2-2015

Explicit Solutions of Imaginary Quadratic Norm Equations

Sandra Sze
Graduate Center, City University of New York

Explicit Solutions of Imaginary Quadratic Norm Equations

by

Sandra Sze

A dissertation submitted to the Graduate Faculty in Mathematics in partial fulfillment of the requirements for the degree of Doctor of Philosophy, The City University of New York.

2015

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirements for the degree of Doctor of Philosophy.

Victor Kolyvagin

_____ _____

Date Chair of Examining Committee

Linda Keen

_____ _____

Date Executive Officer

Victor Kolyvagin

_____

Alexander Gamburd

_____

Kenneth Kramer

_____

_____

Supervisory Committee

THE CITY UNIVERSITY OF NEW YORK

Abstract

Explicit Solutions of Imaginary Quadratic Norm Equations

by

Sandra Sze

Advisor: Victor Kolyvagin

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic extension of $\mathbb{Q}$. Let h be the class number and D be the discriminant of the field K. Assume p is a prime such that $\left(\frac{D}{p}\right) = 1$. Then p splits in K. The elements of the ring of integers $\mathcal{O}_K$ are of the form $x + \sqrt{-d}y$ if $d \equiv 1, 2 \pmod 4$ and $x + \frac{1+\sqrt{-d}}{2}y$ if $d \equiv 3 \pmod 4$, where x and $y \in \mathbb{Z}$. The norm $N_{K/\mathbb{Q}}(x + \sqrt{-d}y) = x^2 + dy^2$ and $N_{K/\mathbb{Q}}\left(x + \frac{1+\sqrt{-d}}{2}y\right) = \frac{(2x+y)^2}{4} + \frac{dy^2}{4}$. In this thesis, we find the elements of norm p^h explicitly. We also prove certain congruences for solutions of norm equations.

Acknowledgements

I would like to first thank my advisor Victor Kolyvagin for coming up with the problem for this thesis, for his patience with me as I worked on it and for the many ideas he had in helping me solve this problem. I would also like to thank the NSF for their support of me through the RTG grant, as well as the National Physical Science Consortium for funding me during my first year at CUNY Graduate Center.

I thank the committee members Kenneth Kramer and Alexander Gamburd for taking the time to read my paper and providing feedback.

I am grateful for other professors who believed in my ability and helped me to learn mathematics: Lucien Szpiro, Jozef Dodziuk, Burton Randol, Raymond Hoobler, Delaram Kahrobaei, Carlos Moreno, Robert Thompson, the late Gilbert Baumslag, Roni Gouraige, Ravi Kulkarni, Wallace Goldberg, Russell Miller.

There are many other mathematicians who have helped me throughout the years. They were willing to talk math with me and helped me to become a better student and mathematician. Please forgive me if I forgot to add you to the list: Robert Suzzi-Valli, Ha Lam, Yunchun Hu, Viveka Erlandsson, Maggie Habeeb, Rebecca Steiner, Shlomo Ben-Har,

Joey Hirsh, Phillip Williams, Nikita Miasnikov, Andrew Stout, Brian Stout, Lloyd West, Liang Zhao, Jorge Florez, Joe Kramer-Miller, John Basias, Ben Hutz, Adam Towsley, Blanca Marmolejo, Iryna Pavlyuk. I will always remember and cherish the hours we spent in the library, in empty classrooms, at Queens College, at different cafes, in the 8th floor cafeteria, working on homework, studying for the qualifiers and reviewing material our professors taught us.

I would like to thank my family and friends at Promise International Fellowship and at Resurrection Williamsburg. There are so many people at both congregations I would like to thank, so I'll only name pastors Timothy Harris and David Stancil as well as their wives Kim Harris and Mia Stancil. Thank you to all my friends who prayed with and for me and gave me encouragement during my years as a graduate student.

Other friends I would like to thank are Monica Chung, Kaisa Ercillo, Khadijah Rentas, Meiling Wang, Stuart Fontek, Joebrielle Basiao, Justin Bernstein, Michael Byrd, Sean Bryd, Ann Chow, Patrick Donnelly.

I would like to thank my family for their support of me as I pursued my career: my parents Jerry Sze and Huang Huang Li, my sisters Cindy and Tiffeny, my brother Allen, my thirteen cousins and my many aunts and uncles and my god sister Maria Mo. I would also like to thank my in-laws, especially Robert, Janet and Ted Williams, Rita Williams and Pam Jacobstein. Lastly, I would like to thank my husband Phillip Williams, mentioned above, who is one of my biggest supporter and an excellent mathematician, for his love,

patience, guidance, and our shared love for yummy food and love for Jesus.

Contents

Chapter 1

Introduction

Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic extension of $\mathbb{Q}$. Let h be the class number and D be the discriminant of the field K. (See Proposition 3.10 in section 3.3 for explicit formula for h.) Assume p is a prime such that $\left(\frac{D}{p}\right) = 1$. Then p splits in K. The elements of the ring of integers $\mathcal{O}_K$ are of the form $x + \sqrt{-d}y$ if $d \equiv 1, 2 \pmod 4$ and $x + \frac{1+\sqrt{-d}}{2}y$ if $d \equiv 3 \pmod 4$, where x and $y \in \mathbb{Z}$. The norm $N_{K/\mathbb{Q}}(x + \sqrt{-d}y) = x^2 + dy^2$ and $N_{K/\mathbb{Q}}\left(x + \frac{1+\sqrt{-d}}{2}y\right) = \frac{(2x+y)^2}{4} + \frac{dy^2}{4}$. In this thesis, we find the elements of norm p^h explicitly. That is, we find the general integer solutions (x, y), $p \nmid y$, to the equations

$$x^2 + dy^2 = p^h$$
$$\frac{(2x+y)^2}{4} + \frac{dy^2}{4} = p^h$$

for any imaginary quadratic field K and prime p such that p splits in K.

We proceed as follows. By a theorem of Kronecker-Weber, K is contained in a cyclo-

tomic field $L = \mathbb{Q}(\zeta_m)$. We can choose m to be $|D|$ if $d \neq 3$, $m = 6$ if $d = 3$.

We can find an element $Z \in \mathscr{O}_K$ such that the ideal $(Z) = \delta_1^h$, where $(p) = \delta_1\delta_2$ in K.

Let $\mathbb{F}_q$ be the residue field of a prime $\wp$ lying above δ_1 in L and ω a Teichmüller character of $\mathbb{F}_q$ for a prime $\mathfrak{p}$ lying above $\wp$ in $\mathbb{Q}(\zeta_{q-1})$. Let $\tau_p(\chi) = -\sum_{a\in\mathbb{F}_q} \chi(a)\zeta_p^{\mathrm{Tr}\,(a)}$ be the Gauss sum associated to a character $\chi : \mathbb{F}_q^\times \to \mu_{q-1}$, $\chi(0) = 0$.

Let $\chi = \omega^{\frac{q-1}{m}}$. Then Z is a ratio W/V, where W is a product of $\tau_p(\chi^{b_i})$, $b_i \in \mathbb{Z}$ and V is a power of p ($d \neq 1,2,3$) or a single Gauss sum ($d = 1,2,3$). We use Stickelberger relations, which give the prime decomposition of Gauss Sums, to find Z.

Let $x, y \in \mathbb{Z}$ such that $x + \sqrt{-d}y = Z$ if $d \equiv 1,2 \pmod 4$, $x + \dfrac{1+\sqrt{-d}}{2}y = Z$ if $d \equiv 3 \pmod 4$. We use the Gross-Koblitz formula, which allows us to write Gauss Sums in terms of $p-$adic Gamma functions, to express the conjugate $\overline{Z}$ of Z as a product of values of $p-$adic Gamma functions up to a sign. This implies an explicit congruence for x or $2x+y \pmod{p^h}$. Taking into account an estimate of the absolute value of x or $2x+y$ (see Proposition 3.6), this allows us to find x or $2x+y$ explicitly. We note that for the cases $d = 1,2,3$, one can use the classical Stickelberger congruences instead of the Gross-Koblitz formula. These cases were motivation for our study in the general case.

Let us describe our results. Let N be a natural number, t a rational $N-$integral number, then $\langle t\rangle_N$ denotes the integer such that $\langle t\rangle_N \equiv t \pmod N$ and $-\dfrac{N}{2} < \langle t\rangle_N \leq \dfrac{N}{2}$. We note that $h = 1$ when $d = 1,3,2$.

Let us first consider the case $d = 1$. If $p \equiv 1 \pmod 4$, then there exist, and are deter-

mined up to a sign and transposition, $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = p$. Let $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ be a binomial coefficient. Let $\langle \quad \rangle = \langle \quad \rangle_p$.

We prove

Theorem 1.1. *For a prime* $p \equiv 1 \pmod 4$

$$\left\langle \frac{1}{2}\binom{\frac{3p-3}{4}}{\frac{p-1}{4}} \right\rangle^2 + \left\langle \frac{1}{2}\frac{(\frac{3p-3}{p})!}{(\frac{p-1}{4})!} \right\rangle^2 = p. \tag{1.1}$$

This equality with $\langle \quad \rangle = \langle \quad \rangle_n$ *characterizes primes equivalent to 1 modulo 4 among the naturals, which are not squares and are equivalent to 1 modulo 4.*

Corollary 1.2. *Let* p *be a prime such that* $p \equiv 1 \pmod 4$ *and* $p = n^2 + m^2$. *Then*

$$\binom{\frac{3p-3}{4}}{\frac{p-1}{4}} \pmod p \in \{\pm 2n, \pm 2m\} \pmod p.$$

Let $d = 3$. If $p \equiv 1 \pmod 3$ and $n^2 + nm + m^2 = p$, then the solutions of $x^2 + xy + y^2 = p$ are

$$\pm(n,m), \pm(-n, n+m), \pm(n+m, -n), \pm(n+m, -m), \pm(-n, n+m), \pm(m,n).$$

Therefore, the possible values for $2x + y$ are

$$\pm(2n+m), \pm(n-m), \pm(n+2m).$$

We prove

Theorem 1.3. *Let* $p \equiv 1 \pmod 3$, $p \neq 7$, $\alpha = \binom{\frac{3p-3}{6}}{\frac{p-1}{6}}$. *Then*

$$\left(\langle\alpha\rangle, \sqrt{\frac{4p - \langle\alpha\rangle^2}{3}}\right)$$

is a solution in integers of the equation $x^2 + 3y^2 = 4p$.

Corollary 1.4. *Let* p *be a prime such that* $p \equiv 1 \pmod 3$ *and* $p = n^2 + nm + m^2$. *Then*

$$\binom{\frac{3p-3}{6}}{\frac{p-1}{6}} \pmod p \in \{\pm(2n+m), \pm(n-m), \pm(n+2m)\} \pmod p$$

We also prove

Theorem 1.5. *Let* $p \equiv 1 \pmod 8$ *and* $\alpha = \frac{1}{2}\binom{\frac{p-1}{2}}{\frac{p-1}{8}}$ *or* $p \equiv 3 \pmod 8$ *and* $\alpha = \frac{1}{2}\binom{\frac{p-1}{2}}{\frac{p-3}{8}}$. *Then*

$$\left(\langle\alpha\rangle, \sqrt{\frac{p - \langle\alpha\rangle^2}{2}}\right)$$

is a solution in integers of the equation $x^2 + 2y^2 = p$.

Corollary 1.6. *Suppose* $p \equiv 1, 3 \pmod 8$ *and* $p = n^2 + 2m^2$. *Then*

$$\binom{\frac{p-1}{2}}{\frac{p-1}{8}} \equiv \pm 2n \pmod p, \quad \text{if } p \equiv 1 \pmod 8$$
$$\binom{\frac{p-1}{2}}{\frac{p-3}{8}} \equiv \pm 2n \pmod p, \quad \text{if } p \equiv 3 \pmod 8$$

In fact, we first proved the congruences in the corollaries, which when combined with Proposition 3.6, imply Theorems 1.1, 1.3 and 1.5.

Theorems 1.1, 1.3 and 1.5 will be proved in section 2.2 (Theorems 2.9, 2.10, 2.11), where we demonstrate our results and techniques for examples $d = 1,3,2$.

For the case $d \neq 1,2,3$ we prove the following. Let p be a prime such that p splits in K, let $m = |D|$,

$$\beta = \prod_{\substack{1 \leq a < m \\ \chi_d(a) = 1}} \Gamma_p\left(\frac{a}{m}\right),$$

where $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^{\times}$ is the $p-$adic Gamma function, $\chi_d : (\mathbb{Z}/m\mathbb{Z})^{\times} \to \{\pm 1\}$ is the quadratic character associated to K (see Proposition 3.10). For an $N-$integral t, let $[t]_N$ be the integer in the interval $[0,N)$ congruent to $t \pmod N$.

Let $c = c(d,p)$ be a natural number defined in Proposition 3.7. Note that if $k = k(h) = \frac{h}{2} + 1$ if h is even, $k = \frac{h+1}{2}$ if h is odd, then $c = k = h$ if $h \leq 2$, $c = k$ or $k+1$ or (if $p = 2$) $k+2$ if $h > 2$, $c = k$ if $d \equiv 1,2 \pmod 4$; $c = k$ if $d \equiv 3 \pmod 4$, d is not a prime, $p \geq 5$; $c = k$ if $d \equiv 3 \pmod 4$ is a prime and $p \geq 17$.

Let $c \leq i \leq h$, $i \neq 2$ if $p = 2$, $\langle \quad \rangle = \langle \quad \rangle_{p^i}$, $[\quad] = [\quad]_{p^i}$. Let $T = \left[\frac{1}{m}\right]$,

$$\alpha = \prod_{\substack{1 \leq a < m \\ \chi_d(a) = 1}} (-1)^{[aT]} \prod_{\substack{1 \leq j < [aT] \\ (j,p) = 1}} j$$

We prove in section 3.5,

Theorem 1.7. *Let $d \neq 1,2,3$, p be a prime that splits in K, $p \neq 2$ if $d = 15$, $p \neq 5$ if $d = 11$.*

Then for $d \equiv 1,2 \pmod 4$,

$$x = \left\langle \frac{1}{2}\alpha \right\rangle = \left\langle \frac{1}{2}\beta \right\rangle,$$
$$y = \pm\sqrt{\frac{p^h - x^2}{d}}$$

is a solution in $\mathbb{Z}$, $p \nmid y$, *of the equation* $x^2 + dy^2 = p^h$.

For $d \equiv 3 \pmod 4$, x *and* y *defined by*

$$2x + y = \langle \alpha \rangle = \langle \beta \rangle,$$
$$y = \pm\sqrt{\frac{4p^h - (2x+y)^2}{d}}$$

is a solution in $\mathbb{Z}$, $p \nmid y$, *of the equation* $(2x+y)^2 + dy^2 = 4p^h$.

Corollary 1.8. *If* $p^h = n^2 + ds^2$ *or* $p^h = \left(n + \frac{s}{2}\right)^2 + d\frac{s^2}{4}$, *with* $n, s \in \mathbb{Z}$, $p \nmid s$, *when* $d \equiv 1,2 \pmod 4$ *or* $d \equiv 3 \pmod 4$, *respectively, then*

$$\alpha \equiv \beta \equiv \pm 2n, \text{ or } \pm(2n+s) \pmod{p^i},$$

respectively.

Theorems 1.1, 1.3, 1.5 and 1.7 provide us with explicitly determined solutions of norm equations. They also imply the corresponding congruences modulo p^h. Theorems 1.1, 1.3, 1.5, 1.7 and their corollaries are the main results of this thesis.

We note that one can also express solutions x, $x + \frac{1}{2}y$ (and then find y) of the norm equations by directly applying the normalized trace to the element Z or its image in $\mathbb{F}_q$

(see section 3.6 for the corresponding formulas).

Let us outline this thesis. In section 2.1, we describe the Stickelberger ideal and give the classical result about Gauss sums. Special cases $d = 1, 2, 3$ are computed in section 2.2. In section 3.1, we give the Gross-Koblitz formula and use it to give the representation of Gauss sums in section 3.4. Section 3.2 contains estimates of solutions of norm equations. We introduce the element Z and consider the cases $d = 1, 2, 3$ in sections 3.4 and 3.5. In section 3.7, we demonstrate examples of computations using our formulas. In chapter 4, we find the height of the Stickelberger ideal.

Chapter 2

Preliminaries and Special Cases

2.1 The Gauss Sums and the Stickelberger Theorem

Let ζ_m denote a primitive m^{th} of unity and let $M/\mathbb{Q}$ be a finite abelian extension. By a theorem of Kronecker-Weber, $M \subset \mathbb{Q}(\zeta_m)$ for some m. We will assume that m is minimal. Let $G = \text{Gal}\,(M/\mathbb{Q})$, a quotient of $G_m = \text{Gal}\,(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \left(\mathbb{Z}/m\mathbb{Z}\right)^{\times}$.

For $(a,m) = 1$, let σ_a denote the element $\zeta_m \mapsto \zeta_m^a$ of G_m as well as its restriction to M.

Definition 2.1. *The* Stickelberger element *in the group-ring $\mathbb{Q}[G]$ is defined to be*

$$\theta = \theta(M) = \sum_{\substack{1 \le a < m \\ (a,m) = 1}} \frac{a}{m}\sigma_a^{-1}.$$

Then $I = I(M) = \mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$ is an ideal of $\mathbb{Z}[G]$ consisting of $\mathbb{Z}[G]$ multiples of θ with coefficients in $\mathbb{Z}$. This ideal is called the Stickelberger ideal.

Lemma 2.2. *If $M = \mathbb{Q}(\zeta_m)$ then $I = I'\theta$, where I' is the ideal of $\mathbb{Z}[G]$ generated by all elements of the form $c - \sigma_c$ for $(c,m) = 1$.*

Proof. See [7]. □

Definition 2.3. *We define the action of* $\mathbb{Z}[G]$ *on ideals by: if* $x = \sum x_\sigma \sigma \in \mathbb{Z}[G]$*, then x acts on ideals A of M by*

$$A^x = \prod (A^\sigma)^{x_\sigma}.$$

We now give some definitions and properties of Gauss and Jacobi Sums.

Let p be an odd prime and $q = p^f$. Let ζ_p be a fixed primitive $p-$th root of unity. The Galois group Gal $(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic, generated by the Frobenius automorphism $\sigma_p : x \mapsto x^p$. Let $\lambda : \mathbb{F}_q \to \mathbb{C}^\times$ be the additive character, defined by $\lambda(x) = \zeta_p^{\mathrm{Tr}\,(x)}$, where Tr $(x) = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = x + x^p + \cdots + x^{p^{f-1}}$ is the trace map. Let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a multiplicative character. We extend χ to $\mathbb{F}_q$ by defining $\chi(0) = 0$, including the trivial character χ_0.

Definition 2.4. *The* Gauss sum corresponding to χ *is*

$$\tau_p(\chi) = -\sum_{a \in \mathbb{F}_q} \chi(a)\lambda(a) = -\sum_{a \in \mathbb{F}_q} \chi(a)\zeta_p^{Tr\,(a)}.$$

The Jacobi sum corresponding to χ_1 and χ_2 *is*

$$J(\chi_1, \chi_2) = -\sum_{a \in \mathbb{F}_q} \chi_1(a)\chi_2(1-a).$$

It can be shown that the Gauss sum and Jacobi sum satisfy the following properties:

1. $\tau_p(\chi_0) = 1$ and $J(\chi_0, \chi_0) = 2 - q$.

2. $\tau_p(\overline{\chi}) = \chi(-1)\overline{\tau_p(\chi)}$.

3. If $\chi \neq \chi_0$, $\tau_p(\chi)\tau_p(\overline{\chi}) = \chi(-1)q$. If $\chi_1\chi_2 \neq \chi_0$, then $J(\chi_1,\chi_2) = \dfrac{\tau_p(\chi_1)\tau_p(\chi_2)}{\tau_p(\chi_1\chi_2)}$. Thus, if χ_1, χ_2 are characters of order dividing m, then $J(\chi_1,\chi_2)$ is an algebraic integer in $\mathbb{Q}(\zeta_m)$.

4. If $\chi \neq \chi_0$, then $\tau_p(\chi)\overline{\tau_p(\chi)} = q$. If $\chi_1,\chi_2,\chi_1\chi_2 \neq \chi_0$, then $J(\chi_1,\chi_2)\overline{J(\chi_1,\chi_2)} = q$.

5. Let $\chi = \chi_1 \cdots \chi_n$. If $\psi = \chi|_{\mathbb{F}_p} = \psi_0$, the trivial character on $\mathbb{F}_p$, then

$$\prod_{i=1}^{n} \tau_p(\chi_i) = (-1)^n \sum_{\text{Tr }(a_1+\cdots+a_n)=0} \chi_1(a_1)\cdots\chi_n(a_n) + (-1)^{n-1} \sum_{\text{Tr }(a_1+\cdots+a_n)=1} \chi_1(a_1)\cdots\chi_n(a_n).$$

If $\psi \neq \psi_0$, then

$$\prod_{i=1}^{n} \tau_p(\chi_i) = (-1)^{n-1}\tau_p(\psi) \sum_{\text{Tr }(a_1+\cdots+a_n)=1} \chi_1(a_1)\cdots\chi_n(a_n).$$

(In these sums, $(a_1,\ldots,a_n)$ ranges over all $n-$tuples of elements in $\mathbb{F}_q^{\times}$.)

Proof. The proof of properties 1 through 4 can be found in [14]. We prove property 5. Let $\mathbf{a} = (a_1,\cdots,a_n)$, $z = z_{\mathbf{a}} = \text{Tr }(a_1+\cdots+a_n)$ and $c_i = \dfrac{a_i}{z}$ if $z \neq 0$. Then

$$\begin{aligned}
\prod_{i=1}^{n}\tau_p(\chi_i) &= (-1)^n \sum_{\mathbf{a}\in(\mathbb{F}_q^\times)^n} \chi_1(a_1)\cdots\chi_n(a_n)\zeta_p^z \\
&= (-1)^n \left[\sum_{\{\mathbf{a}\in(\mathbb{F}_q^\times)^n : z=0\}} \chi_1(a_1)\cdots\chi_n(a_n) + \sum_{\{\mathbf{a}\in(\mathbb{F}_q^\times)^n : z\neq 0\}} \chi_1(a_1)\cdots\chi_n(a_n)\zeta_p^z \right] \\
&= (-1)^n \left[\sum_{\{\mathbf{a}\in(\mathbb{F}_q^\times)^n : z=0\}} \chi_1(a_1)\cdots\chi_n(a_n) + \sum_{\{\mathbf{a}\in(\mathbb{F}_q^\times)^n : z\neq 0\}} \chi_1(zc_1)\cdots\chi_n(zc_n)\zeta_p^z \right] \\
&= (-1)^n \left[\sum_{\{\mathbf{a}\in(\mathbb{F}_q^\times)^n : z=0\}} \chi_1(a_1)\cdots\chi_n(a_n) + \sum_{\{\mathbf{a}\in(\mathbb{F}_q^\times)^n : z\neq 0\}} \chi_1(z)\cdots\chi_n(z)\chi_1(c_1)\cdots\chi_n(c_n)\zeta_p^z \right] \\
&= (-1)^n \sum_{z=0} \chi_1(a_1)\cdots\chi_n(a_n) + (-1)^{n-1} \left(-\sum_{z\in\mathbb{F}_p^\times} \chi(z)\zeta_p^z \right) \left(\sum_{\mathrm{Tr}\,(c_1+\cdots+c_n)=1} \chi_1(c_1)\cdots\chi_n(c_n) \right).
\end{aligned}$$

The last equality follows because the set

$$\{(zc_1,\ldots,zc_n) : z\in\mathbb{F}_p^\times, (c_1,\ldots,c_n)\in(\mathbb{F}_q^\times)^n, \mathrm{Tr}\,(c_1+\cdots+c_n)=1\}$$

is equal to the set $\{(a_1,\ldots,a_n)\in(\mathbb{F}_q^n)^\times : z\neq 0\}$. If $\psi=\psi_0$, then $\tau_p(\psi) = -\sum_{z\in\mathbb{F}_p^\times}\chi(z)\zeta_p^z = 1$, otherwise there exists a $b\in\mathbb{F}_p^\times$ such that $\psi(b)\neq 1$ so

$$\mathrm{Tr}(ba_1+\cdots ba_n) = b\mathrm{Tr}\,(a_1+\cdots+a_n)$$

and

$$\begin{aligned}
\sum_{\mathrm{Tr}\,(a_1+\cdots+a_n)=0} \chi_1(a_1)\cdots\chi_n(a_n) &= \sum_{b\mathrm{Tr}\,(a_1+\cdots+a_n)=0} \chi_1(ba_1)\cdots\chi_n(ba_n) \\
&= \psi(b) \sum_{\mathrm{Tr}\,(a_1+\cdots+a_n)=0} \chi_1(a_1)\cdots\chi_n(a_n),
\end{aligned}$$

which implies that $\sum_{z=0} \chi_1(a_1)\cdots\chi_n(a_n) = 0$. Note that property 3 can be proved the same way by using $z = a_1 + \cdots + a_n$ and $c_i = \frac{a_i}{z}$ if $z \neq 0$. □

The Teichmüller character is defined as follows.

Definition 2.5. *Let $q = p^f$. Let $\mathfrak{p}$ be one of the $\frac{\varphi(q-1)}{f}$ prime ideals of $\mathbb{Q}(\zeta_{q-1})$ lying above the prime number p. Identify $\mathbb{Z}[\zeta_{q-1}] \pmod{\mathfrak{p}}$ with $\mathbb{F}_q$. The equation $X^{q-1} - 1 = 0$ has distinct roots modulo $\mathfrak{p}$. Thus, there is a group isomorphism*

$$\omega : \mathbb{F}_q^\times \to \mu_{q-1},$$

such that $\omega(a) = a \pmod{\mathfrak{p}}$. ω is a character of $\mathbb{F}_q^\times$, called the Teichmüller character corresponding to $\mathfrak{p}$.

The Teichmüller character generates the character group. Thus, any character χ of $\mathbb{F}_q^\times$ can be written as an integral power of ω. Note that since ω has order $q-1$, the powers of ω can be expressed modulo $q-1$.

Now let $\mathfrak{P}$ be a prime above $\mathfrak{p}$ in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$. Let k be an integer and first assume that $0 \leq k < q-1$. We may represent k in its $p-$adic expansion by $k = k_0 + k_1 p + \cdots + k_{f-1}p^{f-1}$, where $0 \leq k_i < p$. Define $s(k)$ and $\gamma(k)$ by $s(k) = k_0 + k_1 + \cdots k_{f-1}$ and $\gamma(k) = k_0!k_1!\cdots k_{f-1}!$. For $k \geq q-1$, use $s(k')$ and $\gamma(k')$ where $k' \equiv k \pmod{q-1}$ and $0 \leq k' < q-1$. We have

Theorem 2.6 (Stickelberger). *(See [9]) For any integer k,*

$$\frac{\tau_p(\omega^{-k})}{(\zeta_p-1)^{s(k)}} \equiv \frac{1}{\gamma(k)} \pmod{\mathfrak{P}},$$

where ω is the Teichmüller character, which generates the character group.

2.2 Solutions of Norm Equations for $d = 1,2,3$

We begin by looking at three examples to motivate and introduce our study.

Example 2.1. *Let $K_1 = \mathbb{Q}(\zeta_4)$, where ζ_4 is a primitive fourth root of unity. Let p be a rational prime with $p \equiv 1 \pmod 4$. p splits in K_1. That is, $p = d_1 d_2$, where $N_{K_1/\mathbb{Q}}(d_i) = p$ for $i = 1,2$. There exists $x + \zeta_4 y \in \mathcal{O}_{K_1} = \mathbb{Z}[\zeta_4]$ such that $(x+\zeta_4 y) = d_i$ because the class number of K_1 is equal to 1. Therefore, $N_{K_1/\mathbb{Q}}((x+\zeta_4 y)) = (N_{K_1/\mathbb{Q}}(x+\zeta_4 y)) = x^2+y^2 = N_{K_1/\mathbb{Q}}(d_i) = p$. Hence, any $p \equiv 1 \pmod 4$ is representable as x^2+y^2, where $x, y \in \mathbb{Z}$.*

We can actually represent these elements of norm p in terms of Gauss sums. We recall that $\tau_p(\chi) = -\sum_{a \in \mathbb{Z}/p\mathbb{Z}} \chi(a)\zeta_p^a$ for the character χ. Let ω be the Teichmüller character corresponding to a fixed prime ideal in K_1 above p. Define $\chi_1 = \omega^{\frac{p-1}{4}}$, $\chi_2 = \omega^{\frac{p-1}{2}}$ and $\chi_1\chi_2 = \omega^{\frac{3p-3}{4}}$. From above, we see that $J(\chi_1,\chi_2)$ is an algebraic integer with $J(\chi_1,\chi_2)\overline{J(\chi_1,\chi_2)} = p$. Therefore, the element $x+\zeta_4 y = \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)}$ in $\mathbb{Z}[\zeta_4]$ has norm p. We may further characterize the x's and y's by using Theorem 2.6. Since $\frac{p-1}{4}$, $\frac{p-2}{4}$ and $\frac{3p-3}{4}$ are all less than $p-1$, they remain the same under $p-$adic expansion. We have,

using the property $\tau_p(\chi)\tau_p(\overline{\chi}) = \chi(-1)p$ and the Stickelberger Theorem (Theorem 2.6),

$$\begin{aligned}
x+\zeta_4 y &= \frac{\tau(\chi_1)\tau(\chi_2)}{\tau(\chi_1\chi_2)} = \frac{\tau(\omega^{\frac{p-1}{4}})\tau(\omega^{\frac{p-1}{2}})}{\tau(\omega^{\frac{3p-3}{4}})} = \frac{p\omega^{\frac{p-1}{4}}(-1)}{\tau(\omega^{-\frac{p-1}{4}})}\cdot\frac{p\omega^{\frac{p-1}{2}}(-1)}{\tau(\omega^{-\frac{p-1}{2}})}\cdot\frac{\tau(\omega^{-\frac{3p-3}{4}})}{p\omega^{\frac{3p-3}{4}}(-1)} \\
&= \frac{p\tau(\omega^{-\frac{3p-3}{4}})}{\tau(\omega^{-\frac{p-1}{4}})\tau(\omega^{-\frac{p-1}{2}})} \equiv \frac{p\frac{(\zeta_p-1)^{\frac{3p-3}{4}}}{(\frac{3p-3}{4})!}}{\frac{(\zeta_p-1)^{\frac{p-1}{4}}}{(\frac{p-1}{4})!}\cdot\frac{(\zeta_p-1)^{\frac{p-1}{2}}}{(\frac{p-1}{2})!}} \pmod{\mathfrak{P}} \\
&= \frac{p(\frac{p-1}{4})!(\frac{p-1}{2})!}{(\frac{3p-3}{4})!} \pmod{\mathfrak{P}}, \\
x+\zeta_4^{-1} y &= \frac{\overline{\tau(\chi_1)\tau(\chi_2)}}{\overline{\tau(\chi_1\chi_2)}} = \frac{\tau(\overline{\chi_1})}{\chi_1(-1)}\cdot\frac{\tau(\overline{\chi_2})}{\chi_2(-1)}\cdot\frac{\chi_1\chi_2(-1)}{\tau(\overline{\chi_1\chi_2})} = \frac{\tau(\overline{\chi_1})\tau(\overline{\chi_2})}{\tau(\overline{\chi_1\chi_2})} \\
&= \frac{\tau(\omega^{-\frac{p-1}{4}})\tau(\omega^{-\frac{p-1}{2}})}{\tau(\omega^{-\frac{3p-3}{4}})} \\
&\equiv \frac{(\frac{3p-3}{4})!}{(\frac{p-1}{4})!(\frac{p-1}{2})!} \pmod{\mathfrak{P}}.
\end{aligned}$$

Hence,

$$2x \equiv \frac{(\frac{3p-3}{4})!}{(\frac{p-1}{4})!(\frac{p-1}{2})!} \pmod{p},$$

or

$$\begin{aligned}
x &\equiv \frac{(\frac{3p-3}{4})!}{2\cdot(\frac{p-1}{4})!(\frac{p-1}{2})!} \pmod{p} \\
&= \frac{1}{2}\binom{\frac{3p-3}{4}}{\frac{p-1}{4}} \pmod{p},
\end{aligned}$$

where $\binom{n}{r} = \frac{n!}{r!(n-r)!}$ is a binomial coefficient.

We can also get the congruence for y by subtracting $x+\zeta_4^{-1}y$ *from* $x+\zeta_4 y$*:*

$$2\zeta_4 y \equiv \frac{(\frac{3p-3}{4})!}{(\frac{p-1}{4})!(\frac{p-1}{2})!} \pmod{\mathfrak{P}}.$$

Wilson's theorem states that $(p-1)! \equiv -1 \pmod{p}$*. That is,*

$$\begin{aligned}(p-1)! &= (p-1)(p-2)\cdots\left(p-\frac{p-1}{2}\right)\left(\frac{p-1}{2}\right)! \\ &= (-1)^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!^2 \pmod{p} \\ &\equiv -1 \pmod{p},\end{aligned}$$

or

$$\left(\frac{p-1}{2}\right)!^2 \equiv (-1)^{\frac{3-p}{2}} \pmod{p}.$$

Since $p \equiv 1 \pmod 4$*, we see that* $\left(\frac{p-1}{2}\right)!^2 \equiv -1 \pmod{p}$*. Thus, we can choose* $\mathfrak{P}$ *such that* $\zeta_4 \equiv \left(\frac{p-1}{2}\right)! \pmod{\mathfrak{P}}$*. Finally,*

$$y \equiv \frac{(\frac{3p-3}{4})!}{2(\frac{p-1}{4})!(\frac{p-1}{2})!^2} \equiv -\frac{(\frac{3p-3}{4})!}{2(\frac{p-1}{4})!} \pmod{p}$$

Now, $N_{K_1/\mathbb{Q}}((x+\zeta_4 y)) = x^2+y^2 = p$ *implies that* $x^2 < p$ *and* $y^2 < p$ *so that* $x < \sqrt{p} < \frac{p}{2}$ *and* $y < \sqrt{p} < \frac{p}{2}$*. Note that* $\sqrt{p} < \frac{p}{2}$ *is true for* $p \geq 5$*.*

Definition 2.7. *Let* $\alpha = \frac{a}{b} \in \mathbb{Q}$*,* $a,b \in \mathbb{Z}$*,* $(n,b) = 1$ *where n is odd. We define the notation* $\langle\alpha\rangle$ *to be the integer such that* $\langle\alpha\rangle \equiv \alpha \pmod{n}$ *and* $-\frac{n-1}{2} \leq \langle\alpha\rangle \leq \frac{n-1}{2}$*.*

Remark 1. *Note that* $\langle -\alpha \rangle = -\langle \alpha \rangle$. *To see this, we have* $\langle -\alpha \rangle \equiv -\alpha \pmod{n}$ *and* $-\langle \alpha \rangle \equiv -\alpha \pmod{n}$. *Also,* $\frac{n-1}{2} \geq -\langle \alpha \rangle \geq -\frac{n-1}{2}$. *Thus,* $\langle -\alpha \rangle = -\langle \alpha \rangle$.

Lemma 2.8. *Let* $n > 0$ *be a natural number such that* $n \equiv 1 \pmod{4}$. *Then n is prime if and only if*

$$\left(\frac{n-1}{2}\right)!^2 \equiv -1 \pmod{n}. \tag{2.1}$$

Furthermore, when n is composite, $n \neq 9$,

$$\left(\frac{n-1}{2}\right)! \equiv 0 \pmod{n}. \tag{2.2}$$

Proof. We showed above that if n is a prime such that $n \equiv 1 \pmod{4}$, then n satisfies (2.1). Suppose now that n is composite and $n \equiv 1 \pmod{4}$. Let p be a prime such that $p|n$. Then $p < \frac{n-1}{2}$ and $\frac{n}{p} < \frac{n-1}{2}$. If n is not the square of a prime, then p and $\frac{n}{p}$ are distinct and therefore $\left(\frac{n-1}{2}\right)! \equiv 0 \pmod{n}$. If $n = p^2$ for some prime p, as long as $p \neq 3$, then $2p < \frac{n-1}{2}$ so that $p^2 | \left(\frac{n-1}{2}\right)!$ and $\left(\frac{n-1}{2}\right)! \equiv 0 \pmod{n}$ in this case as well. If $n = 9$, then $\left(\frac{9-1}{2}\right)! = 24 \equiv 0 \pmod{3}$. □

Theorem 2.9. *Let* $n > 0$ *be a natural number, not a square, such that* $n \equiv 1 \pmod{4}$. *The pair*

$$\left(\left\langle \frac{1}{2} \binom{\frac{3n-3}{4}}{\frac{n-1}{4}} \right\rangle, \left\langle \frac{(\frac{3n-3}{4})!}{2(\frac{n-1}{4})!} \right\rangle \right) \tag{2.3}$$

is a solution to $x^2 + y^2 = n$ *if and only if n is prime.*

Proof. We saw above that if $p \equiv 1 \pmod 4$ and p is prime, then (2.3) is a solution to $x^2+y^2=p$.

Suppose now that n is a composite number, not a square and $n \equiv 1 \pmod 4$. Suppose further that

$$\left\langle \frac{1}{2}\binom{\frac{3n-3}{4}}{\frac{n-1}{4}} \right\rangle^2 + \left\langle \frac{(\frac{3n-3}{4})!}{2(\frac{n-1}{4})!} \right\rangle^2 = n. \tag{2.4}$$

It follows from congruence (2.2) and direct computations for $n=9$ that

$$\frac{(\frac{3n-3}{4})!}{2(\frac{n-1}{4})!} = \frac{1}{2}\binom{\frac{3n-3}{4}}{\frac{n-1}{4}} \left(\frac{n-1}{2}\right)! \equiv 0 \pmod n.$$

Equation (2.4) implies

$$\left\langle \frac{1}{2}\binom{\frac{3n-3}{4}}{\frac{n-1}{4}} \right\rangle^2 = n,$$

contradicting the condition that n is not a square. □

Example 2.2. *Now consider $K_2 = \mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ and let p be a rational prime with $p \equiv 1 \pmod 3$. p splits in K_2, so $p = d_1 d_2$ with $N_{K_2/\mathbb{Q}}(d_i) = p$ for $i = 1,2$. Again, there exists $x+\zeta_6 y \in \mathcal{O}_{K_2} = \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \mathbb{Z}[\zeta_6]$ such that $(x+\zeta_6 y) = d_1$. Therefore,*

$$N_{K_2/\mathbb{Q}}((x+\zeta_6 y)) = (x+\zeta_6 y)(x+\zeta_6^{-1} y) = x^2+xy+y^2 = \left(x+\frac{y}{2}\right)^2 + \frac{3y^2}{4} = p.$$

Similar to the case $K_1 = \mathbb{Q}(\zeta_4)$, we define $\chi_1 = \omega^{\frac{p-1}{6}}$, $\chi_2 = \omega^{\frac{p-1}{3}}$, hence $\chi_1\chi_2 = \omega^{\frac{3p-3}{6}}$

and we have

$$\begin{aligned} x+\zeta_6 y &= \frac{\tau_p(\chi_1)\tau_p(\chi_2)}{\tau_p(\chi_1\chi_2)} = \frac{\tau_p(\omega^{\frac{p-1}{6}})\tau(\omega^{\frac{p-1}{3}})}{\tau_p(\omega^{\frac{3p-3}{6}})} = \frac{p\tau_p(\omega^{-\frac{3p-3}{6}})}{\tau_p(\omega^{-\frac{p-1}{6}})\tau_p(\omega^{-\frac{p-1}{3}})} \\ &\equiv \frac{p(\frac{p-1}{6})!(\frac{p-1}{3})!}{(\frac{3p-3}{6})!} \pmod{\mathfrak{P}}, \\ x+\zeta_6^{-1} y &\equiv \frac{(\frac{3p-3}{6})!}{(\frac{p-1}{6})!(\frac{p-1}{3})!} \pmod{\mathfrak{P}}. \end{aligned}$$

Adding the two equations,

$$\begin{aligned} 2x+y &\equiv \frac{(\frac{3p-3}{6})!}{(\frac{p-1}{6})!(\frac{p-1}{3})!} \pmod{p} \\ &= \binom{\frac{3p-3}{6}}{\frac{p-1}{6}} \pmod{p} \end{aligned}$$

Subtracting the two equations,

$$\sqrt{-3}y \equiv \binom{\frac{3p-3}{6}}{\frac{p-1}{6}} \pmod{p}.$$

One may note that square roots modulo p can be computed. We will proceed without this fact. From $(2x+y)^2 = 4p-3y^2$*, we see that* $(2x+y)^2 < 4p$ *so that* $|2x+y| < 2\sqrt{p} < \frac{p}{2}$ *if* $4\sqrt{p} < p$*, or* $16 < p$*. That is, if* $p \geq 17$*, then* $|2x+y| < \frac{p}{2}$*. Let* $\alpha = \binom{\frac{3p-3}{6}}{\frac{p-1}{6}}$ *and* $\langle\alpha\rangle \equiv \alpha \pmod{p}$ *be the integer such that* $-\frac{p-1}{2} \leq \langle\alpha\rangle \leq \frac{p-1}{2}$*. In this case,* $2x+y = \langle\alpha\rangle$ *and* $y^2 = \frac{4p-(2x+y)^2}{3}$ *implies*

$$y = \pm\sqrt{\frac{4p-\langle\alpha\rangle^2}{3}},$$

and

$$x = \frac{\langle\alpha\rangle - y}{2}.$$

Theorem 2.10. *Let* $p \equiv 1 \pmod 3$, $p \geq 19$. *Let* $\alpha = \binom{\frac{3p-3}{6}}{\frac{p-1}{6}}$. *Then*

$$\left(\frac{\langle\alpha\rangle - \sqrt{\frac{4p-\langle\alpha\rangle^2}{3}}}{2}, \sqrt{\frac{4p-\langle\alpha\rangle^2}{3}}\right)$$

is a solution to $\left(x+\frac{y}{2}\right)^2 + \frac{3y^2}{4} = p$.

Remark 2. *Theorem 2.10 holds for* $p = 13$ *as well. This can be verified directly.*

Example 2.3. *Let* $K_3 = \mathbb{Q}(\sqrt{-2})$. *Then* $K_3 \subset L_3 = \mathbb{Q}(\zeta_8)$. *Let* p *be a rational prime. If* $p \equiv 1 \pmod 8$ *or* $p \equiv 3 \pmod 8$, *then* p *plits in* K_3. *Say* $p\mathcal{O}_{K_3} = d_1 d_2$. *Let* $x+\sqrt{-2}y$ *and* $x-\sqrt{-2}y \in \mathcal{O}_{K_3}$ *such that* $(x+\sqrt{-2}y) = d_1$ *and* $(x-\sqrt{-2}y) = d_2$. *We have* $N_{K_3/\mathbb{Q}}(x+\sqrt{-2}y) = x^2+2y^2 = N_{K_3/\mathbb{Q}}(d_1) = p$.

Gal $(L_3/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *and Gal* (L_3/K_3) *is a subgroup of order 2. Define* $\sigma_i \in$ *Gal* $(L_3/\mathbb{Q})$ *by* $\sigma_i(\zeta_8) = \zeta_8^i$. *Now,* $\sqrt{-2} = \zeta_8 + \zeta_8^3$ *so* $\sigma_1(\sqrt{-2}) = \sqrt{-2}$ *and* $\sigma_3(\sqrt{-2}) = \sqrt{-2}$. *Therefore, Gal* $(L_3/K_3) = \{\sigma_1, \sigma_3\}$.

If $p \equiv 1 \pmod 8$, *let* $\chi_1 = \omega^{\frac{p-1}{8}}$, $\chi_2 = \omega^{\frac{3p-3}{8}}$. *Note that* $J(\chi_1,\chi_2) = \frac{\tau_p(\omega^{\frac{p-1}{8}})\tau_p(\omega^{\frac{3p-3}{8}})}{\tau_p(\omega^{\frac{p-1}{2}})} \in K_3$ *since Gal* (L_3/K_3) *fixes this Jacobi sum. Recall that* $N_{K_3/\mathbb{Q}}(J(\chi_1,\chi_2)) = p$ *since* $\tau_p(\chi)\overline{\tau_p(\chi)} = p$. *As above,* $\frac{p-1}{8}$, $\frac{3p-3}{8}$ *and* $\frac{p-1}{2}$ *are less than* $p-1$, *so they remain the same under* $p-$*adic expansion. We have, using Stickel-*

berger's Theorem,

$$\begin{aligned} x+\sqrt{-2}y &= \frac{\tau_p(\omega^{\frac{p-1}{8}})\tau_p(\omega^{\frac{3p-3}{8}})}{\tau_p(\omega^{\frac{p-1}{2}})} = \frac{p\tau_p(\omega^{-\frac{p-1}{2}})}{\tau_p(\omega^{-\frac{p-1}{8}})\tau_p(\omega^{-\frac{3p-3}{8}})} \equiv \frac{p(\frac{p-1}{8})!(\frac{3p-3}{8})!}{(\frac{p-1}{2})!} \\ &\equiv 0 \pmod{\mathfrak{P}}, \\ x-\sqrt{-2}y &= \frac{\tau_p(\omega^{-\frac{p-1}{8}})\tau_p(\omega^{-\frac{3p-3}{8}})}{\tau_p(\omega^{-\frac{4p-4}{8}})} \equiv \frac{(\frac{p-1}{2})!}{(\frac{p-1}{8})!(\frac{3p-3}{8})!} \pmod{\mathfrak{P}} \end{aligned}$$

so that

$$x \equiv \frac{1}{2}\frac{(\frac{p-1}{2})!}{(\frac{p-1}{8})!(\frac{3p-3}{8})!} \pmod{p}.$$

Hence,

$$x = \left\langle \frac{1}{2}\binom{\frac{p-1}{2}}{\frac{p-1}{8}} \right\rangle$$

because $x^2+2y^2 = p$ *implies* $|x| < \frac{p}{2}$.

If $p \equiv 3 \pmod 8$, *then* $q = p^2 \equiv 1 \pmod 8$. *Let* $\chi = \omega^{\frac{p^2-1}{8}}$, *and* $\psi = \chi|_{\mathbb{F}_p}$. *Note that* $\psi(c) = c^{\frac{p-1}{2}(\frac{p+1}{4})} = c^{\frac{p-1}{2}} \pmod{\mathfrak{P}}$ *because* $\frac{p+1}{4}$ *is odd. Let*

$$Z = \frac{\tau_p(\chi)}{\tau_p(\psi)} = \sum_{\substack{c \in \mathbb{F}_q \\ Tr\,(c)=1}} \chi(c),$$

according to property 5 on page 10. It is clear that Z is invariant under $\sigma_p = \sigma_3$, *so* $Z \in \mathcal{O}_{K_3}$ *and* $N_{K_3/\mathbb{Q}}(Z) = \frac{q}{p} = p$. *Therefore,* $x+\sqrt{-2}y = Z$ *works in this case.*

We have

$$\begin{aligned}
\frac{p^2-1}{8} &= \frac{3p-1}{8} + \frac{p-3}{8}p, \\
x+\sqrt{-2}y &= \frac{p\tau_p(\psi^{-1})}{\tau_p(\chi^{-1})} \equiv 0 \pmod{\mathfrak{P}}, \\
x-\sqrt{-2}y &= \frac{\tau_p(\chi^{-1})}{\tau_p(\psi^{-1})} \equiv \frac{(\frac{p-1}{2})!}{(\frac{p-3}{8})!(\frac{3p-1}{8})!} = \binom{\frac{p-1}{2}}{\frac{p-3}{8}} \pmod{\mathfrak{P}}
\end{aligned}$$

because $\dfrac{\tau_p(\chi^{-1})}{(\zeta_p-1)^{\frac{p-1}{2}}} \equiv \dfrac{1}{(\frac{3p-1}{8})!(\frac{p-3}{8})!} \pmod{\mathfrak{P}}$ *and* $\dfrac{\tau_p(\psi^{-1})}{(\zeta_p-1)^{\frac{p-1}{2}}} \equiv \dfrac{1}{(\frac{p-1}{2})!} \pmod{\mathfrak{P}}$ *by Stickelberger's Theorem (Theorem 2.6). Thus,*

$$x \equiv \frac{1}{2}\binom{\frac{p-1}{2}}{\frac{p-3}{8}} \pmod{p}$$

and

$$x = \left\langle \frac{1}{2}\binom{\frac{p-1}{2}}{\frac{p-3}{8}} \right\rangle$$

because $|x| < \dfrac{p}{2}$.

Theorem 2.11. *Let* $\alpha = \begin{cases} \frac{1}{2}\binom{\frac{p-1}{2}}{\frac{p-1}{8}} & \text{if } p \equiv 1 \pmod 8 \\ \frac{1}{2}\binom{\frac{p-1}{2}}{\frac{p-3}{8}} & \text{if } p \equiv 3 \pmod 8 \end{cases}$. *Then*

$$\left(\langle\alpha\rangle, \sqrt{\frac{p-\langle\alpha\rangle^2}{2}}\right)$$

is a solution to $x^2+2y^2=p$.

We wish to generalize these results to all imaginary quadratic extensions of $\mathbb{Q}$.

Chapter 3

The General Case

Throughout, unless stated otherwise, we will let $q = p^f$, where p is prime.

3.1 The Gross-Koblitz Formula

Before we get to the Gross-Koblitz theorem, we need to the following:

Definition 3.1. *The $p-$adic gamma function is* $\Gamma_p(k) = (-1)^k \prod_{j<k, p\nmid j} j$, *for* $k = 1, 2, 3, \ldots$.

(When $k = 1$, we define $\Gamma_p(1) = -1$.)

Lemma 3.2. *Let $s \in \mathbb{N}$ such that $s \equiv s_0 \pmod{p^n}$. Let $n \neq 2$ if $p = 2$. Then $\Gamma_p(s) \pmod{p^n} \equiv \Gamma_p(s_0)$.*

Proof. We will follow the proof in [8], page 90. Let s and s_0 be natural numbers, $s > s_0$. We will show that if $s \equiv s_0 \pmod{p^n}$, $n \neq 2$ if $p = 2$, then $\Gamma_p(s) \pmod{p^n} \equiv \Gamma_p(s_0)$. To see this, write $s = s_0 + kp^n$. We will prove this for $k = 1$ first. That is, assume $s = s_0 + p^n$.

$\Gamma_p(s) \pmod{p^n} \equiv \Gamma_p(s_0)$ is true if and only if

$$1 \equiv \frac{\Gamma_p(s)}{\Gamma_p(s_0)} = (-1)^{s-s_0} \prod_{\substack{s_0 \le j < s \\ p \nmid j}} j \pmod{p^n} = (-1)^p \prod_{\substack{s_0 \le j < s \\ p \nmid j}} j \pmod{p^n}.$$

Now since $s = s_0 + p^n$, this product runs through every congruence class in $\left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$ exactly once and we have

$$(-1)^p \prod_{\substack{s_0 \le j < s \\ p \nmid j}} j \pmod{p^n} \equiv (-1)^p \prod_{\substack{0 \le j < p^n \\ p \nmid j}} j \pmod{p^n}.$$

Therefore, to complete the case $k = 1$, we need

$$\prod_{\substack{0 \le j < p^n \\ p \nmid j}} j \equiv (-1)^p \pmod{p^n}.$$

In the product, we can pair a number with its inverse. That is, there exists $j^{-1} \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$ such that $jj^{-1} = 1$. Therefore, the product simplifies to

$$\prod_{\substack{0 \le j < p^n \\ p \nmid j}} j \equiv \prod_{\substack{1 \le j < p^n \\ j^2 \equiv 1 \pmod{p^n} \\ p \nmid j}} j.$$

Suppose $j^2 \equiv 1 \pmod{p^n}$. Then $j = pa \pm 1$, where a is even if $p = 2$, $n \ge 3$. Then $j^2 = 1 \pm 2pa + p^2a^2 \equiv 1 \pmod{p^n} \Leftrightarrow 2pa \equiv 0 \pmod{p^n}$. So $j = 1$ or $p^n - 1$ if p is odd;

$j = 1$ if $p = 2$ and $n = 1$; $j = 1, 2^n - 1, 2^{n-1} + 1$ or $2^{n-1} - 1$ if $p = 2, n \geq 3$. In all cases,

$$\prod_{\substack{1 \leq j < p^n \\ j^2 \equiv 1 \pmod{p^n} \\ p \not| j}} j \equiv (-1)^* \pmod{p^n}.$$

We have proven the congruence for $k = 1$. To show this is true for $s = s_0 + kp^n$, $k \neq 1$ we need

$$1 \equiv \frac{\Gamma_p(s)}{\Gamma_p(s_0)} = (-1)^{kp^n} \prod_{\substack{s_0 \leq j < s_0 + kp^n \\ p \not| j}} j \pmod{p^n}$$

This is obtained by multiplying together the following congruences:

$$1 \equiv \frac{\Gamma_p(s_0 + p^n)}{\Gamma_p(s_0)} = (-1)^{s_0 + p^n - s_0} \prod_{\substack{s_0 \leq j < s_0 + p^n \\ p \not| j}} j$$

$$1 \equiv \frac{\Gamma_p(s_0 + 2p^n)}{\Gamma_p(s_0 + p^n)} = (-1)^{s_0 + 2p^n - (s_0 + p^n)} \prod_{\substack{s_0 + p^n \leq j < s_0 + 2p^n \\ p \not| j}} j$$

$$\vdots$$

$$1 \equiv \frac{\Gamma_p(s_0 + kp^n)}{\Gamma_p(s_0 + (k-1)p^n)} = (-1)^{s_0 + kp^n - (s_0 + (k-1)p^n)} \prod_{\substack{s_0 + (k-1)p^n \leq j < s_0 + kp^n \\ p \not| j}} j.$$

□

Proposition 3.3. *Γ_p extends to a well-defined continuous function $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^\times$ defined*

by

$$\Gamma_p(a) = \lim_{t\to a, t\in\mathbb{N}} (-1)^t \prod_{j<t, p\nmid j} j,$$

where $\{t\}$ *is any sequence of natural numbers converging to* $a \in \mathbb{Z}_p$.

Proof. Take a sequence $\{t_i\}$ approaching a. Then the sequence $\{\Gamma_p(t_i)\}$ converges. Define $\Gamma_p(a) = \lim_{i\to\infty} (-1)^{t_i} \prod_{j<t_i, p\nmid j} j$.

To show that $\Gamma_p(a)$ is well-defined, suppose $\{s_i\}$ and $\{s_i'\}$ are two Cauchy sequences of natural numbers converging to a. Then $\{s_i\}$ and $\{s_i'\}$ are in the same equivalence class of Cauchy sequences, so $|s_i - s_i'|_p \to 0$ as $i \to \infty$. We need to show that this implies $|\Gamma_p(s_i) - \Gamma_p(s_i')|_p \to 0$ as $i \to \infty$. This is clear: as shown in Lemma 3.2, if $s_i \equiv s_i' \pmod{p^n}$, then $\Gamma_p(s_i) \equiv \Gamma_p(s_i') \pmod{p^n}$. □

Lemma 3.4. *Let* $s = s_0 + s_1 p + s_2 p^2 + \cdots \in \mathbb{Z}_p$ *such that* $s_i \in \mathbb{Z}$, $0 \le s_i < p$. *Let* $\{k_i\} = \{s_0, s_0 + s_1 p, s_0 + s_1 p + s_2 p^2, \ldots\}$ *for* $i = 0, 1, 2, \ldots$ *be the sequence of partial sums of s,* $k_{n-1} \equiv s \pmod{p^n}$ *for* $n = 1, 2, 3, \ldots$ *(*$n \neq 2$ *if* $p = 2$*). Then* $\Gamma_p(k_{n-1}) \equiv \Gamma_p(s) \pmod{p^n}$. *Furthermore, if* $s, s' \in \mathbb{Z}_p$ *and* $s \equiv s' \pmod{p^n}$, *then* $\Gamma_p(s) \equiv \Gamma_p(s') \pmod{p^n}$.

Proof. It is clear that $\{k_i\}$ converges to s and $\{\Gamma_p(k_i)\}$ converges to $\Gamma_p(s)$. Also, $\Gamma_p(k_i) \equiv \Gamma_p(k_{i+1}) \pmod{p^{i+1}}$ so $\Gamma_p(k_{n-1}) \equiv \Gamma_p(k_i) \pmod{p^n}$ for $i = n, n+1, \ldots$ Since $\Gamma_p(s) = \lim_{i\to\infty} \Gamma_p(k_i)$, this implies that $\Gamma_p(s) - \Gamma_p(k_i) \equiv 0 \pmod{p^n}$ for a large enough i. Therefore, $\Gamma_p(s) \equiv \Gamma_p(k_i) \pmod{p^n}$ so that $\Gamma_p(s) \equiv \Gamma_p(k_{n-1}) \pmod{p^n}$.

Now if $s, s' \in \mathbb{Z}_p$ and $s \equiv s' \pmod{p^n}$, then $k_{n-1} = k'_{n-1}$, $\Gamma_p(s) \equiv \Gamma_p(k_{n-1}) \pmod{p^n}$ and $\Gamma_p(s') \equiv \Gamma_p(k'_{n-1}) \pmod{p^n}$. Also, $\Gamma_p(k_{n-1}) = \Gamma_p(k'_{n-1})$ so $\Gamma_p(s) \equiv \Gamma_p(s') \pmod{p^n}$. □

It can be shown that Γ_p satisfies the following properties:

1. $\dfrac{\Gamma_p(s+1)}{\Gamma_p(s)} = \begin{cases} -s & \text{if } s \in \mathbb{Z}_p^\times \\ -1 & \text{if } s \in p\mathbb{Z}_p \end{cases}$.

2. Suppose p is odd. If $s \in \mathbb{Z}_p$, write $s = s_0 + ps_1$, where $s_0 \in \{1, 2, \ldots, p\}$ is the first digit in s unless $s \in p\mathbb{Z}_p$, $s_0 = p$. Then $\Gamma_p(s)\Gamma_p(1-s) = (-1)^{s_0}$.

3. If $p = 2$, then $\Gamma_p(s)\Gamma_p(1-s) = \begin{cases} -1 & \text{if } s \equiv 0, 1 \pmod 4 \\ 1 & \text{if } s \equiv 2, 3 \pmod 4 \end{cases}$.

See [8] for the proof.

We are now ready to state the Gross-Koblitz theorem:

Theorem 3.5 (Gross-Koblitz)**.** *(See [2]) Let $f \geq 1$ and $q = p^f$. Let $\pi \in \mathscr{K} = \mathbb{Q}_p(\zeta_p)$ be such that $\pi^{p-1} = -p$. Let $\mathscr{L} = \mathscr{K}(\zeta_{q-1})$ and ζ_π be the unique $p-$th root of unity congruent to $1 + \pi$ modulo $\mathfrak{p}^2$, where $\mathfrak{p}$ is the prime ideal above p in $\mathbb{Q}(\zeta_p)$. For $0 \leq a < q-1$, we have*

$$-\sum_{x \in \mathscr{L}, x^{q-1}=1} x^{-a} \zeta_\pi^{Tr_{\mathscr{L}/\mathscr{K}}(x)} = \pi^{S(a)} \prod_{0 \leq i < f} \Gamma_p\left(\frac{a^{(i)}}{q-1}\right)$$

where $S(a)$ is the sum of the digits of a in base p, and the integers $0 \leq a^{(i)} < q-1$ have $p-$adic expansions obtained by cyclic permutation from that of a.

Note that for $a \in \mathbb{Z}_p$, it makes sense to raise ζ_π to the a power, since ζ_π is a $p-$th root of unity.

Remark 3. *When $f = 1$, we have $\mathscr{K} = \mathscr{L}$, since $\mathbb{Q}_p$ contains the $(p-1)$th roots of unity.*

The Gaussian sum in Theorem 3.5 becomes

$$-\sum_{x \in \mathscr{K}, x^{p-1}=1} x^{-a}\zeta_\pi^x = -\sum_{x \in \mu_{p-1}} x^{-a}\zeta_\pi^x.$$

Now let ω be the Teichmüller character corresponding to $\mathfrak{p}$, defined by Definition 2.5 . Let $r_x \in \mathbb{F}_p^\times$ be such that $\omega(r_x) = x \in \mu_{p-1}$. We can then rewrite the sum as

$$\sum_{r_x \in \mathbb{F}_p^\times} \omega^{-a}(r_x)\zeta_\pi^{\omega(r_x)} = \sum_{r_x \in \mathbb{F}_p^\times} \omega^{-a}(r_x)\zeta_\pi^{r_x},$$

since $\omega(r_x) \equiv r_x \pmod{\mathfrak{p}}$. The Gross-Koblitz formula becomes

$$-\sum_{x \in \mathbb{F}_p} \omega^{-a}(x)\zeta_p^x = \pi^a \Gamma_p\left(\frac{a}{p-1}\right).$$

Remark 4. *The Gross-Koblitz formula for $f = 1$, p odd implies Stickelberger's Theorem (Theorem 2.6). To see this, we need to show $\Gamma_p\left(\frac{a}{p-1}\right) \equiv \frac{1}{a!} \pmod{p}$ for $0 \le a < p-1$. From the relations $\frac{1}{1-p} = 1 + p + p^2 + \ldots$ and $-a = (p-a)(1-p) + p(p-a-1)$, we*

see that $\dfrac{a}{p-1} = \dfrac{-a}{1-p} = p-a+(p-a-1)(p+p^2+p^3+\ldots)$. *We have*

$$\begin{aligned}\Gamma_p\left(\frac{a}{p-1}\right) = \Gamma_p\left(\frac{-a}{1-p}\right) &\equiv \Gamma_p(p-a) \pmod{p} \\ &= (-1)^{p-a} \prod_{\substack{j<p-a \\ p\nmid j}} j = (-1)^{p-a}(p-a-1)!,\end{aligned}$$

where the above follows from Lemma 3.4 by choosing $\{k_i\}$ *to be the sequence of partial sums of the* $p-$*adic expansion of* $\dfrac{a}{p-1}$. *From* $(p-1)! \equiv -1 \pmod{p}$,

$$(p-a-1)! \equiv \frac{-1}{(p-1)(p-2)\cdots(p-a)} \pmod{p} \equiv \frac{(-1)^{1-a}}{a!} \pmod{p}.$$

Finally, $\Gamma_p\left(\dfrac{a}{p-1}\right) \equiv (-1)^{p-a}\cdot\dfrac{(-1)^{1-a}}{a!} \pmod{p} = \dfrac{1}{a!} \pmod{p}$.

3.2 Estimates of Solutions of Norm Equations

Recall that the ring of integers for $\mathbb{Q}(\sqrt{-d})$ is $\mathbb{Z}\left[\dfrac{1+\sqrt{-d}}{2}\right]$ if $d \equiv 3 \pmod{4}$ and $\mathbb{Z}[\sqrt{-d}]$ if $d \equiv 1,2 \pmod{4}$. We have

$$\left(x+\frac{1+\sqrt{-d}}{2}y\right)\left(x+\frac{1-\sqrt{-d}}{2}y\right) = \frac{(2x+y)^2}{4}+\frac{dy^2}{4}$$

and

$$(x+\sqrt{-d}y)(x-\sqrt{-d}y) = x^2+dy^2.$$

In both cases, we want the right side of the equation to be p^h, with p splitting in $\mathbb{Q}(\sqrt{-d})$ and $y \not\equiv 0 \pmod{p}$. We estimate the values of x and y as follows.

Proposition 3.6. *Let p be a prime (including $p = 2$) that splits in $\mathbb{Q}(\sqrt{-d})$. Let x, $0 \neq y \in \mathbb{Z}$ be such that*

$$(2x+y)^2 + dy^2 = 4p^h, \quad \text{if } d \equiv 3 \pmod{4} \tag{3.1}$$

$$x^2 + dy^2 = p^h, \quad \text{if } d \equiv 1,2 \pmod{4}. \tag{3.2}$$

Let $b = 2x+y$ or $b = x$, respectively. Then, except the cases when $d = 3$, $p = 7$ or 13; $d = 11$, $p = 5$,

$$|b| \leq \frac{p^h}{2} \tag{3.3}$$

Proof. Let $a = p^h$. We first consider the case $d \equiv 1,2 \pmod{4}$. Suppose equation (3.2) holds. Then $b^2 = a - dy^2 \leq a - d$, so inequality (3.3) holds if $a - d \leq \frac{a^2}{4} \Leftrightarrow a^2 - 4a + 4d \geq 0$. This is true since $a^2 - 4a + 4d \geq a^2 - 4a + 4 = (a-2)^2 \geq 0$.

We now consider the case $d \equiv 3 \pmod{4}$. If equation (3.1) holds, then $b^2 = 4a - dy^2 \leq 4a - d$, so inequality (3.3) holds if $4a - d \leq \frac{a^2}{4} \Leftrightarrow a^2 - 16a + 4d \geq 0 \Leftrightarrow (a-8)^2 + 4d \geq 64 \Leftrightarrow 64 - 4d \leq 0$ or $d < 16$ and $a \geq 8 + \sqrt{64-4d}$ or $a \leq 8 - \sqrt{64-4d}$. So it remains only to examine the cases when $d = 3, 7, 11, 15$ and $8 - \sqrt{64-4d} < a < 8 + \sqrt{64-4d}$.

If $d = 3$ then $h = 1$, so the possible p's are such that $2 \leq p < 15$. For $d = 7$, $h = 1$ and the possible p's are $2 < p < 14$; for $d = 11$, $h = 1$ so $3 < p < 12$; for $d = 15$, $h = 2$ so

$6 < p^2 < 10 \Leftrightarrow p = 3$, but since 3 divides the discriminant, 3 ramifies in $\mathbb{Q}(\sqrt{-15})$. Let us consider each case.

If $d = 3$, p may be 7 or 13 because p must be congruent to 1 $\pmod 3$. For $p = 7$, the solution is $b = 5$, $y = 1$. For $p = 13$, the solution is $b = 7$, $y = 1$. Therefore, inequality (3.3) fails.

If $d = 7$, the condition $\left(\frac{-7}{p}\right) = 1$ leaves only $p = 11$. The only solutions of $b^2 + 7y^2 = 44$ are $(\pm 4, \pm 2)$, so inequality (3.3) holds.

If $d = 11$, the condition $\left(\frac{-11}{p}\right) = 1$ leaves only $p = 5$. The solutions of $b^2 + 11y^2 = 20$ are $(\pm 3, \pm 1)$, so inequality (3.3) fails. □

Suppose that x and y is a solution of equation (3.1) or (3.2). Suppose $d \equiv 3 \pmod 4$. Defining α to be $2x + y \pmod{p^h}$ and letting $\langle \alpha \rangle$ be defined by Definition 2.7 but with n replaced by p^h, if $p \neq 7, 13$ for $d = 3$ and $p \neq 5$ for $d = 11$, we get

$$y = \pm \sqrt{\frac{4p^h - \langle \alpha \rangle^2}{d}}$$

and

$$x = \frac{\langle \alpha \rangle - y}{2}.$$

When $d \equiv 1, 2 \pmod 4$, define $\alpha \equiv x \pmod{p^h}$ so that Proposition 3.6 implies that

$$x = \langle \alpha \rangle,$$

and

$$y = \pm\sqrt{\frac{p^h - \langle\alpha\rangle^2}{d}}.$$

Remark 5. *If (x_0, y_0) is a solution to the norm equation (3.1) or (3.2), then $(-x_0, -y_0)$ is also a solution to the norm equation. Thus, we may replace $\langle -\alpha\rangle$ with $\langle\alpha\rangle$ in our computations and the resulting x and y that we find are still solutions.*

Proposition 3.7. *Let $k = k(h) = \begin{cases} \frac{h}{2}+1 & \text{if } h \text{ is even} \\ \frac{h}{2}+\frac{1}{2} & \text{if } h \text{ is odd} \end{cases}$. Under the conditions of Proposition 3.6, for $d \neq 1, 2$ we have that*

$$|b| \leq \frac{p^c}{2},$$

where for $d \equiv 1, 2 \pmod 4$, $c = k$; for $d \equiv 3 \pmod 4$, $c = k$ if $h \leq 2$, also $c = k$ if d is not a prime, $p \geq 5$ or $p \leq 3$ and $d \geq p^h\left(\frac{16-p^2}{4}\right)$, also $c = k$ if d is a prime, $p \geq 17$ or $p \leq 13$ and $d \geq p^h\left(\frac{16-p}{4}\right)$. Otherwise, for $d \equiv 3 \pmod 4$, $c = k+1$, except the case when d is prime, $h \geq 5$, $p = 2$, $d < 2^{h+1}$ when $c = k+2$.

Proof. If $h \leq 2$, $k = h$, so the estimate with $c = k$ is the same as in Proposition 3.6.

Note that $2k = h+2$ if h is even and $2k = h+1$ if h is odd.

It is known ([1], Chapter 3, Section 8, Theorem 8) that h is even if and only if the number of distinct prime divisors of the discriminant D is bigger than 1. So if $d \equiv 1, 2$

$(\text{mod } 4)$, $d \neq 1,2$, then h is even, so

$$\frac{p^{2k}}{4} = \frac{p^h p^2}{4} \geq p^h \geq |b|^2$$

and the estimate with $c = k$ follows.

Now let $d \equiv 3 \pmod 4$. Recall that $4p^h - d \geq |b|^2$ in this case. If d is not a prime, then h is even, so

$$\frac{p^{2k}}{4} = \frac{p^h p^2}{4} \geq 4p^h - d$$

if $p \geq 5$ or $p \leq 3$ and $d \geq p^h \left(\frac{16 - p^2}{4} \right)$ and the estimate with $c = k$ follows. Also,

$$\frac{p^{2(k+1)}}{4} = \frac{p^h p^4}{4} \geq 4p^h$$

and the estimate with $c = k+1$ follows for remaining cases with $d \equiv 3 \pmod 4$, d not a prime.

If d is a prime, then h is odd, so

$$\frac{p^{2k}}{4} = \frac{p^h p}{4} \geq 4p^h - d$$

if $p \geq 17$ or $2 \leq p \leq 13$ and $d > p^h \left(\frac{16 - p}{4} \right)$ and the estimate with $c = k$ follows. Also,

$$\frac{p^{2(k+1)}}{4} = \frac{p^h p^3}{4} \geq 4p^h - d$$

if $p \geq 3$ or $p = 2$ and $d \geq 2^{h+1}$, so the estimate with $c = k+1$ holds.

If $p = 2$, d is a prime, $d < 2^{h+1}$, then the estimate with $c = k+2$ holds because

$$\frac{2^{2(k+2)}}{4} = \frac{2^h 2^5}{4} > 4(2^h).$$

Note also that if $h = 3$, then $k+1 = h$, so the estimate with $c = k+1$ follows from Proposition 3.6. □

3.3 The Class Number Formulas

The following statements will be used throughout the paper.

Since d is not necessarily prime, we need to modify the definition of the Legendre symbol $\left(\frac{a}{d}\right)$.

Definition 3.8. *Let $d = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ be an positive odd integer and let a be any integer. We define the Jacobi symbol to be*

$$\left(\frac{a}{d}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_n}\right)^{\alpha_n},$$

where $\left(\frac{a}{p_i}\right)$ is the Legendre symbol.

The Jacobi symbol has properties similar to that of the Legendre symbol. Like the Legendre symbol, if $\left(\frac{a}{d}\right) = -1$, then a is a quadratic non residue modulo d. However, no conclusion can be made if $\left(\frac{a}{d}\right) = 1$.

It can be shown as a consequence of a lemma of Gauss that

$$\left(\frac{2}{d}\right) = \begin{cases} 1 & \text{if } d \equiv 1,7 \pmod 8 \\ -1 & \text{if } d \equiv 3,5 \pmod 8 \end{cases}. \tag{3.4}$$

(See page 53 of [5], for example.)

From the Kronecker-Weber theorem, we have

Proposition 3.9. *Let d be a square-free positive integer. If $d \equiv 3 \pmod 4$, set $m = d$. Otherwise, set $m = 4d$. Then $\mathbb{Q}(\sqrt{-d}) \subseteq \mathbb{Q}(\zeta_{m'})$ if and only if m' is a multiple of m. Thus, m is the smallest positive integer m' for which the inclusion holds.*

The proof of this statement can be found in [6].

Proposition 3.10. *For an imaginary quadratic field with discriminant $D < -4$, we have the formula*

$$h = -\frac{1}{|D|} \sum_{\substack{(a,D)=1 \\ 0<a<|D|}} \chi_d(a)a,$$

where χ_d is the character of $\mathbb{Q}(\sqrt{-d})$ defined by

$$\chi_d(a) = \begin{cases} \left(\frac{a}{d}\right) & \text{if } d \equiv 3 \pmod 4 \\ (-1)^{\frac{a-1}{2}} \left(\frac{a}{d}\right) & \text{if } d \equiv 1 \pmod 4 \\ (-1)^{\frac{a^2-1}{8} + \frac{a-1}{2} \cdot \frac{-d'-1}{2}} \left(\frac{a}{d'}\right) & \text{if } d = 2d' \end{cases}$$

for $(a,D)=1$ and $\chi_d(a)=0$ for $(a,D)\neq 1$. Note that

$$D=\begin{cases} -d & \text{if } d\equiv 3 \pmod 4 \\ -4d & \text{if } d\equiv 1,2 \pmod 4 \end{cases}.$$

(see [1], page 344).

The following from page 346 of [1] will be used:

Theorem 3.11. *For an imaginary quadratic field with discriminant $D<-4$ and character χ_d we have*

$$h=\frac{1}{2-\chi_d(2)}\sum_{\substack{0<a<\frac{|D|}{2}\\(a,D)=1}}\chi_d(a).$$

Note that when D is even, $\chi_d(2)=0$.

In particular, when the field is $\mathbb{Q}(\sqrt{-\ell})$, where ℓ is prime, we have

Theorem 3.12. *Let ℓ be a prime number, $\ell\equiv 3 \pmod 4$, $\ell\neq 3$. Let V and N denote the number of quadratic residues and nonresidues in the interval $\left(0,\frac{\ell}{2}\right)$. The number of divisor classes of the field $\mathbb{Q}(\sqrt{-\ell})$ is odd and is given by*

$$\begin{array}{ll} h=V-N & \text{for } \ell\equiv 7 \pmod 8 \\ h=\frac{1}{3}(V-N) & \text{for } \ell\equiv 3 \pmod 8 \end{array}$$

3.4 Representing an Element in $\mathbb{Q}(\sqrt{-d})$ with Norm p^h as a Product of Gauss Sums

We now give the factorization of the Gauss and Jacobi sums. Let $L=\mathbb{Q}(\zeta_m)$ and m be as in section 2.1. Let $\wp_1$ be a prime of $\mathbb{Q}(\zeta_m)$ lying above p. Let ω be the Teichmüller

character from $\mathbb{F}_q^\times$ to μ_{q-1} corresponding to a prime of $\mathbb{Q}(\zeta_{q-1})$ lying above $\wp_1$, and let $\chi = \omega^c$, where $c = \dfrac{q-1}{m}$. We have

Proposition 3.13 (Stickelberger's Relations)**.** *Let $\wp_1$ be a prime of $\mathbb{Q}(\zeta_m)$ lying above p. Then*

1. $(\tau_p(\chi^{-1})^m) = \wp_1^{m\theta} = \wp_1^{\sum_{1\le a<m,(a,m)=1} a\sigma_a^{-1}} = \prod_{1\le a<m,(a,m)=1} (\wp_1^{\sigma_a^{-1}})^a$,

   as ideals in $\mathbb{Q}(\zeta_m)$.

2. *Let j,k be integers such that $j,k,j+k \not\equiv 0 \pmod m$ and define*

$$\theta_{j,k} = \sum_{\substack{1\le a<m\\(a,m)=1}} \left(\left\lfloor \frac{(j+k)a}{m}\right\rfloor - \left\lfloor \frac{ja}{m}\right\rfloor - \left\lfloor \frac{ka}{m}\right\rfloor\right)\sigma_a^{-1}.$$

   Then $(J(\chi^{-j},\chi^{-k})) = \wp_1^{\theta_{j,k}}$ as ideals in $\mathbb{Q}(\zeta_m)$.

Proof. See [7]. □

Let $K = \mathbb{Q}(\sqrt{-d})$, where $d > 0$ is square free. Suppose $\left(\dfrac{D}{p}\right) = 1$, where D is the discriminant of the field. Then $p\mathcal{O}_K = \delta_1\delta_2$. By Proposition 3.9, we see that $K \subset L$, where $L = \mathbb{Q}(\zeta_{|D|})$.

Let f be the order of p in $\left(\mathbb{Z}/|D|\mathbb{Z}\right)^\times$, so $p^f \equiv 1 \pmod{|D|}$. In this case, we have $p\mathcal{O}_L = \wp_1\wp_2\cdots\wp_g$, where $g = \dfrac{\varphi(D)}{f}$ (see [14], Theorem 2.13, page 14). Let M be the maximal subfield of L containing $\mathbb{Q}$ in which p splits completely. M is the fixed field of the decomposition group of $\wp_i$ (see [10], page 17), which is the subgroup of Gal $(L/\mathbb{Q})$

generated by σ_p. Now, $[L:M] = f$ and $[M:\mathbb{Q}] = \dfrac{\varphi(|D|)}{f}$. Thus, each prime lying above p in M has one prime lying above it in L and the residue degree is f. Let $p\mathscr{O}_M = \mathfrak{D}_1\mathfrak{D}_2\cdots\mathfrak{D}_g$ with each $\wp_i$ lying above $\mathfrak{D}_i$. Then $N_{L/M}(\wp_i) = \mathfrak{D}_i^f$.

Let $G_n = \text{Gal}\,(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. The map $b \mapsto \sigma_b$, where $\sigma_b(\zeta_n) = \zeta_n^b$ gives a canonical isomorphism of $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ and G_n. Let $(t,n) = 1$. Then $G_{nt} = G_n \times G_t$ with $\mathbb{Q}(\zeta_t)$, $\mathbb{Q}(\zeta_n)$ being fixed fields for G_n, G_t, respectively. It follows from Galois theory that if $H \subset G_n$ and $F = \mathbb{Q}(\zeta_n)^H$, then $\mathbb{Q}(\zeta_{nt})^H = F(\zeta_t)$.

Let $m = |D|$, $q = p^f$, $\chi : \mathbb{F}_q \to \mu_m$ be a character. Then

$$\sigma_p(-\tau_p(\chi)) = \sigma_p\left(\sum \chi(a)\zeta_p^{\text{Tr}\,(a)}\right) = \sum \chi(a^p)\zeta_p^{\text{Tr}\,(a)} = \sum \chi(a^p)\zeta_p^{\text{Tr}\,(a^p)} = -\tau_p(\chi).$$

Since the fixed field for $\langle\sigma_p\rangle$ in L is M, this implies that $\tau_p(\chi) \in M(\zeta_p)$.

Let $\chi = \omega^{\frac{q-1}{m}}$, where ω is the Teichmüller character associated to a prime of $\mathbb{Q}(\zeta_{q-1})$ above $\wp_1$. Define $W = N_{M(\zeta_p)/K(\zeta_p)}(\tau_p(\chi)) \in K(\zeta_p)$. We will prove that $W \in \mathscr{O}_K$ and for some $\eta \in \mathbb{N}$, we have $Z = W/p^\eta \in \mathscr{O}_K$ and $N_{K/\mathbb{Q}}(Z) = p^h$. Therefore, Z will serve for our purpose of finding solutions of the norm equations in the general case ($d \neq 1,2,3$).

Let $H \subset G_m$ denote Gal (L/K). Let R be a set of representatives of $H/\langle p\rangle$ in the set of integers in the interval $(0,m)$. Then $W = \prod_{b\in R} \tau_p(\chi^b)$. Let $\psi = \left(\prod_{b\in R} \chi^b\right)\Big|_{\mathbb{F}_p}$. We note that for $c \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$, the action of $g_c \in \text{Gal}\,(L(\zeta_p)/L)$ on W is given by

$$g_c(W) = \psi^{-1}(c)W.$$

In fact, we have

$$g_c(\tau_p(\chi^b)) = -\sum \chi^b(a)\zeta_p^{c\mathrm{Tr}\,(a)} = -\sum \chi^b(acc^{-1})\zeta_p^{\mathrm{Tr}\,(ca)} = \chi^{-b}(c)\tau_p(\chi^b).$$

Thus, to show that $W \in K$, we need to show that $\psi = \psi_0$.

Let $[a]_m$ be the integer representing a in the interval $[0,m)$. Let $i = \sum_{a \in H \subset (\mathbb{Z}/m\mathbb{Z})^\times} [a]_m$.

We will show that $\psi = \psi_0$ if $i \equiv 0 \pmod{m}$. In fact, $\psi = \psi_0$ if and only if $\frac{q-1}{m}\left(\sum_{b\in R} b\right) \equiv 0 \pmod{p-1}$ because $\omega|_{\mathbb{F}_p}$ has strict order $p-1$. But

$$\frac{q-1}{m}\left(\sum_{b\in R} b\right) = (p-1)\frac{(1+p+\cdots+p^{f-1})\left(\sum_{b\in R} b\right)}{m} \equiv 0 \pmod{p-1}$$

because

$$(1+p+\cdots+p^{f-1})\left(\sum_{b\in R} b\right) \equiv i \pmod{m} \equiv 0 \pmod{m}.$$

Proposition 3.14. *If $d \neq 1,2,3$ (respectively, $m \neq 4,8,3$), then $i \equiv 0 \pmod{m}$.*

Proof. We note that m is either a power of a prime, or a product of m_1m_2, where $(m_1,m_2) = 1$ and $m_i > 2$ for $i = 1,2$. In the first case, $m = p \equiv 3 \pmod 4$ and the prime p is greater than 3. Note that $4 \pmod{m} \in H$. Hence, $H = 4H$ and

$$i = \sum_{h\in H} [4h]_m \equiv 4\sum_{h\in H} [h]_m \equiv 4i \pmod{p}.$$

So $3i \equiv 0 \pmod{p}$ implies $i \equiv 0 \pmod{p}$.

Now we consider the case $m = m_1 m_2$. Let n be one of m_1, m_2. Let $\gamma : G_m \to G_n$ be the natural surjection. Note that $K \not\subset \mathbb{Q}(\zeta_n)$ by Proposition 3.9, so $\ker\gamma \not\subset H$ by Galois theory. So there exists $c \in \ker\gamma$, $c \notin H$. Then $G_m = cH \cup H$ because H has index 2 in G_m.

We conclude that $G_n = \gamma(G_m) = \gamma(cH) \cup \gamma(H) = (\gamma(c)\gamma(H)) \cup \gamma(H) = \gamma(H)$ since $\gamma(c) = 1$.

Note that $\sum_{b \in G_n} [b]_n = \frac{1}{2}\left(\sum_{b \in G_n} [b]_n + \sum_{b \in G_n} (n - [b]_n)\right) = \frac{1}{2} n\varphi(n)$, where $\varphi(n) = |G_n|$. So $\sum_{b \in G_n} [b]_n \equiv 0 \pmod{n}$ if $n > 2$.

We have $i \pmod{n} = \sum_{h \in H} \gamma(h) = [H/G_n]\left(\sum_{b \in G_n} b\right) \equiv 0 \pmod{n}$. So $i \equiv 0 \pmod{m_1}$, $i \equiv 0 \pmod{m_2}$ and $i \equiv 0 \pmod{m_1 m_2}$ because $(m_1, m_2) = 1$. □

Since $i \equiv 0 \pmod{m}$, then $\psi = \psi_0$.

Now let $\eta = \dfrac{i}{m} \in \mathbb{N}$. We wish to determine the factorization of $W \in K$ into prime divisors of K.

Note that $\tau_p(\chi^{-1})^m \in L$ and by Proposition 3.13,

$$(\tau_p(\chi^{-1})^m) = \wp_1^{\theta}, \quad \text{where } \theta = \sum_{\substack{1 \le a < m \\ (a,m) = 1}} a\sigma_a^{-1}.$$

Note that $\overline{\tau_p(\chi)} = \chi(-1)\tau_p(\chi^{-1})$, so

$$\overline{W} = (\tau_p(\chi^{-1})\chi(-1))^{\sum_{b \in R} \sigma_b} = \tau_p(\chi^{-1})^{\sum_{b \in R} \sigma_b} \psi(-1) = \tau_p(\chi^{-1})^{\sum_{b \in R} \sigma_b},$$

because $\psi = \psi_0$. Therefore,

$$(\overline{W}^m) = \wp_1^{\theta\left(\sum_{b\in R}\sigma_b\right)} = \left(\wp_1^{\sum_{b\in R}\sigma_b}\right)^{\theta}.$$

However, $\wp_1^{\sum_{b\in R}\sigma_b}$ is the image of a prime divisor δ_1 of K above p into the group of divisors of L. Since the action of σ_a on the image of δ_1 depends only on $\sigma_a|_K$,

$$(\overline{W}^m)_K = \delta_1^{\sum a(\sigma_a^{-1})\big|_K} = \delta_1^{\sum_{\chi_d(a)=1} a}\,\delta_2^{\sum_{\chi_d(a)=-1} a},$$

where $\delta_2 = \overline{\delta_1}$ is the conjugate of δ_1, so $\delta_1\delta_2 = (p)$. Therefore,

$$(\overline{W})_K^m = \delta_2^{-\sum \chi_d(a)a}(\delta_2\delta_1)^{\sum_{\chi_d(a)=1} a} = \delta_2^{-\sum \chi_d(a)a}(p)^{m\eta}.$$

Taking into account that by Proposition 3.10, $h = -\frac{1}{m}\sum \chi_d(a)a$, we get that

$$(\overline{W})_K = \delta_2^h(p)^\eta.$$

Finally, $Z = W/p^\eta \in \mathcal{O}_K$ and $(Z) = \delta_1^h$. See section 3.6 for a representation of W as a sum of the $m-$th roots of unity. Also, note that the equality $|Z|^2 = p^h$ implies that $\eta = \dfrac{\varphi(m)/2 - h}{2}$.

3.5 Solutions of Norm Equations in the case $\mathbb{Q}(\sqrt{-d})$, $d > 0$, d square-free, $d \neq 1,2,3$, $\left(\frac{D}{p}\right) = 1$

Let $x + wy = Z = \dfrac{\prod_{b \in R} \tau_p(\omega^{\frac{q-1}{m}b})}{p^\eta}$, where

$$w = \begin{cases} \sqrt{-d} & \text{if } d \equiv 1,2 \pmod 4 \\ \frac{1+\sqrt{-d}}{2} & \text{if } d \equiv 3 \pmod 4 \end{cases}.$$

We showed that $N_{K/\mathbb{Q}}(Z) = p^h$ and $(Z) = \delta_1^h$.

Let $[e]_n$ denote, as usual, the integer in $[0,n)$ representing $e \pmod n$. We want to express $\overline{Z}$ as a product of values of $p-$adic Gamma function using the Gross-Koblitz formula. We have

$$\overline{Z} = \frac{\prod_{b \in R} \tau_p(\omega^{-\frac{q-1}{m}b})}{p^\eta} = \frac{\pi^v}{p^\eta} \prod_{b \in R} \prod_{k=0}^{f-1} \Gamma_p \left(\frac{[\frac{q-1}{m}b]_{q-1}^{(k)}}{q-1} \right),$$

where $a^{(k)}$ in the Gross-Koblitz formula equals $[ap^k]_{q-1}$, so $[\frac{q-1}{m}b]_{q-1}^{(k)} = \frac{q-1}{m}[bp^k]_m$.

We note that $\dfrac{\pi^v}{p^\eta} = (-1)^\eta$ because $\overline{Z}$ and the product of values of Γ_p are δ_1-units, so $v = (p-1)\eta$ and $\dfrac{\pi^v}{p^\eta} = \left(\dfrac{\pi^{p-1}}{p}\right)^\eta = (-1)^\eta$.

Because the set $\{bp^k \pmod m : b \in R, k = 0,1,\ldots,f-1\} = \left\{ a \in \left(\mathbb{Z}/m\mathbb{Z}\right)^\times : \chi_d(a) = 1 \right\}$, we have

$$\overline{Z} = (-1)^\eta \prod_{\substack{1 \le a < m \\ \chi_d(a) = 1}} \Gamma_p\left(\frac{a}{m}\right) = \beta.$$

We also have

$$x+wy \equiv 0 \pmod{\delta_1^h},$$

$$\overline{x+wy} = \beta.$$

Therefore,

$$x \equiv \frac{1}{2}\beta \pmod{p^h} \quad \text{when } d \equiv 1,2 \pmod 4,$$

$$2x+y \equiv \beta \pmod{p^h} \quad \text{when } d \equiv 3 \pmod 4.$$

Let $\langle e \rangle_{p^n}$ denote the integer in the interval $\left(-\frac{p^n}{2}, \frac{p^n}{2}\right]$ representing $e \pmod{p^n}$. Let $c \le n \le h$, where c is defined in Proposition 3.7 in section 3.2. Let $[e] = [e]_{p^n}$, $\langle e \rangle = \langle e \rangle_{p^n}$. Let $T = \left[\frac{1}{m}\right]$ and $\alpha = (-1)^{\eta} \prod_{\substack{1 \le a < m \\ \chi_d(a) = 1}} (-1)^{[aT]} \prod_{\substack{1 \le j < [aT] \\ (j,p) = 1}} j$. We have

Theorem 3.15. *Let $d \neq 1,2,3$ and suppose p splits in $K = \mathbb{Q}(\sqrt{-d})$. Assume $p \neq 2$ if $d = 7$ and $p \neq 5$ if $d = 11$. If $d \equiv 1,2 \pmod 4$, then $x = \left\langle \frac{1}{2}\beta \right\rangle = \left\langle \frac{1}{2}\alpha \right\rangle$, $y = \pm\sqrt{\frac{p^h - x^2}{d}}$ are solutions in $\mathbb{Z}$, $p \nmid y$, of $x^2 + dy^2 = p^h$. If $d \equiv 3 \pmod 4$, then $2x+y = \langle \beta \rangle = \langle \alpha \rangle$ (if $p = 2$, $\langle \beta \rangle = \langle \alpha \rangle$ if $n \neq 2$), $y = \pm\sqrt{\frac{4p^h - (2x+y)^2}{d}}$ are solutions in $\mathbb{Z}$, with x, y not both divisible by p, of $(2x+y)^2 + dy^2 = 4p^h$.*

Proof. We know that p does not divide both x and y because otherwise p divides Z, but $(Z) = \delta_1^h$.

Let $d \equiv 1,2 \pmod 4$. Then $p \neq 2$ (since 2 ramifies in K), so $|x| \neq \frac{p^n}{2}$ because $x \in \mathbb{Z}$.

Also, $|x| \leq \frac{p^n}{2}$ according to Proposition 3.7. Then $\left|x - \left\langle \frac{1}{2}\beta \right\rangle\right| < \frac{p^n}{2} + \frac{p^n}{2}$ and we have shown (see above) that $p^n \left| \left(x - \left\langle \frac{1}{2} \right\rangle \beta\right)\right.$, so $x = \left\langle \frac{1}{2}\beta \right\rangle$.

The proof is the same for the case $d \equiv 3 \pmod 4$ if we show that $|b| \neq \frac{p^n}{2}$, where $b = 2x + y = \langle \beta \rangle$. $|b| \neq \frac{p^n}{2}$ is true if $p \neq 2$. If $p = 2$, then $d \equiv 7 \pmod 8$ because 2 splits in K and we have the norm equality $b^2 + dy^2 = 4(2^h)$. In particular, $1 + d \leq 4(2^h)$. If $h \geq 4$, then $c \geq k \geq 3$ (see the proof of Proposition 3.7), so $n \geq c \geq 3$. If $|b| = \frac{2^n}{2} = 2^{n-1}$, then $4|b \Rightarrow 4|y \Rightarrow 2|x$, a contradiction. If $h = 1$, then $d = 7$, but this case is excluded. If $h = 2$, then $d = 15$, $b = \pm 1$. If $h = 3$, then $d = 23$ or 31 and $b = \pm 3$ or $b = \pm 1$, respectively. Thus, if $h = 2$ or 3, then $n \geq c \geq k \geq 2$, so $|b| \neq \frac{2^n}{2}$.

Now, $\Gamma\left(\frac{a}{m}\right) \equiv \Gamma\left(\left[\frac{a}{m}\right]\right) = \Gamma([aT]) \pmod{p^n}$ and $\Gamma(k) = (-1)^k \prod_{\substack{1 \leq j < k \\ (j,p) = 1}} j$, according to the properties of the $p-$adic Gamma functions in section 3.1.

We note that one can remove $(-1)^*$ from the expressions for β and α, then we get

$$(\pm x, y), (\pm(2x + y), y)$$

instead of

$$(x, y), (2x + y, y)$$

(because $\langle -e \rangle = -\langle e \rangle$), which are also solutions of the norm equations. □

3.6 Solutions of Norm Equations as Normalized Trace of a Ratio of Products of Gauss Sums

In this section, we describe how to compute x when $d \equiv 1,2 \pmod 4$ and $x + \frac{y}{2}$ when $d \equiv 3 \pmod 4$ by applying the normalized trace to Z or its image in $\mathbb{F}_q$.

Let G be an abelian group with elements of finite order. Define a function $t : G \to \mathbb{Q}$ as follows: let $g \in G$ and $n(g)$ be the strict order of g. Then

$$t(g) = \mu(n(g)) \prod_{\ell | n(g)} \frac{1}{\ell - 1},$$

where ℓ runs through all primes dividing $n(g)$ and $\mu(n)$ is the Möbius function defined by

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is not square-free} \\ \prod_{\ell | n} (-1) & \text{otherwise} \end{cases}.$$

In particular, we have defined t on the group of roots of unity in $\overline{\mathbb{Q}}$.

Let a be an algebraic number. Define the normalized trace by $\mathrm{Tr}_0(a) = \dfrac{\mathrm{Tr}_{F/\mathbb{Q}}(a)}{\deg(F/\mathbb{Q})}$, where F is any finite extension of $\mathbb{Q}$ containing a. Note that $\mathrm{Tr}_0(a)$ does not depend on the choice of F.

If ζ is a root of unity, then $\mathrm{Tr}_0(\zeta) = t(\zeta)$. To see this, let $n = \text{order}(\zeta)$ and let $n = \prod_i q_i$ be the decomposition of n into product of powers of distinct primes. The group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \prod_i \mathrm{Gal}(\mathbb{Q}(\zeta_{q_i})/\mathbb{Q})$ and $\mathrm{Tr}_0(\zeta) = \prod_i \mathrm{Tr}_0(\zeta_{q_i})$. However,

$\mathrm{Tr}_{\mathbb{Q}(\zeta_{q_i})/\mathbb{Q}}(\zeta_{q_i}) = 0$ if $q_i = \ell^k$, $k \geq 2$ because

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{\ell^k})/\mathbb{Q}(\zeta_{\ell^{k-1}})}(\zeta_{\ell^k}) = \sum_{j=0}^{\ell-1} \zeta_{\ell^k}^{1+\ell^{k-1}j} = \zeta_{\ell^k}\left(\sum_{j=0}^{\ell-1} \zeta_\ell^j\right) = 0.$$

Also, $\mathrm{Tr}_0(\zeta_\ell) = \dfrac{-1}{\ell-1}$ since the characteristic polynomial of ζ_ℓ is $X^{\ell-1} + \cdots + X + 1$, $\deg(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) = \ell - 1$.

Suppose that $x + wy \in \mathscr{O}_K$ is such that $N_{K/\mathbb{Q}}(x+wy) = p^h$. Here, $w = \sqrt{-d}$ if $d \equiv 1,2 \pmod 4$, $w = \dfrac{1+\sqrt{-d}}{2}$ if $d \equiv 3 \pmod 4$. Then x, $x + \dfrac{y}{2} = \mathrm{Tr}_0(x+wy)$, respectively. In all cases, we found such Z represented as a ratio of Gauss sums, which can be written as $\sum_{\zeta \in S} \zeta$, where S is an explicitly given set of $m-$th roots of unity (or $6-$th roots of unity if $d = 3$). Thus, x, $x + \dfrac{1}{2}y$ can be computed as

$$\mathrm{Tr}_0(Z) = \mathrm{Tr}_0\left(\sum_{\zeta \in S} \zeta\right) = \sum_{\zeta \in S} \mathrm{Tr}_0(\zeta).$$

Suppose $\zeta \neq 1$ is a root of unity, $n = \text{order}\ (\zeta)$. Then

$$\prod_{\xi^n = 1, \xi \neq 1} (1 - \xi) = \left(\frac{X^n - 1}{X - 1}\right)\Bigg|_{X=1} = n,$$

so $(1-\zeta)$ divides n in $\mathscr{O}_{\mathbb{Q}(\zeta)}$.

In particular, if a prime p does not divide m ($p \not| 6$ if $d = 3$), then any prime $\wp$ of $L = \mathbb{Q}(\zeta_m)$ above p does not divide $(1-\zeta)$ if $\zeta \neq 1$ and ζ is an $m-$th root of unity (or $6-$th root of unity if $d = 3$) in L. Therefore, if $\mathbb{F}_q$ is the residue field of $\wp$, then the map

$\mu_m \to \mathbb{F}_q^\times$ ($\mu_6 \to \mathbb{F}_q$ if $d=3$) is injective, so $\mathrm{Tr}_0(\zeta) = t(\zeta \pmod{\wp})$ and

$$\mathrm{Tr}_0(Z) = \sum_{\zeta \in S} t(\zeta \pmod{\wp}).$$

We will now write such formulas explicitly. We extend $t : \mathbb{F}_q^\times \to \mathbb{Q}$ to $\mathbb{F}_q$ by setting $t(0) = 0$.

The case $d = 1$: Here, $Z = J(\chi_1, \chi_2)$ with $\chi_1 = \omega^{\frac{p-1}{2}}$, $\chi_2 = \omega^{\frac{p-1}{4}}$. Then for $p \equiv 1 \pmod 4$,

$$x = \mathrm{Tr}_0\left(\sum_{a \in \mathbb{F}_q, a \neq 0,1} \chi_1(a)\chi_2(1-a)\right) = \sum_{a \in \mathbb{F}_q, a \neq 0,1} \left(\frac{a}{p}\right) \mathrm{Tr}_0(\chi_2(1-a)) =$$
$$= \sum_{a \in \mathbb{F}_q, a \neq 0,1} \left(\frac{a}{p}\right) t((1-a)^{\frac{p-1}{4}}).$$

Here, $\left(\frac{a}{p}\right) = 1$ if a is a square in $\mathbb{F}_p$, $\left(\frac{a}{p}\right) = -1$ otherwise.

The case $d = 3$, $p \equiv 1 \pmod 3$: Here, $Z = J(\chi_1, \chi_2)$ with $\chi_1 = \omega^{\frac{p-1}{6}}$, $\chi_2 = \omega^{\frac{p-1}{3}}$ so

$$x + \frac{1}{2}y = \mathrm{Tr}_0\left(\sum_{a \in \mathbb{F}_p} \chi_1(a)\chi_2(1-a)\right) = \sum_{a \in \mathbb{F}_p} t(a^{\frac{p-1}{6}}(1-a)^{\frac{p-1}{3}}).$$

The case $d = 2$, $p \equiv 1 \pmod 8$: Here, $Z = J(\chi_1, \chi_2)$ with $\chi_1 = \omega^{\frac{p-1}{8}}$, $\chi_2 = \omega^{\frac{3p-3}{8}}$, so

$$x = \mathrm{Tr}_0\left(\sum_{a \in \mathbb{F}_p} \chi_1(a)\chi_2(1-a)\right) = \sum_{a \in \mathbb{F}_p} t(a^{\frac{p-1}{8}}(1-a)^{\frac{3p-3}{8}}).$$

If $d = 2$, $p \equiv 3 \pmod 8$, then $\mathbb{F}_q = \mathbb{F}_{p^2}$, $\chi = \omega^{\frac{p^2-1}{8}}$, $\psi = \chi|_{\mathbb{F}_p}$, $Z = \dfrac{\tau_p(\chi)}{\tau_p(\psi)} =$

$\sum_{a\in\mathbb{F}_{p^2},\mathrm{Tr}\,(a)=1} \chi(a)$. Thus,

$$x = \mathrm{Tr}_0\left(\sum_{a\in\mathbb{F}_{p^2},\mathrm{Tr}\,(a)=1} \chi(a)\right) = \sum_{a\in\mathbb{F}_{p^2},\mathrm{Tr}\,(a)=1} t(a^{\frac{p^2-1}{8}}).$$

If $d \neq 1,2,3$, p splits in $K = \mathbb{Q}(\sqrt{-d})$, except the case $p = 5$ for $d = 11$, then Z is defined as follows. Let $H \subset (\mathbb{Z}/m\mathbb{Z})^\times$ be the kernel of χ_d. Let $R = \{b_i : i = 1,2,\ldots,n\}$ be the set of integers in the interval $[0,m)$ representing the elements of $H/\{1,p,\ldots,p^{f-1}\}$, where f is the period of $p \pmod m$. In particular, $n = \dfrac{\varphi(m)}{2f}$. Let $\chi = \omega^{\frac{q-1}{m}} : \mathbb{F}_{p^f}^\times \to \mu_m$, $\chi_i = \chi^{b_i}$, $q = p^f$, $\psi = (\prod \chi_i)|_{\mathbb{F}_p}$. We proved in section 3.4 that $\psi = \psi_0$. Recall that $\eta = \dfrac{1}{2}\left(\dfrac{\varphi(m)}{2} - h\right) = \dfrac{\sum_{a\in H}[a]_m}{m} \in \mathbb{N}$.

From the results of section 3.4, we can set

$$Z = \frac{\prod_{i=1}^{n} \tau_p(\chi_i)}{p^\eta}.$$

Therefore, by property 5 on page 10,

$$Z = \frac{\left((-1)^n \sum_{\substack{c_i\in\mathbb{F}_q \\ \mathrm{Tr}\,(c_1+\cdots+c_n)=0}} \chi_1(c_1)\cdots\chi_n(c_n) + (-1)^{n-1} \sum_{\substack{c_i\in\mathbb{F}_q \\ \mathrm{Tr}\,(c_1+\cdots+c_n)=1}} \chi_1(c_1)\cdots\chi_n(c_n)\right)}{p^\eta}.$$

So when $d \equiv 3 \pmod 4$ or $d \equiv 1,2 \pmod 4$,

$$x+\frac{y}{2} \text{ or } x = \mathrm{Tr}_0(Z)$$
$$= \frac{1}{p^\eta}\left((-1)^n \sum_{\substack{c_i \in \mathbb{F}_q \\ \mathrm{Tr}(c_1+\cdots+c_n)=0}} t(c_1^{\frac{q-1}{m}b_1}\cdots c_n^{\frac{q-1}{m}b_n}) + (-1)^{n-1} \sum_{\substack{c_i \in \mathbb{F}_q \\ \mathrm{Tr}(c_1+\cdots+c_n)=1}} t(c_1^{\frac{q-1}{m}b_1}\cdots c_n^{\frac{q-1}{m}b_n})\right),$$

respectively.

3.7 Examples

With the aid of Mathematica, we compute some examples.

Example 3.1. *Let $d = 7$ and $p = 29$. Then $h = 1$, $T = 25$ and $2x+y =$ $\langle \Gamma_{29}(\frac{1}{7})\Gamma_{29}(\frac{2}{7})\Gamma_{29}(\frac{4}{7})\rangle = 2$ and $y = \pm\sqrt{\frac{4(29)-2^2}{7}} = \pm 4$.*

Example 3.2. *Let $d = 11$, so $h = 1$. Let $p = 23$. We have $T = 21$, $2x+y = 9$ and $y = \pm\sqrt{\frac{4(23)-9^2}{11}} = \pm 1$.*

Example 3.3. *Let $d = 15$, so $h = 2$. Let $p = 31$. We have $T = 897$, $2x+y = -2$ and $y = \pm\sqrt{\frac{4(31)^2-(-2)^2}{15}} = \pm 16$.*

Example 3.4. *Let $d = 19$ and $p = 191$ so $h = 1$ and $T = 181$. We have $2x+y = 17$ and $y = \pm\sqrt{\frac{4(191)-17^2}{19}} = \pm 5$.*

Example 3.5. *Let $d = 23$ and $p = 47$. Then $h = 3$ and $c = k = 2$ in Proposition 3.7. We have $T = \left[\frac{1}{23}\right]_{47^2} = 2113$, $2x+y = -48$ and $y = \pm\sqrt{\frac{4(47)^3-(-48)^2}{23}} = \pm 134$.*

Example 3.6. *Let $d = 23$ and $p = 2$. We have $h = 3$. By Proposition 3.7, $c = \frac{h+1}{2} + 1 = 3$. We have $T = \left[\frac{1}{23}\right]_{2^3} = 7$, $2x + y = 3$ and $y = \pm\sqrt{\frac{4(2^3)-3^2}{23}} = \pm 1$.*

Example 3.7. *Let $d = 31$ and $p = 2$. Here, $h = 3$ and since $31 > 2^3(\frac{16-2}{4})$, $c = \frac{h+1}{2} = 2$. Now, we cannot take the modulus to be $2^2 = 4$, so we choose $n = 3$. We have $T = \left[\frac{1}{31}\right]_{2^3} = 7$, $2x + y = 1$ and $y = \pm\sqrt{\frac{4(2^3)-1^2}{31}} = \pm 1$.*

Example 3.8. *Let $d = 39$ and $p = 2$. Then $h = 4$ and by Proposition 3.7, $c = 4$. We have $T = \left[\frac{1}{39}\right]_{2^4} = 7$, $2x + y = -5$ and $y = \pm\sqrt{\frac{4(2^4)-(-5)^2}{39}} = \pm 1$.*

Example 3.9. *Let $d = 43$ and $p = 173$. We have $h = 1$ and $T = 169$, $2x + y = -2$ and $y = \pm\sqrt{\frac{4(173)-(-2)^2}{43}} = \pm 4$.*

Example 3.10. *Suppose $d = 51$. Then $h = 2$. Let $p = 103$. Then $T = 10,401$. We have $2x + y = -155$ and $y = \pm\sqrt{\frac{4(103)^2-(-155)^2}{51}} = \pm 19$.*

Example 3.11. *Suppose $d = 119$ and $p = 2$. Then $h = 10$. By Proposition 3.7, we have $c = \frac{10}{2} + 1 + 1 = 7$ so that $T = [\frac{1}{119}]_{2^7} = 71$, $2x + y = -55$ and $y = \pm\sqrt{\frac{4(2^{10})-(-55)^2}{119}} = \pm 3$.*

Example 3.12. *Let $d = 191$ and $p = 2$. Then $h = 13$, $c = \frac{13+1}{2} + 2 = 9$. We have $T = [\frac{1}{191}]_{2^9} = 319$, $2x + y = 153$, $y = \pm\sqrt{\frac{4(2^{13})-153^2}{191}} = \pm 7$.*

Example 3.13. *Let $d = 327$ and $p = 2$. We have $h = 12$ and $c = \frac{12}{2} + 1 + 1 = 8$. We get $T = [\frac{1}{327}]_{2^8} = 119$, $2x + y = 19$ so that $y = \pm\sqrt{\frac{4(2^{12})-19^2}{327}} = \pm 7$.*

Example 3.14. *Let $d = 6$, then $h = 2$. Let $p = 73$. We have $T = 5107$, $x =$*

$\langle \frac{1}{2}\Gamma_{73}(\frac{1}{24})\Gamma_{73}(\frac{5}{24})\Gamma_{73}(\frac{7}{24})\Gamma_{73}(\frac{11}{24})\rangle = -25$ *and* $y = \pm\sqrt{\frac{73^2-(-25)^2}{6}} = \pm 28$.

Example 3.15. *Let $d = 21$ so that $h = 4$ and $c = k = 3$ in Proposition 3.7. Let $p = 337$.*

Then $T = 37,817,125$,

$x = \langle \frac{1}{2}\Gamma_{337}(\frac{1}{84})\Gamma_{337}(\frac{5}{84})\Gamma_{337}(\frac{11}{84})\Gamma_{337}(\frac{17}{84})\Gamma_{337}(\frac{19}{84})\Gamma_{337}(\frac{23}{84})\Gamma_{337}(\frac{25}{84})\Gamma_{337}(\frac{31}{84})\Gamma_{337}(\frac{37}{84})\Gamma_{337}(\frac{41}{84})\Gamma_{337}(\frac{55}{84})\Gamma_{337}(\frac{71}{84})\rangle$

$= 110,881$ *and* $y = \pm\sqrt{\frac{337^4-(110,881)^2}{21}} = \pm 5,360$.

Chapter 4

Finding the Height of the Stickelberger Ideal

Let ζ_m be a primitive $m-$th root of unity, $M/\mathbb{Q}$ be a finite abelian extension, $G = \text{Gal}\ (M/\mathbb{Q})$ and $G_m = \text{Gal}\ (\mathbb{Q}(\zeta_m)/\mathbb{Q})$. For $(a,m) = 1$, let $\sigma_a \in G_m$ denote the element such that $\zeta_m \mapsto \zeta_m^a$ as well as its restriction to M. Let $I = I(M)$ be the Stickelberger ideal (see section 2.1).

Case 1: $M = \mathbb{Q}(\zeta_m)$.

Assuming $M = \mathbb{Q}(\zeta_m)$, we want to compute $\min \left(\sum_{\substack{\sigma \in G_m \\ 0 \neq \sum \alpha_\sigma \sigma \in I \\ \alpha_\sigma \geq 0 \text{ for all } \sigma}} \alpha_\sigma \right)$.

We first note that the map $\phi : \sum \alpha_\sigma \sigma \mapsto \sum \alpha_\sigma$ is a homomorphism. Now let $\sum x_i \sigma_i \in \mathbb{Z}[G] \backslash \{0\}$ such that $(\sum x_i \sigma_i)\theta \in \mathbb{Z}[G]$. That is,

$$\left(\sum_i x_i \sigma_i \right) \left(\sum_b \frac{b}{m} \sigma_{b^{-1}} \right) = \sum_b \sum_i \frac{x_i b}{m} \sigma_{ib^{-1}} = \sum_a \sum_i \frac{i a x_i}{m} \sigma_{a^{-1}} \in \mathbb{Z}[G],$$

where $a^{-1} \equiv ib^{-1} \pmod{m}$. By the homomorphism ϕ, we get

$$\left(\sum_i x_i\right)\left(\sum_b \frac{b}{m}\right) = \sum_a \sum_i \frac{iax_i}{m} \in \mathbb{Z}. \tag{4.1}$$

Since

$$\sum_{\substack{1 \le b < m \\ (b,m)=1}} \frac{b}{m} = \frac{m \cdot \varphi(m)/2}{m} = \frac{\varphi(m)}{2},$$

equation (4.1) is equivalent to

$$\left(\sum_i x_i\right)\frac{\varphi(m)}{2} = \sum_a \sum_i \frac{iax_i}{m} \in \mathbb{Z}. \tag{4.2}$$

Since we want to consider only cases where the coefficients are nonnegative, this means that $\sum_i x_i \in \mathbb{Z}^+$. That is, $\min\left(\sum_a \sum_i \frac{iax_i}{m}\right) \ge \frac{\varphi(m)}{2}$. To determine the actual minimum, we look at two cases:

The first case is $(2,m) = 1$. In this case, we have

$$(2-\sigma_2)\theta = (2-\sigma_2) \sum_{\substack{1 \le a < m \\ (a,m)=1}} \frac{a}{m}\sigma_a^{-1} = \sum_{\substack{1 \le a < m \\ (a,m)=1}} \frac{2a}{m}\sigma_{a^{-1}} - \sum_{\substack{1 \le a < m \\ (a,m)=1}} \frac{a}{m}\sigma_{2a^{-1}}. \tag{4.3}$$

Let $b^{-1} \equiv 2a^{-1} \pmod{m}$ and write $[b]_m = [b]$ to mean the integer in $[0,m)$ representing b

$(\text{mod } m)$. Thus, equation (4.3) equals

$$\sum_{\substack{1 \le a < m \\ (a,m)=1}} \frac{2a}{m}\sigma_{a^{-1}} - \sum_{\substack{1 \le b < m \\ (b,m)=1}} \frac{[2b]}{m}\sigma_{b^{-1}} = \sum_{\substack{1 \le b < m \\ (b,m)=1}} \frac{2b-[2b]}{m}\sigma_{b^{-1}} \tag{4.4}$$

$$= \sum_{\substack{1 \le b < m \\ (b,m)=1}} \left\lfloor \frac{2b}{m} \right\rfloor \sigma_{b^{-1}}, \tag{4.5}$$

where $\lfloor x \rfloor$ denotes the greatest integer function.

For $2b < m$, $\left\lfloor \frac{2b}{m} \right\rfloor = 0$. For $2b > m$, we note that since we are summing values of b for which $b < m$, then $2b < 2m$, so that $\left\lfloor \frac{2b}{m} \right\rfloor = 1$. This means that the summation (4.5) is equivalent to

$$\sum_{\substack{\frac{m}{2} < b < m \\ (b,m)=1}} \sigma_b^{-1}.$$

Hence, we want to look at $\sum_{\substack{\frac{m}{2} < b < m \\ (b,m)=1}} 1$. We consider the question of how many b's satisfy $m < 2b$ and $(b,m) = 1$. The residues relatively prime to m are distributed symmetrically about $\frac{m}{2}$, so there are $\frac{\varphi(m)}{2}$ many such b's. Therefore, $\sum_{\substack{\frac{m}{2} < b < m \\ (b,m)=1}} 1 = \frac{\varphi(m)}{2}$.

We have shown that there is an element in the Stickelberger ideal such that the sum of the coefficients is equal to $\frac{\varphi(m)}{2}$. That is, when $(m,2) = 1$, we have

$$\min\left(\sum_{\substack{\sigma\in G_m\\ 0\neq\sum\alpha_\sigma\sigma\in I\\ \alpha_\sigma\geq 0 \text{ for all } \sigma}} \alpha_\sigma\right) = \frac{\varphi(m)}{2}.$$

For the case $(m,2)\neq 1$, we claim that $\min\left(\sum_{\substack{\sigma\in G_m\\ 0\neq\sum\alpha_\sigma\sigma\in I\\ \alpha_\sigma\geq 0 \text{ for all } \sigma}} \alpha_\sigma\right) = \varphi(m)$. To see that there exists an element in the Stickelberger ideal such that the sum of coefficients is equal to $\varphi(m)$, consider

$$\begin{aligned}(\sigma_1+\sigma_{m-1})\theta &= (\sigma_1+\sigma_{-1})\left(\sum_b \frac{b}{m}\sigma_{b^{-1}}\right) = \sum_b \frac{b}{m}\sigma_{b^{-1}} + \sum_b \frac{b}{m}\sigma_{-b^{-1}}\\ &= \sum_b \frac{b}{m}\sigma_{b^{-1}} + \sum_a \frac{m-a}{m}\sigma_{a^{-1}} = \sum_b \sigma_{b^{-1}}.\end{aligned}$$

This element of the Stickelberger ideal has $\sum_b 1 = \varphi(m)$.

Now, to see that there are no elements in the Stickelberger ideal with $\sum \alpha_\sigma = \frac{\varphi(m)}{2}$, we assume there is one and obtain a contradiction. From equation (4.2), we have $\left(\sum_i x_i\right)\frac{\varphi(m)}{2} = \sum_a\sum_i \frac{iax_i}{m} \in \mathbb{Z}$. This sum being equal to $\frac{\varphi(m)}{2}$ implies that $\sum_i x_i = 1$. On the other hand, $\sum_a\sum_i \frac{iax_i}{m}\sigma_{a^{-1}} \in \mathbb{Z}[G]$ tells us that $\sum_i \frac{iax_i}{m} \in \mathbb{Z}$, or $\sum_i iax_i \equiv 0 \pmod m$. Since $(m,2)\neq 1$ and $(i,m) = (a,m) = 1$, this tells us that $\sum_i x_i \equiv 0 \pmod 2$, which contradicts $\sum_i x_i = 1$. Thus, there are no elements in the Stickelberger ideal such that

$\sum \alpha_\sigma = \dfrac{\varphi(m)}{2}$ for the case $(m,2) \neq 1$. Since there is an element with $\sum x_i = 2$ (equivalently, $\sum \alpha_\sigma = \varphi(m)$), we see that $\min \left(\sum_{\substack{\sigma \in G_m \\ 0 \neq \sum \alpha_\sigma \sigma \in I \\ \alpha_\sigma \geq 0 \text{ for all } \sigma}} \alpha_\sigma \right) = \varphi(m)$.

Case 2: $M \subset \mathbb{Q}(\zeta_m)$.

More generally, we will assume that M is a proper subfield of $\mathbb{Q}(\zeta_m)$. The result follows almost immediately from the above. For the case $(2,m) = 1$, we see that $(2-\sigma_2)\theta \in \mathbb{Z}[G_m]$ actually implies $(2-\sigma_2)\theta \in \mathbb{Z}[G]$, where $G = \text{Gal}\,(M/\mathbb{Q}) \cong \dfrac{G_m}{\text{Gal}\,(\mathbb{Q}(\zeta_m)/M)}$. Note that when we pass to the quotient, the coefficients of elements in G will be sums of coefficients of elements in G_m, and thus will be in $\mathbb{Z}$ also. Hence, the minimum will again be $\dfrac{\varphi(m)}{2}$. Similarly, for $(2,m) \neq 1$, $(\sigma_1 + \sigma_{m-1})\theta \in \mathbb{Z}[G_m]$ implies $(\sigma_1 + \sigma_{m-1})\theta \in \mathbb{Z}[G]$ and the minimum of the sum of the coefficients will be $\varphi(m)$.

Bibliography

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[2] Henri Cohen, *Number Theory*, vol. II: Analytic and Modern Tools, Springer-Verlag, 2007.

[3] ———, *Number Theory*, vol. I: Tools and Diophantine Equations, Springer-Verlag, 2007.

[4] Benedict H. Gross and Neal Koblitz, *Gauss sums and the* $\mathfrak{p}$*-adic* Γ*-function*, Annals of Mathematics **109** (1979), no. 3, 569–581.

[5] Kenneth Ireland and Michael Rosen, *A classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, 2010.

[6] Gerald J. Janusz, *Algebraic Number Fields*, 2nd ed., American Mathematical Society, 1996.

[7] S. A. Katre, *Gauss-Jacobi sums and Stickelberger's Theorem*, Cyclotomic fields and related topics (2000), 75–92.

[8] Neal Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Springer, 1984.

[9] Serg Lang, *Cyclotomic Fields I and II*, combined 2nd ed., Springer-Verlag, 1990.

[10] ———, *Algebraic Number Theory*, 2nd ed., Springer-Verlag, 1994.

[11] Daniel A. Marcus, *Number Fields*, Springer, 1977.

[12] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.

[13] Alain M. Robert, *The Gross-Koblitz Formula Revisited*, Rendiconti del Seminario Matematico della Università di Padova **105** (2001), 157–170.

[14] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer, 1997.