨11, 0, 15⟩	660	⟨13, 4, 13⟩	667	⟨11, ±9, 17⟩
672	⟨1, 0, 168⟩	672	⟨3, 0, 56⟩	672	⟨4, 4, 43⟩	672	⟨7, 0, 24⟩
672	⟨8, 0, 21⟩	672	⟨8, 8, 23⟩	672	⟨12, 12, 17⟩	672	⟨13, 2, 13⟩
708	⟨1, 0, 177⟩	708	⟨2, 2, 89⟩	708	⟨3, 0, 59⟩	708	⟨6, 6, 31⟩
715	⟨1, 1, 179⟩	715	⟨5, 5, 37⟩	715	⟨11, 11, 19⟩	715	⟨13, 13, 17⟩
720	⟨7, ±6, 27⟩	720	⟨8, ±4, 23⟩	723	⟨11, ±5, 17⟩	736	⟨5, ±2, 37⟩
736	⟨11, ±10, 19⟩	760	⟨1, 0, 190⟩	760	⟨2, 0, 95⟩	760	⟨5, 0, 38⟩
760	⟨10, 0, 19⟩	763	⟨13, ±11, 17⟩	768	⟨7, ±4, 28⟩	768	⟨13, ±8, 16⟩
772	⟨11, ±8, 19⟩	792	⟨9, ±6, 23⟩	792	⟨13, ±12, 18⟩	795	⟨1, 1, 199⟩
795	⟨3, 3, 67⟩	795	⟨5, 5, 41⟩	795	⟨15, 15, 17⟩	819	⟨5, ±1, 41⟩
819	⟨9, ±3, 23⟩	820	⟨11, ±4, 19⟩	820	⟨13, ±8, 17⟩	832	⟨7, ±6, 31⟩
832	⟨11, ±2, 19⟩	840	⟨1, 0, 210⟩	840	⟨2, 0, 105⟩	840	⟨3, 0, 70⟩
840	⟨5, 0, 42⟩	840	⟨6, 0, 35⟩	840	⟨7, 0, 30⟩	840	⟨10, 0, 21⟩
840	⟨14, 0, 15⟩	852	⟨7, ±4, 31⟩	852	⟨14, ±10, 17⟩	868	⟨11, ±10, 22⟩
868	⟨13, ±4, 17⟩	880	⟨7, ±4, 32⟩	880	⟨13, ±2, 17⟩	900	⟨9, ±6, 26⟩
900	⟨13, ±6, 18⟩	912	⟨8, ±4, 29⟩	912	⟨11, ±10, 23⟩	915	⟨7, ±3, 33⟩
915	⟨11, ±3, 21⟩	928	⟨1, 0, 232⟩	928	⟨4, 4, 59⟩	928	⟨8, 0, 29⟩
928	⟨8, 8, 31⟩	952	⟨11, ±4, 22⟩	952	⟨13, ±6, 19⟩	955	⟨7, ±5, 35⟩
960	⟨1, 0, 240⟩	960	⟨3, 0, 80⟩	960	⟨4, 4, 61⟩	960	⟨5, 0, 48⟩
960	⟨12, 12, 23⟩	960	⟨15, 0, 16⟩	960	⟨16, 16, 19⟩	960	⟨17, 14, 17⟩
987	⟨11, ±5, 23⟩	987	⟨13, ±1, 19⟩	1003	⟨11, ±3, 23⟩	1008	⟨9, ±6, 29⟩
1008	⟨11, ±2, 23⟩	1012	⟨1, 0, 253⟩	1012	⟨2, 2, 127⟩	1012	⟨11, 0, 23⟩
1012	⟨17, 12, 17⟩	1027	⟨7, ±3, 37⟩	1032	⟨7, ±2, 37⟩	1032	⟨14, ±12, 21⟩
1035	⟨7, ±1, 37⟩	1035	⟨9, ±3, 29⟩	1056	⟨5, ±2, 53⟩	1056	⟨7, ±6, 39⟩
1056	⟨13, ±6, 21⟩	1056	⟨15, ±12, 20⟩	1060	⟨7, ±2, 38⟩	1060	⟨14, ±2, 19⟩
1092	⟨1, 0, 273⟩	1092	⟨2, 2, 137⟩	1092	⟨3, 0, 91⟩	1092	⟨6, 6, 47⟩
1092	⟨7, 0, 39⟩	1092	⟨13, 0, 21⟩	1092	⟨14, 14, 23⟩	1092	⟨17, 8, 17⟩
1120	⟨1, 0, 280⟩	1120	⟨4, 4, 71⟩	1120	⟨5, 0, 56⟩	1120	⟨7, 0, 40⟩
1120	⟨8, 0, 35⟩	1120	⟨8, 8, 37⟩	1120	⟨17, 6, 17⟩	1120	⟨19, 18, 19⟩

|Δ|	⟨A, B, C⟩	|Δ|	⟨A, B, C⟩	|Δ|	⟨A, B, C⟩	|Δ|	⟨A, B, C⟩
1128	⟨11, ±4, 26⟩	1128	⟨13, ±4, 22⟩	1131	⟨5, ±3, 57⟩	1131	⟨15, ±3, 19⟩
1140	⟨7, ±6, 42⟩	1140	⟨11, ±2, 26⟩	1140	⟨13, ±2, 22⟩	1140	⟨14, ±6, 21⟩
1152	⟨11, ±6, 27⟩	1152	⟨16, ±8, 19⟩	1155	⟨1, 1, 289⟩	1155	⟨3, 3, 97⟩
1155	⟨5, 5, 59⟩	1155	⟨7, 7, 43⟩	1155	⟨11, 11, 29⟩	1155	⟨15, 15, 23⟩
1155	⟨17, 1, 17⟩	1155	⟨19, 17, 19⟩	1204	⟨5, ±4, 61⟩	1204	⟨10, ±6, 31⟩
1227	⟨11, ±7, 29⟩	1240	⟨11, ±6, 29⟩	1240	⟨17, ±16, 22⟩	1243	⟨17, ±7, 19⟩
1248	⟨1, 0, 312⟩	1248	⟨3, 0, 104⟩	1248	⟨4, 4, 79⟩	1248	⟨8, 0, 39⟩
1248	⟨8, 8, 41⟩	1248	⟨12, 12, 29⟩	1248	⟨13, 0, 24⟩	1248	⟨19, 14, 19⟩
1275	⟨11, ±1, 29⟩	1275	⟨13, ±5, 25⟩	1288	⟨13, ±8, 26⟩	1288	⟨17, ±2, 19⟩
1312	⟨7, ±2, 47⟩	1312	⟨13, ±12, 28⟩	1320	⟨1, 0, 330⟩	1320	⟨2, 0, 165⟩
1320	⟨3, 0, 110⟩	1320	⟨5, 0, 66⟩	1320	⟨6, 0, 55⟩	1320	⟨10, 0, 33⟩
1320	⟨11, 0, 30⟩	1320	⟨15, 0, 22⟩	1332	⟨9, ±6, 38⟩	1332	⟨18, ±6, 19⟩
1344	⟨5, ±4, 68⟩	1344	⟨11, ±8, 32⟩	1344	⟨15, ±6, 23⟩	1344	⟨17, ±4, 20⟩
1360	⟨8, ±4, 43⟩	1360	⟨11, ±2, 31⟩	1380	⟨1, 0, 345⟩	1380	⟨2, 2, 173⟩
1380	⟨3, 0, 115⟩	1380	⟨5, 0, 69⟩	1380	⟨6, 6, 59⟩	1380	⟨10, 10, 37⟩
1380	⟨15, 0, 23⟩	1380	⟨19, 8, 19⟩	1387	⟨13, ±11, 29⟩	1395	⟨13, ±3, 27⟩
1395	⟨17, ±13, 23⟩	1408	⟨13, ±10, 29⟩	1408	⟨16, ±8, 23⟩	1411	⟨5, ±3, 71⟩
1428	⟨1, 0, 357⟩	1428	⟨2, 2, 179⟩	1428	⟨3, 0, 119⟩	1428	⟨6, 6, 61⟩
1428	⟨7, 0, 51⟩	1428	⟨14, 14, 29⟩	1428	⟨17, 0, 21⟩	1428	⟨19, 4, 19⟩
1435	⟨1, 1, 359⟩	1435	⟨5, 5, 73⟩	1435	⟨7, 7, 53⟩	1435	⟨19, 3, 19⟩
1440	⟨7, ±4, 52⟩	1440	⟨9, ±6, 41⟩	1440	⟨11, ±10, 35⟩	1440	⟨13, ±4, 28⟩
1443	⟨11, ±3, 33⟩	1443	⟨17, ±11, 23⟩	1467	⟨9, ±3, 41⟩	1488	⟨8, ±4, 47⟩
1488	⟨17, ±12, 24⟩	1507	⟨13, ±1, 29⟩	1540	⟨1, 0, 385⟩	1540	⟨2, 2, 193⟩
1540	⟨5, 0, 77⟩	1540	⟨7, 0, 55⟩	1540	⟨10, 10, 41⟩	1540	⟨11, 0, 35⟩
1540	⟨14, 14, 31⟩	1540	⟨22, 22, 23⟩	1555	⟨17, ±3, 23⟩	1560	⟨7, ±6, 57⟩
1560	⟨14, ±8, 29⟩	1560	⟨17, ±2, 23⟩	1560	⟨19, ±6, 21⟩	1600	⟨13, ±8, 32⟩
1600	⟨17, ±10, 25⟩	1632	⟨1, 0, 408⟩	1632	⟨3, 0, 136⟩	1632	⟨4, 4, 103⟩
1632	⟨8, 0, 51⟩	1632	⟨8, 8, 53⟩	1632	⟨12, 12, 37⟩	1632	⟨17, 0, 24⟩
1632	⟨23, 22, 23⟩	1635	⟨11, ±9, 39⟩	1635	⟨13, ±9, 33⟩	1659	⟨5, ±1, 83⟩
1659	⟨15, ±9, 29⟩	1672	⟨7, ±6, 61⟩	1672	⟨14, ±8, 31⟩	1680	⟨8, ±4, 53⟩
1680	⟨11, ±6, 39⟩	1680	⟨13, ±6, 33⟩	1680	⟨19, ±12, 24⟩	1683	⟨7, ±5, 61⟩
1683	⟨9, ±3, 47⟩	1716	⟨5, ±2, 86⟩	1716	⟨10, ±2, 43⟩	1716	⟨15, ±12, 31⟩
1716	⟨17, ±16, 29⟩	1752	⟨13, ±4, 34⟩	1752	⟨17, ±4, 26⟩	1768	⟨11, ±6, 41⟩
1768	⟨22, ±16, 23⟩	1771	⟨5, ±3, 89⟩	1771	⟨13, ±7, 35⟩	1780	⟨13, ±12, 37⟩
1780	⟨19, ±14, 26⟩	1792	⟨11, ±10, 43⟩	1792	⟨16, ±8, 29⟩	1824	⟨5, ±4, 92⟩
1824	⟨13, ±10, 37⟩	1824	⟨15, ±6, 31⟩	1824	⟨20, ±4, 23⟩	1827	⟨17, ±3, 27⟩
1827	⟨19, ±15, 27⟩	1848	⟨1, 0, 462⟩	1848	⟨2, 0, 231⟩	1848	⟨3, 0, 154⟩
1848	⟨6, 0, 77⟩	1848	⟨7, 0, 66⟩	1848	⟨11, 0, 42⟩	1848	⟨14, 0, 33⟩
1848	⟨21, 0, 22⟩	1860	⟨7, ±4, 67⟩	1860	⟨13, ±8, 37⟩	1860	⟨14, ±10, 35⟩
1860	⟨21, ±18, 26⟩	1920	⟨11, ±4, 44⟩	1920	⟨13, ±2, 37⟩	1920	⟨16, ±8, 31⟩
1920	⟨17, ±16, 32⟩	1947	⟨13, ±9, 39⟩	1947	⟨17, ±5, 29⟩	1992	⟨13, ±6, 39⟩
1992	⟨23, ±20, 26⟩	1995	⟨1, 1, 499⟩	1995	⟨3, 3, 167⟩	1995	⟨5, 5, 101⟩
1995	⟨7, 7, 73⟩	1995	⟨15, 15, 37⟩	1995	⟨19, 19, 31⟩	1995	⟨21, 21, 29⟩
1995	⟨23, 11, 23⟩	2016	⟨5, ±2, 101⟩	2016	⟨13, ±8, 40⟩	2016	⟨19, ±6, 27⟩
2016	⟨20, ±12, 27⟩	2020	⟨11, ±2, 46⟩	2020	⟨22, ±2, 23⟩	2035	⟨7, ±3, 73⟩
2035	⟨19, ±13, 29⟩	2040	⟨7, ±2, 73⟩	2040	⟨13, ±12, 42⟩	2040	⟨14, ±12, 39⟩
2040	⟨21, ±12, 26⟩	2067	⟨11, ±1, 47⟩	2067	⟨19, ±17, 31⟩	2080	⟨1, 0, 520⟩
2080	⟨4, 4, 131⟩	2080	⟨5, 0, 104⟩	2080	⟨8, 0, 65⟩	2080	⟨8, 8, 67⟩
2080	⟨13, 0, 40⟩	2080	⟨20, 20, 31⟩	2080	⟨23, 6, 23⟩	2088	⟨9, ±6, 59⟩
2088	⟨18, ±12, 31⟩	2100	⟨11, ±10, 50⟩	2100	⟨17, ±12, 33⟩	2100	⟨19, ±16, 31⟩
2100	⟨22, ±10, 25⟩	2112	⟨7, ±4, 76⟩	2112	⟨17, ±8, 32⟩	2112	⟨19, ±4, 28⟩
2112	⟨21, ±18, 29⟩	2115	⟨9, ±3, 59⟩	2115	⟨13, ±11, 43⟩	2128	⟨8, ±4, 67⟩
2128	⟨13, ±2, 41⟩	2139	⟨5, ±1, 107⟩	2139	⟨15, ±9, 37⟩	2163	⟨11, ±9, 51⟩
2163	⟨17, ±9, 33⟩	2208	⟨7, ±2, 79⟩	2208	⟨11, ±6, 51⟩	2208	⟨17, ±6, 33⟩
2208	⟨21, ±12, 28⟩	2212	⟨17, ±10, 34⟩	2212	⟨19, ±12, 31⟩	2244	⟨5, ±4, 113⟩
2244	⟨10, ±6, 57⟩	2244	⟨15, ±6, 38⟩	2244	⟨19, ±6, 30⟩	2272	⟨11, ±4, 52⟩
2272	⟨13, ±4, 44⟩	2275	⟨19, ±9, 31⟩	2275	⟨23, ±5, 25⟩	2280	⟨7, ±4, 82⟩
2280	⟨14, ±4, 41⟩	2280	⟨17, ±10, 35⟩	2280	⟨21, ±18, 31⟩	2340	⟨11, ±6, 54⟩
2340	⟨19, ±4, 31⟩	2340	⟨22, ±6, 27⟩	2340	⟨23, ±12, 27⟩	2368	⟨19, ±8, 32⟩
2368	⟨23, ±22, 31⟩	2392	⟨7, ±4, 86⟩	2392	⟨14, ±4, 43⟩	2400	⟨7, ±6, 87⟩
2400	⟨11, ±8, 56⟩	2400	⟨21, ±6, 29⟩	2400	⟨25, ±20, 28⟩	2436	⟨5, ±2, 122⟩
2436	⟨10, ±2, 61⟩	2436	⟨15, ±12, 43⟩	2436	⟨23, ±18, 30⟩	2451	⟨5, ±3, 123⟩
2451	⟨15, ±3, 41⟩	2464	⟨5, ±4, 124⟩	2464	⟨17, ±16, 40⟩	2464	⟨19, ±14, 35⟩
2464	⟨20, ±4, 31⟩	2475	⟨23, ±3, 27⟩	2475	⟨25, ±15, 27⟩	2496	⟨5, ±2, 125⟩

$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$	$\|\Delta\|$	$\langle A, B, C\rangle$
2496	⟨11, ±10, 59⟩	2496	⟨15, ±12, 44⟩	2496	⟨20, ±12, 33⟩	2520	⟨9, ±6, 71⟩
2520	⟨17, ±8, 38⟩	2520	⟨18, ±12, 37⟩	2520	⟨19, ±8, 34⟩	2580	⟨11, ±4, 59⟩
2580	⟨17, ±2, 38⟩	2580	⟨19, ±2, 34⟩	2580	⟨22, ±18, 33⟩	2632	⟨19, ±16, 38⟩
2632	⟨23, ±6, 29⟩	2640	⟨8, ±4, 83⟩	2640	⟨13, ±8, 52⟩	2640	⟨19, ±18, 39⟩
2640	⟨24, ±12, 29⟩	2667	⟨17, ±11, 41⟩	2667	⟨23, ±1, 29⟩	2688	⟨13, ±4, 52⟩
2688	⟨16, ±8, 43⟩	2688	⟨17, ±10, 41⟩	2688	⟨23, ±16, 32⟩	2715	⟨7, ±1, 97⟩
2715	⟨21, ±15, 35⟩	2755	⟨13, ±1, 53⟩	2755	⟨17, ±13, 43⟩	2760	⟨11, ±10, 65⟩
2760	⟨13, ±10, 55⟩	2760	⟨22, ±12, 33⟩	2760	⟨26, ±16, 29⟩	2772	⟨13, ±6, 54⟩
2772	⟨17, ±4, 41⟩	2772	⟨26, ±6, 27⟩	2772	⟨27, ±24, 31⟩	2788	⟨19, ±10, 38⟩
2788	⟨23, ±8, 31⟩	2832	⟨8, ±4, 89⟩	2832	⟨24, ±12, 31⟩	2880	⟨7, ±2, 103⟩
2880	⟨23, ±8, 32⟩	2880	⟨27, ±24, 32⟩	2880	⟨27, ±12, 28⟩	2907	⟨27, ±21, 31⟩
2907	⟨27, ±15, 29⟩	2968	⟨13, ±10, 59⟩	2968	⟨26, ±16, 31⟩	3003	⟨1, 1, 751⟩
3003	⟨3, 3, 251⟩	3003	⟨7, 7, 109⟩	3003	⟨11, 11, 71⟩	3003	⟨13, 13, 61⟩
3003	⟨21, 21, 41⟩	3003	⟨29, 19, 29⟩	3003	⟨31, 29, 31⟩	3040	⟨1, 0, 760⟩
3040	⟨4, 4, 191⟩	3040	⟨5, 0, 152⟩	3040	⟨8, 0, 95⟩	3040	⟨8, 8, 97⟩
3040	⟨19, 0, 40⟩	3040	⟨20, 20, 43⟩	3040	⟨29, 18, 29⟩	3060	⟨9, ±6, 86⟩
3060	⟨11, ±8, 71⟩	3060	⟨18, ±6, 43⟩	3060	⟨22, ±14, 37⟩	3108	⟨11, ±4, 71⟩
3108	⟨13, ±8, 61⟩	3108	⟨22, ±18, 39⟩	3108	⟨26, ±18, 33⟩	3168	⟨9, ±6, 89⟩
3168	⟨13, ±2, 61⟩	3168	⟨19, ±10, 43⟩	3168	⟨23, ±12, 36⟩	3172	⟨19, ±18, 46⟩
3172	⟨23, ±18, 38⟩	3192	⟨11, ±8, 74⟩	3192	⟨17, ±2, 47⟩	3192	⟨22, ±8, 37⟩
3192	⟨31, ±30, 33⟩	3220	⟨11, ±6, 74⟩	3220	⟨13, ±2, 62⟩	3220	⟨22, ±6, 37⟩
3220	⟨26, ±2, 31⟩	3243	⟨17, ±15, 51⟩	3243	⟨19, ±5, 43⟩	3315	⟨1, 1, 829⟩
3315	⟨3, 3, 277⟩	3315	⟨5, 5, 167⟩	3315	⟨13, 13, 67⟩	3315	⟨15, 15, 59⟩
3315	⟨17, 17, 53⟩	3315	⟨29, 7, 29⟩	3315	⟨31, 23, 31⟩	3355	⟨13, ±5, 65⟩
3355	⟨23, ±7, 37⟩	3360	⟨1, 0, 840⟩	3360	⟨3, 0, 280⟩	3360	⟨4, 4, 211⟩
3360	⟨5, 0, 168⟩	3360	⟨7, 0, 120⟩	3360	⟨8, 0, 105⟩	3360	⟨8, 8, 107⟩
3360	⟨12, 12, 73⟩	3360	⟨15, 0, 56⟩	3360	⟨20, 20, 47⟩	3360	⟨21, 0, 40⟩
3360	⟨24, 0, 35⟩	3360	⟨24, 24, 41⟩	3360	⟨28, 28, 37⟩	3360	⟨29, 2, 29⟩
3360	⟨31, 22, 31⟩	3432	⟨17, ±6, 51⟩	3432	⟨19, ±8, 46⟩	3432	⟨23, ±8, 38⟩
3432	⟨31, ±28, 34⟩	3480	⟨13, ±2, 67⟩	3480	⟨19, ±4, 46⟩	3480	⟨23, ±4, 38⟩
3480	⟨26, ±24, 39⟩	3507	⟨13, ±9, 69⟩	3507	⟨23, ±9, 39⟩	3520	⟨7, ±6, 127⟩
3520	⟨13, ±4, 68⟩	3520	⟨17, ±4, 52⟩	3520	⟨28, ±20, 35⟩	3588	⟨11, ±8, 83⟩
3588	⟨17, ±4, 53⟩	3588	⟨22, ±14, 43⟩	3588	⟨33, ±30, 34⟩	3627	⟨9, ±3, 101⟩
3627	⟨11, ±5, 83⟩	3640	⟨11, ±10, 85⟩	3640	⟨17, ±10, 55⟩	3640	⟨22, ±12, 43⟩
3640	⟨31, ±24, 34⟩	3648	⟨11, ±2, 83⟩	3648	⟨23, ±20, 44⟩	3648	⟨29, ±8, 32⟩
3648	⟨32, ±24, 33⟩	3712	⟨16, ±8, 59⟩	3712	⟨31, ±16, 32⟩	3795	⟨13, ±1, 73⟩
3795	⟨17, ±9, 57⟩	3795	⟨19, ±9, 51⟩	3795	⟨29, ±27, 39⟩	3808	⟨11, ±8, 88⟩
3808	⟨13, ±12, 76⟩	3808	⟨19, ±12, 52⟩	3808	⟨29, ±22, 37⟩	3828	⟨7, ±6, 138⟩
3828	⟨14, ±6, 69⟩	3828	⟨21, ±6, 46⟩	3828	⟨23, ±6, 42⟩	3840	⟨16, ±8, 61⟩
3840	⟨17, ±6, 57⟩	3840	⟨19, ±6, 51⟩	3840	⟨23, ±22, 47⟩	3843	⟨9, ±3, 107⟩
3843	⟨17, ±13, 59⟩	4020	⟨13, ±6, 78⟩	4020	⟨17, ±14, 62⟩	4020	⟨26, ±6, 39⟩
4020	⟨31, ±14, 34⟩	4032	⟨9, ±6, 113⟩	4032	⟨11, ±4, 92⟩	4032	⟨23, ±4, 44⟩
4032	⟨29, ±12, 36⟩	4048	⟨8, ±4, 127⟩	4048	⟨17, ±10, 61⟩	4123	⟨17, ±5, 61⟩
4123	⟨29, ±13, 37⟩	4128	⟨7, ±4, 148⟩	4128	⟨21, ±18, 53⟩	4128	⟨23, ±14, 47⟩
4128	⟨28, ±4, 37⟩	4180	⟨17, ±6, 62⟩	4180	⟨23, ±12, 47⟩	4180	⟨29, ±24, 41⟩
4180	⟨31, ±6, 34⟩	4260	⟨13, ±2, 82⟩	4260	⟨23, ±8, 47⟩	4260	⟨26, ±2, 41⟩
4260	⟨31, ±24, 39⟩	4323	⟨19, ±3, 57⟩	4323	⟨23, ±1, 47⟩	4368	⟨8, ±4, 137⟩
4368	⟨17, ±16, 68⟩	4368	⟨23, ±18, 51⟩	4368	⟨24, ±12, 47⟩	4420	⟨7, ±2, 158⟩
4420	⟨14, ±2, 79⟩	4420	⟨19, ±8, 59⟩	4420	⟨35, ±30, 38⟩	4440	⟨11, ±2, 101⟩
4440	⟨19, ±14, 61⟩	4440	⟨22, ±20, 55⟩	4440	⟨33, ±24, 38⟩	4452	⟨11, ±6, 102⟩
4452	⟨17, ±6, 66⟩	4452	⟨22, ±6, 51⟩	4452	⟨33, ±6, 34⟩	4480	⟨16, ±8, 71⟩
4480	⟨17, ±12, 68⟩	4480	⟨19, ±2, 59⟩	4480	⟨32, ±16, 37⟩	4488	⟨13, ±6, 87⟩
4488	⟨26, ±20, 47⟩	4488	⟨29, ±6, 39⟩	4488	⟨31, ±10, 37⟩	4512	⟨11, ±8, 104⟩
4512	⟨13, ±8, 88⟩	4512	⟨31, ±18, 39⟩	4512	⟨33, ±30, 41⟩	4515	⟨13, ±3, 87⟩
4515	⟨19, ±11, 61⟩	4515	⟨23, ±19, 53⟩	4515	⟨29, ±3, 39⟩	4680	⟨9, ±6, 131⟩
4680	⟨18, ±12, 67⟩	4680	⟨23, ±14, 53⟩	4680	⟨31, ±30, 45⟩	4740	⟨11, ±10, 110⟩
4740	⟨22, ±10, 55⟩	4740	⟨29, ±4, 41⟩	4740	⟨33, ±12, 37⟩	4788	⟨9, ±6, 134⟩
4788	⟨13, ±10, 94⟩	4788	⟨18, ±6, 67⟩	4788	⟨26, ±10, 47⟩	4960	⟨11, ±10, 115⟩
4960	⟨17, ±2, 73⟩	4960	⟨23, ±10, 55⟩	4960	⟨29, ±12, 44⟩	4992	⟨16, ±8, 79⟩
4992	⟨19, ±10, 67⟩	4992	⟨29, ±24, 48⟩	4992	⟨32, ±16, 41⟩	5083	⟨19, ±3, 67⟩
5083	⟨31, ±1, 41⟩	5115	⟨7, ±3, 183⟩	5115	⟨17, ±11, 77⟩	5115	⟨21, ±3, 61⟩
5115	⟨35, ±25, 41⟩	5152	⟨13, ±10, 101⟩	5152	⟨17, ±4, 76⟩	5152	⟨19, ±4, 68⟩
5152	⟨31, ±26, 47⟩	5160	⟨13, ±12, 102⟩	5160	⟨17, ±12, 78⟩	5160	⟨26, ±12, 51⟩
5160	⟨34, ±12, 39⟩	5187	⟨11, ±7, 119⟩	5187	⟨17, ±7, 77⟩	5187	⟨29, ±27, 51⟩

$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$
5187	⟨33, ±15, 41⟩	5208	⟨19, ±6, 69⟩	5208	⟨23, ±6, 57⟩	5208	⟨37, ±34, 43⟩
5208	⟨38, ±32, 41⟩	5280	⟨1, 0, 1320⟩	5280	⟨3, 0, 440⟩	5280	⟨4, 4, 331⟩
5280	⟨5, 0, 264⟩	5280	⟨8, 0, 165⟩	5280	⟨8, 8, 167⟩	5280	⟨11, 0, 120⟩
5280	⟨12, 12, 113⟩	5280	⟨15, 0, 88⟩	5280	⟨20, 20, 71⟩	5280	⟨24, 0, 55⟩
5280	⟨24, 24, 61⟩	5280	⟨33, 0, 40⟩	5280	⟨37, 14, 37⟩	5280	⟨40, 40, 43⟩
5280	⟨41, 38, 41⟩	5355	⟨9, ±3, 149⟩	5355	⟨13, ±1, 103⟩	5355	⟨23, ±21, 63⟩
5355	⟨31, ±15, 45⟩	5412	⟨13, ±10, 106⟩	5412	⟨23, ±4, 59⟩	5412	⟨26, ±10, 53⟩
5412	⟨39, ±36, 43⟩	5440	⟨11, ±4, 124⟩	5440	⟨31, ±4, 44⟩	5440	⟨32, ±24, 47⟩
5440	⟨32, ±8, 43⟩	5460	⟨1, 0, 1365⟩	5460	⟨2, 2, 683⟩	5460	⟨3, 0, 455⟩
5460	⟨5, 0, 273⟩	5460	⟨6, 6, 229⟩	5460	⟨7, 0, 195⟩	5460	⟨10, 10, 139⟩
5460	⟨13, 0, 105⟩	5460	⟨14, 14, 101⟩	5460	⟨15, 0, 91⟩	5460	⟨21, 0, 65⟩
5460	⟨26, 26, 59⟩	5460	⟨30, 30, 53⟩	5460	⟨35, 0, 39⟩	5460	⟨37, 4, 37⟩
5460	⟨42, 42, 43⟩	5467	⟨19, ±9, 73⟩	5467	⟨31, ±19, 47⟩	5520	⟨8, ±4, 173⟩
5520	⟨19, ±16, 76⟩	5520	⟨24, ±12, 59⟩	5520	⟨37, ±20, 40⟩	5712	⟨8, ±4, 179⟩
5712	⟨19, ±8, 76⟩	5712	⟨24, ±12, 61⟩	5712	⟨29, ±28, 56⟩	5952	⟨17, ±10, 89⟩
5952	⟨29, ±14, 53⟩	5952	⟨32, ±24, 51⟩	5952	⟨32, ±8, 47⟩	6160	⟨8, ±4, 193⟩
6160	⟨23, ±2, 67⟩	6160	⟨31, ±28, 56⟩	6160	⟨40, ±20, 41⟩	6195	⟨11, ±3, 141⟩
6195	⟨31, ±25, 55⟩	6195	⟨33, ±3, 47⟩	6195	⟨37, ±13, 43⟩	6240	⟨7, ±2, 223⟩
6240	⟨17, ±4, 92⟩	6240	⟨19, ±12, 84⟩	6240	⟨21, ±12, 76⟩	6240	⟨23, ±4, 68⟩
6240	⟨28, ±12, 57⟩	6240	⟨29, ±16, 56⟩	6240	⟨35, ±30, 51⟩	6307	⟨19, ±1, 83⟩
6307	⟨23, ±15, 71⟩	6420	⟨11, ±2, 146⟩	6420	⟨22, ±2, 73⟩	6420	⟨31, ±20, 55⟩
6420	⟨33, ±24, 53⟩	6435	⟨9, ±3, 179⟩	6435	⟨17, ±5, 95⟩	6435	⟨19, ±5, 85⟩
6435	⟨37, ±15, 45⟩	6528	⟨16, ±8, 103⟩	6528	⟨23, ±2, 71⟩	6528	⟨32, ±16, 53⟩
6528	⟨37, ±24, 48⟩	6580	⟨11, ±8, 151⟩	6580	⟨17, ±4, 97⟩	6580	⟨22, ±14, 77⟩
6580	⟨34, ±30, 55⟩	6612	⟨17, ±16, 101⟩	6612	⟨23, ±14, 74⟩	6612	⟨34, ±18, 51⟩
6612	⟨37, ±14, 46⟩	6688	⟨7, ±2, 239⟩	6688	⟨28, ±12, 61⟩	6688	⟨31, ±16, 56⟩
6688	⟨37, ±34, 53⟩	6708	⟨23, ±10, 74⟩	6708	⟨29, ±22, 62⟩	6708	⟨31, ±22, 58⟩
6708	⟨37, ±10, 46⟩	6720	⟨11, ±10, 155⟩	6720	⟨13, ±12, 132⟩	6720	⟨19, ±14, 91⟩
6720	⟨31, ±10, 55⟩	6720	⟨32, ±24, 57⟩	6720	⟨32, ±8, 53⟩	6720	⟨33, ±12, 52⟩
6720	⟨39, ±12, 44⟩	6820	⟨19, ±18, 94⟩	6820	⟨29, ±16, 61⟩	6820	⟨37, ±32, 53⟩
6820	⟨38, ±18, 47⟩	6840	⟨9, ±6, 191⟩	6840	⟨18, ±12, 97⟩	6840	⟨29, ±2, 59⟩
6840	⟨43, ±30, 45⟩	7008	⟨13, ±8, 136⟩	7008	⟨17, ±8, 104⟩	7008	⟨39, ±18, 47⟩
7008	⟨43, ±42, 51⟩	7035	⟨11, ±7, 161⟩	7035	⟨23, ±7, 77⟩	7035	⟨31, ±23, 61⟩
7035	⟨33, ±15, 55⟩	7072	⟨11, ±10, 163⟩	7072	⟨23, ±14, 79⟩	7072	⟨29, ±2, 61⟩
7072	⟨41, ±12, 44⟩	7140	⟨13, ±6, 138⟩	7140	⟨19, ±2, 94⟩	7140	⟨23, ±6, 78⟩
7140	⟨26, ±6, 69⟩	7140	⟨29, ±20, 65⟩	7140	⟨37, ±36, 57⟩	7140	⟨38, ±2, 47⟩
7140	⟨39, ±6, 46⟩	7315	⟨13, ±11, 143⟩	7315	⟨29, ±15, 65⟩	7315	⟨31, ±1, 59⟩
7315	⟨37, ±23, 53⟩	7392	⟨1, 0, 1848⟩	7392	⟨3, 0, 616⟩	7392	⟨4, 4, 463⟩
7392	⟨7, 0, 264⟩	7392	⟨8, 0, 231⟩	7392	⟨8, 8, 233⟩	7392	⟨11, 0, 168⟩
7392	⟨12, 12, 157⟩	7392	⟨21, 0, 88⟩	7392	⟨24, 0, 77⟩	7392	⟨24, 24, 83⟩
7392	⟨28, 28, 73⟩	7392	⟨33, 0, 56⟩	7392	⟨43, 2, 43⟩	7392	⟨44, 44, 53⟩
7392	⟨47, 38, 47⟩	7395	⟨7, ±5, 265⟩	7395	⟨21, ±9, 89⟩	7395	⟨31, ±13, 61⟩
7395	⟨35, ±5, 53⟩	7480	⟨19, ±14, 101⟩	7480	⟨23, ±8, 82⟩	7480	⟨38, ±24, 53⟩
7480	⟨41, ±8, 46⟩	7540	⟨17, ±12, 113⟩	7540	⟨23, ±2, 82⟩	7540	⟨34, ±22, 59⟩
7540	⟨41, ±2, 46⟩	7755	⟨7, ±1, 277⟩	7755	⟨19, ±15, 105⟩	7755	⟨21, ±15, 95⟩
7755	⟨35, ±15, 57⟩	7968	⟨13, ±12, 156⟩	7968	⟨23, ±6, 87⟩	7968	⟨29, ±6, 69⟩
7968	⟨39, ±12, 52⟩	7995	⟨19, ±17, 109⟩	7995	⟨23, ±3, 87⟩	7995	⟨29, ±3, 69⟩
7995	⟨37, ±21, 57⟩	8008	⟨17, ±4, 118⟩	8008	⟨29, ±24, 74⟩	8008	⟨34, ±4, 59⟩
8008	⟨37, ±24, 58⟩	8052	⟨19, ±2, 106⟩	8052	⟨31, ±16, 67⟩	8052	⟨38, ±2, 53⟩
8052	⟨41, ±36, 57⟩	8160	⟨7, ±4, 292⟩	8160	⟨13, ±2, 157⟩	8160	⟨21, ±18, 101⟩
8160	⟨28, ±4, 73⟩	8160	⟨35, ±10, 59⟩	8160	⟨39, ±24, 56⟩	8160	⟨41, ±32, 56⟩
8160	⟨43, ±28, 52⟩	8320	⟨16, ±8, 131⟩	8320	⟨23, ±12, 92⟩	8320	⟨31, ±22, 71⟩
8320	⟨32, ±16, 67⟩	8352	⟨9, ±6, 233⟩	8352	⟨31, ±24, 72⟩	8352	⟨36, ±12, 59⟩
8352	⟨37, ±26, 61⟩	8512	⟨13, ±4, 164⟩	8512	⟨32, ±24, 71⟩	8512	⟨32, ±8, 67⟩
8512	⟨41, ±4, 52⟩	8547	⟨17, ±15, 129⟩	8547	⟨23, ±3, 93⟩	8547	⟨31, ±3, 69⟩
8547	⟨43, ±15, 51⟩	8580	⟨7, ±4, 307⟩	8580	⟨14, ±10, 155⟩	8580	⟨21, ±18, 106⟩
8580	⟨29, ±2, 74⟩	8580	⟨31, ±10, 70⟩	8580	⟨35, ±10, 62⟩	8580	⟨37, ±2, 58⟩
8580	⟨42, ±18, 53⟩	8680	⟨13, ±2, 167⟩	8680	⟨26, ±24, 89⟩	8680	⟨29, ±22, 79⟩
8680	⟨43, ±36, 58⟩	8715	⟨19, ±5, 115⟩	8715	⟨23, ±5, 95⟩	8715	⟨41, ±31, 59⟩
8715	⟨43, ±33, 57⟩	8835	⟨11, ±3, 201⟩	8835	⟨33, ±3, 67⟩	8835	⟨41, ±29, 59⟩
8835	⟨43, ±25, 55⟩	8932	⟨13, ±8, 173⟩	8932	⟨19, ±6, 118⟩	8932	⟨26, ±18, 89⟩
8932	⟨38, ±6, 59⟩	9108	⟨9, ±6, 254⟩	9108	⟨17, ±2, 134⟩	9108	⟨18, ±6, 127⟩
9108	⟨34, ±2, 67⟩	9120	⟨7, ±6, 327⟩	9120	⟨17, ±14, 137⟩	9120	⟨21, ±6, 109⟩
9120	⟨28, ±20, 85⟩	9120	⟨31, ±26, 79⟩	9120	⟨35, ±20, 68⟩	9120	⟨41, ±8, 56⟩

$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$
9120	⟨51, ±48, 56⟩	9240	⟨13, ±4, 178⟩	9240	⟨17, ±12, 138⟩	9240	⟨23, ±12, 102⟩
9240	⟨26, ±4, 89⟩	9240	⟨34, ±12, 69⟩	9240	⟨37, ±26, 67⟩	9240	⟨39, ±30, 65⟩
9240	⟨46, ±12, 51⟩	9568	⟨7, ±6, 343⟩	9568	⟨28, ±20, 89⟩	9568	⟨43, ±8, 56⟩
9568	⟨53, ±48, 56⟩	9867	⟨29, ±15, 87⟩	9867	⟨37, ±7, 67⟩	9867	⟨43, ±25, 61⟩
9867	⟨47, ±35, 59⟩	10080	⟨9, ±6, 281⟩	10080	⟨17, ±16, 152⟩	10080	⟨19, ±16, 136⟩
10080	⟨36, ±12, 71⟩	10080	⟨37, ±24, 72⟩	10080	⟨43, ±38, 67⟩	10080	⟨45, ±30, 61⟩
10080	⟨47, ±42, 63⟩	10528	⟨19, ±6, 139⟩	10528	⟨23, ±12, 116⟩	10528	⟨29, ±12, 92⟩
10528	⟨41, ±38, 73⟩	10560	⟨13, ±10, 205⟩	10560	⟨19, ±2, 139⟩	10560	⟨29, ±24, 96⟩
10560	⟨32, ±24, 87⟩	10560	⟨32, ±8, 83⟩	10560	⟨39, ±36, 76⟩	10560	⟨41, ±10, 65⟩
10560	⟨52, ±36, 57⟩	10920	⟨11, ±6, 249⟩	10920	⟨19, ±10, 145⟩	10920	⟨22, ±16, 127⟩
10920	⟨29, ±10, 95⟩	10920	⟨33, ±6, 83⟩	10920	⟨38, ±28, 77⟩	10920	⟨55, ±50, 61⟩
10920	⟨57, ±48, 58⟩	10948	⟨37, ±2, 74⟩	10948	⟨41, ±32, 73⟩	10948	⟨43, ±24, 67⟩
10948	⟨47, ±12, 59⟩	11040	⟨11, ±2, 251⟩	11040	⟨13, ±6, 213⟩	11040	⟨29, ±26, 101⟩
11040	⟨33, ±24, 88⟩	11040	⟨39, ±6, 71⟩	11040	⟨43, ±22, 67⟩	11040	⟨44, ±20, 65⟩
11040	⟨52, ±20, 55⟩	11067	⟨13, ±3, 213⟩	11067	⟨37, ±25, 79⟩	11067	⟨39, ±3, 71⟩
11067	⟨47, ±5, 59⟩	11328	⟨31, ±24, 96⟩	11328	⟨32, ±24, 93⟩	11328	⟨32, ±8, 89⟩
11328	⟨43, ±14, 67⟩	11715	⟨17, ±7, 173⟩	11715	⟨29, ±1, 101⟩	11715	⟨43, ±29, 73⟩
11715	⟨51, ±27, 61⟩	11872	⟨13, ±6, 229⟩	11872	⟨31, ±30, 103⟩	11872	⟨41, ±10, 73⟩
11872	⟨52, ±20, 59⟩	12160	⟨16, ±8, 191⟩	12160	⟨29, ±22, 109⟩	12160	⟨32, ±16, 97⟩
12160	⟨43, ±40, 80⟩	12180	⟨13, ±12, 237⟩	12180	⟨17, ±14, 182⟩	12180	⟨26, ±14, 119⟩
12180	⟨34, ±14, 91⟩	12180	⟨37, ±20, 85⟩	12180	⟨39, ±12, 79⟩	12180	⟨51, ±48, 71⟩
12180	⟨53, ±40, 65⟩	12768	⟨11, ±6, 291⟩	12768	⟨17, ±4, 188⟩	12768	⟨31, ±2, 103⟩
12768	⟨33, ±6, 97⟩	12768	⟨37, ±16, 88⟩	12768	⟨44, ±28, 77⟩	12768	⟨47, ±4, 68⟩
12768	⟨51, ±30, 67⟩	12915	⟨9, ±3, 359⟩	12915	⟨19, ±9, 171⟩	12915	⟨45, ±15, 73⟩
12915	⟨53, ±21, 63⟩	13195	⟨11, ±7, 301⟩	13195	⟨43, ±7, 77⟩	13195	⟨47, ±23, 73⟩
13195	⟨55, ±15, 61⟩	13440	⟨16, ±8, 211⟩	13440	⟨29, ±4, 116⟩	13440	⟨31, ±18, 111⟩
13440	⟨32, ±16, 107⟩	13440	⟨37, ±18, 93⟩	13440	⟨41, ±34, 89⟩	13440	⟨47, ±40, 80⟩
13440	⟨48, ±24, 73⟩	13728	⟨17, ±12, 204⟩	13728	⟨19, ±16, 184⟩	13728	⟨23, ±16, 152⟩
13728	⟨31, ±6, 111⟩	13728	⟨37, ±6, 93⟩	13728	⟨51, ±12, 68⟩	13728	⟨53, ±30, 69⟩
13728	⟨57, ±54, 73⟩	13860	⟨9, ±6, 386⟩	13860	⟨18, ±6, 193⟩	13860	⟨23, ±20, 155⟩
13860	⟨31, ±20, 115⟩	13860	⟨41, ±30, 90⟩	13860	⟨45, ±30, 82⟩	13860	⟨46, ±26, 79⟩
13860	⟨62, ±42, 63⟩	13920	⟨13, ±4, 268⟩	13920	⟨19, ±8, 184⟩	13920	⟨23, ±8, 152⟩
13920	⟨39, ±30, 95⟩	13920	⟨41, ±26, 89⟩	13920	⟨52, ±4, 67⟩	13920	⟨57, ±30, 65⟩
13920	⟨61, ±54, 69⟩	14280	⟨11, ±8, 326⟩	14280	⟨22, ±8, 163⟩	14280	⟨23, ±16, 158⟩
14280	⟨33, ±30, 115⟩	14280	⟨46, ±16, 79⟩	14280	⟨47, ±14, 77⟩	14280	⟨55, ±30, 69⟩
14280	⟨59, ±36, 66⟩	14560	⟨11, ±2, 331⟩	14560	⟨17, ±14, 217⟩	14560	⟨31, ±14, 119⟩
14560	⟨41, ±6, 89⟩	14560	⟨43, ±24, 88⟩	14560	⟨44, ±20, 85⟩	14560	⟨53, ±42, 77⟩
14560	⟨55, ±20, 68⟩	14763	⟨23, ±7, 161⟩	14763	⟨47, ±29, 83⟩	14763	⟨53, ±17, 71⟩
14763	⟨59, ±39, 69⟩	14820	⟨17, ±2, 218⟩	14820	⟨29, ±12, 129⟩	14820	⟨34, ±2, 109⟩
14820	⟨43, ±12, 87⟩	14820	⟨47, ±28, 83⟩	14820	⟨51, ±36, 79⟩	14820	⟨58, ±46, 73⟩
14820	⟨59, ±44, 71⟩	16192	⟨17, ±14, 241⟩	16192	⟨32, ±24, 131⟩	16192	⟨32, ±8, 127⟩
16192	⟨61, ±20, 68⟩	16555	⟨29, ±27, 149⟩	16555	⟨37, ±13, 113⟩	16555	⟨41, ±3, 101⟩
16555	⟨47, ±41, 97⟩	17220	⟨17, ±16, 257⟩	17220	⟨29, ±8, 149⟩	17220	⟨31, ±4, 139⟩
17220	⟨34, ±18, 129⟩	17220	⟨43, ±18, 102⟩	17220	⟨51, ±18, 86⟩	17220	⟨58, ±50, 85⟩
17220	⟨62, ±58, 83⟩	17472	⟨17, ±2, 257⟩	17472	⟨23, ±10, 191⟩	17472	⟨32, ±24, 141⟩
17472	⟨32, ±8, 137⟩	17472	⟨47, ±24, 96⟩	17472	⟨51, ±36, 92⟩	17472	⟨59, ±46, 83⟩
17472	⟨68, ±36, 69⟩	17760	⟨11, ±4, 404⟩	17760	⟨19, ±10, 235⟩	17760	⟨33, ±18, 137⟩
17760	⟨44, ±4, 101⟩	17760	⟨47, ±10, 95⟩	17760	⟨55, ±40, 88⟩	17760	⟨57, ±48, 88⟩
17760	⟨61, ±28, 76⟩	17952	⟨13, ±12, 348⟩	17952	⟨29, ±12, 156⟩	17952	⟨31, ±20, 148⟩
17952	⟨37, ±20, 124⟩	17952	⟨39, ±12, 116⟩	17952	⟨47, ±40, 104⟩	17952	⟨52, ±12, 87⟩
17952	⟨53, ±42, 93⟩	18720	⟨9, ±6, 521⟩	18720	⟨23, ±18, 207⟩	18720	⟨31, ±2, 151⟩
18720	⟨36, ±12, 131⟩	18720	⟨45, ±30, 109⟩	18720	⟨53, ±28, 92⟩	18720	⟨67, ±24, 72⟩
18720	⟨72, ±48, 73⟩	19320	⟨17, ±14, 287⟩	19320	⟨29, ±20, 170⟩	19320	⟨34, ±20, 145⟩
19320	⟨41, ±14, 119⟩	19320	⟨51, ±48, 106⟩	19320	⟨53, ±48, 102⟩	19320	⟨58, ±20, 85⟩
19320	⟨73, ±68, 82⟩	19380	⟨13, ±4, 373⟩	19380	⟨23, ±20, 215⟩	19380	⟨26, ±22, 191⟩
19380	⟨39, ±30, 130⟩	19380	⟨43, ±20, 115⟩	19380	⟨46, ±26, 109⟩	19380	⟨65, ±30, 78⟩
19380	⟨69, ±66, 86⟩	19635	⟨19, ±7, 259⟩	19635	⟨31, ±9, 159⟩	19635	⟨37, ±7, 133⟩
19635	⟨41, ±39, 129⟩	19635	⟨43, ±39, 123⟩	19635	⟨53, ±9, 93⟩	19635	⟨57, ±45, 95⟩
19635	⟨59, ±37, 89⟩	20020	⟨19, ±14, 266⟩	20020	⟨23, ±6, 218⟩	20020	⟨37, ±16, 137⟩
20020	⟨38, ±14, 133⟩	20020	⟨46, ±6, 109⟩	20020	⟨47, ±40, 115⟩	20020	⟨61, ±54, 94⟩
20020	⟨74, ±58, 79⟩	20640	⟨13, ±2, 397⟩	20640	⟨17, ±10, 305⟩	20640	⟨39, ±24, 136⟩
20640	⟨51, ±24, 104⟩	20640	⟨52, ±28, 103⟩	20640	⟨61, ±10, 85⟩	20640	⟨65, ±50, 89⟩
20640	⟨68, ±44, 83⟩	20832	⟨19, ±12, 276⟩	20832	⟨23, ±12, 228⟩	20832	⟨37, ±6, 141⟩
20832	⟨41, ±18, 129⟩	20832	⟨43, ±18, 123⟩	20832	⟨47, ±6, 111⟩	20832	⟨57, ±12, 92⟩

$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$	$\lvert\Delta\rvert$	$\langle A, B, C\rangle$
20832	$\langle 69, \pm 12, 76\rangle$	21120	$\langle 16, \pm 8, 331\rangle$	21120	$\langle 32, \pm 16, 167\rangle$	21120	$\langle 37, \pm 28, 148\rangle$
21120	$\langle 41, \pm 6, 129\rangle$	21120	$\langle 43, \pm 6, 123\rangle$	21120	$\langle 48, \pm 24, 113\rangle$	21120	$\langle 61, \pm 48, 96\rangle$
21120	$\langle 71, \pm 40, 80\rangle$	21840	$\langle 8, \pm 4, 683\rangle$	21840	$\langle 24, \pm 12, 229\rangle$	21840	$\langle 37, \pm 8, 148\rangle$
21840	$\langle 40, \pm 20, 139\rangle$	21840	$\langle 43, \pm 2, 127\rangle$	21840	$\langle 53, \pm 46, 113\rangle$	21840	$\langle 56, \pm 28, 101\rangle$
21840	$\langle 59, \pm 52, 104\rangle$	22080	$\langle 19, \pm 6, 291\rangle$	22080	$\langle 32, \pm 24, 177\rangle$	22080	$\langle 32, \pm 8, 173\rangle$
22080	$\langle 37, \pm 34, 157\rangle$	22080	$\langle 57, \pm 6, 97\rangle$	22080	$\langle 59, \pm 24, 96\rangle$	22080	$\langle 71, \pm 70, 95\rangle$
22080	$\langle 76, \pm 44, 79\rangle$	22848	$\langle 19, \pm 16, 304\rangle$	22848	$\langle 29, \pm 2, 197\rangle$	22848	$\langle 32, \pm 24, 183\rangle$
22848	$\langle 32, \pm 8, 179\rangle$	22848	$\langle 57, \pm 54, 113\rangle$	22848	$\langle 61, \pm 24, 96\rangle$	22848	$\langle 73, \pm 72, 96\rangle$
22848	$\langle 76, \pm 60, 87\rangle$	24640	$\langle 23, \pm 4, 268\rangle$	24640	$\langle 31, \pm 6, 199\rangle$	24640	$\langle 32, \pm 24, 197\rangle$
24640	$\langle 32, \pm 8, 193\rangle$	24640	$\langle 41, \pm 40, 160\rangle$	24640	$\langle 59, \pm 50, 115\rangle$	24640	$\langle 61, \pm 2, 101\rangle$
24640	$\langle 67, \pm 4, 92\rangle$	27360	$\langle 9, \pm 6, 761\rangle$	27360	$\langle 29, \pm 4, 236\rangle$	27360	$\langle 36, \pm 12, 191\rangle$
27360	$\langle 43, \pm 26, 163\rangle$	27360	$\langle 45, \pm 30, 157\rangle$	27360	$\langle 59, \pm 4, 116\rangle$	27360	$\langle 72, \pm 48, 103\rangle$
27360	$\langle 72, \pm 24, 97\rangle$	29568	$\langle 16, \pm 8, 463\rangle$	29568	$\langle 32, \pm 16, 233\rangle$	29568	$\langle 43, \pm 4, 172\rangle$
29568	$\langle 47, \pm 18, 159\rangle$	29568	$\langle 48, \pm 24, 157\rangle$	29568	$\langle 53, \pm 18, 141\rangle$	29568	$\langle 73, \pm 56, 112\rangle$
29568	$\langle 83, \pm 48, 96\rangle$	29920	$\langle 19, \pm 10, 395\rangle$	29920	$\langle 23, \pm 16, 328\rangle$	29920	$\langle 41, \pm 16, 184\rangle$
29920	$\langle 53, \pm 48, 152\rangle$	29920	$\langle 67, \pm 30, 115\rangle$	29920	$\langle 76, \pm 28, 101\rangle$	29920	$\langle 79, \pm 10, 95\rangle$
29920	$\langle 92, \pm 76, 97\rangle$	31395	$\langle 17, \pm 15, 465\rangle$	31395	$\langle 31, \pm 15, 255\rangle$	31395	$\langle 43, \pm 9, 183\rangle$
31395	$\langle 47, \pm 1, 167\rangle$	31395	$\langle 51, \pm 15, 155\rangle$	31395	$\langle 61, \pm 9, 129\rangle$	31395	$\langle 71, \pm 49, 119\rangle$
31395	$\langle 85, \pm 15, 93\rangle$	32032	$\langle 17, \pm 8, 472\rangle$	32032	$\langle 29, \pm 10, 277\rangle$	32032	$\langle 37, \pm 26, 221\rangle$
32032	$\langle 59, \pm 8, 136\rangle$	32032	$\langle 68, \pm 60, 131\rangle$	32032	$\langle 71, \pm 42, 119\rangle$	32032	$\langle 79, \pm 68, 116\rangle$
32032	$\langle 89, \pm 50, 97\rangle$	33915	$\langle 11, \pm 3, 771\rangle$	33915	$\langle 33, \pm 3, 257\rangle$	33915	$\langle 41, \pm 19, 209\rangle$
33915	$\langle 55, \pm 25, 157\rangle$	33915	$\langle 61, \pm 1, 139\rangle$	33915	$\langle 67, \pm 11, 127\rangle$	33915	$\langle 77, \pm 63, 123\rangle$
33915	$\langle 79, \pm 23, 109\rangle$	34720	$\langle 13, \pm 4, 668\rangle$	34720	$\langle 29, \pm 14, 301\rangle$	34720	$\langle 43, \pm 14, 203\rangle$
34720	$\langle 52, \pm 4, 167\rangle$	34720	$\langle 65, \pm 30, 137\rangle$	34720	$\langle 79, \pm 44, 116\rangle$	34720	$\langle 89, \pm 48, 104\rangle$
34720	$\langle 91, \pm 56, 104\rangle$	36960	$\langle 13, \pm 8, 712\rangle$	36960	$\langle 17, \pm 10, 545\rangle$	36960	$\langle 23, \pm 22, 407\rangle$
36960	$\langle 37, \pm 22, 253\rangle$	36960	$\langle 39, \pm 18, 239\rangle$	36960	$\langle 51, \pm 24, 184\rangle$	36960	$\langle 52, \pm 44, 187\rangle$
36960	$\langle 65, \pm 60, 156\rangle$	36960	$\langle 67, \pm 52, 148\rangle$	36960	$\langle 68, \pm 44, 143\rangle$	36960	$\langle 69, \pm 24, 136\rangle$
36960	$\langle 85, \pm 10, 109\rangle$	36960	$\langle 89, \pm 8, 104\rangle$	36960	$\langle 91, \pm 70, 115\rangle$	36960	$\langle 92, \pm 68, 113\rangle$
36960	$\langle 104, \pm 96, 111\rangle$	40755	$\langle 23, \pm 1, 443\rangle$	40755	$\langle 31, \pm 17, 331\rangle$	40755	$\langle 41, \pm 9, 249\rangle$
40755	$\langle 43, \pm 3, 237\rangle$	40755	$\langle 69, \pm 45, 155\rangle$	40755	$\langle 79, \pm 3, 129\rangle$	40755	$\langle 83, \pm 9, 123\rangle$
40755	$\langle 93, \pm 45, 115\rangle$	43680	$\langle 11, \pm 10, 995\rangle$	43680	$\langle 19, \pm 18, 579\rangle$	43680	$\langle 29, \pm 20, 380\rangle$
43680	$\langle 33, \pm 12, 332\rangle$	43680	$\langle 44, \pm 12, 249\rangle$	43680	$\langle 55, \pm 10, 199\rangle$	43680	$\langle 57, \pm 18, 193\rangle$
43680	$\langle 61, \pm 22, 181\rangle$	43680	$\langle 67, \pm 2, 163\rangle$	43680	$\langle 76, \pm 20, 145\rangle$	43680	$\langle 77, \pm 56, 152\rangle$
43680	$\langle 83, \pm 12, 132\rangle$	43680	$\langle 87, \pm 78, 143\rangle$	43680	$\langle 88, \pm 56, 133\rangle$	43680	$\langle 88, \pm 32, 127\rangle$
43680	$\langle 95, \pm 20, 116\rangle$	57120	$\langle 11, \pm 6, 1299\rangle$	57120	$\langle 23, \pm 14, 623\rangle$	57120	$\langle 33, \pm 6, 433\rangle$
57120	$\langle 44, \pm 28, 329\rangle$	57120	$\langle 47, \pm 28, 308\rangle$	57120	$\langle 55, \pm 50, 271\rangle$	57120	$\langle 59, \pm 46, 251\rangle$
57120	$\langle 69, \pm 60, 220\rangle$	57120	$\langle 77, \pm 28, 188\rangle$	57120	$\langle 79, \pm 32, 184\rangle$	57120	$\langle 88, \pm 72, 177\rangle$
57120	$\langle 88, \pm 16, 163\rangle$	57120	$\langle 89, \pm 14, 161\rangle$	57120	$\langle 92, \pm 60, 165\rangle$	57120	$\langle 109, \pm 66, 141\rangle$
57120	$\langle 115, \pm 60, 132\rangle$	77280	$\langle 17, \pm 6, 1137\rangle$	77280	$\langle 29, \pm 18, 669\rangle$	77280	$\langle 41, \pm 28, 476\rangle$
77280	$\langle 51, \pm 6, 379\rangle$	77280	$\langle 53, \pm 10, 365\rangle$	77280	$\langle 68, \pm 28, 287\rangle$	77280	$\langle 73, \pm 10, 265\rangle$
77280	$\langle 85, \pm 40, 232\rangle$	77280	$\langle 87, \pm 18, 223\rangle$	77280	$\langle 107, \pm 98, 203\rangle$	77280	$\langle 109, \pm 108, 204\rangle$
77280	$\langle 116, \pm 76, 179\rangle$	77280	$\langle 119, \pm 28, 164\rangle$	77280	$\langle 123, \pm 54, 163\rangle$	77280	$\langle 136, \pm 96, 159\rangle$
77280	$\langle 136, \pm 40, 145\rangle$	87360	$\langle 32, \pm 24, 687\rangle$	87360	$\langle 32, \pm 8, 683\rangle$	87360	$\langle 37, \pm 16, 592\rangle$
87360	$\langle 43, \pm 4, 508\rangle$	87360	$\langle 53, \pm 14, 413\rangle$	87360	$\langle 59, \pm 14, 371\rangle$	87360	$\langle 96, \pm 72, 241\rangle$
87360	$\langle 96, \pm 24, 229\rangle$	87360	$\langle 101, \pm 56, 224\rangle$	87360	$\langle 111, \pm 90, 215\rangle$	87360	$\langle 113, \pm 92, 212\rangle$
87360	$\langle 127, \pm 4, 172\rangle$	87360	$\langle 129, \pm 90, 185\rangle$	87360	$\langle 139, \pm 40, 160\rangle$	87360	$\langle 148, \pm 132, 177\rangle$
87360	$\langle 159, \pm 120, 160\rangle$						

Table A.2: Classically Integral Quaternary Forms with Square Discriminant

$\langle c_{11}, c_{12}, c_{13}, c_{14}, c_{22}, c_{23}, c_{24}, c_{33}, c_{34}, c_{44}\rangle$	Class Number	Highest Denominator
$\langle 1,0,0,0,1,0,0,1,0,4\rangle$	1	2
$\langle 1,0,0,0,1,0,0,2,0,2\rangle$	1	2
$\langle 1,0,0,0,2,0,2,2,2,2\rangle$	1	2
$\langle 1,0,0,0,1,0,0,2,2,5\rangle$	1	3
$\langle 1,0,0,0,1,0,0,3,0,3\rangle$	1	2
$\langle 1,0,0,0,2,2,0,2,0,3\rangle$	1	1
$\langle 1,0,0,0,1,0,0,2,0,8\rangle$	2	4
$\langle 1,0,0,0,2,0,0,2,0,4\rangle$	2	2
$\langle 1,0,0,0,2,0,0,3,2,3\rangle$	1	4
$\langle 1,0,0,0,1,0,0,2,2,13\rangle$	3	5
$\langle 1,0,0,0,2,0,2,3,2,5\rangle$	3	5

$\langle 1,0,0,0,2,2,0,3,0,5\rangle$	1	2
$\langle 1,0,0,0,2,0,0,3,0,6\rangle$	2	2
$\langle 1,0,0,0,2,0,2,4,0,5\rangle$	2	6
$\langle 1,0,0,0,2,0,2,4,4,6\rangle$	2	6
$\langle 1,0,0,0,2,0,2,3,2,9\rangle$	5	7
$\langle 1,0,0,0,2,2,0,4,0,7\rangle$	3	3
$\langle 1,0,0,0,2,0,0,4,0,8\rangle$	2	4
$\langle 1,0,0,0,2,0,0,5,0,10\rangle$	2	8

Table A.3: Not-Classically Integral Quaternary Forms with Square Discriminant

$\langle c_{11},c_{12},c_{13},c_{14},c_{22},c_{23},c_{24},c_{33},c_{34},c_{44}\rangle$	Class Number	Highest Denominator
$\langle 1,0,0,1,1,0,1,1,1,1\rangle$	1	1
$\langle 1,1,0,0,1,0,0,1,1,1\rangle$	1	1
$\langle 1,1,1,0,1,1,0,1,0,2\rangle$	1	1
$\langle 1,1,1,0,1,1,1,2,2,2\rangle$	1	1
$\langle 1,0,0,1,1,0,1,1,1,3\rangle$	1	3
$\langle 1,1,0,0,1,0,0,1,0,3\rangle$	1	2
$\langle 1,1,1,0,1,1,1,1,1,5\rangle$	1	1
$\langle 1,0,1,1,1,1,1,2,1,2\rangle$	1	1
$\langle 1,1,0,0,1,0,0,2,2,2\rangle$	1	1
$\langle 1,0,1,0,1,0,1,2,0,2\rangle$	1	1
$\langle 1,1,1,0,1,1,0,1,0,8\rangle$	2	4
$\langle 1,0,0,1,1,0,1,2,2,3\rangle$	2	4
$\langle 1,1,0,0,1,0,1,2,0,3\rangle$	1	4
$\langle 1,0,0,1,1,0,1,1,1,7\rangle$	2	5
$\langle 1,1,1,0,1,1,1,1,1,13\rangle$	2	5
$\langle 1,1,1,0,2,2,-1,2,1,3\rangle$	1	1
$\langle 1,0,0,1,2,2,0,2,2,3\rangle$	2	5
$\langle 1,1,0,0,1,0,1,2,2,5\rangle$	2	5
$\langle 1,0,0,0,2,1,-1,2,1,2\rangle$	2	2
$\langle 1,0,1,1,1,1,1,3,1,3\rangle$	1	1
$\langle 1,1,1,0,1,1,0,2,0,5\rangle$	2	2
$\langle 1,0,1,0,1,0,1,3,0,3\rangle$	3	2
$\langle 1,1,0,0,1,0,0,2,0,6\rangle$	2	2
$\langle 1,0,0,0,1,0,1,3,3,4\rangle$	2	4
$\langle 1,0,1,1,2,2,2,3,0,3\rangle$	2	2
$\langle 1,0,1,0,1,1,0,3,2,4\rangle$	2	6
$\langle 1,0,0,1,2,0,0,2,2,3\rangle$	2	6
$\langle 1,1,1,0,2,1,0,2,0,3\rangle$	2	4
$\langle 1,1,1,0,2,1,2,2,2,4\rangle$	1	2
$\langle 1,1,0,1,2,1,1,2,2,4\rangle$	1	1
$\langle 1,1,0,0,1,0,1,2,2,9\rangle$	3	7
$\langle 1,0,1,1,2,0,2,3,0,3\rangle$	3	7
$\langle 1,0,1,1,2,1,-1,3,2,3\rangle$	2	2
$\langle 1,0,1,0,1,0,0,2,0,7\rangle$	2	4
$\langle 1,0,1,0,1,1,0,3,1,5\rangle$	3	7
$\langle 1,1,0,0,2,0,0,2,2,4\rangle$	3	2
$\langle 1,0,0,1,2,2,0,2,2,5\rangle$	3	7
$\langle 1,0,0,1,2,1,0,2,0,4\rangle$	3	2
$\langle 1,1,1,1,2,1,0,2,0,5\rangle$	3	5
$\langle 1,1,0,0,2,1,1,3,1,3\rangle$	3	3
$\langle 1,1,1,1,2,2,0,2,1,6\rangle$	2	3
$\langle 1,1,0,0,2,0,2,3,3,4\rangle$	3	5
$\langle 1,1,1,0,2,2,-1,3,2,5\rangle$	3	2
$\langle 1,0,1,0,2,0,2,3,3,5\rangle$	4	9
$\langle 1,0,1,1,2,2,0,3,2,5\rangle$	4	9
$\langle 1,0,1,0,2,2,2,3,1,5\rangle$	1	3
$\langle 1,1,1,0,2,1,2,3,3,6\rangle$	3	2
$\langle 1,0,0,1,2,0,0,2,2,7\rangle$	6	10

$\langle 1,0,1,1,2,0,0,4,3,4\rangle$	3	8
$\langle 1,0,0,0,2,1,-1,2,1,7\rangle$	4	4
$\langle 1,1,1,0,2,2,0,2,0,10\rangle$	3	8
$\langle 1,0,1,1,2,0,0,3,2,5\rangle$	6	10
$\langle 1,1,0,0,2,1,0,3,0,5\rangle$	4	4
$\langle 1,0,1,0,2,2,0,3,2,6\rangle$	6	10
$\langle 1,1,0,0,2,0,0,3,3,6\rangle$	3	2
$\langle 1,0,1,0,1,0,0,3,0,11\rangle$	5	8
$\langle 1,0,1,0,2,0,2,3,0,6\rangle$	1	1
$\langle 1,0,1,1,2,2,0,3,0,7\rangle$	6	11
$\langle 1,0,0,1,2,2,0,5,5,5\rangle$	6	11
$\langle 1,0,0,1,2,1,0,3,0,6\rangle$	6	4
$\langle 1,0,1,1,2,0,0,3,2,7\rangle$	3	12
$\langle 1,0,1,0,2,2,0,3,0,8\rangle$	6	12
$\langle 1,0,1,1,2,2,2,5,1,5\rangle$	6	36
$\langle 1,1,0,0,2,1,0,2,0,13\rangle$	4	12
$\langle 1,0,1,0,2,0,2,3,3,9\rangle$	8	39
$\langle 1,0,1,0,2,2,2,5,4,6\rangle$	8	39
$\langle 1,0,1,0,2,2,2,3,0,10\rangle$	8	13
$\langle 1,0,0,1,2,2,0,5,1,5\rangle$	8	13
$\langle 1,0,0,0,2,1,-1,5,3,5\rangle$	4	12
$\langle 1,0,1,0,2,0,0,5,4,6\rangle$	12	14
$\langle 1,0,1,0,2,2,0,5,2,6\rangle$	12	42
$\langle 1,0,1,1,2,1,2,4,1,8\rangle$	6	6
$\langle 1,0,1,0,2,2,2,3,1,13\rangle$	6	15
$\langle 1,0,1,1,2,2,0,3,2,13\rangle$	5	15
$\langle 1,0,1,1,2,0,2,5,3,7\rangle$	6	15
$\langle 1,0,0,1,2,2,2,5,1,7\rangle$	6	15
$\langle 1,0,0,1,2,2,0,5,3,7\rangle$	5	15
$\langle 1,0,1,1,2,2,0,5,2,7\rangle$	6	15
$\langle 1,0,0,1,2,1,0,4,0,8\rangle$	6	12
$\langle 1,0,1,1,2,0,2,5,4,9\rangle$	14	17
$\langle 1,0,1,0,2,2,2,5,1,9\rangle$	3	3
$\langle 1,0,1,1,2,1,2,5,1,10\rangle$	4	20
$\langle 1,0,1,0,2,0,2,5,0,10\rangle$	4	3
$\langle 1,0,0,0,2,1,0,3,0,23\rangle$	14	24
$\langle 1,0,0,0,2,1,0,4,0,31\rangle$	19	80