INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

SOME RESULTS ON CONGRUENCE p-ADIC GROUP ACTIONS ON THE $(p+1)$-REGULAR TREE, AND ON THE REPRESENTATION OF NUMBERS IN THE FORM $\sum_{i=1}^{4} C_i(L_i x_i + a_i)^2$

by

David Lee Stephenson

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
1998

Doctoral Committee:

Professor Allen Moy, Chair
Associate Professor Trevor D. Wooley
Professor Gopal Prasad
Professor Emeritus Frank A. Raymond
Assistant Professor Gary S. Tyson

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

UMI Number: 9840653

UMI Microform 9840653
Copyright 1998, by UMI Company. All rights reserved.

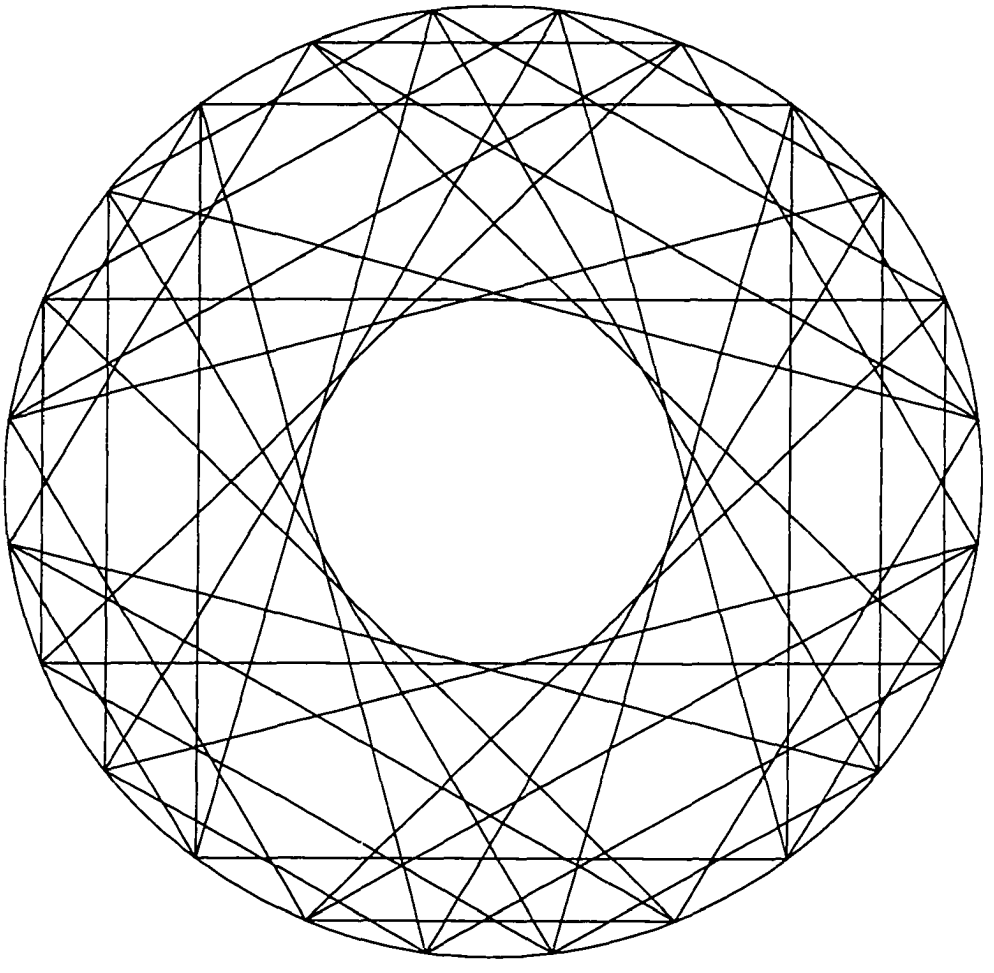
This microform edition is protected against unauthorized copying under Title 17, United States Code.

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

© David Lee Stephenson 1998
All Rights Reserved

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.



This is the quotient graph induced by the action of the congruence subgroup $\Gamma_{5,6}$ of $Q^1(\mathbb{Z}[1/5])$ on the $(5+1)$-regular tree $\mathcal{T}_5$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

This work is dedicated with love
to my parents Robert and Rosina,
my sister Cindy,
and my companion Ben.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

ACKNOWLEDGEMENTS

I would like to express my gratitude to all of the people who have shaped my life, molded my character, and made me into the person I am today. Of course, that would double the size of this document, so I will have to settle for an incomplete and inadequate thank you to:

- The members of my doctoral committee: Allen Moy, for his patience, encouragement and availability; Trevor Wooley, for taking a sabbatical from his sabbatical to critique the second half; Gopal Prasad, for his interest and assistance, particularly for his insight into strong approximation; Frank Raymond, for diving in at the last moment; and Gary Tyson, for submitting himself to a crash course in p-adic Lie groups, and for advice and contacts for my job search;
- All those mentors, instructors, and students who helped me to become a better teacher, particularly Pat Shure and Bob Megginson;
- The staff and instructors of the University of Michigan Mathematics and EECS departments;
- All my friends at the University of Michigan, for being there; especially: An-Chun Tien, Buck Koon Goh, Betsy Law, Bill Sung, Camille Tam, Daniel Kirkwood, Frank Tzu-Chung Hsieh, Jim Huggins, Jing-Yi Ruan, John Szaro, Joseph Ping Shun Lam and the guys from Hong Kong, Khai Pham, Kok-Ming Teo, Pat Ting, Paul Taylor, Saburo Matsumoto, Seung Il Kim, Kannan Soundararajan, Tim Wagenmaker, and Wah Keung Chan.
- Larry and June Au, and Pastor William Moore of Trinity Presbyterian Church in Plymouth, MI;
- My classmates at M.I.T., particularly the members of United Christian Fellowship, and especially: Adam and Jinny Kim Szabo, Chester Loh, Daniel Maung, Ernest Prabakar, Jolly Chen, Kevin and Cathy Wilson, Terence Sim, Todd Rider, Tony Eng, Tracy Vail and Victor Luchangco;
- The InterVarsity staff, particularly John Ratichek, John Smith, Jonathan and Betsy Goodell and Kevin Ford;

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

- The teachers of Irmo High and Middle Schools, and Seven Oaks Elementary School, particularly Dale Krueger;
- My friends and classmates at Irmo, particularly Jason Matthews, Greg Cowley, Kevin Wilhide, Patrick Sprawls and David Bailey;
- The MathCounts teams and the "Bridges are Forever" team;
- The members of St. Andrews Presbyterian Church in Irmo, SC, particularly Pastor Bill Barton;
- The leaders and fellow scouts of Boy Scout Troop 91 in Columbia, SC, particularly Blair Baldwin and Richard Hilton;
- The staff members of Camp Old Indian, SC and Pilgrim Pines, NH; and
- My family, for the many years of financial support, thanksgiving dinners, encouragement and love.

Finally, I believe that mathematics comes as close to truth as any of the sciences can achieve. I thank and praise God who is the Truth and the source of all truth for the opportunity to contemplate and to seek to understand the beauty and wonder revealed through mathematics.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

TABLE OF CONTENTS

DEDICATION ii

ACKNOWLEDGEMENTS iii

LIST OF FIGURES viii

LIST OF TABLES ix

CHAPTER

I. Introduction 1

1.1 Part I: Subgroups of $GL_2(\mathbb{Q}_p)$ and their Actions on $\mathcal{T}_p$ 1
1.2 Part II: An Extension of Kloosterman's Method 4
1.3 Overview 6

II. Preliminaries 8

2.1 p-adic Numbers 8
2.2 Graphs and Trees 9
2.3 Regular Trees 11
2.4 Automorphism Groups of Regular Trees 14
2.5 Actions of Matrices on Trees 15
2.6 The Standard Quaternion Algebra 16

III. The Quotient Graphs $\mathcal{X}_{p,L} = \Gamma_{p,L}\backslash\mathcal{T}_p$ and $\mathcal{X}'_{p,L} = \Gamma'_{p,L}\backslash\mathcal{T}_p$ 19

3.1 The Action of $M \in GL_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$ 20
3.2 The Action of $Q^1(\mathbb{Z}[1/p])$ on $\mathcal{T}_p$ and Quotient Actions 25
3.3 Two Congruence Subgroups over $\mathbb{Q}_p$ 29
3.4 Vertex Count 33

IV. Computation of Quotient Graphs 42

4.1 Overview of the Programs 42
4.2 Representation of the Groups $Q^1(\mathbb{Z}[1/p])$, $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ . . . 43

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

4.2.1 Files of Tuples 45
4.2.2 Tuple Programs 46
4.2.3 Implementation Notes 47
4.3 Representation of p-adic Integers 47
4.4 Representation of Tree Vertices 49
4.4.1 Standard Form for Lattices 49
4.4.2 Standard Form for Lattices 51
4.5 Computation of the Action of $M \in \mathrm{SL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$ 53
4.6 Representation of the Tree $\mathcal{T}_p$ 57
4.6.1 Selection of `RadiusMax` 57
4.6.2 Enumeration of the Vertices of the Subtree 58
4.6.3 An Important Optimization 61
4.7 Representation of the Quotient Maps 62
4.7.1 Quotient Map File Names 62
4.7.2 Quotient Map Files and Programs 63
4.8 Stopping Conditions and Program Correctness 64
4.9 Program Results 66

V. Lemmas 76

5.1 Definitions and Chapter Goals 78
5.2 Reduction of $G_{C,L,a}(h,k,\nu)$ to a Gaussian Sum 79
5.3 Evaluation of the sums $G(h,k)$ and $G_{C,L,a}(h,k,\nu)$ 84
5.4 Evaluation of the Sum σ 87

VI. Extending Kloosterman's Proof 93

6.1 Step 1: Express $r(n)$ as a Complex Path Integral 94
6.2 Step 2: Break the Circle Γ Up into Farey-Arcs 95
6.3 Step 3: Rewrite $\theta_{C,L,a}(w)$ for the Farey-arc $\phi_{h,k}$ 96
6.4 Intermission: Many Useful Lemmas 98
6.5 Step 4: Split J_0 into $J_{0,1} + J_{0,2} + J_{0,3}$ 103
6.6 Step 5: Further Split $J_{0,2}$ 103
6.7 Step 6: Evaluate $J_{0,2,2}$ and $J_{0,2,3}$ 105
6.8 Step 7: Complete the Evaluation of $J_{0,2}$ 106
6.9 Step 8: Evaluate $J_{0,1}$ and $J_{0,3}$, Then J_0 107
6.10 Step 9: Begin to Evaluate One of the Remaining Terms . . . 109
6.11 Step 10: Evaluate I_1 and I_3, Then I 111
6.12 Conclusion 113

VII. Evaluation of the Singular Series 114

7.1 Evaluation of $G_{C,L,a}(h,k)$ 116
7.2 Evaluation of $A(p^e,n)$ 119

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

7.3 Computation of $S(n)$ 123

VIII. Future Work **131**

8.1 Part I: Subgroups of $\mathrm{GL}_2(\mathbb{Q}_p)$ and their Actions on $\mathcal{T}_p$ 131
8.2 Part II: An Extension of Kloosterman's Method 132

BIBLIOGRAPHY **135**

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

LIST OF FIGURES

Figure

1.1 The quotient graphs $\mathcal{X}_{3,4}$, $\mathcal{X}_{5,4}$ and $\mathcal{X}_{7,4}$ 4

2.1 A portion of the $(3+1)$-regular tree $\mathcal{T}_3$ 11

2.2 $(3+1)$-regular tree with numbered vertices 12

3.1 A fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ 20

4.1 Representation of vertices 52

4.2 Enumeration of subtree vertices 60

4.3 The quotient graph $\mathcal{X}_{5,3}$ 67

4.4 The quotient graph $\mathcal{X}_{7,3}$ 68

4.5 The quotient graph $\mathcal{X}_{3,4}$ 69

4.6 The quotient graph $\mathcal{X}_{5,4}$ 70

4.7 The quotient graph $\mathcal{X}_{7,4}$ 71

4.8 The quotient graph $\mathcal{X}_{3,5}$ 72

4.9 The quotient graph $\mathcal{X}_{5,6}$ 73

4.10 The quotient graph $\mathcal{X}_{3,7}$ 74

4.11 The quotient graph $\mathcal{X}_{3,8}$ 75

8.1 The graph $\mathcal{X}_{3,5}$ and two of its quotient graphs 133

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

LIST OF TABLES

Table

2.1 Lifting solutions to $x^2 \equiv 6 \pmod{5^r}$ 9

3.1 Sizes of $Q^1(\mathbb{Z}/(L))$ and $N(\mathbb{Z}/(L))$ 41

4.1 Prefixes for tuple file names 46

4.2 Values for `ExponentMax` and `PadicMod` for 64-bit numbers 48

4.3 Number of vertices in subtrees of $\mathcal{T}_p$ 58

4.4 Values for `RadiusMax` and `PowerMax` used to compute $\mathcal{X}_{p,L}$ 66

7.1 Computation of $\beta_{C,L,a}(h,k)$. 118

7.2 Computation of $G_{C,L,a}(h,k)$. 118

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER I

Introduction

This dissertation is divided into two nearly independent parts. Chapters II, III and IV examine the action of certain subgroups of $\mathrm{GL}_2(\mathbb{Q}_p)$ on the regular tree $\mathcal{T}_p$. Chapters V, VI and VII extend a theorem of Kloosterman from analytic number theory estimating the number of representations of an integer n in the form

$$n = C_1x_1^2 + C_2x_2^2 + C_3x_3^2 + C_4x_4^2.$$

The proof of the main result in the first part requires a corollary of the main result from the second part.

1.1 Part I: Subgroups of $\mathrm{GL}_2(\mathbb{Q}_p)$ and their Actions on $\mathcal{T}_p$

Let p be an odd prime. The first half of this dissertation is concerned with the group $\mathrm{GL}_2(\mathbb{Q}_p)$ of invertible 2×2 matrices over the p-adic numbers and its action on the $(p+1)$-regular tree $\mathcal{T}_p$, obtained by identifying the vertices of $\mathcal{T}_p$ with equivalence classes of lattices over $\mathbb{Q}_p$. This action is analogous to the action of $\mathrm{SL}_2(\mathbb{R})$ on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} \mid |\operatorname{Im} z > 0\}$.

With respect to a fixed base, let v_0 be the vertex corresponding to the lattice

$$\mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

The action of a particular matrix $M \in \mathrm{GL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$ is characterized by its determinant and trace:

Theorem 3.4 (p. 23). *Select $M \in \mathrm{GL}_2(\mathbb{Q}_p)$. Write $\operatorname{tr} M = p^tT'$ and $\det M = p^dD'$, where $t, d \in \mathbb{Z}$ and $T', D' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Let μ be the maximum integer such that $p^{-\mu}M \in \mathrm{GL}_2(\mathbb{Z}_p)$. Let Δ be the discriminant $\Delta = (\operatorname{tr} M)^2/4 - (\det M)$ of the characteristic polynomial. Then M acts on $\mathcal{T}_p$ so that the vertex v_0 is moved a distance $d - 2\mu$, and*

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(1) If Δ is a non-zero square in $\mathbb{Q}_p$ and $d > 2t$, then M translates some geodesic in $\mathcal{T}_p$ by a distance $d - 2t$. The distance between v_0 and the translated geodesic is $t - \mu$.

(2) If Δ is a non-zero square in $\mathbb{Q}_p$ and $d \leq 2t$, then M fixes every vertex on some geodesic in $\mathcal{T}_p$.

(3) If Δ is a non-square in $\mathbb{Q}_p$ and d is even, then M is a rotation. The distance between v_0 and the closest fixed vertex is $d/2 - \mu$.

(4) If Δ is a non-square in $\mathbb{Q}_p$ and d is odd, then M is an inversion. The distance between v_0 and the center of the inverted edge is $d/2 - \mu$.

(5) If $\Delta = 0$ and M is a scalar multiple of the identity, then M fixes every vertex in $\mathcal{T}_p$.

(6) If $\Delta = 0$ but M is not a scalar multiple of the identity, then M fixes one boundary point and infinitely many vertices. The distance between v_0 and the closest fixed vertex is $t - \mu = d/2 - \mu$.

Let $Q(\mathbb{Q}_p)$ be the standard quaternion algebra over $\mathbb{Q}_p$ with basis $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ and multiplicative relations

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j} \quad \text{and} \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}.$$

Let $Q^1(\mathbb{Q}_p)$ denote the group

$$Q^1(\mathbb{Q}_p) = \left\{ a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k} \in Q(\mathbb{Q}_p) \mid a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1 \right\}.$$

Then $Q(\mathbb{Q}_p) \cong \mathrm{M}_2(\mathbb{Q}_p)$ as algebras, and $Q^1(\mathbb{Q}_p) \cong \mathrm{SL}_2(\mathbb{Q}_p)$ as groups. $Q^1(\mathbb{Q}_p)$ inherits the action of $\mathrm{GL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$. On the subgroup $Q^1(\mathbb{Z}[1/p])$ of $Q^1(\mathbb{Q}_p)$, Theorem 3.4 can be significantly simplified:

Corollary 3.6 (p. 25). *For p an odd prime, select*

$$x = \frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k} \in Q^1(\mathbb{Z}[1/p])$$

with $a_i \in \mathbb{Z}$ and not all of the a_i divisible by p. So $a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n}$ and $\operatorname{tr} x = 2a_1/p^n$. Let p^t be the largest power of p dividing a_1. Then:

(1) If $n = 0$, then x is a rotation that fixes the vertex v_0.

(2) If $n > 0$, then x translates some geodesic a distance of $2n - 2t$. The vertex v_0 is moved a distance $2n$, and the distance between v_0 and the geodesic translated by x is t.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Now, for integers $L > 1$ not divisible by p, define maps

$$\phi : Q^1(\mathbb{Z}[1/p]) \longrightarrow Q^1(\mathbb{Z}/(L)) \quad \text{and}$$
$$\phi' : Q^1(\mathbb{Z}[1/p]) \longrightarrow P^1(\mathbb{Z}/(L))$$

by

$$\frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \quad \longmapsto \quad \overline{a_1 p^{-n}}\,\mathbf{1} + \overline{a_2 p^{-n}}\,\mathbf{i} + \overline{a_3 p^{-n}}\,\mathbf{j} + \overline{a_4 p^{-n}}\,\mathbf{k},$$

where $Q^1(\mathbb{Z}/(L))$ is the group of standard quaternions of norm 1 over the ring $\mathbb{Z}/(L)$, and

$$P^1(\mathbb{Z}/(L)) = Q^1(\mathbb{Z}/(L)) \,/\, N(\mathbb{Z}/(L)),$$

where $N(\mathbb{Z}/(L))$ is the central, normal subgroup

$$N(\mathbb{Z}/(L)) = \left\{ \bar{a}_1\,\mathbf{1} + 0\,\mathbf{i} + 0\,\mathbf{j} + 0\,\mathbf{k} \;\middle|\; \bar{a}_1^2 \equiv 1 \,(\mathrm{mod}\, L) \right\}.$$

So the groups $Q^1(\mathbb{Z}/(L))$ and $P(\mathbb{Z}/(L))$ are the quaternion analogues of $\mathrm{SL}_2(\mathbb{Z}/(L))$ and $\mathrm{PSL}_2(\mathbb{Z}/(L))$, respectively.

Let $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ be the kernels of the maps ϕ and ϕ', respectively, so that

$$\Gamma_{p,L} = \left\{ \frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \in Q^1(\mathbb{Z}[1/p]) \;\middle|\; a_2 \equiv a_3 \equiv a_4 \equiv 0 \,(\mathrm{mod}\, L) \right\}$$

and

$$\Gamma'_{p,L} = \left\{ \frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \in \Gamma_{p,L} \;\middle|\; a_1 \equiv p^n \,(\mathrm{mod}\, L) \right\}.$$

Then $\Gamma'_{p,L} \leq \Gamma_{p,L} < Q^1(\mathbb{Z}[1/p]) < Q^1(\mathbb{Q}_p)$.

The actions of the groups $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ on the $(p+1)$-regular tree $\mathcal{T}_p$ induce compact quotient graphs

$$\mathcal{X}_{p,L} = \Gamma_{p,L}\backslash\mathcal{T}_p \qquad \text{and} \qquad \mathcal{X}'_{p,L} = \Gamma'_{p,L}\backslash\mathcal{T}_p.$$

The quotient graph $\mathcal{X}_{5,6}$ is displayed in the front of this dissertation. Other examples appear at the end of Chapter IV.

The primary goal of the first part of this dissertation is to obtain information about these graphs and about the groups $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}$ and $Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}$ which act on $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$, respectively. These two quotient groups are isomorphic to the images of $Q^1(\mathbb{Z}[1/p])$ in $P^1(\mathbb{Z}/(L))$ and $Q^1(\mathbb{Z}/(L))$ under ϕ and ϕ', respectively. The difficulty lies in determining the images of ϕ and ϕ'. This is accomplished by invoking a corollary of the main result from the second half of this dissertation.

The main result of this first half is a formula for the number of vertices in $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Corollary 3.31 (p. 39). *Write $L = 2^\ell L'$, with L' odd. Then:*

$$2\,|V\mathcal{X}_{p,L}| = |Q^1(\mathbb{Z}[1/p])\,/\,\Gamma_{p,L}|$$

$$= L^3 \prod_{q|L'} \left(\frac{1-1/q^2}{2}\right) \cdot \begin{cases} 1, & \text{if } \ell = 0 \text{ so } L \equiv 1 \pmod 2; \\ 1/2, & \text{if } \ell = 1 \text{ so } L \equiv 2 \pmod 4; \\ 1/4, & \text{if } \ell \geq 2 \text{ so } L \equiv 0 \pmod 4. \end{cases}$$

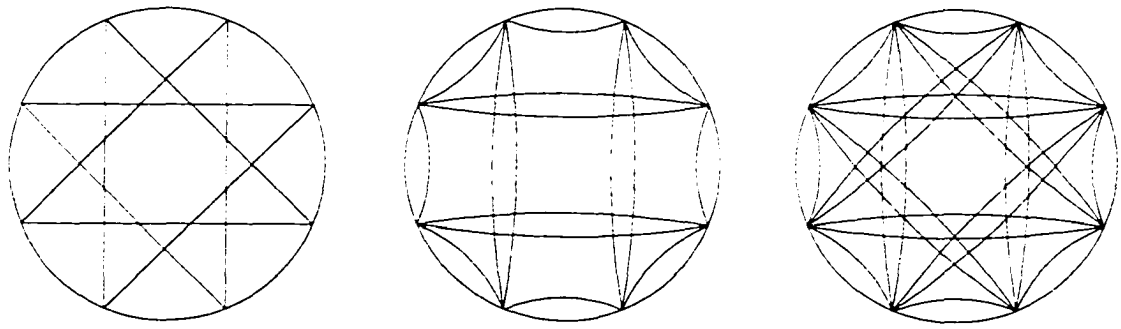
and

$$4\,|V\mathcal{X}'_{p,L}| = |Q^1(\mathbb{Z}[1/p])\,/\,\Gamma'_{p,L}|$$

$$= L^3 \prod_{q|L'} \left(1-\frac{1}{q^2}\right) \cdot \begin{cases} 1, & \text{if } L \text{ odd}; \\ 1, & \text{if } 8 \mid L \text{ and } p^{2m} \equiv L+1 \pmod{2L} \\ & \quad \text{for some } m \in \mathbb{Z}; \\ 1/2, & \text{if } L > 2 \text{ even and } p^{2m} \not\equiv L+1 \pmod{2L} \\ & \quad \text{for all } m \in \mathbb{Z}; \end{cases}$$

$$|V\mathcal{X}'_{p,L}| = |V\mathcal{X}_{p,L}| = 2 \text{ if } L = 2.$$

In particular, the number of vertices in $\mathcal{X}_{p,L}$ (but not $\mathcal{X}'_{p,L}$) is independent of p. Figure 1.1 displays $\mathcal{X}_{p,L}$ for $L = 4$ and each of the values $p = 3$, $p = 5$ and $p = 7$. All three graphs contain eight vertices.



$p = 3$ $\qquad$ $p = 5$ $\qquad$ $p = 7$

Figure 1.1: The quotient graphs $\mathcal{X}_{3,4}$, $\mathcal{X}_{5,4}$ and $\mathcal{X}_{7,4}$

1.2 Part II: An Extension of Kloosterman's Method

In his paper "On the Representation of Numbers of the Form $ax^2+by^2+cz^2+dt^2$", H. D. Kloosterman proves an asymptotic formula for the number $r(n)$ of represen-

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

tations of a positive integer n in the form $C_1x_1^2 + C_2x_2^2 + C_3x_3^2 + C_4x_4^2$, for constants C_i:

$$r(n) = \frac{\pi^2}{\sqrt{C_1C_2C_3C_4}}\, n\, S(n) + O\left(n^{17/18+\epsilon}\right)$$

for every positive ϵ, where

$$S(n) = \sum_{k=1}^{\infty} A(k,n),$$

$$A(k,n) = k^{-4} \sum_{h\leq k}{}' \exp\left[\frac{-2\pi ihn}{k}\right] \prod_{i=1}^{4} G_{C_i}(h,k),$$

$$G_C(h,k) = \sum_{j=0}^{k-1} \exp\left[\frac{2\pi ih}{k} Cj^2\right],$$

and where $\sum_{h\leq k}{}'$ indicates the sum over integers h with $1 \leq h \leq k$ and $\gcd(h,k) = 1$.

Kloosterman then studies the singular series $S(n)$ in order to determine which values of C_1, C_2, C_3 and C_4 guarantee $r(n) > 0$ for all but finitely many n.

Kloosterman's proof follows a method developed by G. H. Hardy and J. E. Littlewood, but requires significantly more analysis to establish an error bound less than $O(n)$.

The second half of this dissertation extends Kloosterman's proof to apply to representations of integers in the form

$$n = C_1y_1^2 + C_2y_2^2 + C_3y_3^2 + C_4y_4^2$$

under the congruence restrictions $y_i \equiv a_i \pmod{L_i}$ for $i = 1, 2, 3, 4$. This is equivalent to counting representations of n in the form

$$n = C_1(L_1x_1 + a_1)^2 + C_2(L_2x_2 + a_2)^2 + C_3(L_3x_3 + a_3)^2 + C_4(L_4x_4 + a_4)^2,$$

where the x_i are integers.

In particular, the following results are obtained:

Theorem 6.2 (p. 93). *For each $i = 1, 2, 3, 4$, let C_i, L_i and a_i be fixed integers with C_i and L_i positive. For each non-negative integer n, let $r(n)$ equal the number of integral solutions in the set*

$$\left\{ (y_1, y_2, y_3, y_4) \;\middle|\; n = C_1y_1^2 + C_2y_2^2 + C_3y_3^2 + C_4y_4^2 \text{ and } y_i \equiv a_i \bmod L_i \text{ for each } i \right\}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Then:

$$r(n) = \frac{\pi^2}{L_1 L_2 L_3 L_4 \sqrt{C_1 C_2 C_3 C_4}}\, n\, S(n) + O\left(n^{17/18+\epsilon}\right)$$

for every positive ϵ*, where*

$$S(n) = \sum_{k=1}^{\infty} A(k,n),$$

$$A(k,n) = k^{-4} \sum_{h \le k}{}' \exp\left[\frac{-2\pi i h n}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k),$$

$$G_{C,L,a}(h,k) = \sum_{j=0}^{k-1} \exp\left[\frac{2\pi i h}{k} C(Lj+a)^2\right],$$

and where $\sum'_{h \le k}$ *indicates the sum over integers* h *such that* $1 \le h \le k$ *and* $\gcd(h,k) = 1$.

Theorem 7.9 (p. 128). *Let* p *and* L *be positive integers with* p *prime and* L *not divisible by* p*. Let* a_1*,* a_2*,* a_3 *and* a_4 *be integers with* $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{L}$*. Let* S *be the set of representable integers*

$$S = \left\{ n \mid n = y_1^2 + y_2^2 + y_3^2 + y_4^2 \text{ for some } y_i \in \mathbb{Z} \text{ with } y_i \equiv a_i \pmod{L} \right\},$$

and let C *be the set of positive integral candidates*

$$C = \begin{cases} \left\{ n \mid n \equiv 1 \pmod{L} \right\} & \text{if } L \text{ odd,} \\ \left\{ n \mid n \equiv 1 \pmod{2L} \right\} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L}, \\ \left\{ n \mid n \equiv 1 + L \pmod{2L} \right\} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \not\equiv 1 \pmod{2L}. \end{cases}$$

Also, for each positive integer m*, put*

$$M_m = \left\{ n \mid 2^m \text{ divides } n \right\}.$$

Then $S \subseteq C$*. If* L *is even, then* $C \setminus S$ *is finite. If* L *is odd, then* $(C \setminus M_m) \setminus S$ *is finite for every positive integer* m*.*

1.3 Overview

The first half of this dissertation examines the actions of $\mathrm{GL}_2(\mathbb{Q}_p)$, $Q^1(\mathbb{Z}[1/p])$, $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ on the tree $\mathcal{T}_p$, and presents properties of the quotient graphs $\mathcal{X}_{p,L} =$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$\Gamma_{p,L}\backslash\mathcal{T}_p$ and $\mathcal{X}'_{p,L} = \Gamma'_{p,L}\backslash\mathcal{T}_p$. Chapter II reviews the p-adic numbers, the $(p+1)$-regular tree and its automorphism group, the action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$, and the standard quaternion algebra. Chapter III describes the action of a matrix in $\mathrm{GL}_2(\mathbb{Q}_p)$ in terms of its determinant and trace, examines the structure of $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}$ and $Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}$, and derives formulas for the orders of $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}$ and $Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}$ and for the number of vertices in $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$. Chapter IV describes a set of programs written in ANSI C used to obtain instances of the quotient graphs $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$for particular values of p and L.

The second half extends Kloosterman's result to incorporate congruence restrictions, and derives a corollary required in the first half. Chapter V defines and evaluates or bounds appropriate analogs and variants of $G_C(h,k)$ and $A(k,n)$. Chapter VI modifies Kloosterman's proof to obtain an asymptotic formula for representations of n satisfying the congruence restrictions. Chapter VII evaluates the singular series $S(n)$ for the case $C_i = 1$ and $L_i = L$, for all i, in order to obtain the required corollary.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER II

Preliminaries

This chapter provides some background on the p-adic numbers and the action of $\mathrm{GL}_2(\mathbb{Q}_p)$ on the $(p+1)$-regular tree. The presentation is a mixture of informal examples and more formal definitions and propositions. Proofs of most of the following facts can be found in [FTN91].

2.1 p-adic Numbers

Definition 2.1. Fix p prime. Define the *p-adic norm* on the rationals $\mathbb{Q}$ by $|0|_p = 0$ and $|x|_p = p^{-n}$, where $x = (h/k)p^n$ with $h, k, n \in \mathbb{Z}$ and $\gcd(h,p) = \gcd(k,p) = 1$. The field of *p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic norm. $\mathbb{Q}_p$ is a totally disconnected locally compact field of characteristic 0. The ring of *p-adic integers* $\mathbb{Z}_p$ is the completion of the integers $\mathbb{Z}$ within $\mathbb{Q}_p$. $\mathbb{Z}_p$ consists of all p-adic numbers with norm less than or equal to one.

Informally, a p-adic integer can be thought of as the limit of a sequence

$$a_1 \pmod{p},\ a_2 \pmod{p^2},\ a_3 \pmod{p^3},\ a_4 \pmod{p^4},\ a_5 \pmod{p^5},\ \ldots$$

such that $a_r \equiv a_{r+1} \pmod{p^r}$ for each $r \geq 1$.

Example 2.2. The equivalence $x^2 \equiv 6 \pmod 5$ has two solutions, $x \equiv 1$ and $4 \pmod 5$. Each of these solutions can be lifted to a solution to $x^2 \equiv 6 \pmod{25}$. For example, the solution $x \equiv 1 \pmod 5$ can be lifted to $x \equiv 16 \pmod{25}$. This solution can be continue to be lifted to solutions to $x^2 \equiv 6$ modulo 125, 625, 3125 and all higher powers of 5, as illustrated in Table 2.1.

When written in base 5, these solutions form a sequence

$$1,\ 31,\ 031,\ 4031,\ 24031,\ 124031,\ 2124031,\ 32124031,\ 132124031,\ \ldots.$$

in which each solution gains an additional left digit over its predecessor. The limit of this sequence is a 5-adic integer.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

5^r	A solution to $x^2 \equiv 6 \pmod{5^r}$
5^1	$1 = 1$
5^2	$16 = 1 + 3 \cdot 5$
5^3	$16 = 1 + 3 \cdot 5 + 0 \cdot 5^2$
5^4	$516 = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3$
5^5	$1766 = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4$
5^6	$4891 = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 1 \cdot 5^5$
5^7	$36141 = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 1 \cdot 5^5 + 2 \cdot 5^6$
5^8	$270516 = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 1 \cdot 5^5 + 2 \cdot 5^6 + 3 \cdot 5^7$
5^9	$661141 = 1 + 3 \cdot 5 + 0 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 1 \cdot 5^5 + 2 \cdot 5^6 + 3 \cdot 5^7 + 1 \cdot 5^8$

Table 2.1: Lifting solutions to $x^2 \equiv 6 \pmod{5^r}$

Two p-adic integers are considered to be "close" to each other (as measured by the p-adic norm) if they are the limits of two sequences that begin with identical subsequences. They can be added, subtracted, and multiplied by performing the operation on their integer sequences. Each p-adic integer has a multiplicative inverse, except for those divisible by p.

A p-adic number is a fraction of two p-adic integers with non-zero denominator. Each p-adic number can be represented as a p-adic integer divided by a power of p. Consequently, a p-adic number can be expressed as the limit of a sequence

$$\frac{a_1 \pmod{p}}{p^\ell}, \frac{a_2 \pmod{p^2}}{p^\ell}, \frac{a_3 \pmod{p^3}}{p^\ell}, \frac{a_4 \pmod{p^4}}{p^\ell}, \frac{a_5 \pmod{p^5}}{p^\ell}, \ldots$$

The fraction $(a_r \pmod{p^r})/p^\ell$ is "the same" as $(p^k a_r \pmod{p^{r+k}})/p^{\ell+k}$ for every $k \in \mathbb{N}$.

Example 2.3. The inverse of 100 in the field of 5-adic numbers is the limit of the sequence of rationals

0.04, 0.34, 3.34, 33.34, 333.34, 3333.34, 33333.34, 333333.34, 3333333.34, ...

displayed in base 5.

2.2 Graphs and Trees

Definition 2.4. A *graph* $\mathcal{X}$ consists of a set of *vertices* $V\mathcal{X}$ and a set of *edges* $E\mathcal{X}$. Each edge is a two element subset of $V\mathcal{X}$. Two vertices $x, y \in V\mathcal{X}$ are *adjacent* if $\{x, y\}$ is an edge. The *degree* of a vertex $x \in V\mathcal{X}$ is the number of edges $e \in E\mathcal{X}$ with $x \in e$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

A *path* in $\mathcal{X}$ of *length* n is a finite sequence $x_0, \ldots, x_n \in V\mathcal{X}$ such that $\{x_i, x_{i+1}\} \in E\mathcal{X}$ for all $0 \leq i < n$. A *chain* is a path $x_0, \ldots, x_n$ such that $x_i \neq x_{i+2}$ for all $0 \leq i \leq n-2$. A *circuit* is a chain $x_0, \ldots, x_n$ such that $x_0 = x_n$.

A graph $\mathcal{X}$ is *connected* if, for every $x, y \in V\mathcal{X}$, there exists a path $x_0, \ldots, x_n$ such that $x_0 = x$ and $x_n = y$. A *tree* is a connected graph with no circuits.

Definition 2.5. Let $\mathcal{T}$ be a tree. For $x, y \in V\mathcal{T}$, let $[x, y]$ denote the unique chain $x_0, \ldots, x_n$ such that $x_0 = x$ and $x_n = y$.

The *distance* $d(x, y)$ between two vertices $x, y \in V\mathcal{T}$ is the length of the chain $[x, y]$. Then d gives $\mathcal{T}$ the topology of a metric space.

Definition 2.6. An *infinite chain* is an infinite sequence of vertices $\langle x_i \mid i \in \mathbb{N} \rangle$ in $V\mathcal{T}$ such that $\{x_i, x_{i+1}\} \in E\mathcal{T}$ and $x_i \neq x_{i+2}$ for all $i \in \mathbb{N}$. A *geodesic* (or *doubly infinite chain*) is a two-way infinite sequence of vertices $\langle x_i \mid i \in \mathbb{Z} \rangle$ in $V\mathcal{T}$ such that $\{x_i, x_{i+1}\} \in E\mathcal{T}$ and $x_i \neq x_{i+2}$ for all $i \in \mathbb{Z}$.

The infinite chains $\langle x_i \mid i \in \mathbb{Z} \rangle$ and $\langle y_i \mid i \in \mathbb{Z} \rangle$ are *equivalent* if they have an infinite intersection. That is, if there exists $n, k \in \mathbb{Z}$ such that $x_i = y_{i+k}$ for all $i \geq n$. Two geodesics $\langle x_i \rangle$ and $\langle y_i \rangle$ are *equivalent* if there exists $k \in \mathbb{Z}$ with $x_i = y_{i+k}$ for all $i \in \mathbb{Z}$.

The *boundary* Ω of $\mathcal{T}$ is the set of equivalence classes of infinite chains. So Ω consists of the "points at infinity." Alternatively, fix any $x_0 \in V\mathcal{T}$. Then the boundary points Ω are in bijective correspondence with the set of infinite chains beginning at x_0. There also is a bijection between equivalence classes of geodesics and ordered pairs (ω_1, ω_2) of distinct boundary points.

Write (ω_1, ω_2) for a geodesic joining the boundary points $\omega_1, \omega_2 \in \Omega$. Also, write $[x, \omega)$ for an infinite chain $x = x_0, x_1, x_2, \ldots$ belonging to the equivalence class ω.

Definition 2.7. Let $\mathcal{T}$ be a tree. For $x, y \in V\mathcal{T}$, put:

$$B_{x,y} = \left\{ z \in V\mathcal{T} \;\middle|\; y \in [x, z] \right\} \cup \left\{ \omega \in \Omega \;\middle|\; y \in [x, \omega) \right\}.$$

Then the collection of all sets $\{x\}$ where $x \in V\mathcal{T}$ and all sets $B_{x,y}$ with $x, y \in V\mathcal{T}$ is a basis for a topology on $V\mathcal{T} \cap \Omega$.

Under this topology, $V\mathcal{T} \cup \Omega$ is compact. $V\mathcal{T}$ is dense in $V\mathcal{T} \cup \Omega$, and the restriction of the topology to $V\mathcal{T}$ is the discrete topology. The restriction of the topology to Ω is given by the basis sets

$$\Omega(x, y) = \left\{ \omega \in \Omega \;\middle|\; y \in [x, \omega) \right\}.$$

This is the same compact topology as that of the projective line over $\mathbb{Q}_p$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

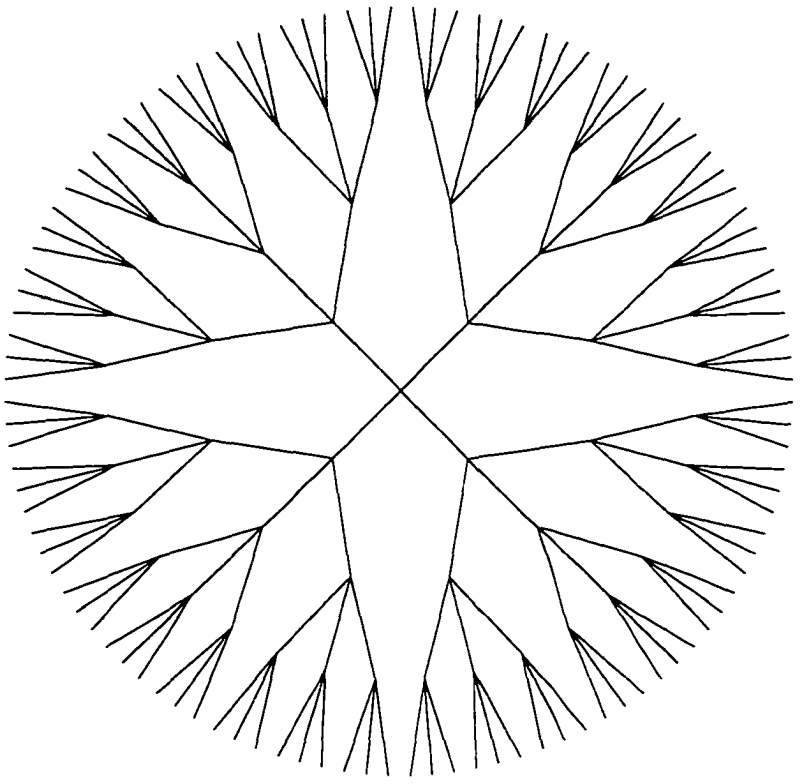


Figure 2.1: A portion of the $(3+1)$-regular tree $\mathcal{T}_3$

2.3 Regular Trees

Definition 2.8. The *regular tree* of degree $p+1$, denoted $\mathcal{T}_p$, is an unbounded tree in which each vertex has degree $p+1$. Figure 2.1 illustrates a portion of $\mathcal{T}_3$. The figure's outermost circle of vertices actually should continue to split 3-way.

Informally, the vertices of the $(p+1)$-regular tree can be identified with the fractions $(a_r \pmod{p^r})/p^\ell$ used to construct the sequences whose limits are the p-adic numbers. The vertices identified with the fractions $(a_r \pmod{p^r})/p^\ell$ and $(a_{r+1} \pmod{p^{r+1}})/p^\ell$ are adjacent if $a_r \equiv a_{r+1} \pmod{p^r}$. Figure 2.2 shows a portion of the $(3+1)$-adic tree, with the vertices labeled with numbers $(a_r \pmod{p^r})/p^\ell$, written in base 3.

The vertices in an infinite chain $x_0, x_1, \ldots$ have now been identified with a sequence of fractions whose limit is a p-adic number. Hence, the boundary points Ω of $\mathcal{T}_p$ can be identified with the p-adic numbers, plus an "infinity" number, representing the limit of the "backwards" sequence

$$0 \pmod{p},\ 0 \pmod{1},\ \frac{0 \pmod{1}}{p},\ \frac{0 \pmod{1}}{p^2},\ \frac{0 \pmod{1}}{p^3},\ \frac{0 \pmod{1}}{p^4},\ \ldots.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

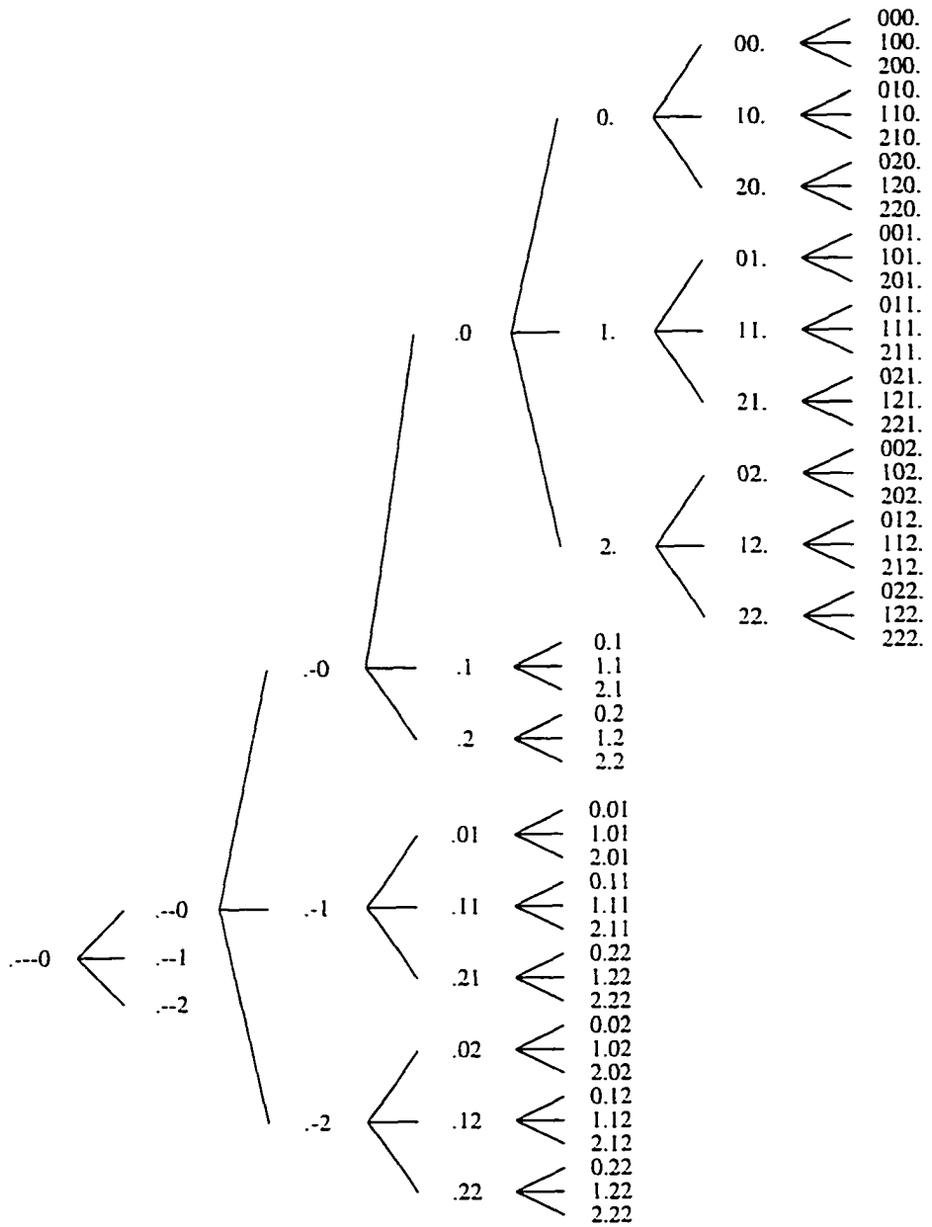


Figure 2.2: $(3+1)$-regular tree with numbered vertices

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Alternatively, the boundary points can be identified with points on the projective line,

$$\left\{ \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \;\middle|\; a_i \in \mathbb{Q}_p \right\}$$

where $[a_0 \;\; a_1]^t$ and $[b_0 \;\; b_1]^t$ are equal if $a_0 b_1 = a_1 b_0$. If $a_1 \neq 0$, then the projective point $[a_0 \;\; a_1]^t$ corresponds to the p-adic number $a_0 a_1^{-1}$. The point $[1 \;\; 0]^t$ corresponds to the "infinity" number.

Formalizing this correspondence requires a more precise understanding of the fraction $(a_r \pmod{p^r})/p^\ell$. Interpreted in terms of the projective line over $\mathbb{Q}_p$, the fraction represents the collection of all projective points

$$\begin{bmatrix} a_r \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix} = \left\{ \begin{bmatrix} a_r + kp^r \\ p^\ell \end{bmatrix} \;\middle|\; k \in \mathbb{Z}_p \right\}.$$

Compare this to the lattice

$$\mathbb{Z}_p \begin{bmatrix} a_r \\ p^\ell \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix}$$

as lattices are defined in the following definition.

Definition 2.9. Fix a vector space V of dimension 2 over $\mathbb{Q}_p$. A *lattice* of V is a compact open subset of V which is also a module over $\mathbb{Z}_p$. Two lattices L and L' are *equivalent* if $L = \alpha L'$ for some $\alpha \in \mathbb{Q}_p^*$.

Lemma 2.10. *If L is a lattice, then L/pL is a two-dimensional vector space over the finite field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/(p)$. If $e_1 \in L$ and $e_1 \notin pL$, then there exists e_2 such that $L = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$.*

Proposition 2.11. *Let L and L' be two lattices of V, belonging to equivalence classes Λ and Λ' respectively. Then there exist vectors e_1 and e_2 and integers m and n such that $L = \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ and $L' = \mathbb{Z}_p e_1 p^m \oplus \mathbb{Z}_p e_2 p^n$. Moreover, the set $\{m, n\}$ depends only upon Λ and Λ'. Consequently, define $d(\Lambda, \Lambda') = |m - n|$.*

Proposition 2.12. *Let $\mathcal{T}_p$ be a graph whose vertices are the equivalence classes of lattices in V, and whose edges consist of all pairs (Λ, Λ') such that $d(\Lambda, \Lambda') = 1$. Then $\mathcal{T}_p$ is the regular tree of degree $p + 1$.*

Proposition 2.13. *Let $\omega \in \Omega$ be a point of the boundary of $\mathcal{T}_p$ associated to the infinite chain*

$$\{\Lambda_0, \Lambda_1, \ldots, \Lambda_n, \ldots\}.$$

Let $L_i \in \Lambda_i$ be such that $L_j \subseteq L_{j-1}$ and $L_j \not\subseteq pL_{j-1}$. Then $\bigcap_{j=0}^{\infty} L_j$ generates a one-dimensional subspace r of V, and the correspondence $\omega \mapsto r$ is a bijection between Ω and the set of one dimensional subspaces of V.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

2.4 Automorphism Groups of Regular Trees

Definition 2.14. An *automorphism* of a tree $\mathcal{T}$ is a bijective map $g : V\mathcal{T} \to V\mathcal{T}$ that preserves edges. That is, $\{x, y\}$ is an edge if and only is $\{g(x), g(y)\}$ is an edge. The automorphisms of $\mathcal{T}$ are exactly the isometries of the metric space $(\mathcal{T}, d)$.

Theorem 2.15. *Suppose g is an automorphism of a regular tree $\mathcal{T}_p$. Then exactly one of the following is true:*

(1) There is a vertex $x \in V\mathcal{T}_p$ with $g(x) = x$;

(2) There is an edge $\{x, y\} \in E\mathcal{T}_p$ with $g(x) = y$ and $g(y) = x$;

(3) There are a geodesic $\langle x_i \mid i \in \mathbb{Z} \rangle$ and an integer $k \neq 0$ such that $g(x_i) = g(x_{i+k})$ for all $i \in \mathbb{Z}$.

Automorphisms are called *rotations*, *inversions* and *translations* (by distance k) if they fall into cases (1), (2) and (3), respectively.

Proposition 2.16. *(1) The composition of two inversions on distinct edges is a translation by an even distance.*

(2) The composition of an inversion on an edge and a rotation that does not fix both vertices on the edge is a translation by an odd distance that contains that edge.

(3) If $\mathcal{T}_p$ is a regular tree of degree $p + 1 > 2$, then every automorphism of $\mathcal{T}_p$ can be expressed as a composition of translations.

Definition 2.17. Suppose $\mathcal{T}_p$ is a regular tree of degree $p + 1$. Let $\operatorname{Aut} \mathcal{T}_p$ denote the group of automorphisms of $\mathcal{T}_p$.

For each $g \in \operatorname{Aut} \mathcal{T}_p$ and each finite subset $F \subset V\mathcal{T}_p$, put

$$U_F(g) = \{ h \in \operatorname{Aut} \mathcal{T}_p \mid g(x) = h(x) \text{ for all } x \in F \}.$$

The collection of sets $U_F(g)$ is a basis for a topology on $\operatorname{Aut} \mathcal{T}_p$.

Proposition 2.18. *Under this topology, $\operatorname{Aut} \mathcal{T}_p$ is a totally disconnected, locally compact topological group. Each basis element $U_F(g)$ is both open and closed. All finite subsets of $\operatorname{Aut} \mathcal{T}_p$ are closed.*

For each finite subset F of $V\mathcal{T}_p$, the collection of sets

$$\{ U_F(g) \mid g \in \operatorname{Aut} \mathcal{T}_p \}$$

forms a disjoint open cover of $\operatorname{Aut} \mathcal{T}_p$. Also, $U_F(id)$ is a subgroup of $\operatorname{Aut} \mathcal{T}_p$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proposition 2.19 (Maximal Compact Subgroups). *For each vertex $x \in V\mathcal{T}_p$ and each edge $\{y,z\} \in E\mathcal{T}_p$, put*

$$K_x = \{\, g \in \operatorname{Aut}\mathcal{T}_p \mid g(x) = x \,\}, \quad \text{and}$$
$$K_{\{y,z\}} = \{\, g \in \operatorname{Aut}\mathcal{T}_p \mid g(\{y,z\}) = \{y,z\} \,\}.$$

Then K_x and $K_{\{y,z\}}$ are compact, open and closed subgroups of $\operatorname{Aut}\mathcal{T}_p$. Furthermore, every compact subgroup of $\operatorname{Aut}\mathcal{T}_p$ is contained inside K_x for some $x \in V\mathcal{T}_p$ or inside $K_{\{y,z\}}$ for some $\{y,z\} \in E\mathcal{T}_p$.

Definition 2.20. A subgroup Γ of $\operatorname{Aut}\mathcal{T}_p$ is *faithful* if $\Gamma \cap K_x = \{id\}$ for each $x \in V\mathcal{T}_p$. Also, Γ is *transitive* if, for every $x, y \in V\mathcal{T}_p$, there exists $g \in \Gamma$ with $g \cdot x = y$.

Theorem 2.21 (Faithful Transitive Subgroups). *Suppose $x \in V\mathcal{T}_p$ and $A \subseteq \operatorname{Aut}\mathcal{T}_p$ with $|A| = p+1$ satisfies:*

(1) $A = A^{-1}$; and

(2) $\{a \cdot x \mid a \in A\} = \{y \mid d(x,y) = 1\}$.

Then A generates a faithful transitive subgroup Γ of $\operatorname{Aut}\mathcal{T}_p$. Also, Γ is isomorphic to the free product of t copies of $\mathbb{Z}$ and s copies of $\mathbb{Z}_2$, for some $t, s \in \mathbb{N}$ satisfying $2t + s = p + 1$.

Moreover, if Γ is a faithful transitive subgroup of $\operatorname{Aut}\mathcal{T}_p$, then there exists $A \subseteq \operatorname{Aut}\mathcal{T}_p$ with $|A| = p+1$ satisfying (1) and (2), which generates Γ.

Theorem 2.22. *If $\Gamma \subseteq \operatorname{Aut}\mathcal{T}_p$ is a transitive subgroup of $\operatorname{Aut}\mathcal{T}_p$, then $\operatorname{Aut}\mathcal{T}_p = K_x \cdot \Gamma$ for each $x \in V\mathcal{T}_p$.*

2.5 Actions of Matrices on Trees

As described in Section 2.3, each vertex in $\mathcal{T}_p$ is identified with an equivalence class of lattices within a two dimensional vector space V over $\mathbb{Q}_p$. Every nonsingular matrix over $\mathbb{Q}_p$ defines an automorphism of $\mathcal{T}_p$. If the vertex v is associated with the lattice $\mathbb{Z}_p w_1 \oplus \mathbb{Z}_p w_2$, then $M \cdot v$ is associated with the lattice $\mathbb{Z}_p(Mw_1) \oplus \mathbb{Z}_p(Mw_2)$.

Matrices M and M' define the same automorphism if and only if $M = \alpha M'$ for some $\alpha \in \mathbb{Q}_p^*$. Hence there is an action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$.

Proposition 2.23. *On the boundary Ω of $\mathcal{T}_p$, $\mathrm{PGL}_2(\mathbb{Q}_p)$ is the group of projective transformations of Ω. $\mathrm{PGL}_2(\mathbb{Q}_p)$ acts transitively on $\mathcal{T}_p$ and Ω. $\mathrm{PSL}_2(\mathbb{Q}_p)$ is non-compact, acts transitively on Ω, and has exactly two orbits on $\mathcal{T}_p$.*

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Lemma 2.24. *Let v_0 be the vertex associated with the lattice*

$$\mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

$\mathrm{PSL}_2(\mathbb{Z}_p)$ is the subgroup of $\mathrm{PGL}_2(\mathbb{Q}_p)$ which maps v_0 onto itself. $\mathrm{PSL}_2(\mathbb{Z}_p)$ is a closed subgroup of K_{Λ_0} and acts transitively on Ω. $\mathrm{PGL}_2(\mathbb{Q}_p)$ is a proper subgroup of $\mathrm{Aut}(\mathcal{T}_p)$, and $\mathrm{PSL}_2(\mathbb{Z}_p)$ is a proper subgroup of K_{Λ_0}.

Proposition 2.25. *Let t and s be non-negative integers such that $q+1 = 2t+s$. Then there exists a discrete subgroup $\Gamma \subseteq \mathrm{PGL}_2(\mathbb{Q}_p)$ such that*

(1) Γ acts faithfully and transitively on $\mathcal{T}_p$,

(2) Γ is isomorphic to the free product of s copies of $\mathbb{Z}_2$ and t copies of $\mathbb{Z}$,

(3) $\mathrm{PGL}_2(\mathbb{Q}_p) = \Gamma \cdot \mathrm{PGL}_2(\mathbb{Z}_p)$.

Proposition 2.26. *Under the action of $\mathrm{PGL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$:*

(1) Under any basis for V, the matrix $\begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}$ is an inversion.

(2) Fix $\omega \in \Omega$. A basis $\{e_1, e_2\}$ for V can be chosen with respect to which every element of $\mathrm{PGL}(2, \mathbb{Q}_p)$ which fixes ω can be written as $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, with $ad \neq 0$. Furthermore, A is a rotation if and only if $|a|_p = |d|_p = 1$.

(3) Let $\gamma = (\omega, \omega')$ be a doubly infinite geodesic; then there exists a basis of V with respect to which every element A of $\mathrm{PGL}(2, \mathbb{Q}_p) \cap G_\gamma$ can be written as

$$A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \quad \textit{(for } A \cdot \omega = \omega \textit{ and } A \cdot \omega' = \omega' \textit{) or}$$

$$A = \begin{pmatrix} 0 & b \\ c & 0 \end{pmatrix} \quad \textit{(for } A \cdot \omega = \omega' \textit{ and } A \cdot \omega' = \omega \textit{).}$$

2.6 The Standard Quaternion Algebra

For any commutative ring R, let $Q(R)$ be the four dimensional algebra over R with basis $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ and multiplicative relations

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}, \quad \mathbf{jk} = -\mathbf{kj} = \mathbf{i}, \quad \mathbf{ki} = -\mathbf{ik} = \mathbf{j} \quad \text{and} \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Define the *norm* and *trace* from $Q(R)$ into R by

$$\|a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k}\| = a_1^2 + a_2^2 + a_3^2 + a_4^2; \quad \text{and}$$
$$\operatorname{tr}(a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k}) = 2a_1.$$

An element $a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k}$ of $Q(R)$ has a multiplicative inverse in $Q(R)$ if and only if its norm is invertible in R. Its inverse is

$$(a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k})^{-1} = (a_1^2 + a_2^2 + a_3^2 + a_4^2)^{-1}(a_1\,\mathbf{1} - a_2\,\mathbf{i} - a_3\,\mathbf{j} - a_4\,\mathbf{k}).$$

Consequently, $Q(R)$ is a division algebra if and only if the norm of every non-zero element of $Q(R)$ is invertible in R.

Suppose that 2 is invertible in R, and there exist $x, y \in R$ such that $x^2 + y^2 = -1$. Then the algebra $Q(R)$ is isomorphic to $\mathrm{M}_2(R)$ via the isomorphism

$$a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k}$$
$$\longmapsto a_1\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} + a_2\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix} + a_3\begin{pmatrix}x & y\\ y & -x\end{pmatrix} + a_4\begin{pmatrix}y & -x\\ -x & -y\end{pmatrix}$$

and its inverse

$$2\begin{pmatrix}m_{11} & m_{12}\\ m_{21} & m_{22}\end{pmatrix} \longmapsto (m_{11} + m_{22})\,\mathbf{1} + (m_{12} - m_{21})\,\mathbf{i}$$
$$+ (-x(m_{11} - m_{22}) - y(m_{12} + m_{21}))\,\mathbf{j} + (-y(m_{11} - m_{22}) + x(m_{12} + m_{21}))\,\mathbf{k}.$$

In this case, the norm and trace in $Q(R)$ agree with the determinant and trace in $\mathrm{M}_2(R)$.

Consequently, if p and L are odd with p prime, then $Q(\mathbb{Q}_p) \cong \mathrm{M}_2(\mathbb{Q}_p)$ and $Q(\mathbb{Z}/(L)) \cong \mathrm{M}_2(\mathbb{Z}/(L))$. Also, $Q(\mathbb{Q}_2)$ is a division algebra, but $Q(\mathbb{Z}/(2))$ is not.

Let $Q^*(R)$ denote the group of units in $Q(R)$ under multiplication, and let $Q^1(R)$ denote the subgroup of $Q^*(R)$ containing elements of norm 1. If $Q(R) \cong \mathrm{M}_2(R)$, then the same isomorphism gives $Q^*(R) \cong \mathrm{GL}_2(R)$ and $Q^1(R) \cong \mathrm{SL}_2(R)$. In particular, this holds for $R = \mathbb{Q}_p$ and $R = \mathbb{Z}/(L)$, with p and L odd, and p prime.

Further, define $Q^1(\mathbb{Z}[1/p])$ to be the subgroup

$$Q^1(\mathbb{Z}[1/p]) = \left\{ \frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k} \;\middle|\; a_i \in \mathbb{Z} \text{ and } a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n} \right\}.$$

The subgroup $Q^1(\mathbb{Z}[1/p])$ of $Q^1(\mathbb{Q}_p)$ is analogous to the subgroup $\mathrm{SL}_2(\mathbb{Z}[1/p])$ of $\mathrm{SL}_2(\mathbb{Q}_p)$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

The diagram below summarizes the relationships of all these groups and algebras. Arrows indicate inclusions, and equalities indicate isomorphisms.

$$\begin{array}{ccccccc} Q^1(\mathbb{Z}[1/p]) & \longrightarrow & Q^1(\mathbb{Q}_p) & \longrightarrow & Q^*(\mathbb{Q}_p) & \longrightarrow & Q(\mathbb{Q}_p) \\ & & \| & & \| & & \| \\ \mathrm{SL}_2(\mathbb{Z}[1/p]) & \longrightarrow & \mathrm{SL}_2(\mathbb{Q}_p) & \longrightarrow & \mathrm{GL}_2(\mathbb{Q}_p) & \longrightarrow & M_2(\mathbb{Q}_p) \end{array}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER III

The Quotient Graphs $\mathcal{X}_{p,L} = \Gamma_{p,L}\backslash\mathcal{T}_p$ and $\mathcal{X}'_{p,L} = \Gamma'_{p,L}\backslash\mathcal{T}_p$

The group $\mathrm{SL}_2(\mathbb{R})$ acts on the upper half plane

$$\mathcal{H} = \{ z \in \mathbb{C} \mid \mathrm{Im}\, z > 0 \}$$

via the linear fractional transformations

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \cdot z = \frac{m_{11}z + m_{12}}{m_{21}z + m_{22}}.$$

The subgroups of $\mathrm{SL}_2(\mathbb{R})$ can be studied by examining their actions on $\mathcal{H}$.

The *fundamental domain* of a discrete subgroup Γ of $\mathrm{SL}_2(\mathbb{R})$ containing -1 is an open set $\mathcal{D} \subseteq \mathcal{H}$ such that $g \cdot \mathcal{D} \cap \overline{\mathcal{D}} = \emptyset$ for all $g \in \Gamma \setminus \{1\}$ and $\bigcup_{g\in\Gamma} g \cdot \overline{\mathcal{D}} = \mathcal{H}$.

The modular group $\mathrm{SL}_2(\mathbb{Z})$ is an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$. One fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ is the region

$$\{ z \in \mathbb{C} \mid |z| > 1 \text{ and } |\mathrm{Re}\, z| < 1/2 \},$$

shown in Figure 3.1.

For each integer $L > 1$, a natural homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/(L))$ is obtained by mapping the matrix entries $\mathbb{Z} \to \mathbb{Z}/(L)$. The kernel of this homomorphism,

$$\Gamma_L = \left\{ \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \;\middle|\; \begin{array}{c} m_{ij} \in \mathbb{Z}, \quad m_{11}m_{22} - m_{12}m_{21} = 1, \\ m_{11} \equiv m_{22} \equiv 1 \text{ and } m_{12} \equiv m_{21} \equiv 0 \pmod{L} \end{array} \right\},$$

is called the *principle congruence subgroup of degree L*. Also, the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/(L))$ is surjective. Consequently, $\mathrm{SL}_2(\mathbb{Z}/(L))$ is isomorphic to $\mathrm{SL}_2(\mathbb{Z})/\Gamma_L$.

This chapter examines some congruence subgroups of matrix and quaternion groups over the p-adic numbers that are analogous to the congruence group Γ_L. The action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$ is replaced by the action of $\mathrm{SL}_2(\mathbb{Q}_p)$ on the $(p+1)$-regular tree, and the role of the fundamental domain is replaced by the quotient graph of $\mathcal{T}_p$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

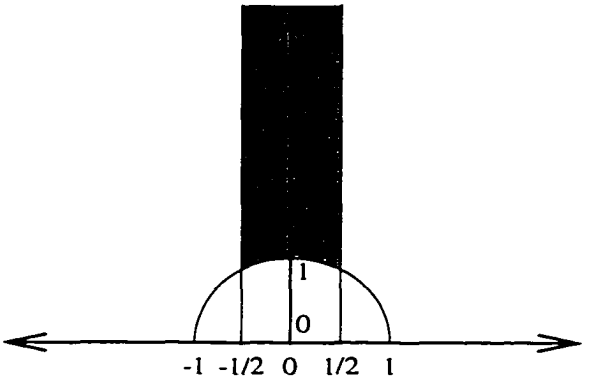


Figure 3.1: A fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

Sections 3.1 and 3.2 examine the actions of $\mathrm{GL}_2(\mathbb{Q}_p)$ and $Q^1(\mathbb{Z}[1/p])$ on $\mathcal{T}_p$. Section 3.3 defines two particular congruence subgroups $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ of $Q(\mathbb{Z}[1/p])$ as the kernels of homomorphisms. Section 3.4 applies the results from Sections 3.2 and 3.3 to obtain formulas for the orders of $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}$ and $Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}$ and for the number of vertices in the quotient graphs induced by their actions on $\mathcal{T}_p$.

3.1 The Action of $M \in \mathrm{GL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$

Let M be a matrix in $\mathrm{GL}_2(\mathbb{Q}_p)$. The action of M on $\mathcal{T}_p$ can be understood by determining which boundary points of $\mathcal{T}_p$ are held fixed by M. These points can be determined by solving

$$M\begin{bmatrix} h \\ k \end{bmatrix} = \begin{bmatrix} \lambda h \\ \lambda k \end{bmatrix} \qquad \text{or} \qquad (M - \lambda I_2)\begin{bmatrix} h \\ k \end{bmatrix} = 0.$$

That is, the fixed boundary points correspond to the eigenvectors of M.

Lemma 3.1. *The characteristic polynomial for $M \in \mathrm{GL}_2(\mathbb{Q}_p)$ is*

$$\lambda^2 - (\mathrm{tr}\, M)\lambda + (\det M).$$

The discriminant of this quadratic polynomial is

$$\Delta = (\mathrm{tr}\, M)^2/4 - (\det M)$$

Write $\Delta = p^\delta \Delta'$, where $\delta \in \mathbb{Z}$ and $\Delta' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, so that Δ is a square in $\mathbb{Q}_p$ if and only if δ is even and Δ' is a square modulo p.

Then M has:

(1) A repeated eigenvalue at $\lambda = (\mathrm{tr}\, M)/2$ if $\Delta = 0$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(2) Two distinct eigenvalues $\lambda = ((\operatorname{tr} M) \pm \sqrt{\Delta})/2$ *if* Δ *is a nonzero square in* $\mathbb{Q}_p$.

(3) No eigenvalues in $\mathbb{Q}_p$ *if* Δ *is a non-square in* $\mathbb{Q}_p$. *However,* M *does have two distinct eigenvalues lying in a quadratic field extension of* $\mathbb{Q}_p$.

Proof. The characteristic polynomial for M is

$$\begin{aligned}\det \begin{pmatrix} m_{11} - \lambda & m_{12} \\ m_{21} & m_{22} - \lambda \end{pmatrix} &= (m_{11} - \lambda)(m_{22} - \lambda) - (m_{12})(m_{21}) \\ &= \lambda^2 - (m_{11} + m_{22})\lambda + (m_{11}m_{22} - m_{12}m_{21}) \\ &= \lambda^2 - (\operatorname{tr} M)\lambda + (\det M).\end{aligned}$$

Solve $\lambda^2 - (\operatorname{tr} M)\lambda + (\det M) = 0$ by completing the square:

$$(\lambda - (\operatorname{tr} M)/2)^2 = (\operatorname{tr} M)^2/4 - (\det M) = \Delta.$$

Write $\Delta = p^\delta \Delta'$. If Δ' is a square modulo p, then $\Delta' \equiv d_0^2 \pmod{p}$ for some d_0. By Hensel's lemma, d_0 can be lifted to a solution to $\Delta' = D'^2$ in the p-adic integers, since p is odd. Then $(p^{\delta/2}D')^2 = p^\delta \Delta' = \Delta$ in $\mathbb{Q}_p$ when δ is even.

On the other hand, if Δ is the square of D in $\mathbb{Q}_p$, then write $D = p^d D'$ with $d \in \mathbb{Z}$ and $D' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Then $\Delta = D^2 = p^{2d}D'^2$, so $\delta = 2d$ is even and $\Delta' = D'^2$ lies in $\mathbb{Z}_p \setminus p\mathbb{Z}_p$.

If Δ is a square in $\mathbb{Q}_p$, then Δ has exactly two square roots, say $\pm\sqrt{\Delta}$. Then

$$\lambda = \left(\operatorname{tr} M \pm \sqrt{\Delta}\right)/2.$$

If $\Delta = p^\delta \Delta'$ is not a square, then δ is odd or Δ' is a non-square modulo p. Fix any non-square $\tau \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. If Δ' is a non-square, then $\Delta'\tau^{-1}$ is a square in $\mathbb{Q}_p$. So:

$$\lambda = \begin{cases} \left(\operatorname{tr} M \pm \sqrt{\tau}\sqrt{\tau^{-1}\Delta}\right)/2 \in \mathbb{Q}_p[\sqrt{\tau}], & \text{if } \delta \text{ even and } \Delta' \text{ non-square;} \\ \left(\operatorname{tr} M \pm \sqrt{p}\sqrt{p^{-1}\Delta}\right)/2 \in \mathbb{Q}_p[\sqrt{p}], & \text{if } \delta \text{ odd and } \Delta' \text{ square;} \\ \left(\operatorname{tr} M \pm \sqrt{p\tau}\sqrt{(p\tau)^{-1}\Delta}\right)/2 \in \mathbb{Q}_p[\sqrt{p\tau}], & \text{if } \delta \text{ odd and } \Delta' \text{ non-square.} \end{cases}$$

□

Proposition 3.2. *Select* $M \in \mathrm{GL}_2(\mathbb{Q}_p)$ *with discriminant* $\Delta = (\operatorname{tr} M)^2/4 - (\det M)$ *a non-zero square in* $\mathbb{Q}_p$. *Write* $\operatorname{tr} M = p^t T'$ *and* $\det M = p^d D'$, *where* $t, d \in \mathbb{Z}$ *and* $T', D' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$.

(1) If $d > 2t$, *then* M *translates a geodesic in* $\mathcal{T}_p$ *by a distance* $d - 2t$.

(2) If $d \leq 2t$, *then* M *fixes every vertex on a geodesic in* $\mathcal{T}_p$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof. By Lemma 3.1, M has distinct eigenvalues $\lambda_1, \lambda_2 \in \mathbb{Q}_p$ with corresponding linearly independent eigenvectors w_1 and w_2. Write $\lambda_1 = p^{l_1}\lambda_1'$ and $\lambda_2 = p^{l_2}\lambda_2'$ with $\lambda_1', \lambda_2' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ and $l_1, l_2 \in \mathbb{Z}$.

The eigenvectors w_1 and w_2 correspond to boundary points of the tree $\mathcal{T}_p$. The vertices lying on the geodesic from w_1 to w_2 are exactly those lattices of the form $v = \mathbb{Z}_p p^a w_1 \oplus \mathbb{Z}_p p^b w_2$, with $a, b \in \mathbb{Z}$. Applying M to each of these vertices yields

$$\begin{aligned} M \cdot (\mathbb{Z}_p p^a w_1 \oplus \mathbb{Z}_p p^b w_2) &= \mathbb{Z}_p p^a \lambda_1 w_1 \oplus \mathbb{Z}_p p^b \lambda_2 w_2 \\ &= \mathbb{Z}_p \lambda_1' p^{a+l_1} w_1 \oplus \mathbb{Z}_p \lambda_2' p^{b+l_2} w_2 = \mathbb{Z}_p p^{a+l_1} w_1 \oplus \mathbb{Z}_p p^{b+l_2} w_2, \end{aligned}$$

and by Proposition 2.11,

$$d(v, M \cdot v) = |l_1 - l_2|\,.$$

From the characteristic polynomial, either $t = \min(l_1, l_2)$ or $l_1 = l_2 \leq t$ because $\lambda_1 + \lambda_2 = \operatorname{tr} M$. Also, $\lambda_1\lambda_2 = \det M$ implies that $l_1 + l_2 = d$.

If $l_1 < l_2$ then $l_1 = t$ and $l_2 = d - t$ so $l_2 - l_1 = d - 2t$. If $l_1 > l_2$ then $l_2 = t$ and $l_1 = d - t$ so $l_1 - l_2 = d - 2t$. In both of these cases, $l_1 \neq l_2$ and $t = \min(l_1, l_2)$, so $d = l_1 + l_2 > 2\min(l_1, l_2) = 2t$, and hence $d > 2t$.

If $l_1 = l_2$ then $l_1 = l_2 = d/2 \leq t$ so $l_1 - l_2 = 0$ and $d \leq 2t$. □

Proposition 3.3. *With respect to the basis $\{e_1, e_2\}$ for V, let v_0 be the vertex in $\mathcal{T}_p$ corresponding to the lattice*

$$\mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Choose any matrix $M = (m_{ij}) \in \mathrm{GL}_2(\mathbb{Q}_p)$. Write $\det M = p^d D'$ and $m_{ij} = p^{\mu_{ij}} m_{ij}'$, where $d, \mu_{ij} \in \mathbb{Z}$ and $D', m_{ij}' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Set $\mu = \min(\mu_{ij})$, so that $p^{-\mu}M \in \mathrm{GL}_2(\mathbb{Z}_p)$. Then $d(v_0, M \cdot v_0) = d - 2\mu$.

Proof. The matrix $p^{-\mu}M$ has determinant $p^{d-2\mu}D'$ and its entries all lie in $\mathbb{Z}_p$. Since the matrices M and $p^{-\mu}M$ have the same action on $\mathcal{T}_p$, it is enough to prove that $d(v_0, M \cdot v_0) = d$ for matrices $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ with at least one $\mu_{ij} = 0$. If $\mu_{21} = 0$ then

$$\begin{aligned} M \cdot v_0 &= \mathbb{Z}_p \begin{bmatrix} m_{11} \\ m_{21} \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{12} \\ m_{22} \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} m_{11} \\ m_{21} \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{12}m_{21} - m_{11}m_{22} \\ m_{22}m_{21} - m_{21}m_{22} \end{bmatrix} \\ &= \mathbb{Z}_p \begin{bmatrix} m_{11}m_{21}^{-1} \\ 1 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} -p^d D' \\ 0 \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} m_{11}m_{21}^{-1} \\ 1 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} p^d \\ 0 \end{bmatrix}. \end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$\text{So} \quad v_0 = \mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{11}m_{21}^{-1} \\ 1 \end{bmatrix} \quad \longmapsto \quad M \cdot v_0 = p^d \mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{11}m_{21}^{-1} \\ 1 \end{bmatrix}.$$

If $\mu_{11} = 0$ then

$$\begin{aligned} M \cdot v_0 &= \mathbb{Z}_p \begin{bmatrix} m_{11} \\ m_{21} \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{12} \\ m_{22} \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} m_{11} \\ m_{21} \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{12}m_{11} - m_{11}m_{12} \\ m_{22}m_{11} - m_{21}m_{12} \end{bmatrix} \\ &= \mathbb{Z}_p \begin{bmatrix} 1 \\ m_{21}m_{11}^{-1} \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 0 \\ p^d D' \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} 1 \\ m_{21}m_{11}^{-1} \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 0 \\ p^d \end{bmatrix}. \end{aligned}$$

$$\text{So} \quad v_0 = \mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 1 \\ m_{11}^{-1}m_{21} \end{bmatrix} \quad \longmapsto \quad M \cdot v_0 = p^d \mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 1 \\ m_{11}^{-1}m_{21} \end{bmatrix}.$$

Similarly, if $\mu_{22} = 0$ then

$$v_0 = \mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{12}m_{22}^{-1} \\ 1 \end{bmatrix} \quad \longmapsto \quad M \cdot v_0 = p^d \mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} m_{12}m_{22}^{-1} \\ 1 \end{bmatrix},$$

and if $\mu_{12} = 0$ then

$$v_0 = \mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 1 \\ m_{12}^{-1}m_{22} \end{bmatrix} \quad \longmapsto \quad M \cdot v_0 = p^d \mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix} \oplus \mathbb{Z}_p \begin{bmatrix} 1 \\ m_{12}^{-1}m_{22} \end{bmatrix}.$$

In each case, vectors w_1 and w_2 exist so that v_0 and $M \cdot v_0$ can be written as

$$v_0 = \mathbb{Z}_p w_1 \oplus \mathbb{Z}_p w_2 \qquad \text{and} \qquad M \cdot v_0 = p^d \mathbb{Z}_p w_1 \oplus \mathbb{Z}_p w_2.$$

By Proposition 2.11, $d(v_0, M \cdot v_0) = d$. □

Now, combine the results from Lemma 3.1 and Propositions 3.2 and 3.3.

Theorem 3.4. *Select $M \in \mathrm{GL}_2(\mathbb{Q}_p)$. Write $\operatorname{tr} M = p^t T'$ and $\det M = p^d D'$, where $t, d \in \mathbb{Z}$ and $T', D' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Let μ be the maximum integer such that $p^{-\mu} M \in \mathrm{GL}_2(\mathbb{Z}_p)$. Let Δ be the discriminant $\Delta = (\operatorname{tr} M)^2/4 - (\det M)$ of the characteristic polynomial. Then M acts on $\mathcal{T}_p$ so that the vertex v_0 is moved a distance $d - 2\mu$, and*

(1) If Δ is a non-zero square in $\mathbb{Q}_p$ and $d > 2t$, then M translates some geodesic in $\mathcal{T}_p$ by a distance $d - 2t$. The distance between v_0 and the translated geodesic is $t - \mu$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(2) If Δ is a non-zero square in $\mathbb{Q}_p$ and $d \leq 2t$, then M fixes every vertex on some geodesic in $\mathcal{T}_p$.

(3) If Δ is a non-square in $\mathbb{Q}_p$ and d is even, then M is a rotation. The distance between v_0 and the closest fixed vertex is $d/2 - \mu$.

(4) If Δ is a non-square in $\mathbb{Q}_p$ and d is odd, then M is an inversion. The distance between v_0 and the center of the inverted edge is $d/2 - \mu$.

(5) If $\Delta = 0$ and M is a scalar multiple of the identity, then M fixes every vertex in $\mathcal{T}_p$.

(6) If $\Delta = 0$ but M is not a scalar multiple of the identity, then M fixes one boundary point and infinitely many vertices. The distance between v_0 and the closest fixed vertex is $t - \mu = d/2 - \mu$.

Proof. If M translates a geodesic, then exactly two boundary points are fixed, so Δ is a square in $\mathbb{Q}_p$ by Lemma 3.1. Consequently, if Δ is a non-square, then M must act as a rotation or an inversion. In this case, by Proposition 3.3, the distance between v_0 and its closest fixed point is $d(v_0, M \cdot v_0)/2 = d/2 - \mu$. Cases (3) and (4) follow.

Cases (1) and (2) follow from Proposition 3.2.

If $\Delta = 0$, then M has one repeated eigenvalue. If the eigenspace is two dimensional, then M is a scalar multiple of the identity. Otherwise, the eigenspace is one dimensional, so M fixes exactly one boundary point, ω, so M is neither a translation nor a reflection. Consequently, M fixes at least one vertex v, and also all vertices in the infinite chain $[v, \omega)$. □

Lemma 3.5. *Fix an odd prime p, and choose $x, y \in \mathbb{Z}_p$ with $x^2 + y^2 = -1$. For $a_i \in \mathbb{Q}_p$, let $M \in \mathrm{M}_2(\mathbb{Q}_p)$ be the matrix*

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = \begin{pmatrix} a_1 + a_3x + a_4y & a_2 + a_3y - a_4x \\ -a_2 + a_3y - a_4x & a_1 - a_3x - a_4y \end{pmatrix}.$$

Write $a_i = p^{\alpha_i} a_i'$ and $m_{ij} = p^{\mu_{ij}} m_{ij}'$, where $\alpha_i, \mu_{ij} \in \mathbb{Z}$ and $a_i', m_{ij}' \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Then $\min(\alpha_i) = \min(\mu_{ij})$.

Proof. The formulas for the m_{ij} in terms of the a_i require $\min(\alpha_i) \leq \min(\mu_{ij})$. The formulas for the a_i in terms of the m_{ij} are

$$2a_1 = m_{11} + m_{22}; \qquad 2a_3 = -x(m_{11} - m_{22}) - y(m_{12} + m_{21}); \quad \text{and}$$
$$2a_2 = m_{12} - m_{21}; \qquad 2a_4 = -y(m_{11} - m_{22}) + x(m_{12} + m_{21}).$$

Since p is odd, these inverse formulas yield $\min(\alpha_i) \geq \min(\mu_{ij})$. □

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Corollary 3.6. *For p an odd prime, select*

$$x = \frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k} \in Q^1(\mathbb{Z}[1/p])$$

with $a_i \in \mathbb{Z}$ and not all of the a_i divisible by p. So $a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n}$ and $\operatorname{tr} x = 2a_1/p^n$. Let p^t be the largest power of p dividing a_1. Then:

(1) If $n = 0$, then x is a rotation that fixes the vertex v_0.

(2) If $n > 0$, then x translates some geodesic a distance of $2n - 2t$. The vertex v_0 is moved a distance $2n$, and the distance between v_0 and the geodesic translated by x is t.

Proof. Let M be the matrix in $\mathrm{GL}_2(\mathbb{Z}_p)$ identified with $p^n x$. Then $\det M = p^{2n} \geq a_1^2$, $\operatorname{tr} M = \operatorname{tr}(p^n x) = 2a_1$, and M and x have identical actions on $\mathcal{T}_p$. By Lemma 3.5, not all of the entries of M are divisible by p. Now, apply Proposition 3.4 with $\mu = 0$, $t = t$ and $d = 2n$. The discriminant of M is

$$\Delta = (\operatorname{tr} M)^2/4 - (\det M) = -(p^{2n} - a_1^2) = -(a_2^2 + a_3^2 + a_4^2).$$

If $\Delta = 0$, then $a_1^2 = p^{2n}$ so x is the identity and $n = t = 0$.

If $\Delta \neq 0$, then $a_1^2 < p^{2n}$ so $t < n$. Then $\Delta \equiv a_1^2 \pmod{p^{2n}}$ is a square in $\mathbb{Q}_p$. Now apply parts (1) and (3) of Proposition 3.4. □

3.2 The Action of $Q^1(\mathbb{Z}[1/p])$ on $\mathcal{T}_p$ and Quotient Actions

The group $Q^1(\mathbb{Z}[1/p])$ embedded in $\mathrm{GL}_2(\mathbb{Q}_p)$ acts on the regular tree $\mathcal{T}_p$ of degree $p + 1$. Let $\Gamma \subseteq Q^1(\mathbb{Z}[1/p])$ be a normal subgroup of finite index. Let $\mathcal{X}$ be the quotient graph $\mathcal{X} = \Gamma\backslash\mathcal{T}_p$, so vertices $v_1, v_2 \in \mathcal{T}_p$ are identified $\overline{v}_1 = \overline{v}_2$ in $\mathcal{X}$ if and only if there exists $a \in \Gamma$ with $a \cdot v_1 = v_2$. The quotient group $Q^1(\mathbb{Z}[1/p])/\Gamma$ acts naturally on the quotient graph $\mathcal{X}$.

The goal of this section is to establish a relationship between the number of vertices in $\mathcal{X}$ and the order of the quotient group $Q^1(\mathbb{Z}[1/p])/\Gamma$. A later section will consider the structure of $Q^1(\mathbb{Z}[1/p])/\Gamma$.

Definition 3.7. With respect to the base $\{e_1, e_2\}$, let v_0 denote the vertex in $\mathcal{T}_p$ identified with the lattice $\mathbb{Z}_p\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right] \oplus \mathbb{Z}_p\left[\begin{smallmatrix}0\\1\end{smallmatrix}\right]$. Split the vertices of $\mathcal{T}_p$ into two disjoint sets according to the distance, modulo 2, of the vertices from v_0.

$$V\mathcal{T}_p^0 = \{\, v \in V\mathcal{T}_p \mid d(v_0, v) \equiv 0 \pmod 2 \,\}$$
$$V\mathcal{T}_p^1 = \{\, v \in V\mathcal{T}_p \mid d(v_0, v) \equiv 1 \pmod 2 \,\}.$$

So $V\mathcal{T}_p = V\mathcal{T}_p^0 \cup V\mathcal{T}_p^1$ and $V\mathcal{T}_p^0 \cap V\mathcal{T}_p^1 = \emptyset$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Definition 3.8. Define a map of sets $\alpha : Q^1(\mathbb{Z}[1/p]) \longrightarrow \mathcal{T}_p$ by $\alpha(x) = x \cdot v_0$.

The first goal is to show that the image of α in $\mathcal{T}_p$ is exactly $\mathcal{T}_p^0$.

Lemma 3.9. *For $x \in Q^1(\mathbb{Z}[1/p])$, $x \cdot v_0 = v_0$ if and only if $x \in \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$. Consequently, for each $v \in \alpha(Q^1(\mathbb{Z}[1/p]))$, there are exactly eight $x \in Q^1(\mathbb{Z}[1/p])$ such that $x \cdot v_0 = v$.*

Proof. Write

$$x = \frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k}$$

with $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ and $a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n}$ and not all of a_1, a_2, a_3 and a_4 divisible by p. By Proposition 3.4, x translates v_0 distance $2n$, so

$$x \cdot v_0 = v_0 \iff n = 0 \iff a_1^2 + a_2^2 + a_3^2 + a_4^2 = 1 \iff x \in \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}.$$

Next, suppose $v = z \cdot v_0$ for $z \in Q^1(\mathbb{Z}[1/p])$. Then for all $x \in Q^1(\mathbb{Z}[1/p])$,

$$\begin{aligned} x \cdot v_0 = v &\iff x \cdot v_0 = z \cdot v_0 \iff (z^{-1}x) \cdot v_0 = v_0 \\ &\iff z^{-1}x \in \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\} \iff x \in \{\pm z\mathbf{1}, \pm z\mathbf{i}, \pm z\mathbf{j}, \pm z\mathbf{k}\}. \end{aligned}$$

□

Theorem (Jacobi). *For each positive integer n, let $\sigma'(n)$ equal the sum of those divisors of n that are not divisible by 4. Then the equation $a_1^2 + a_2^2 + a_3^2 + a_4^2 = n$ has exactly $8\sigma'(n)$ integral solutions.*

Proof. See page 30 of [Gro85]. □

Lemma 3.10. *If $v \in \mathcal{T}_p$ and $d(v_0, v) = 2$, then $x \cdot v_0 = v$ for some $x \in Q^1(\mathbb{Z}[1/p])$.*

Proof. By Jacobi's Theorem, $a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^2$ has exactly $8\sigma'(p^2) = 8(1 + p + p^2)$ integral solutions. By Lemma 3.9, exactly eight of these fix v_0, namely

$$\pm p\mathbf{1},\ \pm p\mathbf{i},\ \pm p\mathbf{j},\ \text{and}\ \pm p\mathbf{k}.$$

By Proposition 3.4, the remaining $8(p + p^2)$ solutions correspond to group elements

$$x = \frac{a_1}{p}\,\mathbf{1} + \frac{a_2}{p}\,\mathbf{i} + \frac{a_3}{p}\,\mathbf{j} + \frac{a_4}{p}\,\mathbf{k} \in Q^1(\mathbb{Z}[1/p])$$

which displace v_0 by distance 2. Then by Lemma 3.9, there are exactly $p + p^2$ vertices in the image $\alpha(Q^1(\mathbb{Z}[1/p]))$ of distance 2 from v_0.

Now, in the $(p+1)$-regular tree T_p, there are $p + 1$ vertices adjacent to the vertex v_0, and $(p+1)p$ vertices of distance 2 away from the vertex v_0, so every vertex v with $d(v_0, v) = 2$ must lie in the image $\alpha(Q^1(\mathbb{Z}[1/p]))$. □

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proposition 3.11. *The image $\alpha(Q^1(\mathbb{Z}[1/p]))$ is exactly $\mathcal{T}_p^0$.*

Proof. For each $m \in \mathbb{N}$, set

$$S_m = \{ v \in \mathcal{T}_p \mid d(v_0, v) = m \}, \qquad \text{so} \qquad \mathcal{T}_p^0 = \bigcup_{m \text{ even}} S_m.$$

By Proposition 3.4, $d(v_0, x \cdot v_0)$ is even for every $x \in Q^1(\mathbb{Z}[1/p])$. Consequently, $\alpha(Q^1(\mathbb{Z}[1/p])) \subseteq \mathcal{T}_p^0$. To show $\mathcal{T}_p^0 \subseteq \alpha(Q^1(\mathbb{Z}[1/p]))$, apply induction on m. First, $S_0 = \{v_0\} \subseteq \alpha(Q^1(\mathbb{Z}[1/p]))$ because $1 \cdot v_0 = v_0$. Also, $S_2 \subseteq \alpha(Q^1(\mathbb{Z}[1/p]))$ by the previous lemma.

Now, fix some even $m \geq 4$, and assume $S_{m-2} \subseteq \alpha(Q^1(\mathbb{Z}[1/p]))$. Choose any vertex $v \in S_m$, and then let v' denote the unique vertex in S_{m-2} with $d(v', v) = 2$. By the inductive hypothesis, $v' \in \alpha(Q^1(\mathbb{Z}[1/p]))$, so choose $x \in Q^1(\mathbb{Z}[1/p])$ with $x \cdot v_0 = v'$. Then

$$d(v_0, x^{-1} \cdot v) = d(x \cdot v_0, v) = d(v', v) = 2,$$

so $x^{-1} \cdot v \in S_2$. Since $S_2 \subseteq \alpha(Q^1(\mathbb{Z}[1/p]))$, choose $y \in Q^1(\mathbb{Z}[1/p])$ with $y \cdot v_0 = x^{-1} \cdot v$. Then $(xy) \cdot v_0 = v$, so $\alpha(xy) = v$. Therefore, $S_m \subseteq \alpha(Q^1(\mathbb{Z}[1/p]))$ for all even m. □

Definition 3.12. Let Γ be any normal subgroup of $Q^1(\mathbb{Z}[1/p])$ of finite index. The action of $Q^1(\mathbb{Z}[1/p])$ on $\mathcal{T}_p$ induces a quotient graph $\mathcal{X} = \Gamma \backslash \mathcal{T}_p$. The quotient group $Q^1(\mathbb{Z}[1/p])/\Gamma$ acts naturally on $\mathcal{X}$. Let $V\mathcal{X}^0$ and $V\mathcal{X}^1$ denote the images in $V\mathcal{X}$ of $V\mathcal{T}_p^0$ and $V\mathcal{T}_p^1$ respectively. Then $V\mathcal{X} = V\mathcal{X}^0 \cup V\mathcal{X}^1$, and $V\mathcal{X}^0 \cap V\mathcal{X}^1 = \emptyset$ because $d(v, x \cdot v)$ is even for all $x \in Q^1(\mathbb{Z}[1/p])$ and $v \in \mathcal{T}_p$.

Definition 3.13. The map $\alpha : Q^1(\mathbb{Z}[1/p]) \longrightarrow \mathcal{T}_p$ induces a map

$$\overline{\alpha} : Q^1(\mathbb{Z}[1/p])/\Gamma \longrightarrow \mathcal{X}.$$

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma & \longrightarrow & Q^1(\mathbb{Z}[1/p]) & \longrightarrow & Q^1(\mathbb{Z}[1/p])/\Gamma & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha|_\Gamma} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \overline{\alpha}} & & \\ & & \mathcal{T}_p & & \mathcal{T}_p & \longrightarrow & \Gamma \backslash \mathcal{T}_p & & \end{array}$$

Note that $\overline{\alpha}$ is well-defined, because if $x, y \in Q^1(\mathbb{Z}[1/p])$ with $\overline{x} = \overline{y}$ in $Q^1(\mathbb{Z}[1/p])/\Gamma$, then $xy^{-1} \in \Gamma$, so $x = ya$ for some $a \in \Gamma$. Then

$$\overline{\alpha}(\overline{x}) = \overline{x \cdot v_0} = \overline{(ya) \cdot v_0} = \overline{y \cdot (a \cdot v_0)} = \overline{y \cdot v_0} = \overline{\alpha}(\overline{y})$$

since $\overline{a \cdot v_0} = \overline{v}_0$ in $\mathcal{X} = \Gamma \backslash \mathcal{T}_p$.

Lemma 3.14. *$\mathcal{X} = \Gamma \backslash \mathcal{T}_p$ is bipartite, and $|V\mathcal{X}^0| = |V\mathcal{X}^1|$.*

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof. Every vertex in $V\mathcal{T}_p$ has degree $p+1$, and every edge in $E\mathcal{T}_p$ has one endpoint in $V\mathcal{T}_p^0$ and one in $V\mathcal{T}_p^1$, because $\mathcal{T}_p$ is bipartite. Consequently, every vertex in $\mathcal{X}$ has degree $p+1$, and every edge in $E\mathcal{X}$ has one endpoint in $V\mathcal{X}^0$ and one in $V\mathcal{X}^1$, so $\mathcal{X}$ is bipartite.

The quotient group $Q^1(\mathbb{Z}[1/p])/\Gamma$ is finite and the map $\overline{\alpha} : Q^1(\mathbb{Z}[1/p])/\Gamma \longrightarrow V\mathcal{X}^0$ is surjective, so $|V\mathcal{X}^0|$ is finite. Counting the number of edges in $\mathcal{X}$ two different ways yields:

$$(p+1)\left|V\mathcal{X}^0\right| = |E\mathcal{X}| = (p+1)\left|V\mathcal{X}^1\right|.$$

□

Proposition 3.15. *Suppose $\Gamma \subseteq Q^1(\mathbb{Z}[1/p])$ is a normal subgroup of finite index. Put $\mathcal{X} = \Gamma\backslash\mathcal{T}_p$.*

(1) If $-\mathbf{1}, \mathbf{i}, \mathbf{j} \in \Gamma$, then $|V\mathcal{X}| = 2\,|Q^1(\mathbb{Z}[1/p])/\Gamma|$.

(2) If $-\mathbf{1} \in \Gamma$ but $\mathbf{i}, \mathbf{j}, \mathbf{k} \notin \Gamma$, then $2\,|V\mathcal{X}| = |Q^1(\mathbb{Z}[1/p])/\Gamma|$.

(3) If $-\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k} \notin \Gamma$, then $4\,|V\mathcal{X}| = |Q^1(\mathbb{Z}[1/p])/\Gamma|$.

Proof. Lemma 3.14 implies $|V\mathcal{X}| = 2\,|V\mathcal{X}^0|$. For each $\overline{v} \in V\mathcal{X}^0$, there is at least one coset $x\Gamma$ with $\overline{\alpha}(x\Gamma) = \overline{v}$ because $\overline{\alpha} : Q^1(\mathbb{Z}[1/p])/\Gamma \longrightarrow V\mathcal{X}^0$ is surjective. Then

$$\overline{\alpha}(x\mathbf{1}\Gamma) = \overline{\alpha}(x\mathbf{i}\Gamma) = \overline{\alpha}(x\mathbf{j}\Gamma) = \overline{\alpha}(x\mathbf{k}\Gamma) = \overline{v}.$$

Suppose $y\Gamma \in Q^1(\mathbb{Z}[1/p])/\Gamma$ also satisfies $\overline{\alpha}(y\Gamma) = \overline{v}$. Then $(x\Gamma)\cdot\overline{v}_0 = (y\Gamma)\cdot\overline{v}_0 = \overline{v}$ in $\mathcal{X}$, so there exist $g, h \in \Gamma$ such that $(xg)\cdot v_0 = (yh)\cdot v_0 = v$ in $\mathcal{T}_p$. Then $(g^{-1}x^{-1}yh)\cdot v_0 = v_0$ so $g^{-1}x^{-1}yh \in \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ by Lemma 3.9. Therefore, $y\Gamma \in \{\pm x\mathbf{1}\Gamma, \pm x\mathbf{i}\Gamma, \pm x\mathbf{j}\Gamma, \pm x\mathbf{k}\Gamma\}$.

In Case (1), $\{\pm x\mathbf{1}\Gamma, \pm x\mathbf{i}\Gamma, \pm x\mathbf{j}\Gamma, \pm x\mathbf{k}\Gamma\} = \{x\Gamma\}$ contains just one coset, so $|V\mathcal{X}^0| = |Q^1(\mathbb{Z}[1/p])|$.

In Case (2), $\{\pm x\mathbf{1}\Gamma, \pm x\mathbf{i}\Gamma, \pm x\mathbf{j}\Gamma, \pm x\mathbf{k}\Gamma\} = \{\pm x\mathbf{1}\Gamma, x\mathbf{i}\Gamma, x\mathbf{j}\Gamma, x\mathbf{k}\Gamma\}$ contains four distinct cosets, so $|V\mathcal{X}^0| = 4\,|Q^1(\mathbb{Z}[1/p])|$.

In Case (3), all eight of the cosets in $\{\pm x\mathbf{1}\Gamma, \pm x\mathbf{i}\Gamma, \pm x\mathbf{j}\Gamma, \pm x\mathbf{k}\Gamma\}$ are distinct, so $|V\mathcal{X}^0| = 8\,|Q^1(\mathbb{Z}[1/p])|$. □

Corollary 3.16. *The bipartite quotient graph $Q^1(\mathbb{Z}[1/p])\backslash\mathcal{T}_p$ contains two vertices.*

Proof. Apply Case (1) of Proposition 3.15 with $\Gamma = Q^1(\mathbb{Z}[1/p])$. □

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

3.3 Two Congruence Subgroups over $\mathbb{Q}_p$

All of the groundwork is now in place. In the remainder of this chapter, attention is restricted to two specific collections of congruence subgroups of $Q^1(\mathbb{Z}[1/p])$.

The definitions below make one abuse of notation. If L is even and $a' \in \mathbb{Z}/(2L)$, then the value of a'^2 modulo $2L$ depends only on the equivalence class of a' modulo L, because

$$(a' + L)^2 = a'^2 + 2a'L + L^2 \equiv a'^2 \pmod{2L}.$$

Consequently, for $a \in \mathbb{Z}/(L)$ and L even, the notation "$a^2 \equiv m \pmod{2L}$" indicates that each $a' \in \mathbb{Z}/(2L)$ with $a' \equiv a \pmod{L}$ satisfies $a'^2 \equiv m \pmod{2L}$.

Definition 3.17. For all positive integers L, $Q^1(\mathbb{Z}/(L))$ is the group

$$Q^1(\mathbb{Z}/(L)) = \left\{ \bar{a}_1\,\mathbf{1} + \bar{a}_2\,\mathbf{i} + \bar{a}_3\,\mathbf{j} + \bar{a}_4\,\mathbf{k} \;\middle|\; \bar{a}_i \in \mathbb{Z}/(L); \sum_{i=1}^{4} \bar{a}_i^2 \equiv 1 \pmod{L} \right\}.$$

Define $N(\mathbb{Z}/(L))$ to be the central, normal subgroup

$$N(\mathbb{Z}/(L)) = \left\{ \bar{a}_1\,\mathbf{1} + 0\,\mathbf{i} + 0\,\mathbf{j} + 0\,\mathbf{k} \;\middle|\; \bar{a}_1 \in \mathbb{Z}/(L) \text{ and } \bar{a}_1^2 \equiv 1 \pmod{L} \right\}.$$

and set

$$P^1(\mathbb{Z}/(L)) = Q^1(\mathbb{Z}/(L)) \;/\; N(\mathbb{Z}/(L)).$$

Also, for all even L, define $Q_e^1(\mathbb{Z}/(L))$ and $P_e^1(\mathbb{Z}/(L))$ to be the groups

$$Q_e^1(\mathbb{Z}/(L)) = \left\{ \bar{a}_1\,\mathbf{1} + \bar{a}_2\,\mathbf{i} + \bar{a}_3\,\mathbf{j} + \bar{a}_4\,\mathbf{k} \;\middle|\; \bar{a}_i \in \mathbb{Z}/(L); \sum_{i=1}^{4} \bar{a}_i^2 \equiv 1 \pmod{2L} \right\};$$

$$\begin{aligned} N_e(\mathbb{Z}/(L)) &= N(\mathbb{Z}/(L)) \cap Q_e^1(\mathbb{Z}/(L)) \\ &= \left\{ \bar{a}_1\,\mathbf{1} + 0\,\mathbf{i} + 0\,\mathbf{j} + 0\,\mathbf{k} \;\middle|\; \bar{a}_1 \in \mathbb{Z}/(L) \text{ and } \bar{a}_1^2 \equiv 1 \pmod{2L} \right\}; \quad \text{and} \end{aligned}$$

$$P_e^1(\mathbb{Z}/(L)) = Q_e^1(\mathbb{Z}/(L)) \;/\; N_e(\mathbb{Z}/(L)).$$

Definition 3.18. Define $\phi : Q^1(\mathbb{Z}[1/p]) \longrightarrow Q^1(\mathbb{Z}/(L))$ by

$$\frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k} \quad \longmapsto \quad \overline{a_1 p^{-n}}\,\mathbf{1} + \overline{a_2 p^{-n}}\,\mathbf{i} + \overline{a_3 p^{-n}}\,\mathbf{j} + \overline{a_4 p^{-n}}\,\mathbf{k}.$$

For each integer $L > 1$ not divisible by p, define $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ to be the groups

$$\Gamma_{p,L} = \left\{ \frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k} \in Q^1(\mathbb{Z}[1/p]) \;\middle|\; a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{L} \right\};$$

$$\Gamma'_{p,L} = \left\{ \frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k} \in \Gamma_{p,L} \;\middle|\; a_1 \equiv p^n \pmod{L} \right\}.$$

So $\Gamma'_{p,L} \leq \Gamma_{p,L} < Q^1(\mathbb{Z}[1/p]) < Q^1(\mathbb{Q}_p)$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Lemma 3.19. *The kernel of ϕ is $\phi^{-1}(\{\mathbf{1}\}) = \Gamma'_{p,L}$. The inverse image of $N(\mathbb{Z}/(L))$ is $\phi^{-1}(N(\mathbb{Z}/(L))) = \Gamma_{p,L}$.*

Proof. Choose

$$x = \frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \in Q^1(\mathbb{Z}[1/p]).$$

Then

$$x \in \Gamma_{p,L} \iff a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{L}$$
$$\iff a_2 p^{-n} \equiv a_3 p^{-n} \equiv a_4 p^{-n} \equiv 0 \pmod{L} \iff \phi(x) = \mathbf{1},$$

because $\gcd(p, L) = 1$. Now for all $x \in \Gamma_{p,L}$,

$$x \in \Gamma'_{p,L} \iff a_1 \equiv p^n \pmod{L} \iff a_1 p^{-n} \equiv 1 \pmod{L} \iff \phi(x) \in N(\mathbb{Z}/(L)).$$

□

In the previous section, Proposition 3.15 established a correspondence between $|V\mathcal{X}|$ and $|Q^1(\mathbb{Z}[1/p])/\Gamma|$ for $\mathcal{X} = \Gamma\backslash\mathcal{T}_p$. Also, $Q^1(\mathbb{Z}[1/p])/\Gamma$ acts on the graph $\Gamma\backslash\mathcal{T}_p$, so information about the structure of $Q^1(\mathbb{Z}[1/p])/\Gamma$ translates into information about the symmetries of $\Gamma\backslash\mathcal{T}_p$.

If $\phi : Q^1(\mathbb{Z}[1/p]) \to Q^1(\mathbb{Z}/(L))$ is surjective, then $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L} \cong P^1(\mathbb{Z}/(L))$ and $Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L} \cong Q^1(\mathbb{Z}/(L))$. In fact, the truth is a little more complicated.

Corollary 7.10 (p. 129). *Let p and L be positive integers with p prime and L not divisible by p. Let a_1, a_2, a_3 and a_4 be integers with $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{L}$. Then there exist integers y_1, y_2, y_3, y_4 and n such that $y_1^2 + y_2^2 + y_3^2 + y_4^2 = p^{2n}$ and $y_i \equiv a_i \pmod{L}$ for $i = 1, 2, 3, 4$ if and only if either*

(1) L is odd,

(2) L is even and $p^{2m} \equiv 1 + L \pmod{2L}$ for some positive integer m, or

(3) L is even and $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L}$.

Proof. This corollary shall be proved in Chapter VII as a consequence of Theorem 6.2. □

Proposition 3.20. *If L is odd or if L is even but $p^{2m} \equiv L + 1 \pmod{2L}$ for some $m \in \mathbb{Z}$, then the map $\phi : Q^1(\mathbb{Z}[1/p]) \longrightarrow Q^1(\mathbb{Z}/(L))$ is surjective. If L is even and $p^{2m} \not\equiv L + 1 \pmod{2L}$ for all $m \in \mathbb{Z}$, then the image $\phi(Q^1(\mathbb{Z}[1/p]))$ is exactly $Q_e^1(\mathbb{Z}/(L))$.*

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof. Choose some $a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k} \in Q^1(\mathbb{Z}/(L))$. If L is odd or if L is even and $p^{2m} \equiv L + 1 \pmod{2L}$ for some $m \in \mathbb{Z}$, then Corollary 7.10 implies that there exist integers y_1, y_2, y_3, y_4 and n such that $y_1^2 + y_2^2 + y_3^2 + y_4^2 = p^{2n}$ and $y_i \equiv a_i \pmod{L}$ for each i. Put

$$x = \frac{y_1}{p^n}\,\mathbf{1} + \frac{y_2}{p^n}\,\mathbf{i} + \frac{y_3}{p^n}\,\mathbf{j} + \frac{y_4}{p^n}\,\mathbf{k} \in Q^1(\mathbb{Z}[1/p]).$$

Then $\phi(x) = a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k}$.

On the other hand, if L is even and $p^{2m} \not\equiv L + 1 \pmod{2L}$ for all $m \in \mathbb{Z}$, then condition (3) of Corollary 7.10 implies that $a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k} \in Q^1(\mathbb{Z}/(L))$ is in the image of ϕ if and only if $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L}$. This condition holds exactly for the elements of $Q_e^1(\mathbb{Z}/(L))$. □

Proposition 3.20 can also be proven as a consequence of strong approximation for semi-simple groups over a number field.

Theorem 3.21. *Let p and L be positive integers with p prime and L not divisible by p. Let $\phi : Q^1(\mathbb{Z}[1/p]) \longrightarrow Q^1(\mathbb{Z}/(L))$ be the homomorphism given by*

$$\frac{a_1}{p^n}\,\mathbf{1} + \frac{a_2}{p^n}\,\mathbf{i} + \frac{a_3}{p^n}\,\mathbf{j} + \frac{a_4}{p^n}\,\mathbf{k} \quad \longmapsto \quad \overline{a_1 p^{-n}}\,\mathbf{1} + \overline{a_2 p^{-n}}\,\mathbf{i} + \overline{a_3 p^{-n}}\,\mathbf{j} + \overline{a_4 p^{-n}}\,\mathbf{k}.$$

(1) If L is odd or if L is even but $p^{2m} \equiv L + 1 \pmod{2L}$ for some $m \in \mathbb{Z}$, then the maps

$$\overline{\phi} : Q^1(\mathbb{Z}[1/p]) \,/\, \Gamma_{p,L} \longrightarrow P^1(\mathbb{Z}/(L)) \quad \textit{and}$$
$$\overline{\phi}' : Q^1(\mathbb{Z}[1/p]) \,/\, \Gamma'_{p,L} \longrightarrow Q^1(\mathbb{Z}/(L))$$

induced by ϕ are group isomorphisms.

(2) If L is even and $p^{2m} \not\equiv L + 1 \pmod{2L}$ for all $m \in \mathbb{Z}$, then the maps

$$\overline{\phi} : Q^1(\mathbb{Z}[1/p]) \,/\, \Gamma_{p,L} \longrightarrow P_e^1(\mathbb{Z}/(L)) \quad \textit{and}$$
$$\overline{\phi}' : Q^1(\mathbb{Z}[1/p]) \,/\, \Gamma'_{p,L} \longrightarrow Q_e^1(\mathbb{Z}/(L))$$

induced by ϕ are group isomorphisms.

Proof of (1). By Proposition 3.20, the map ϕ is surjective. By Lemma 3.19,

$$\phi^{-1}(\{\mathbf{1}\}) = \Gamma'_{p,L} \quad \text{and} \quad \phi^{-1}(N(\mathbb{Z}/(L))) = \Gamma_{p,L}.$$

$N(\mathbb{Z}/(L))$ is central and hence normal in $Q^1(\mathbb{Z}/(L))$. Consequently, $\overline{\phi}$ and $\overline{\phi}'$ are isomorphisms by the first isomorphism theorem of groups.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof of (2). By Proposition 3.20, the image of the map ϕ in $Q^1(\mathbb{Z}/(L))$ is $Q_e^1(\mathbb{Z}/(L))$. Since

$$N_e(\mathbb{Z}/(L)) = N(\mathbb{Z}/(L)) \cap P_e^1(\mathbb{Z}/(L)),$$

Lemma 3.19, implies that

$$\phi^{-1}(\{1\}) = \Gamma'_{p,L} \quad \text{and} \quad \phi^{-1}(N_e(\mathbb{Z}/(L))) = \phi^{-1}(N(\mathbb{Z}/(L))) = \Gamma_{p,L}.$$

The first isomorphism theorem of groups complete the proof. □

The following diagrams illustrate the homomorphisms in part (1) of Theorem 3.21 for $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L} \cong P^1(\mathbb{Z}/(L))$:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma_{p,L} & \longrightarrow & Q^1(\mathbb{Z}[1/p]) & \longrightarrow & Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi|_{\Gamma_{p,L}}} & & \downarrow{\scriptstyle \phi} & & \cong\downarrow{\scriptstyle \bar{\phi}} & & \\ 1 & \longrightarrow & N(\mathbb{Z}/(L)) & \longrightarrow & Q^1(\mathbb{Z}/(L)) & \longrightarrow & P^1(\mathbb{Z}/(L)) & \longrightarrow & 1 \end{array}$$

and for $Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L} \cong Q^1(\mathbb{Z}/(L))$:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma'_{p,L} & \longrightarrow & Q^1(\mathbb{Z}[1/p]) & \longrightarrow & Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \phi|_{\Gamma_{p,L}}} & & \downarrow{\scriptstyle \phi} & & \cong\downarrow{\scriptstyle \bar{\phi}'} & & \\ 1 & \longrightarrow & 1 & \longrightarrow & Q^1(\mathbb{Z}/(L)) & \longrightarrow & Q^1(\mathbb{Z}/(L)) & \longrightarrow & 1. \end{array}$$

Proposition 3.22. *(1) If $L = L_1L_2$ and $\gcd(L_1, L_2) = 1$, then*

$$\begin{aligned} Q^1(\mathbb{Z}/(L)) &\cong Q^1(\mathbb{Z}/(L_1)) \times Q^1(\mathbb{Z}/(L_2)); \\ P^1(\mathbb{Z}/(L)) &\cong P^1(\mathbb{Z}/(L_1)) \times P^1(\mathbb{Z}/(L_2)); \text{ and} \\ N(\mathbb{Z}/(L)) &\cong N(\mathbb{Z}/(L_1)) \times N(\mathbb{Z}/(L_2)). \end{aligned}$$

Also, if $L = L_1L_2$, $\gcd(L_1, L_2) = 1$ and L_1 is even, then

$$\begin{aligned} Q_e^1(\mathbb{Z}/(L)) &\cong Q_e^1(\mathbb{Z}/(L_1)) \times Q^1(\mathbb{Z}/(L_2)); \\ P_e^1(\mathbb{Z}/(L)) &\cong P_e^1(\mathbb{Z}/(L_1)) \times P^1(\mathbb{Z}/(L_2)); \text{ and} \\ N_e(\mathbb{Z}/(L)) &\cong N_e(\mathbb{Z}/(L_1)) \times N(\mathbb{Z}/(L_2)). \end{aligned}$$

(2) If L is odd, then $Q^1(\mathbb{Z}/(L)) \cong \mathrm{SL}_2(\mathbb{Z}/(L))$ and $P^1(\mathbb{Z}/(L)) \cong \mathrm{PSL}_2(\mathbb{Z}/(L))$.

Proof of (1). The first three identities follow from the Chinese remainder theorem. The second three hold because

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L_1L_2}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$\iff a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \,(\mathrm{mod}\, 2L_1) \quad \text{and} \quad a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \,(\mathrm{mod}\, L_2),$$

and

$$a_1^2 \equiv 1 \,(\mathrm{mod}\, 2L_1L_2) \iff a_1^2 \equiv 1 \,(\mathrm{mod}\, 2L_1) \quad \text{and} \quad a_1^2 \equiv 1 \,(\mathrm{mod}\, L_2).$$

Proof of (2). Refer back to Section 2.6. □

Proposition 3.23. *For even L, $Q_e^1(\mathbb{Z}/(L))$ is normal in $Q^1(\mathbb{Z}/(L))$ of index 2. If L also is divisible by 8, then $N_e(\mathbb{Z}/(L))$ is normal in $N(\mathbb{Z}/(L))$ of index 2. and $|P_e^1(\mathbb{Z}/(L))| = |P^1(\mathbb{Z}/(L))|$. If L is even but not divisible by 8, then $N_e(\mathbb{Z}/(L)) = N(\mathbb{Z}/(L))$ and so $P_e^1(\mathbb{Z}/(L))$ is normal in $P^1(\mathbb{Z}/(L))$ of index 2.*

Proof. Define $\theta : Q^1(\mathbb{Z}/(L)) \longrightarrow \mathbb{Z}/(2L)$ by

$$a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k} \longmapsto a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Since $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \,(\mathrm{mod}\, L)$, the image of θ is a subgroup of $\{1, 1+L\}$ within $\mathbb{Z}/(2L)$. This image includes $1+L$ because every positive integer can be written as the sum of four squares. Hence, $\theta^{-1}(\{1, 1+L\}) = Q^1(\mathbb{Z}/(L))$ and $\theta^{-1}(\{1\}) = Q_e^1(\mathbb{Z}/(L))$.

Next, restrict θ to $N(\mathbb{Z}/(L))$. If L is divisible by 8, then

$$(1 + L/2)^2 = 1 + L + L^2/4 \equiv 1 + L \,(\mathrm{mod}\, 2L),$$

so $1+L \in \theta(N(\mathbb{Z}/(L))$. Then $\theta^{-1}(\{1, 1+L\}) = N(\mathbb{Z}/(L))$ and $\theta^{-1}(\{1\}) = N_e(\mathbb{Z}/(L))$.

If L is even but not divisible by 8, then $N(\mathbb{Z}/(L)) = N_e(\mathbb{Z}/(L))$, because

$$a_1^2 \equiv 1 \bmod 2 \iff a_1^2 \equiv 1 \bmod 4 \iff a_1^2 \equiv 1 \bmod 8$$

for all $a_1 \in \mathbb{Z}$. □

3.4 Vertex Count

The goal of Section 3.4 is to combine the results of Theorem 3.21 and Propositions 3.15 and 3.23 with some techniques from number theory to obtain formulas for the order of the groups

$$Q^1(\mathbb{Z}[1/p]) \,/\, \Gamma_{p,L} \qquad \text{and} \qquad Q^1(\mathbb{Z}[1/p]) \,/\, \Gamma'_{p,L},$$

and formulas for the number of vertices in the graphs

$$\mathcal{X}_{p,L} = \Gamma_{p,L} \backslash \mathcal{T}_p \qquad \text{and} \qquad \mathcal{X}'_{p,L} = \Gamma'_{p,L} \backslash \mathcal{T}_p.$$

Corollary 3.24 combines Theorem 3.21, Propositions 3.15 and 3.23, and the fact that if L is even and $p^{2m} \equiv L + 1 \,(\mathrm{mod}\, 2L)$ for some $m \in \mathbb{Z}$, then L is divisible by 8.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Corollary 3.24. *Let p and L be positive integers with p prime and* $\gcd(p, L) = 1$.

(1) If L is odd or L is divisible by 8, then

$$2\,|V\mathcal{X}_{p,L}| = |Q^1(\mathbb{Z}[1/p])\,/\,\Gamma_{p,L}| = |Q^1(\mathbb{Z}/(L))|\;/\;|N(\mathbb{Z}/(L))|\,.$$

If L is even but not divisible by 8, then

$$2\,|V\mathcal{X}_{p,L}| = |Q^1(\mathbb{Z}[1/p])\,/\,\Gamma_{p,L}| = |Q^1(\mathbb{Z}/(L))|\;/\;2\,|N(\mathbb{Z}/(L))|\,.$$

(2) If L is odd, or L is even but $p^{2m} \equiv L + 1 \pmod{2L}$ for some $m \in \mathbb{Z}$ (hence, $8 \mid L$), then

$$4\,|V\mathcal{X}'_{p,L}| = |Q^1(\mathbb{Z}[1/p])\,/\,\Gamma'_{p,L}| = |Q^1(\mathbb{Z}/(L))|\,.$$

If $L > 2$ is even and $p^{2m} \not\equiv L + 1 \pmod{2L}$ for all $m \in \mathbb{Z}$, then

$$4\,|V\mathcal{X}'_{p,L}| = |Q^1(\mathbb{Z}[1/p])\,/\,\Gamma'_{p,L}| = |Q^1(\mathbb{Z}/(L))|\;/\,2.$$

If $L = 2$, then $\Gamma'_{p,L} = \Gamma_{p,L}$ and $|V\mathcal{X}'_{p,L}| = |V\mathcal{X}_{p,L}|$.

Proof. From Proposition 3.15,

$$2\,|V\mathcal{X}_{p,L}| = |Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}|\,,$$

because $-\mathbf{1} \in \Gamma_{p,L}$ but $\mathbf{i}, \mathbf{j}, \mathbf{k} \notin \Gamma_{p,L}$. Also, if $L > 2$, then

$$4\,|V\mathcal{X}'_{p,L}| = |Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}|\,,$$

because $-\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k} \notin \Gamma'_{p,L}$. If $L = 2$, then $\Gamma_{p,L} = \Gamma'_{p,L}$ and $|V\mathcal{X}_{p,L}| = |V\mathcal{X}'_{p,L}|$, because $a_1 \equiv p^n \pmod 2 \iff a_1^2 \equiv p^{2n} \pmod 2$.

Now by Theorem 3.21, if L is odd or L is even but $p^{2m} \equiv 1 + L \pmod{2L}$ for some $m \in \mathbb{Z}$ (hence $8 \mid L$), then

$$|Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}| = |P^1(\mathbb{Z}/(L))|\,, \quad \text{and}$$
$$|Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}| = |Q^1(\mathbb{Z}/(L))|\,.$$

However, if L is even but $p^{2m} \not\equiv 1 + L \pmod{2L}$ for all $m \in \mathbb{Z}$, then

$$|Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}| = |P^1_e(\mathbb{Z}/(L))|\,, \quad \text{and}$$
$$|Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}| = |Q^1_e(\mathbb{Z}/(L))|\,.$$

By Proposition 3.23,

$$2\,|Q^1_e(\mathbb{Z}/(L))| = |Q^1(\mathbb{Z}/(L))|\,;$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

and

$$2\left|P_e^1(\mathbb{Z}/(L))\right| = \left|P^1(\mathbb{Z}/(L))\right| \quad \text{if } 8 \nmid L, \quad \text{and}$$
$$\left|P_e^1(\mathbb{Z}/(L))\right| = \left|P^1(\mathbb{Z}/(L))\right| \quad \text{if } 8 \mid L.$$

Combining these equalities yields the corollary. □

It remains to obtain formulas for $|Q^1(\mathbb{Z}/(L))|$ and $|N(\mathbb{Z}/(L))|$ as functions of L. First, a few lemmas are required. The proofs were suggested by a homework problem in [NZM91].

Lemma 3.25. *Define*

$$s(m,q) = \sum_{b=0}^{q-1} \left(\frac{b(m-b)}{q}\right)$$

using the Legendre symbol

$$\left(\frac{a}{q}\right) = \begin{cases} 0, & \text{if } q \text{ divides } a; \\ 1, & \text{if } a \text{ is a quadratic residue modulo } q; \\ -1, & \text{if } a \text{ is a nonresidue modulo } q. \end{cases}$$

Then

$$s(m,q) = \begin{cases} q-1, & \text{if } m \equiv 0 \pmod q \text{ and } q \equiv 1 \pmod 4; \\ 1-q, & \text{if } m \equiv 0 \pmod q \text{ and } q \equiv 3 \pmod 4; \\ -1, & \text{if } m \not\equiv 0 \pmod q \text{ and } q \equiv 1 \pmod 4; \\ 1, & \text{if } m \not\equiv 0 \pmod q \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

Proof. For $m = 0$,

$$s(0,q) = \sum_{b=0}^{q-1} \left(\frac{-b^2}{q}\right) = \left(\frac{0}{q}\right) + \sum_{b=1}^{q-1} \left(\frac{-b^2}{q}\right) = \begin{cases} +(q-1), & \text{if } q \equiv 1 \pmod 4; \\ -(q-1), & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

For $m \not\equiv 0 \pmod q$,

$$\begin{aligned} s(m,q) &= \sum_{b=0}^{q-1} \left(\frac{b(m-b)}{q}\right) = \sum_{b=0}^{q-1} \left(\frac{(mb)(m-mb)}{q}\right) \\ &= \sum_{b=0}^{q-1} \left(\frac{m^2 b(1-b)}{q}\right) = \sum_{b=0}^{q-1} \left(\frac{b(1-b)}{q}\right) = s(1,q). \end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

The sum $s(0,q)+\cdots+s(q-1,q)$ equals zero, because

$$\sum_{m=0}^{q-1} s(m,q) = \sum_{m=0}^{q-1}\sum_{b=0}^{q-1}\left(\frac{b(m-b)}{q}\right) = \sum_{b=0}^{q-1}\sum_{m=0}^{q-1}\left(\frac{b(m-b)}{q}\right)$$
$$= \sum_{b=0}^{q-1}\sum_{m=0}^{q-1}\left(\frac{bm}{q}\right) = q\left(\frac{0}{q}\right) + \sum_{b=1}^{q-1}\sum_{m=0}^{q-1}\left(\frac{m}{q}\right) = 0+(q-1)(0) = 0.$$

Therefore

$$0 = \sum_{m=0}^{q-1} s(m,q) = s(0,q) + \sum_{m=1}^{q-1} s(m,q) = s(0,q) + (q-1)s(1,q).$$

Hence, for each $m \not\equiv 0 \pmod q$,

$$s(m,q) = s(1,q) = -\frac{s(0,q)}{q-1} = \begin{cases} -1, & \text{if } q \equiv 1 \pmod 4; \\ +1, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

□

Lemma 3.26. *For q an odd prime, let $t(m,q)$ denote the number of solutions to $a^2+b^2 \equiv m \pmod q$. Then*

$$t(m,q) = \begin{cases} 2q-1, & \text{if } m \equiv 0 \pmod q \text{ and } q \equiv 1 \pmod 4; \\ 1, & \text{if } m \equiv 0 \pmod q \text{ and } q \equiv 3 \pmod 4; \\ q-1, & \text{if } m \not\equiv 0 \pmod q \text{ and } q \equiv 1 \pmod 4; \\ q+1, & \text{if } m \not\equiv 0 \pmod q \text{ and } q \equiv 3 \pmod 4. \end{cases}$$

Proof. If $m \equiv 0$, then $a^2+b^2 \equiv 0 \pmod q \implies a \equiv b \equiv 0 \pmod q$ or $(ab^{-1})^2 \equiv -1 (\mathrm{mod} q)$. If $q \equiv 3 (\mathrm{mod} 4)$, then $x^2 \equiv -1 (\mathrm{mod} q)$ has no solutions, so $t(m,q) = 1+0$. If $q \equiv 1 \pmod 4$, then $x^2 \equiv -1 \pmod q$ has two solutions. Choose either for x. For each $b \not\equiv 0 \pmod q$, $a^2 \equiv -b^2 \pmod q \implies a \equiv \pm xb \pmod q$. Therefore, $t(m,q) = 1+(q-1)(2) = 2q-1$.

For a given value of b, $a^2 \equiv m-b^2 \pmod q$ has $1+\left(\frac{m-b^2}{q}\right)$ solutions. If m_r is a quadratic residue (say $m_r \equiv k^2 \pmod q$), then the number of solutions to $a^2+b^2 \equiv m_r \pmod q$ is

$$t(m_r,q) = \sum_{b=0}^{q-1}\left[1+\left(\frac{m_r-b^2}{q}\right)\right] = q + \sum_{b=0}^{q-1}\left(\frac{k^2-b^2}{q}\right) = q + \sum_{b=0}^{q-1}\left(\frac{(k+b)(k-b)}{q}\right)$$
$$= q + \sum_{b=0}^{q-1}\left(\frac{b(2k-b)}{q}\right) = q + s(2k,q) = \begin{cases} q-1, & \text{if } q \equiv 1 \pmod 4; \\ q+1, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

If m_1, m_2 are both quadratic residues or both quadratic non-residues, then

$$\left(\frac{m_1 m_2^{-1}}{q}\right) = \left(\frac{m_1}{q}\right)\left(\frac{m_2}{q}\right) = 1,$$

so there exists k with $m_1 = k^2 m_2$. Then $t(m_1, q) = t(m_2, q)$ because

$$q + \sum_{b=0}^{q-1}\left(\frac{m_1 - b^2}{q}\right) = q + \sum_{b=0}^{q-1}\left(\frac{k^2 m_2 - (kb)^2}{q}\right) = q + \sum_{b=0}^{q-1}\left(\frac{m_2 - b^2}{q}\right).$$

As a and b range over $0, \ldots, q-1$, the pair (a, b) takes on a total of q^2 solutions to $a^2 + b^2 \equiv m \pmod q$ for various values of $0 \le m < q$. Hence:

$$\begin{aligned} q^2 = \sum_{m=0}^{q-1} t(m, q) &= t(0, q) + \sum_{\text{residues } m_r} t(m_r, q) + \sum_{\text{nonresidues } m_n} t(m_n, q) \\ &= t(0, q) + \frac{q-1}{2}\, t(m_r, q) + \frac{q-1}{2}\, t(m_n, q) \end{aligned}$$

where m_r is any residue and m_n is any non-residue. Then:

$$t(m_n, q) = \frac{2}{q-1}\left(q^2 - t(0, q)\right) - t(m_r, q).$$

We already have

$$t(0, q) = \begin{cases} 2q - 1, & \text{if } q \equiv 1 \pmod 4; \\ 1, & \text{if } q \equiv 3 \pmod 4. \end{cases} \quad \text{and} \quad t(m, q) = \begin{cases} q - 1, & \text{if } q \equiv 1 \pmod 4; \\ q + 1, & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

If $q \equiv 1 \pmod 4$,

$$t(m_n, q) = \frac{2}{q-1}\left(q^2 - (2q-1)\right) - (q-1) = 2(q-1) - (q-1) = q - 1.$$

If $q \equiv 3 \pmod 4$,

$$t(m_n, q) = \frac{2}{q-1}\left(q^2 - (1)\right) - (q+1) = 2(q+1) - (q+1) = q + 1.$$

□

Corollary 3.27. *For q an odd prime, $|Q^1(\mathbb{Z}/(q))| = (q^2 - 1)q$.*

Proof. To determine the number of solutions to $(a_1^2 + a_2^2) + (a_3^2 + a_4^2) \equiv 1 \pmod q$, count the solutions to $a_1^2 + a_2^2 \equiv m \pmod q$ and $a_3^2 + a_4^2 \equiv 1 - m \pmod q$ as m runs through $0, \ldots, m-1$.

$$\left|Q^1(\mathbb{Z}/(q))\right| = \sum_{m=0}^{q-1}\left[t(m, q)\, t(1-m, q)\right] = 2\, t(0, q)\, t(1, q) + \sum_{m=2}^{q-1}\left[t(m, q)\, t(1-m, q)\right].$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

If $q \equiv 1 \pmod 4$ then

$$|Q^1(\mathbb{Z}/(q))| = 2(2q-1)(q-1) + (q-2)(q-1)(q-1) = q^3 - q.$$

If $q \equiv 3 \pmod 4$ then

$$|Q^1(\mathbb{Z}/(q))| = 2(1)(q+1) + (q-2)(q+1)(q+1) = q^3 - q.$$

□

Lemma 3.28. *Each solution for $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{q^m}$. lifts to q^3 solutions modulo q^{m+1}.*

Proof. Solve

$$\begin{aligned}
&(a_1 + a_1' q^m)^2 + (a_2 + a_2' q^m)^2 + (a_3 + a_3' q^m)^2 + (a_4 + a_4' q^m)^2 \equiv 1 \pmod{q^{m+1}} \\
&\iff (a_1^2 + a_2^2 + a_3^2 + a_4^2 - 1) + 2q^m(a_1 a_1' + a_2 a_2' + a_3 a_3' + a_4 a_4') \\
&\quad + q^{2m}(a_1'^2 + a_2'^2 + a_3'^2 + a_4'^2 \equiv 0 \pmod{q^{m+1}} \\
&\iff \frac{a_1^2 + a_2^2 + a_3^2 + a_4^2 - 1}{q^m} + 2(a_1 a_1' + a_2 a_2' + a_3 a_3' + a_4 a_4') \equiv 0 \pmod q.
\end{aligned}$$

At least one of a_1, a_2, a_3, a_4 is not divisible by q, so pick one, say a_1. Then we can choose a_2', a_3', a_4' to have any values modulo q, and the value for a_1' is forced:

$$a_1' \equiv a_1^{-1}\left[-\left(\frac{a_1^2 + a_2^2 + a_3^2 + a_4^2 - 1}{q^n}\right)2^{-1} - a_2 a_2' - a_3 a_3' - a_4 a_4'\right] \pmod q.$$

So, (a_1, a_2, a_3, a_4) lifts to $(1)(q)(q)(q) = q^3$ solutions. □

Lemma 3.29. *Let m be odd and $n \geq 3$. Then $x^2 \equiv m \pmod{2^n}$ has 4 solutions. If x_0 is one solution, then the others are $-x_0$ and $\pm x_0 + 2^{n-1}$.*

Proof. This follows from page 105 of [NZM91]. □

Proposition 3.30. *Write $L = 2^\ell L'$, with L' odd. Then the orders of $Q^1(\mathbb{Z}/(L))$ and $N(\mathbb{Z}/(L))$ are given by:*

$$|Q^1(\mathbb{Z}/(L))| = L^3 \prod_{q|L'}\left(1 - \frac{1}{q^2}\right);$$

$$|N(\mathbb{Z}/(L))| = \left[\prod_{q|L'} 2\right] \cdot \begin{cases} 1, & \text{if } \ell < 2 \text{ so } L \not\equiv 0 \pmod 4; \\ 2, & \text{if } \ell = 2 \text{ so } L \equiv 4 \pmod 8; \\ 4, & \text{if } \ell > 2 \text{ so } L \equiv 0 \pmod 8. \end{cases}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof. First, suppose $L = L_1 L_2$ and $\gcd(L_1, L_2) = 1$. The Chinese Remainder Theorem implies a bijective identification between solutions (mod $L_1 L_2$) and pairs of solutions (mod L_1, mod L_2). Hence,

$$Q^1(\mathbb{Z}/(L_1 L_2)) = Q^1(\mathbb{Z}/(L_1)) \times Q^1(\mathbb{Z}/(L_2)); \quad \text{and}$$
$$N(\mathbb{Z}/(L_1 L_2)) = N(\mathbb{Z}/(L_1)) \times N(\mathbb{Z}/(L_2)).$$

For odd primes q and positive integers m, Corollary 3.27 and Lemma 3.28 imply

$$\left|Q^1(\mathbb{Z}/(q^m))\right| = (q^2 - 1)q^{3m-2}.$$

$|Q^1(\mathbb{Z}/(2))| = 8$, because $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \,(\mathrm{mod}\, 2)$ has eight solutions, namely permutations of $(1, 0, 0, 0)$ and $(1, 1, 1, 0)$.

When $L = 4$, one of the a_i is odd, and the other three are even. The odd value is either 1 or 3 modulo 4, and the even values are each either 0 or 2 modulo 4. So there are $|Q^1(\mathbb{Z}/(4))| = (4)(2)(2)(2)(2) = 64$ solutions.

If $m \geq 3$, then one of the a_i (say a_1) is odd and the others are even. Then $n - a_1^2 \equiv 0 \,(\mathrm{mod}\, 8)$, so count all a_2, a_3 and a_4 with either $a_2^2 \equiv a_3^2 \equiv a_4^2 \equiv 0 \,(\mathrm{mod}\, 8)$ or (a_2, a_3, a_4) equivalent to a permutation of $(4, 4, 0)$ modulo 8. For each choice of a_2, a_3 and a_4, there are 4 choices for a_1, by Lemma 3.29. The total number of solutions is:

$$(4)\left[(2^{m-2})(2^{m-2})(2^{m-2})(4) + (3)(2^{m-2})(2^{m-2})(2^{m-2})(4)\right] = 16(2^{m-2})^3 = 2^{3m}.$$

Therefore $|Q^1(\mathbb{Z}/(2^m))| = 2^{3m}$ for $m \geq 3$.

Let $q > 2$ be prime, so either $\gcd(q, a - 1) = 1$ or $\gcd(q, a + 1) = 1$. Then

$$a^2 \equiv 1 \,(\mathrm{mod}\, q^{2m}) \iff q^{2m} | (a - 1)(a + 1) \iff a \equiv \pm 1 \,(\mathrm{mod}\, q^{2m}).$$

Hence, $|N(\mathbb{Z}/(q^m))| = 2$.

$|N(\mathbb{Z}/(2))| = 1$ because $a^2 \equiv 1 \,(\mathrm{mod}\, 2) \iff a \equiv 1 \,(\mathrm{mod}\, 2)$.

$|N(\mathbb{Z}/(4))| = 2$ because $a^2 \equiv 1 \,(\mathrm{mod}\, 4) \iff a \equiv 1$ or $3 \,(\mathrm{mod}\, 4)$.

For $m \geq 3$,

$$a^2 \equiv 1 \,(\mathrm{mod}\, 2^m) \iff a \equiv \pm 1 \text{ or } \pm 1 + 2^{m-1} \,(\mathrm{mod}\, 2^m).$$

Therefore, $|N(\mathbb{Z}/(2^m))| = 4$ if $m \geq 3$. □

Corollary 3.31. *Write $L = 2^\ell L'$, with L' odd. Then:*

$$2\,|V\mathcal{X}_{p,L}| = \left|Q^1(\mathbb{Z}[1/p])\,/\,\Gamma_{p,L}\right|$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$= L^3 \prod_{q|L'} \left(\frac{1 - 1/q^2}{2} \right) \cdot \begin{cases} 1, & \text{if } \ell = 0 \text{ so } L \equiv 1 \pmod 2; \\ 1/2, & \text{if } \ell = 1 \text{ so } L \equiv 2 \pmod 4; \\ 1/4, & \text{if } \ell \geq 2 \text{ so } L \equiv 0 \pmod 4. \end{cases}$$

and

$$4 \left| V\mathcal{X}'_{p,L} \right| = \left| Q^1(\mathbb{Z}[1/p]) \,/\, \Gamma'_{p,L} \right|$$

$$= L^3 \prod_{q|L'} \left(1 - \frac{1}{q^2} \right) \cdot \begin{cases} 1, & \text{if } L \text{ odd}; \\ 1, & \text{if } 8 \mid L \text{ and } p^{2m} \equiv L + 1 \pmod{2L} \\ & \quad \text{for some } m \in \mathbb{Z}; \\ 1/2, & \text{if } L > 2 \text{ even and } p^{2m} \not\equiv L + 1 \pmod{2L} \\ & \quad \text{for all } m \in \mathbb{Z}; \end{cases}$$

$\left| V\mathcal{X}'_{p,L} \right| = |V\mathcal{X}_{p,L}| = 2$ *if* $L = 2$.

Consequently, $|V\mathcal{X}_{p,L}| = \left| V\mathcal{X}'_{p,L} \right|$ (and $\mathcal{X}_{p,L} = \mathcal{X}'_{p,L}$) if and only if either

(1) $L = 2$;

(2) $L \not\equiv 0 \pmod 4$ and $L' > 1$ is a power of a prime;

(3) $L \equiv 0 \pmod 4$ and $L' = 1$; or

(4) $L \equiv 0 \pmod 8$ and $L' = 1$ and $p \equiv \pm 1 \pmod 8$.

For values of L between 1 and 50, Table 3.1 lists the orders of the groups $Q^1(\mathbb{Z}/(L))$ and $N(\mathbb{Z}/(L))$, and the number of vertices in the quotient graphs $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$. Numbers marked with "*" ($\left| V\mathcal{X}'_{p,L} \right|$ for $8 \mid L$) are doubled if $p^{2m} \equiv L + 1 \pmod{2L}$ for some $m \in \mathbb{Z}$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

L	Q	N	$V\mathcal{X}_{p,L}$	$V\mathcal{X}'_{p,L}$	L	Q	N	$V\mathcal{X}_{p,L}$	$V\mathcal{X}'_{p,L}$
1	1	1			26	17472	2	2184	2184
2	8	1	2	2	27	17496	2	4374	4374
3	24	2	6	6	28	21504	4	1344	2688
4	64	2	8	8	29	24360	2	6090	6090
5	120	2	30	30	30	23040	4	1440	2880
6	192	2	24	24	31	29760	2	7440	7440
7	336	2	84	84	32	32768	4	4096	4096*
8	512	4	64	64*	33	31680	4	3960	7920
9	648	2	162	162	34	39168	2	4896	4896
10	960	2	120	120	35	40320	4	5040	10080
11	1320	2	330	330	36	41472	4	2592	5184
12	1536	4	96	192	37	50616	2	12654	12654
13	2184	2	546	546	38	54720	2	6840	6840
14	2688	2	336	336	39	52416	4	6552	13104
15	2880	4	360	720	40	61440	8	3840	7680*
16	4096	4	512	512*	41	68880	2	17220	17220
17	4896	2	1224	1224	42	64512	4	4032	8064
18	5184	2	648	648	43	79464	2	19866	19866
19	6840	2	1710	1710	44	84480	4	5280	10560
20	7680	4	480	960	45	77760	4	9720	19440
21	8064	4	1008	2016	46	97152	2	12144	12144
22	10560	2	1320	1320	47	103776	2	25944	25944
23	12144	2	3036	3036	48	98304	8	6144	12288*
24	12288	8	768	1536*	49	115248	2	28812	28812
25	15000	2	3750	3750	50	120000	4	15000	15000

Table 3.1: Sizes of $Q^1(\mathbb{Z}/(L))$ and $N(\mathbb{Z}/(L))$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER IV

Computation of Quotient Graphs

A set of computer programs were written in ANSI C and executed in order to generate representations of the quotient graphs $\mathcal{X}_{p,L} = \Gamma_{p,L}\backslash\mathcal{T}_p$ and $\mathcal{X}'_{p,L} = \Gamma'_{p,L}\backslash\mathcal{T}_p$ for particular values of p and L. These graphs were used to test hypotheses and to encourage the discovery of facts and patterns through direct inspection.

Two programming issues stood out. First, the computation of $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$ involves a number of mathematical objects that are unbounded or require infinite precision to fully represent, so the programs must approximate them using finite data structures without compromising the accuracy of the final output. Second, the programs must not only produce correct results, but complete execution within a reasonable amount of time. Earlier versions of the main program required a week to execute; later optimized versions could accomplish the same task in an hour.

This chapter discusses some of the programming issues that arose during the development of these programs and displays some of the quotient graphs produced. Sections 4.1 through 4.7 detail the approaches taken to represent p-adic integers, the groups $\Gamma_{p,L}$ and $\Gamma'_{p,L}$, the $(p+1)$-regular graph $\mathcal{T}_p$, and the quotient maps $\mathcal{T}_p \longrightarrow \mathcal{X}_{p,L}$ and $\mathcal{T}_p \longrightarrow \mathcal{X}'_{p,L}$. Section 4.8 discusses halting conditions and the correctness of the program results. Section 4.9 displays some of the quotient graphs generated by the programs and relates them to results proved in Chapter III.

4.1 Overview of the Programs

The C code is organized into a collection of files and programs. This section briefly describes the most useful programs. More description and implementation details are presented in later sections.

The header file `select.h` defines values for some global constants used in many of the files and programs. These constants determine which integer data types are used to represent p-adic numbers and to number vertices in $\mathcal{T}_p$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Within the C code, elements of the groups $Q(\mathbb{Z}[1/p])$, $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ are represented as tuples $(n : a_1, a_2, a_3, a_4)$ of five integers and are stored temporarily in large files on disk. The programs `TupleCount`, `TupleCreate1`, `TupleCreate2`, `TupleCreate3`, `TupleExpand`, `TupleFilter`, `TupleHunt`, `TupleProduct`, `TupleProductCount`, `TupleSort`, `TupleTrim` and `PrintProduct` manipulate these lists of tuples. The procedures in the files `tuple.h` and `tuple.c` access these tuples during the computation of the quotient map $\mathcal{T}_p \longrightarrow \mathcal{X}_{p,L}$ or $\mathcal{T}_p \longrightarrow \mathcal{X}'_{p,L}$. Section 4.2 describes these programs in more detail.

The files `padic.h` and `padic.c` provide support for p-adic integers, represented as unsigned integers. Details are provided in Section 4.3. The files `matrices.h` and `matrices.c` implement operations on $M_2(\mathbb{Z}_p)$, and procedures in `tuptomat.h` and `tuptomat.c` convert tuples from $Q(\mathbb{Z}[1/p])$ into matrices in $\mathrm{GL}_2(\mathbb{Z}_p)$.

Code in the files `vertices.h` and `vertices.c` computes the action of a matrix from $\mathrm{GL}_2(\mathbb{Z}_p)$ on a vertex of $\mathcal{T}_p$.

The files `tree.h` and `tree.c` number the vertices of the tree $\mathcal{T}_p$ and maintain the quotient map $\mathcal{T}_p \longrightarrow \mathcal{X}_{p,L}$ or $\mathcal{T}_p \longrightarrow \mathcal{X}'_{p,L}$.

The programs in `ApplyMatrix.c` and `ApplyTuple.c` display the action of one element of $\mathrm{GL}_2(\mathbb{Z}_p)$ and $Q(\mathbb{Z}[1/p])$, respectively, on vertices in the tree $\mathcal{T}_p$.

Finally, the programs `MapCreate`, `MapPrint`, `MapSmush` and `TupleSmush` act on a representation of the quotient map $\mathcal{T}_p \longrightarrow \mathcal{X}_{p,L}$ or $\mathcal{T}_p \longrightarrow \mathcal{X}'_{p,L}$. In particular, `MapSmush` and `TupleSmush` perform the computation of the quotient maps. Once a map is completely determined, the program `QuotientGraph` converts the quotient map into a representation of the quotient graph $\mathcal{X}_{p,L}$ or $\mathcal{X}'_{p,L}$.

4.2 Representation of the Groups $Q^1(\mathbb{Z}[1/p])$, $\Gamma_{p,L}$ and $\Gamma'_{p,L}$

Calculating the quotient graph $\mathcal{X}_{p,L}$ or $\mathcal{X}'_{p,L}$ involves applying elements of $\Gamma_{p,L}$ or $\Gamma'_{p,L}$ to a representation of the graph $\mathcal{T}_p$. The groups $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ are infinite, but the elements can be ordered according to the distance they translate vertices in $\mathcal{T}_p$. Elements that translate vertices shorter distances provide more information, and are considered first.

Let p and L be fixed positive integers, with p an odd prime. Recall the group descriptions

$$Q^1(\mathbb{Z}[1/p]) = \left\{ \frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \;\middle|\; n, a_i \in \mathbb{Z} \text{ and } a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n} \right\};$$

$$\Gamma_{p,L} = \left\{ \frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \in Q^1(\mathbb{Z}[1/p]) \;\middle|\; a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{L} \right\};$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

and

$$\Gamma'_{p,L} = \left\{ \frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \in Q^1(\mathbb{Z}[1/p]) \;\middle|\; \begin{array}{c} a_1 \equiv p^n \pmod{L} \\ a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{L} \end{array} \right\}.$$

So $\Gamma'_{p,L} < \Gamma_{p,L} < Q^1(\mathbb{Z}[1/p]) < Q^1(\mathbb{Q}_p)$.

Definition 4.1. The group element

$$\frac{a_1}{p^n}\mathbf{1} + \frac{a_2}{p^n}\mathbf{i} + \frac{a_3}{p^n}\mathbf{j} + \frac{a_4}{p^n}\mathbf{k} \in Q^1(\mathbb{Z}[1/p]).$$

can be represented by a *tuple* $(n : a_1, a_2, a_3, a_4)$ where $n, a_1, a_2, a_3, a_4 \in \mathbb{Z}$,

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n},$$

and not all of a_1, a_2, a_3 and a_4 are divisible by p.

Group elements are calculated and stored as tuples in large files before being used to calculate the quotient graph. In order to save memory, group elements that differ only by choice of signs and permutation of the values a_1, a_2, a_3 and a_4 are lumped together and represented by a single tuple.

Definition 4.2. The tuple $(n : a_1, a_2, a_3, a_4)$ is called *standard* if

$$\begin{array}{rl} a_1 \geq a_2 \geq a_3 \geq a_4 \geq 0 & \text{in } Q^1(\mathbb{Z}[1/p]); \\ a_2 \geq a_3 \geq a_4 \geq 0 \text{ and } a_1 > 0 & \text{in } \Gamma_{p,L}; \quad \text{and} \\ a_2 \geq a_3 \geq a_4 \geq 0 & \text{in } \Gamma'_{p,L}. \end{array}$$

A *variant* of $(n : a_1, a_2, a_3, a_4)$ in $Q^1(\mathbb{Z}[1/p])$ is any tuple that can be obtained by permuting and changing the signs of a_1, a_2, a_3 and a_4. In $\Gamma_{p,L}$ and $\Gamma'_{p,L}$, variants are obtained by permuting a_2, a_3 and a_4 and changing the signs of a_2, a_3 and a_4 and changing the sign of a_1 in $\Gamma_{p,L}$ but not in $\Gamma'_{p,L}$.

Example 4.3. In $\Gamma_{3,5}$, the standard tuple $(3 : 23, 10, 10, 0)$ represents the 24 variants:

$(3 : 23, 10, 10, 0)$,	$(3 : 23, 10, 0, 10)$,	$(3 : 23, 0, 10, 10)$,
$(3 : 23, 10, -10, 0)$,	$(3 : 23, 10, 0, -10)$,	$(3 : 23, 0, 10, -10)$,
$(3 : 23, -10, 10, 0)$,	$(3 : 23, -10, 0, 10)$,	$(3 : 23, 0, -10, 10)$,
$(3 : 23, -10, -10, 0)$,	$(3 : 23, -10, 0, -10)$,	$(3 : 23, 0, -10, -10)$,
$(3 : -23, 10, 10, 0)$,	$(3 : -23, 10, 0, 10)$,	$(3 : -23, 0, 10, 10)$,
$(3 : -23, 10, -10, 0)$,	$(3 : -23, 10, 0, -10)$,	$(3 : -23, 0, 10, -10)$,
$(3 : -23, -10, 10, 0)$,	$(3 : -23, -10, 0, 10)$,	$(3 : -23, 0, -10, 10)$,
$(3 : -23, -10, -10, 0)$,	$(3 : -23, -10, 0, -10)$,	$(3 : -23, 0, -10, -10)$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

A tuple can have up to $(4!)(2^4) = 384$ variants in $Q^1(\mathbb{Z}[1/p])$, $(3!)(2^4) = 96$ variants in $\Gamma_{p,L}$, and $(3!)(2^3) = 48$ variants in $\Gamma'_{p,L}$.

Assign a dictionary ordering to the set of all tuples. Write

$$(n_1 : a_1, a_2, a_3, a_4) < (n_2 : b_1, b_2, b_3, b_4)$$

whenever any of the following conditions hold:

(1) $n_1 < n_2$;

(2) $n_1 = n_2$ and $|a_1| < |b_1|$;

(3) $n_1 = n_2$ and $|a_1| = |b_1|$ and $a_1 > b_1$;

(4) $n_1 = n_2$, $a_1 = b_1$ and $a_2 < b_2$;

(5) $n_1 = n_2$, $a_1 = b_1$, $a_2 = b_2$ and $a_3 < b_3$; or

(6) $n_1 = n_2$, $a_1 = b_1$, $a_2 = b_2$, $a_3 = b_3$ and $a_4 < b_4$.

Example 4.4. The standard tuples in $Q^1(\mathbb{Z}[1/3])$ with $n \leq 2$ are

$$(0 : 1, 0, 0, 0) < (1 : 2, 2, 1, 0) < (2 : 6, 5, 4, 2) < (2 : 7, 4, 4, 0) < (2 : 8, 3, 2, 2) < (2 : 8, 4, 1, 0).$$

The standard tuples in $\Gamma_{3,5}$ with $n \leq 3$ are

$$(0 : 1, 0, 0, 0) < (3 : 2, 20, 15, 10) < (3 : 2, 25, 10, 0) < (3 : 23, 10, 10, 0).$$

Finally, the standard tuples in $\Gamma'_{3,5}$ with $n \leq 3$ are

$$(0 : 1, 0, 0, 0) < (3 : 2, 20, 15, 10) < (3 : 2, 25, 10, 0) < (3 : -23, 10, 10, 0).$$

4.2.1 Files of Tuples

Tuples are stored in text files with names indicating the contents of the file. The first letter of the file name is always `T`, indicating that the file contains tuples. The second letter indicates the name of the program that created the file, as indicated in Table 4.1. The rest of the file name indicates the group ("`G1`" for $Q^1(\mathbb{Z}[1/p])$, "`G2`" for $\Gamma_{p,L}$ and "`G3`" for $\Gamma'_{p,L}$), the values for p and L, and bounds on the power n.

Example 4.5. A file named "`TC-G1-P3-T6-7`" would have been created by the program `TupleCreate1` and should contain an ordered list of all standard tuples $(n : a_1, a_2, a_3, a_4)$ in $Q^1(\mathbb{Z}[1/p])$ with $6 \leq n \leq 7$. A file named "`TC-G2-P3-L5-T0-3`" would contain exactly four tuples:

$$(1 : 1, 0, 0, 0) < (3 : 2, 20, 15, 10) < (3 : 2, 25, 10, 0) < (3 : 23, 10, 10, 0),$$

because these are the only standard tuples in the group $\Gamma_{3,5}$ with $0 \leq n \leq 3$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Program	File Name Prefix
TupleCreate1	TC-G1-
TupleCreate2	TC-G2-
TupleCreate3	TC-G3-
TupleTrim	TT-
TupleProduct	TP-
TupleExpand	TE-
TupleSort	TS-
TupleSmush	TU-

Table 4.1: Prefixes for tuple file names

4.2.2 Tuple Programs

Several programs were written to manipulate tuples and files of tuples.

`TupleCreate1`, `TupleCreate2` and `TupleCreate3` each generate a file containing an ordered list of all standard tuples $(n : a_1, a_2, a_3, a_4)$ for the groups $Q^1(\mathbb{Z}[1/p])$, $\Gamma_{p,L}$ and $\Gamma'_{p,L}$, respectively.

`TupleCount` counts the number of tuples in the input file.

`TupleExpand` creates a file containing all variants of the tuples in the input file.

`TupleSort` sorts the tuples in the input file and puts them in standard form. The resulting ordered list of standard tuples is stored in an output file.

`TupleProduct` reads an ordered list of standard tuples from an input file. It then creates a file containing an ordered list of all standard tuples that can be represented as the product of variants of two tuples in the input file.

`TupleTrim` reads lists of tuples from two input files. It then creates a file containing all tuples that occur in the first input file but not in the second. Both input files must be ordered.

The last two programs were written in order to identify and discard group elements that are generated by group elements already in the list. These two programs were not used in practice, because it was discovered that the time required to eliminate these tuples was much longer than any time saved by removing them. Also, it is not clear that removing these tuples from consideration is wise.

Finally, the files `tuple.h` and `tuple.c` contain two procedures that read standard tuples from an input file, then produce all variants of those tuples. These procedures are invoked by other programs while computing the quotient graph $\mathcal{X}_{p,L}$ or $\mathcal{X}'_{p,L}$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

4.2.3 Implementation Notes

The generation of tuples by the programs `TupleCreate1`, `TupleCreate2` and `TupleCreate3` can be quite slow and may require more time than the actual computation of the quotient graph. For each n, the algorithm iterates through all integers a_1, a_2, a_3 and a_4 such that

$$p^n \geq a_1 \geq a_2 \geq a_3 \geq a_4 \geq 0,$$

and then produces all instances such that

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n}$$

and that p does not divide all of a_1, a_2, a_3 and a_4.

This algorithm is very slow, requiring about $p^{4n}/24$ tests. The execution time is improved to around $p^{3n}/60$ tests by restricting the ranges to:

$$\begin{aligned} p^{2n} \geq a_1^2 &\geq p^{2n}/4, \\ p^{2n} - a_1^2 \geq a_2^2 &\geq \left(p^{2n} - a_1^2\right)/3, \\ p^{2n} - a_1^2 - a_2^2 \geq a_3^2 &\geq \left(p^{2n} - a_1^2 - a_2^2\right)/2, \\ a_4^2 &= p^{2n} - a_1^2 - a_2^2 - a_3^2. \end{aligned}$$

4.3 Representation of p-adic Integers

Like real numbers, p-adic integers can be arbitrarily precise, requiring an infinite number of digits when displayed in base p. It is possible to obtain exact computational precision by representing p-adic integers by functions that produce any requested digit when invoked. However, this approach introduces unnecessary complexity and computational slowness if only limited precision is required.

The C code in the files `padic.h` and `padic.c` represent p-adic integers using one of C's unsigned integer types. Only finitely many digits of a p-adic integer are maintained; the rest are truncated. `ExponentMax` equals the number of digits of accuracy that are maintained. All p-adic integers are represented by integers between 0 and `PadicMod` -1, where `PadicMod` $= p^{\texttt{ExponentMax}}$. In effect, the ring $\mathbb{Z}/(\texttt{PadicMod})$ is used to approximate $\mathbb{Z}_p$.

`ExponentMax` is chosen so that the computation of the sum of two p-adic integers (computed as the remainder modulo `PadicMod` of the sum of the two integers) will never overflow the unsigned integer type used to represent p-adic numbers. In particular, the number $2(\texttt{PadicMod}-1)$ must be no larger than the maximum representable integer. Also, `ExponentMax` must be even, to facilitate multiplication.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

For example, if p-adic integers are represented as 64-bit integers, then ExponentMax is the largest even integer such that

$$2(\texttt{PadicMod} - 1) \leq 2^{64} - 1 \iff \texttt{PadicMod} \leq 2^{63}.$$

Table 4.2 lists values for ExponentMax and PadicMod for various values of p. In each case,

$$\texttt{PadicMod} \leq 2^{63} = 9223372036854775808.$$

More precision can be obtained by using a larger integer type. In practice, 64-bit integers proved sufficient for obtaining the quotient graphs, while 32-bit integers were only sufficient for the smaller quotient graphs.

P	ExponentMax	PadicMod
3	38	$3^{38} = 1350851717672992089$
5	26	$5^{26} = 1490116119384765625$
7	22	$7^{22} = 3909821048582988049$
11	18	$11^{18} = 5559917313492231481$
13	16	$13^{16} = 665416609183179841$
17	14	$17^{14} = 168377826559400929$
19	14	$19^{14} = 799006685782884121$

Table 4.2: Values for ExponentMax and PadicMod for 64-bit numbers

Functions in the file padic.c implement a number of operations on the ring $\mathbb{Z}/(\texttt{PadicMod})$. The function InitializePadic initializes the values of P $= p$, ExponentMax and PadicMod. Also, some commonly used values, such as

$$\texttt{PtoN}[n] = p^n \qquad \text{and} \qquad \texttt{SumPtoN1}[n] = p^0 + p^1 + \cdots + p^{n-1} = \frac{p^n - 1}{p - 1},$$

for various n, are computed and saved in order to speed up later computations.

The functions PdAdd, PdSubtract, PdNegate, PdMultiply, PdMultThenAdd, PdMultThenSubtract and PdAddTwoMults perform combinations of addition, subtraction and multiplication. All are implemented so that the results lie between 0 and PadicMod -1, and overflow errors never occur. To improve efficiency, many functions are defined as macros.

PdMultPtoN multiplies a p-adic number by a power of p, and PdMultThenModPtoN multiplies a p-adic number by one power of p then finds the remainder modulo another. It is also sometimes desirable to divide (using normal division, /) a p-adic number by a power of p. This reduces the number of accurate digits, and must be used with care.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

`PdInverse` and `PdSqrt` obtain the multiplicative inverse and a square root, respectively, of a number in $\mathbb{Z}/(\texttt{PadicMod})$, or zero if no inverse or square root exists. Both functions are implemented iteratively, requiring $\log_2(\texttt{ExponentMax})$ and `ExponentMax` iterations, respectively. Since `PdInverse` is invoked very often, its implementation has been optimized further by having `InitializePadic` preevaluate the computations done during the first few iterations. Also, `PdSqrt` is deterministic; the same square root will be returned each time `PdSqrt` is called with the same argument.

4.4 Representation of Tree Vertices

Each vertex of the tree $\mathcal{T}_p$ is associated with an equivalence class of lattices. Fix a basis $\{e_1, e_2\}$ for the vector space V used in Chapter II to define these lattices. All lattices and matrices in the remainder of this chapter are written with respect to this same basis.

4.4.1 Standard Form for Lattices

In order to establish a representation for the vertices of $\mathcal{T}_p$, it is first necessary to choose one representative lattice from each equivalence class. These representatives can then be converted into numbers that the computer can store and manipulate.

Proposition 4.6. *With respect to the basis $\{e_1, e_2\}$, every lattice is equivalent to exactly one lattice of the form*

$$\mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix}$$

where $0 \leq b < p^r$ and either $\ell = 0$, $r = 0$ or $p \nmid b$.

Proof. Pick any lattice of V This lattice is equivalent to a lattice

$$\mathbb{Z}_p \begin{bmatrix} a_{11} \\ a_{12} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a_{21} \\ a_{22} \end{bmatrix}$$

with $a_{11}, a_{21} \in \mathbb{Q}_p$, $a_{12}, a_{21} \in \mathbb{Z}_p$ and either a_{12} or a_{22} not in $p\mathbb{Z}_p$. If $a_{12} \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, then the lattice can be rewritten as

$$\mathbb{Z}_p \begin{bmatrix} a_{11} \\ a_{12} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a_{21} - a_{11}a_{12}^{-1}a_{22} \\ a_{22} - a_{12}a_{12}^{-1}a_{22} \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} a_{11}a_{12}^{-1} \\ 1 \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a_{21} - a_{11}a_{12}^{-1}a_{22} \\ 0 \end{bmatrix}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Then put $a_1 = a_{11}a_{12}^{-1}$ and $a_2 = a_{21} - a_{11}a_{12}^{-1}a_{22}$. On the other hand, if $a_{22} \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, then rewrite the lattice as

$$\mathbb{Z}_p \begin{bmatrix} a_{11} - a_{21}a_{22}^{-1}a_{12} \\ a_{12} - a_{22}a_{22}^{-1}a_{12} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a_{21} \\ a_{22} \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} a_{11} - a_{21}a_{22}^{-1}a_{12} \\ 0 \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a_{21}a_{22}^{-1} \\ 1 \end{bmatrix}.$$

Then set $a_1 = a_{21}a_{22}^{-1}$ and $a_2 = a_{11} - a_{21}a_{22}^{-1}a_{12}$. In either case, the lattice can be rewritten in the form

$$\mathbb{Z}_p \begin{bmatrix} a_1 \\ 1 \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a_2 \\ 0 \end{bmatrix}$$

for some $a_1, a_2 \in \mathbb{Q}_p$.

Now, for $i = 1, 2$, write $a_i = p^{\alpha_i}a_i'$ with each $\alpha_i \in \mathbb{Z}$ and $a_i' \in \mathbb{Z}_p$ but $a_i' \notin p\mathbb{Z}_p$. Set $\ell = \min\{-\alpha_1, -\alpha_2, 0\}$ and $r = \ell + \alpha_2$. Then ℓ and r are non-negative and the lattice $\mathbb{Z}_p \begin{bmatrix} a_1 \\ 1 \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} a_2 \\ 0 \end{bmatrix}$ is equivalent to

$$\mathbb{Z}_p \begin{bmatrix} p^\ell a_1 \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^\ell a_2 \\ 0 \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} p^\ell a_1 \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{\ell+\alpha_2}a_2' \\ 0 \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} p^\ell a_1 \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix}.$$

Since $\ell + \alpha_1 \geq 0$, $p^\ell a_1 \in \mathbb{Z}_p$ and can be written as $p^\ell a_1 = b + p^r a_3$ where $a_3 \in \mathbb{Z}_p$, $b \in \mathbb{Z}$ and $0 \leq b < p^r$. Then the lattice can be expressed as:

$$\mathbb{Z}_p \begin{bmatrix} b + p^r a_3 \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix}.$$

It remains to show that this representation is unique. Suppose that the lattices

$$L = \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix} \qquad \text{and} \qquad L' = \mathbb{Z}_p \begin{bmatrix} b' \\ p^{\ell'} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{r'} \\ 0 \end{bmatrix}$$

are equivalent, so the distance between them is zero.

First, assume that $bp^{\ell'} \neq b'p^\ell$, so that $\begin{bmatrix} b \\ p^\ell \end{bmatrix}$ and $\begin{bmatrix} b' \\ p^{\ell'} \end{bmatrix}$ are linearly independent. Write $bp^{\ell'} - b'p^\ell = ap^\alpha$ where $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Then $\alpha < r + \ell'$ because $0 \leq b < p^r$, so

$$\begin{aligned} \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} p^\alpha + \mathbb{Z}_p \begin{bmatrix} b' \\ p^{\ell'} \end{bmatrix} p^{\ell+r} &= \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} p^\alpha + \mathbb{Z}_p \begin{bmatrix} b'p^{\ell+r} - bp^{\ell'+r} \\ p^{\ell+\ell'+r} - p^{\ell+\ell'+r} \end{bmatrix} \\ &= \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} p^\alpha + \mathbb{Z}_p \begin{bmatrix} ap^\alpha \\ 0 \end{bmatrix} p^r = \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} p^\alpha + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix} p^\alpha. \end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Similarly, $\alpha < r' + \ell$ because $0 \leq b' < p^{r'}$, so

$$\mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} p^{\ell'+r'} + \mathbb{Z}_p \begin{bmatrix} b' \\ p^{\ell'} \end{bmatrix} p^\alpha = \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} p^\alpha + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix} p^\alpha.$$

Therefore, by Proposition 2.11, the distance between L and L' is $\ell + \ell' + r + r' - 2\alpha$. However, $\alpha < r + \ell'$ and $\alpha < r' + \ell$, so this distance is positive, which contradicts $d(L, L') = 0$. Consequently, $bp^{\ell'} = b'p^\ell$.

Now, the distance between

$$L = \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} bp^{\ell'} \\ p^{\ell+\ell'} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{r+\ell'} \\ 0 \end{bmatrix}$$

and

$$L' = \mathbb{Z}_p \begin{bmatrix} b' \\ p^{\ell'} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{r'} \\ 0 \end{bmatrix} = \mathbb{Z}_p \begin{bmatrix} b'p^\ell \\ p^{\ell'+\ell} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{r'+\ell} \\ 0 \end{bmatrix}$$

is $|(r + \ell') - (r' + \ell)|$, so $r + \ell' = r' + \ell$. This, combined with the facts that either $\ell = 0$, $r = 0$ or $p \nmid b$, and either $\ell' = 0$, $r' = 0$ or $p \nmid b'$, yields $r = r'$, $\ell = \ell'$ and $b = b'$. □

Each vertex in the tree $\mathcal{T}_p$ is now identified with a unique lattice in standard form. In the remainder of this chapter, the two will be used interchangeably. In addition, the vertex corresponding to the lattice

$$\mathbb{Z}_p \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

will receive special attention; denote this vertex v_0.

4.4.2 Standard Form for Lattices

The files `vertices.h` and `vertices.c` represent a vertex as a `struct` of three non-negative integers (ℓ, r, b), called the `Limb`, `Radius` and `Branch`, corresponding to the equivalence class of the lattice

$$\mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix}.$$

While the `Limb` and `Radius` are small integers, `Branch` can be as large as $p^{\texttt{Radius}} - 1$. Consequently, the `Radius` must be small enough so that $p^{\texttt{Radius}}$ can be represented by one of C's unsigned integer types. The vertex v_0 is denoted $(0, 0, 0)$. The "vertex" $(-1, 0, 0)$ is used to signal computation errors.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

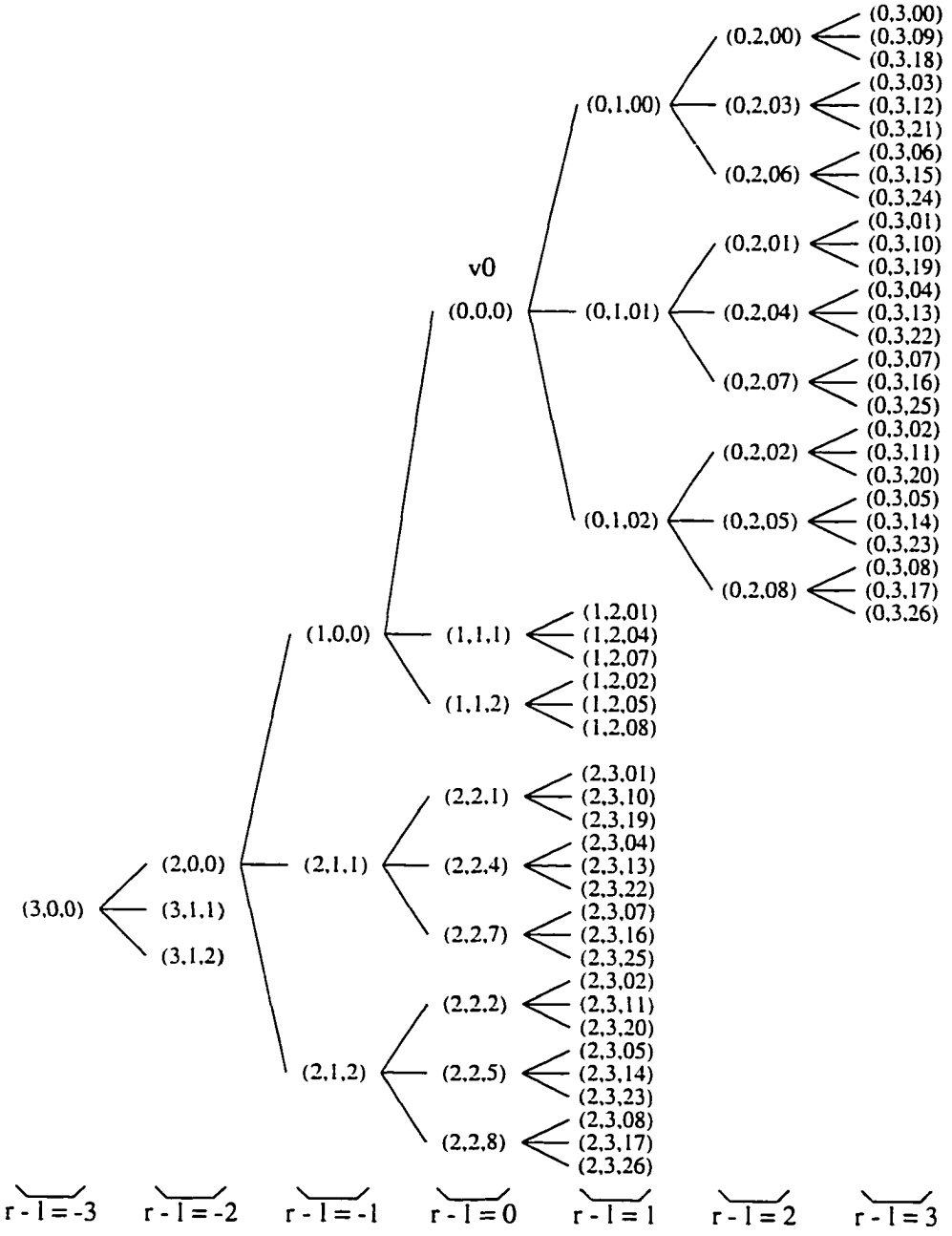


Figure 4.1: Representation of vertices

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

As an example, the diagram in Figure 4.1 displays a portion of the tree $\mathcal{T}_p$ for $p = 3$, with the vertices labeled (`Limb`, `Radius`, `Branch`).

Notice that each vertex (ℓ, r, b) is adjacent to the vertex numbered $(\ell+1, r, b)$ or $(\ell, r-1, b/p)$, and to the p vertices $(\ell, r+1, b+kp^r)$, for $k = 0, 1, \ldots, p-1$. The distance of the vertex (ℓ, r, b) from the center vertex $v_0 = (0, 0, 0)$ is $\ell + r$.

Two functions are provided in `vertices.c`. `Distance` calculates the length of the shortest path connecting two vertices in the tree $\mathcal{T}_p$. The function `ApplyGroupElement` calculates the effect of applying a matrix from $\mathrm{GL}_2(\mathbb{Z})$ to a vertex of $\mathcal{T}_p$. Section 4.5 discusses this computation in detail.

4.5 Computation of the Action of $M \in \mathrm{SL}_2(\mathbb{Q}_p)$ on $\mathcal{T}_p$

Let M be a matrix in $\mathrm{SL}_2(\mathbb{Q}_p)$. Since every p-adic rational in $\mathbb{Q}_p$ can be written as a p-adic integer in $\mathbb{Z}_p$ divided by a power of p, the matrix M can be written as

$$M = \frac{1}{p^n}\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix},$$

where the m_{ij} are p-adic integers, $m_{11}m_{22} - m_{12}m_{21} = p^{2n}$ in $\mathbb{Z}_p$, and not all of the m_{ij} are divisible by p. The matrix M has the same action on the tree as the matrix

$$p^n M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p).$$

Consequently, matrices in $\mathrm{SL}_2(\mathbb{Q}_p)$ can be identified with matrices from $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ with $\det M = p^{2n}$ for some $n \in \mathbb{N}$, for the purpose of programming a computer to find a quotient graph.

The action of this matrix on a lattice in standard form is given by

$$\mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix} \quad \longmapsto \quad \mathbb{Z}_p \begin{bmatrix} m_{11}b + m_{12}p^\ell \\ m_{21}b + m_{22}p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} m_{11}p^r \\ m_{21}p^r \end{bmatrix}.$$

Proposition 4.7 rewrites the resulting lattice in standard form. The computation splits into two cases, because one particular value for b requires special handling, somewhat analogous to the case division by zero on a projective line.

Proposition 4.7. *Choose a matrix $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ with $\det M = p^{2n}$ along with a vertex $v \in \mathcal{T}_p$ represented as a lattice in standard form, so that*

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \qquad \text{and} \qquad v = \mathbb{Z}_p \begin{bmatrix} b \\ p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^r \\ 0 \end{bmatrix}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Let s equal the largest power of p dividing $(m_{21}b + m_{22}p^{\ell})$, and let t equal the largest power of p dividing m_{21}. If $(m_{21}b + m_{22}p^{\ell}) = 0$, treat s as $+\infty$. If $m_{21} = 0$, treat t as $+\infty$.

(1) (Special Case) If $s \geq r + t$, then

$$b \equiv -(m_{22}p^{\ell}/p^{t})(m_{21}/p^{t})^{-1} \pmod{p^{r}}$$

and the action of M on the vertex v is given by

$$\mathbb{Z}_p \begin{bmatrix} b \\ p^{\ell} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{r} \\ 0 \end{bmatrix} \longmapsto \mathbb{Z}_p \begin{bmatrix} (m_{11})(m_{21}/p^{t})^{-1}p^{r} \\ p^{r+t} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{2n+\ell-t} \\ 0 \end{bmatrix}.$$

(2) (Normal Case) If $s \leq r + t$, then M acts on v by

$$\mathbb{Z}_p \begin{bmatrix} b \\ p^{\ell} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{r} \\ 0 \end{bmatrix} \longmapsto$$
$$\mathbb{Z}_p \begin{bmatrix} (m_{11}b + m_{12}p^{\ell})((m_{21}b + m_{22}p^{\ell})/p^{s})^{-1} \\ p^{s} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{2n+\ell+r-s} \\ 0 \end{bmatrix}.$$

In each case, the resulting lattice may still require a power of p to be factored out in order to reduce it to standard form.

Proof. First note that if $(m_{21}b + m_{22}p^{\ell}) = 0$ and $m_{21} = 0$, then $m_{22} = 0$, so $\det M = m_{11}m_{22} - m_{12}m_{21} = 0$, which is not possible since the determinant of M is p^{2n}.

Proof of Special Case. If $s \geq r + t$ then b is uniquely determined by ℓ, r, m_{21} and m_{22}.

$$\begin{aligned} m_{21}b + m_{22}p^{\ell} &\equiv 0 \pmod{p^{r+t}} \\ p^{t}(m_{21}/p^{t})b &\equiv -m_{22}p^{\ell} \pmod{p^{r+t}} \\ p^{t}b &\equiv -m_{22}p^{\ell}(m_{21}/p^{t})^{-1} \pmod{p^{r+t}} \\ b &\equiv -(m_{22}p^{\ell}/p^{t})(m_{21}/p^{t})^{-1} \pmod{p^{r}}. \end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In this special case:

$$\begin{aligned}
&\mathbb{Z}_p \begin{bmatrix} m_{11}p^r \\ m_{21}p^r \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} m_{11}b + m_{12}p^\ell \\ m_{21}b + m_{22}p^\ell \end{bmatrix} \\
&= \mathbb{Z}_p \begin{bmatrix} m_{11}p^r \\ m_{21}p^r \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} (m_{11}b + m_{12}p^\ell)(m_{21}/p^t) - (m_{11}p^r)(m_{21}b + m_{22}p^\ell)/p^{r+t} \\ (m_{21}b + m_{22}p^\ell)(m_{21}/p^t) - (m_{21}p^r)(m_{21}b + m_{22}p^\ell)/p^{r+t} \end{bmatrix} \\
&= \mathbb{Z}_p \begin{bmatrix} m_{11}p^r \\ (m_{21}/p^t)p^{r+t} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} (m_{12}m_{21} - m_{11}m_{22})(p^\ell/p^t) \\ 0 \end{bmatrix} \\
&= \mathbb{Z}_p \begin{bmatrix} m_{11}(m_{21}/p^t)^{-1}p^r \\ p^{r+t} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} -p^{2n+\ell-t} \\ 0 \end{bmatrix}.
\end{aligned}$$

Proof of Usual Case. In the usual case, $s \leq r + t$:

$$\begin{aligned}
&\mathbb{Z}_p \begin{bmatrix} m_{11}b + m_{12}p^\ell \\ m_{21}b + m_{22}p^\ell \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} m_{11}p^r \\ m_{21}p^r \end{bmatrix} \\
&= \mathbb{Z}_p \begin{bmatrix} m_{11}b + m_{12}p^\ell \\ m_{21}b + m_{22}p^\ell \end{bmatrix} \\
&\quad + \mathbb{Z}_p \begin{bmatrix} (m_{11}p^r)((m_{21}b + m_{22}p^\ell)/p^s) - (m_{11}b + m_{12}p^\ell)((m_{21}p^r)/p^s) \\ (m_{21}p^r)((m_{21}b + m_{22}p^\ell)/p^s) - (m_{21}b + m_{22}p^\ell)((m_{21}p^r)/p^s) \end{bmatrix} \\
&= \mathbb{Z}_p \begin{bmatrix} m_{11}b + m_{12}p^\ell \\ p^s(m_{21}b + m_{22}p^\ell)/p^s \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} (m_{11}m_{22} - m_{12}m_{21})(p^{r+\ell}/p^s) \\ 0 \end{bmatrix} \\
&= \mathbb{Z}_p \begin{bmatrix} (m_{11}b + m_{12}p^\ell)((m_{21}b + m_{22}p^\ell)/p^s)^{-1} \\ p^s \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{2n+\ell+r-s} \\ 0 \end{bmatrix}.
\end{aligned}$$

□

The function `ApplyGroupElement` in the file `vertices.c` applies a matrix $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ to a vertex $v \in \mathcal{T}_p$, using the formulas from Proposition 4.7, and returns the resulting vertex. However, there is an additional complication. As discussed in Section 4.3, the p-adic entries $m_{ij} \in \mathbb{Z}_p$ of M are approximated by numbers in $\mathbb{Z}/(\texttt{PadicMod})$, so only `ExponentMax` digits of accuracy are available for the computation. If this is not enough, then `ApplyGroupElement` signals an error by returning a "vertex" `ErrorVert` with a negative value for `Limb`.

The code performing the computation is given below. First, the program calculates s, t, $v_1 = (m_{21}b + m_{22}p^\ell)/p^s$ and $v_2 = m_{21}/p^t$:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

```
/* Calculate S, T, v1, v2 */
v1 = PdAddTwoMults(m21, (Padic) Vert.Branch, m22, PtoN[Vert.Limb]);
v2 = m21;
if (v1 == 0) {
  if (v2 == 0) return ErrorVert;
  S = ExponentMax;
} else { S = 0; while (v1 % P == 0) { S++; v1 /= P; } }
if (v2 == 0) T = ExponentMax;
else { T = 0; while (v2 % P == 0) { T++; v2 /= P; } }
```

In the special case of $s \geq r + t$, the target vertex is

$$\mathbb{Z}_p \begin{bmatrix} (m_{11})(m_{21}/p^t)^{-1}p^r \\ p^{r+t} \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{2n+\ell-t} \\ 0 \end{bmatrix}.$$

Since only ExponentMax accurate digits are known for m_{11} and m_{21}, the expression "$(m_{11})(m_{21}/p^t)^{-1}p^r$" can only be computed up to ExponentMax $- t + r$ digits of accuracy. In order to reduce this to a branch number between 0 and $p^{2n+\ell-t}$, the program requires $2n + \ell - t$ accurate digits. Otherwise, the computation cannot be completed, and an error must be reported. The code for this case is:

```
/* Handle Special Case */
if (T + Vert.Radius <= S) {
  VertTo.Radius = TwiceTuplePower + Vert.Limb - T;
  if (ExponentMax - T + Vert.Radius < VertTo.Radius)
    return ErrorVert;
  VertTo.Limb = Vert.Radius + T;
  if (VertTo.Radius < Vert.Radius) v3 = 0;
  else {
    v3 = PdMultiply(m11, PdInverse(v2));
    v3 = (v3 % PtoN[VertTo.Radius - Vert.Radius])
         * PtoN[Vert.Radius];
  }
}
```

In the normal case of $s \leq r + t$, the target vertex is

$$\mathbb{Z}_p \begin{bmatrix} (m_{11}b + m_{12}p^\ell)((m_{21}b + m_{22}p^\ell)/p^s)^{-1} \\ p^s \end{bmatrix} + \mathbb{Z}_p \begin{bmatrix} p^{2n+\ell+r-s} \\ 0 \end{bmatrix}.$$

The expression "$(m_{11}b + m_{12}p^\ell)((m_{21}b + m_{22}p^\ell)/p^s)^{-1}$" can be computed with an accuracy of ExponentMax $- s$ digits. In order to obtain the new branch number, $2n + \ell + r - s$ digits of accuracy are required. The code below performs this computation.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

```
/* Handle General Case */
else {
  VertTo.Radius = TwiceTuplePower + Vert.Limb + Vert.Radius - S;
  if (ExponentMax - S < VertTo.Radius) return ErrorVert;
  VertTo.Limb = S;
  v3 = PdAddTwoMults(m11, (Padic) Vert.Branch, m12,
                     PtoN[Vert.Limb]);
  v3 = PdMultiply(v3, PdInverse(v1)) % PtoN[VertTo.Radius];
}
```

For the final step of the computation, any extra factors of p are factored out of the new lattice in order to reduce it to standard form.

```
/* Reduce to Standard Form */
while (VertTo.Limb > 0 && VertTo.Radius > 0 && v3 % P == 0)
  { VertTo.Limb--; VertTo.Radius--; v3 /= P; }
VertTo.Branch = (VertexNum) v3;
if ((Padic) VertTo.Branch != v3) VertTo.Limb = -2;
return VertTo;
```

4.6 Representation of the Tree $\mathcal{T}_p$

The $(p+1)$-regular tree $\mathcal{T}_p$ is unbounded and cannot be represented in a computer's finite memory. Instead, a maximum radius, RadiusMax, is chosen, and the subtree consisting of all vertices (ℓ, r, b) satisfying $\ell + r \leq$ RadiusMax is used as a substitute. Figure 2.1 (p. 11) shows a subtree of $\mathcal{T}_3$ with RadiusMax $= 4$.

4.6.1 Selection of RadiusMax

In order to obtain the complete quotient graph $\mathcal{X}_{p,L}$, the value selected for RadiusMax must yield a subtree large enough to completely cover $\mathcal{X}_{p,L}$. In order to cover every edge in the quotient graph, each of the outermost vertices in the covering subtree must be identified in $\mathcal{X}_{p,L}$ with one of the subtree's inner vertices.

On the other hand, an increase in RadiusMax significantly increases the time and memory required for the computation of the quotient graph. The resources required by the program grow as an exponential function of RadiusMax. Consequently, it is desirable to choose RadiusMax to be as large as necessary, but no larger.

There are p^r vertices with Limb $= 0$ and Radius $= r$. There are another p^{r-1} vertices with Limb > 0 and Limb + Radius $= r$. (See Figure 4.2 on page 60.) Hence,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

the subtree of $\mathcal{T}_p$ with maximum radius RadiusMax contains

$$(p^0 + \cdots + p^{\texttt{RadiusMax}}) + (p^0 + \cdots + p^{\texttt{RadiusMax}-1}) = \frac{p^{\texttt{RadiusMax}}(p+1) - 2}{p-1}$$

vertices. Table 4.3 gives the number of vertices, VertexNumMax for values of p and RadiusMax with $p \leq 17$ and VertexNumMax $< 10^8$.

RadiusMax	$p = 3$	$p = 5$	$p = 7$	$p = 11$	$p = 13$	$p = 17$
1	5	7	9	13	15	19
2	17	37	65	145	197	325
3	53	187	457	1597	2563	5527
4	161	937	3201	17569	33321	93961
5	485	4687	22409	193261	433175	1597339
6	1457	23437	156865	2125873	5631277	27154765
7	4373	117187	1098057	23384605	73206603	
8	13121	585937	7686401			
9	39365	2929687	53804809			
10	118097	14648437				
11	354293	73242187				
12	1062881					
13	3188645					
14	9565937					
15	28697813					
16	86093442					

Table 4.3: Number of vertices in subtrees of $\mathcal{T}_p$

Table 4.4 on page 66 lists the values for RadiusMax that were actually required to compute the quotient graph $\mathcal{X}_{p,L}$ for various values of p and L. The largest value used was RadiusMax = 13 and VertexNumMax = 3188645, for the quotient graphs $\mathcal{X}_{3,35}$ and $\mathcal{X}_{3,40}$.

4.6.2 Enumeration of the Vertices of the Subtree

Once the values for RadiusMax and VertexMax have been selected, each vertex in the subtree is assigned a positive integer from 1 up through VertexMax. First, the vertices with Limb = 0 are assigned numbers in order of Radius and then Branch. So when $p = 3$ and RadiusMax = 3, the numbering begins:

$$(0,0,0) = 1, \quad (0,2,0) = 5, \quad (0,2,4) = 9, \quad (0,2,8) = 13,$$
$$(0,1,0) = 2, \quad (0,2,1) = 6, \quad (0,2,5) = 10, \quad (0,3,0) = 14,$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$(0,1,1) = 3, \quad (0,2,2) = 7, \quad (0,2,6) = 11, \quad \ldots,$$
$$(0,1,2) = 4, \quad (0,2,3) = 8, \quad (0,2,7) = 12, \quad (0,3,26) = 40.$$

Consequently, vertex $(0, \texttt{Radius}, \texttt{Branch})$ is assigned the number

$$1 + \left(p^0 + p^1 + \cdots + p^{\texttt{Radius}-1}\right) + \texttt{Branch} = 1 + \texttt{SumPtoN1}[\texttt{Radius} - 1] + \texttt{Branch}.$$

After all vertices with $\texttt{Limb} = 0$ are numbered, the vertices on the other side of the tree are assigned numbers in order of $\texttt{Limb} + \texttt{Radius}$ and then $p^{\texttt{Limb}-1} \cdot \texttt{Branch}$. So when $p = 3$ and $\texttt{RadiusMax} = 3$, the numbering continues:

$$(1,0,0) = 41, \quad (3,0,0) = 45, \quad (1,2,4) = 49, \quad (1,2,8) = 53.$$
$$(2,0,0) = 42, \quad (1,2,1) = 46, \quad (1,2,5) = 50,$$
$$(1,1,1) = 43, \quad (1,2,2) = 47, \quad (2,1,2) = 51,$$
$$(1,1,2) = 44, \quad (2,1,1) = 48, \quad (1,2,7) = 52,$$

The vertex $(\texttt{Limb}, \texttt{Radius}, \texttt{Branch})$ with $\texttt{Limb} > 0$ is assigned the number

$$1 + \texttt{SumPtoN1}[\texttt{RadiusMax} + 1] + \texttt{SumPtoN1}[\texttt{Limb} + \texttt{Radius} - 1] + p^{\texttt{Limb}-1}\texttt{Branch}.$$

The vertex number 0 is reserved to signal an error.

The graph in Figure 4.2 illustrates the vertex numbering scheme for a subtree of $\mathcal{T}_p$ with $p = 3$ and $\texttt{RadiusMax} = 3$.

Under this enumeration, a vertex with limb $\ell = 0$, radius r and number `VertNum` is adjacent to the p vertices numbered:

$$\left\{ \texttt{VertNum} + p^r, \texttt{VertNum} + 2p^r, \ldots, \texttt{VertNum} + p^{r+1} \right\}.$$

If $r > 0$, the vertex is also adjacent to the vertex numbered:

$$\left[(\texttt{VertNum} - \texttt{SumPtoN1}[r] - 1) \bmod p^{r-1}\right] + \texttt{SumPtoN1}[r - 1] + 1.$$

One useful feature of this enumeration is that the numbers assigned to vertices with $\texttt{Limb} = 0$ are independent of the value of `RadiusMax`. One consequence is that after the quotient graph has been completely computed, the vertex numbers in the quotient graph are independent of the choice of `RadiusMax` used to generate the graph.

The file `tree.h` provides two useful macros. `VertToVertNum` converts a vertex from the representation $(\texttt{Limb}, \texttt{Radius}, \texttt{Branch})$ into the number assigned to it. The macro `IterateThroughHalfTree(Vert, VertNum)` expands into code which iterates `Vert` through all of the tree vertices with $\texttt{Vert.Limb} = 0$. Simultaneously, `VertNum` iterates through the corresponding vertex numbers.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

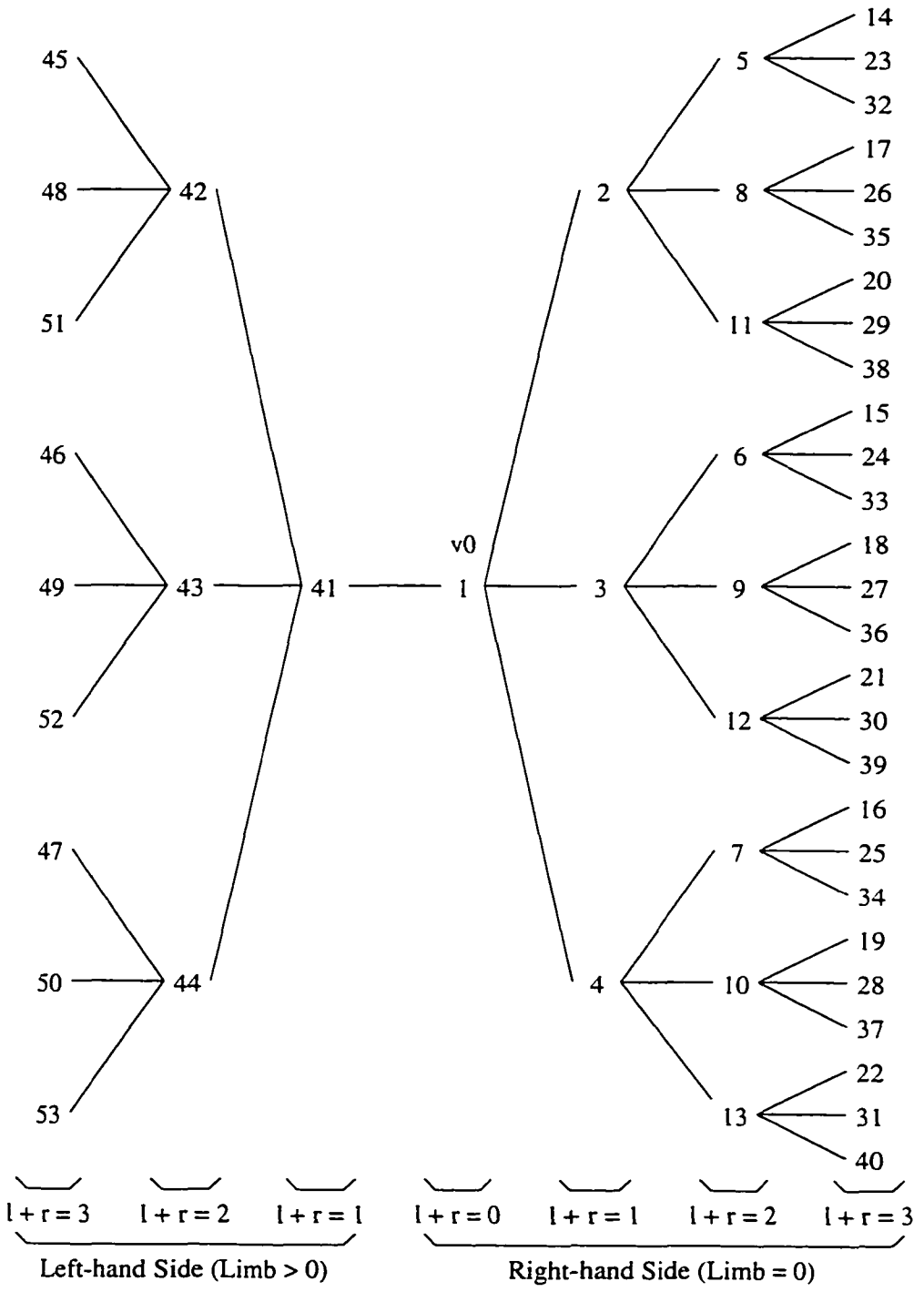


Figure 4.2: Enumeration of subtree vertices

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

4.6.3 An Important Optimization

During the computation of the quotient graph, an early version of the program applied each group element $(n : a_1, a_2, a_3, a_4)$ in the tuple input file to every vertex within the subtree of radius `RadiusMax`. Consequently, the number of times the function `ApplyGroupElement` was executed per tuple was an exponent function of `RadiusMax`. This is very slow. The computation of the quotient graph $\mathcal{X}_{3,40}$ required a subtree of over three million vertices.

Most of these computations do not provide any useful information. Given $M \in \Gamma_{p,L}$ and a vertex v in the subtree, the vertex $M \cdot v$ usually lies outside the subtree, so the information obtained by computing $M \cdot v$ is discarded.

For a given M, it is possible to use the eigenvectors of M to identify those vertices v such that both v and $M \cdot v$ lie within the subtree before bothering to compute $M \cdot v$.

Suppose that

$$\lambda = a \pm \sqrt{-(p^{2n} - a^2)} \quad \text{is an eigenvalue of} \quad M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p),$$

where $0 < a < p^n$, $\det M = p^{2n}$, $\operatorname{tr} M = 2a$ and $a = p^t a'$ with $p \nmid a'$. Then

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \begin{bmatrix} P \\ Q \end{bmatrix} = \lambda \begin{bmatrix} P \\ Q \end{bmatrix} \Longrightarrow$$

$$(m_{11} - \lambda)P + (m_{12})Q = 0 \text{ and } (m_{21})P + (m_{22} - \lambda)Q = 0,$$

so an eigenvector of M for λ is given by

$$\begin{bmatrix} P \\ Q \end{bmatrix} = \begin{bmatrix} m_{12} \\ \lambda - m_{11} \end{bmatrix} = \begin{bmatrix} \lambda - m_{22} \\ m_{21} \end{bmatrix}.$$

If $m_{12} = 0$ and $m_{11} = \lambda$, then the first vector formula produces $[0\ \ 0]^t$, so use the second. If $m_{21} = 0$ and $m_{22} = \lambda$, then use the first. If both vector formulas produce $[0\ \ 0]^t$, then M is a scalar multiple of the identity, so all vertices are held fixed.

M is a translation, so M has two distinct eigenvalues, λ_0 and λ_1, with

$$\lambda_0 \equiv 0 \pmod{p^n} \quad \text{and} \quad \lambda_1 \equiv 2a \pmod{p^n},$$

because

$$0 = \lambda^2 - (\operatorname{tr} M)\lambda + (\det M) \equiv \lambda^2 - 2a\lambda = \lambda(\lambda - 2a) \pmod{p^{2n}}$$

and $0 < a < p^n$. Let ω_0 and ω_1 be the boundary points in Ω corresponding to the eigenvectors of λ_0 and λ_1, respectively.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

By Proposition 3.2, M translates the geodesic (ω_0, ω_1) by distance $2n - 2t$ from ω_0 towards ω_1. By Proposition 3.3, the distance from v_0 to (ω_0, ω_1) is t. There are two important consequences:

(1) If v is a vertex with both v and $M \cdot v$ within distance RadiusMax of v_0, then $2n - 2t \leq 2(\texttt{RadiusMax} - t)$ so $n \leq \texttt{RadiusMax}$. Therefore, only tuples $(n : a_1, a_2, a_3, a_4)$ with $n \leq \texttt{RadiusMax}$ are worth consideration.

(2) All such v form a subtree of radius $\texttt{RadiusMax} - n$ within the domain of Map[] including the point closest to the boundary point ω_0.

Consequently, it is now only necessary to apply a tuple $(n : a_1, a_2, a_3, a_4)$ to vertices in the appropriate subtree of radius $\texttt{RadiusMax} - n$, instead of a subtree of radius RadiusMax. This is an extremely good improvement, in part because n is nearly as large as RadiusMax for the vast majority of the tuples under consideration.

4.7 Representation of the Quotient Maps

The quotient map

$$\phi : \mathcal{T}_p \longrightarrow \mathcal{X}_{p,L} = \Gamma_{p,L} \backslash \mathcal{T}_p \quad \text{or} \quad \phi' : \mathcal{T}_p \longrightarrow \mathcal{X}'_{p,L} = \Gamma'_{p,L} \backslash \mathcal{T}_p$$

is represented by an array Map[] with indices $0, 1, \ldots,$ VertexNumMax, where VertexNumMax equals the number of vertices in the subtree of $\mathcal{T}_p$ with radius RadiusMax. The quotient map ϕ is computed by applying elements of the group $\Gamma_{p,L}$ to vertices in the tree $\mathcal{T}_p$, and updating the array Map[] to include the new information.

Initially, $\texttt{Map}[v] = v$ for each vertex number v, representing the identity map $\mathcal{T}_p \longrightarrow \mathcal{T}_p$. Each time a group element x is applied to a vertex v, the array Map is updated so that $\texttt{Map}[v] = \texttt{Map}[x \cdot v]$, indicating that the vertices v and $x \cdot v$ are identified in the quotient graph. After the quotient map has been entirely determined, $\texttt{Map}[v] = w$, where w is the smallest vertex number such that the vertices represented by v and w are identified in the quotient graph $\mathcal{X}_{p,L}$.

4.7.1 Quotient Map File Names

Quotient maps are stored in files whose names indicate the values of p and L, the radius RadiusMax of the subtree of $\mathcal{T}_p$ used for the domain, and the value for PowerMax, which indicates the group elements whose actions have already been incorporated into the quotient map.

For example, a file named "M-P3-R5-T0" contains a list of numbers representing a quotient map from the subtree of the $(3+1)$-regular tree $\mathcal{T}_3$ with $\texttt{RadiusMax} = 5$. No

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

tuples have yet been applied to this map, as `PowerMax = 0`, so the file still contains an isomorphism.

A file named "`M-G2-P3-L40-R13-T12`" contains the current state of computation of the quotient map $\mathcal{T}_3 \longrightarrow \mathcal{X}_{3,40}$ with $p = 3$ and $L = 40$. A value of 13 was chosen for `RadiusMax`, and all tuples $(n : a_1, a_2, a_3, a_4)$ in the group $\Gamma_{3,40}$ with $n \leq 12$ have already been applied to the subtree, and the results reflected in the quotient map `M-G2-P3-L40-R13-T12`.

4.7.2 Quotient Map Files and Programs

The files `tree.h` and `tree.c` allocate memory for the quotient map and provide functions to read and store the map to disk. The function `LoadMap` reads a quotient map from a file and loads it into the computer's memory. `SaveMap` stores the current state of the quotient map into a file with an appropriate file name.

The program `MapCreate` generates an quotient map for given values of p and `RadiusMax`, initialized as an isomorphism.

The program `MapPrint` reads a map from an input file and displays a representation of the quotient graph image. Each distinct vertex in the quotient graph is displayed, along with a list of adjacent vertices. If the quotient map does not correspond to a complete compact graph, then adjacent vertices that lie outside of `RadiusMax` are printed within brackets. Thus, MapPrint can be used to judge how close the computation of a quotient graph is to completion.

Once the computation of a quotient map is complete, the program `QuotientGraph` reads the file containing the quotient map $\mathcal{T}_p \longrightarrow \mathcal{X}_{p,L}$ or $\mathcal{T}_p \longrightarrow \mathcal{X}'_{p,L}$ and creates a new file containing a representation of the quotient graph $\mathcal{X}_{p,L}$ or $\mathcal{X}'_{p,L}$. The name of the new file indicates its contents. A file named "`Q-G2-P3-L5-V30`" contains a representation of the quotient graph $\mathcal{X}_{3,5}$, displayed in Figure 4.8. The "`V30`" indicates that the graph has 30 vertices.

The actual computation of the quotient graph is performed by the program `MapSmush`. When provided with one input file containing a list of group elements represented as standard tuples and another input file containing a quotient map, `MapSmush` applies each variant of each of the tuples to the vertices in the subtree of radius `RadiusMax`. The resulting information is incorporated into the quotient map, and a new file is created containing the updated quotient map. As an example, the execution of "`MapSmush M-G2-P3-L40-R13-T4 TC-G2-P3-L40-T5-8`" will store its output in "`MapSmush M-G2-P3-L40-R13-T8`".

The program `TupleSmush` performs the same function as `MapSmush`, except that `TupleSmush` also creates a file listing only those tuples which provided useful information during the computation of the quotient map. Many of the tuples generated

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

by TupleCreate produce redundant information because they identify vertices that have already been identified by an earlier group element. This additional feature of TupleSmush is intended to permit quotient map files to be recomputed by MapSmush using only a fraction of the running time required during the initial computation. The full quotient map file can require much more disk space than the trimmed file of tuples required to generate it. Tuples output from TupleSmush need to be sorted by TupleSort.

TupleFilter loads a quotient map from one input file and reads tuples from another. Most tuples with non-trivial action on the quotient tree are eliminated, and the remaining tuples are stored in a named "TF-G%d-P%d-L%d-T%d-%d". As currently implemented, some wrong tuples can slip into the output file, but no correct tuples will be omitted. If the radius is larger, then errors are less likely to occur.

TupleHunt is given a short list of vertex numbers and a file of standard tuples. TupleHunt identifies any tuple variant that maps one of the given vertex numbers to a smaller numbered vertex. This program is intended to be used when a file of tuples is too large to be handled by TupleProduct plus TupleTrim and MapSmush. The optimization to MapSmush described in Section subsection:program-tree-optimization has largely rendered this use of TupleHunt obsolete.

The programs TupleFilter and TupleHunt proved useful during the debugging of MapSmush. When an obviously incorrect quotient graph was generated by MapSmush, these two programs could be used to identify which tuple was involved in the erroneous computation. Errors in the implementation were usually discovered when the computed quotient graph contained only one or two vertices.

4.8 Stopping Conditions and Program Correctness

Given values for p and L, the computation of $\mathcal{X}_{p,L}$ or $\mathcal{X}'_{p,L}$ proceeds as follows:

(1) Select a value for RadiusMax, as discussed in Section 4.6.1.

(2) Invoke MapCreate to create a file "M-P⟨p⟩-R⟨RadiusMax⟩-T0" containing a map $\mathcal{T}_p \longrightarrow \mathcal{T}_p$, restricted to a subtree of radius RadiusMax, initialized as an isomorphism. Change the name of this file to "M-G⟨G⟩-P⟨p⟩-L⟨L⟩-R⟨RadiusMax⟩-T0".

(3) Select a positive integer for PowerMax, at most RadiusMax. Set PowerMin = 1.

(4) Invoke TupleCreate1 (for $Q^1(\mathbb{Z}[1/p])$), TupleCreate2 (for $\mathcal{X}_{p,L}$) or TupleCreate3 (for $\mathcal{X}'_{p,L}$) to generate the file "TC-G⟨G⟩-P⟨p⟩-L⟨L⟩-T⟨PowerMin⟩-⟨PowerMax⟩".

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(5) Invoke `MapSmush` (or `TupleSmush`) to apply these tuples to update the quotient map $\mathcal{T}_p \longrightarrow \mathcal{T}_p$. A new file "`M-G`$\langle G \rangle$`-P`$\langle p \rangle$`-L`$\langle L \rangle$`-R`$\langle$`RadiusMax`$\rangle$`-T`$\langle$`PowerMax`$\rangle$" will be produced.

(6) Use `MapPrint` or `QuotientGraph` to determine if the resulting quotient map has a compact image. If so, then invoke `QuotientGraph` to produce $\mathcal{X}_{p,L}$.

(7) If the image is not compact, and if `PowerMax` $<$ `RadiusMax`, then change `PowerMin` to `PowerMin` $=$ `PowerMax` $+ 1$. Choose `PowerMax` with `PowerMin` $\leq$ `PowerMax` $\leq$ `RadiusMax`. Go back to step (4).

(8) If `PowerMax` $\geq$ `RadiusMax` but the imap image is not yet compact, then `RadiusMax` is too small. Increase `RadiusMax`, then return to step (2) and try again.

This procedure terminates when the image of $\mathcal{T}_p \longrightarrow \mathcal{T}_p$ given by `Map[]` is compact. That is, when each of the outermost vertices in the radius `RadiusMax` subtree is identified with one of the inner vertices. There are two problems that could arise:

(1) The computed image never becomes compact; or

(2) The procedure terminates with a compact image, but the image is still larger than the actual quotient graph.

Both problems arise because two vertices in `Map[]` may not identified correctly, so that `Map`$[v_1] \neq$ `Map`$[v_2]$ even though v_1 and v_2 are identified in the quotient graph.

For every choice of p and L, $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$ are compact, so there must exist some value of `RadiusMax` so that the subtree of $\mathcal{T}_p$ covers $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$. Then, for every two vertices in this subtree whose images should be identified in the quotient graph, there exists some tuple $(n : a_1, a_2, a_3, a_4)$ in the relevant group, $\Gamma_{p,L}$ or $\Gamma'_{p,L}$, with $n \leq$ `RadiusMax` that maps one to the other.

The only remaining problem is that the computation of the tuple's action on the vertex may not complete if the computation requires more than `ExponentMax` digits on accuracy.

In any case, it is always possible to detect whether or not the computed quotient graph is correct. Both `MapPrint` and `QuotientGraph` can determine whether the computed quotient map `Map[]` is compact and to count the number of vertices in its image. Then the computed quotient graph is correct if and only if it is compact and the number of vertices agrees with the formula in Corollary 3.31.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

4.9 Program Results

Table 4.4 lists all values p and L for which quotient graphs $\mathcal{X}_{p,L}$ were computed. In each case, the number of vertices in the computed quotient graph agreed with the formulas derived in Chapter III and the values listed in Table 3.1. The p-adic numbers were represented using unsigned 64-bit integers. Also, columns R and T give the values for `RadiusMax` and `PowerMax` required to produce the quotient graph.

Figures 4.3 through 4.11 illustrate some of the quotient graphs generated by these programs. In each graph, the vertices are arranged in a circle and labeled with the smallest nembers assigned to vertices in their inverse images in $\mathcal{T}_p$. The numbering system is the same one described in Section 4.6.2.

P	L	R	T
3	2	2	1
3	4	4	2
3	5	6	4
3	7	7	6
3	8	7	6
3	10	7	6
3	11	10	9
3	13	10	8
3	14	8	6
3	16	9	8
3	17	10	8
3	19	11	10
3	20	9	8
3	22	10	9
3	25	12	10
3	26	11	10
3	28	11	10
3	32	12	10
3	35	13	11
3	40	13	12

P	L	R	T
5	2	2	1
5	3	3	2
5	4	4	3
5	6	4	3
5	7	5	4
5	8	7	6
5	9	6	4
5	11	7	6
5	12	5	4
5	13	7	6
5	14	7	6
5	16	7	6
5	18	7	6

P	L	R	T
7	2	3	2
7	3	4	3
7	4	3	2
7	5	4	3
7	6	4	3
7	8	5	4
7	9	6	5
7	10	5	4
7	11	6	5
7	12	5	4
7	13	6	5
7	15	6	5
7	16	6	4
7	18	6	5

Table 4.4: Values for `RadiusMax` and `PowerMax` used to compute $\mathcal{X}_{p,L}$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

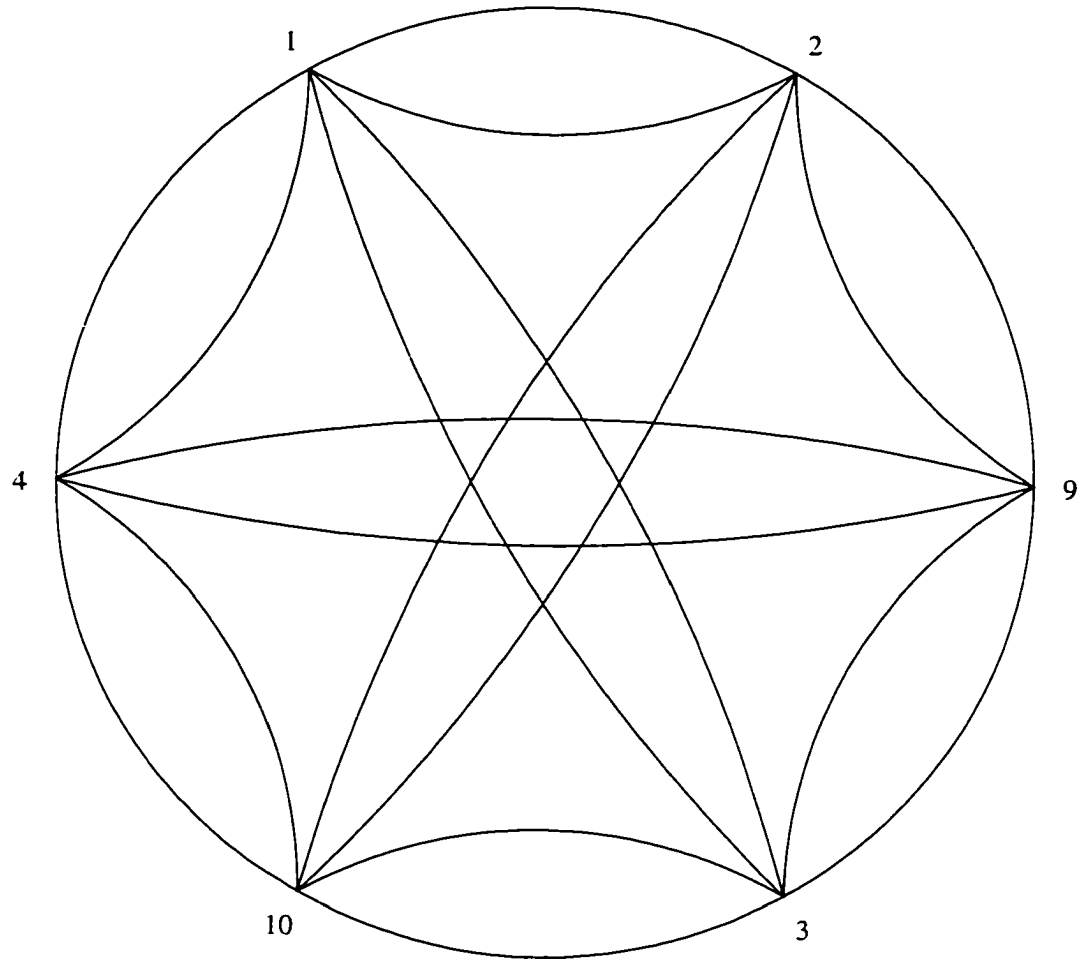


Figure 4.3: The quotient graph $\mathcal{X}_{5,3} = \Gamma_{5,3}\backslash\mathcal{T}_5$ has 6 vertices and 18 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

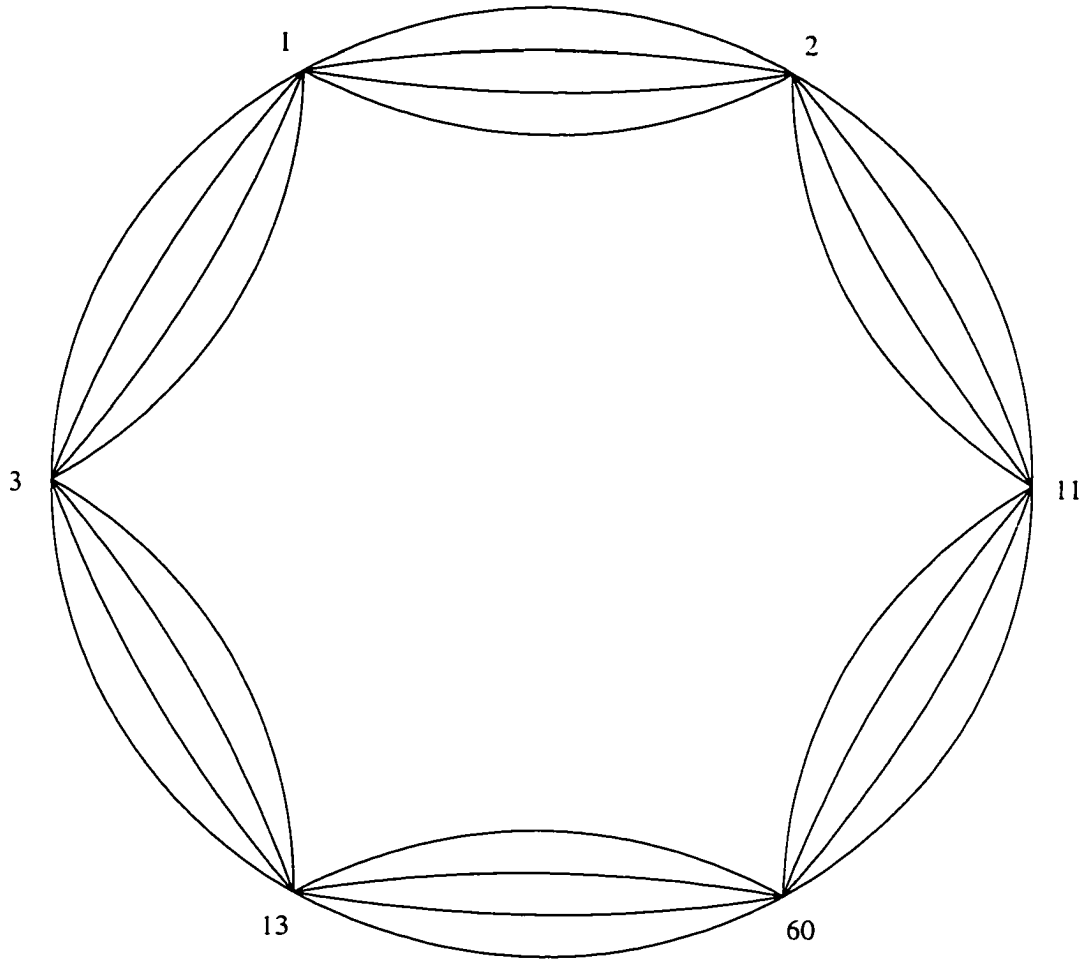


Figure 4.4: The quotient graph $\mathcal{X}_{7,3} = \Gamma_{7,3} \backslash \mathcal{T}_7$ has 6 vertices and 24 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

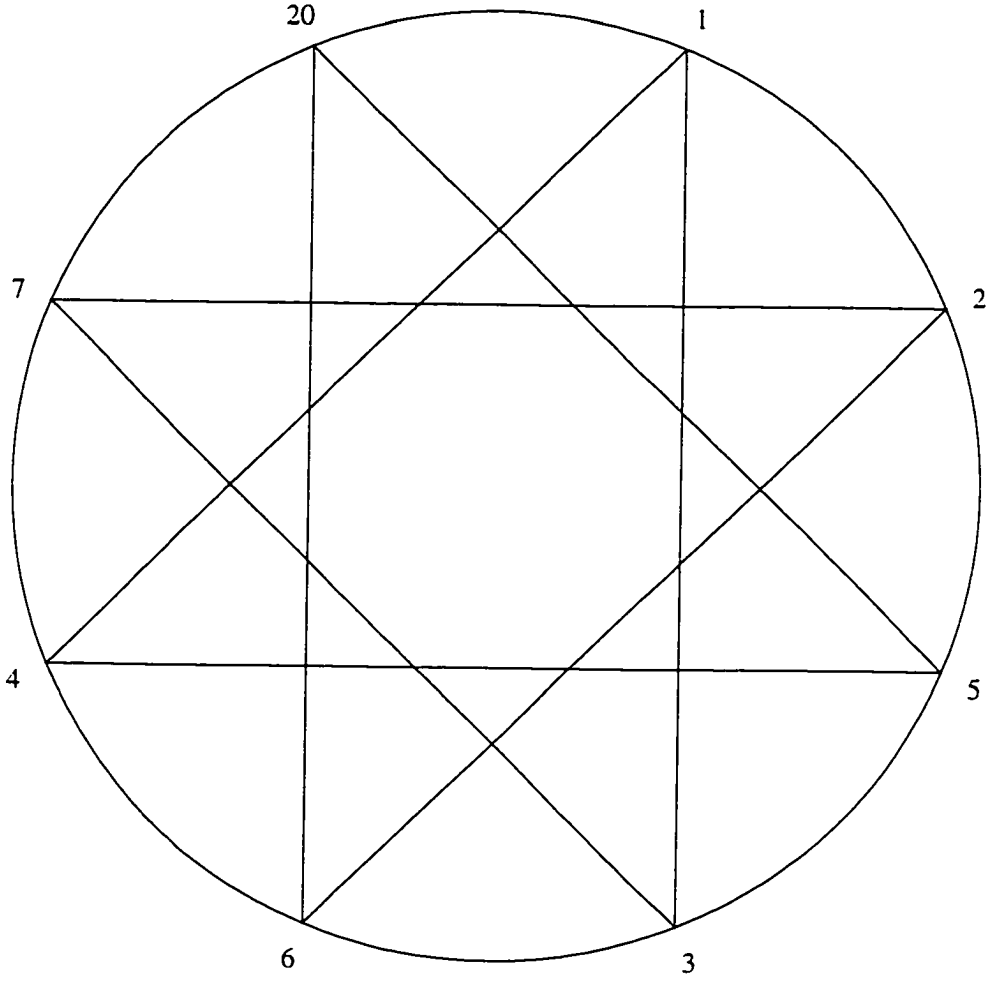


Figure 4.5: The quotient graph $\mathcal{X}_{3,4} = \Gamma_{3,4} \backslash \mathcal{T}_3$ has 8 vertices and 16 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

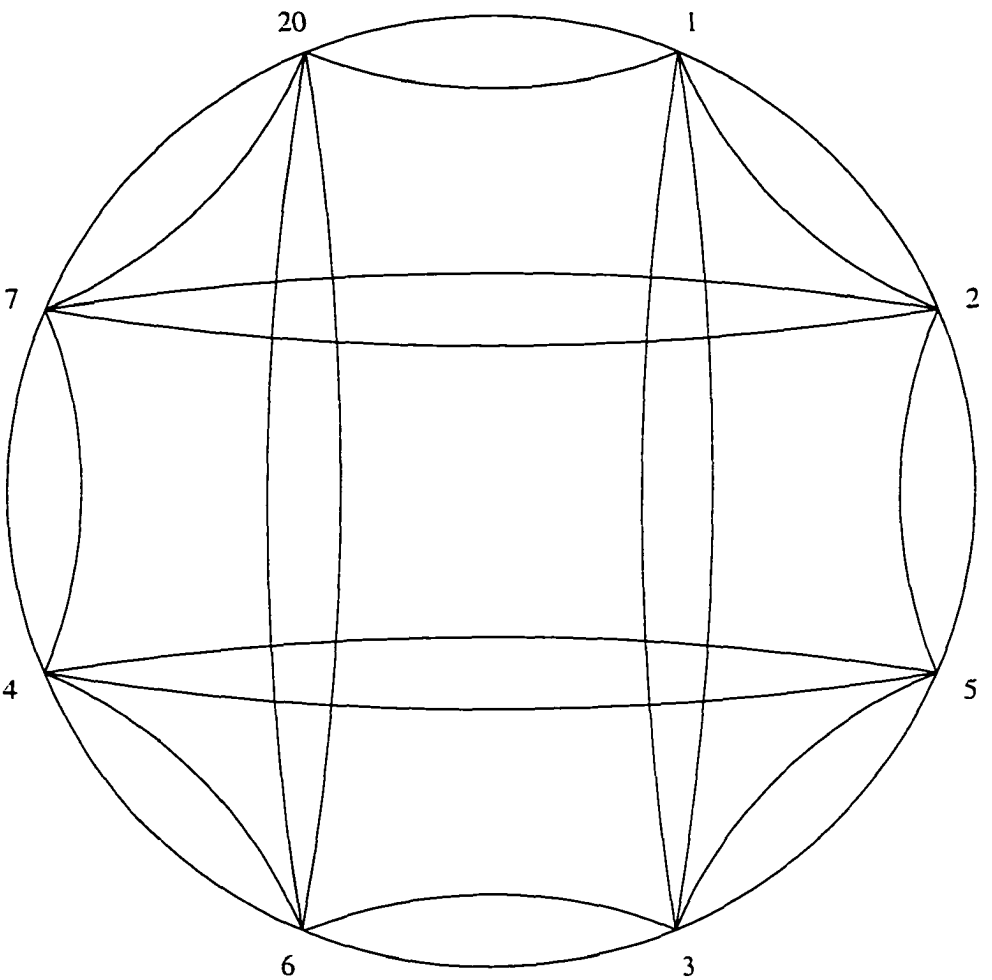


Figure 4.6: The quotient graph $\mathcal{X}_{5,4} = \Gamma_{5,4} \backslash \mathcal{T}_5$ has 8 vertices and 24 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

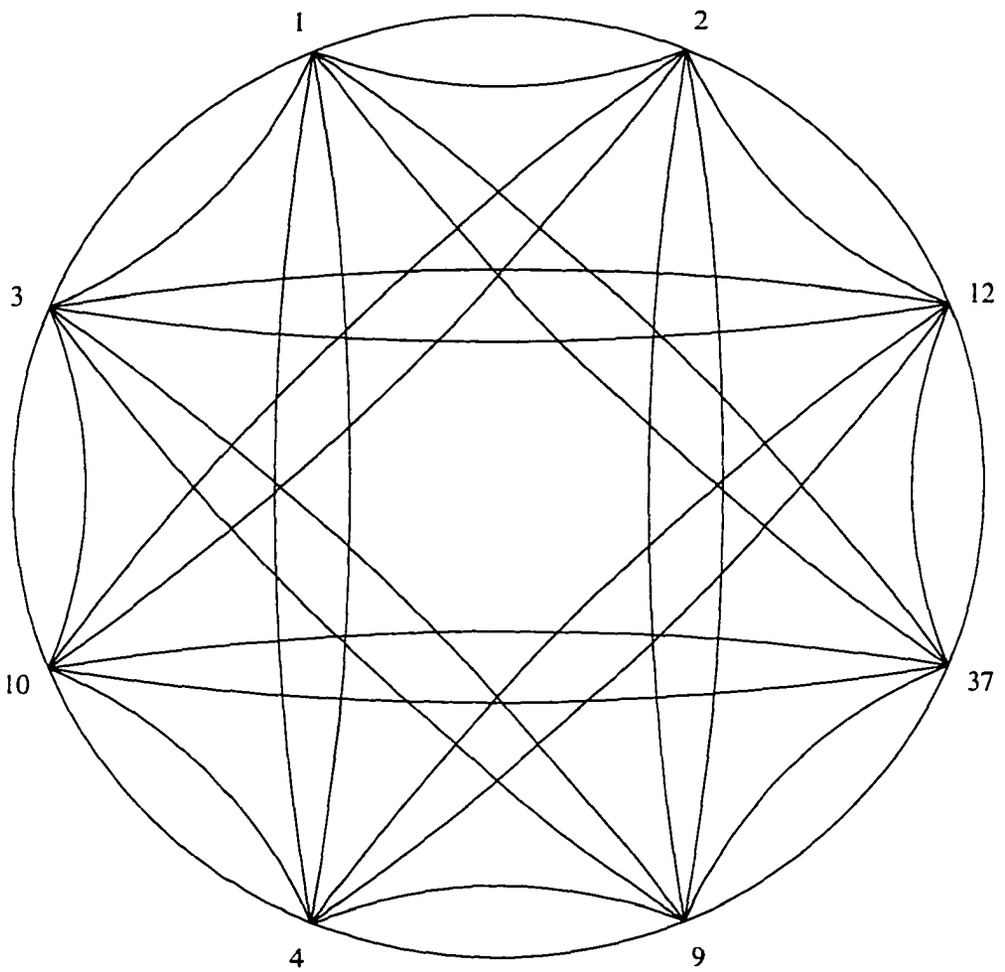


Figure 4.7: The quotient graph $\mathcal{X}_{7,4} = \Gamma_{7,4} \backslash \mathcal{T}_7$ has 8 vertices and 32 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

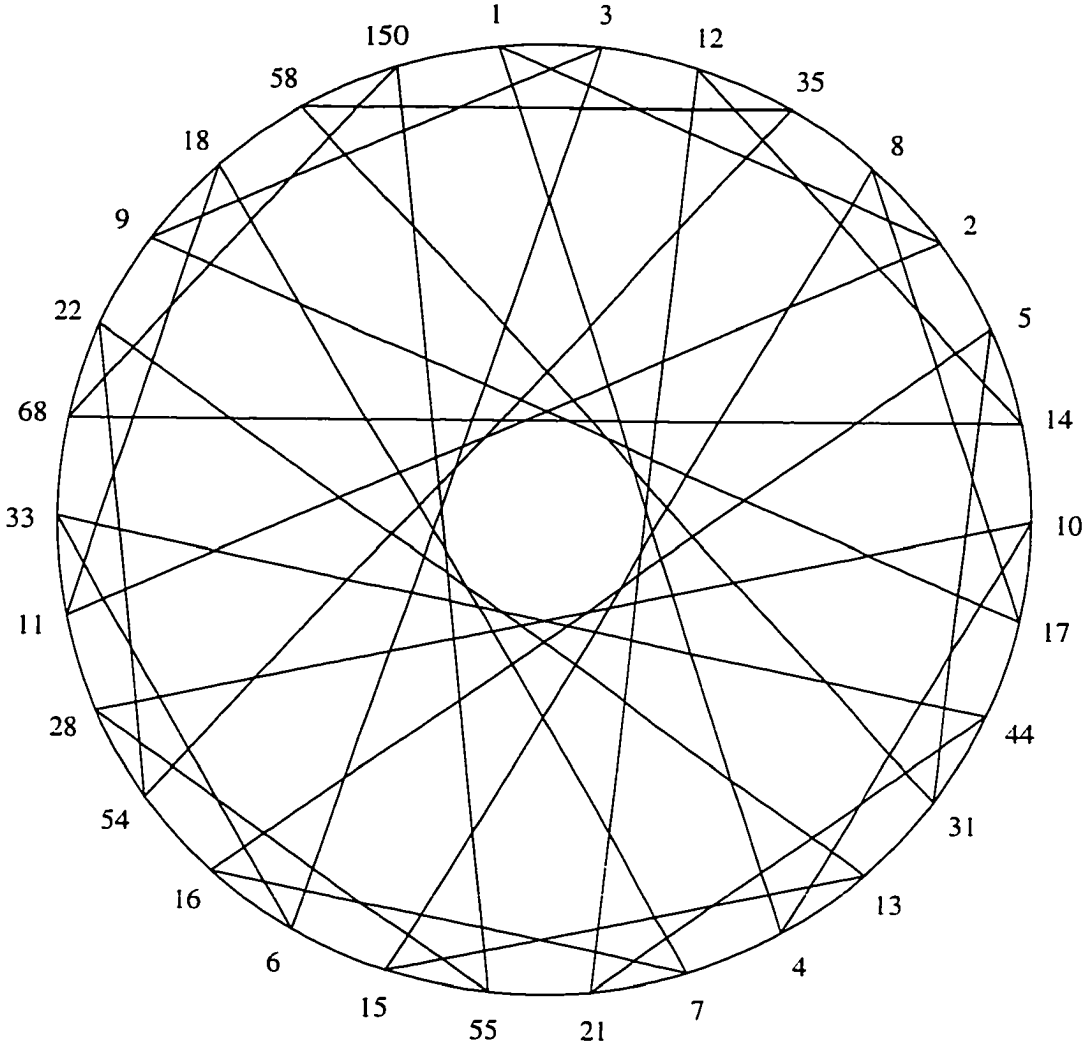


Figure 4.8: The quotient graph $\mathcal{X}_{3,5} = \Gamma_{3,5}\backslash\mathcal{T}_3$ has 30 vertices and 60 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

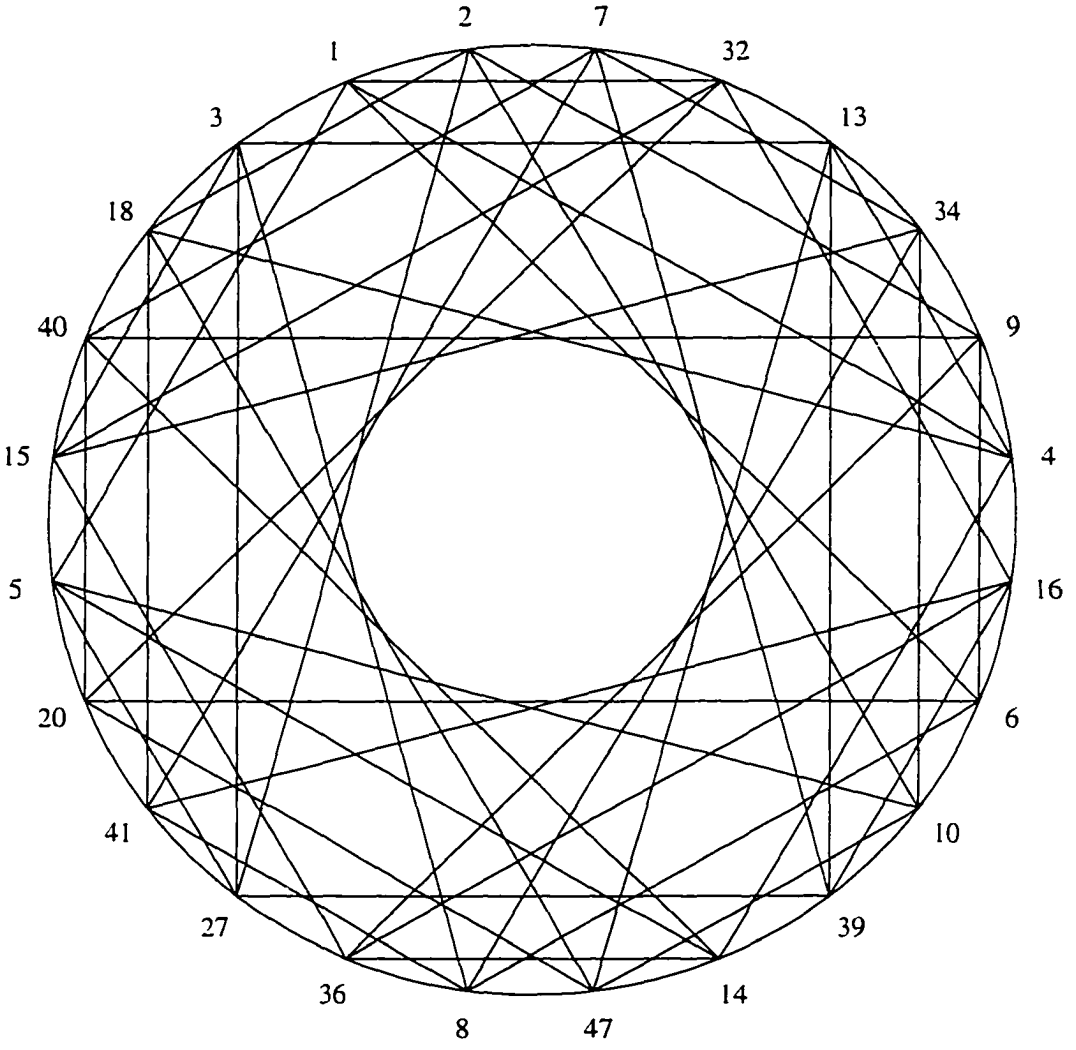


Figure 4.9: The quotient graph $\mathcal{X}_{5,6} = \Gamma_{5,6} \backslash \mathcal{T}_5$ has 24 vertices and 72 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

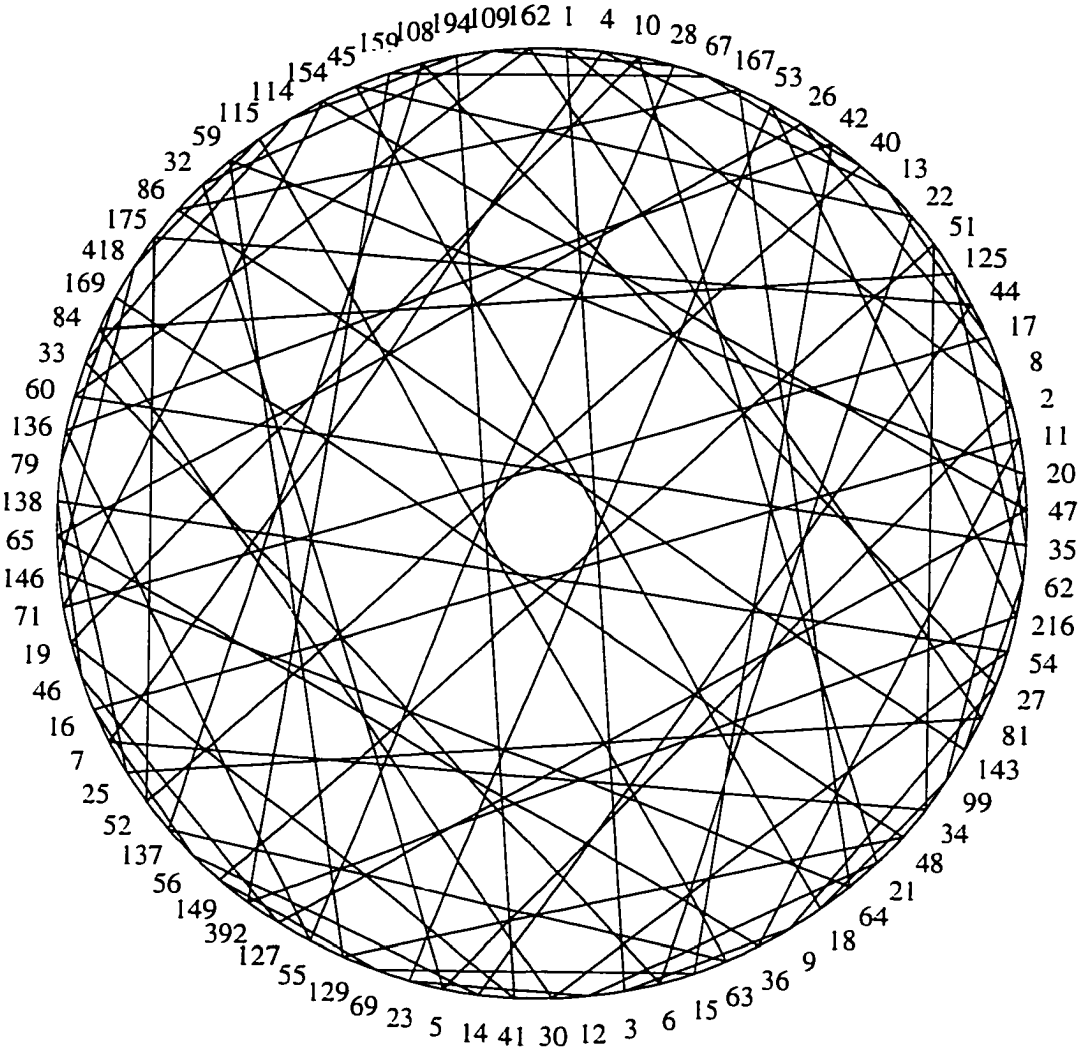


Figure 4.10: The quotient graph $\mathcal{X}_{3,7} = \Gamma_{3,7}\backslash\mathcal{T}_3$ has 84 vertices and 168 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

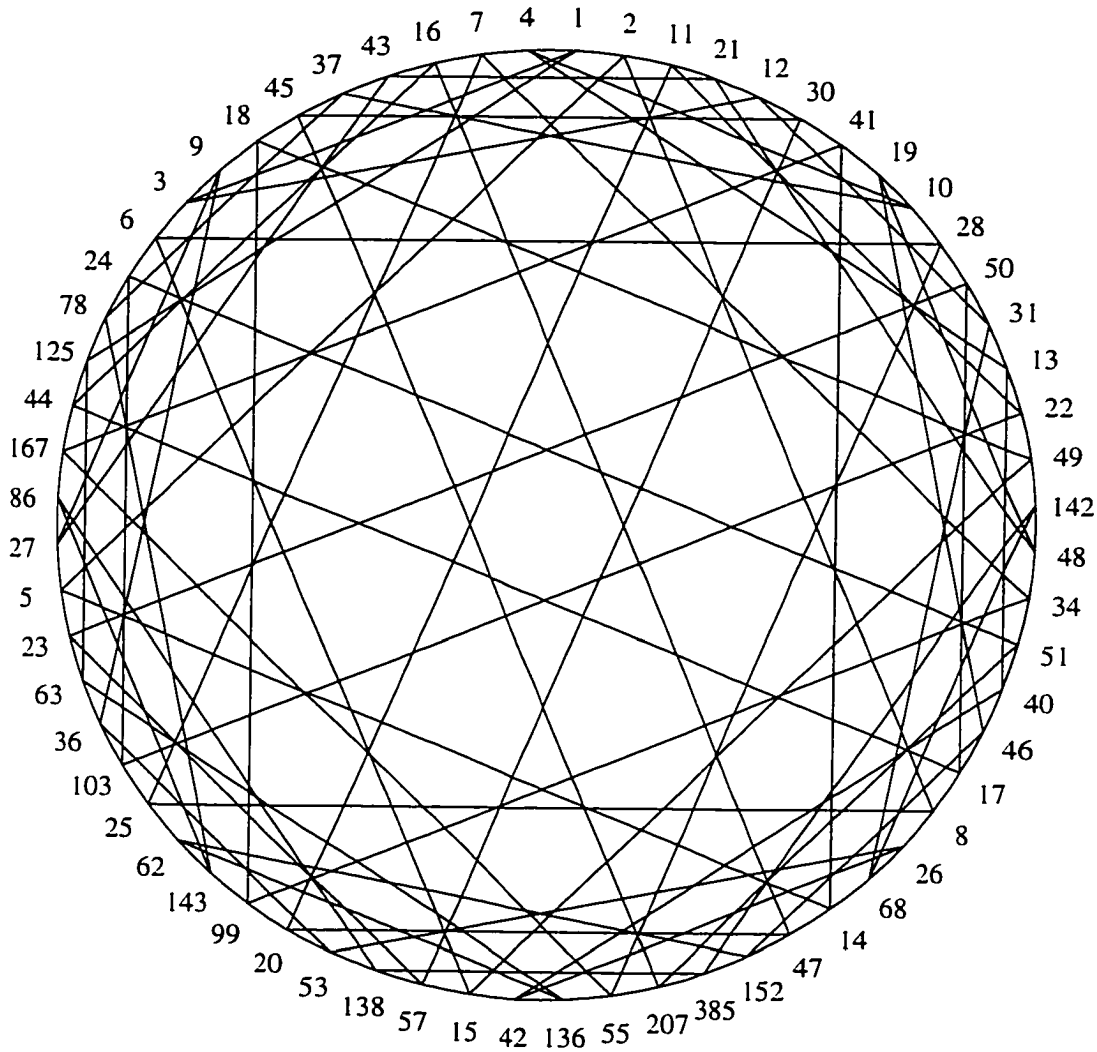


Figure 4.11: The quotient graph $\mathcal{X}_{3,8} = \Gamma_{3,8} \backslash \mathcal{T}_3$ has 64 vertices and 128 edges.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER V

Lemmas

In how many ways can a positive integer n be represented as the sum of s squares? Let $r_s(n)$ be this number. In an 1828 paper [Jac28], Jacobi applied the theory of elliptic functions to obtain the definitive answer for $s = 4$.

Theorem (Jacobi). *Let $\sigma'(n)$ denote the sum of those divisors of n that are not divisible by 4. Then $r_4(n) = 8\,\sigma'(n)$.*

Formulas for $r_s(n)$ in terms of the divisors of n have also been obtained for certain other small values of s. Many of these are derived in [Gro85].

An alternative approach produces an asymptotic formula for $r_s(n)$. This "circle method" was developed by Hardy [Har20], with later contributions by Ramanujan, Littlewood, Rademacher, and others. A more modern proof by Estermann is given in [Est36].

Theorem (Hardy). *For $s \geq 5$,*

$$r_s(n) = \frac{\pi^{s/2}}{\Gamma(s/2)}\, n^{s/2-1}\, S(n) + O\left(n^{s/4}\right)$$

where Γ is the gamma function

$$\Gamma(m) = \int_{t=0}^{\infty} t^{m-1} e^{-t}\, dt,$$

$S(n)$ is the singular series

$$S(n) = \sum_{k=1}^{\infty} A(k,n), \qquad A(k,n) = k^{-s} \sum_{h \leq k}{}' \exp\left[-\frac{2\pi i h n}{k}\right] G(h,k)^s,$$

$G(h,k)$ is the Gaussian sum

$$G(h,k) = \sum_{j=0}^{k-1} \exp\left[\frac{2\pi i h}{k}\, j^2\right],$$

and $\sum'_{h \leq k}$ denotes the sum over integers h with $1 \leq h \leq k$ and $\gcd(h,k) = 1$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In his dissertation, Kloosterman applied the circle method to representations of integers in the form

$$C_1x_1^2 + C_2x_2^2 + \cdots + C_sx_s^2,$$

for positive integer constants C_i, and obtained the formula

$$r_s(n) = \frac{\pi^{s/2}}{\Gamma(s/2)\sqrt{C_1C_2\cdots C_s}}\, n^{s/2-1}S(n) + O\left(n^{s/4+\epsilon}\right) + O\left(n^{s/2-5/4+\epsilon}\right).$$

for all positive integers s and all real $\epsilon > 0$, where

$$S(n) = \sum_{k=1}^{\infty} A(k,n), \qquad A(k,n) = k^{-s} \sum_{h\le k}{}' \exp\left[-\frac{2\pi i h n}{k}\right] \prod_{i=1}^{4} G(C_i h, k),$$

and $G(h,k)$ is the Gaussian sum.

Neither Hardy's nor Kloosterman's formulas are useful if $s \le 4$, because the first error term overcomes the asymptotic term. In a later paper [Klo26], Kloosterman performed more careful analysis and produced an asymptotic formula for $r_4(n)$ with a smaller error term:

$$r_4(n) = \frac{\pi^2}{\sqrt{C_1C_2C_3C_4}}\, n\, S(n) + O\left(n^{17/18+\epsilon}\right).$$

A result by Weil in [Wei48] and adapted by Estermann in [Est61] improves the error term to $O\left(n^{7/8+\epsilon}\right)$.

This and the following two chapters apply Kloosterman's method to representations of positive integers in the form $C_1y_1^2 + C_2y_2^2 + C_3y_3^2 + C_4y_4^2$ under the congruence restrictions $y_i \equiv a_i \pmod{L_i}$ for $i = 1, 2, 3, 4$. In Chapter VI, the following result is proved.

Theorem 6.2 (p. 93). *For each $i = 1, 2, 3, 4$, let C_i, L_i and a_i be fixed integers with C_i and L_i positive. For each non-negative integer n, let $r(n)$ equal the number of integral solutions in the set*

$$\left\{(y_1, y_2, y_3, y_4) \;\middle|\; n = C_1y_1^2 + C_2y_2^2 + C_3y_3^2 + C_4y_4^2 \text{ and } y_i \equiv a_i \pmod{L_i} \text{ for each } i\right\}.$$

Then,

$$r(n) = \frac{\pi^2}{L_1L_2L_3L_4\sqrt{C_1C_2C_3C_4}}\, n\, S(n) + O\left(n^{15/16+\epsilon}\right)$$

for every positive ϵ, where

$$S(n) = \sum_{k=1}^{\infty} A(k,n),$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$A(k,n) = k^{-4} \sum_{h \le k}{}' \exp\left[-\frac{2\pi i h n}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k),$$

$$G_{C,L,a}(h,k) = \sum_{j=0}^{k-1} \exp\left[\frac{2\pi i h}{k} C(Lj+a)^2\right],$$

and $\sum_{h \le k}{}'$ *indicates the sum over integers* h *with* $1 \le h \le k$ *and* $\gcd(h,k) = 1$.

In order to make use of this result, Chapter VII evaluates $S(n)$ in the case of all $C_i = 1$ and $L_i = L$ in order to verify that the asymptotic term grows significantly larger than the error term. The following result provides necessary and nearly sufficient conditions for representing a number as a sum $y_1^2 + y_2^2 + y_3^2 + y_4^2$ under the congruence restrictions $y_i \equiv a_i \pmod{L}$.

Theorem 7.9 (p. 128). *Let* p *and* L *be positive integers with* p *prime and* L *not divisible by* p. *Let* a_1, a_2, a_3 *and* a_4 *be integers with* $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{L}$. *Let* S *be the set of representable integers*

$$S = \left\{ n \mid n = y_1^2 + y_2^2 + y_3^2 + y_4^2 \text{ for some } y_i \in \mathbb{Z} \text{ with } y_i \equiv a_i \pmod{L} \right\},$$

and let C *be the set of positive integral candidates*

$$C = \begin{cases} \{ n \mid n \equiv 1 \pmod{L} \} & \text{if } L \text{ odd,} \\ \{ n \mid n \equiv 1 \pmod{2L} \} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L}, \\ \{ n \mid n \equiv 1 + L \pmod{2L} \} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \not\equiv 1 \pmod{2L}. \end{cases}$$

Also, for each positive integer m, *put*

$$M_m = \left\{ n \mid 2^m \text{ divides } n \right\}.$$

Then $S \subseteq C$. *If* L *is even, then* $C \setminus S$ *is finite. If* L *is odd, then* $(C \setminus M_m) \setminus S$ *is finite for every positive integer* m.

The remainder of this chapter performs computations and estimations in preparation for Chapters VI and VII.

5.1 Definitions and Chapter Goals

Throughout Chapters V, VI and VII, the letters C, L, a and C_i, L_i and a_i (for $i = 1, 2, 3, 4$) denote integer constants, with C, L and all of the C_i's and L_i's positive. Also, write $\mathrm{e}[x]$ as a shorthand notation for

$$\mathrm{e}[x] = \exp[2\pi i\, x].$$

Hence, $\mathrm{e}[x] = 1$ if and only if x is an integer.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Definition 5.1. For integers h, k and ν with $\gcd(h,k) = 1$ and k positive, let $G_{C,L,a}(h,k,\nu)$ denote the sum

$$G_{C,L,a}(h,k,\nu) = \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{hC}{k}(Lj+a)^2 + \frac{\nu}{Lk}(Lj+a)\right].$$

The sum $G_{C,L,a}(h,k,\nu)$ is a generalization of the *Gaussian sum* $G(h,k)$ and will play a major role in the proof of Theorem 6.2. Sections 5.2 and 5.3 of this chapter derive a set of formulas for evaluating $G_{C,L,a}(h,k,\nu)$. Section 5.4 uses these formulas to establish a bound on the sum

$$\sigma = \sum_{h''\le\mu}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k,\nu_i),$$

where $\sum'_{h''\le\mu}$ denotes the sum over all $1 \le h \le k$ such that $\gcd(h,k) = 1$ and $h'' \le \mu$, where h'' is the unique solution to $h(h''+N)+1 \equiv 0 \pmod{k}$ in the domain $1 \le h'' \le k$.

The proofs of these formulas are modified from lemmas appearing in Section 2 of Kloosterman's paper [Klo26].

5.2 Reduction of $G_{C,L,a}(h,k,\nu)$ to a Gaussian Sum

The first step towards evaluating $G_{C,L,a}(h,k,\nu)$ is to rewrite it in terms of a Gaussian sum.

Lemma 5.2. *Given integers h,k,ν with $\gcd(h,k) = 1$ and k positive, put $d = \gcd(CL^2,k)$, and write $CL^2 = C'd$ and $k = k'd$.*

(0) If d does not divide $2hCLa+\nu$, then $G_{C,L,a}(h,k,\nu) = 0$.

Otherwise, d must also divide ν^2, so write $\nu^2 = \nu' d$. Define

$$E_{C,L,a}(h,h',m,k,\nu) = \mathrm{e}\left[\frac{hCa^2}{k}(1-C'm) + \frac{a\nu}{Lk}(1-C'm) + \frac{h'm\nu'}{4k}\right].$$

(1) If k' is odd, then

$$G_{C,L,a}(h,k,\nu) = d\,E_{C,L,a}(h,h',m,k,\nu)\,G(hC',k'),$$

where h' and m are any integers satisfying

$$hh'+1 \equiv 0 \pmod{k} \quad \textit{and} \quad C'm \equiv 1 \pmod{k'} \quad \textit{and} \quad m \equiv 0 \pmod{4}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(2) If k' and w' are even, then

$$G_{C,L,a}(h,k,\nu) = d\, E_{C,L,a}(h,h',m,k,\nu)\, G(hC',k'),$$

where h' and m are any integers satisfying

$$hh'+1 \equiv 0 \pmod{k} \quad \textit{and} \quad C'm \equiv 1 \pmod{k'}.$$

Also, ν' is divisible by 4.

(3) If $k' \equiv 0 \pmod 4$, and w' is odd, then $G_{C,L,a}(h,k,\nu) = 0$.

(4) If $k' \equiv 2 \pmod 4$, and w' is odd, then

$$G_{C,L,a}(h,k,\nu) = \frac{d}{2}\, E_{C,L,a}(h,h',m,k,\nu)\, G(hC',4k'),$$

where h' and m are any integers satisfying

$$hh'+1 \equiv 0 \pmod{4k} \quad \textit{and} \quad C'm \equiv 1 \pmod{4k'}.$$

Hence, h', m and ν' are odd.

Furthermore, if m can be chosen with $C'm \equiv 1 \pmod k$, then the first term within $E_{C,L,a}(h,h',m,k,\nu)$ vanishes. If m can be chosen with $C'm \equiv 1 \pmod{Lk}$, then the first two terms vanish.

Proof. First, use the factorization $k = k'd$ to split the sum over $j = 0,\dots,k-1$ into the product of sums over $j_1 = 0,\dots,k'-1$ and $j_2 = 0,\dots,d-1$, with $j = j_1 + k'j_2$:

$$\begin{aligned}
G_{C,L,a}(h,k,\nu) &= \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{hC}{k}(Lj+a)^2 + \frac{\nu}{Lk}(Lj+a)\right] \\
&= \sum_{j_1=0}^{k'-1}\sum_{j_2=0}^{d-1} \mathrm{e}\left[\frac{hC}{k}(L(j_1+k'j_2)+a)^2 + \frac{\nu}{Lk}(L(j_1+k'j_2)+a)\right] \\
&= \sum_{j_1=0}^{k'-1} \mathrm{e}\left[\frac{hC}{k}(Lj_1+a)^2 + \frac{\nu}{Lk}(Lj_1+a)\right] \\
&\qquad \cdot \sum_{j_2=0}^{d-1} \mathrm{e}\left[\frac{hC}{k}\left(L^2k'^2j_2^2 + 2L^2k'j_1j_2 + 2Lak'j_2\right) + \frac{\nu}{Lk}(Lk'j_2)\right] \\
&= \sum_{j_1=0}^{k'-1} \mathrm{e}\left[\frac{hC}{k}(Lj_1+a)^2 + \frac{\nu}{Lk}(Lj_1+a)\right] \sum_{j_2=0}^{d-1} \mathrm{e}\left[\frac{2hCLa+\nu}{d}j_2\right].
\end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Now, the inner sum over j_2 equals zero unless d divides $2hCLa + \nu$. If d does divide $2hCLa + \nu$, then:

$$G_{C,L,a}(h,k,\nu) = d \sum_{j=0}^{k'-1} \mathrm{e}\left[\frac{hC}{k}(Lj+a)^2 + \frac{\nu}{Lk}(Lj+a)\right].$$

Also, d also divides $L\nu$ and ν^2 because

$$L\nu = L(2hCLa+\nu) - 2ha(CL^2) \qquad \text{and} \qquad \nu^2 = \nu(2hCLa+\nu) - 2hCa(L\nu),$$

so write $2hCLa + \nu = w'd$, $L\nu = L'd$, and $\nu^2 = \nu' d$.

Next, replace j by $j + x$ in equation 5.2:

$$\begin{aligned} G_{C,L,a}(h,k,\nu) &= d \sum_{j=0}^{k'-1} \mathrm{e}\left[\frac{hC}{k}(L(j+x)+a)^2 + \frac{\nu}{Lk}(L(j+x)+a)\right] \\ &= d\,\mathrm{e}\left[\frac{1}{k}\left((hCL^2)x^2 + (2hCLa+\nu)x + hCa^2\right) + \frac{\nu a}{Lk}\right] \\ &\quad \cdot \sum_{j=0}^{k'-1} \mathrm{e}\left[\frac{1}{k}\left((hCL^2)j^2 + (2hCL^2x + 2hCLa + \nu)j\right)\right]. \end{aligned}$$

So

$$\begin{aligned} G_{C,L,a}(h,k,\nu) = d\,\mathrm{e}&\left[\frac{1}{k}\left((hC'x^2 + w'x)d + hCa^2\right) + \frac{\nu a}{Lk}\right] \\ &\cdot \sum_{j=0}^{k'-1} \mathrm{e}\left[\frac{1}{k'}\left(hC'j^2 + (2hC'x + w')j\right)\right]. \end{aligned} \tag{5.1}$$

An ideal choice for x would satisfy $2hC'x + w' \equiv 0 \pmod{k'}$ so that

$$\begin{aligned} G_{C,L,a}(h,k,\nu) &= d\,\mathrm{e}\left[\frac{1}{k}\left((hC'x^2 + w'x)d + hCa^2\right) + \frac{\nu a}{Lk}\right] \sum_{j=0}^{k'-1} \mathrm{e}\left[\frac{hC'}{k'}j^2\right] \\ &= d\,\mathrm{e}\left[\frac{1}{k}\left((hC'x^2 + w'x)d + hCa^2\right) + \frac{\nu a}{Lk}\right] G(hC', k'). \end{aligned} \tag{5.2}$$

Case (1). If k' is odd, then $\gcd(2hC', k') = 1$, so $2hC'x + w' \equiv 0 \pmod{k'}$ has one solution. Let x be that solution, so equation 5.2 holds. Choose m' with $(4C')m' \equiv 1 \pmod{k'}$; then set $m = 4m'$, so that $C'm \equiv 1 \pmod{k'}$ and 4 divides m. Also, choose h' with $hh' + 1 \equiv 0 \pmod{k}$. Then,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$(hC')(h'm)w'^2 \equiv -w'^2 = -w'(2w' - w')$$
$$\equiv (2hC'x)(2w' + 2hC'x) = 4hC'(hC'x^2 + w'x) \pmod{k'},$$

so $h'(m/4)w'^2 \equiv hC'x^2 + w'x \pmod{k'}$. Also,

$$w'^2d^2 = (2hCLa + \nu)^2 = 4h^2Ca^2(CL^2) + 4hCa(L\nu) + \nu^2,$$

so $w'^2d = 4h^2Ca^2C' + 4hCaL' + \nu'$. Hence,

$$(hC'x^2 + w'x)d \equiv h'(m/4)w'^2d = h'(m/4)(4h^2Ca^2C' + 4hCaL' + \nu')$$
$$\equiv -hCa^2C'm - CaL'm + h'\nu'(m/4) \pmod{k}.$$

Also, $CaL'm = CaL^2\nu m/Ld = C'a\nu m/L$. Now, substitute the above into equation 5.2 to obtain

$$G_{C,L,a}(h,k,\nu)$$
$$= d\ \mathrm{e}\left[\frac{1}{k}\left(-hCa^2C'm - CaL'm + \frac{h'\nu'm}{4} + hCa^2 + \frac{\nu a}{L}\right)\right] G(hC',k')$$
$$= d\ \mathrm{e}\left[\frac{hCa^2}{k}(1 - C'm) + \frac{a\nu}{Lk}(1 - C'm) + \frac{h'm\,\nu'}{4k}\right] G(hC',k').$$

Case (2). If k' and w' are even, then let x be the solution to $hC'x+(w'/2) \equiv 0(\mathrm{mod}k')$. Also, choose h' and m with $hh' + 1 \equiv 0 \pmod{k}$ and $C'm \equiv 1 \pmod{k'}$. Then equation 5.2 holds, and

$$(hC')(h'm)\frac{w'^2}{4} \equiv -\frac{w'^2}{4} = -\frac{w'}{2}\left(w' - \frac{w'}{2}\right)$$
$$\equiv hC'x(w' + hC'x) = hC'(hC'x^2 + w'x) \pmod{k'},$$

so $(h'm)(w'^2/4) \equiv hC'x^2 + w'x \pmod{k'}$. Also, $w'^2d = 4h^2Ca^2C' + 4hCaL' + \nu'$ as before, and ν' is divisible by 4, because w' is even. Hence,

$$(hC'x^2 + w'x)d \equiv (h'm)(w'^2/4)d = (h'm)(h^2Ca^2C' + hCaL' + \nu'/4)$$
$$\equiv -hCa^2C'm - CaL'm + h'(\nu'/4)m \pmod{k}.$$

Therefore, as in case (1),

$$G_{C,L,a}(h,k,\nu) = d\ \mathrm{e}\left[\frac{hCa^2}{k}(1 - C'm) + \frac{a\nu}{Lk}(1 - C'm) + \frac{h'm\,\nu'}{4k}\right] G(hC',k').$$

Cases (3) and (4). If k' is even and w' is odd, then $2hC'x + w' \equiv 0 \pmod{k'}$ has no solution. Instead, the equation $hC'x' + w' \equiv 0 \pmod{4k'}$ has a solution for x', and w'

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

odd implies that x' is odd, so let x be a solution to $hC'(2x-1)+w' \equiv 0 \pmod{4k'}$. Substitute $2hC'x + w' \equiv hC' \pmod{4k'}$ into equation 5.1 to obtain

$$G_{C,L,a}(h,k,\nu) = d\,\mathrm{e}\left[\frac{1}{k}\left((hC'x^2+w'x)d+hCa^2\right)+\frac{\nu a}{Lk}\right]\sum_{j=0}^{k'-1}\mathrm{e}\left[\frac{hC'}{k'}(j^2+j)\right]. \tag{5.3}$$

Case (3). Since k' is even, write $k' = 2k_0$. Also, h and L' are odd. Then,

$$\begin{aligned}\sum_{j=0}^{k'-1}\mathrm{e}\left[\frac{hC'}{k'}(j^2+j)\right] &= \sum_{j_1=0}^{k_0-1}\sum_{j_2=0}^{1}\exp\left[\frac{hC'}{2k_0}\left((j_1+j_2k_0)^2+(j_1+j_2k_0)\right)\right]\\ &= \sum_{j_1=0}^{k_0-1}\mathrm{e}\left[\frac{hC'}{k'}(j_1^2+j_1)\right]\sum_{j_2=0}^{1}\mathrm{e}\left[\frac{hC'}{2}(2j_1j_2k_0+j_2^2k_0+j_2)\right]\\ &= \sum_{j_1=0}^{k_0-1}\mathrm{e}\left[\frac{hC'}{k'}(j_1^2+j_1)\right]\left(1+\mathrm{e}\left[\frac{k_0+1}{2}\right]\right).\end{aligned}$$

Now if $k' \equiv 0 \pmod 4$, then k_0 is even, $\mathrm{e}[(k_0+1)/2] = -1$, and $G_{C,L,a}(h,k,\nu) = 0$.

Case (4). The next goal is to rewrite the inner sum of equation 5.3 in terms of $G(hC', 4k')$.

$$\begin{aligned}G(hC',4k') &= \sum_{j=0}^{4k'-1}\mathrm{e}\left[\frac{hC'}{4k'}j^2\right] = \sum_{j_1=0}^{2k'-1}\sum_{j_2=0}^{1}\mathrm{e}\left[\frac{hC'}{4k'}(j_1+2k'j_2)^2\right]\\ &= 2\sum_{j_1=0}^{2k'-1}\mathrm{e}\left[\frac{hC'}{4k'}j_1^2\right] = 2\sum_{j=0}^{k'-1}\mathrm{e}\left[\frac{hC'}{4k'}(2j)^2\right]+2\sum_{j=0}^{k'-1}\mathrm{e}\left[\frac{hC'}{4k'}(2j+1)^2\right].\end{aligned}$$

Evaluate the first term.

$$\begin{aligned}\sum_{j=0}^{k'-1}\mathrm{e}\left[\frac{hC'}{k'}j^2\right] &= \sum_{j_1=0}^{k_0-1}\sum_{j_2=0}^{1}\mathrm{e}\left[\frac{hC'}{2k_0}(j_1+k_0j_2)^2\right]\\ &= \sum_{j_1=0}^{k_0-1}\mathrm{e}\left[\frac{hC'}{2k_0}j_1^2\right]\sum_{j_2=0}^{1}\mathrm{e}\left[\frac{hC'}{2k_0}(2j_1j_2+j_2^2k_0)\right]\\ &= \sum_{j_1=0}^{k_0-1}\mathrm{e}\left[\frac{hC'}{2k_0}j_1^2\right]\left(1+\mathrm{e}\left[\frac{hC'k_0}{2}\right]\right).\end{aligned}$$

This is zero, because C' and h and $k_0 = k'/2$ are all odd. Hence,

$$G(hC',4k') = 2\sum_{j=0}^{k'-1}\mathrm{e}\left[\frac{hC'}{4k'}(2j+1)^2\right] = 2\,\mathrm{e}\left[\frac{hCL^2}{4k}\right]\sum_{j=0}^{k'-1}\mathrm{e}\left[\frac{hC'}{k'}(j^2+j)\right].$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Combine this formula with equation 5.3 to obtain

$$\begin{aligned} G_{C,L,a}(h,k,\nu) &= d\,\mathrm{e}\left[\frac{1}{k}\left((hC'x^2+w'x)d+hCa^2\right)+\frac{\nu a}{Lk}\right] \\ &\quad\cdot\frac{1}{2}\sum_{j=0}^{k'-1}\mathrm{e}\left[-\frac{h}{4k}CL^2\right]G(hC',4k') \\ &= \frac{d}{2}\,\mathrm{e}\left[\frac{1}{4k}\left((4hC'x^2+4w'x-hC')d+4hCa^2\right)+\frac{\nu a}{Lk}\right] \\ &\quad\cdot G(hC',4k'). \end{aligned}$$

Now choose h' and m with $hh'+1\equiv 0 \pmod{4k}$ and $C'm\equiv 1 \pmod{4k'}$. Then $hC'(2x-1)\equiv -w' \pmod{4k'}$ implies

$$\begin{aligned} &(hC')(h'm)w'^2 \equiv -w'^2 = -w'(2w'-w') \equiv hC'(2x-1)(2w'+hC'(2x-1)) \\ &= hC'(4w'x-2w'+hC'(2x-1)^2) \equiv hC'(4w'x+2hC'(2x-1)+hC'(2x-1)^2) \\ &\qquad = hC'(4hC'x^2+4w'x-hC') \pmod{4k'}, \end{aligned}$$

so $h'mw'^2\equiv 4hC'x^2+4w'x-hC' \pmod{4k'}$. Also, $w'^2d = 4h^2Ca^2C'+4hCaL'+\nu'$ as before. Hence

$$\begin{aligned} (4hC'x^2+4w'x-hC')d &\equiv (h'm)w'^2d = (h'm)(4h^2Ca^2C'+4hCaL'+\nu') \\ &\equiv -4hCa^2C'm-4CaL'm+h'\nu'm \pmod{4k}. \end{aligned}$$

Therefore:

$$\begin{aligned} &G_{C,L,a}(h,k,\nu) \\ &\quad= \frac{d}{2}\,\mathrm{e}\left[\frac{1}{4k}\left(-4hCa^2C'm-4CaL'm+h'\nu'm+4hCa^2\right)+\frac{\nu a}{Lk}\right]G(hC',4k') \\ &\quad= \frac{d}{2}\,\mathrm{e}\left[\frac{hCa^2}{k}(1-C'm)+\frac{a\nu}{Lk}(1-C'm)+\frac{h'm\,\nu'}{4k}\right]G(hC',4k'). \end{aligned}$$

This concludes the proof of Lemma 5.2. □

5.3 Evaluation of the sums $G(h,k)$ and $G_{C,L,a}(h,k,\nu)$

The problem of computing $G_{C,L,a}(h,k,\nu)$ has now been reduced to the computation of $G(h,k)$. The following approach for computing Gaussian sums follows from results on page 138 of [Gro85].

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Lemma 5.3. *If* $\gcd(h,k)=1$ *and* $k>0$ *is factored as* $k=2^{\kappa}k''$ *with* k'' *odd, then*

$$G(h,k)=\left(\frac{h}{k''}\right)\varepsilon(k'')\sqrt{k}\cdot\begin{cases}1 & \text{for } \kappa=0,\\ 0 & \text{for } \kappa=1,\\ 1+\exp[hk''/4] & \text{for even } \kappa>0,\\ (2/k'')\sqrt{2}\ \mathrm{e}[hk''/8] & \text{for odd } \kappa>1.\end{cases}$$

where

$$\varepsilon(k'')=\begin{cases}1 & \text{if } k''\equiv 1 \pmod 4,\\ i & \text{if } k''\equiv 3 \pmod 4.\end{cases}$$

Now combine Lemmas 5.2 and 5.3 to obtain a formula for $G_{C,L,a}(h,k,\nu)$.

Theorem 5.4. *Let* h, k *and* ν *be integers with* $\gcd(h,k)=1$ *and* $k>0$. *Write* $d=\gcd(CL^2,k)$, $CL^2=C'd$, $k=k'd$, *and* $k'=2^{\kappa}k''$ *with* k'' *odd. Also, put* $\nu'=\nu^2/d\in\mathbb{Q}$. *Then*

$$G_{C,L,a}(h,k,\nu)=E_{C,L,a}(h,h',m,k,\nu)\left(\frac{hC'}{k''}\right)\varepsilon(k'')\,\alpha_{C'}(h,k')\,\beta_{C,L,a}(h,k,\nu)\sqrt{kd},$$

where

$$E_{C,L,a}(h,h',m,k,\nu)=\mathrm{e}\left[\frac{hCa^2}{k}(1-C'm)+\frac{h'm\,\nu'}{4k}+\frac{1}{k}\,\frac{a\nu}{L}(1-C'm)\right];$$

$$\varepsilon(k'')=\begin{cases}1 & \text{if } k''\equiv 1 \pmod 4,\\ i & \text{if } k''\equiv 3 \pmod 4;\end{cases}$$

$$\alpha_{C'}(h,k')=\begin{cases}1 & \text{if } \kappa=0,\\ 1+\mathrm{e}[hC'k''/4] & \text{for even } \kappa>0,\\ (2/k'')\sqrt{2}\ \mathrm{e}[hC'k''/8] & \text{for odd } \kappa>1;\end{cases}$$

$$\beta_{C,L,a}(h,k,\nu)=\begin{cases}0 & \text{if } 2hCLa+\nu\not\equiv 0 \pmod d,\\ 0 & \text{if } 2hCLa+\nu\equiv 0 \pmod{2d} \text{ and } k'\equiv 2 \pmod 4,\\ 0 & \text{if } 2hCLa+\nu\equiv d \pmod{2d} \text{ and } k'\equiv 0 \pmod 4,\\ 1 & \text{otherwise,}\end{cases}$$

and where h' *and* m *are any solutions to*

$$hh'+1\equiv 0 \pmod k \quad \text{and} \quad C'm\equiv 1 \pmod{k'} \quad \text{and} \quad 4\mid m \quad \text{if } k' \text{ is odd, and}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$hh' + 1 \equiv 0 \pmod{4k} \quad \textit{and} \quad C'm \equiv 1 \pmod{4k'} \qquad \textit{if } k' \textit{ is even.}$$

Note that if $\beta_{C,L,a}(h,k,\nu) \neq 0$, *then* $d \mid \nu^2$, *so* $\nu' \in \mathbb{Z}$. *Hence, either* $G_{C,L,a}(h,k,\nu) = 0$ *for all* h *or* $\nu' \in \mathbb{Z}$.

Proof. If $2hCLa + \nu \not\equiv 0 \pmod{d}$ or if $2hCLa + \nu \equiv d \pmod{2d}$ and $k' \equiv 0 \pmod{4}$, then $G_{C,L,a}(h,k,\nu) = 0$ by Lemma 5.2 and $\beta_{C,L,a}(h,k,\nu) = 0$, so the left and right sides agree. Otherwise, Lemmas 5.2 and 5.3 together imply that

$$G_{C,L,a}(h,k,\nu) = E_{C,L,a}(h,h',m,k,\nu)\left(\frac{hC'}{k''}\right)\varepsilon(k'')\sqrt{kd}\,\gamma$$

where

$$\gamma = \begin{cases} 1 & \text{if } \kappa = 0 \text{ and } 2hCLa + \nu \equiv 0 \pmod{d}, \\ 0 & \text{if } \kappa = 1 \text{ and } 2hCLa + \nu \equiv 0 \pmod{2d}, \\ 1 + \mathrm{e}[hC'k''/4] & \text{if } \kappa > 0 \text{ even and } 2hCLa + \nu \equiv 0 \pmod{2d}, \\ (2/k'')\sqrt{2}\ \mathrm{e}[hC'k''/8] & \text{if } \kappa > 0 \text{ odd and } 2hCLa + \nu \equiv 0 \pmod{2d}, \\ (2/k'')\sqrt{2}\ \mathrm{e}[hC'k''/8] & \text{if } \kappa = 1 \text{ and } 2hCLa + \nu \equiv d \pmod{2d}. \end{cases}$$

It only remains to verify that

$$\alpha_{C'}(h,k')\,\beta_{C,L,a}(h,k,\nu) = \gamma.$$

If $\kappa = 1$ and $2hCLa + \nu \equiv 0 \pmod{2d}$, then $\beta_{C,L,a}(h,k,\nu) = 0$ and $\gamma = 0$. In each of the other four cases, $\beta_{C,L,a}(h,k,\nu) = 1$ and the value of $\alpha_{C'}(h,k')$ equals γ. □

Corollary 5.5. *For integers* h, k *and* ν *with* $\gcd(h,k) = 1$ *and* k *positive,*

$$G_{C,L,a}(h,k,\nu) = O\left(\sqrt{k}\right).$$

Proof. For all C, L, a, h', and k'' with k'' an odd divisor of k,

$$\left|E_{C,L,a}(h,h',m,k,\nu)\right| = 1, \qquad \left|\left(\frac{hC'}{k''}\right)\right| = 1, \qquad \left|\varepsilon(k'')\right| = 1,$$
$$\left|\alpha_{C'}(h,k')\right| \leq \sqrt{2}, \qquad \text{and} \qquad \left|\beta_{C,L,a}(h,k,\nu)\right| \leq 1$$

so Theorem 5.4 implies

$$\left|G_{C,L,a}(h,k,\nu)\right| \leq \sqrt{2} \cdot \sqrt{kd},$$

and $d \leq CL^2$, which is constant. □

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

5.4 Evaluation of the Sum σ

Definition 5.6. Let n, k, μ, ν_1, ν_2, ν_3 and ν_4 be integers with $0 < \mu \leq k \leq N = \lfloor \sqrt{n} \rfloor$. Then let σ denote the sum

$$\sigma = \sum_{h'' \leq \mu}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k,\nu_i),$$

where $\sum'_{h'' \leq \mu}$ denotes the sum over all $1 \leq h \leq k$ such that $\gcd(h,k) = 1$ and $h'' \leq \mu$, where h'' is the unique solution to

$$h(h'' + N) + 1 \equiv 0 \pmod{k}$$

in the domain $1 \leq h'' \leq k$.

The goal of the remainder of this chapter is to establish an upper bound on the sum σ analogous to the fundamental lemma in Kloosterman's paper. Applying Corollary 5.5 to σ produces

$$\sigma = O\left(\sum_{h'' \leq \mu}{}' \prod_{i=1}^{4} \sqrt{k}\right) = O(k^2\mu) = O(k^3),$$

but a slightly better bound shall be required to prove Theorem 6.2.

Lemma 5.7. *Let $\alpha_{C'}$ and $\beta_{C,L,a}$ be defined as in Theorem 5.4. Then for all h, k and ν with $\gcd(h,k) = 1$, $k > 0$, $d_i = \gcd(C_iL_i^2, k)$, $C_iL_i^2 = C_i'd_i$, $k = k_i'd_i$ and $k_i' = 2^{r_i}k_i''$:*

$$\begin{aligned}
\alpha_{C_i'}(h,k_i') &= \alpha_{C_i'}(h+\Lambda,k_i') && \text{if } 8 \mid \Lambda \text{ or } r_i = 0,\\
\beta_{C_i,L_i,a_i}(h,k,\nu_i) &= \beta_{C_i,L_i,a_i}(h+\Lambda,k,\nu_i) && \text{if } d_i \mid \Lambda,\\
\prod_{i=1}^{4}\left(\frac{h}{k_i''}\right) &= \prod_{i=1}^{4}\left(\frac{h+\Lambda}{k_i''}\right) && \text{if } d_i \mid \Lambda \text{ for all } i.
\end{aligned}$$

Proof. The first two equalities follow from the definitions of α and β. For the third, write $k = 2^c k''$ and $d_i = 2^{c_i}d_i''$ to match $k_i' = 2^{r_i}k_i''$. Then $k'' = k_i''d_i''$, so

$$\prod_{i=1}^{4}\left(\frac{h}{k_i''}\right)\left(\frac{h}{d_i''}\right) = \prod_{i=1}^{4}\left(\frac{h}{k''}\right) = \left(\frac{h}{k''}\right)^4 = 1, \qquad \text{and so} \qquad \prod_{i=1}^{4}\left(\frac{h}{k_i''}\right) = \prod_{i=1}^{4}\left(\frac{h}{d_i''}\right).$$

Then $d_i \mid \Lambda$ for all i implies

$$\prod_{i=1}^{4}\left(\frac{h}{k_i''}\right) = \prod_{i=1}^{4}\left(\frac{h}{d_i''}\right) = \prod_{i=1}^{4}\left(\frac{h+\Lambda}{d_i''}\right) = \prod_{i=1}^{4}\left(\frac{h+\Lambda}{k_i''}\right).$$

□

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Lemma 5.8. *Let n, N, k and μ be integers with $0 < \mu \leq k$. If k is even, then*

$$\sum_{h'' \leq \mu}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k,\nu_i) = \sum_{H'' \leq \mu}{}' \mathrm{e}\left[-\frac{Hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(H,k,\nu_i)$$

where $\sum'_{h'' \leq \mu}$ and $\sum'_{H'' \leq \mu}$ denote the sums over all $1 \leq h \leq k$ and $1 \leq H \leq 4k$ such that $\gcd(h,k) = \gcd(H,4k) = 1$ and $h'', H'' \leq \mu$, where h'' and H'' are the unique solutions to

$$h(h''+N)+1 \equiv 0 \pmod{k} \quad \textit{and} \quad H(H''+N)+1 \equiv 0 \pmod{4k} \tag{5.4}$$

in the domains $1 \leq h'' \leq k$ and $1 \leq H'' \leq 4k$.

Proof. The equations 5.4 establish two bijections $h \longleftrightarrow h''$ and $H \longleftrightarrow H''$ between h and h'', and H and H'' satisfying $1 \leq h, h'' \leq k$, $1 \leq H, H'' \leq 4k$, and

$$\gcd(h,k) = \gcd(h''+N,k) = \gcd(H,4k) = \gcd(H''+N,4k) = 1.$$

Since k is even,

$$\gcd(H,4k) = 1 \iff \gcd(H,k) = 1$$

and

$$\gcd(H''+N,4k) = 1 \iff \gcd(H''+N,k) = 1.$$

So $\sum'_{h'' \leq \mu}$ and $\sum'_{H'' \leq \mu}$ sum over the same set of h'' and H''. When $h'' = H''$ and $\gcd(h''+N,k) = 1$,

$$h(h''+N)+1 \equiv H(H''+N)+1 \pmod{k} \quad \Longrightarrow \quad h \equiv H \pmod{k}.$$

So,

$$\mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k,\nu_i) = \mathrm{e}\left[-\frac{Hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(H,k,\nu_i).$$

□

The heart of the computation of σ is accomplished using a pair of lemmas from Kloosterman's paper [Klo26].

Lemma 5.9 (Kloosterman). *If $u, v, \Lambda, \lambda, k, N \in \mathbb{Z}$ with $0 < \Lambda \leq k$ and $\Lambda \mid k$ then*

$$\sum_{h \equiv \lambda \bmod \Lambda}{}' \mathrm{e}\left[\frac{uh+vh'}{k}\right] = O\left(k^{3/4+\epsilon} \gcd(u,k)^{1/4}\right)$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

where $1 + hh' \equiv 0 \pmod{k}$. *Consequently, if* $0 < \mu \leq k$ *then*

$$\sum_{\substack{h'' \leq \mu \\ h \equiv \lambda \bmod \Lambda}}{}' \mathrm{e}\left[\frac{uh + vh'}{k}\right] = O\left(k^{7/8+\epsilon} \gcd(u, k)^{1/4}\right)$$

where $1 + hh' \equiv 0 \pmod{k}$, *and* $h' \equiv h'' + N \pmod{k}$.

Proof. See Lemmas 4 and 5 of [Klo26]. □

In [Wei48], Weil invoked the Riemann hypothesis in function-fields to prove a tighter bound on the Kloosterman sum:

$$\sum_{h \leq k}{}' \mathrm{e}\left[\frac{uh + vh'}{k}\right] \leq 2\sqrt{k}$$

for k prime and u and v not divisible by k. Estermann, in [Est61], applied this sum to improve the error bound in Kloosterman's method.

Now we are ready to analyze the sum σ.

Theorem 5.10. *Given integers* n, k *and* μ *with* $0 < \mu \leq k \leq N = \lfloor \sqrt{n} \rfloor$, *and integers* ν_1, ν_2, ν_3, *and* ν_4, *then for any positive real* ϵ:

$$\sum_{h'' \leq \mu}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i, L_i, a_i}(h, k, \nu_i) = O\left(k^{23/8+\epsilon} \gcd(u, k)^{1/4}\right),$$

where $u = O(n)$, *and* $\sum'_{h'' \leq \mu}$ *denotes the sum over all* $1 \leq h \leq k$ *with* $\gcd(h, k) = 1$ *and* $h'' \leq \mu$, *where* h'' *is the unique solution to* $h(h'' + N) + 1 \equiv 0 \pmod{k}$ *in the domain* $1 \leq h'' \leq k$.

Proof. First, recall some notation from Theorem 5.4. For $i = 1, 2, 3, 4$, write $d_i = \gcd(C_i L_i^2, k)$, $C_i L_i^2 = C_i' d_i$, $k = k_i' d_i$, and $k_i' = 2^{r_i} k_i''$ with k_i'' odd. Also, put $\nu_i' = \nu^2 / d_i$. If $d_i \nmid \nu^2$ for any i, then $G_{C_i, L_i, a_i}(h, k, \nu_i) = 0$ for all h, so $\sigma = 0$. Hence, assume that all ν_i' are integers.

Let $E_{C,L,a}(h, h', m, k, \nu)$, $\varepsilon(k'')$, $\alpha_{C'}(h, k')$ and $\beta_{C,L,a}(h, k, \nu)$ be defined as in Theorem 5.4. For each i, choose $0 < m_i < 4k_i'$ such that

$$\begin{aligned} C_i' m_i &\equiv 1 \pmod{k_i'} \quad \text{and } 4 \mid m_i \quad \text{if } k_i' \text{ is odd, and} \\ C_i' m_i &\equiv 1 \pmod{4k_i'} \qquad\qquad\quad \text{if } k_i' \text{ is even.} \end{aligned}$$

Now, there are two cases to consider:

(1) If all of the k_i' are odd, then set $\Lambda = \mathrm{lcm}(d_1, d_2, d_3, d_4)$, so that $\Lambda \mid k$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(2) If instead at least one of the k_i' is even, then put $G = \operatorname{lcm}(d_1, d_2, d_3, d_4)$ and

$$\Lambda = \begin{cases} G & \text{if } 8 \mid G, \\ 2G & \text{if } G \equiv 4 \pmod 8, \\ 4G & \text{if } G \equiv 2 \pmod 4, \\ 8G & \text{if } G \text{ is odd.} \end{cases}$$

Then $\Lambda \mid 4k$ because k_i' even implies that k is even.

In both cases, each d_i divides Λ, and either $r_i = 0$ for all i, or $8 \mid \Lambda$. Hence, Λ satisfies the conditions for the three equalities of Lemma 5.7. Furthermore, Λ is bounded above by a constant independent of k and n, namely $8 \operatorname{lcm}(C_1 L_1^2, C_2 L_2^2, C_3 L_3^2, C_4 L_4^2)$.

In case (1), $\Lambda \mid k$, so the domain of the sum σ can be separated into equivalence classes modulo Λ. In case (2), first invoke Lemma 5.8 (as k is even) to rewrite σ as a sum over $1 \le h, h'' \le 4k$ with $\gcd(h, 4k) = 1$ and $h(h'' + N) + 1 \equiv 0 \pmod{4k}$. Then $\Lambda \mid 4k$, so the domain of σ can be separated into equivalence classes modulo Λ.

In either case,

$$\sigma = \sum_{\lambda=1}^{\Lambda} \sum_{\substack{h'' \le \mu \\ h \equiv \lambda \bmod \Lambda}}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i, L_i, a_i}(h, k, \nu_i).$$

where h can range up to k in case (1) and up to $4k$ in case (2). Substitute the formulas from Theorem 5.4 for $G_{C_i, L_i, a_i}(h, k, \nu_i)$:

$$\sigma = \sum_{\lambda=1}^{\Lambda} \sum_{\substack{h'' \le \mu \\ h \equiv \lambda \bmod \Lambda}}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \cdot \prod_{i=1}^{4} E_{C_i, L_i, a_i}(h, h', m_i, k, \nu_i) \left(\frac{C_i' h}{k_i''}\right) \varepsilon(k_i'') \, \alpha_{C_i'}(h, k_i') \, \beta_{C_i, L_i, a_i}(h, k, \nu_i) \sqrt{k d_i}.$$

Use Lemma 5.7 to extract terms from the inside of the summation over h:

$$\sigma = \left[\prod_{i=1}^{4} \left(\frac{C_i'}{k_i''}\right) \varepsilon(k_i'')\right] k^2 \sqrt{d_1 d_2 d_3 d_4} \sum_{\lambda=1}^{\Lambda} \left[\prod_{i=1}^{4} \left(\frac{\lambda}{k_i''}\right) \alpha_{C_i'}(h, k_i') \, \beta_{C_i, L_i, a_i}(h, k, \nu_i)\right] \cdot \sum_{\substack{h'' \le \mu \\ h \equiv \lambda \bmod \Lambda}}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} E_{C_i, L_i, a_i}(h, h', m_i, k, \nu_i).$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Rewrite the innermost sum over h:

$$\sigma = \left[\prod_{i=1}^{4}\left(\frac{C_i'}{k_i''}\right)\varepsilon(k_i'')\right] k^2\sqrt{d_1d_2d_3d_4}\sum_{\lambda=1}^{\Lambda}\left[\prod_{i=1}^{4}\left(\frac{\lambda}{k_i''}\right)\alpha_{C_i'}(\lambda,k_i')\,\beta_{C_i,L_i,a_i}(\lambda,k,\nu_i)\right]$$
$$\cdot\,\mathrm{e}\left[\frac{w}{k}\right]\sum_{\substack{h''\le\mu\\ h\equiv\lambda \bmod\Lambda}}{}'\ \mathrm{e}\left[\frac{uh}{k}+\frac{vh'}{4k}\right],$$

where $u, v \in \mathbb{Z}$ and $w \in \mathbb{Q}$ are

$$u = -n + C_1a_1^2(1-C_1'm_1) + C_2a_2^2(1-C_2'm_2)$$
$$+ C_3a_3^2(1-C_3'm_3) + C_4a_4^2(1-C_4'm_4),$$
$$v = m_1\nu_1' + m_2\nu_2' + m_3\nu_3' + m_4\nu_4',$$
$$w = \frac{a_1\nu_1}{L_1}(1-C_1'm_1) + \frac{a_2\nu_2}{L_2}(1-C_2'm_2) + \frac{a_3\nu_3}{L_3}(1-C_3'm_3) + \frac{a_4\nu_4}{L_4}(1-C_4'm_4).$$

Then $\sqrt{d_1d_2d_3d_4} \le L_1L_2L_3L_4\sqrt{C_1C_2C_3C_4}$ implies that

$$|\sigma| \le K\,k^2\sum_{\lambda=1}^{\Lambda}\left|\sum_{\substack{h''\le\mu\\ h\equiv\lambda \bmod\Lambda}}{}'\ \mathrm{e}\left[\frac{uh}{k}+\frac{vh'}{4k}\right]\right|. \tag{5.5}$$

where K is some positive constant independent of k and n.

In case (1), all of the k_i' are odd, so then all of the m_i are divisible by 4. Hence, $v = m_1\nu_1' + m_2\nu_2' + m_3\nu_3' + m_4\nu_4'$ is divisible by 4. Apply Kloosterman's Lemma to equation 5.5 to obtain a bound for σ:

$$|\sigma| \le K\,k^2\sum_{\lambda=1}^{\Lambda}\left|\sum_{\substack{h''\le\mu\\ h\equiv\lambda \bmod\Lambda}}{}'\ \mathrm{e}\left[\frac{uh+(v/4)h'}{k}\right]\right|$$
$$\le K\,k^2\sum_{\lambda=1}^{\Lambda}k^{7/8+\epsilon}\gcd(u,k)^{1/4} = K\Lambda\,k^{2+7/8+\epsilon}\gcd(u,k)^{1/4}.$$

Since Λ is bounded above by a constant,

$$\sigma = O\left(k^{23/8+\epsilon}\gcd(u,k)^{1/4}\right).$$

In case (2), the sum $\sum'_{\substack{h''\le\mu\\ h\equiv\lambda \bmod\Lambda}}$ in equation 5.5 is taken over $1 \le h \le 4k$ instead, so apply Kloosterman's Lemma to 5.5 using $4k$ instead of k:

$$|\sigma| \le K\,k^2\sum_{\lambda=1}^{\Lambda}\left|\sum_{\substack{h''\le\mu\\ h\equiv\lambda \bmod\Lambda}}{}'\ \mathrm{e}\left[\frac{(4u)h+vh'}{4k}\right]\right|$$
$$\le K\,k^2\sum_{\lambda=1}^{\Lambda}k^{7/8+\epsilon}\gcd(4u,k)^{1/4} = K\Lambda k^{2+7/8+\epsilon}\gcd(4u,k)^{1/4}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Since $\gcd(4u, k) \leq 4\gcd(u, k)$,

$$\sigma = O\left(k^{23/8+\epsilon}\gcd(u, k)^{1/4}\right).$$

Finally, note that $0 < m_i < 4k_i' \leq 4k < 4n$ for all i, so

$$u = -n + C_1a_1^2(1 - C_1'm_1) + C_2a_2^2(1 - C_2'm_2) + C_3a_3^2(1 - C_3'm_3) + C_4a_4^2(1 - C_4'm_4)$$

is a function of k and n, and $u = O(n)$.

This completes the proof of Theorem 5.10. □

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER VI

Extending Kloosterman's Proof

Definition 6.1. For $i = 1, 2, 3, 4$, let C_i, L_i and a_i be fixed integers with C_i and L_i positive. For each non-negative integer n, let $r(n)$ equal the number of integer solutions in the set

$$\left\{ (y_1, y_2, y_3, y_4) \;\middle|\; n = C_1 y_1^2 + C_2 y_2^2 + C_3 y_3^2 + C_4 y_4^2 \text{ and } y_i \equiv a_i \pmod{L_i} \text{ for each } i \right\}.$$

This is equivalent to counting the number of integer solutions in the set

$$\left\{ (x_1, x_2, x_3, x_4) \;\middle|\; n = \sum_{i=1}^{4} C_i (L_i x_i + a_i)^2 \right\}.$$

The goal of this chapter is to prove the following asymptotic formula for $r(n)$:

Theorem 6.2.

$$r(n) = \frac{\pi^2}{L_1 L_2 L_3 L_4 \sqrt{C_1 C_2 C_3 C_4}}\, n\, S(n) + O\left(n^{15/16+\epsilon}\right)$$

for every positive real ϵ, *where*

$$S(n) = \sum_{k=1}^{\infty} A(k, n),$$

$$A(k, n) = k^{-4} \sum_{h \le k}{}' \exp\left[-\frac{2\pi i h n}{k}\right] \prod_{i=1}^{4} G_{C_i, L_i, a_i}(h, k),$$

$$G_{C,L,a}(h, k) = \sum_{j=0}^{k-1} \exp\left[\frac{2\pi i h}{k} C(Lj + a)^2\right],$$

and $\sum'_{h \le k}$ *indicates the sum over integers* h *with* $1 \le h \le k$ *and* $\gcd(h, k) = 1$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

The proof uses Corollary 5.5 and Theorem 5.10 from the previous chapter, and it follows Kloosterman's proof closely. First, Cauchy's theorem is applied to a representation of the generating function of $r(n)$ in order to express $r(n)$ by a path integral over a small circle around the origin in $\mathbb{C}^2$. Next, the integral is rewritten as a sum of integers. The remainder of the proof consists of the evaluation and estimation of these integrals. One integral eventually yields the asymptotic term in the formula 6.1, and all the other integrals are subsumed into the error term.

As in Chapter V, C, L, a, C_i, L_i and a_i denote integer constants, with C, L, C_i and L_i positive. Also, $\mathrm{e}[x] = \exp[2\pi i\, x]$.

6.1 Step 1: Express $r(n)$ as a Complex Path Integral

In the language of generating functions,

$$\sum_{n=0}^{\infty} r(n)x^n = \prod_{i=1}^{4} \theta_{C_i,L_i,a_i}(x) \qquad \text{where} \qquad \theta_{C,L,a}(x) = \sum_{m=-\infty}^{\infty} x^{C(Lm+a)^2}.$$

Now, recall some useful facts from complex analysis. If $f(z)$ is analytic in the region $R \setminus \{\alpha\}$, then the Laurent series for $f(z)$

$$\sum_{n=-\infty}^{\infty} c_n(z-\alpha)^n = \cdots + c_{-1}(z-\alpha)^{-1} + c_0 + c_1(z-\alpha)^1 + c_2(z-\alpha)^2 + \cdots$$

converges uniformly to $f(z)$ within any closed annulus contained in R and centered at α. If Γ is a counterclockwise circle around α within R, then

$$c_n = \frac{1}{2\pi i} \int_{\Gamma} \frac{f(z)}{(z-\alpha)^{n+1}}\, dz.$$

In particular,

$$\int_{\Gamma} f(z)\, dz = 2\pi i\, c_{-1},$$

and c_{-1} is called the *residue* of $f(z)$ at α.

Applying these facts to the generating function for $r(n)$, produces

$$r(n) = \frac{1}{2\pi i} \int_{\Gamma} \theta_{C_1,L_1,a_1}(w)\, \theta_{C_2,L_2,a_2}(w)\, \theta_{C_3,L_3,a_3}(w)\, \theta_{C_4,L_4,a_4}(w)\, \frac{dw}{w^{n+1}}. \qquad (6.1)$$

where Γ is a sufficiently small circle about the origin.

It can be shown that the Taylor series for $\theta_{C,L,a}(x)$ and hence for $\prod_{i=1}^{4} \theta_{C_i,L_i,a_i}(x)$ converges when $|x| < 1$, and that the unit circle is a natural boundary for $\theta_{C,L,a}(x)$. Choose Γ to be a circle of radius $e^{-1/n}$. As $n \to \infty$, the radius of Γ approaches 1 from below.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

6.2 Step 2: Break the Circle Γ Up into Farey-Arcs

As $|x| \to 1$ from below, it can be shown that $|\theta_{C,L,a}(x)|$ grows large particularly quickly when x approaches a root of unity $\exp[2\pi i\,(h/k)]$ with a small denominator k. Consequently, the evaluation of the integral in equation 6.1 should focus on intervals around these roots of unity.

Let $N = \lfloor\sqrt{n}\rfloor$. The *Farey series* of order N is the set of fractions h/k with $0 \le h \le k \le N$ and $\gcd(h,k) = 1$, ordered by size. For example, the Farey series of order 7 is

$$\frac{0}{1} < \frac{1}{7} < \frac{1}{6} < \frac{1}{5} < \frac{1}{4} < \frac{2}{7} < \frac{1}{3} < \frac{2}{5} < \frac{3}{7} < \frac{1}{2} < \frac{4}{7} < \frac{3}{5} < \frac{2}{3} < \frac{3}{4} < \frac{4}{5} < \frac{5}{6} < \frac{6}{7} < \frac{1}{1}.$$

If $h_1/k_1 < h/k < h_2/k_2$ are three consecutive terms in a Farey series, then:

(1) $k_1 h - k h_1 = k h_2 - k_2 h = 1$,

(2) $N < k_1 + k < 2N$ and $N < k + k_2 < 2N$,

(3) $\dfrac{h_1}{k_1} < \dfrac{h_1+h}{k_1+k} < \dfrac{h}{k} < \dfrac{h+h_2}{k+k_2} < \dfrac{h_2}{k_2}$, and

(4) $\dfrac{h_1+h}{k_1+k} = \dfrac{h}{k} - \dfrac{1}{k(k_1+k)}$ and $\dfrac{h+h_2}{k+k_2} = \dfrac{h}{k} + \dfrac{1}{k(k+k_2)}$.

The fractions $\dfrac{h_1+h}{k_1+k}$ and $\dfrac{h+h_2}{k+k_2}$ are the *mediants* between h_1/k_1 and h/k, and h/k and h_2/k_2, respectively.

We use the mediants to break the circle Γ up into *Farey-arcs* $\phi_{h,k}$, where the Farey-arc $\phi_{h,k}$ is described by

$$w = \exp\left[-\frac{1}{n} + \frac{2\pi i h}{k} + i\theta\right] \qquad \text{where} \qquad \frac{-2\pi}{k(k_1+k)} \le \theta \le \frac{2\pi}{k(k+k_2)}.$$

Here, $\phi_{1,1}$ denotes the union of the two extreme intervals, so $\phi_{1,1}$ corresponds to

$$w = \exp\left[-\frac{1}{n} + i\theta\right] \qquad \text{where} \qquad \frac{-2\pi}{1(N+1)} \le \theta \le \frac{2\pi}{1(1+N)}.$$

Let $\sum'_{h\le k}$ denote a summation over integers h with $1 \le h \le k$ and $\gcd(h,k) = 1$. Then

$$r(n) = \frac{1}{2\pi i}\sum_{k=1}^{N}\sum'_{h\le k}\int_{\phi_{h,k}} \theta_{C_1,L_1,a_1}(w)\,\theta_{C_2,L_2,a_2}(w)\,\theta_{C_3,L_3,a_3}(w)\,\theta_{C_4,L_4,a_4}(w)\,\frac{dw}{w^{n+1}}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

6.3 Step 3: Rewrite $\theta_{C,L,a}(w)$ for the Farey-arc $\phi_{h,k}$

On the arc $\phi_{h,k}$,

$$\theta_{C,L,a}(w) = \sum_{m=-\infty}^{\infty} w^{C(Lm+a)^2} = \sum_{m=-\infty}^{\infty} \exp\left[\left(-\frac{1}{n} + \frac{2\pi i h}{k} + i\theta\right) C(Lm+a)^2\right].$$

Some of the terms inside the exponent depend only on the congruence class of m modulo k. Rewrite m as $m = \nu k + j$, where $\nu, j \in \mathbb{Z}$ and $0 \le j < k$. Then $Lm + a = L\nu k + (Lj + a)$ and

$$\begin{aligned}\theta_{C,L,a}(w) &= \sum_{j=0}^{k-1} \sum_{\nu=-\infty}^{\infty} \exp\left[\left(\frac{2\pi i h}{k} - \frac{1}{n} + i\theta\right) C(L\nu k + (Lj+a))^2\right] \\ &= \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{h}{k} C(Lj+a)^2\right] \sum_{\nu=-\infty}^{\infty} \exp\left[-\left(\frac{1}{n} - i\theta\right) C(Lk)^2 \left(\nu + \frac{Lj+a}{Lk}\right)^2\right].\end{aligned}$$

Theorem 8.1 in [Gro85] implies that for any α and t with $\mathrm{Re}\ t > 0$,

$$\sum_{\nu=-\infty}^{\infty} \exp\left[-\pi t(\nu+\alpha)^2\right] = t^{-1/2} \sum_{\nu=-\infty}^{\infty} \exp\left[2\pi i \nu\alpha - \frac{\pi\nu^2}{t}\right].$$

Applying this formula to $\theta_{C,L,a}(w)$ using

$$t = \frac{C(Lk)^2}{\pi}\left(\frac{1}{n} - i\theta\right) \quad \text{and} \quad \alpha = \frac{Lj+a}{Lk}$$

produces

$$\begin{aligned}\theta_{C,L,a}(w) &= \sqrt{\frac{\pi}{L^2 C}} \frac{1}{k} \left(\frac{1}{n} - i\theta\right)^{-1/2} \\ &\quad \cdot \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{h}{k} C(Lj+a)^2\right] \sum_{\nu=-\infty}^{\infty} \exp\left[\frac{2\pi i \nu}{Lk}(Lj+a) - \frac{\pi^2\nu^2}{C(Lk)^2}\left(\frac{1}{n} - i\theta\right)^{-1}\right].\end{aligned}$$

Separate the inner sum into three cases: $\nu = 0$, $\nu > 0$ and $\nu < 0$. For $\nu < 0$, replace j by $-j \bmod k$ and ν by $-\nu$. Then we obtain

$$\begin{aligned}\theta_{C,L,a}(w) = \sqrt{\frac{\pi}{L^2 C}} \frac{1}{k} \left(\frac{1}{n} - i\theta\right)^{-1/2} &\left[\sum_{j=0}^{k-1} \mathrm{e}\left[\frac{h}{k} C(Lj+a)^2\right]\right. \\ &+ \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{h}{k} C(Lj+a)^2\right] \sum_{\nu=1}^{\infty} \exp\left[\frac{2\pi i \nu}{Lk}(Lj+a) - \frac{\pi^2\nu^2}{C(Lk)^2}\left(\frac{1}{n} - i\theta\right)^{-1}\right] \\ &\left. + \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{h}{k} C(Lj-a)^2\right] \sum_{\nu=1}^{\infty} \exp\left[\frac{2\pi i \nu}{Lk}(Lj-a) - \frac{\pi^2\nu^2}{C(Lk)^2}\left(\frac{1}{n} - i\theta\right)^{-1}\right]\right].\end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

As in Definition 5.1, put

$$G_{C,L,a}(h,k,\nu) = \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{h}{k}C(Lj+a)^2 + \frac{\nu}{Lk}(Lj+a)\right]$$

and

$$G_{C,L,a}(h,k) = G_{C,L,a}(h,k,0) = \sum_{j=0}^{k-1} \mathrm{e}\left[\frac{h}{k}C(Lj+a)^2\right].$$

Then

$$\theta_{C,L,a}(w) = \sqrt{\frac{\pi}{L^2C}}\,\frac{1}{k}\left(\frac{1}{n}-i\theta\right)^{-1/2}\left[G_{C,L,a}(h,k) + \sum_{\nu=1}^{\infty}\Big(G_{C,L,a}(h,k,\nu)+G_{C,L,-a}(h,k,\nu)\Big)\exp\left[-\frac{\pi^2\nu^2}{C(Lk)^2}\left(\frac{1}{n}-i\theta\right)^{-1}\right]\right].$$

Finally, write

$$\varphi_{C,L,a}(w) = \frac{1}{k}\left(\frac{1}{n}-i\theta\right)^{-1/2} G_{C,L,a}(h,k)$$

and

$$\Phi_{C,L,a}(w) = \frac{1}{k}\left(\frac{1}{n}-i\theta\right)^{-1/2}\sum_{\nu=1}^{\infty} G_{C,L,a}(h,k,\nu)\exp\left[-\frac{\pi^2\nu^2}{C(Lk)^2}\left(\frac{1}{n}-i\theta\right)^{-1}\right]$$

so that

$$\theta_{C,L,a}(w) = \sqrt{\frac{\pi}{L^2C}}\left[\varphi_{C,L,a}(w) + \Phi_{C,L,a}(w) + \Phi_{C,L,-a}(w)\right].$$

In this last formula, $\varphi_{C,L,a}(w)$ is the most important term, while the $\Phi_{C,L,\pm a}(w)$ terms will be subsumed into the error term.

Now, recall the integral formula for $r(n)$:

$$r(n) = \frac{1}{2\pi i}\sum_{k=1}^{N}{\sum_{h\le k}}' \int_{\phi_{h,k}} \theta_{C_1,L_1,a_1}(w)\,\theta_{C_2,L_2,a_2}(w)\,\theta_{C_3,L_3,a_3}(w)\,\theta_{C_4,L_4,a_4}(w)\,\frac{dw}{w^{n+1}}.$$

Substitute for $\theta_{C,L,a}(w)$ and distribute terms to obtain

$$r(n) = \frac{\pi^2}{L_1L_2L_3L_4\sqrt{C_1C_2C_3C_4}}\left[J_0 + (J_1+J_2+J_3+J_4)\right]$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

where

$$J_0 = \frac{1}{2\pi i}\sum_{k=1}^{N}{\sum_{h\le k}}' \int_{\phi_{h,k}} \varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\varphi_{C_4,L_4,a_4}(w)\frac{dw}{w^{n+1}}$$

$$J_1 = \frac{1}{2\pi i}\sum_{k=1}^{N}{\sum_{h\le k}}' \int_{\phi_{h,k}} \sum \varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\Phi_{C_4,L_4,\pm a_4}(w)\,\frac{dw}{w^{n+1}}$$

$$J_2 = \frac{1}{2\pi i}\sum_{k=1}^{N}{\sum_{h\le k}}' \int_{\phi_{h,k}} \sum \varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\Phi_{C_3,L_3,\pm a_3}\,\Phi_{C_4,L_4,\pm a_4}(w)\,\frac{dw}{w^{n+1}}$$

$$J_3 = \frac{1}{2\pi i}\sum_{k=1}^{N}{\sum_{h\le k}}' \int_{\phi_{h,k}} \sum \varphi_{C_1,L_1,a_1}\,\Phi_{C_2,L_2,\pm a_2}\,\Phi_{C_3,L_3,\pm a_3}\,\Phi_{C_4,L_4,\pm a_4}(w)\,\frac{dw}{w^{n+1}}$$

$$J_4 = \frac{1}{2\pi i}\sum_{k=1}^{N}{\sum_{h\le k}}' \int_{\phi_{h,k}} \sum \Phi_{C_1,L_1,\pm a_1}\,\Phi_{C_2,L_2,\pm a_2}\,\Phi_{C_3,L_3,\pm a_3}\,\Phi_{C_4,L_4,\pm a_4}(w)\,\frac{dw}{w^{n+1}}.$$

In the formulas for J_1, J_2, J_3 and J_4, the innermost sums represent sums over permutations of (C_1, L_1, a_1), (C_2, L_2, a_2), (C_3, L_3, a_3) and (C_4, L_4, a_4), and alternative sign choices for $\pm a_i$. For example, in J_1,

$$\sum \varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\Phi_{C_4,L_4,\pm a_4}(w)$$

represents the sum

$$\begin{aligned}
&\varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\Phi_{C_4,L_4,a_4}(w) + \varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\Phi_{C_4,L_4,-a_4}(w)\\
&+ \varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\Phi_{C_3,L_3,a_3}\,\varphi_{C_4,L_4,a_4}(w) + \varphi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\Phi_{C_3,L_3,-a_3}\,\varphi_{C_4,L_4,a_4}(w)\\
&+ \varphi_{C_1,L_1,a_1}\,\Phi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\varphi_{C_4,L_4,a_4}(w) + \varphi_{C_1,L_1,a_1}\,\Phi_{C_2,L_2,-a_2}\,\varphi_{C_3,L_3,a_3}\,\varphi_{C_4,L_4,a_4}(w)\\
&+ \Phi_{C_1,L_1,a_1}\,\varphi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\varphi_{C_4,L_4,a_4}(w) + \Phi_{C_1,L_1,-a_1}\,\varphi_{C_2,L_2,a_2}\,\varphi_{C_3,L_3,a_3}\,\varphi_{C_4,L_4,a_4}(w).
\end{aligned}$$

In the formula for $r(n)$ given above, the first sum of integrals J_0 will (eventually) produce the asymptotic estimate for $r(n)$. The other sums are error terms, so we will need to demonstrate that they are all of order $O\left(n^{15/16+\epsilon}\right)$.

6.4 Intermission: Many Useful Lemmas

The rest of this chapter is devoted to the evaluation of the sums J_0, J_1, J_2, J_3 and J_4. Each evaluation will require breaking up the summation over k and the integral over θ into a sum of sums and integrals. All but one of the resulting terms will then be estimated using the steps below. The remaining term, obtained from J_0, will become the asymptotic estimate.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

This section presents the general approach that will be used to evaluate each term. The lemmas in this section contain calculations invoked repeatedly in the rest of the chapter.

Step 1. Substitute θ for w using

$$w = \exp\left[-\frac{1}{n} + \frac{2\pi i h}{k} + i\theta\right] \quad \Longrightarrow \quad \frac{dw}{w^{n+1}} = i\,e\,\exp\left[-\frac{2\pi i h}{k}\,n - ni\theta\right] d\theta,$$

then rearrange the sums and integrals so that the summation over h is innermost, and apply Theorem 5.10 to obtain an upper bound. In a few cases, apply Corollary 5.5 instead; then replace the summation over h by $\phi(k)$.

Corollary 5.5 (p. 86). *For* $\gcd(h,k) = 1$ *and any* ν,

$$G_{C,L,a}(h,k,\nu) = O\left(\sqrt{k}\right).$$

Theorem 5.10 (p. 89). *Given integers* n, k *and* μ *with* $0 \le \mu < k \le N = \lfloor\sqrt{n}\rfloor$, *and integers* ν_1, ν_2, ν_3 *and* ν_4, *then for any positive real* ϵ:

$$\sum_{h''\le\mu}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k,\nu_i) = O\left(k^{23/8+\epsilon}\gcd(u,k)^{1/4}\right),$$

where $u = O(n)$, *and* $\sum'_{h''\le\mu}$ *denotes the sum over all* $1 \le h \le k$ *with* $\gcd(h,k) = 1$ *and* $h'' \le \mu$, *where* h'' *is the unique solution to* $h(h''+N)+1 \equiv 0 \bmod k$ *in the domain* $1 \le h'' \le k$.

Step 2. If the term contains summations over ν_i resulting from some of the error terms $\Phi_{L_i,\pm a_i}(w)$, then apply Corollary 6.5 (either part (a) or (b)) to remove the sums.

Lemma 6.3. *Let* n *be a positive integer.*

(a) *If* $N = \lfloor\sqrt{n}\rfloor$ *then* $1 \le \dfrac{n}{N^2} \le 3$.

(b) *If* $1 \le k \le N = \lfloor\sqrt{n}\rfloor$ *and* $0 \le \theta \le \dfrac{2\pi}{kN}$, *then* $\dfrac{n}{k^2(1+n^2\theta^2)} > \dfrac{1}{120}$.

(c) *If* $1 \le k \le n^{1/2-\ell}$ *and* $0 \le \theta \le k^{-1}n^{-1/2-\ell}$ *then* $\dfrac{n}{k^2(1+n^2\theta^2)} \ge \dfrac{n^{2\ell}}{2}$.

Proof of (a). $N = \lfloor\sqrt{n}\rfloor$ implies that $N^2 \le n < (N+1)^2$. Then $n/N^2 \ge N^2/N^2 = 1$ for all n. If $N = 1$, then $n \le 3$ so $n/N^2 \le 3/1^2 = 3$. For $N \ge 2$,

$$\frac{n}{N^2} < \frac{(N+1)^2}{N^2} = 1 + \frac{2}{N} + \frac{1}{N^2} \le 1 + \frac{2}{2} + \frac{1}{4} < 3.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof of (b) Use the given bounds and part (a).

$$\frac{n}{k^2(1+n^2\theta^2)} \geq \frac{n}{k^2(1+n^2(2\pi/kN)^2)} = \frac{1}{(k^2/n)+n(4\pi^2/N^2)}$$
$$\geq \frac{1}{(N^2/n)+4\pi^2(n/N^2)} \geq \frac{1}{1+12\pi^2} > \frac{1}{120}.$$

Proof of (c) Use the given bounds.

$$\frac{n}{k^2(1+n^2\theta^2)} \geq \frac{n}{k^2(1+n^2(k^{-1}n^{-1/2-\ell})^2)} = \frac{n}{k^2+n^{1-2\ell}} \geq \frac{n}{(n^{1/2-\ell})^2+n^{1-2\ell}} = \frac{n^{2\ell}}{2}.$$

□

Lemma 6.4. *If $k > 0$ then* $\sum_{\nu=1}^{\infty} \exp[-k\nu^2] < \left(\sqrt{\pi/4k}+1\right)\exp[-k/2]$.

Proof.

$$\sum_{\nu=1}^{\infty} \exp[-k\nu^2] = \exp[-k] + \sum_{\nu=2}^{\infty} \exp[-k\nu^2] \leq \exp(-k) + \int_{\nu=1}^{\infty} \exp[-k\nu^2]\,d\nu.$$

Put $I = \int_{\nu=1}^{\infty} \exp[-k\nu^2]\,d\nu$. Then:

$$I^2 = \left[\int_{x=1}^{\infty} \exp[-kx^2]\,dx\right]\left[\int_{y=1}^{\infty} \exp[-ky^2]\,dy\right] = \int_{x=1}^{\infty}\int_{y=1}^{\infty} \exp[-k(x^2+y^2)]\,dy\,dx$$
$$< \int_{r=1}^{\infty}\int_{\theta=0}^{\pi/2} \exp[-kr^2]\,r\,d\theta\,dr = \frac{\pi}{2}\frac{1}{-2k}\exp[-kr^2]\Big|_{r=1}^{\infty} = \frac{\pi}{4k}\exp[-k].$$

So $I < \sqrt{\frac{\pi}{4k}}\exp\left[-\frac{k}{2}\right]$ and

$$\sum_{\nu=1}^{\infty} \exp[-k\nu^2] < \exp[-k] + \sqrt{\frac{\pi}{4k}}\exp\left[-\frac{k}{2}\right] < \left(\sqrt{\frac{\pi}{4k}}+1\right)\exp\left[-\frac{k}{2}\right].$$

□

Corollary 6.5. *Let n and L be positive integers with L a constant.*
(a) If $1 \leq k \leq N = \lfloor\sqrt{n}\rfloor$ and $0 \leq \theta \leq 2\pi/kN$, then

$$\sum_{\nu=1}^{\infty} \exp\left[-\frac{\pi^2\nu^2}{L^2k^2}\frac{n}{1+n^2\theta^2}\right] < K,$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(b) If $1 \le k \le n^{1/2-\ell}$ *and* $0 \le \theta \le k^{-1}n^{-1/2-\ell}$ *with* $\ell > 0$, *then*

$$\sum_{\nu=1}^{\infty} \exp\left[-\frac{\pi^2\nu^2}{L^2k^2}\frac{n}{1+n^2\theta^2}\right] < K\exp\left[-Kn^{2\ell}\right],$$

where each instance of K *denotes some positive constant depending only upon* L.

Proof. Apply Lemmas 6.3 then 6.4.

$$\sum_{\nu=1}^{\infty} \exp\left[-\frac{\pi^2\nu^2}{L^2k^2}\frac{n}{1+n^2\theta^2}\right] < \sum_{\nu=1}^{\infty} \exp\left[-\frac{\pi^2\nu^2}{120L^2}\right] < \left(L\sqrt{\frac{30}{\pi}}+1\right)\exp\left[-\frac{\pi^2}{240L^2}\right].$$

and

$$\sum_{\nu=1}^{\infty} \exp\left[-\frac{\pi^2\nu^2}{L^2k^2}\frac{n}{1+n^2\theta^2}\right] < \sum_{\nu=1}^{\infty} \exp\left[-\frac{\pi^2n^{2\ell}\nu^2}{2L^2}\right] < \left(\frac{L}{n^\ell\sqrt{2\pi}}+1\right)\exp\left[-\frac{\pi^2n^{2\ell}}{4L^2}\right].$$

and $n^\ell > 1$. □

Step 3. Evaluate the integral over θ by using either the first or second equation from Lemma 6.6.

Lemma 6.6. *If* $A > 0$, *then*

$$(a) \quad \int_{\theta=0}^{\infty}\left(\frac{1}{n^2}+\theta^2\right)^{-1}d\theta = n\arctan(n\theta)\Big|_{\theta=0}^{\infty} = \frac{\pi}{2}n; \quad \textit{and}$$

$$(b) \quad \int_{\theta=A}^{\infty}\left(\frac{1}{n^2}+\theta^2\right)^{-1}d\theta < \int_{\theta=A}^{\infty}\theta^{-2}d\theta = \frac{1}{\theta}\Big|_{\theta=A}^{\infty} = \frac{1}{A}.$$

Step 4. Remove the summation over k by applying one of the formulas from Lemma 6.9.

Lemma 6.7. *Let* $d(u)$ *be the number of divisors of* u. *Then* $d(u) = O(u^\epsilon)$ *for any* $\epsilon > 0$.

Proof. This is based on a proof from p. 69 of [Nar83]. Put

$$S_\epsilon = \left\{p^a \;\middle|\; \frac{a+1}{(p^\epsilon)^a} > 1\right\}.$$

Now, fix p and consider the graph of $f(a) = (a+1)/(p^\epsilon)^a$. The equation $f(a) = 1$ has solutions at $a = 0$ and $a = a_{p,\epsilon}$ (> 0), and $f(a) > 1 \iff 0 < a < a_{p,\epsilon}$. Moreover,

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$a_{p,\epsilon}$ decreases as p increases. If $p^\epsilon \geq 2$, then $a_{p,\epsilon} \leq 1$. Consequently, $p^a \in S_\epsilon$ if and only if $p < 2^{1/\epsilon}$ and $a < a_{p,\epsilon}$. Hence, S_ϵ is a finite set, so we can define

$$M_\epsilon = \prod_{p^a \in S_\epsilon} \frac{a+1}{(p^\epsilon)^a}.$$

Now, for any $u = \prod_i p_i^{a_i}$,

$$\frac{d(u)}{u^\epsilon} = \frac{\prod_i (a_i+1)}{[\prod_i p_i^{a_i}]^\epsilon} = \prod_i \frac{a_i+1}{(p_i^\epsilon)^{a_i}} \leq \prod_{p^a \in S_\epsilon} \frac{a+1}{(p^\epsilon)^a} = M_\epsilon.$$

So, $d(u) \leq M_\epsilon u^\epsilon$ for all u. □

Corollary 6.8. *If $k \geq 0$, then $\sum_{\delta|u} \frac{1}{\delta^k} = O(u^\epsilon)$ for any $\epsilon > 0$.*

Proof. $\sum_{d|u} d^k \leq \sum_{d|u} 1 = d(u) \leq M_\epsilon u^\epsilon$. □

Lemma 6.9. *Let $u \in \mathbb{Z}$ and $N_0, \epsilon \in \mathbb{R}$ all be positive. Then*

(a) $\displaystyle\sum_{k=1}^{N_0} k^{-1/8} \gcd(u,k)^{1/4} = O\left(N_0^{7/8} u^\epsilon\right)$; *and*

(b) $\displaystyle\sum_{k>N_0}^{\infty} k^{-9/8} \gcd(u,k)^{1/4} = O\left(N_0^{-1/8} u^\epsilon\right)$.

Proof of (a).

$$\sum_{k=1}^{N_0} k^{-1/8} \gcd(u,k)^{1/4} = \sum_{\delta|u} \sum_{\substack{k=1 \\ (k,u)=\delta}}^{N_0} k^{-1/8} \delta^{1/4} \leq \sum_{\delta|u} \sum_{k\delta \leq N_0} (k\delta)^{-1/8} \delta^{1/4}$$

$$= \sum_{\delta|u} \delta^{1/8} \sum_{k\delta \leq N_0} k^{-1/8} < \sum_{\delta|u} \delta^{1/8} \int_0^{N_0/\delta} k^{-1/8}\, dk = \sum_{\delta|u} \delta^{1/8} \frac{k^{7/8}}{7/8}\Big|_0^{N_0/\delta}$$

$$= \frac{8}{7} N_0^{7/8} \sum_{\delta|u} \delta^{1/8} \delta^{-7/8} = \frac{8}{7} N_0^{7/8} \sum_{\delta|u} \delta^{-3/4} = O\left(N_0^{7/8} u^\epsilon\right).$$

Proof of (b)

$$\sum_{k>N_0}^{\infty} k^{-9/8} \gcd(u,k)^{1/4} = \sum_{\delta|u} \sum_{\substack{k>N_0 \\ (k,u)=\delta}}^{\infty} k^{-9/8} \delta^{1/4} \leq \sum_{\delta|u} \sum_{k\delta > N_0} (k\delta)^{-9/8} \delta^{1/4}$$

$$= \sum_{\delta|u} \delta^{-7/8} \sum_{k>N_0/\delta}^{\infty} k^{-9/8} < \sum_{\delta|u} \delta^{-7/8} \int_{N_0/\delta}^{\infty} k^{-9/8}\, dk = \sum_{\delta|u} \delta^{-7/8} \frac{k^{-1/8}}{-1/8}\Big|_{N_0/\delta}^{\infty}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$= 8N_0^{-1/8} \sum_{\delta|u} \delta^{-7/8}\delta^{1/8} = 8N_0^{-1/8} \sum_{\delta|u} \delta^{-3/4} = O\left(N_0^{-1/8} u^{\epsilon}\right).$$

□

6.5 Step 4: Split J_0 into $J_{0,1} + J_{0,2} + J_{0,3}$

Definition 6.10 (Notation). Throughout the rest of the chapter, the letter K represents some constant positive number, depending only on the values of C_i, L_i and a_i for $i = 1, 2, 3, 4$. Different instances of K may represent different constant values, even within the same formula.

Sections 6.6 though 6.9 are dedicated to the evaluation of the sum

$$J_0 = \frac{1}{2\pi i} \sum_{k=1}^{N} {\sum_{h\le k}}' \int_{\phi_{h,k}} \varphi_{C_1,L_1,a_1}\, \varphi_{C_2,L_2,a_2}\, \varphi_{C_3,L_3,a_3}\, \varphi_{C_4,L_4,a_4}(w)\, \frac{dw}{w^{n+1}}$$

where $\varphi_{C,L,a}(w) = (1/k)(1/n - i\theta)^{-1/2} G_{C,L,a}(h,k)$, so that

$$J_0 = \frac{1}{2\pi i} \sum_{k=1}^{N} \frac{1}{k^4} {\sum_{h\le k}}' \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \int_{\phi_{h,k}} \left(\frac{1}{n} - i\theta\right)^{-2} \frac{dw}{w^{n+1}}.$$

Begin by breaking up the interval of integration $\phi_{h,k}$ into three subintervals:

$$\int_{-2\pi/k(k+k_1)}^{2\pi/k(k+k_2)} = \int_{-2\pi/k(k+k_1)}^{-2\pi/k(k+N)} + \int_{-2\pi/k(k+N)}^{2\pi/k(k+N)} + \int_{2\pi/k(k+N)}^{2\pi/k(k+k_2)},$$

and write $J_0 = J_{0,1} + J_{0,2} + J_{0,3}$. The asymptotic estimate for $r(n)$ will be obtained from the sum $J_{0,2}$, while $J_{0,1}$ and $J_{0,3}$ will be subsumed within the error term.

6.6 Step 5: Further Split $J_{0,2}$

In preparation for the evaluation of $J_{0,2}$, define

$$F(x) = \sum_{\alpha=0}^{\infty} \alpha x^{\alpha} = \frac{x}{(1-x)^2} \quad \text{so that} \quad F(e^z) = \sum_{\alpha=0}^{\infty} \alpha e^{\alpha z} = \frac{e^z}{(1-e^z)^2}.$$

The function $F(e^z)$ has Laurent series

$$\frac{e^z}{(1-e^z)^2} = \frac{1}{z^2} - \frac{1}{12} + \frac{1}{240} z^2 - \frac{1}{6048} z^4 + \frac{1}{172800} z^6 + \cdots$$

converging for all $z \neq 0$. Put $z = -1/n + i\theta$. If $|\theta| \le 2\pi/N$ and $N = \lfloor \sqrt{n} \rfloor$, then

$$|z| = \sqrt{\frac{1}{n^2} + \theta^2} \le \sqrt{\frac{1}{n^2} + \frac{4\pi^2}{N^2}} \le \frac{1}{N}\sqrt{\frac{1}{n} + 4\pi^2} < \frac{41}{N}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

So,

$$F(e^z) = \frac{e^z}{(1-e^z)^2} = \frac{1}{z^2} + O(1) \qquad \text{and} \qquad \left(\frac{1}{n} - i\theta\right)^{-2} = F(e^z) + O(1).$$

Then

$$\left|\int_{\theta=-2\pi/k(k+N)}^{2\pi/k(k+N)} K\frac{dw}{w^{n+1}}\right| \le K\int_{\theta=-2\pi/k(k+N)}^{2\pi/k(k+N)} \left|\frac{dw}{w^{n+1}}\right| < K\int_{\theta=-\pi/kN}^{\pi/kN} \left|\frac{dw}{w^{n+1}}\right|$$
$$= K\int_{\theta=-\pi/kN}^{\pi/kN} e\,d\theta = K\,\frac{2\pi e}{kN} = O\left(\frac{1}{kN}\right).$$

Therefore

$$\int_{\theta=-2\pi/k(k+N)}^{2\pi/k(k+N)} \left(\frac{1}{n} - i\theta\right)^{-2} \frac{dw}{w^{n+1}} = \int_{\theta=-2\pi/k(k+N)}^{2\pi/k(k+N)} F(e^z)\frac{dw}{w^{n+1}} + O\left(\frac{1}{kN}\right).$$

This fact, combined with Corollary 5.5 produces:

$$J_{0,2} = \frac{1}{2\pi i}\sum_{k=1}^{N}\frac{1}{k^4}\sum_{h\le k}{}' \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \int_{\theta=-2\pi/k(k+N)}^{2\pi/k(k+N)} \left(\frac{1}{n} - i\theta\right)^{-2} \frac{dw}{w^{n+1}}.$$

$$J_{0,2} = \frac{1}{2\pi i}\sum_{k=1}^{N}\frac{1}{k^4}\sum_{h\le k}{}' \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right]$$
$$\cdot \int_{\theta=-2\pi/k(k+N)}^{2\pi/k(k+N)} F(e^z)\frac{dw}{w^{n+1}} + O\left(\sum_{k=1}^{N}\frac{1}{k^4}\sum_{h\le k}{}'(k^2)\left(\frac{1}{kN}\right)\right).$$

Simplify the error term:

$$\sum_{k=1}^{N}\frac{1}{k^4}\sum_{h\le k}{}'(k^2)\left(\frac{1}{kN}\right) = \frac{1}{N}\sum_{k=1}^{N}\frac{\phi(k)}{k^3} < \frac{1}{N}\sum_{k=1}^{\infty}\frac{1}{k^2} = \frac{1}{N}\,\frac{\pi^2}{6} = O\left(n^{-1/2}\right).$$

Let Γ denote the circle of radius $e^{-1/n}$, and ζ be the complement of the arc $-2\pi/k(k+N) \le \theta \le 2\pi/k(k+N)$. To evaluate the rest of $J_{2,1}$, we split the interval of integration in terms of Γ and ζ, and then we rewrite the sum over k as a difference of two sums:

$$J_{0,2} = \frac{1}{2\pi i}\sum_{k=1}^{\infty}\frac{1}{k^4}\sum_{h\le k}{}' \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \int_{\Gamma} F(e^z)\frac{dw}{w^{n+1}}$$
$$- \frac{1}{2\pi i}\sum_{k=1}^{N}\frac{1}{k^4}\sum_{h\le k}{}' \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \int_{\zeta} F(e^z)\frac{dw}{w^{n+1}}$$
$$- \frac{1}{2\pi i}\sum_{k=N+1}^{\infty}\frac{1}{k^4}\sum_{h\le k}{}' \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \int_{\Gamma} F(e^z)\frac{dw}{w^{n+1}} + O\left(n^{-1/2}\right).$$

So $J_{0,2} = J_{0,2,1} - J_{0,2,2} - J_{0,2,3} + O(n^{-1/2})$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

6.7 Step 6: Evaluate $J_{0,2,2}$ and $J_{0,2,3}$

One additional lemma is required to evaluate the error terms $J_{0,2,2}$ and $J_{0,2,3}$.

Lemma 6.11. *If $z \neq 0$ and $|Im(z)| \leq \pi$, then* $\left|\dfrac{e^z}{(1-e^z)^2}\right| < \dfrac{\pi^2}{4|z|^2}$.

Proof. If $z = x + iy$, then $\sinh z = (\sinh x)(\cos y) + i(\cosh x)(\sin y)$ so

$$|\sinh z|^2 = (\sinh^2 x)(1 - \sin^2 y) + (1 + \sinh^2 x)(\sin^2 y) = (\sinh x)^2 + (\sin y)^2.$$

Now, $|\sinh x| \geq |x|$ for all real x, and $|\sin y| \geq (2/\pi)\,|y|$ for all $|y| \leq \pi/2$. Therefore

$$|\sinh z|^2 = (\sinh x)^2 + (\sin y)^2 \geq x^2 + \frac{4}{\pi^2}y^2 > \frac{4}{\pi^2}(x^2 + y^2) = \frac{4}{\pi^2}\,|z|^2.$$

Then $|Im(z/2)| \leq \pi/2$ implies

$$\left|\frac{e^z}{(1-e^z)^2}\right| = \frac{1}{4\,|\sinh(z/2)|^2} < \frac{1}{(4)(4/\pi^2)(|z|/2)^2} = \frac{\pi^2}{4\,|z|^2}.$$

□

Estimate the second term first. Substitute for w and move the summation over h to the inside:

$$J_{0,2,2} = K\sum_{k=1}^{N}\frac{1}{k^4}\int_{\zeta}\frac{e^z}{(1-e^z)^2}\exp(-in\theta)\,d\theta\sum_{h\leq k}{}'\,\mathrm{e}\left[-\frac{hn}{k}\right]\prod_{i=1}^{4}G_{C_i,L_i,a_i}(h,k).$$

Apply Lemma 6.9 and Theorem 5.10 (with $\mu = k$):

$$\begin{aligned}|J_{0,2,2}| &= K\sum_{k=1}^{N}\frac{1}{k^4}\,2\int_{\theta=2\pi/k(k+N)}^{\pi}\left|\frac{e^z}{(1-e^z)^2}\right|d\theta\left|\sum_{h\leq k}{}'\,\mathrm{e}\left[-\frac{hn}{k}\right]\prod_{i=1}^{4}G_{C_i,L_i,a_i}(h,k)\right| \\ &< K\sum_{k=1}^{N}\frac{1}{k^4}k^{23/8+\epsilon}\gcd(u,k)^{1/4}\int_{\theta=2\pi/k(k+N)}^{\pi}K\left|-\frac{1}{n}+i\theta\right|^{-2}d\theta \\ &< K\sum_{k=1}^{N}k^{-9/8+\epsilon}\gcd(u,k)^{1/4}\int_{\theta=\pi/kN}^{\infty}\left(\frac{1}{n^2}+\theta^2\right)^{-1}d\theta\end{aligned}$$

Apply Lemma 6.5(b):

$$|J_{0,2,2}| < K\sum_{k=1}^{N}k^{-9/8+\epsilon}\gcd(u,k)^{1/4}\,\frac{kN}{\pi} = KN\sum_{k=1}^{N}k^{-1/8+\epsilon}\gcd(u,k)^{1/4}.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Use Lemma 6.8(a) and the fact that $u = O(n)$ and $N = \lfloor \sqrt{n} \rfloor$ to finish the computation:

$$J_{0,2,2} = O\left(NN^{7/8}u^{\epsilon}\right) = O\left(n^{15/16+\epsilon}\right).$$

Next, use the same approach to estimate the sum $J_{0,2,3}$:

$$J_{0,2,3} = K \sum_{k=N+1}^{\infty} \frac{1}{k^4} \int_{\Gamma} \frac{e^z}{(1-e^z)^2} \exp(-in\theta)\, d\theta \sum_{h\le k}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k).$$

Apply Lemma 6.9 and Theorem 5.10 (with $\mu = k$):

$$\begin{aligned}
|J_{0,2,3}| &= K \sum_{k=N+1}^{\infty} \frac{1}{k^4} 2 \int_{\theta=0}^{\pi} \left|\frac{e^z}{(1-e^z)^2}\right| d\theta \left| \sum_{h\le k}{}' \mathrm{e}\left[\frac{-hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right| \\
&< K \sum_{k=N+1}^{\infty} \frac{1}{k^4} k^{23/8+\epsilon} \gcd(u,k)^{1/4} \int_{\theta=0}^{\pi} K \left|-\frac{1}{n} + i\theta\right|^{-2} d\theta \\
&< K \sum_{k=N+1}^{\infty} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \int_{\theta=0}^{\infty} \left(\frac{1}{n^2} + \theta^2\right)^{-1} d\theta.
\end{aligned}$$

Next, apply Lemma 6.5(a):

$$|J_{0,2,3}| < K \sum_{k=N+1}^{\infty} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} n = Kn^{1+\epsilon} \sum_{k=N+1}^{\infty} k^{-9/8} \gcd(u,k)^{1/4}.$$

Finish by applying Lemma 6.8(b) and recalling that $u = O(n)$:

$$J_{0,2,3} = O\left(n^{1+\epsilon}N^{-1/8}u^{\epsilon}\right) = O\left(n^{15/16+\epsilon}\right).$$

6.8 Step 7: Complete the Evaluation of $J_{0,2}$

Combining the results from Section 6.8 and 6.9 produces

$$\begin{aligned}
J_{0,2} &= J_{0,2,1} - O\left(n^{15/16+\epsilon}\right) - O\left(n^{15/16+\epsilon}\right) + O\left(n^{-1/2}\right) \\
&= \frac{1}{2\pi i} \sum_{k=1}^{\infty} \frac{1}{k^4} \sum_{h\le k}{}' \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \int_{\Gamma} F(e^z) \frac{dw}{w^{n+1}} + O\left(n^{15/16+\epsilon}\right).
\end{aligned}$$

To evaluate the remaining integral, substitute for $F(e^z)$

$$\int_{\Gamma} F(e^z) \frac{dw}{w^{n+1}} = \int_{\Gamma} \sum_{\alpha=1}^{\infty} \alpha w^{\alpha} \mathrm{e}\left[-\frac{h\alpha}{k}\right] \frac{dw}{w^{n+1}}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$= \sum_{\alpha=1}^{\infty} \alpha \, \mathrm{e}\left[-\frac{h\alpha}{k}\right] \int_{\Gamma} w^{\alpha-(n+1)}\, dw = 2\pi i\, n \, \mathrm{e}\left[-\frac{hn}{k}\right],$$

because the integrand $w^{\alpha-(n+1)}$ is analytic if $\alpha \geq n+1$, and the integrand has residue zero unless $\alpha - (n+1) = -1 \iff \alpha = n$.

Therefore:

$$\begin{aligned} J_{0,2} &= n \sum_{k=1}^{\infty} \frac{1}{k^4} \sideset{}{'}\sum_{h \leq k} \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k) + O\left(n^{15/16+\epsilon}\right) \\ &= n\, S(n) + O\left(n^{15/16+\epsilon}\right), \end{aligned}$$

where $S(n)$ is the singular series defined in the statement of Theorem 6.1.

6.9 Step 8: Evaluate $J_{0,1}$ and $J_{0,3}$, Then J_0

In contrast to that of $J_{0,2}$, the evaluation of the sums $J_{0,1}$ and $J_{0,3}$ is relatively straightforward, although it does require the full power of Theorem 5.10.

To estimate $J_{0,3}$, break up the integral into a sum of integrals

$$\int_{\theta=2\pi/k(k+N)}^{2\pi/k(k+k_2)} = \sum_{\mu=k_2+k-N}^{k-1} \int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)},$$

so that

$$\begin{aligned} J_{0,3} &= K \sum_{k=1}^{N} \frac{1}{k^4} \sideset{}{'}\sum_{h \leq k} \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \int_{\theta=2\pi/k(k+N)}^{2\pi/k(k+k_2)} \left(\frac{1}{n} - i\theta\right)^{-2} \frac{dw}{w^{n+1}} \\ &= K \sum_{k=1}^{N} \frac{1}{k^4} \sideset{}{'}\sum_{h \leq k} \left[\prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k)\right] \\ &\quad \cdot \sum_{\mu=k_2+k-N}^{k-1} \int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)} \left(\frac{1}{n} - i\theta\right)^{-2} \exp\left[1 - ni\theta - \frac{2\pi i h n}{k}\right] d\theta. \end{aligned}$$

Then move the sum over h to the inside, past the sum over μ, taking care to fix the indices:

$$\begin{aligned} J_{0,3} = K \sum_{k=1}^{N} \frac{1}{k^4} \sum_{\mu=1}^{k-1} \int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)} \left(\frac{1}{n} - i\theta\right)^{-2} \exp\left(-ni\theta\right) d\theta \\ \cdot \sideset{}{'}\sum_{\substack{h \leq k \\ k_2+k-N \leq \mu}} \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h,k). \end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In a Farey series, $(k_2 + k)h + 1 \equiv 0 \pmod{k}$ because $h_2 k - k_2 h = 1$. Also, $0 < k_2 + k - N \leq k$, so $k_2 + k - N$ is exactly the number h'' in the statement of Theorem 5.10.

$$|J_{0,3}| \leq K \sum_{k=1}^{N} \frac{1}{k^4} \sum_{\mu=1}^{k-1} \int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)} \left(\frac{1}{n^2} + \theta^2\right)^{-1} d\theta \cdot \left| \sum_{h'' \leq \mu}{}' \mathrm{e}\left[-\frac{hn}{k}\right] \prod_{i=1}^{4} G_{C_i, L_i, a_i}(h, k) \right|.$$

Apply Theorem 5.10:

$$|J_{0,3}| \leq K \sum_{k=1}^{N} \frac{1}{k^4} k^{23/8+\epsilon} \gcd(u,k)^{1/4} \sum_{\mu=1}^{k-1} \int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)} \left(\frac{1}{n^2} + \theta^2\right)^{-1} d\theta$$

Recombine the sum of integrals:

$$\begin{aligned} |J_{0,3}| &\leq K \sum_{k=1}^{N} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \int_{\theta=2\pi/k(N+k)}^{2\pi/k(N+1)} \left(\frac{1}{n^2} + \theta^2\right)^{-1} d\theta \\ &< K \sum_{k=1}^{N} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \int_{\theta=\pi/kN}^{\infty} \left(\frac{1}{n^2} + \theta^2\right)^{-1} d\theta \end{aligned}$$

Apply Lemma 6.5(b):

$$|J_{0,3}| < K \sum_{k=1}^{N} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \frac{kN}{\pi} < KNn^{\epsilon} \sum_{k=1}^{N} k^{-1/8} \gcd(u,k)^{1/4}.$$

Apply Lemma 6.8(a):

$$|J_{0,3}| < Kn^{\epsilon} N N^{7/8} u^{\epsilon} \leq Kn^{15/16+\epsilon}$$

so $J_{0,3} = O\left(n^{15/16+\epsilon}\right)$.

Exactly the same argument obtains $J_{0,1} = O\left(n^{15/16+\epsilon}\right)$. Therefore, combine the results from this and the previous section to obtain

$$J_0 = J_{0,1} + J_{0,2} + J_{0,3} = n\,S(n) + O\left(n^{15/16+\epsilon}\right).$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

6.10 Step 9: Begin to Evaluate One of the Remaining Terms

It still remains to evaluate each term making up the sums J_1, J_2, J_3 and J_4. The following sections evaluate one term of J_2, namely:

$$I = \frac{1}{2\pi i}\sum_{k=1}^{N}\sum_{h\le k}{}'\int_{\phi_{h,k}}\sum \varphi_{C_1,L_1,a_1}\varphi_{C_2,L_2,a_2}\Phi_{C_3,L_3,a_3}\Phi_{C_4,L_4,a_4}(w)\frac{dw}{w^{n+1}}$$
$$= K\sum_{k=1}^{N}\frac{1}{k^4}\sum_{\nu_3=1}^{\infty}\sum_{\nu_4=1}^{\infty}\sum_{h\le k}{}'\left[\mathrm{e}\left[-\frac{hn}{k}\right]\prod_{i=1}^{4}G_{C_i,L_i,a_i}(h,k,\nu_i)\right]$$
$$\cdot\int_{\phi_{h,k}}\left(\frac{1}{n}-i\theta\right)^{-2}e^{ni\theta}\exp\left[-\frac{\pi^2}{k^2}\left(\frac{\nu_3^2}{C_3L_3^2}+\frac{\nu_4^2}{C_4L_4^2}\right)\left(\frac{1}{n}-i\theta\right)^{-1}\right]d\theta,$$

where $\nu_1 = 0$ and $\nu_2 = 0$. Other terms within J_1, J_2, J_3 and J_4 differ only in the number of summations over ν_i and in the choice of $i \in \{1,2,3,4\}$. The procedure for evaluating these other terms is identical to the procedure given below.

As before, in the case of J_0, break up the interval of integration $\phi_{h,k}$ into three subintervals:

$$\int_{-2\pi/k(k+k_1)}^{2\pi/k(k+k_2)} = \int_{-2\pi/k(k+k_1)}^{-2\pi/k(k+N)} + \int_{-2\pi/k(k+N)}^{2\pi/k(k+N)} + \int_{2\pi/k(k+N)}^{2\pi/k(k+k_2)}$$

so that $I = I_1 + I_2 + I_3$.

First evaluate I_2. The real part of $(1/n - i\theta)^{-1}$ is $n/(1+n^2\theta^2)$, so

$$|I_2| \le K\sum_{k=1}^{N}\frac{1}{k^4}\sum_{\nu_3=1}^{\infty}\sum_{\nu_4=1}^{\infty}\int_{\theta=-2\pi/k(k+N)}^{2\pi/k(k+N)}\left(\frac{1}{n^2}+\theta^2\right)^{-1}$$
$$\cdot\exp\left[-\frac{\pi^2}{k^2}\left(\frac{\nu_3^2}{C_3L_3^2}+\frac{\nu_4^2}{C_4L_4^2}\right)\frac{n}{1+n^2\theta^2}\right]d\theta\left|\sum_{h\le k}{}'\mathrm{e}\left[-\frac{hn}{k}\right]\prod_{i=1}^{4}G_{C_i,L_i,a_i}(h,k,\nu_i)\right|.$$

Apply Theorem 5.10:

$$|I_2| \le K\sum_{k=1}^{N}k^{-9/8+\epsilon}\gcd(u,k)^{1/4}$$
$$\cdot\int_{\theta=0}^{2\pi/k(k+N)}\left(\frac{1}{n^2}+\theta^2\right)^{-1}\left[\prod_{i=3,4}\sum_{\nu_i=1}^{\infty}\exp\left(-\frac{\pi^2}{k^2}\frac{\nu_i^2}{C_iL_i^2}\frac{n}{1+n^2\theta^2}\right)\right]d\theta.$$

Next, fix a small positive number ℓ and split the sum over k and the integral over θ into three separate sums:

$$\sum_{k=1}^{n}\int_{\theta=0}^{2\pi/k(k+N)}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$$= \sum_{0<k\le n^{1/2-\ell}} \int_{\theta=0}^{k^{-1}n^{-1/2-\ell}} + \sum_{0<k\le n^{1/2-\ell}} \int_{\theta=k^{-1}n^{-1/2-\ell}}^{2\pi/k(k+N)} + \sum_{n^{1/2-\ell}<k\le n} \int_{\theta=0}^{2\pi/k(k+N)},$$

so that $|I_2| \le I_{2,1} + I_{2,2} + I_{2,3}$.

Evaluate $I_{2,1}$:

$$I_{2,1} = K \sum_{0<k\le n^{1/2-\ell}} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \cdot \int_{\theta=0}^{k^{-1}n^{-1/2-\ell}} \left(\frac{1}{n^2}+\theta^2\right)^{-1} \left[\prod_{i=3,4} \sum_{\nu_i=1}^{\infty} \exp\left(-\frac{\pi^2}{k^2}\frac{\nu_i^2}{C_i L_i^2}\frac{n}{1+n^2\theta^2}\right)\right] d\theta.$$

Apply Corollary 6.4(b):

$$I_{2,1} < K\left[\exp\left(-Kn^{2\ell}\right)\right]^2 \sum_{0<k\le n^{1/2-\ell}} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \int_{\theta=0}^{k^{-1}n^{-1/2-\ell}} \left(\frac{1}{n^2}+\theta^2\right)^{-1} d\theta.$$

Apply Lemma 6.5(a):

$$I_{2,1} < Kn\exp\left(-Kn^{2\ell}\right) \sum_{0<k\le n^{1/2-\ell}} k^{-9/8+\epsilon} \gcd(u,k)^{1/4}.$$

Now, $\gcd(u,k)^{1/4} \le k^{1/4}$ so

$$\sum_{0<k\le n^{1/2-\ell}} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \le \sum_{0<k\le n^{1/2-\ell}} k^{-7/8+\epsilon} \le \sum_{0<k\le n^{1/2}} (n^{1/2})^{-7/8+\epsilon}$$
$$\le (n^{1/2})(n^{1/2})^{-7/8+\epsilon} = n^{1/16+\epsilon/2}.$$

So

$$I_{2,1} \le Kn\exp\left(-Kn^{2\ell}\right) n^{1/16+\epsilon/2} = Kn^{17/16+\epsilon}\exp\left(-Kn^{2\ell}\right) = O(1).$$

Next, evaluate $I_{2,2}$.

$$I_{2,2} = K \sum_{0<k\le n^{1/2-\ell}} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \cdot \int_{\theta=k^{-1}n^{-1/2-\ell}}^{2\pi/k(k+N)} \left(\frac{1}{n^2}+\theta^2\right)^{-1} \left[\prod_{i=3,4} \sum_{\nu_i=1}^{\infty} \exp\left(-\frac{\pi^2}{k^2}\frac{\nu_i^2}{C_i L_i^2}\frac{n}{1+n^2\theta^2}\right)\right] d\theta.$$

Apply Corollary 6.4(a):

$$I_{2,2} < K \sum_{0<k\le n^{1/2-\ell}} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \int_{\theta=k^{-1}n^{-1/2-\ell}}^{2\pi/k(k+N)} \left(\frac{1}{n^2}+\theta^2\right)^{-1} d\theta$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Apply Lemma 6.5(b):

$$I_{2,2} < K \sum_{0<k\le n^{1/2-\ell}} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \frac{1}{k^{-1}n^{-1/2-\ell}}$$
$$= Kn^{1/2+\ell} \sum_{0<k\le n^{1/2-\ell}} k^{-1/8+\epsilon} \gcd(u,k)^{1/4}.$$

Apply Lemma 6.8(a):

$$I_{2,2} < Kn^{1/2+\ell+\epsilon}(n^{1/2-\ell})^{7/8}u^{\epsilon} = Kn^{15/16+\ell/8+2\epsilon}.$$

So $I_{2,2} = O\left(n^{15/16+\ell/8}\right)$.

Next, evaluate $I_{2,3}$.

$$I_{2,3} = K \sum_{n^{1/2-\ell}<k\le N} k^{-9/8+\epsilon} \gcd(u,k)^{1/4}$$
$$\cdot \int_{\theta=0}^{2\pi/k(k+N)} \left(\frac{1}{n^2}+\theta^2\right)^{-1} \left[\prod_{i=3,4} \sum_{\nu_i=1}^{\infty} \exp\left(-\frac{\pi^2}{k^2}\frac{\nu_i^2}{C_iL_i^2}\frac{n}{1+n^2\theta^2}\right)\right] d\theta.$$

Apply Corollary 6.4(a):

$$I_{2,3} < K \sum_{n^{1/2-\ell}<k\le N} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \int_{\theta=0}^{2\pi/k(k+N)} \left(\frac{1}{n^2}+\theta^2\right)^{-1} d\theta$$

Apply Lemma 6.5(a):

$$I_{2,3} < K \sum_{n^{1/2-\ell}<k\le N} k^{-9/8+\epsilon} \gcd(u,k)^{1/4} \frac{\pi}{2} n = Kn^{1+\epsilon} \sum_{n^{1/2-\ell}<k\le N} k^{-9/8} \gcd(u,k)^{1/4}.$$

Apply Lemma 6.8(b):

$$I_{2,3} < Kn^{1+\epsilon}(n^{1/2-\ell})^{-1/8}u^{\epsilon} = Kn^{15/16+\epsilon+\ell/8}.$$

Hence, $I_{2,3} = O\left(n^{15/16+\epsilon+\ell/8}\right)$.

Since ℓ can be arbitrarily small,

$$I_2 = O(1) + O(n^{15/16+\ell/8}) + O(n^{15/16+\ell/8}) = O(n^{15/16+\epsilon}).$$

6.11 Step 10: Evaluate I_1 and I_3, Then I

The evaluation of I_3 follows the same approach as the evaluation of $J_{0,3}$, with one additional step. First, break the integral up into a sum of integrals:

$$\int_{\theta=2\pi/k(k+N)}^{2\pi/k(k+k_2)} = \sum_{\mu=k_2+k-N}^{k-1} \int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)},$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

so that

$$I_3 = K\sum_{k=1}^{N}\frac{1}{k^4}\sum_{\nu_3=1}^{\infty}\sum_{\nu_4=1}^{\infty}\left[\sum_{h\le k}{}'\,\mathrm{e}\left[-\frac{hn}{k}\right]\prod_{i=1}^{4}G_{C_i,L_i,a_i}(h,k,\nu_i)\right]$$
$$\cdot\sum_{\mu=k_2+k-N}^{k-1}\int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)}\left(\frac{1}{n}-i\theta\right)^{-2}e^{-ni\theta}$$
$$\cdot\exp\left[-\frac{\pi^2}{k^2}\left(\frac{\nu_3^2}{C_3L_3^2}+\frac{\nu_4^2}{C_4L_4^2}\right)\left(\frac{1}{n}-i\theta\right)^{-1}\right]d\theta.$$

Switch the order of the summation over h with the sum over ν.

$$I_3 = K\sum_{k=1}^{N}\frac{1}{k^4}\sum_{\mu=1}^{k-1}\int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)}\left(\frac{1}{n}-i\theta\right)^{-2}e^{-ni\theta}$$
$$\cdot\sum_{\nu_3=1}^{\infty}\sum_{\nu_4=1}^{\infty}\exp\left[-\frac{\pi^2}{k^2}\left(\frac{\nu_3^2}{C_3L_3^2}+\frac{\nu_4^2}{C_4L_4^2}\right)\left(\frac{1}{n}-i\theta\right)^{-1}\right]d\theta$$
$$\cdot\sum_{\substack{h\le k\\ k_2+k-N\le\mu}}{}'\,\mathrm{e}\left[-\frac{hn}{k}\right]\prod_{i=1}^{4}G_{C_i,L_i,a_i}(h,k,\nu_i).$$

Apply Theorem 5.10:

$$|I_3| \le K\sum_{k=1}^{N}k^{-9/8+\epsilon}\gcd(u,k)^{1/4}\sum_{\mu=1}^{k-1}\int_{\theta=2\pi/k(N+\mu+1)}^{2\pi/k(N+\mu)}\left(\frac{1}{n^2}+\theta^2\right)^{-1}$$
$$\cdot\sum_{\nu_3=1}^{\infty}\sum_{\nu_4=1}^{\infty}\exp\left[-\frac{\pi^2}{k^2}\left(\frac{\nu_3^2}{C_3L_3^2}+\frac{\nu_4^2}{C_4L_4^2}\right)\frac{n}{1+n^2\theta^2}\right]d\theta.$$

Recombine the sum of integrals and apply Corollary 6.4(a):

$$|I_3| < K\sum_{k=1}^{N}k^{-9/8+\epsilon}\gcd(u,k)^{1/4}\int_{\theta=2\pi/k(N+k)}^{2\pi/k(N+1)}\left(\frac{1}{n^2}+\theta^2\right)^{-1}d\theta.$$

Finish with Lemmas 6.5(b) and 6.8(a):

$$|I_3| < Kn^{\epsilon}N\sum_{k=1}^{N}k^{-1/8}\gcd(u,k)^{1/4} \le Kn^{\epsilon}NN^{7/8}u^{\epsilon} \le Kn^{15/16+\epsilon},$$

so $I_3 = O\left(n^{15/16+\epsilon}\right)$.

Exactly the same argument obtains $I_1 = O\left(n^{15/16+\epsilon}\right)$. Therefore,

$$I = I_1 + I_2 + I_3 = O\left(n^{15/16+\epsilon}\right).$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

6.12 Conclusion

Each of the terms in J_1, J_2, J_3 and J_4 can be evaluated using the exact same approach used for I. The only differences are in the number and choice of summations over ν_i. Consequently,

$$J_i = O\left(n^{15/16+\epsilon}\right) \qquad \text{for each } i = 1, 2, 3, 4.$$

Therefore:

$$r(n) = \frac{\pi^2}{L_1 L_2 L_3 L_4 \sqrt{C_1 C_2 C_3 C_4}}\, n\, S(n) + O(n^{15/16+\epsilon}).$$

The proof of Theorem 6.2 is now complete.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER VII

Evaluation of the Singular Series

For $i = 1, 2, 3, 4$, let a_i, L_i and C_i be fixed integers with L_i and C_i positive. For each non-negative integer n, let $r(n)$ equal the number distinct representations of n in the form

$$n = C_1 y_1^2 + C_2 y_2^2 + C_3 y_3^2 + C_4 y_4^2$$

such that $y_i \equiv a_i \pmod{L_i}$ for each i.

Chapter VI established an asymptotic formula for $r(n)$.

Theorem 6.2 (p. 93). *For each $i = 1, 2, 3, 4$, let C_i, L_i and a_i be fixed integers with C_i and L_i positive. For each non-negative integer n, let $r(n)$ equal the number of integral solutions in the set*

$$\left\{ (y_1, y_2, y_3, y_4) \;\middle|\; n = C_1 y_1^2 + C_2 y_2^2 + C_3 y_3^2 + C_4 y_4^2 \text{ and } y_i \equiv a_i \pmod{L_i} \text{ for each } i \right\}.$$

Then:

$$r(n) = \frac{\pi^2}{L_1 L_2 L_3 L_4 \sqrt{C_1 C_2 C_3 C_4}}\, n\, S(n) + O\left(n^{17/18+\epsilon}\right)$$

for every positive ϵ, where

$$S(n) = \sum_{k=1}^{\infty} A(k, n),$$

$$A(k, n) = k^{-4} \sum_{h \le k}{}' \exp\left[-\frac{2\pi i h n}{k}\right] \prod_{i=1}^{4} G_{C_i, L_i, a_i}(h, k),$$

$$G_{C,L,a}(h, k) = \sum_{j=0}^{k-1} \exp\left[\frac{2\pi i h}{k} C(Lj + a)^2\right],$$

and $\sum'_{h \le k}$ indicates the sum over integers h with $1 \le h \le k$ and $\gcd(h, k) = 1$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

This theorem is only useful when the asymptotic term is known to be larger than the error term. If the singular series $S(n)$ can be bounded below by a constant or by a function that decays slower than the function $n^{-1/16}$, then $r(n)$ is guaranteed to grow arbitrarily large, for arbitrarily many n.

The goal of this chapter is to establish enough information about the singular series $S(n)$ to prove the following theorem.

Theorem 7.9 (p. 128). *Let p and L be positive integers with p prime and L not divisible by p. Let a_1, a_2, a_3 and a_4 be integers with $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{L}$. Let S be the set of representable integers*

$$S = \left\{ n \mid n = y_1^2 + y_2^2 + y_3^2 + y_4^2 \text{ for some } y_i \in \mathbb{Z} \text{ with } y_i \equiv a_i \pmod{L} \right\},$$

and let C be the set of positive integral candidates

$$C = \begin{cases} \left\{ n \mid n \equiv 1 \pmod{L} \right\} & \text{if } L \text{ odd,} \\ \left\{ n \mid n \equiv 1 \pmod{2L} \right\} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L}, \\ \left\{ n \mid n \equiv 1 + L \pmod{2L} \right\} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \not\equiv 1 \pmod{2L}. \end{cases}$$

Also, for each positive integer m, put

$$M_m = \left\{ n \in \mathbb{Z} \mid 2^m \text{ divides } n \right\}.$$

Then $S \subseteq C$. If L is even, then $C \setminus S$ is finite. If L is odd, then $(C \setminus M_m) \setminus S$ is finite for every positive integer m.

The approach taken here to compute $S(n)$ relies upon the fact that

$$A(k_1 k_2, n) = A(k_1, n) A(k_2, n) \qquad \text{when } \gcd(k_1, k_2) = 1$$

to rewrite $S(n)$ as

$$S(n) = \prod_{\text{primes } p} \left[\sum_{e=0}^{\infty} A(p^e, n) \right].$$

Section 7.1 derives formulas for $G_{C,L,a}(h,k)$ in the case when $k = p^e$ is a prime power. Section 7.2 obtains formulas for $A(p^e, n)$ under the restriction that $C_i = 1$ and $L_i = L$ for each i, and $\gcd(L, a_1, a_2, a_3, a_4) = 1$. Finally, Section 7.3 obtains a lower bound for $S(n)$ and proves Theorem 7.9.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

7.1 Evaluation of $G_{C,L,a}(h,k)$

The first goal is to evaluate $G_{C,L,a}(h,k)$. Recall the formulas obtained in Chapter V for the sum $G_{C,L,a}(h,k,\nu)$, and substitute $\nu = 0$.

Theorem 7.9 (p. 128) (with $\nu = 0$). *For $h, k \in \mathbb{Z}$ with $\gcd(h,k) = 1$ and $k > 0$, put $d = \gcd(CL^2, k)$. Write $CL^2 = C'd$, $k = k'd$ and $k' = 2^\kappa k''$ with k'' odd. Then*

$$G_{C,L,a}(h,k) = E_{C,L,a}(h,m,k)\left(\frac{C'h}{k''}\right)\varepsilon(k'')\,\alpha_{C'}(h,k')\,\beta_{C,L,a}(h,k)\sqrt{kd},$$

where

$$E_{C,L,a}(h,m,k) = \exp\left[\frac{2\pi i}{k}h(Ca^2)(1-C'm)\right];$$

$$\varepsilon(k'') = \begin{cases} 1 & \text{if } k'' \equiv 1 \pmod 4, \\ i & \text{if } k'' \equiv 3 \pmod 4; \end{cases}$$

$$\alpha_{C'}(h,k') = \begin{cases} 1 & \text{if } \kappa = 0, \\ 1 + \exp[\pi i h C' k''/2] & \text{for even } \kappa > 0, \\ (2/k'')\sqrt{2}\,\exp[\pi i h C' k''/4] & \text{for odd } \kappa > 1; \end{cases}$$

$$\beta_{C,L,a}(h,k) = \begin{cases} 0 & \text{if } 2hCLa \not\equiv 0 \pmod d, \\ 0 & \text{if } 2hCLa \equiv 0 \pmod{2d} \text{ and } k' \equiv 2 \pmod 4, \\ 0 & \text{if } 2hCLa \equiv d \pmod{2d} \text{ and } k' \equiv 0 \pmod 4, \\ 1 & \text{otherwise;} \end{cases}$$

and where m is any integer satisfying

$$\begin{aligned} &C'm \equiv 1 \pmod{k'} \quad \text{and} \quad 4 \mid m && \text{if } k' \text{ is odd, and} \\ &C'm \equiv 1 \pmod{4k'} && \text{if } k' \text{ is even.} \end{aligned}$$

The goal of this chapter, the evaluation of $S(n)$, only requires formulas for $G_{C,L,a}(h,k)$ when $k = p^e$ is a power of a prime. In this case, the formulas from Theorem 7.9 can be simplified.

Corollary 7.1. *Let $k = p^e$ where p and e are positive integers, with p prime. Write $C' = CL^2/\gcd(CL^2,k)$, $C = C_0 p^c$, $L = L_0 p^\ell$ and $a = a_0 p^\alpha$, where C_0, L_0 and a_0 are not divisible by p. Then if p is odd:*

(1) If $e \le c + 2\ell$ and $e > c + \ell + \alpha$, then $G_{C,L,a}(h,p^e) = 0$.

(2) If $e \le c + 2\ell$ and $e \le c + \ell + \alpha$, then $G_{C,L,a}(h,p^e) = \exp[2\pi i h C a^2/p^e]\,p^e$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(3) If $e \geq c + 2\ell$ *and* $\ell > \alpha$, *then* $G_{C,L,a}(h, p^e) = 0$.

(4) If $e \geq c + 2\ell$ *and* $\ell \leq \alpha$ *and* $e + c$ *is even, then* $G_{C,L,a}(h, p^e) = p^{(e+c)/2+\ell}$.

(5) If $e \geq c + 2\ell$, $\ell \leq \alpha$, $e + c$ *is odd, and* $p \equiv 1 \pmod 4$, *then*

$$G_{C,L,a}(h, p^e) = (hC'/p)\, p^{(e+c)/2+\ell}.$$

(6) If $e \geq c + 2\ell$, $\ell \leq \alpha$, $e + c$ *is odd, and* $p \equiv 3 \pmod 4$, *then*

$$G_{C,L,a}(h, p^e) = i(hC'/p)\, p^{(e+c)/2+\ell}.$$

If $p = 2$, *then:*

(7) If $e \leq c + 2\ell$ *and* $e > c + \ell + \alpha + 1$, *then* $G_{C,L,a}(h, 2^e) = 0$.

(8) If $e \leq c + 2\ell$ *and* $e \leq c + \ell + \alpha + 1$, *then* $G_{C,L,a}(h, 2^e) = \exp[2\pi i h C a^2/2^e]\, 2^e$.

(9) If $e > c + 2\ell$ *and* $\ell > \alpha + 1$, *then* $G_{C,L,a}(h, 2^e) = 0$.

(10) If $e > c + 2\ell + 1$ *and* $\ell < \alpha + 1$ *and* $e + c$ *is even, then*

$$G_{C,L,a}(h, 2^e) = (1 + \exp[\pi i h C'/2])\, 2^{(e+c)/2+\ell}.$$

(11) If $e > c + 2\ell + 1$ *and* $\ell < \alpha + 1$ *and* $e + c$ *is odd, then*

$$G_{C,L,a}(h, 2^e) = \sqrt{2}\, \exp[\pi i h C'/4]\, 2^{(e+c)/2+\ell}.$$

(12) If $e > c + 2\ell + 1$ *and* $\ell = \alpha + 1$, *then* $G_{C,L,a}(h, 2^e) = 0$.

(13) If $e = c + 2\ell + 1$ *and* $\ell < \alpha + 1$, *then* $G_{C,L,a}(h, 2^e) = 0$.

(14) If $e = c + 2\ell + 1$ *and* $\ell = \alpha + 1$, *then* $G_{C,L,a}(h, 2^e) = \exp[\pi i h C'/4]\, 2^e$.

Also:

(15) $G_{C,L,a}(h, 1) = 1$.

In cases (5), (6), (10), (11) and (14), $C' = C_0 L_0^2$.

Proof. Use the same notation as in Theorem 5.4. For each of the 15 cases, the first and second conditions are listed in columns A and B of Table 7.1, along with the values for d, k' and $\beta_{C,L,a}(h, k)$. The value of $d = \gcd(CL^2, k)$ is either p^e or $p^{c+2\ell}$, depending upon condition A. Likewise, $k' = k/d = p^e/d$ is either 1 or $p^{e-c-2\ell}$. The value for $\beta_{C,L,a}(h, k)$ is then computed from k' and from condition B, which indicates

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Case	A	d	k'	B	$\beta_{C,L,a}(h,k)$
(1)	$e \le c+2\ell$	p^e	1	$e > c+\ell+\alpha$	0
(2)	$e \le c+2\ell$	p^e	1	$e \le c+\ell+\alpha$	1
(3)	$e \ge c+2\ell$	$p^{c+2\ell}$	$p^{e-c-2\ell}$	$\ell > \alpha$	0
(4)	$e \ge c+2\ell$	$p^{c+2\ell}$	$p^{e-c-2\ell}$	$\ell \le \alpha$	1
(5)	$e \ge c+2\ell$	$p^{c+2\ell}$	$p^{e-c-2\ell}$	$\ell \le \alpha$	1
(6)	$e \ge c+2\ell$	$p^{c+2\ell}$	$p^{e-c-2\ell}$	$\ell \le \alpha$	1
(7)	$e \le c+2\ell$	2^e	1	$e > c+\ell+\alpha+1$	0
(8)	$e \le c+2\ell$	2^e	1	$e \le c+\ell+\alpha+1$	1
(9)	$e > c+2\ell$	$2^{c+2\ell}$	$2^{e-c-2\ell}$	$\ell > \alpha+1$	0
(10)	$e > c+2\ell+1$	$2^{c+2\ell} > 2$	$2^{e-c-2\ell}$	$\ell < \alpha+1$	1
(11)	$e > c+2\ell+1$	$2^{c+2\ell} > 2$	$2^{e-c-2\ell}$	$\ell < \alpha+1$	1
(12)	$e > c+2\ell+1$	$2^{c+2\ell} > 2$	$2^{e-c-2\ell}$	$\ell = \alpha+1$	0
(13)	$e = c+2\ell+1$	$2^{c+2\ell} = 2$	$2^{e-c-2\ell}$	$\ell < \alpha+1$	0
(14)	$e = c+2\ell+1$	$2^{c+2\ell} = 2$	$2^{e-c-2\ell}$	$\ell = \alpha+1$	1
(15)		1	1		1

Table 7.1: Computation of $\beta_{C,L,a}(h,k)$.

whether the value of $2hCLa = 2hC_0L_0a_0p^{c+\ell+\alpha}$ (or $2hCLa = hC_0L_0a_0 2^{c+\ell+\alpha+1}$ if $p = 2$) is not divisible by d, divisible by d but not by $2d$, or divisible by $2d$. If $\beta_{C,L,a}(h,k) = 0$ then $G_{C,L,a}(h,k) = 0$.

For those cases in which $\beta_{C,L,a}(h,k) = 1$, the parity of $e+c$ and the values for (hC'/k''), $\varepsilon(k'')$, $\alpha_{C'}(h,k')$, $\sqrt{kd}$ and $E_{C,L,a}(h,m,k)$ are evaluated and listed in Table 7.2.

Case	$e+c$	(hC'/k'')	$\varepsilon(k'')$	$\alpha_{C'}(h,k')$	$\sqrt{kd}$	$E_{C,L,a}(h,m,k)$
(2)		1	1	1	p^e	$\exp[2\pi i hCa^2/p^e]$
(4)	even	1	1	1	$p^{(e+c)/2+\ell}$	1
(5)	odd	(hC'/p)	1	1	$p^{(e+c)/2+\ell}$	1
(6)	odd	(hC'/p)	i	1	$p^{(e+c)/2+\ell}$	1
(8)		1	1	1	2^e	$\exp[2\pi i hCa^2/2^e]$
(10)	even	1	1	$1+\mathrm{e}[hC'/4]$	$2^{(e+c)/2+\ell}$	1
(11)	odd	1	1	$\sqrt{2}\,\mathrm{e}[hC'/8]$	$2^{(e+c)/2+\ell}$	1
(14)	odd	1	1	$\sqrt{2}\,\mathrm{e}[hC'/8]$	$2^{(2e-1)/2}$	1
(15)		1	1	1	1	1

Table 7.2: Computation of $G_{C,L,a}(h,k)$.

If $p = 2$ or $k' = 1$, then $k'' = 1$ so $(hC'/k'') = 1$ and $\varepsilon(k'') = 1$. If $k' = p^{e-c-2\ell}$ with p odd but $e+c$ even, then $k'' = (p^{(e-c)/2-\ell})^2$ is a square, so $(hC'/k'') = 1$ and

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

$\varepsilon(k'') = 1$ since $k'' \equiv 1 \pmod 4$. In the remaining cases (5) and (6), k'' is a square times p, so $(hC'/k'') = (hC'/p)$ and $k'' = p^{e-c-2\ell} \equiv p \pmod 4$. Only in case (6), when $p \equiv 3 \pmod 4$, is $\varepsilon(k'') = i$.

If p is odd or $k' = 1$, then $r = 0$ so $\alpha_{C'}(h, k') = 1$. In the remaining cases (9) through (14), $r = e - c - 2\ell$ is even or odd according to whether $e + c$ is even or odd. The parity of r then determines $\alpha_{C'}(h, k')$.

Regarding $\sqrt{kd}$, note that in cases (13) and (14), $e-c-2\ell = 1$ so $e+c+2\ell = 2e-1$.

It remains to determine the value of $E_{C,L,a}(h, m, k)$. In cases (3) through (6), $k = p^e$ and $p \nmid 4C'$ so m can be chosen such that $4 \mid m$ and $1 - C'm \equiv 0 \pmod k$. Then $E_{C,L,a}(h, m, k) = 0$.

Similarly, in cases (9) through (14), $k = 2^e$ and $2 \nmid C'$, so choose m such that $1 - C'm \equiv 0 \pmod{4k}$. Then $E_{C,L,a}(h, m, k) = 0$.

Finally, $k' = 1$ in cases (2) and (8), so choose $m = 0$. Then $E_{C,L,a}(h, m, k) = \exp[2\pi i h C a^2/k]$. □

7.2 Evaluation of $A(p^e, n)$

For the remainder of Chapter VII, computations are restricted to the case with $C_i = 1$ and $L_i = L$ for $i = 1, 2, 3, 4$, and $\gcd(L, a_1, a_2, a_3, a_4) = 1$. This section evaluates

$$A(k, n) = k^{-4} \sideset{}{'}\sum_{h \le k} \exp\left[-\frac{2\pi i h n}{k}\right] \prod_{i=1}^{4} G_{1,L,a_i}(h, k)$$

for k a prime power.

Lemma 7.2. *For any prime p and positive integers e and n, write $n = n_0 p^m$. Then*

$$\sideset{}{'}\sum_{h \le p^e} \exp\left[-\frac{2\pi i h n}{p^e}\right] = \begin{cases} 0 & \text{if } e > m+1; \\ -p^{e-1} & \text{if } e = m+1; \\ -p^{e-1} + p^e & \text{if } e \le m. \end{cases}$$

Let $\psi(p^e, n)$ denote this sum, and put $\psi(1, n) = A(1, n) = 1$. Then for any non-negative integer ℓ,

$$\sum_{e=0}^{\ell} \psi(p^e, n) = \begin{cases} p^\ell & \text{if } \ell \le m; \\ 0 & \text{if } \ell > m. \end{cases}$$

and

$$\sum_{e=0}^{\infty} p^{-2e} \psi(p^e, n) = (1 + p^{-1})(1 - p^{-m-1}).$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof. Write

$$\sum_{h\le p^e}{}' \exp\left[-\frac{2\pi i h n}{p^e}\right] = \sum_{h=0}^{p^e-1} \exp\left[-\frac{2\pi i h n}{p^e} n\right] - \sum_{h'=0}^{p^{e-1}-1} \exp\left[-\frac{2\pi i h'}{p^e} pn\right].$$

The first sum is zero unless p^e divides n, in which case the sum is p^e. The second sum is zero unless p^{e-1} divides n, in which case the sum is p^{e-1}.

Now, if $\ell > m$, then

$$\sum_{e=0}^{\ell} \psi(p^e, n) = 1 + (-1+p) + (-p+p^2) + \cdots + (-p^{m-1}+p^m) + (-p^m) = 0.$$

If $0 < \ell \le m$, then

$$\sum_{e=0}^{\ell} \psi(p^e, n) = 1 + (-1+p) + (-p+p^2) + \cdots + (-p^{\ell-1}+p^\ell) = p^\ell.$$

If $\ell = 0$, then the sum totals to $\psi(1, n) = 1$.

Finally, if $m > 0$ then

$$\begin{aligned}\sum_{e=0}^{\infty} p^{-2e}\psi(p^e, n) &= 1 + \left[\sum_{e=1}^{m} p^{-2e}(p^e - p^{e-1})\right] + p^{-2m-2}(-p^m) \\ &= 1 + (p^{-1} - p^{-2}) + (p^{-2} - p^{-3}) + \cdots + (p^{-m} - p^{-m-1}) - p^{-m-2} \\ &= 1 + p^{-1} - p^{-m-1} - p^{-m-2} = (1+p^{-1})(1-p^{-m-1}).\end{aligned}$$

If $m = 0$, then

$$\sum_{e=0}^{\infty} p^{-2e}\psi(p^e, n) = 1 - p^{-2} = (1+p^{-1})(1-p^{-1}).$$

□

Theorem 7.3. *Let p, e, n, L, a_1, a_2, a_3 and a_4 be integers with p, e, n and L positive and p prime such that $\gcd(L, a_1, a_2, a_3, a_4) = 1$. Put $k = p^e$ and $\Delta = n - (a_1^2 + a_2^2 + a_3^2 + a_4^2)$. Write $L = L_0 p^\ell$. Then if p is odd:*

(1) If $e > \ell > 0$ then $A(p^e, n) = 0$.

(2) If $e \le \ell$ then $A(p^e, n) = \psi(p^e, \Delta)$.

(3) If $\ell = 0$ then $A(p^e, n) = p^{-2e}\,\psi(p^e, n)$.

If $p = 2$, then:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(4) If $\ell > 1$ *and* $e > \ell + 1$ *then* $A(2^e, n) = 0$.

(5) If $\ell = 1$ *and* $e > 3$ *then* $A(2^e, n) = 0$.

(6) If $\ell > 0$ *and* $e \leq \ell + 1$ *then* $A(2^e, n) = \psi(2^e, \Delta)$.

(7) If $\ell = 0$ *and* $e > 1$ *then* $A(2^e, n) = -2^{-2e+2}\,\psi(2^e, n)$.

(8) If $\ell = 0$ *and* $e = 1$ *then* $A(2, n) = 0$.

(9) If $\ell = 1$ *and* $e = 3$ *and any of the* a_i *are even, then* $A(8, n) = 0$.

(10) If $\ell = 1$ *and* $e = 3$ *and all of the* a_i *are odd, then* $A(8, n) = -\psi(8, n)$.

Also, for any prime p *and* $e = 0$*:*

(11) $A(1, n) = \psi(1, n) = \psi(1, \Delta) = p^{-2e}\psi(1, n) = 1$.

Proof. It is safe to assume that at least one of the a_i is not divisible by p, because if p divides all of the a_i, then $p \nmid L$ because $\gcd(L, a_1, a_2, a_3, a_4) = 1$. In this case, replace a_1 by $a_1 + L$. Then a_1 is no longer divisible by p, and the value of $A(p^e, n)$ is unchanged, because $a \equiv a' \pmod{L}$ implies $G_{C,L,a}(h, k) = G_{C,L,a'}(h, k)$.

Since each $C_i = 1$ and each $L_i = L$,

$$A(p^e, n) = p^{-4e} \sideset{}{'}\sum_{h \leq p^e} \exp\left[-\frac{2\pi i h n}{p^e}\right] \prod_{i=1}^{4} G_{1,L,a_i}(h, p^e).$$

If, for any i, $G_{1,L,a_i}(h, p^e) = 0$ for all h, then $A(p^e, n) = 0$. Cases (1), (3), (7), (9), (12) and (13) of Corollary 7.1 list conditions which imply $G_{1,L,a_i}(h, p^e) = 0$ for all h. Since one of the a_i is not divisible by p, $A(p^e, n) = 0$ for all h if any of these "zero" conditions are fulfilled when $\alpha = 0$.

Proof of (1). By part (1) of Corollary 7.1, $A(p^e, n) = 0$ whenever $2\ell \geq e > \ell$. Part (3) implies that $A(p^e, n) = 0$ when $e \geq 2\ell$ and $\ell > 0$.

Proof of (2). Case (2) follows from part (2) of Corollary 7.1:

$$\begin{aligned} A(p^e, n) &= p^{-4e} \sideset{}{'}\sum_{h \leq p^e} \exp\left[-\frac{2\pi i h n}{p^e}\right] \prod_{i=1}^{4} \exp\left[\frac{2\pi i h}{p^e} a_i^2\right] p^e \\ &= \sideset{}{'}\sum_{h \leq p^e} \exp\left[-\frac{2\pi i h}{p^e} n\right] \exp\left[\frac{2\pi i h}{p^e}(a_1^2 + a_2^2 + a_3^2 + a_4^2)\right] \\ &= \sideset{}{'}\sum_{h \leq p^e} \exp\left[-\frac{2\pi i h}{p^e}\Delta\right] = \psi(p^e, \Delta). \end{aligned}$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof of (3). If $\ell = 0$, then by parts (4), (5) and (6),

$$A(p^e, n) = p^{-4e} \sum_{h \le p^e}{}' \exp\left[-\frac{2\pi i h n}{p^e}\right] \prod_{i=1}^{4} \varepsilon\, p^{e/2+0} = p^{-2e} \sum_{h \le p^e}{}' \exp\left[-\frac{2\pi i h n}{p^e}\right] \varepsilon^4$$

where

$$\varepsilon = \begin{cases} 1 & \text{if } e \text{ is even,} \\ (hC'/p) & \text{if } e \text{ is odd and } p \equiv 1 \pmod 4, \\ i(hC'/p) & \text{if } e \text{ is odd and } p \equiv 3 \pmod 4. \end{cases}$$

In each case, $\varepsilon^4 = 1$, so $A(p^e, n) = p^{-2e}\psi(p^e, n)$.

Proof of (4). Part (7) implies that $A(2^e, n) = 0$ whenever $2\ell \ge e > \ell + 1$. Part (9) implies that $A(2^e, n) = 0$ when $e > 2\ell$ and $\ell > 1$.

Proof of (5). This follows from part (12), with $\ell = 1$.

Proof of (6). This follows from part (8):

$$\begin{aligned} A(2^e, n) &= 2^{-4e} \sum_{h \le 2^e}{}' \exp\left[-\frac{2\pi i h n}{2^e}\right] \prod_{i=1}^{4} \exp\left[\frac{2\pi i h}{2^e} a_i^2\right] 2^e \\ &= \sum_{h \le 2^e}{}' \exp\left[-\frac{2\pi i h}{2^e} n\right] \exp\left[\frac{2\pi i h}{2^e}(a_1^2 + a_2^2 + a_3^2 + a_4^2)\right] \\ &= \sum_{h \le 2^e}{}' \exp\left[-\frac{2\pi i h}{2^e}\Delta\right] = \psi(2^e, \Delta). \end{aligned}$$

Proof of (7). If $\ell = 0$ and $e > 1$, then by parts (10) and (11),

$$A(2^e, n) = 2^{-4e} \sum_{h \le 2^e}{}' \exp\left[-\frac{2\pi i h n}{2^e}\right] \prod_{i=1}^{4} \varepsilon\, 2^{e/2+0} = 2^{-2e} \sum_{h \le 2^e}{}' \exp\left[-\frac{2\pi i h n}{2^e}\right] \varepsilon^4$$

where

$$\varepsilon = \begin{cases} 1 + \exp[\pi i h C'/2] & \text{if } e \text{ is even,} \\ \sqrt{2}\, \exp[\pi i h C'/4] & \text{if } e \text{ is odd.} \end{cases}$$

In each case, $\varepsilon^4 = -4$, so $A(2^e, n) = -2^{-2e+2}\psi(2^e, n)$.

Proof of (8). This case follows from part (13).

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof of (9) and (10). Let $\ell = 1$ and $e = 3$. If $2 \mid a_i$, then part (13) implies $A(2^3, n) = 0$. If all the a_i are odd, then part (14) implies

$$A(2^3, n) = 2^{-12} \sum_{h \le 2^3}{}' \exp\left[-\frac{2\pi i h n}{2^3}\right] \prod_{i=1}^{4} \exp\left[\frac{\pi i h C'}{4}\right] 2^3 = -\sum_{h \le 2^3}{}' \exp\left[-\frac{2\pi i h n}{2^3}\right]$$
$$= -\psi(2^3, n).$$

Proof of (11). If $k = 1$, then part (15) implies that

$$A(2^3, n) = 1^{-4} \sum_{h \le 1}{}' \exp\left[-\frac{2\pi i h n}{1}\right] \prod_{i=1}^{4} G_{1,L,a_i}(h, 1) = 1.$$

Also, $\psi(1, n) = \psi(1, \Delta) = 1$ by the definition of ψ. □

7.3 Computation of $S(n)$

It remains to combine the formulas for $A(p^e, n)$ to obtain a lower bound on $S(n)$. This is accomplished by rewriting $S(n)$ as a product

$$S(n) = \prod_{p \text{ prime}} S_p(n) = S_2(n) \cdot \left[\prod_{p \mid L} S_p(n)\right] \cdot \left[\prod_{p \nmid L} S_p(n)\right]$$

where

$$S_p(n) = \sum_{e=0}^{\infty} A(p^e, n).$$

After each $S_p(n)$ is evaluated, each of the three factors in this expression for $S(n)$ is evaluated separately, and then the results are combined.

Gaussian sums $G(h, k)$ satisfy the multiplicative property

$$G(h, k_1 k_2) = G(hk_2, k_1)\, G(hk_1, k_2) \qquad \text{when } \gcd(k_1, k_2) = 1.$$

The sums $G_{C,L,a}(h, k)$ satisfy a similar property:

$$G_{C,L,a}(h, k_1 k_2) = G_{C,L,a}(hk_2', k_1)\, G_{C,L,a}(hk_1', k_2) \qquad \text{when } \gcd(k_1, k_2) = 1$$

where

$$k_1 k_1' = 1 \pmod{k_2} \qquad \text{and} \qquad k_2 k_2' = 1 \pmod{k_1}.$$

This is enough to establish:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Lemma 7.4. *For positive integers n, k_1, k_2 with* $\gcd(k_1, k_2) = 1$,

$$G_{C,L,a}(h_1k_2 + h_2k_1, k_1k_2) = G_{C,L,a}(h_1, k_1)\, G_{C,L,a}(h_2, k_2)$$

and hence

$$A(k_1k_2, n) = A(k_1, n)\, A(k_2, n).$$

Proof. Write $h = h_1k_2 + h_2k_1$ and $k = k_1k_2$. Break the summation over $j = 0, \ldots k_1k_2 - 1$ into sums over $j_1 = 0, \ldots, k_1 - 1$ and $j_2 = 0, \ldots, k_2 - 1$ with $j = j_1k_2 + j_2k_1$. Then,

$$\begin{aligned}
&G_{C,L,a}(h_1k_2 + h_2k_1, k_1k_2) \\
&\quad = \sum_{j_1=0}^{k_1-1} \sum_{j_2=0}^{k_2-1} \exp\left[\frac{2\pi i}{k_1k_2}(h_1k_2 + h_2k_1)C(Lj_1k_2 + Lj_2k_1 + a)^2\right] \\
&\quad = \sum_{j_1=0}^{k_1-1} \sum_{j_2=0}^{k_2-1} \exp\left[\frac{2\pi i}{k_1k_2}(h_1k_2)C(Lj_1k_2 + a)^2 + \frac{2\pi i}{k_1k_2}(h_2k_1)C(Lj_2k_1 + a)^2\right] \\
&\quad = \sum_{j_1=0}^{k_1-1} \exp\left[\frac{2\pi i h_1}{k_1} C(Lj_1k_2 + a)^2\right] \cdot \sum_{j_2=0}^{k_2-1} \exp\left[\frac{2\pi i h_2}{k_2} C(Lj_2k_1 + a)^2\right] \\
&\quad = G_{C,L,a}(h_1, k_1)\, G_{C,L,a}(h_2, k_2).
\end{aligned}$$

Next, within the formula for $A(k_1k_2, n)$, break the summation over $h = 0, \ldots, k-1$ into sums over $h_1 = 0, \ldots, k_1 - 1$ and $h_2 = 0, \ldots, k_2 - 1$ with $h = h_1k_2 + h_2k_1$. Then,

$$\begin{aligned}
A(k_1k_2, n) &= k^{-4} \sum_{h \le k_1k_2}{}' \exp\left[-\frac{2\pi i h}{k_1k_2} n\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h, k) \\
&= (k_1k_2)^{-4} \sum_{h_1 \le k_1}{}' \sum_{h_2 \le k_2}{}' \exp\left[-2\pi i \left(\frac{h_1}{k_1} + \frac{h_2}{k_2}\right) n\right] \\
&\qquad \cdot \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h_1k_2 + h_2k_1, k_1k_2) \\
&= \left(k_1^{-4} \sum_{h_1 \le k_1}{}' \exp\left[-\frac{2\pi i h_1}{k_1} n\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h_1, k_1)\right) \\
&\qquad \cdot \left(k_2^{-4} \sum_{h_2 \le k_2}{}' \exp\left[-\frac{2\pi i h_2}{k_2} n\right] \prod_{i=1}^{4} G_{C_i,L_i,a_i}(h_2, k_2)\right) \\
&= A(k_1, n)\, A(k_2, n).
\end{aligned}$$

□

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Corollary 7.5.

$$S(n) = \sum_{q=1}^{\infty} A(q,n) = \prod_{p \text{ prime}} S_p(n), \qquad \text{where} \qquad S_p(n) = \sum_{e=0}^{\infty} A(p^e, n).$$

The next step is to evaluate each $S_p(n)$.

Proposition 7.6. *For p prime, write $\Delta = n-(a_1^2+a_2^2+a_3^2+a_4^2)$, $L = L_0 p^\ell$, $n = n_0 p^m$ and $\Delta = \Delta_0 p^\delta$. Then:*

(1) If p is odd and $\ell > \delta$, then $S_p(n) = 0$.

(2) If p is odd and $\delta \geq \ell > 0$, then $S_p(n) = p^\ell$.

(3) If p is odd and $\ell = 0$, then $S_p(n) = (1+p^{-1})(1-p^{-m-1})$.

(4) If $p = 2$, $\ell \geq 1$ and $\ell \geq \delta$, then $S_2(n) = 0$.

(5) If $p = 2$ and $\delta > \ell > 1$, then $S_2(n) = 2^{\ell+1}$.

(6) If $p = 2$, $\ell = 1$, $\delta \geq 2$ and any of the a_i are even, then $S_2(n) = 4$.

(7) If $p = 2$, $\ell = 1$, $\delta = 2$ and all of the a_i are odd, then $S_2(n) = 0$.

(8) If $p = 2$, $\ell = 1$, $\delta > 2$ and all of the a_i are odd, then $S_2(n) = 8$.

(9) If $p = 2$, $\ell = 0$ and $m \geq 1$, then $S_2(n) = 3 \cdot 2^{-m}$.

(10) If $p = 2$, $\ell = 0$ and $m = 0$, then $S_2(n) = 1$.

To facilitate the proof, split case (4) into:
(4a) If $p = 2$, $\ell > 1$ and $\ell \geq \delta$, then $S_2(n) = 0$.
(4b) If $p = 2$, $\ell = 1$ and $1 \geq \delta$, then $S_2(n) = 0$.

Proof of (1) and (2). If p is odd and $\ell > 0$, then apply parts (1), (2) and (11) of Theorem 7.3 followed by Lemma 7.2:

$$S_p(n) = \sum_{e=0}^{\infty} A(p^e, n) = \sum_{e=0}^{\ell} \psi(p^e, \Delta) = \begin{cases} 0 & \text{if } \ell > \delta; \\ p^\ell & \text{if } \ell \leq \delta. \end{cases}$$

Proof of (3). If p is odd and $\ell = 0$, apply parts (3) and (11) of 7.3, then Lemma 7.2:

$$S_p(n) = \sum_{e=0}^{\infty} A(p^e, n) = \sum_{e=0}^{\infty} p^{-2e} \psi(p^e, n) = (1+p^{-1})(1-p^{-m-1}).$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof of (4a) and (5). If $p = 2$ and $\ell > 1$, then apply parts (4), (5) and (11) of Theorem 7.3 followed by Lemma 7.2:

$$S_2(n) = \sum_{e=0}^{\infty} A(2^e, n) = \sum_{e=0}^{\ell+1} \psi(2^e, \Delta) = \begin{cases} 0 & \text{if } \ell + 1 > \delta; \\ 2^{\ell+1} & \text{if } \ell + 1 \leq \delta. \end{cases}$$

Proof of (4b), (6), (7) and (8) If $p = 2$ and $\ell = 1$, then by parts (5) and (6) of 7.3.

$$S_2(n) = \sum_{e=0}^{\infty} A(2^e, n) = 1 + \psi(2^1, \Delta) + \psi(2^2, \Delta) + A(2^3, n).$$

By part (9), if any of the a_i are even, then $S_2(n) = 1 + \psi(2^1, \Delta) + \psi(2^2, \Delta)$, and

$$\begin{aligned} \delta = 0 &\implies S_2(n) = 1 + (-2^0) + 0 = 0, \\ \delta = 1 &\implies S_2(n) = 1 + (2^1 - 2^0) + (-2^1) = 0, \\ \delta \geq 2 &\implies S_2(n) = 1 + (2^1 - 2^0) + (2^2 - 2^1) = 4. \end{aligned}$$

By part (10), if all of the a_i are odd, then $S_2(n) = 1 + \psi(2^1, \Delta) + \psi(2^2, \Delta) - \psi(2^3, n)$. Also, $n - \Delta = a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 4 \pmod 8$. Consequently,

$$\begin{aligned} \delta = 0 &\iff m = 0 \implies S_2(n) = 0 - \psi(2^3, n) = 0 - 0 = 0, \\ \delta = 1 &\iff m = 1 \implies S_2(n) = 0 - \psi(2^3, n) = 0 - 0 = 0, \\ \delta = 2 &\iff m > 2 \implies S_2(n) = 4 - \psi(2^3, n) = 4 - (2^3 - 2^2) = 0, \\ \delta > 2 &\iff m = 2 \implies S_2(n) = 4 - \psi(2^3, n) = 4 - (-2^2) = 8. \end{aligned}$$

Proof of (9) and (10). If $p = 2$ and $\ell = 0$, then parts (7), (8) and (11) of Theorem 7.3, followed by Lemma 7.2 imply

$$\begin{aligned} S_2(n) = \sum_{e=0}^{\infty} A(2^e, n) &= 1 + 0 - \sum_{e=2}^{\infty} 2^{-2e+2} \psi(2^e, n) \\ &= 1 + 0 + 2^2 \psi(2^0, n) + 2^0 \psi(2^1, n) - 4 \sum_{e=0}^{\infty} 2^{-2e} \psi(2^e, n) \\ &= 1 + 0 + 4(1) + \psi(2, n) - 4(1 + 2^{-1})(1 - 2^{-m-1}) \\ &= -1 + 3 \cdot 2^{-m} + \psi(2, n). \end{aligned}$$

Then,

$$\begin{aligned} S_2(n) &= -1 + 3 \cdot 2^{-0} - 2^0 = 1, && \text{if } m = 0; \\ S_2(n) &= -1 + 3 \cdot 2^{-m} + (-2^0 + 2^1) = 3 \cdot 2^{-m}, && \text{if } m \geq 1. \end{aligned}$$

□

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Lemma 7.7.

$$\prod_{p|n}(1-p^{-1}) > \frac{K}{\log\log n}$$

for some positive constant K.

Theorem 7.8. *Let n, L, a_1, a_2, a_3 and a_4 be integers with $\gcd(L, a_1, a_2, a_3, a_4) = 1$ and n and L positive. Write $\Delta = n - (a_1^2 + a_2^2 + a_3^2 + a_4^2)$, $n = 2^m n_0$ and $L = L_0 2^\ell$ with n_0 and L_0 odd. Then,*

(1) If $L_0 \nmid \Delta$ then $S(n) = 0$.

(2) If L is even and $2^{\ell+1} \nmid \Delta$, then $S(n) = 0$.

(3) If $L \equiv 2 \pmod 4$, $\Delta \equiv 4 \pmod 8$, and all of the a_i are odd, then $S(n) = 0$. Otherwise,

(4) If L is odd and n is even, then

$$S(n) > \frac{KL}{2^m \log\log n},$$

where K is a positive constant independent of n, L, and the a_i's.

(5) If L is even or n is odd, then

$$S(n) > \frac{KL}{\log\log n},$$

where K is a positive constant independent of n, L, and the a_i's.

Proof. Let P_L be the set of all odd primes that divide L, and P_{NL} be the set of all odd primes that do not divide L. Then:

$$S(n) = \prod_{\text{primes } p} S_p(n) = S_2(n) \cdot \left[\prod_{p \in P_{NL}} S_p(n)\right] \cdot \left[\prod_{p \in P_L} S_p(n)\right].$$

Write $L_0 = \prod_{p \in P_L} p^{\ell_p}$. If there is an odd prime $p \in P_L$ with $p^{\ell_p} \nmid \Delta$, then $S_p(n) = 0$ by part (1) of Proposition 7.6. Otherwise, part (2) implies:

$$\prod_{p \in P_L} S_p(n) = \prod_{p \in P_L} p^{\ell_p} = L_0.$$

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Also,

$$\prod_{p\in P_{NL}} S_p(n) = \prod_{\substack{p\in P_{NL}\\ p|n}} (1+p^{-1})(1-p^{-m-1}) > \prod_{p|n}(1-p^{-1}) > \frac{K}{\log\log n}.$$

By part (4) of Proposition 7.6, if L is even and $2^{\ell+1} \nmid \Delta$, then $S_2(n) = 0$. By part (7), if $L \equiv 2 \pmod 4$ and $\Delta \equiv 4 \pmod 8$ and all of the a_i are odd, then $S_2(n) = 0$. In either case, $S(n) = 0$.

Now, suppose that none of conditions (1), (2) and (3) in the statement are satisfied. If L is odd and n is even, then part (9) of Proposition 7.6 implies

$$S(n) = S_2(n) \cdot \left[\prod_{p\in P_{NL}} S_p(n)\right] \cdot \left[\prod_{p\in P_L} S_p(n)\right] > \left(3\cdot 2^{-m}\right)(L_0)\left(\frac{K}{\log\log n}\right).$$

If L is even or n is odd, then parts (5), (6), (8) and (10) imply

$$S(n) = S_2(n) \cdot \left[\prod_{p\in P_{NL}} S_p(n)\right] \cdot \left[\prod_{p\in P_L} S_p(n)\right] > \left(2^{\ell}\right)(L_0)\left(\frac{K}{\log\log n}\right).$$

□

Theorem 7.9. *Let p and L be positive integers with p prime and L not divisible by p. Let a_1, a_2, a_3 and a_4 be integers with $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod L$. Let S be the set of representable integers*

$$S = \left\{ n \mid n = y_1^2 + y_2^2 + y_3^2 + y_4^2 \text{ for some } y_i \in \mathbb{Z} \text{ with } y_i \equiv a_i \pmod L \right\},$$

and let C be the set of positive integral candidates

$$C = \begin{cases} \{ n \mid n \equiv 1 \pmod L \} & \text{if } L \text{ odd,} \\ \{ n \mid n \equiv 1 \pmod{2L} \} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L}, \\ \{ n \mid n \equiv 1 + L \pmod{2L} \} & \text{if } L \text{ even and } a_1^2 + a_2^2 + a_3^2 + a_4^2 \not\equiv 1 \pmod{2L}. \end{cases}$$

Also, for each positive integer m, put

$$M_m = \left\{ n \mid 2^m \text{ divides } n \right\}.$$

Then $S \subseteq C$. If L is even, then $C \setminus S$ is finite. If L is odd, then $(C \setminus M_m) \setminus S$ is finite for every positive integer m.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof. First, $\gcd(L, a_1, a_2, a_3, a_4) = 1$, because L divides $(a_1^2 + a_2^2 + a_3^2 + a_4^2 - 1)$.

If $n \in S$, then

$$n = y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{L}.$$

Also, if L is even, then $y_i - a_i$ is divisible by L and hence is even. Then $y_i + a_i$ is also even, so $2L$ divides $(y_i + a_i)(y_i - a_i) = y_i^2 - a_i^2$ and so $y_i^2 \equiv a_i^2 \pmod{2L}$. Consequently,

$$n = y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \pmod{2L}.$$

Therefore, $n \in S$ implies $n \in C$.

Next, consider the first three cases of Theorem 7.8. The definition of C guarantees that neither condition (1) nor (2) is satisfied for any $n \in C$. Also, if all the a_i are odd and $L \equiv 2 \pmod{4}$, then $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 + 1 + 1 + 1 \equiv 0 \pmod{2}$, contradicting the fact that $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{L}$. Therefore, condition (3) is also not satisfied.

Consequently, if L is odd, then Theorems 6.2 and 7.8 imply that for all $n \in C \setminus M_m$ and $\epsilon > 0$,

$$r(n) = \frac{\pi^2}{L^2} n\, S(n) + O\left(n^{15/16+\epsilon}\right) > K \frac{n}{2^m \log\log n} + O\left(n^{15/16+\epsilon}\right),$$

where m and K are positive constants independent of n. The asymptotic term grows larger than the error term, so $r(n) > 0$ and $n \in S$ for all but finitely many $n \in C\ M_m$.

If L is even, then for all $n \in C$ and $\epsilon > 0$,

$$r(n) = \frac{\pi^2}{L^2} n\, S(n) + O\left(n^{15/16+\epsilon}\right) > K \frac{n}{\log\log n} + O\left(n^{15/16+\epsilon}\right),$$

where K is a positive constant independent of n. Therefore, $r(n) > 0$ and $n \in S$ for all but finitely many $n \in C$. □

Corollary 7.10. *Let p and L be positive integers with p prime and L not divisible by p. Let a_1, a_2, a_3 and a_4 be integers with $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{L}$. Then there exist integers y_1, y_2, y_3, y_4 and n such that $y_1^2 + y_2^2 + y_3^2 + y_4^2 = p^{2n}$ and $y_i \equiv a_i \pmod{L}$ for $i = 1, 2, 3, 4$ if and only if either*

(1) L is odd,

(2) L is even and $p^{2e} \equiv 1 + L \pmod{2L}$ for some positive integer e, or

(3) L is even and $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 \pmod{2L}$.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

Proof. Define S, C and M_m as in the previous proof. Since p is odd, $p^e \notin M_1$ for all e. Since $\gcd(p, 2L) = 1$, there exists a positive integer e with $p^e \equiv 1 \pmod{2L}$. If either condition (1) or (3) is met, then $p^{2ek} \in C \setminus M_1$ for all positive integers k, and Theorem 7.9 implies that all but finitely many of these p^{2ek} are in S. Instead, if condition (2) is met, then choose e with $p^{2e} \equiv 1 + L \pmod{2L}$. For all odd positive integers k, $p^{2ek} \in C \setminus M$, and Theorem 7.9 implies that all but finitely many of these p^{2ek} are in S.

If L is even, $a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 1 + L \pmod{2L}$ and $p^e \not\equiv 1 + L \pmod{2L}$ for all integers e, then $p^e \notin C$, and hence $p^e \notin S$ for all $e \in \mathbb{Z}$. □

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

CHAPTER VIII

Future Work

8.1 Part I: Subgroups of $GL_2(\mathbb{Q}_p)$ and their Actions on $\mathcal{T}_p$

There are a lot more questions that could be asked about the graphs $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$. For example:

(1) What is the length of the shortest cycle? Restated in number theoretic terms, the question becomes: What is the smallest positive integer n such that the equation

$$a_1^2 + a_2^2 + a_3^2 + a_4^2 = p^{2n}$$

has integral solutions satisfying $a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{L}$, and in the case of $\mathcal{X}'_{p,L}$, $a_1 \equiv p^n \pmod{L}$?

(2) Each of the graphs displayed in Chapter IV contain a Hamiltonian cycle. Is this true of all $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$?

(3) The graphs $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$ exhibit a lot of symmetry. Much of this symmetry is reflected in the structure of the quotient groups $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L}$ and $Q^1(\mathbb{Z}[1/p])/\Gamma'_{p,L}$ which act on $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$. Is all of the symmetry reflected in these quotient groups?

(4) For many values of L,

$$Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L} \cong Q^1(\mathbb{Z}/(L)) \cong SL_2(\mathbb{Z}/(L)).$$

How is the structure of $SL_2(\mathbb{Z}/(L))$ reflected in the symmetries of the $\mathcal{X}_{p,L}$?

(5) What is the spectrum of the graphs $\mathcal{X}_{p,L}$ and $\mathcal{X}'_{p,L}$?

Many of the results obtained in Chapter III could be extended to other subgroups of $SL_2(\mathbb{Q}_p)$ and $Q^1(\mathbb{Q}_p)$ defined using congruence relations on $SL_2(\mathbb{Z}[1/p])$ or $Q^1(\mathbb{Z}[1/p])$. Also, the programs used to obtain the graphs in Chapter IV can easily be modified to produce quotient graphs of other groups. Some choices are:

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

(1) The congruence groups $\Gamma_{p,L}$ and $\Gamma'_{p,L}$ were defined using the standard quaternion algebra. Replace this by a non-standard quaternion algebra, with multiplicative relations

$$\mathbf{i}^2 = A, \quad \mathbf{j}^2 = B \quad \text{and} \quad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}.$$

and norm

$$\|a_1\,\mathbf{1} + a_2\,\mathbf{i} + a_3\,\mathbf{j} + a_4\,\mathbf{k}\| = a_1^2 + Aa_2^2 + Ba_3^2 + ABa_4^2,$$

for some $A, B \in \mathbb{Z}$.

(2) Congruence groups can be defined as the kernel of the map $\mathrm{SL}_2(\mathbb{Z}[1/p]) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/(L))$, or as the kernel of maps involving other matrix groups.

For these other group choices, what are the analogues, if any, of the results in Chapter III? What are the vertex counts for the quotient graphs induced by these groups? The key step is the determination of the images of the maps corresponding to

$$\phi : Q^1(\mathbb{Z}[1/p]) \longrightarrow Q^1(\mathbb{Z}/(L)) \quad \text{and} \quad \alpha : Q^1(\mathbb{Z}[1/p]) \longrightarrow \mathcal{T}_0$$

for the new groups.

Whenever L_1 divides L_2, there is a covering map $\mathcal{X}_{p,L_2} \longrightarrow \mathcal{X}_{p,L_1}$ and group homomorphisms $\Gamma_{p,L_2} \longrightarrow \Gamma_{p,L_1}$ and $Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L_2} \longrightarrow Q^1(\mathbb{Z}[1/p])/\Gamma_{p,L_1}$. Are there intermediate groups between Γ_{p,L_2} and Γ_{p,L_1} that produce intermediate quotient graphs? For example, the graph $\mathcal{X}_{3,5}$ covers the two bipartite graphs shown in Figure 8.1. Is there an intermediate group G with $\Gamma_{3,5} < G < Q^1(\mathbb{Z}[1/3])$ that produces one of these as a quotient graph $G\backslash\mathcal{T}_p$?

8.2 Part II: An Extension of Kloosterman's Method

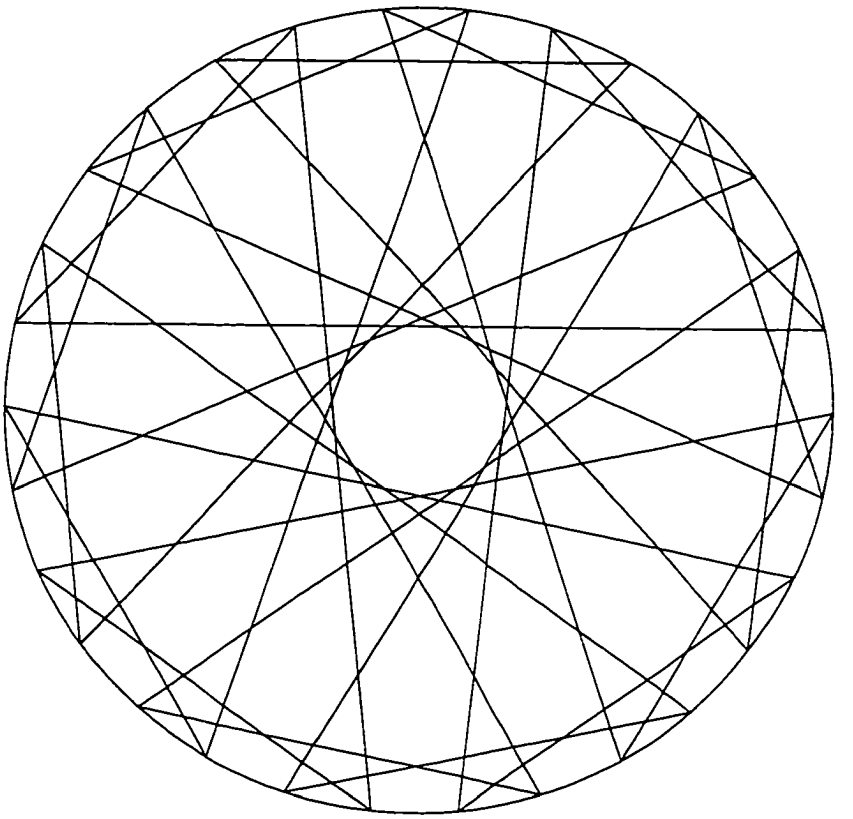
The proof of Theorem 6.2 given here closely follows the method used by Kloosterman in his paper [Klo26]. A more modern proof developed by Estermann is given in [Est36]. In addition, a result by Weil in [Wei48] improves the error term to $O\left(n^{7/8+\epsilon}\right)$. Both of these improvements should be incorporated into the proof of Theorem 6.2.

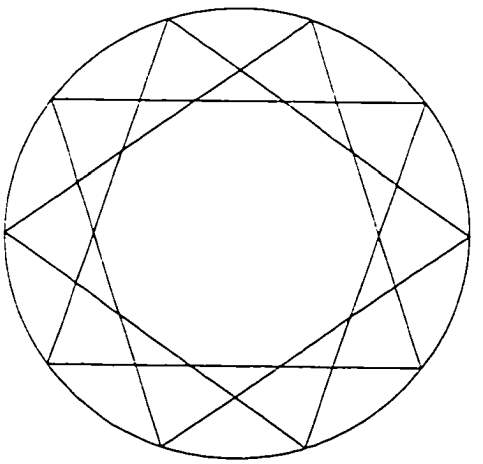
One natural extension to Theorem 6.2 would be to establish an asymptotic formula for the number of representations of n in the form

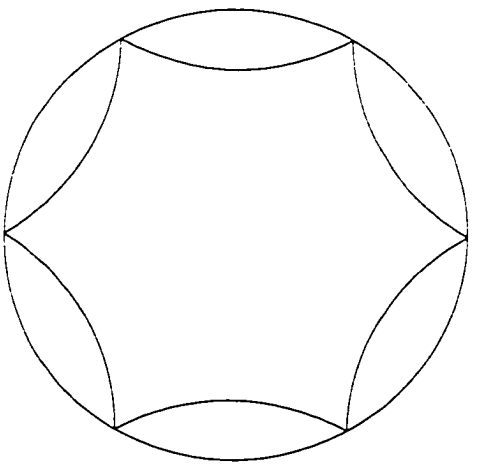
$$n = \sum_{i=1}^{s} C_i y_i^2 \qquad \text{with } y_i \equiv a_i \pmod{L_i} \text{ for } i = 1, \ldots, s,$$

for values of s other than 4. Another extension would be to allow negative values for some of the C_i, as in [Est61].

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.







3-fold

5-fold

Figure 8.1: The graph $\mathcal{X}_{3,5}$ and two of its quotient graphs

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

In order to apply Theorem 6.2, Chapter VII evaluates the singular series $S(n)$ in the limited case of $C_i = 1$ and $L_i = L$, for all i. Completing the evaluation of $S(n)$ in the most general case, with arbitrary C_i, L_i and a_i, would be necessary to apply Theorem 6.2 in a more general setting.

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

BIBLIOGRAPHY

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

BIBLIOGRAPHY

[Est36] Th. Estermann. On the representation of a number as a sum of squares. *Acta Arith.*, 2:47–79, 1936.

[Est61] Th. Estermann. On Kloosterman's sum. *Mathematika*, 8:83–86, 1961.

[FTN91] Alessandro Figà-Talamanca and Claudio Nebbia. *Harmonic Analysis and Representation Theory for Groups Acting on Homogeneous Trees*, volume 162 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1991.

[GGPS69] I. M. Gel'fand, M. I. Graev, and I. I. Pyatetskii-Shapiro. *Representation Theory and Automorphic Functions*. W. B. Saunders Company, 1969.

[Gro85] Emil Grosswald. *Representations of Integers as Sums of Squares*. Springer-Verlag, 1985.

[Har20] G. H. Hardy. On the representation of a number as a sum of any number of squares and in particular of 5. *Trans. Amer. Math. Soc.*, 17:255–284, 1920.

[Jac28] C. G. J. Jacobi. Note sur la décomposition d'un nombre donné en quatre carrés. *J. Reine Angew. Math.*, 3, 1828.

[Klo26] H. D. Kloosterman. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$. *Acta Mathematica*, 49:407–464, 1926.

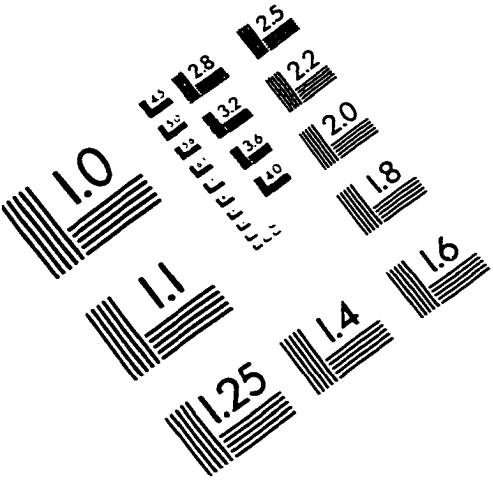
[Nar83] W. Narkiewicz. *Number Theory*. Cambridge University Press, 1983.

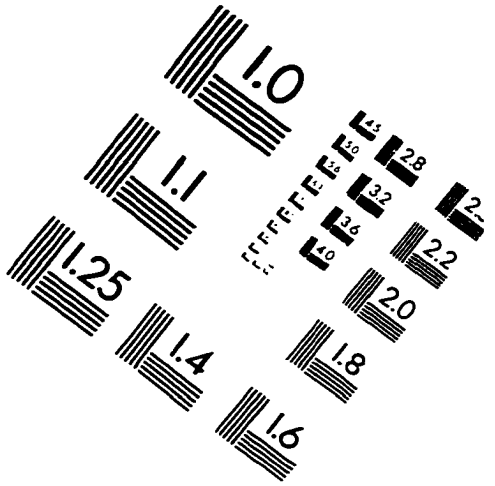
[NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley & Sons, Inc., fifth edition, 1991.

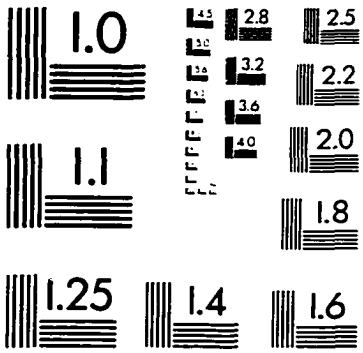
[Wei48] A. Weil. On some exponential sums. *Proc. Nat. Acad. of Sciences*, 34:204–207, 1948.

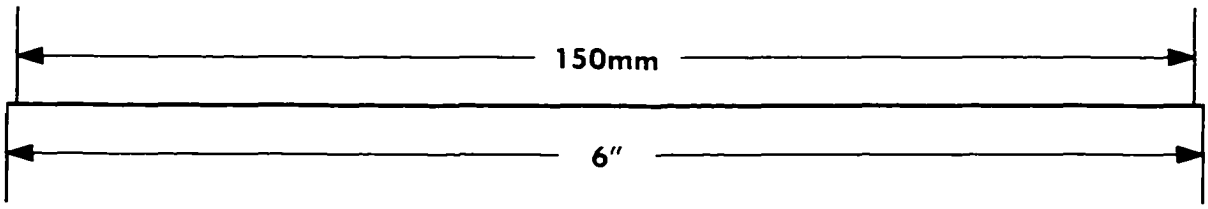
Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

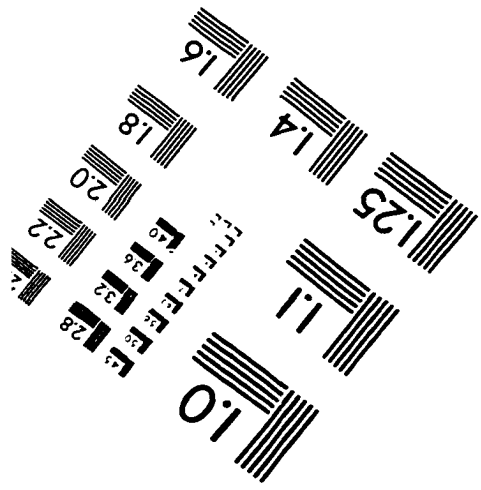
IMAGE EVALUATION
TEST TARGET (QA-3)

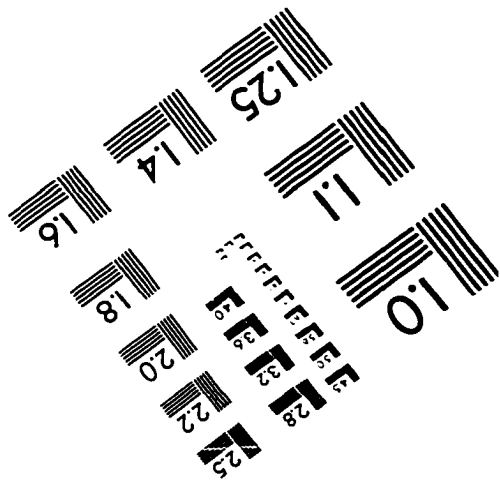












APPLIED IMAGE, Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989

© 1993, Applied Image, Inc., All Rights Reserved

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.