Quadratic Form Gauss Sums

by

Greg Doyle, B.Math, M.Sc. (Carleton University)

A thesis submitted to
the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of
the requirements for the degree of
Doctor of Philosophy

School of Mathematics and Statistics
Ottawa-Carleton Institute for Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada

Abstract

Let p be a prime, $n, r \in \mathbb{N}$, $S \in \mathbb{Z}$ such that $(S, p) = 1$. We let

$$Q_r = \sum_{1 \leq i \leq j \leq r} t_{ij} x_i x_j \in \mathbb{Z}[x_1, \ldots, x_r]$$

be an integral r-dimensional quadratic form. For convenience, set $e(\alpha) = e^{2\pi i \alpha}$, where $\alpha \in \mathbb{Q}$. Denote the quadratic Gauss sum by

$$G(S; p^n) = \sum_{x=0}^{p^n - 1} e\left(\frac{Sx^2}{p^n}\right).$$

The evaluation of this sum was completed by Gauss in the early 19th century. Many proofs of Gauss's results have subsequently been obtained through a variety of methods.

We are interested in the so called quadratic form Gauss sum, given by

$$G(Q_r; S; p^n) = \sum_{x_1, \ldots, x_r = 0}^{p^n - 1} e\left(\frac{S}{p^n} \cdot Q_r\right)$$

Under certain assumptions on Q_r, we show how we may express $G(Q_r; S; p^n)$ as a product of quadratic Gauss sums.

Acknowledgements

I would like to thank my supervisor, Saban Alaca, for his guidance and help in guiding me through this project. I would also like to thank Kenneth Williams for his efforts on my behalf throughout my graduate career. As well, I would like to thank Ayse Alaca for her help with my research.

I am indebted to all my professors at Carleton University for all their help and guidance. I would like to specifically thank David Amundsen, Inna Bumagin and Paul Mezo for their help in furthering my career in mathematics.

I would like to thank the number theory community for being so receptive to my work. In particular, I would like to thank Damien Roy for his comments on my early research.

Finally, I would like to thank all my colleagues and staff at the school of Mathematics and Statistics at Carleton University.

Contents

Chapter 1

Introduction

We let $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denote the sets of natural numbers, integers, rational numbers, real numbers and complex numbers, respectively, and we let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. If $x \geq 0$ then $x^{\frac{1}{2}}$ denotes the principal square root of x, and if $x < 0$ then $x^{\frac{1}{2}}$ denotes the root in the upper half plane. If z is any complex number, we let $\Re(z)$ denote the real part of z. For any two integers a and b, we let (a, b) denote their greatest common divisor. For notational convenience, for any $\alpha \in \mathbb{Q}$ we set $e(\alpha) = e^{2\pi i \alpha}$, so that $e(\alpha + \beta) = e(\alpha)e(\beta)$. For this chapter, let $q \in \mathbb{N}$ and $S \in \mathbb{Z}$ satisfy $(S, q) = 1$ and let k be an arbitrary odd positive integer. In general, we let $\left(\frac{S}{q}\right)$ denote the Jacobi symbol.

The exponential sum given by

$$G(S; q) = \sum_{x=0}^{q-1} e\left(\frac{Sx^2}{q}\right)$$

is called the *quadratic Gauss sum* modulo q. This sum was first studied by Gauss in the early 19^{th} century [42], from where it gets its name. In 1811, Gauss [41] was able to determine

the incredible formula

$$G(S;q) = \begin{cases} \left(\frac{S}{q}\right) q^{\frac{1}{2}} & \text{if } q \equiv 1 \pmod 4 \\ 0 & \text{if } q \equiv 2 \pmod 4 \\ i\left(\frac{S}{q}\right) q^{\frac{1}{2}} & \text{if } q \equiv 3 \pmod 4 \\ \left(\frac{q}{S}\right)(1+i^S) q^{\frac{1}{2}} & \text{if } q \equiv 0 \pmod 4. \end{cases} \tag{1.1}$$

The formula for the quadratic Gauss sum is a deep theorem. There are a wide variety of proofs which may deduce results analogous to (1.1). These methods begin with Gauss and are still being found in the 21st century

The method used by Gauss was to study the polynomial

$$f_z(n) = \sum_{j=0}^{n} (-1)^j \left(\prod_{i=1}^{j-1} \frac{1-z^{n-i}}{1-z^{i+1}} \right) = \sum_{j=0}^{n} (-1)^j \begin{bmatrix} n \\ j \end{bmatrix},$$

for $z \in \mathbb{C}$ with $z \neq 1$. Note that the symbol $\begin{bmatrix} n \\ j \end{bmatrix}$ is often called the Gaussian coefficient, or Gaussian polynomial [10, p. 42]. For p an odd prime and $z = e\left(\frac{1}{p}\right)$, Gauss showed that

$$G(1;p) = f_z(p-1) e\left(\frac{p^2-1}{8}\right) (-1)^{\frac{(p-1)(p-3)}{8}}. \tag{1.2}$$

Gauss then used the properties of f_z and (1.2) to arrive at (1.1); see, e.g. [93, pp. 177-180]. Note that it is straightforward to show $|G(1;k)| = k^{\frac{1}{2}}$. Given the correct unit expression for $G(1;k)$, one can use elementary methods to arrive at the formula given in (1.1). Thus, to evaluate $G(S;q)$ it is sufficient to determine that $G(1;p) = i^{\left(\frac{p-1}{2}\right)^2} p^{\frac{1}{2}}$ for p an odd prime; see, e.g. [12, pp. 18-24].

Dirichlet, beginning in 1835, published a series of papers which reproduced Gauss' results; [28], [29], [30]; see also [31, pp. 287-292]. Dirichlet used a variation of the Poisson summation

formula to show

$$G(1;q) = \frac{1}{2}(1+i)(1+i^{-q})q^{\frac{1}{2}}. \tag{1.3}$$

Due to the multiplicative structure of the quadratic Gauss sum, one can recover Gauss' formula in (1.1) from the expression given in (1.3). A modern exposition of Dirichlet's proof may be found in the book by Davenport [24, pp. 13-16] and the paper by Casselman [17]. In 1840, Cauchy [18, pp. 566-572] gave a proof of Gauss' results using the transformation formula for the classical theta function $\theta(z) = \sum_{n=-\infty}^{\infty} e\left(\frac{izn^2}{2}\right)$, defined for $\Re(z) > 0$ [11, p. 112]. A modern exposition of Cauchy's proof is given in the book by Chandrasekharan [19, p. 141-144]. Additionally, in the same paper, Cauchy [18, pp. 560-565] gave an elementary proof of (1.3). Circa 1850, Schaar used the Poisson summation formula to determine the sign of $G(1;k)$ [98]. Subsequently, using similar methods, Schaar developed a reciprocity formula for the quadratic Gauss sum [99], from which one can deduce the expression given in (1.3). This latter formula is now called *Schaar's identity* [11, p. 111]. Shortly after, in 1852, Genocchi [44] used the Abel-Plana summation formula to deduce Gauss' results. Later, in 1889, Kronecker [69] used contour integration to develop a general reciprocity formula for a generalized quadratic Gauss sum, of which Schaar's identity is a special case. This method of proof can be found in the books by Apostol [5, pp. 195-200] and Berndt, Evans and Williams [12, pp. 13-14]. Kronecker was quite taken with the quadratic Gauss sum, as earlier he gave an elementary proof determining the sign of $G(1;k)$ [67], as well as a refinement of Cauchy's methods for theta functions [68] and a discussion of Dirichlet's method [70]; see also the books by Krazer [65, pp. 183-193], Bellman [8, pp. 38-39] and Eichler [34, pp. 44-48]. Near the end of the century, in 1896, Mertens [86] gave an elementary proof establishing the sign of $G(1;k)$.

More methods of proof and refinements of these methods would follow in the 20^{th} century. In 1903, Lerch [75] further simplified and generalized the theta function approaches of Cauchy

and Kronecker. In 1918, Mordell [89] simplified Kronecker's contour integration method to arrive at the expression given in (1.3). Shortly thereafter, in 1921, Schur [100] used the determinants of certain matrices to evaluate $G(1;k)$. The proofs of Mertens, Schur and the contour integration proof of Kronecker are given in the book by Landau [71, pp. 203-218]. In 1945, Estermann [35] gave a very elegant proof determining the sign of $G(1;k)$. Later, in 1958, Shanks [102] gave an elementary evaluation of $G(1;k)$ using a certain product and sum identity. Shortly after, in 1960, Siegel [104] gave a proof of (1.3) using a similar approach to Mordell, as well as a generalized reciprocity theorem. In the same year, Mordell [91] gave an elementary proof of the sign of $G(1;k)$. A similar method to that of Schur would follow in 1966 by Carlitz [16]. Waterhouse [110], in 1970, would simplify Schur's method to determine the sign of $G(1;k)$. In 1973, Berndt [9] used contour integration to develop a very general reciprocity theorem, of which Siegel's result follows. A more general theorem would follow by Berndt and Schoenfeld [13] in 1975, using the Poisson summation formula. In 1981, Bressoud [15] follows the method of Gauss using a certain q-series identity, to deduce the value of $G(1;k)$. More recently, in 1995, Sczech [101] was able to deduce the value of $G(1;k)$ using Jacobi's triple product identity. One can consult the survey by Berndt and Evans [11] as well as the book by Berndt, Evans and Williams [12, pp. 50-54] for detailed developments of these results.

New methods for Gauss' results are still being discovered in the 21^{st} century. In 2000, Danas [23] was able to determine the value of $G(1;p)$, for p an odd prime, using a circulant matrix with Legendre symbol entries. In 2010, Gurevich, Hadani and Howe [48] have been able to determine the sign of $G(1;k)$ using the finite Weil representation. A 2014 paper by Grant [47] demonstrates a wide variety of elementary proofs of $G(1;p)$, for p an odd prime.

We mention that we have restricted the scope of our discussion specifically to the quadratic Gauss sum. The quadratic Gauss sum will generalize to a certain type of character sum over a ring of integers [5, p. 165], as well as an exponential sum over a finite field [12, p. 9]. Indeed, the quadratic Gauss sum is only a particular type of exponential sum, of which there

are a wide variety [12, p. 55]. We will discuss these generalizations in our final chapter.

We are interested in extending the quadratic Gauss sum over multiple variables using a quadratic form argument. Let $r \in \mathbb{N}$. We let Q_r denote an arbitrary r-dimensional integral quadratic form, given by

$$Q_r = \sum_{1 \leq i \leq j \leq r} t_{ij} x_i x_j \in \mathbb{Z}[x_1, \ldots, x_r].$$

Thus, we define $G(Q_r; S; q)$ to be the exponential sum given by

$$G(Q_r; S; q) = \sum_{x_1, \ldots, x_r = 0}^{q-1} e\left(\frac{SQ_r}{q}\right),$$

and we call this a *quadratic form Gauss sum.* For convenience, we let $t_i = t_{ii}$ for each i. Observe that if Q_r is a diagonal form, say $Q_r = \sum_{i=1}^{r} t_i x_i^2$, then our quadratic form Gauss sum reduces to a product of quadratic Gauss sums, as

$$G(Q_r; S; q) = \sum_{x_1, \ldots, x_r = 0}^{q-1} e\left(\frac{S\sum_{i=1}^{r} t_i x_i^2}{q}\right) = \prod_{i=1}^{r} \sum_{x_i = 0}^{q-1} e\left(\frac{S t_i x_i^2}{q}\right) = \prod_{i=1}^{r} G(S t_i; q).$$

We will examine how we may appropriately diagonalize Q_r to express the quadratic form Gauss sum as a product of quadratic Gauss sums. In particular, we do so in an elementary manner.

The quadratic form Gauss sum was first investigated in the 19^{th} century. In a paper published in 1872, H. Weber [111] investigated the sum $G(Q_r; 1; q)$ where Q_r is of the form $\sum_{i=1}^{r} t_i x_i^2 + 2 \sum_{1 \leq i < j \leq r} t_{ij} x_i x_j$. His method appears to be to determine a change of variables for which he may write $Q_r = Ax_1^2 + Q_{r-1}(x_2, \ldots, x_r)$, so that an expression for the quadratic form Gauss sum can be determined recursively. Weber first evaluates $G(Q_r; 1; p)$, for p an odd prime, and generalizes these results using the Chinese remainder theorem. This work

was simplified very shortly afterwards by Jordan [61], whose paper was published in 1871. Despite the disparity in publishing dates, Jordan makes explicit reference to the paper by Weber in his article. Additionally, the paper by Jordan does not contain any general results. These papers were written in German and French, respectively, and an English translation does not appear to be available. References to these papers are rare.

The quadratic form Gauss sum was then most prominently seen afterwards in the statement of various reciprocity theorems. We emphasize that none of these reciprocity theorems use the results of Weber. To limit our scope of discussion, we mention only a few related results. In a 1912 manuscript dedicated to Weber, Krazer [66], using a multi-variable Poisson summation formula, develops a reciprocity theorem for a certain quadratic form Gauss sum. The reciprocity theorem of Krazer would be generalized by Siegel [103] in 1935. Note that this paper by Siegel is a seminal treatment in the classification of quadratic forms, and introduces his mass formula.

More recently, in 1998, Deloup [26] and Turaev [107] establish more general reciprocity theorems, of which Krazer's and Siegel's are special cases. Further, the paper of Turaev shows that the reciprocity theorem first discovered by Kronecker is also a special case of his formula. These generalizations are treated in the book by Polishchuk [96, pp. 58-60]. We mention that the papers by both Deloup and Turaev make reference to a preprint by R. Dabrowski entitled *Multivariate Gauss Sums*, which does not appear to have been published. This paper claims to have proven the reciprocity theorem of Krazer by use of p-adic numbers [25, p. 71]. A paper available online by Taylor [106] gives a brief exposition which reproduces Krazer's results. One can consult the exhaustive work by Lemmermeyer [74] to track the development of reciprocity theorems. They have deep connections with the quadratic Gauss sum.

An important application of the quadratic form Gauss sums is in determining the number

of solutions to the congruence

$$Q_r \equiv t \pmod{q}. \tag{1.4}$$

We see that the number of solutions to this congruence is given by

$$\frac{1}{q}\sum_{y=0}^{q-1}\sum_{x_1,\ldots,x_r=0}^{q-1} e\left(\frac{y(Q_r-t)}{q}\right) = \frac{1}{q}\sum_{y=0}^{q-1} e\left(\frac{-yt}{q}\right) G(Q_r; y; q). \tag{1.5}$$

Historically, there appear to be few applications of the methods of Weber and Jordan concerning this problem. In fact, Jordan investigated the number of such solutions both in 1866 [59] and 1872 [62]; see also, [60, pp. 156-161]. However, he did not use an exponential sum method. A note by Jordan [63, p. 25] in 1881 indicates he was aware of the method given in (1.5).

A rare reference to the quadratic form Gauss sum is given in a 1954 paper by Cohen [22]. In this paper, Cohen uses the results of Weber [22, p. 14] in his investigation into the number of solutions of

$$a_1x_1^2 + \cdots + a_rx_r^2 \equiv t \pmod{q}. \tag{1.6}$$

However, Cohen does not use the results of Weber directly in a manner similar to (1.5). He instead attains his results by evaluating a certain singular series. Cohens singular series is similar to the series introduced by Hardy [54, p. 256] in a paper investigating the representation of integers as a sum of squares. There are intricate connections with these types of singular series and the quadratic Gauss sums. Cohen [22, p. 27] himself states:

> It is of interest to note that, although the Gauss sum $G(1;q)$ is of fundamental importance in the preceding treatment of quadratic congruences, at no point was it necessary to use the precise evaluation of $G(1;q)$.

Determining the number of solutions for $a_1 = \ldots = a_r = 1$ in (1.6) is given as an exercise in

[12, p. 46].

Determining the number of solutions to the congruence in (1.4) is an ongoing and active problem. There are some recent results which use the approach given in (1.5), without making explicit mention of the quadratic form Gauss sum. The 2004 paper of Araujo and Fernandez [6] used a sum analogous to the quadratic form Gauss sum to investigate the number of solutions to a diagonal quadratic form congruence, similar to that in (1.6). The 2012 paper by A. Alaca and Williams [3] and current preprint of Alaca, Alaca and Williams [2] use explicit evaluations of quadratic Gauss sums in order to determine the number of solutions to a particular quaternary form congruence. As this form is diagonal, they implicitly use the quadratic form Gauss sum. Indeed, the paper by Alaca and Williams uses the sum given in (1.5) in connection with Siegel's mass formula. In this fashion, given an expression for $G(Q_r; S; q)$, the evaluation of (1.5) will have deep results.

We look to evaluate $G(Q_r; S; q)$. To simplify our evaluation, we fix $q = p^n$ for p prime and look to evaluate $G(Q_r; S; p^n)$. Our primary motivation is given by a recent paper by Alaca, Alaca, and Williams [1]. In this paper, they use elementary methods to evaluate the so-called double Gauss sum

$$G(Q_2; S; p^n) = \sum_{x,y=0}^{p^n-1} e\left(\frac{S(ax^2 + bxy + cy^2)}{p^n}\right),$$

where $a, b, c \in \mathbb{Z}$ are such that $(a, b, c) = 1$ and $4ac - b^2 \neq 0$. We give a brief overview of their method

Observe that the quadratic form $Q_2 = ax^2 + bxy + cy^2$ can be expressed as the 1×1 matrix product

$$Q_2 = [x\ y] \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} [x\ y]^T.$$

The approach by Alaca, et al. is to determine integers ρ, σ, τ, μ such that, modulo p^n, we

have

$$Q_2 \equiv [x\ y] \begin{bmatrix} \rho & \tau \\ \sigma & \mu \end{bmatrix} \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} \rho & \tau \\ \sigma & \mu \end{bmatrix}^T [x\ y]^T \pmod{p^n}.$$

Subsequently, they show that there exists an automorphism λ defined on $\mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ which is given by $\lambda(x, y) = (\rho x + \sigma y, \tau x + \mu y)$. Due to their choice of integers, by setting $A = a\rho^2 + b\rho\tau + c\tau^2$, we have

$$Q_2 \equiv Ax^2 + A(4ac - b^2)y^2 \pmod{p^n}, \tag{1.7}$$

and in particular we will have $(A, p) = 1$. Hence, it follows that

$$\begin{aligned} G(Q_2; S; p^n) &= \sum_{x,y=0}^{p^n-1} e\left(\frac{S(Ax^2 + A(4ac - b^2)y^2)}{p^n}\right) \\ &= G(SA(4ac - b^2); p^n)G(SA; p^n). \end{aligned} \tag{1.8}$$

We mention that this will hold in general for p an odd prime. When $p = 2$, one must consider certain cases with respect to the coefficients of Q_2.

Our method is similar. We find a diagonalization of our quadratic form Q_r which will result in a change of variables that yields a similar congruence as seen in (1.7). Consider the matrix

$$\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} = \frac{1}{2}M.$$

Under the assumption $a \neq 0$, the symmetric matrix M can be decomposed into the LDL^T

decomposition given by

$$\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{b}{2a} & 1 \end{pmatrix} \begin{pmatrix} 2a & 0 \\ 0 & \frac{4ac-b^2}{2a} \end{pmatrix} \begin{pmatrix} 1 & \frac{b}{2a} \\ 0 & 1 \end{pmatrix}.$$

Hence, we see that

$$\begin{aligned} ax^2 + bxy + cy^2 &= [x\ y]\frac{M}{2}[x\ y]^T = [x\ y]L\frac{D}{2}L^T[x\ y]^T \\ &= [X\ Y]\frac{D}{2}[X\ Y]^T, \end{aligned}$$

where $X = x + \dfrac{by}{2a}$ and $Y = y$. Thus, our quadratic form can be written as a diagonal form with rational coefficients, that is,

$$ax^2 + bxy + cy^2 = aX^2 + \frac{(4ac - b^2)}{4a}Y^2.$$

We multiply this equation by the least common denominator, to arrive at

$$4aQ_2 = (2aX)^2 + (4ac - b^2)Y^2. \tag{1.9}$$

Assume for the sake of discussion that p is an odd prime. As $a \neq 0$ we may write $2a = p^\alpha A$ for $\alpha \in \mathbb{N}_0$ and $A \in \mathbb{Z}$ coprime to p. We then reduce the equation in (1.9) with respect to the modulus $p^{n+\alpha}$. This yields

$$p^\alpha Q_2 \equiv (2A)^{-1}(p^\alpha AX)^2 + (2A)^{-1}(4ac - b^2)Y^2 \pmod{p^{n+\alpha}}.$$

It will then follow due to the structure of the quadratic Gauss sum that

$$G(Q_2; S; p^n) = \frac{1}{p^{2\alpha}} \sum_{y=0}^{p^{n+\alpha}-1} e\left(\frac{S(2A)^{-1}(4ac - b^2)Y^2}{p^{n+\alpha}}\right) \sum_{x=0}^{p^{n+\alpha}-1} e\left(\frac{S(2A)^{-1}(p^\alpha AX)^2}{p^{n+\alpha}}\right).$$

If we assume that $(a, b, c) = 1$, we can show that each of these indexed sums will be a quadratic Gauss sum, so we may conclude that

$$G(Q_2; S; p^n) = \frac{1}{p^{2\alpha}} G(2SA(4ac - b^2); p^{n+\alpha}) G(2SAp^{2\alpha}; p^{n+\alpha}).$$

Due to various simplification properties inherent in the quadratic Gauss sum, this will yield the same result as given by Alaca, et al. in (1.8). Further, our method for the even prime case will be similar.

This procedure for a given binary quadratic form can be expanded in a similar fashion to higher dimensional quadratic forms. Let $r \in \mathbb{N}$ and Q_r an integral quadratic form in r variables. Under certain assumptions on the coefficients of Q_r, one may decompose its associated symmetric matrix into an LDL^T decomposition. From here, one can show that

$$CQ_r \equiv \sum_{i=1}^{r} \tau_i X_i^2 \pmod{p^n}$$

where $\tau_i \in \mathbb{Z}$, $C \in \mathbb{Z}$ and X_i is an integral function of $r - i + 1$ variables. Assume for the sake of discussion that $C = 1$. We nest our sums so that, for sufficiently large n, X_i will behave like x_i modulo p^n. This diagonalization of Q_r will yield

$$\begin{aligned} G(Q_r; S; p^n) &= \sum_{x_1,\ldots,x_r=0}^{p^n-1} e\left(\frac{S}{p^n} \sum_{i=1}^{r} \tau_i X_i^2\right) = \sum_{x_1,\ldots,x_r=0}^{p^n-1} \prod_{i=1}^{r} e\left(\frac{S\tau_i X_i^2}{p^n}\right) \\ &= \sum_{x_r=0}^{p^n-1} e\left(\frac{S\tau_r X_r^2}{p^n}\right) \cdots \sum_{x_1=0}^{p^n-1} e\left(\frac{S\tau_1 X_1^2}{p^n}\right) \\ &= \prod_{i=1}^{r} G(s\tau_i; p^n). \end{aligned}$$

A necessary requirement for our results is that, for an integral quadratic form in r variables, the first $r-1$ leading principal minors of its associated symmetric matrix be non-zero. Set Δ to be the product of these minors, which we call the associated minor product. Under the assumption $\Delta \neq 0$, we will achieve our results depending on the divisibility of the

factors of Δ. Specifically, for a prime power p^n, we will attain an expression for $G(Q_r; S; p^n)$ under the following conditions: Δ is coprime to p, the factors of Δ have favorable divisibility properties, n is sufficiently large. We note that the result for each case will be the same, but the manner in which these results were obtained will vary.

We begin in Chapter 2 by going over some basic properties and notation we'll need to prove our main results. In particular, we review some basic properties concerning quadratic residues and the Legendre symbol. Chapter 3 looks at properties of the quadratic Gauss sum. The quadratic Gauss sum will possess various cancellation properties which we will make use of. As well, we will look at a quadratic Gauss sum with congruence conditions imposed on the index. Chapter 4 shows how we may diagonalize a quadratic form. This will demonstrate the necessity of the condition $\Delta \neq 0$, as the diagonalization will follow after row reducing an associated symmetric matrix to row echelon form. In Chapter 5, using what was established in the previous two chapters, we present our main results. In particular, we determine a complete solution for $G(Q_2; S; p^n)$ for both p odd and even. Additionally, we give an expression for the ternary quadratic form Gauss sum $G(Q_3; S; p^n)$ under unfavorable divisibility conditions. Finally, we present multiple methods to evaluate $G(Q_r; S; p^n)$ under varying conditions, for which the binary and ternary forms will follow as specific examples. In Chapter 6, we present an application of the evaluation of $G(Q_r; S; p^n)$. Specifically, we will determine the number of solutions of the congruence $Q_2 \equiv k \pmod{p^n}$, where Q_2 is any binary quadratic form with integer coefficients, and k is any integer. Finally, we present further avenues of research in Chapter 7. We first show how we may generalize the quadratic form Gauss sum to an arbitrary odd positive modulus, say $G(Q_r; S; q)$. As well, using our main results we demonstrate some obvious multiplicative properties. Subsequently, we investigate how we might generalize the quadratic form Gauss sum to other types of Gauss sums. Finally, we mention current applications of various Gauss sums and their generalizations.

Chapter 2

Basic Properties

In this chapter, we review the basic notation, definitions and propositions we will be using.

2.1 Notation

As in the introduction, we let $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}$ and $\mathbb{Q}$ denote the natural numbers, the non-negative integers, the integers and rational numbers, respectively. As well, we let (x, y) denote the greatest common divisor of the integers x and y. For any $x \in \mathbb{Q}$, we let $[x]$ denote the greatest non-negative integer less than or equal to x. For $p \in \mathbb{N}$ and $q \in \mathbb{Z}$, we write $p \mid q$ to indicate p divides q. Otherwise, we write $p \nmid q$. We write $x \equiv y \pmod{p}$ to indicate $p \mid (x - y)$.

From now on, we will let p denote a prime. We let $n \in \mathbb{N}$ and $S \in \mathbb{Z}$ be such that $(S, p) = 1$. Let $t \in \mathbb{Z}$ be arbitrary. In general, if $t \neq 0$ we will write $t = p^\tau T$, where $\tau \in \mathbb{N}_0$ and $T \in \mathbb{Z}$ is such that $(T, p) = 1$. Our convention for integer notation is that lower case letters will be arbitrary integers, upper case letters will be integers co-prime to p and Greek letters will denote non-negative integers. Generally, we are concerned with the divisibility of residues modulo a prime power. We let $1, \ldots, p^n$ denote the system of residues modulo p^n. In this fashion, for any nonzero $t \in \mathbb{Z}$, we may write $t \equiv p^\tau T \pmod{p^n}$ for some $\tau \in \mathbb{N}_0$ and $1 \leq T \leq p^n$ coprime to p. If $t = 0$, then by convention we set $\tau = n$ and $T = 1$.

For any $\alpha \in \mathbb{Q}$ we write $e(\alpha) = e^{2\pi i \alpha}$ so that $e(\alpha + \beta) = e(\alpha)e(\beta)$, for arbitrary $\alpha, \beta \in \mathbb{Q}$.

Further, it is clear that

$$e(t) = 1, \ e\left(\frac{t}{2}\right) = (-1)^t \text{ and } e\left(\frac{t}{4}\right) = i^t.$$

For arbitrary $\alpha, \beta \in \mathbb{Q}$ we adopt the convention that $e^{\beta}(\alpha) = (e(\alpha))^{\beta} = e(\alpha \cdot \beta)$. Note that $e\left(\frac{S}{p}\right)$ is a p^{th} root of unity, so that $e\left(\frac{t}{p}\right) = 1$ if and only if $p \mid t$. Further, $e\left(\frac{t}{p}\right)$ is periodic with period p, that is, $e\left(\frac{x+yp}{p}\right) = e\left(\frac{x}{p}\right)$, for arbitrary $x, y \in \mathbb{Z}$. Hence, we say that $e\left(\frac{t}{p}\right)$ is periodic modulo p, and refer to p as the modulus.

Fix $q \in \mathbb{N}$ arbitrarily. We let $\mathbb{Z}_q$ denote the commutative ring of residues modulo q and we let $\mathbb{Z}_q^*$ denote the associated multiplicative group. We let $\phi(q)$ denote the number of positive integers less than q which are also relatively prime to q. In such a manner, we have $|\mathbb{Z}_q^*| = \phi(q)$. The set of all residues contained in $\mathbb{Z}_q$ is called a complete residue system modulo q, and the set of all residues in $\mathbb{Z}_q^*$ is called a reduced residue system modulo q. When q is understood, we identify every integer t with its residue $\bar{t} \pmod{q}$, so we may speak of the element t of $\mathbb{Z}_q$. For $t \in \mathbb{Z}$ coprime to q, we identify the symbol t^{-1} with its positive integer residue modulo q.

Finally, we let $\mathbb{Z}[x_1, \ldots, x_n]$ denote the ring of polynomials in n variables with integer coefficients.

2.2 Exponential Sums

Our discussion will center around the quadratic Gauss sum, a type of exponential sum. As such, we will need the following propositions concerning various exponential sums.

Proposition 2.1 (Geometric Sum)**.** *Let $k \in \mathbb{N}$. Then*

$$\sum_{x=0}^{k-1} e\left(\frac{tx}{k}\right) = \begin{cases} 0 & \text{if } t \not\equiv 0 \pmod{k} \\ k & \text{if } t \equiv 0 \pmod{k}. \end{cases}$$

Proof. We have that

$$\sum_{x=0}^{k-1} e\left(\frac{tx}{k}\right) = 1 + e\left(\frac{t}{k}\right) + e\left(\frac{t}{k}\right)^2 + \ldots + e\left(\frac{t}{k}\right)^{k-1}. \tag{2.1}$$

If $t \not\equiv 0 \pmod{k}$, then $e\left(\frac{t}{k}\right) \neq 1$. Hence, we have that (2.1) becomes

$$\frac{e\left(\frac{t}{k}\right)^k - 1}{e\left(\frac{t}{k}\right) - 1} = 0.$$

Otherwise, if $t \equiv 0 \pmod{k}$ then $e\left(\frac{t}{k}\right) = 1$ and so (2.1) evaluates to k in this case. □

Proposition 2.2. *Let $k \in \mathbb{N}$. Then*

$$\sum_{x,y=0}^{k-1} e\left(\frac{txy}{k}\right) = k \cdot (t,k).$$

Proof. From Proposition 2.1, we have that

$$\sum_{x,y=0}^{k-1} e\left(\frac{txy}{k}\right) = k + \sum_{x=1}^{k-1}\sum_{y=0}^{k-1} e\left(\frac{txy}{k}\right) = k + k \sum_{\substack{x=1 \\ tx \equiv 0 \pmod{k}}}^{k-1} 1 = k \sum_{\substack{x=0 \\ tx \equiv 0 \pmod{k}}}^{k-1} 1. \tag{2.2}$$

If $t \equiv 0 \pmod{k}$ then the statement of the proposition follows. Hence, we may assume otherwise, and in particular, $t \neq 0$. Let $d = (k,t)$ so that $k = dk_1$, $t = dt_1$ for some $k_1 \in \mathbb{N}$,

$t_1 \in \mathbb{Z}$ such that $(k_1, t_1) = 1$. Hence,

$$\sum_{\substack{x=0 \\ tx \equiv 0 \pmod{k}}}^{k-1} 1 = \sum_{\substack{x=0 \\ t_1 x \equiv 0 \pmod{k)_1}}}^{dk_1-1} 1 = \sum_{\substack{x=0 \\ x|k_1}}^{dk_1-1} 1 = d,$$

and with (2.2), the statement of the proposition follows. □

Proposition 2.3. *Let $\alpha \in \mathbb{N}_0$ and $k \in \mathbb{N}$. Then for any prime p, we have*

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\alpha x^k}{p^n}\right) = \begin{cases} p^n & \text{if } \alpha \geq n \\ p^\alpha \displaystyle\sum_{x=0}^{p^{n-\alpha}-1} e\left(\frac{Sx^k}{p^{n-\alpha}}\right) & \text{if } \alpha < n. \end{cases}$$

Proof. The statement is clear when $\alpha \geq n$ and so we may assume that $\alpha < n$. We have

$$\begin{aligned} \sum_{x=0}^{p^n-1} e\left(\frac{Sp^\alpha x^k}{p^n}\right) = \sum_{x=0}^{p^{n-\alpha}-1} e\left(\frac{Sx^k}{p^{n-\alpha}}\right) + \sum_{x=p^{n-\alpha}}^{2p^{n-\alpha}-1} e\left(\frac{Sx^k}{p^{n-\alpha}}\right) + \cdots \\ + \cdots + \sum_{x=(p^\alpha-1)p^{n-\alpha}}^{p^n-1} e\left(\frac{Sx^k}{p^{n-\alpha}}\right). \end{aligned} \tag{2.3}$$

As $e\left(\frac{\cdot}{p^n}\right)$ is periodic modulo p^n, we have $e\left(\frac{(x+p^{n-\alpha})^k}{p^{n-\alpha}}\right) = e\left(\frac{x^k}{p^{n-\alpha}}\right)$. Hence, for each sum in (2.3), we can re-index as many times as necessary by $x \mapsto x + p^{n-\alpha}$. This will result in p^α copies of the sum $\displaystyle\sum_{x=0}^{p^{n-\alpha}-1} e\left(\frac{Sx^k}{p^{n-\alpha}}\right)$, yielding the statement of the proposition. □

Corollary 2.1. *Let $\alpha \in \mathbb{N}_0$. Then for $k \in \mathbb{N}$ we have*

$$\sum_{x=0}^{2^n-1} e\left(\frac{S2^\alpha x^k}{2^n}\right) = \begin{cases} 2^n & \text{if } \alpha \geq n \\ 0 & \text{if } 1 = n - \alpha \\ 2^\alpha \displaystyle\sum_{x=0}^{2^{n-\alpha}-1} e\left(\frac{Sx^k}{2^{n-\alpha}}\right) & \text{if } 2 \leq n - \alpha. \end{cases}$$

Proof. We take $p = 2$ in Proposition 2.3 and note that

$$\sum_{x=0}^{1} e\left(\frac{Sx^k}{2}\right) = 0.$$

□

Corollary 2.2. *Let $\alpha \in \mathbb{N}_0$. Then for any prime p we have*

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\alpha x}{p^n}\right) = \begin{cases} p^n & \text{if } \alpha \geq n \\ 0 & \text{if } \alpha < n. \end{cases}$$

Proof. This follows by taking $k = 1$ in Proposition 2.3, and subsequently deducing the results for $\alpha < n$ from Proposition 2.1. □

2.3 Residues and Congruences

Proposition 2.4. *Let $a, b \in \mathbb{Z}$. If $m \leq n$, then $p^m a \equiv b \pmod{p^n}$ implies $p^m \mid b$ and $a \equiv \dfrac{b}{p^m} \pmod{p^{n-m}}$.*

Proof. Suppose $p^m a \equiv b \pmod{p^n}$. Then there exists some integer q such that $p^m a - b = p^n q$. Hence, we manipulate this equation to find $b = p^m (a - p^{n-m} q)$, and so $p^m \mid b$. Thus, we may write $\dfrac{b}{p^m} = c$ for some integer c. We have that $p^n q = p^m (a - c)$ which means $p^{n-m} q = a - c$ and so $a \equiv c \pmod{p^{n-m}}$. □

We emphasize that Proposition 2.4 is valid for all primes p.

Proposition 2.5. *Suppose that the set of integers $\{r_1, \ldots, r_n\}$ forms a complete system of residues modulo n and $\{s_1, \ldots, s_{\phi(n)}\}$ forms a reduced system of residues modulo n. If $a \in \mathbb{Z}$ is such that $(a, n) = 1$, then for any $b \in \mathbb{Z}$, we have that*

$$\{ar_1 + b, ar_2 + b, \ldots, ar_n + b\}$$

is a complete system of residues modulo n and

$$\{as_1, as_2, \ldots, as_{\phi(n)}\}$$

is a reduced system of residues modulo n.

Proof. First, we observe that by the pigeon-hole principle, any set of n incongruent integers forms a complete system of residues modulo n. Hence, suppose that for some $1 \leq j, k \leq n$, we have that $ar_j + b \equiv ar_k + b \pmod{n}$. But this implies $ar_j \equiv ar_k \pmod{n}$. As $(a, n) = 1$, we have $a \in \mathbb{Z}_n^*$ and hence a^{-1} exists modulo n. Thus, we deduce that $r_j \equiv r_k \pmod{n}$. But as the elements $r_1, \ldots, r_n$ are all incongruent, we must have that $j = k$. Thus, we have shown that $\{ar_1 + b, \ldots, ar_n + b\}$ contains a set of n incongruent integers and so this set comprises a complete system of residues modulo n.

In a similar fashion, a set of $\phi(n)$ incongruent integers, each of which is coprime to n, forms a reduced system of residues modulo n. If we suppose for some $1 \leq j, k \leq \phi(n)$ we have $as_j \equiv as_k \pmod{n}$, then as $(a, n) = 1$ it will follow that $s_j \equiv s_k \pmod{n}$ and hence $\{as_1, \ldots, as_{\phi(n)}\}$ will be a set of $\phi(n)$ incongruent residues, each coprime to n. □

Proposition 2.6 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_n$ be pairwise relatively prime integers. Then the system of congruences*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \ldots, \quad x \equiv a_r \pmod{m_n}$$

has a unique solution modulo $M = \prod_{i=1}^{n} m_i$.

Proof. Set $M_j = \dfrac{M}{m_j}$ for $j = 1, \ldots, n$ and observe that $(M_j, m_j) = 1$. Thus, for each $j = 1, \ldots, n$, there exists some element $b_j \in \mathbb{Z}_{m_j}^*$ such that $b_j M_j \equiv 1 \pmod{m_j}$. We set

$$x = \sum_{j=1}^{n} a_j b_j M_j.$$

Hence, for arbitrary k satisfying $1 \leq k \leq n$ we have

$$x \equiv \sum_{j=1}^{n} a_j b_j M_j \pmod{m_k} \rightarrow x \equiv a_k \pmod{m_k}.$$

It remains to show x is unique modulo M. Suppose y also satisfies $y \equiv a_j \pmod{m_j}$ for $j = 1, \ldots, n$. Then we have $x \equiv y \pmod{m_j}$ which means $m_j \mid (x - y)$ for each $j = 1, \ldots, n$. It follows that $M \mid (x - y)$ and so $x \equiv y \pmod{M}$ which shows x is unique with respect to M. □

2.4 Quadratic Residues

Definition 2.1. Let $q \in \mathbb{N}$ and let $t \in \mathbb{Z}$ be such that $(q, t) = 1$. If there exists some integer x such that $x^2 \equiv t \pmod{q}$, then t is called a quadratic residue modulo q. If no such integer x exists, then t is called a quadratic non-residue modulo q.

As the quadratic Gauss sum is intricately linked with quadratic residues, we present a basic proposition concerning such residues.

Proposition 2.7. *Let p be an odd prime. Then there are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues modulo p. Further, the quadratic residues are given by the residue classes $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.*

Proof. First, note that the numbers

$$1,\ 2,\ \ldots,\ \frac{p-1}{2}$$

are all distinct modulo p. Thus, suppose $1 \leq x, y \leq \frac{p-1}{2}$ and $x^2 \equiv y^2 \pmod{p}$. In this case, this means that

$$(x - y)(x + y) \equiv 0 \pmod{p}.$$

But $2 \leq x + y \leq p - 1$ which means we must have $x - y \equiv 0 \pmod{p}$ which implies $x = y$. Hence, this means that the residues

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 \tag{2.4}$$

are all distinct modulo p. Further, if $1 \leq x \leq \dfrac{p-1}{2}$ then $(p-x)^2 \equiv x^2 \pmod{p}$ and so every quadratic residue modulo p is given by exactly one number in (2.4). Thus, it follows that there are exactly $\dfrac{p-1}{2}$ quadratic residues and hence, there are $\dfrac{p-1}{2}$ quadratic non-residues. □

For an odd prime p, the structure of the quadratic residues will be multiplicative in various ways. This structure is generalized in the Legendre, Jacobi and Kronecker symbols.

Definition 2.2. For p an odd prime and $t \in \mathbb{Z}$ we let $\left(\dfrac{t}{p}\right)$ denote the Legendre symbol, given by

$$\left(\frac{t}{p}\right) = \begin{cases} 0 & \text{if } p \mid t \\ 1 & \text{if } t \text{ is a quadratic residue modulo } p \\ -1 & \text{if } t \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Definition 2.3. Suppose q is an odd positive integer, such that $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ for distinct primes $p_1, \ldots, p_k$ and positive integers $\alpha_1, \ldots, \alpha_k$. Then we let $\left(\dfrac{t}{q}\right)$ denote the Jacobi symbol, which is given by

$$\left(\frac{t}{q}\right) = \left(\frac{t}{p_1^{\alpha_1}}\right)\left(\frac{t}{p_2^{\alpha_2}}\right)\cdots\left(\frac{t}{p_k^{\alpha_k}}\right) = \left(\frac{t}{p_1}\right)^{\alpha_1}\left(\frac{t}{p_2}\right)^{\alpha_2}\cdots\left(\frac{t}{p_k}\right)^{\alpha_k}.$$

Definition 2.4. Let q be a non-zero integer such that $q = u2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where u denotes the sign of q, $\alpha \in \mathbb{N}_0$, $p_1, \ldots, p_k$ are distinct odd primes and $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Then we let

$\left(\frac{t}{q}\right)$ denote the Kronecker symbol, which is given by

$$\left(\frac{t}{q}\right) = \left(\frac{t}{u}\right)\left(\frac{t}{2}\right)^{\alpha}\prod_{i=1}^{k}\left(\frac{t}{p_i}\right)^{\alpha_i},$$

where $\left(\frac{t}{u}\right) = 1$ when $u = 1$ and

$$\left(\frac{t}{-1}\right) = \begin{cases} 1 & \text{if } t \geq 0 \\ -1 & \text{if } t < 0, \end{cases}$$

and

$$\left(\frac{t}{2}\right) = \begin{cases} 0 & \text{if } t \equiv 0 \pmod 2 \\ \left(\frac{2}{|t|}\right) & \text{if } t \equiv 1 \pmod 2. \end{cases}$$

In this thesis, we will only have occasion to evaluate the Kronecker symbol for odd integers q. We now present some basic properties of the Legendre and Jacobi symbols.

Proposition 2.8 (Euler's Criterion)**.** *For p an odd prime, we have that*

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

Proof. If $p \mid t$ then the result holds. Hence, we may assume $(t, p) = 1$. Suppose first that t is a quadratic residue, and that y is an integer such that $y^2 \equiv t \pmod p$. Then

$$t^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1 \pmod p.$$

In particular, as the polynomial $x^{\frac{p-1}{2}} - 1$ has at most $\frac{p-1}{2}$ solutions, we see that the congruence $x^{\frac{p-1}{2}} \equiv 1 \pmod p$ is satisfied by the quadratic residues of p. Hence, if t is a quadratic non-

residue, we must have that $t^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Thus, as $t^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$, we must have that $t^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. The result will follow by Definition 2.2. □

Proposition 2.9. *Let p be an odd prime and let $a, b \in \mathbb{Z}$. Then*

(a) if $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,

(c) if $(a, p) = 1$ then $\left(\frac{a^2}{p}\right) = 1$,

(d) if $(a, p) = 1$ then $\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right)$,

(e) $\sum_{x=1}^{p-1} \left(\frac{x}{p}\right) = 0$.

Proof. Part (a) is clear whenever at least one of $a, b \equiv 0 \pmod{p}$. Hence, we may assume $(ab, p) = 1$. Clearly, as $a \equiv b \pmod{p}$, the residuacity of a will be equal to that of b, which shows part (a). For part (b), in a similar fashion, we may assume $(ab, p) = 1$. Then, from Euler's criterion, we have

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

As we have a congruence of units, it follows that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Part (c) is clear from the definition. For part (d), we use parts (b) and (c), so that

$$\left(\frac{a^{-1}}{p}\right) = \left(\frac{a^2}{p}\right)\left(\frac{a^{-1}}{p}\right) = \left(\frac{a}{p}\right).$$

Finally, for part (e), by Proposition 2.7, it follows that

$$\sum_{x=1}^{p-1} e\left(\frac{x}{p}\right) = \sum_{\left(\frac{x}{p}\right)=1}^{p-1} 1 - \sum_{\left(\frac{x}{p}\right)=-1}^{p-1} 1 = \frac{p-1}{2} - \left(\frac{p-1}{2}\right) = 0.$$

□

Proposition 2.10. *If p is an odd prime, then* $(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)$.

Proof. From Euler's criterion, we have that $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. As $\left(\frac{-1}{p}\right)$ is either 1 or -1, this congruence will become an equality. □

Proposition 2.11. *If p is an odd prime, then*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

Proof. Consider the following congruences:

$$\begin{aligned} p - 1 &\equiv 1(-1)^1 \pmod{p} \\ 2 &\equiv 2(-1)^2 \pmod{p} \\ p - 3 &\equiv 3(-1)^3 \pmod{p} \\ 4 &\equiv 4(-1)^4 \pmod{p} \\ &\vdots \\ r &\equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \pmod{p}, \end{aligned}$$

where r is either $p - \frac{p-1}{2}$ or $\frac{p-1}{2}$ depending on the residue of p modulo 4. We take the product of these congruences to obtain

$$\begin{aligned} 2 \cdot 4 \cdots (p-1) &\equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}} \pmod{p} \\ 2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &\equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{(p-1)(p+1)}{8}} \pmod{p} \\ 2^{\frac{p-1}{2}} &\equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}. \end{aligned}$$

From Euler's criterion we therefore have $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}$ and as each expression

is ± 1, equality will follow. The final equality of the proposition will follow as $\frac{(\pm 3)^2 - 1}{8}$ is odd and $\frac{(\pm 1)^2 - 1}{8}$ is even. $\square$

Proposition 2.12 (The Law of Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

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

We present a proof of this in the next chapter. The law of quadratic reciprocity is a very deep theorem, with over two hundred fifty proofs; see [73]. Our proof will depend on the evaluation of the quadratic Gauss sum. At the moment, we generalize some of our above propositions for arbitrary odd positive integers.

Proposition 2.13. *If P is an odd positive integer, then* $(-1)^{\frac{P-1}{2}} = \left(\frac{-1}{P}\right)$.

Proof. Let $P = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ for distinct odd primes $p_1, \ldots, p_k$ and $\alpha_i \in \mathbb{N}$ for $i = 1, \ldots, k$. Then by Proposition 2.10, and the definition of the Jacobi symbol, we have

$$\begin{aligned}\left(\frac{-1}{P}\right) &= \left(\frac{-1}{p_1}\right)^{\alpha_1} \cdots \left(\frac{-1}{p_k}\right)^{\alpha_k} \\ &= (-1)^{\alpha_1\left(\frac{p_1-1}{2}\right)+\cdots+\alpha_k\left(\frac{p_k-1}{2}\right)}. \end{aligned} \tag{2.5}$$

We may write $P = (1 + (p_1 - 1))^{\alpha_1} \cdots (1 + (p_k - 1))^{\alpha_k}$. We examine the j^{th} factor modulo 4. As p_j is odd, we have

$$(1 + (p_j - 1))^{\alpha_j} \equiv \begin{cases} 1 \pmod 4 & \text{if } p_j \equiv 1 \pmod 4 \text{ or } \alpha_j \equiv 0 \pmod 2 \\ 3 \pmod 4 & \text{if } p_j \equiv 3 \pmod 4 \text{ and } \alpha_j \equiv 1 \pmod 2 \end{cases}$$

$$\equiv 1 + \alpha_j(p_j - 1) \pmod 4.$$

Further, as $p_j - 1$ is even, we have

$$(1 + \alpha_i(p_i - 1))(1 + \alpha_j(p_j - 1)) \equiv 1 + \alpha_i(p_i - 1) + \alpha_j(p_j - 1) \pmod 4.$$

Hence, we deduce that

$$\begin{aligned} P &\equiv \prod_{i=1}^{k}(1 + \alpha_j(p_j - 1)) \pmod 4 \\ &\equiv 1 + \alpha_1(p_1 - 1) + \ldots + \alpha_k(p_k - 1) \pmod 4, \end{aligned}$$

which, by Proposition 2.4, implies that

$$\frac{P-1}{2} \equiv \alpha_1 \left(\frac{p_1 - 1}{2}\right) + \ldots + \alpha_k \left(\frac{p_k - 1}{2}\right) \pmod 2.$$

Substituting this congruence into (2.5) yields the statement of the proposition. □

Proposition 2.14 (The General Law of Quadratic Reciprocity)**.** *Let P and Q be odd, positive integers which are coprime. Then*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right)}.$$

Proof. Suppose $P = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$ and $Q = q_1^{\beta_1} \cdots q_n^{\beta_n}$, for distinct odd primes p_i, q_j and positive integers α_i, β_j for $i = 1, \ldots, m$ and $j = 1, \ldots, n$. Then from Proposition 2.12 and the definition of the Jacobi symbol, we have

$$\begin{aligned} \left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) &= \prod_{i=1}^{m}\prod_{j=1}^{n}\left(\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right)^{\alpha_i\beta_j} \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}\left((-1)^{\left(\frac{p_i-1}{2}\right)\cdot\left(\frac{q_j-1}{2}\right)}\right)^{\alpha_i\beta_j} \\ &= \prod_{i=1}^{m}\prod_{j=1}^{n}(-1)^{\left(\frac{\alpha_i(p_i-1)}{2}\right)\cdot\left(\frac{\beta_j(q_j-1)}{2}\right)} \end{aligned}$$

$$= (-1)^{\sum_{1\leq i\leq m}\sum_{1\leq j\leq n}\left(\frac{\alpha_i(p_i-1)}{2}\right)\cdot\left(\frac{\beta_j(p_j-1)}{2}\right)}$$
$$= (-1)^{\sum_{1\leq i\leq m}\frac{\alpha_i(p_i-1)}{2}\sum_{1\leq j\leq n}\frac{\beta_j(q_j-1)}{2}} \tag{2.6}$$

As in the proof of Proposition 2.13, we see that

$$\frac{P-1}{2} \equiv \sum_{i=1}^{m} \frac{\alpha_i(p_i-1)}{2} \pmod 2$$

and

$$\frac{Q-1}{2} \equiv \sum_{j=1}^{n} \frac{\beta_j(q_j-1)}{2} \pmod 2.$$

Hence, substituting these congruences into (2.6) yields the statement of the general law of quadratic reciprocity. □

2.5 Unit Expressions

The evaluation of our main results and its applications will involve various imaginary unit expressions. We determine some of these expressions to aid in our exposition.

Proposition 2.15. *Let $n \in \mathbb{N}$ be odd. Then*

$$i^{\left(\frac{n-1}{2}\right)^2} = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 4 \\ i & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Proof. We see that

$$\frac{n-1}{2} \equiv \begin{cases} 0 \pmod 2 & \text{if } n \equiv 1 \pmod 4 \\ 1 \pmod 2 & \text{if } n \equiv 3 \pmod 4. \end{cases}$$

Then $0^2 \equiv 2^2 \equiv 0 \pmod 4$ and $1^2 \equiv 3^2 \equiv 1 \pmod 4$ and we deduce the statement of the

proposition. □

In particular, if p is an odd prime, we have that

$$i^{\left(\frac{p^n-1}{2}\right)^2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \text{ or } n \equiv 0 \pmod 2 \\ i & \text{if } p \equiv 3 \pmod 4 \text{ and } n \equiv 1 \pmod 2. \end{cases}$$

Hence, we see that if m is any even integer, $i^{\left(\frac{p^{n\pm m}-1}{2}\right)^2} = i^{\left(\frac{p^n-1}{2}\right)^2}$. When evaluating this imaginary unit expression, we are primarily concerned with the parity of the exponent of p. Thus, for an arbitrary integer m, we may write $i^{\left(\frac{p^{n+m}-1}{2}\right)^2}$ instead of $i^{\left(\frac{p^{n-m}-1}{2}\right)^2}$.

Proposition 2.16. *Let p be an odd prime and let $m, n \in \mathbb{N}$. Then*

$$i^{\left(\frac{p^n-1}{2}\right)^2} i^{\left(\frac{p^{n+m}-1}{2}\right)^2} = \left(\frac{-1}{p}\right)^{(m+1)n} i^{\left(\frac{p^m-1}{2}\right)^2}.$$

Proof. If m is even, from Propositions 2.13 and 2.15, we see that

$$\begin{aligned} i^{\left(\frac{p^n-1}{2}\right)^2} i^{\left(\frac{p^{n+m}-1}{2}\right)^2} &= (-1)^{\left(\frac{p^n-1}{2}\right)^2} = (-1)^{\left(\frac{p^n-1}{2}\right)} = \left(\frac{-1}{p}\right)^n \\ &= \left(\frac{-1}{p}\right)^{(m+1)n} i^{\left(\frac{p^m-1}{2}\right)^2}. \end{aligned}$$

Otherwise, if m is odd, then

$$\begin{aligned} i^{\left(\frac{p^n-1}{2}\right)^2} i^{\left(\frac{p^{n+m}-1}{2}\right)^2} &= \begin{cases} i^{\left(\frac{p^n-1}{2}\right)^2} & \text{if } n \equiv 1 \pmod 2 \\ i^{\left(\frac{p^m-1}{2}\right)^2} & \text{if } n \equiv 0 \pmod 2 \end{cases} \\ &= i^{\left(\frac{p^m-1}{2}\right)^2} = \left(\frac{-1}{p}\right)^{(m+1)n} i^{\left(\frac{p^m-1}{2}\right)^2}. \end{aligned}$$

□

The following definition will be useful when considering Gauss sums with even prime

power modulus.

Definition 2.5. For any integer t, we define the integer parity function $\mathbb{O} : \mathbb{Z} \to \{0, 1\}$ by

$$\mathbb{O}(t) = \frac{(1 + (-1)^t)}{2} = \begin{cases} 1 & \text{if } t \text{ even} \\ 0 & \text{if } t \text{ odd.} \end{cases}$$

This function will have a number of basic properties due to the structure of residues modulo 2.

Proposition 2.17. *Let $m, t \in \mathbb{Z}$. Then $\mathbb{O}$ has the following properties.*

(a) $\mathbb{O}(t+1) = \begin{cases} 1 & \text{if } t \equiv 1 \pmod 2 \\ 0 & \text{if } t \equiv 0 \pmod 2, \end{cases}$

(b) $\mathbb{O}(t+m) = \begin{cases} 1 & \text{if } t \equiv m \pmod 2 \\ 0 & \text{if } t \not\equiv m \pmod 2, \end{cases}$

(c) $\mathbb{O}(t) = \mathbb{O}(t + 2m)$,

(d) $\mathbb{O}(t - m) = \mathbb{O}(t + m)$,

(e) $\mathbb{O}(-t) = \mathbb{O}(t)$.

Proof. Part (a) follows from the definition. We see that $t + m \equiv 0 \pmod 2$ if and only if $t \equiv m \pmod 2$, and so part (b) follows from part (a). Parts (c), (d) and (e) will follow as it is clear that $\mathbb{O}$ is periodic modulo 2. □

Proposition 2.18. *If A is any odd integer, we have*

$$i^{\frac{A}{2}} = 2^{-\frac{1}{2}} \left(\frac{2}{A}\right) (1 + i^A).$$

Proof. Observe that $i^{\frac{1}{2}} = \dfrac{(1+i)}{2^{\frac{1}{2}}}$. Hence,

$$
\begin{aligned}
i^{\frac{A}{2}} &= 2^{\frac{-A}{2}}(1+i)^A = 2^{\frac{-A}{2}} \begin{cases} (-4)^{4\left(\frac{A-1}{4}\right)}(1+i) & \text{if } A \equiv 1 \pmod 4 \\ (-4)^{4\left(\frac{A-3}{4}\right)}(1+i)^3 & \text{if } A \equiv 3 \pmod 4 \end{cases} \\
&= 2^{\frac{-A}{2}} \begin{cases} (-1)^{\frac{A-1}{4}} 2^{\frac{A-1}{2}}(1+i) & \text{if } A \equiv 1 \pmod 4 \\ (-1)^{\frac{A-3}{4}} 2^{\frac{A-3}{4}}(2i)(1+i) & \text{if } A \equiv 3 \pmod 4 \end{cases} \\
&= 2^{\frac{-A}{2}} \begin{cases} (-1)^{\frac{A-1}{4}} 2^{\frac{A-1}{2}}(1+i) & \text{if } A \equiv 1 \pmod 4 \\ (-1)^{\frac{A-3}{4}} 2^{\frac{A-1}{2}}(i-1) & \text{if } A \equiv 3 \pmod 4 \end{cases} \\
&= 2^{\frac{-1}{2}} \begin{cases} (-1)^{\frac{A-1}{4}}(1+i) & \text{if } A \equiv 1 \pmod 4 \\ (-1)^{\frac{A+1}{4}}(1-i) & \text{if } A \equiv 3 \pmod 4 \end{cases} \\
&= 2^{\frac{-1}{2}}(1+i^A) \begin{cases} (-1)^{\frac{A-1}{4}} & \text{if } A \equiv 1 \pmod 4 \\ (-1)^{\frac{A+1}{4}} & \text{if } A \equiv 3 \pmod 4. \end{cases}
\end{aligned}
$$

The result follows now by Proposition 2.11 and considering the possible values of A modulo 8.

□

Proposition 2.19. *Let A and B be odd integers. Then*

$$(1+i^A)(1+i^{AB}) = 2i^{A\left(\frac{B+1}{2}\right)^2}$$

and

$$(1-i^A)(1-i^{AB}) = 2(-1)^{\frac{B+1}{2}} i^{A\left(\frac{B+1}{2}\right)^2}.$$

Proof. We have

$$(1+i^A)(1+i^{AB}) = \begin{cases} 2i & \text{if } A \equiv B \equiv 1 \pmod 4 \\ 2 & \text{if } A \equiv 1 \pmod 4, B \equiv 3 \pmod 4 \\ -2i & \text{if } A \equiv 3 \pmod 4, B \equiv 1 \pmod 4 \\ 2 & \text{if } A \equiv B \equiv 3 \pmod 4. \end{cases}$$

Hence, when $B \equiv 1 \pmod 4$, the product $(1+i^A)(1+i^{AB})$ is imaginary, with the sign corresponding to the residue of A modulo 4. Thus, with Proposition 2.15, we deduce the statement of the proposition for this product. For the remaining equation of the proposition, we let $A \mapsto -A$ in $2i^{A\left(\frac{B+1}{2}\right)^2}$ to arrive at the desired result. □

Proposition 2.20. *Let A, B and C be arbitrary odd integers. Then*

$$(1+i^{AB})(1+i^{AC}) = 2i^{AB\left(\frac{B+C}{2}\right)^2}$$

and

$$(1-i^{AB})(1-i^{AC}) = 2(-1)^{\frac{B+C}{2}} i^{AB\left(\frac{B+C}{2}\right)^2}.$$

Proof. If $A \equiv 1 \pmod 4$, we have

$$(1+i^{AB})(1+i^{AC}) = (1+i^B)(1+i^C) = \begin{cases} 2i & \text{if } B \equiv C \equiv 1 \pmod 4 \\ 2 & \text{if } B \not\equiv C \pmod 4 \\ -2i & \text{if } B \equiv C \equiv 3 \pmod 4. \end{cases}$$

Similarly, if $A \equiv 3 \pmod 4$, we have

$$(1+i^{AB})(1+i^{AC}) = (1-i^B)(1-i^C) = \begin{cases} -2i & \text{if } B \equiv C \equiv 1 \pmod 4 \\ 2 & \text{if } B \not\equiv C \pmod 4 \\ 2i & \text{if } B \equiv C \equiv 3 \pmod 4. \end{cases}$$

Our results will follow now in a similar manner as in the proof of Proposition 2.19. □

Proposition 2.21. *Let A and B be arbitrary odd integers. Then*

$$1 - i^A - i^B - i^{A+B} = 2(1-i^A)\mathbb{O}\left(\frac{A-B}{2}\right).$$

Proof. We see first that if $A \not\equiv B \pmod 4$, then $1 - i^A - i^B - i^{A+B} = 0$. Hence, assuming $A \equiv B \pmod 4$, we have $A + B \equiv 2 \pmod 4$ so that $1 - i^A - i^B - i^{A+B} = 2(1 - i^A)$. The proposition now follows as $\mathbb{O}(\frac{A-B}{2}) = 1$ if and only if $A \equiv B \pmod 4$. □

Chapter 3

Gauss and Quadratic Exponential Sums

The purpose of this section is to examine the quadratic Gauss sum. We will look at some basic properties that arise due to its structure.

3.1 The Quadratic Gauss Sum

Theorem 3.1 (The Quadratic Gauss Sum)**.** *Let $q \in \mathbb{N}$. Then for any integer S coprime to q, we have*

$$G(S;q) = \begin{cases} \left(\frac{S}{q}\right) q^{\frac{1}{2}} & \text{if } q \equiv 1 \pmod 4 \\ 0 & \text{if } q \equiv 2 \pmod 4 \\ i\left(\frac{S}{q}\right) q^{\frac{1}{2}} & \text{if } q \equiv 3 \pmod 4 \\ (1+i^S)\left(\frac{q}{S}\right) q^{\frac{1}{2}} & \text{if } q \equiv 0 \pmod 4. \end{cases}$$

Note that in $G(S;q)$, we refer to q as the modulus of the quadratic Gauss sum. Due to the limit of our scope, we avoid a rigorous proof of the above theorem. In addition to the wide variety of proofs mention in the introduction, one can see the book by Berndt, Evans and Williams [12, pp. 18-28] for an elementary proof of Theorem 3.1.

Proposition 3.1. *Let $m, n \in \mathbb{N}$ be such that $(m,n) = 1$ and let t be an arbitrary integer.*

Then we have

$$G(t; mn) = G(tm; n)G(tn; m).$$

Proof. Observe that

$$(mx)^2 + (ny)^2 \equiv (mx + ny)^2 \pmod{mn}.$$

Further, as $(m, n) = 1$, by the Chinese remainder theorem, there exists a unique integer $z \pmod{mn}$ such that $z \equiv mx \pmod{n}$ and $z \equiv ny \pmod{m}$, for arbitrary $x \in \mathbb{Z}_n$ and $y \in \mathbb{Z}_m$. Thus, as x runs through a complete residue system modulo n and as y runs through a complete residue system modulo m, z will run through a complete residue system modulo mn. Thus, we have that

$$\begin{aligned} G(tm; n)G(tn; m) &= \sum_{x=0}^{n-1} e\left(\frac{tmx^2}{n}\right) \sum_{y=0}^{m-1} e\left(\frac{tny^2}{m}\right) \\ &= \sum_{x=0}^{n-1} \sum_{y=0}^{m-1} e\left(\frac{t((mx)^2 + (ny)^2)}{mn}\right) \\ &= \sum_{x=0}^{n-1} \sum_{y=0}^{m-1} e\left(\frac{t(mx + ny)^2}{mn}\right) \\ &= \sum_{z=0}^{mn-1} e\left(\frac{tz^2}{mn}\right) = G(t; mn). \end{aligned}$$

□

With this we may present a proof of quadratic reciprocity.

Proof of Proposition 2.12. Let p and q be distinct odd primes. Then by Theorem 3.1 and Proposition 3.1 we have

$$G(1; pq) = G(p; q)G(q; p) = \left(\frac{p}{q}\right) i^{\left(\frac{q-1}{2}\right)^2} q^{\frac{1}{2}} \left(\frac{q}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} p^{\frac{1}{2}}$$

$$= \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)(pq)^{\frac{1}{2}} i^{\left(\frac{q-1}{2}\right)^2} i^{\left(\frac{p-1}{2}\right)^2}. \tag{3.1}$$

From Proposition 2.15 and Theorem 3.1 we have

$$G(1;pq) = i^{\left(\frac{pq-1}{2}\right)^2}(pq)^{\frac{1}{2}}. \tag{3.2}$$

By equating (3.1) and (3.2), we see that

$$i^{\left(\frac{pq-1}{2}\right)^2} = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) i^{\left(\frac{q-1}{2}\right)^2} i^{\left(\frac{p-1}{2}\right)^2} \tag{3.3}$$

Observe that if $p \equiv q \pmod 4$ then $pq \equiv 1 \pmod 4$. Similarly, if $p \not\equiv q \pmod 4$ then $pq \equiv 3 \pmod 4$. Hence, if $p \equiv q \equiv 1 \pmod 4$ or $p \not\equiv q \pmod 4$, we have $i^{\left(\frac{pq-1}{2}\right)^2} = i^{\left(\frac{p-1}{2}\right)^2} i^{\left(\frac{q-1}{2}\right)^2}$. Thus, for these cases, (3.3) is given by

$$1 = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right). \tag{3.4}$$

Otherwise, if $p \equiv q \equiv 3 \pmod 4$, then (3.3) will reduce to

$$-1 = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right). \tag{3.5}$$

As $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ if and only if $p \equiv q \equiv 3 \pmod 4$, from (3.4) and (3.5) we deduce that

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

□

3.2 Simplification Properties of Gauss Sums

Due to the structure of the quadratic Gauss sum, there will be some basic cancellation properties which we review here.

Proposition 3.2 (The Reduction Property)**.** *Let $\alpha \in \mathbb{N}_0$. Then for any prime p, we have*

$$G(Sp^\alpha; p^n) = \begin{cases} p^n & \text{if } \alpha \geq n \\ p^\alpha \cdot G(S; p^{n-\alpha}) & \text{if } \alpha < n. \end{cases}$$

Proof. This follows by setting $k = 2$ in Proposition 2.3. □

In particular, for any prime p and any $\alpha \in \mathbb{N}_0$, we have that

$$G(S; p^n) = \frac{1}{p^\alpha} G(Sp^\alpha; p^{n+\alpha}). \tag{3.6}$$

For the remainder of this chapter, we will assume that p is an odd prime. We examine how the quadratic Gauss sum will act when its index is restricted to certain residues with respect to its modulus. As such, we will consider odd prime power moduli and even prime power moduli in turn.

Proposition 3.3. *Suppose that $\alpha \in \mathbb{N}_0$ is such that $2\alpha \leq n$. Then for $w \in \mathbb{Z}$, we have*

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{p^\alpha} \\ G(S; p^n) & \text{if } w \equiv 0 \pmod{p^\alpha}. \end{cases}$$

Proof. We have that

$$\begin{aligned} \sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right) &= \sum_{x=0}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right) \frac{1}{p^\alpha} \sum_{y=0}^{p^\alpha-1} e\left(\frac{y(x-w)}{p^\alpha}\right) \\ &= \frac{1}{p^\alpha} \sum_{y=0}^{p^\alpha-1} e\left(\frac{-wy}{p^\alpha}\right) \sum_{x=0}^{p^n-1} e\left(\frac{Sx^2}{p^n} + \frac{yx}{p^\alpha}\right) \end{aligned}$$

$$= \frac{1}{p^\alpha} \sum_{y=0}^{p^\alpha - 1} e\left(\frac{-wy}{p^\alpha}\right) \sum_{x=0}^{p^n-1} e\left(\frac{Sx^2 + p^{n-\alpha}yx}{p^n}\right). \tag{3.7}$$

As $(S, p) = 1$ and p is odd, there exists some integer T such that $2ST \equiv 1 \pmod{p^n}$. Hence, (3.7) becomes

$$\frac{1}{p^\alpha} \sum_{y=0}^{p^\alpha - 1} e\left(\frac{-wy}{p^\alpha}\right) \sum_{x=0}^{p^n-1} e\left(\frac{S(x^2 + 2Tp^{n-\alpha}yx)}{p^n}\right). \tag{3.8}$$

Observe that

$$x^2 + 2Tp^{n-\alpha}yx = (x + p^{n-\alpha}Ty)^2 - p^{2(n-\alpha)}T^2y^2.$$

As $2\alpha \leq n$, we have $e\left(\frac{-p^{2(n-\alpha)}T^2y^2}{p^n}\right) = 1$. Hence, with Proposition 2.5, (3.8) becomes

$$\frac{1}{p^\alpha} \sum_{y=0}^{p^\alpha - 1} e\left(\frac{-wy}{p^\alpha}\right) \sum_{x=0}^{p^n-1} e\left(\frac{S(x + p^{n-\alpha}Ty)^2}{p^n}\right) = \frac{G(S; p^n)}{p^\alpha} \sum_{y=0}^{p^\alpha - 1} e\left(\frac{-wy}{p^\alpha}\right).$$

The results will now follow by Proposition 2.1. □

We have a similar proposition for the even prime case.

Proposition 3.4. *Suppose that $\alpha \in \mathbb{N}_0$ is such that $2\alpha + 2 \leq n$. Then for $w \in \mathbb{Z}$, we have*

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{sx^2}{2^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{2^\alpha} \\ G(s; 2^n) & \text{if } w \equiv 0 \pmod{2^\alpha}. \end{cases}$$

Proof. Similar to Proposition 3.3, with (3.7) we deduce that

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{sx^2}{2^n}\right) = \frac{1}{2^\alpha} \sum_{y=0}^{2^\alpha - 1} e\left(\frac{-wy}{2^\alpha}\right) \sum_{x=0}^{2^n-1} e\left(\frac{S(x^2 + 2^{n-\alpha}Txy)}{2^n}\right),$$

where T is an odd integer satisfying $ST \equiv 1 \pmod{2^n}$. As $n \geq 2\alpha + 2$, we may complete the square as before. Thus, it follows that

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{sx^2}{2^n}\right) = \frac{G(S;2^n)}{2^\alpha} \sum_{y=0}^{2^\alpha-1} e\left(\frac{-wy}{2^\alpha}\right),$$

and we deduce the statement of the proposition. □

We mention that Proposition 3.4. is given as Lemma 3.1. in the paper by Alaca, Alaca and Williams [1, pp. 83-85]. There is a similar reduction property to that of Proposition 3.2 for these types of Gauss sums.

Proposition 3.5. *Suppose $\alpha, \beta \in \mathbb{N}_0$ are such that $2\alpha + \beta \leq n$. Then for $w \in \mathbb{Z}$, we have*

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) = p^\beta \sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^{n-\beta}-1} e\left(\frac{Sx^2}{p^{n-\beta}}\right).$$

Proof. As in the proof of Proposition 2.3, we see that

$$\begin{aligned} &\sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) \\ &\qquad = \sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^{n-\beta}-1} e\left(\frac{Sx^2}{p^{n-\beta}}\right) + \cdots + \sum_{\substack{x=(p^\beta-1)p^{n-\beta} \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sx^2}{p^{n-\beta}}\right) \end{aligned} \tag{3.9}$$

Observe that as $n \geq 2\alpha + \beta \geq \alpha + \beta$, we have that

$$x + p^{n-\beta} \equiv w \pmod{p^\alpha} \to x \equiv w \pmod{p^\alpha}.$$

Thus, we reindex each sum by setting $x \mapsto x + p^{n-\beta}$ as many times as necessary. This yields

p^β copies of the first sum in (3.9), that is

$$p^\beta \sum_{\substack{x=0 \\ x\equiv w \pmod{p^\alpha}}}^{p^{n-\beta}-1} e\left(\frac{sx^2}{p^{n-\beta}}\right).$$

□

Proposition 3.6. *Suppose that $\alpha, \beta \in \mathbb{N}_0$ are such that $2\alpha + \beta + 2 \leq n$. Then for $w \in \mathbb{Z}$, we have that*

$$\sum_{\substack{x=0 \\ x\equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{S2^\beta x^2}{2^n}\right) = 2^\beta \sum_{\substack{x=0 \\ x\equiv w \pmod{2^\alpha}}}^{2^{n-\beta}-1} e\left(\frac{Sx^2}{2^{n-\beta}}\right).$$

Proof. The proof is conducted in a similar manner to that of Proposition 3.5. □

We mention that the conditions in Proposition 3.6. were chosen so that we would not run over any quadratic Gauss sums with modulus 2. Hence, by Propositions 3.3 and 3.5, and by Propositions 3.4 and 3.6, we deduce the following corollaries, respectively.

Corollary 3.1. *Suppose $\alpha, \beta \in \mathbb{N}_0$ are such that $2\alpha + \beta \leq n$. Then for $w \in \mathbb{Z}$, we have*

$$\sum_{\substack{x=0 \\ x\equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{p^\alpha} \\ p^\beta G(S; p^{n-\beta}) & \text{if } w \equiv 0 \pmod{p^\alpha}. \end{cases}$$

Corollary 3.2. *Supppose $\alpha, \beta \in \mathbb{N}_0$ are such that $2\alpha + \beta + 2 \leq n$. Then for $w \in \mathbb{Z}$, we have*

$$\sum_{\substack{x=0 \\ x\equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{S2^\beta x^2}{2^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{2^\alpha} \\ 2^\beta G(S; 2^{n-\beta}) & \text{if } w \equiv 0 \pmod{2^\alpha}. \end{cases}$$

We will have occasion to consider Gauss sums of the following forms:

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x+w)^2}{p^n}\right), \quad \sum_{x=0}^{2^n-1} e\left(\frac{S2^\beta(2^\gamma x+w)^2}{2^n}\right) \tag{3.10}$$

and

$$\sum_{\substack{x=0\\ x\equiv w_1 \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x+w_2)^2}{p^n}\right), \quad \sum_{\substack{x=0\\ x\equiv w_1 \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{S2^\beta(2^\gamma x+w_2)^2}{2^n}\right), \tag{3.11}$$

where $\alpha, \beta, \gamma \in \mathbb{N}_0$ and w, w_1 and w_2 are arbitrary integers. We look to mimic the proof of Proposition 3.3 to investigate the necessary restrictions on α, β, γ.

Consider the sum given in (3.10) for an odd prime p. If $\beta \geq n$ then clearly this sum resolves to p^n. Hence, suppose that $\beta < n$. Assume without loss of generality that $0 \leq w < p^\gamma$. We look to reindex (3.10) by setting $y = p^\gamma x + w$. As x runs through a complete residue system modulo p^n, y will obtain its values over the interval $[0, p^{n+\gamma}-1]$. Hence, we see that (3.10) can be written as

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x+w)^2}{p^n}\right) = \sum_{\substack{y=0\\ y\equiv w \pmod{p^\gamma}}}^{p^{n+\gamma}-1} e\left(\frac{Sp^\beta y^2}{p^n}\right). \tag{3.12}$$

Then following the proof of Proposition 3.3, we see that (3.12) becomes

$$\begin{aligned}\sum_{\substack{y=0\\ y\equiv w \pmod{p^\gamma}}}^{p^{n+\gamma}-1} e\left(\frac{Sp^\beta y^2}{p^n}\right) &= \sum_{y=0}^{p^{n+\gamma}-1} e\left(\frac{Sp^\beta y^2}{p^n}\right)\frac{1}{p^\gamma}\sum_{z=0}^{p^\gamma-1} e\left(\frac{z(y-w)}{p^\gamma}\right)\\ &= \frac{1}{p^\gamma}\sum_{z=0}^{p^\gamma-1} e\left(\frac{-wz}{p^\gamma}\right)\sum_{y=0}^{p^{n+\gamma}-1} e\left(\frac{Sy^2}{p^{n-\beta}}+\frac{yz}{p^\gamma}\right).\end{aligned} \tag{3.13}$$

In order to take $p^{n-\beta}$ as a common denominator, we require that $n-\beta \geq \gamma$. Under this

assumption (3.13) becomes

$$\begin{aligned}
&= \frac{1}{p^\gamma} \sum_{z=0}^{p^\gamma-1} e\left(\frac{-wz}{p^\gamma}\right) \sum_{y=0}^{p^{n+\gamma}-1} e\left(\frac{Sy^2 + p^{n-\beta-\gamma}yz}{p^{n-\beta}}\right) \\
&= \frac{1}{p^\gamma} \sum_{z=0}^{p^\gamma-1} e\left(\frac{-wz}{p^\gamma}\right) \sum_{y=0}^{p^{n+\gamma}-1} e\left(\frac{S(y^2 + 2Tp^{n-\beta-\gamma}yz)}{p^{n-\beta}}\right),
\end{aligned} \tag{3.14}$$

where T is some integer such that $2ST \equiv 1 \pmod{p^{n-\beta}}$. We may complete the square given in the innermost sum of (3.14). We have that

$$y^2 + 2p^{n-\beta-\gamma}Tyz = (y + p^{n-\beta-\gamma}Tz)^2 - p^{2(n-\beta-\gamma)}T^2z^2. \tag{3.15}$$

Thus, (3.15) shows that if we have $n \geq 2\gamma + \beta$, we have

$$y^2 + 2p^{n-\beta-\gamma}Tyz \equiv (y + p^{n-\beta-\gamma}Tz)^2 \pmod{p^{n-\beta}}.$$

Under the assumption $n \geq 2\gamma + \beta$, with Propositions 2.5 and 3.2, (3.14) becomes

$$\begin{aligned}
&= \frac{1}{p^\gamma} \sum_{z=0}^{p^\gamma-1} e\left(\frac{-wz}{p^\gamma}\right) \sum_{y=0}^{p^{n+\gamma}-1} e\left(\frac{S(y + 2p^{n-\beta-\gamma}Tz)^2}{p^{n-\beta}}\right) \\
&= \frac{1}{p^\gamma} \sum_{z=0}^{p^\gamma-1} e\left(\frac{-wz}{p^\gamma}\right) p^{\beta+\gamma} \sum_{y=0}^{p^{n-\beta}-1} e\left(\frac{S(y + 2p^{n-\beta-\gamma}Tz)^2}{p^{n-\beta}}\right) \\
&= p^\beta G(S; p^{n-\beta}) \sum_{z=0}^{p^\gamma-1} e\left(\frac{-wz}{p^\gamma}\right) \\
&= \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{p^\gamma} \\ p^{\beta+\gamma} G(S; p^{n-\beta}) & \text{if } w \equiv 0 \pmod{p^\gamma}. \end{cases}
\end{aligned} \tag{3.16}$$

We arrive at (3.16) under the assumptions that n satisfies $n > \beta$ and $n \geq 2\gamma + \beta$. In the

case where $\gamma = 0$, the condition $w \equiv 0 \pmod{p^\gamma}$ is trivially satisfied, and we have

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x + w)^2}{p^n}\right) = \sum_{x=0}^{p^n-1} e\left(\frac{Sp^\beta(x+w)^2}{p^n}\right) = p^\beta G(S; p^{n-\beta}),$$

which holds for $n = \beta$. Thus, with (3.12)-(3.14) and (3.16) we have shown the following proposition.

Proposition 3.7. *Suppose $\beta, \gamma \in \mathbb{N}_0$ are such that $n \geq 2\gamma + \beta$. Then for $w \in \mathbb{Z}$ we have that*

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x + w)^2}{p^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{p^\gamma} \\ p^{\beta+\gamma} G(S; p^{n-\beta}) & \text{if } w \equiv 0 \pmod{p^\gamma}. \end{cases}$$

The even prime case will follow in a similar fashion.

Proposition 3.8. *Suppose $\beta, \gamma \in \mathbb{N}_0$ are such that $n \geq 2\gamma + \beta + 2$. Then for $w \in \mathbb{Z}$, we have that*

$$\sum_{x=0}^{2^n-1} e\left(\frac{S2^\beta(2^\gamma x + w)^2}{2^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{p^\gamma} \\ 2^{\beta+\gamma} G(S; 2^{n-\beta}) & \text{if } w \equiv 0 \pmod{p^\gamma}. \end{cases}$$

Proof. Let T be an integer such that $ST \equiv 1 \pmod{2^{n-\beta}}$. Then as in the proof of Proposition 3.7, we deduce that

$$\sum_{x=0}^{2^n-1} e\left(\frac{S2^\beta(2^\gamma x + w)^2}{2^n}\right) = \frac{1}{2^\gamma} \sum_{z=0}^{2^\gamma-1} e\left(\frac{-wz}{2^\gamma}\right) \sum_{y=0}^{2^{n+\gamma}-1} e\left(\frac{S(y^2 + 2^{n-\beta-\gamma}Tyz)}{2^{n-\beta}}\right). \tag{3.17}$$

In order to complete the square, we require that $n - \beta - \gamma \geq 1$, which follows from $n \geq 2\gamma + \beta + 2$. Hence, we find that

$$y^2 + 2^{n-\beta-\gamma}Tyz = (y + 2^{n-\beta-\gamma-1}Tyz)^2 - 2^{2(n-\beta-\gamma-1)}Tyz.$$

Thus, as $n \geq 2\gamma + \beta + 2$, we see that (3.17) is given by

$$\begin{aligned}\frac{1}{2^\gamma} \sum_{z=0}^{2^\gamma-1} e\left(\frac{-wz}{2^\gamma}\right) \sum_{y=0}^{2^{n+\gamma}-1} e\left(\frac{s(y+2^{n-\beta-\gamma-1}tyz)^2}{2^{n-\beta}}\right) \\ = 2^\beta G(S; 2^{n-\beta}) \sum_{z=0}^{2^\gamma-1} e\left(\frac{-wz}{2^\gamma}\right),\end{aligned}$$

which yields the statement of the proposition. □

We use these same methods to evaluate (3.11).

Proposition 3.9. *Suppose $\alpha, \beta, \gamma \in \mathbb{N}_0$ are such that $n \geq 2(\alpha+\gamma)+\beta$. Then for $w_1, w_2 \in \mathbb{Z}$, we have that*

$$\sum_{\substack{x=0 \\ x \equiv w_1 \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x + w_2)^2}{p^n}\right)$$

$$= \begin{cases} 0 & \text{if } w_2 \not\equiv 0 \pmod{p^\gamma} \\ 0 & \text{if } w_2 \equiv 0 \pmod{p^\gamma} \text{ and } w_1 \not\equiv 0 \pmod{p^\alpha} \\ p^{\beta+2\gamma} G(S; p^{n-\beta-2\gamma}) & \text{if } w_1 \equiv 0 \pmod{p^\gamma} \text{ and } w_1 \equiv 0 \pmod{p^\alpha}. \end{cases}$$

Proof. Similar to the proof of Proposition 3.7, we have that

$$\begin{aligned}\sum_{\substack{x=0 \\ x \equiv w_1 \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x + w_2)^2}{p^n}\right) &= \sum_{x=0}^{p^{n-\alpha}-1} e\left(\frac{Sp^\beta(p^{\alpha+\gamma}x + p^\gamma w_1 + w_2)^2}{p^n}\right) \\ &= \sum_{\substack{x=0 \\ x \equiv p^\gamma w_1 + w_2 \pmod{p^{\alpha+\gamma}}}}^{p^{n+\gamma}-1} e\left(\frac{Sp^\beta x^2}{p^n}\right). \qquad (3.18)\end{aligned}$$

Set $w = p^\gamma w_1 + w_2$ and let T be an integer such that $2ST \equiv 1 \pmod{p^{n-\beta}}$. As $n \geq 2(\alpha+\gamma)+\beta$, we see that we can write (3.18) as

$$\frac{1}{p^{\alpha+\gamma}} \sum_{y=0}^{p^{\alpha+\gamma}-1} e\left(\frac{-yw}{p^{\alpha+\gamma}}\right) \sum_{x=0}^{p^{n+\gamma}-1} e\left(\frac{Sx^2}{p^{n-\beta}} + \frac{xy}{p^{\alpha+\gamma}}\right)$$

$$= \frac{1}{p^{\alpha+\gamma}} \sum_{y=0}^{p^{\alpha+\gamma}-1} e\left(\frac{-yw}{p^{\alpha+\gamma}}\right) \sum_{x=0}^{p^{n+\gamma}-1} e\left(\frac{S(x^2+2Tp^{n-\beta-\alpha-\gamma}xy)}{p^{n-\beta}}\right)$$

$$= \frac{1}{p^{\alpha+\gamma}} \sum_{y=0}^{p^{\alpha+\gamma}-1} e\left(\frac{-yw}{p^{\alpha+\gamma}}\right) \sum_{x=0}^{p^{n+\gamma}-1} e\left(\frac{S(x+p^{n-\beta-\alpha-\gamma}Ty)^2}{p^{n-\beta}}\right)$$

$$= \frac{p^{\beta+\gamma}G(S;p^{n-\beta})}{p^{\alpha+\gamma}} \sum_{y=0}^{p^{\alpha+\gamma}-1} e\left(\frac{-yw}{p^{\alpha+\gamma}}\right). \tag{3.19}$$

Hence, the sum given in (3.19) will be non-zero whenever $w = p^\gamma w_1 + w_2 \equiv 0 \pmod{p^{\alpha+\gamma}}$. Suppose that $w_2 \not\equiv 0 \pmod{p^\gamma}$. Assume, by way of contradiction, that w_1 is some integer satisfying $p^\gamma w_1 + w_2 \equiv 0 \pmod{p^{\gamma+\alpha}}$. But this implies there exists some integer z such that $zp^{\alpha+\gamma} = p^\gamma w_1 + w_2$ which implies $p^\gamma \mid w_2$, a contradiction. Thus, if $w_2 \not\equiv 0 \pmod{p^\gamma}$, $p^\gamma w_1 + w_2 \not\equiv 0 \pmod{p^{\gamma+\alpha}}$ and so (3.19) is zero in this case.

Hence, suppose instead $w_2 \equiv 0 \pmod{p^\gamma}$ and write $w_2 = p^\gamma w_2'$. By Proposition 3.7, as $n \geq 2(\alpha+\gamma)+\beta$, we have that

$$\sum_{\substack{x=0 \\ x\equiv w_1 \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta(p^\gamma x + w_2)^2}{p^n}\right) = \sum_{\substack{x=0 \\ x\equiv w_1 \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^{\beta+2\gamma}(x+w_2')^2}{p^n}\right)$$

$$= \begin{cases} 0 & \text{if } w_1 \not\equiv 0 \pmod{p^\alpha} \\ p^{\beta+2\gamma}G(S;p^{n-\beta-2\gamma}) & \text{if } w_1 \equiv 0 \pmod{p^\alpha}. \end{cases}$$

□

Proposition 3.10. *Suppose $\alpha, \beta, \gamma \in \mathbb{N}_0$ are such that $n \geq 2(\alpha+\gamma)+\beta+2$. Then for $w_1, w_2 \in \mathbb{Z}$ we have*

$$\sum_{\substack{x=0 \\ x\equiv w_1 \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{S2^\beta(2^\gamma x + w_2)^2}{2^n}\right)$$

$$= \begin{cases} 0 & \text{if } w_2 \not\equiv 0 \pmod{2^\gamma} \\ 0 & \text{if } w_2 \equiv 0 \pmod{2^\gamma} \text{ and } w_1 \not\equiv 0 \pmod{2^\alpha} \\ 2^{\beta+2\gamma} G(S; 2^{n-\beta-2\gamma}) & \text{if } w_2 \equiv 0 \pmod{2^\gamma} \text{ and } w_1 \equiv 0 \pmod{2^\alpha}. \end{cases}$$

Proof. The proof follows in the same fashion as Proposition 3.10. □

Proposition 3.11. *For $m \in \mathbb{N}_0$, we have*

(a) $G(S; p^{n+2m}) = p^m \cdot G(S; p^n)$,

(b) if $n > 2m$, $G(S; p^{n-2m}) = \dfrac{1}{p^m} G(S; p^n)$,

(c) if $n > 2m$, $G(Sp^{2m}; p^n) = p^m \cdot G(S; p^n)$,

(d) if $n > 2m$, $G(Sp^{2m}; p^n) = G(S; p^{n+2m})$,

(e) if $n > m$, $p^m G(S; p^{n-m}) = G(S; p^{n+m})$.

Proof. By Theorem 3.1 and Proposition 2.15,

$$\begin{aligned} G(S; p^{n+2m}) &= \left(\frac{S}{p}\right)^{n+2m} i^{\left(\frac{p^{n+2m}-1}{2}\right)^2} p^{\frac{n+2m}{2}} = p^m \left(\frac{S}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} \\ &= p^m G(S; p^n), \end{aligned}$$

which shows (a). For (b), by Theorem 3.1 we see that if $n > 2m$,

$$\begin{aligned} G(S; p^{n-2m}) &= \left(\frac{S}{p}\right)^{n-2m} i^{\left(\frac{p^{n-2m}-1}{2}\right)^2} p^{\frac{n-2m}{2}} = \frac{1}{p^m} \left(\frac{S}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} \\ &= \frac{1}{p^m} G(S; p^n). \end{aligned}$$

Similarly, for (c), if $n > 2m$, then by Proposition 3.2 and part (b) we have

$$G(Sp^{2m}; p^n) = p^{2m} G(S; p^{n-2m}) = p^m G(S; p^n).$$

Part (d) follows immediately by equating (a) and (c). Finally, for part (e), we have

$$p^m G(S;p^{n-m}) = p^m \left(\frac{S}{p}\right)^{n-m} i^{\left(\frac{p^{n-m}-1}{2}\right)^2} p^{\frac{n-m}{2}} = \left(\frac{S}{p}\right)^{n+m} i^{\left(\frac{p^{n+m}-1}{2}\right)^2} p^{\frac{n+m}{2}} = G(S;p^{n+m}).$$

□

We have similar cancellation properties for the even prime case.

Proposition 3.12. *For $m \in \mathbb{N}_0$, we have*

(a) $G(S;2^{n+2m}) = 2^m G(S;2^n)$,

(b) if $n > 2m+1$ *then* $G(S;2^{n-2m}) = \frac{1}{2^m} G(S;2^n)$,

(c) if $n > 2m+1$ *then* $G(S2^{2m};2^n) = 2^m G(S;2^n)$,

(d) if $n > 2m+1$ *then* $G(S2^{2m};2^n) = G(S;2^{n+2m})$,

(e) if $n > m+1$, *then* $2^m G(S;2^{n-m}) = G(S;2^{n+m})$.

Proof. For part (a), by Theorem 3.1, we have

$$G(S;2^{n+2m}) = \left(\frac{2}{S}\right)^{n+2m} \left(1+i^S\right) 2^{\frac{n+2m}{2}} = 2^m G(S;2^n).$$

For part (b), if $n > 2m+1$, then $G(S;2^{n-2m}) \neq 0$ and so by Theorem 3.1 we have

$$G(S;2^{n-2m}) = \left(\frac{2}{S}\right)^{n-2m} (1+i^S) 2^{\frac{n-2m}{2}} = \frac{1}{2^m} G(S;2^n).$$

Similarly, for part (c), if $n > 2m+1$, then by Proposition 3.2 and part (b),

$$G(S2^{2m};2^n) = 2^{2m} G(S;2^{n-2m}) = 2^m G(S;2^n).$$

Part (d) follows from parts (a) and (c). Finally, part (e) is given by

$$2^m G(S;2^{n-m}) = 2^m(1+i^S)\left(\frac{2}{S}\right)^{n-m} 2^{\frac{n-m}{2}} = (1+i^S)\left(\frac{2}{S}\right)^{n+m} 2^{\frac{n+m}{2}} = G(S;2^{n+m}).$$

□

Finally, due to the structure of our Gauss sums, we may make some simplifications for certain coefficients.

Proposition 3.13. *We have*

$$G(S^2;p^n) = G(1;p^n) \quad \textit{and} \quad G(S^{-1};p^n) = G(S;p^n).$$

Proof. From Theorem 3.1, we have

$$G(S^2;p^n) = \left(\frac{S^2}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} = i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} = G(1;p^n).$$

Similarly, we have

$$\begin{aligned} G(S^{-1};p^n) &= \left(\frac{S^{-1}}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} = \left(\frac{S^2}{p}\right)^n \left(\frac{S^{-1}}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} \\ &= \left(\frac{S}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} = G(S;p^n). \end{aligned}$$

□

Proposition 3.14. *We have*

$$G(S^2;2^n) = G(1;2^n) \textit{ and } G(S^{-1};2^n) = G(S;2^n).$$

Proof. Any odd number S satisfies $S^2 \equiv 1 \pmod 4$. Hence, by Theorem 3.1 we have

$$G(S^2;2^n) = \left(\frac{2^n}{S}\right)^2 (1+i^{S^2})2^{\frac{n}{2}} = (1+i)2^{\frac{n}{2}} = G(1;2^n).$$

Similarly, by Theorem 3.1, we have

$$G(S^{-1}; 2^n) = (1 + i^{S^{-1}}) \left(\frac{2}{S^{-1}}\right)^n 2^{\frac{n}{2}}.$$

We observe that $S \equiv S^{-1} \pmod 4$ and so we have $(1 + i^{S^{-1}}) = (1 + i^S)$. Further, any odd number modulo 8 is its own inverse. Hence, by Proposition 2.11, we have $S^{-1} \equiv S \pmod 8$, which means

$$\left(\frac{2}{S^{-1}}\right) = (-1)^{\left(\frac{(S^{-1})^2-1}{8}\right)} = (-1)^{\left(\frac{S^2-1}{8}\right)} = \left(\frac{2}{S}\right),$$

and hence we conclude the statement of the proposition. □

Chapter 4

Diagonalization of a Quadratic Form

It is well known that under certain conditions, an integral quadratic form Q_r can be expressed as a diagonal form $Q_r = \sum_{i=1}^{n} t_i y_i^2$ where $t_i \in \mathbb{Q}$ and $y_i \in \mathbb{Q}[x_i, \ldots, x_r]$; see [27, p. 69]. Our method is to diagonalize a quadratic form in this manner, then multiply both sides of this equation by a common denominator to arrive at an expression with integer coefficients.

4.1 Matrix Notation

For the following two sections, we will use capital letters to denote matrices. For any matrix M, we let M^T denote its transpose. From now on we let M denote an $n \times n$ integral symmetric matrix, and write this as

$$M = \begin{pmatrix} t_{11} & t_{12} & \ldots & t_{1n} \\ t_{21} & t_{22} & & t_{2n} \\ \vdots & & \ddots & \vdots \\ t_{2n} & t_{n2} & \cdots & t_{nn} \end{pmatrix},$$

where $t_{ij} = t_{ji}$ for all $1 \leq i \leq j \leq n$, and due to symmetry we label our elements using the upper triangular notation. For convenience, we let $t_i = t_{ii}$ for each i. For $i = 1, \ldots, n$, we

let M_i denote the i^{th} *leading principal submatrix* of M, i.e.,

$$M_i = \begin{pmatrix} t_1 & t_{12} & \dots & t_{1i} \\ t_{12} & t_2 & & t_{2i} \\ \vdots & & \ddots & \vdots \\ t_{1i} & t_{2i} & \cdots & t_i \end{pmatrix}.$$

The determinant of M_i is called the i^{th} *principal minor* of M, and we denote this by $m_i = \det(M_i)$. For convenience, we let $m_0 = 1$. Observe that m_n is the determinant of M. We call the product of the first $n-1$ minors of M the *associated minor product*, and denote this by

$$\Delta = \prod_{i=1}^{n-1} m_i.$$

Observe that the associated minor product of a 1×1 matrix M is one. For this reason we generally assume $n > 1$. Note that if N is any $n \times n$ matrix, we may write N_i to indicate the i^{th} principal submatrix of N.

4.2 Decomposition of a Symmetric Matrix

We look to express the matrix M as the matrix product $LDL^T = M$, where L is unit lower triangular and D is diagonal. As M is symmetric, we will show that such matrices exist, and then solve for the entries recursively. Our major assumption on the matrix M is that its associated minor product is non-zero.

Theorem 4.1. *If $\Delta \neq 0$, then there exists a unique diagonal matrix D and a unique unit lower triangular matrix L such that $LDL^T = M$.*

Proof. By Theorem 3.2.1 from [45, p. 97], it is given that M has an LU factorization if $\Delta \neq 0$, where L is unit lower triangular and U is upper triangular. In particular, Corollary

2 of [32, p. 35] tells us that this LU factorization is unique. Subsequently, Algorithm 4.1.2 of [45, p. 138] tells us if M is symmetric with an LU factorization, there exists a diagonal matrix D such that $M = LDL^T$. Thus, we deduce that D must also be unique which shows the theorem. □

We assume from now on that $\Delta \neq 0$. Hence, let L and D be matrices with rational entries such that $LDL^T = M$. We write $D = (d_i)$ and, due to symmetry, we write $L = (\ell_{ij})$ where

$$\ell_{ij} = \begin{cases} \ell_{ji} & \text{if } i < j \\ 1 & \text{if } i = j \\ 0 & \text{if } i > j \end{cases}.$$

We emphasize that $\ell_{ij} \in \mathbb{Q}$. We first determine an expression for the elements d_i and subsequently show that the elements ℓ_{ij} will each have a common denominator with respect to i.

Lemma 4.1. *For $i = 1, \ldots, n$, we have that $M_i = L_i D_i (L_i)^T$.*

Proof. Without loss of generality, we fix i arbitrarily such that $1 \leq i \leq n-1$. We may express the decomposition $M = LDL^T$ in block matrix notation so that

$$M = \begin{pmatrix} M_i & A_i \\ A_i^T & B_i \end{pmatrix} = \begin{pmatrix} L_i & 0 \\ P_i & Q_i \end{pmatrix} \begin{pmatrix} D_i & 0 \\ 0 & C_i \end{pmatrix} \begin{pmatrix} L_i^T & P_i^T \\ 0 & Q_i^T \end{pmatrix} = LDL^T, \tag{4.1}$$

where the matrices B_i, Q_i and C_i are of size $n-i \times n-i$, and A_i and P_i^T are of size $i \times n-i$. In particular, M_i, L_i and D_i are all $i \times i$ matrices, and correspond to the i^{th} leading principal submatrix of their respective matrices. Hence, from (4.1) we take the block products to find

$$\begin{pmatrix} M_i & A_i \\ A_i^T & B_i \end{pmatrix} = \begin{pmatrix} L_i D_i L_i^T & L_i D_i P_i^T \\ (L_i D_i P_i^T)^T & Q_i C_i Q_i^T \end{pmatrix}.$$

Thus, by equating the blocks we see that $M_i = L_i D_i L_i^T$. □

Lemma 4.2. *For $i = 1, \ldots, n$, we have $d_i = \dfrac{m_i}{m_{i-1}}$.*

Proof. From Lemma 4.1, and as L is unit lower triangular, we see that for i such that $1 \leq i \leq n$, we have

$$\det(M_i) = \det(L_i D_i (L_i)^T) = \det(D_i) = \prod_{k=1}^{i} d_k.$$

Thus, for $i = 1, \ldots, n$ we have $m_i = d_1 \cdots d_i$. Hence, for a given i, as $\Delta \neq 0$ we have

$$d_i = \frac{m_i}{d_{i-1} \cdots d_1} = m_i \cdot \frac{m_{i-2}}{m_{i-1}} \cdot \frac{m_{i-3}}{m_{i-2}} \cdot \cdots \cdot \frac{m_0}{m_1} = \frac{m_i}{m_{i-1}}.$$

where we have tacitly used the idea that each d_i is recursively generated. □

Theorem 4.2. *For $1 \leq i < j \leq n$ we have $m_i \ell_{ij} \in \mathbb{Z}$.*

Proof. We have that M is a symmetric matrix with non-zero associated minor product. Through standard Gaussian elimination, we can row reduce M to an upper triangular matrix through the use of scalar multiplication and adding a multiple of one row to another. In this fashion, the elements strictly above the diagonal will be integers, as they will be the result of sums and products of integers. This standard elimination procedure will yield an upper triangular matrix U such that the i^{th} diagonal entry corresponds to the i^{th} leading principal minor of M.

If we let $E_1, \ldots, E_k$ denote the elementary matrices associated with this Gaussian elimination, we have that

$$(E_k \cdots E_1 L D) L^T = U.$$

We can write U as the product $U = D'U'$, where D' is a diagonal matrix with unit entries along each diagonal except for the determinant m_r in the n^{th} diagonal entry, and U' agrees

with the matrix U in every entry except for a 1 inserted in the n^{th} diagonal. Hence, we can transform U' into an upper triangular matrix by dividing the i^{th} row by m_i, for $i = 1, \ldots, n-1$. By the equation, it's clear that this unit upper triangular matrix agrees with L^T. For $1 \leq i < j \leq n$, let m_{ij} denote the strictly upper triangular element of U'. Hence we have that

$$\ell_{ij} = \frac{m_{ij}}{m_i}.$$

It follows that $m_i \ell_{ij} \in \mathbb{Z}$ for all $1 \leq i < j \leq n$. □

We note that, in light of Theorem 4.2, for $1 \leq i < j \leq n$ we let $\ell_{ij} = \frac{m_{ij}}{m_i}$, for some $m_{ij} \in \mathbb{Z}$, and we refer to m_{ij} as the *mixed minors* of M. Using the combinatorial definition of the determinant, it will follow from the diagonalization in Theorem 4.2 that, for $1 \leq i < j \leq r$, m_{ij} is the i^{th} leading principal minor of the matrix obtained by interchanging columns i and j in M. In other words, if we interchange columns i and j in M, then m_{ij} will be the determinant of the $i \times i$ leading principal submatrix of this matrix.

4.3 Diagonalization of a Quadratic Form

Let $r \in \mathbb{N}$. We let Q_r denote an integral quadratic form in r variables, given by

$$Q_r = \sum_{1 \leq i \leq j \leq r} t_{ij} x_i x_j \in \mathbb{Z}[x_1, \ldots, x_n].$$

For convenience, we let $t_i = t_{ii}$ for each $i = 1, \ldots, r$. We let M denote the integral, symmetric *two's in* matrix associated with Q_r, which we write as

$$M = \begin{pmatrix} 2t_1 & t_{12} & \cdots & t_{1n} \\ t_{12} & 2t_2 & & t_{2n} \\ \vdots & & \ddots & \vdots \\ t_{1n} & t_{2n} & \cdots & 2t_n \end{pmatrix}.$$

In this fashion, Q_r can be written as the 1×1 matrix product

$$Q_r = [x_1 \ldots x_r] \frac{M}{2} [x_1 \ldots x_r]^T.$$

As above we let $m_1, \ldots, m_r$ denote the r leading principal minors of M. If $m_i \neq 0$ we write $m_i = p^{\alpha_i} A_i$ for some $\alpha_i \in \mathbb{N}_0$ and $A_i \in \mathbb{Z}$ such that $(A_i, p) = 1$. Observe that if $p = 2$, we have $m_1 = 2t_1 = 2^{\alpha_1} A_1$ so that $\alpha_1 \geq 1$ in this case. Otherwise, for p odd, we have $m_1 = p^{\alpha_1} A_1$ where $2 \mid A_1$. For notational convenience we set $m_0 = p^{\alpha_0} A_0$ so that $\alpha_0 = 0$ and $A_0 = 1$. As above, we let $\Delta = \prod_{i=1}^{r-1} m_i$, and we refer to Δ as the associated minor product of Q_r. We will be primarily concerned with the prime divisibility of the first $r-1$ minors of Q_r. Thus, if $\Delta \neq 0$ we set

$$\alpha = \sum_{i=1}^{r-1} \alpha_i \quad \text{and} \quad A = \prod_{i=1}^{r-1} A_j,$$

so that $\Delta = p^{\alpha} A$.

Hence, assume $\Delta \neq 0$. By Theorems 4.1-4.3, we write $M = LDL^T$, where $D = \left(\frac{m_i}{m_{i-1}} \right)$ and for $1 \leq i < j \leq r$ we have $L = \left(\frac{m_{ij}}{m_i} \right)$. By our matrix product expression for Q_r, we have

$$Q_r = [x_1 \, x_2 \, \ldots \, x_r] L \frac{D}{2} L^T [x_1 \, x_2 \, \ldots \, x_r]^T$$

$$= [X_1\ X_2\ \ldots\ X_r] \left(\frac{m_i}{2m_{i-1}} \right) [X_1\ X_2\ \ldots\ X_r]^T,$$

where

$$\begin{aligned} X_i &= x_i + \frac{m_{ii+1}}{m_i} x_{i+1} + \ldots + \frac{m_{ir}}{m_i} x_r \\ &= \frac{1}{m_i} \left(m_i x_i + m_{ii+1} x_{i+1} + \ldots + m_{ir} x_r \right). \end{aligned}$$

Observe that $X_r = x_r$. Thus, we see that

$$Q_r = \sum_{i=1}^{r} \frac{m_i}{2m_{i-1}} X_i^2 = \sum_{i=1}^{r} \frac{1}{2m_{i-1}m_i} (m_i X_i)^2. \tag{4.2}$$

For $i = 1, \ldots, r-1$ we set

$$y_i = m_i X_i \in \mathbb{Z}[x_i, x_{i+1}, \ldots, x_r]. \tag{4.3}$$

With this notation, we see that (4.2) becomes

$$Q_r = \sum_{i=1}^{r-1} \frac{y_i^2}{2m_{i-1}m_i} + \frac{m_r x_r^2}{2m_{r-1}}. \tag{4.4}$$

We multiply (4.4) by the least common denominator 2Δ to get

$$2\Delta Q_r = \sum_{i=1}^{r-1} \frac{\Delta y_i^2}{m_{i-1}m_i} + \frac{\Delta_r x_r^2}{m_{r-1}},$$

or, with $\Delta = p^\alpha A$,

$$2Ap^\alpha Q_r = \sum_{i=1}^{r-1} \frac{A}{A_{i-1}A_i} p^{\alpha-\alpha_i-\alpha_{i-1}} y_i^2 + \frac{Am_r}{A_{r-1}} p^{\alpha-\alpha_{r-1}} x_r^2. \tag{4.5}$$

We have expressed our quadratic form as a diagonal form with integer coefficients. For

$i = 1, \ldots, r-1$, the variable y_i is a linear expression in $r - i + 1$ variables with integer coefficients. Hence, we reduce (4.5) modulo a prime power to arrive at the following theorem.

Theorem 4.3. *Let Q_r be an integral quadratic form with associated minor product $\Delta \neq 0$. Then for $n \in \mathbb{N}$ we have*

$$p^{\alpha} Q_r \equiv \sum_{i=1}^{r-1} (2A_i A_{i-1})^{-1} p^{\alpha - \alpha_i - \alpha_{i-1}} y_i^2 + (2A_{r-1})^{-1} m_r p^{\alpha - \alpha_{r-1}} x_r^2 \pmod{p^{n+\alpha}},$$

when p is an odd prime, and

$$2^{\alpha+1} Q_r \equiv \sum_{i=1}^{r-1} (A_i A_{i-1})^{-1} 2^{\alpha - \alpha_i - \alpha_{i-1}} y_i^2 + (A_{r-1})^{-1} m_r 2^{\alpha - \alpha_{r-1}} x_r^2 \pmod{2^{n+\alpha+1}}.$$

Proof. The statement of the theorem follows by reducing (4.5) modulo $p^{n+\alpha}$ and modulo $2^{n+\alpha+1}$, respectively. □

Chapter 5

Main Results

In this chapter we present our main results. We maintain the notation previously established. In particular, we emphasize that p will denote a prime of arbitrary parity. Further, unconditionally, we have $n, r \in \mathbb{N}$ and $S \in \mathbb{Z}$ is such that $(S, p) = 1$. Additionally, recall that for a given quadratic form in r variables, for $i = 1, \ldots, r$, m_i denotes the i^{th} leading principal minor of an integral symmetric matrix associated with the form. Further, the product $\Delta = \prod_{i=1}^{r-1} m_i$ is called the associated minor product of a quadratic form. We let

$$Q_r = \sum_{i=1}^{r} t_i x_i^2 + \sum_{1 \leq i < j \leq r} t_{ij} x_i x_j \in \mathbb{Z}[x_1, \ldots, x_n]$$

denote an integral quadratic form with associated minor product $\Delta \neq 0$. With this, we define the *quadratic form Gauss sum* by

$$G(Q_r; S; p^n) = \sum_{x_1, \ldots, x_r = 0}^{p^n - 1} e\left(\frac{SQ_r}{p^n}\right).$$

We have a basic reduction property for the quadratic form Gauss sum, similar to Proposition 3.2.

Proposition 5.1 (The Extended Reduction Property)**.** *For $\alpha \in \mathbb{N}_0$ we have that*

$$G(Q_r; Sp^\alpha; p^n) = \begin{cases} p^{nr} & \text{if } \alpha \geq n \\ p^{\alpha r} \cdot G(Q_r; S; p^{n-\alpha}) & \text{if } \alpha < n. \end{cases}$$

Proof. If $\alpha < n$, as the exponential $e\left(\frac{\cdot}{p^{n-\alpha}}\right)$ is periodic modulo $p^{n-\alpha}$, similar to Propositions 2.3 and 3.2, we see that

$$\begin{aligned} G(Q_r; Sp^\alpha; p^n) &= \sum_{x_1,\ldots,x_r=0}^{p^n-1} e\left(\frac{SQ_r}{p^{n-\alpha}}\right) = (p^\alpha)^r \sum_{x_1,\ldots,x_r=0}^{p^{n-\alpha}-1} e\left(\frac{SQ_r}{p^{n-\alpha}}\right) \\ &= p^{\alpha r} G(Q_r; S; p^{n-\alpha}). \end{aligned}$$

Otherwise, if $\alpha \geq n$, then we have $G(Q_r; Sp^\alpha; p^n) = \sum_{x_1,\ldots,x_r=0}^{p^n-1} 1 = p^{nr}$. □

Similar to (3.6), it follows that for any $\alpha \in \mathbb{N}_0$ we have that

$$G(Q_r; s; p^n) = \frac{1}{p^{\alpha r}} G(Q_r; sp^\alpha; p^{n+\alpha}). \tag{5.1}$$

Further, we see that Proposition 3.2 is the special case of Proposition 5.1 where $r = 1$. In light of Proposition 5.1, we may assume without loss of generality that the coefficients of Q_r are mutually relatively prime, that is, there is no prime number which divides every coefficient.

We proceed by first evaluating the binary and ternary quadratic cases. These evaluations will reveal our methods and demonstrate the difficulties in generalizing $G(Q_r; s; p^n)$ for larger r, when the coefficients of Q_r are arbitrarily chosen. The binary quadratic form Gauss sum was recently investigated by Alaca, Alaca and Williams [1]. We show how we may attain their results using Theorem 5.1 and 5.2 below.

5.1 Binary Quadratic Form Gauss Sums

For this section, we assume $a, b, c \in \mathbb{Z}$ are arbitrary integers such that $a \neq 0$ and $(a, b, c) = 1$. Hence, we let

$$Q_2 = ax_1^2 + bx_1x_2 + cx_2^2.$$

We let $2a = p^\alpha A$ for $A \in \mathbb{Z}$ coprime to p and $\alpha \in \mathbb{N}_0$. Observe that if $p = 2$, we have $\alpha \geq 1$ in this case. Finally, we may choose our coefficients a and c such that if $p^m \mid\mid a$ for some $m \in \mathbb{N}_0$, then $p^m \mid c$.

Theorem 5.1. *Let p be an odd prime. Then for $n \in \mathbb{N}$ we have*

$$G(Q_2; S; p^n) = \begin{cases} p^n & \text{if } \alpha \geq n \\ G(2SA; p^{n-\alpha}) \cdot G(2SAm_2; p^{n+\alpha}) & \text{if } \alpha < n. \end{cases}$$

Proof. Let $\beta \in \mathbb{N}_0$ and $B \in \mathbb{Z}$ be such that $b \equiv p^\beta B \pmod{p^{n+\alpha}}$. Suppose first that $\alpha \geq n$. Under our assumptions, this means $\beta = 0$ and $Q_2 \equiv Bx_1x_2 \pmod{p^n}$. Hence, by Proposition 2.2 we have

$$G(Q_r; S; p^n) = \sum_{x_1, x_2 = 0}^{p^n - 1} e\left(\frac{SBx_1x_2}{p^n}\right) = p^n.$$

Thus, suppose $\alpha < n$. By Theorem 4.3, we have

$$p^\alpha Q_2 \equiv (2A)^{-1}y_1^2 + (2A)^{-1}m_2y_2^2 \pmod{p^{n+\alpha}}, \tag{5.2}$$

where $y_1 = 2ax_1 + bx_2$ and $y_2 = x_2$. Hence, by (5.1) and (5.2), it follows that

$$G(Q_2; S; p^n) = \frac{1}{p^{2\alpha}} G(Q_2; Sp^\alpha; p^{n+\alpha})$$

$$= \frac{1}{p^{2\alpha}} \sum_{x_1,x_2=0}^{p^{n+\alpha}-1} e\left(\frac{Sp^{\alpha}Q_2}{p^{n+\alpha}}\right)$$
$$= \frac{1}{p^{2\alpha}} \sum_{x_2=0}^{p^{n+\alpha}-1} e\left(\frac{S(2A)^{-1}m_2x_2^2}{p^{n+\alpha}}\right) \sum_{x_1=0}^{p^{n+\alpha}-1} e\left(\frac{S(2A)^{-1}y_1^2}{p^{n+\alpha}}\right). \tag{5.3}$$

Observe that $y_1 \equiv p^{\alpha}Ax_1 + p^{\beta}Bx_2 \pmod{p^{n+\alpha}}$. As $n > \alpha$, by Proposition 3.8, the sum indexed by x_1 is non-zero if and only if $p^{\beta}Bx_2 \equiv 0 \pmod{p^{n+\alpha}}$. Hence, with Propositions 3.11(b) and 3.13, (5.3) will simplify to

$$G(2AS; p^{n-\alpha}) \sum_{\substack{x_2=0 \\ p^{\beta}x_2 \equiv 0 \pmod{p^{\alpha}}}}^{p^{n+\alpha}-1} e\left(\frac{S(2A)^{-1}m_2x_2^2}{p^{n+\alpha}}\right). \tag{5.4}$$

Therefore, if $\beta \geq \alpha$, by Proposition 3.13, (5.4) will simplify to $G(2AS; p^{n-\alpha}) \cdot G(2ASm_2; p^{n+\alpha})$. Thus, suppose $\beta < \alpha$. This implies $\alpha \geq 1$ and so we must have $\beta = 0$ in this case. In particular, this means that $(m_2, p) = 1$. Hence, as $n > \alpha$, by Corollary 3.1, (5.4) will again simplify to $G(2AS; p^{n-\alpha}) \cdot G(2ASm_2; p^{n+\alpha})$. □

Theorem 5.1 agrees with Theorem 1.1 of Alaca, Alaca and Williams [1, p. 67] for $\alpha = 0$ and $4ac - b^2 \neq 0$. Under these assumptions, we have $m_2 = p^{\alpha_2}A_2$ for some $\alpha_2 \in \mathbb{N}_0$ and $A_2 \in \mathbb{Z}$ coprime to p. Hence, along with Theorem 3.1 and Proposition 2.16, Theorem 5.1 yields

$$\begin{aligned} G(Q_2; S; p^n) &= G(2SA; p^n) \cdot G(2SAm_2; p^n) \\ &= \left(\frac{2SA}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)} p^{\frac{n}{2}} \cdot G(2SAp^{\alpha_2}A_2; p^n) \\ &= \left(\frac{2SA}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)} p^{\frac{n}{2}} \cdot \begin{cases} p^n & \text{if } \alpha_2 \geq n \\ p^{\frac{n+\alpha_2}{2}} \left(\frac{2SAA_2}{p}\right)^{n+\alpha_2} i^{\left(\frac{p^{n+\alpha_2}-1}{2}\right)^2} & \text{if } \alpha_2 \leq n \end{cases} \end{aligned}$$

$$= \begin{cases} \left(\frac{2SA}{p}\right)^n p^{\frac{3n}{2}} i^{\left(\frac{p^n-1}{2}\right)^2} & \text{if } \alpha_2 \geq n \\ \left(\frac{2SA}{p}\right)^{\alpha_2} \left(\frac{A_2}{p}\right)^{n+\alpha_2} p^{n+\frac{\alpha_2}{2}} \left(\frac{-1}{p}\right)^{(\alpha_2+1)n} i^{\left(\frac{p^{\alpha_2}-1}{2}\right)^2} & \text{if } \alpha_2 \leq n. \end{cases}$$

Under our notation, we have $2a = A$, and so the above expression will become

$$G(Q_2; S; p^n) = \begin{cases} \left(\frac{aS}{p}\right)^n p^n \sqrt{(-1)^{(p^n-1)/2} p^n} & \text{if } \alpha_2 \geq n \\ \left(\frac{-1}{p}\right)^{(\alpha_2+1)n} \left(\frac{aS}{p}\right)^{\alpha_2} \left(\frac{A_2}{p}\right)^{\alpha_2+n} p^n \sqrt{(-1)^{(p^{\alpha_2}-1)/2} p^{\alpha_2}} & \text{if } \alpha_2 \leq n. \end{cases}$$

This corresponds exactly to the expression given by Alaca, et al. We will determine similar explicit formulae in Corollary 5.1 below.

We look now at the case where p is a power of 2. Recall from Definition 2.5 that

$$\mathbb{O}(n) = \frac{(1+(-1)^n)}{2} = \begin{cases} 1 & \text{if } n \text{ even} \\ 0 & \text{if } n \text{ odd.} \end{cases}$$

Theorem 5.2. *For $n \in \mathbb{N}$, we have*

$$G(Q_2; S; 2^n) = \begin{cases} 2^n & \text{if } \alpha \geq n > 1 \\ 2(-1)^c \mathbb{O}(m_2+1) & \text{if } \alpha = n = 1 \\ \frac{1}{4} G(SA; 2^{n+1-\alpha}) \cdot G(SAm_2; 2^{n+1+\alpha}) & \text{if } \alpha < n. \end{cases}$$

Proof. Recall $2a = 2^\alpha A$ so that $\alpha = 1$ implies a is odd. As well, without loss of generality we have $2^{\alpha-1} \mid c$. Let $\beta \in \mathbb{N}_0$ and $B \in \mathbb{Z}$ be such that $b \equiv 2^\beta B \pmod{2^{n+\alpha+1}}$, for B odd. Similar to the proof of Theorem 5.1, if $\alpha > n$, as $(a, b, c) = 1$ it will follow that $\beta = 0$ and $Q_2 \equiv Bx_1x_2 \pmod{2^n}$. Hence, by Proposition 2.2,

$$G(Q_2; S; 2^n) = \sum_{x_1, x_2 = 0}^{2^n-1} e\left(\frac{SBx_1x_2}{2^n}\right) = 2^n.$$

Thus, suppose that $\alpha \leq n$. By Theorem 4.3 we have that

$$2^{\alpha+1}Q_r \equiv A^{-1}y_1^2 + A^{-1}m_2y_2^2 \pmod{2^{n+\alpha+1}}.$$

Hence, we deduce that

$$G(Q_2;S;2^n) = \frac{1}{2^{2(\alpha+1)}} \sum_{x_2=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA^{-1}m_2x_2^2}{2^{n+\alpha+1}}\right) \sum_{x_1=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA^{-1}y_1^2}{2^{n+\alpha+1}}\right). \tag{5.5}$$

We would like to use Proposition 3.8 to evaluate the innermost sum of (5.5). However, the case $n = \alpha$ will not satisfy the conditions of this proposition. Thus, we treat this case separately.

Suppose $\alpha = n$. By definition, we have

$$\begin{aligned}
G(Q_2;S;2^n) &= \sum_{x_1,x_2=0}^{2^n-1} e\left(\frac{S(2^{n-1}Ax_1^2 + bx_1x_2 + cx_2^2)}{2^n}\right) \\
&= \sum_{x_2=0}^{2^n-1} e\left(\frac{Scx_2^2}{2^n}\right) \sum_{x_1=0}^{2^n-1} (-1)^{x_1} e\left(\frac{Sbx_1x_2}{2^n}\right) \\
&= \sum_{x_2=0}^{2^n-1} e\left(\frac{Scx_2^2}{2^n}\right) \left(\sum_{\substack{x_1=0 \\ x_1 \text{ even}}}^{2^n-1} e\left(\frac{Sbx_1x_2}{2^n}\right) - \sum_{\substack{x_1=0 \\ x_1 \text{ odd}}}^{2^n-1} e\left(\frac{Sbx_1x_2}{2^n}\right) \right) \\
&= \sum_{x_2=0}^{2^n-1} e\left(\frac{Scx_2^2}{2^n}\right) \left(2\sum_{\substack{x_1=0 \\ x_1 \text{ even}}}^{2^n-1} e\left(\frac{Sbx_1x_2}{2^n}\right) - \sum_{x_1=0}^{2^n-1} e\left(\frac{Sbx_1x_2}{2^n}\right) \right) \\
&= \sum_{x_2=0}^{2^n-1} e\left(\frac{Scx_2^2}{2^n}\right) \left(2\sum_{x_1=0}^{2^{n-1}-1} e\left(\frac{Sbx_1x_2}{2^{n-1}}\right) - \sum_{\substack{x_1=0 \\ bx_2 \equiv 0 \pmod{2^n}}}^{2^n-1} 1 \right) \\
&= \sum_{x_2=0}^{2^n-1} e\left(\frac{Scx_2^2}{2^n}\right) \left(2\sum_{\substack{x_1=0 \\ bx_2 \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 - \sum_{\substack{x_1=0 \\ bx_2 \equiv 0 \pmod{2^n}}}^{2^n-1} 1 \right).
\end{aligned} \tag{5.6}$$

Write $c = 2^{n-1}c'$ for some $c' \in \mathbb{Z}$ which means $e\left(\frac{Scx_2^2}{2^n}\right) = (-1)^{c'x_2}$. Hence, we write (5.6)

as

$$= \sum_{\substack{x_2=0 \\ x_2 \text{ even}}}^{2^n-1} \left(2 \sum_{\substack{x_1=0 \\ bx_2 \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 - \sum_{\substack{x_1=0 \\ bx_2 \equiv 0 \pmod{2^n}}}^{2^n-1} 1 \right)$$
$$+ (-1)^{c'} \sum_{\substack{x_2=0 \\ x_2 \text{ odd}}}^{2^n-1} \left(2 \sum_{\substack{x_1=0 \\ b \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 - \sum_{\substack{x_1=0 \\ b \equiv 0 \pmod{2^n}}}^{2^n-1} 1 \right). \tag{5.7}$$

If $\alpha = n = 1$, then $c' = c$ in this case, and (5.7) simplifies to

$$\left(2 - \sum_{x_1=0}^{1} 1 \right) + (-1)^c \left(2 - \sum_{\substack{x_1=0 \\ b \text{ even}}}^{1} 1 \right) = \begin{cases} 2(-1)^c & \text{if } b \text{ odd} \\ 0 & \text{if } b \text{ even.} \end{cases} \tag{5.8}$$

As b is odd if and only if m_2 is odd, we see that (5.8) simplifies to $2(-1)^c \mathbb{O}(m_2 + 1)$, which agrees with the statement of the theorem. Otherwise, for $\alpha = n > 1$, this implies a and c are even, so that we must have b odd. Hence, (5.7) simplifies to

$$2 \sum_{\substack{x_2=0 \\ x_2 \equiv 0 \pmod{2^{n-1}}}}^{2^n-1} 2^{n-1} - \sum_{\substack{x_2=0 \\ x_2 \equiv 0 \pmod{2^n}}}^{2^n-1} 2^n = 2^n \cdot 2 - 2^n = 2^n. \tag{5.9}$$

We see that (5.9) agrees with the statement of the theorem in this case.

Thus, we now assume that $n > \alpha$ and in particular this means $n \geq 2$. From Proposition 3.8, the sum indexed by x_1 in (5.5) is non-zero whenever $2^\beta B x_2 \equiv 0 \pmod{2^\alpha}$. Hence, by Propositions 3.8, 3.12(b) and 3.14, (5.5) will simplify to

$$\frac{G(SA; 2^{n-\alpha+1})}{2^2} \sum_{\substack{x_2=0 \\ 2^\beta x_2 \equiv 0 \pmod{2^\alpha}}}^{2^{n+\alpha+1}} e\left(\frac{SA^{-1} m_2 x_2^2}{2^{n+\alpha+1}} \right). \tag{5.10}$$

If $\beta \geq \alpha$, then with Proposition 3.14, (5.10) simplifies to $\frac{1}{4} G(SA; 2^{n-\alpha+1}) \cdot G(SAm_2; 2^{n+\alpha+1})$. Thus, suppose $\beta < \alpha$. Observe that we must have $\alpha \geq 1$ which means $\beta = 0$ in this case.

Hence, as $\alpha + 1 \leq n$, with Corollary 3.2, (5.10) will again simplify to $\frac{1}{4}G(SA; 2^{n-\alpha+1}) \cdot G(SAm_2; 2^{n+\alpha+1})$. □

Both Theorem 1.2 [1, p. 69] and Theorem 1.3 [1, p. 70] of Alaca, et al. will agree with Theorem 5.2 above under certain conditions. Suppose first that $4ac - b^2 \neq 0$, a is odd and b is even. Write $4ac - b^2 = 2^{\alpha_2}A_2$ for $\alpha_2 \geq 2$ and $A_2 \in \mathbb{Z}$ odd. Observe as well that under these assumptions, $\alpha = 1$. Hence, with Theorem 3.1, Theorem 5.2 yields

$$
\begin{aligned}
G(Q_2; S; p^n) &= \begin{cases} 2(-1)^c \mathbb{O}(2^{\alpha_2}A_2 + 1) & \text{if } n = 1 \\ \frac{1}{4}G(SA; 2^n) \cdot G(SA2^{\alpha_2}A_2; 2^{n+2}) & \text{if } n > 1 \end{cases} \\
&= \begin{cases} 0 & \text{if } n = 1 \\ \frac{1}{4}\left(\frac{2}{SA}\right)^n (1 + i^{SA})2^{\frac{n}{2}} \cdot G(SA2^{\alpha_2}A_2; 2^{n+2}) & \text{if } n > 1 \end{cases} \\
&= \begin{cases} 0 & \text{if } n = 1 \\ \frac{1}{4}\left(\frac{2}{SA}\right)^n (1 + i^{SA})2^{\frac{n}{2}} \cdot 2^{n+2} & \text{if } \alpha_2 \geq n + 2 \\ 0 & \text{if } n + 1 = \alpha_2 \\ \frac{1}{4}\left(\frac{2}{SA}\right)^n (1 + i^{SA})2^{\frac{n}{2}} \cdot 2^{\frac{n+2+\alpha_2}{2}} \left(\frac{2}{SAA_2}\right)^{n+\alpha_2} (1 + i^{SAA_2}) & \text{if } \alpha_2 \leq n \end{cases} \\
&= \begin{cases} 0 & \text{if } n = 1 \\ \left(\frac{2}{SA}\right)^n (1 + i^{SA})2^{\frac{3n}{2}} & \text{if } 2 \leq n \leq \alpha_2 - 2 \\ 0 & \text{if } n = (\alpha_2 - 2) + 1 \geq 2 \\ \left(\frac{2}{SA}\right)^{\alpha_2} \left(\frac{2}{A_2}\right)^{n+\alpha_2} (1 + i^{SA})(1 + i^{SAA_2})2^{n+\frac{(\alpha_2-2)}{2}} & \text{if } n \geq (\alpha_2 - 2) + 2. \end{cases}
\end{aligned}
\tag{5.11}
$$

We see that (5.11) agrees with Theorem 1.2 of Alaca, et al. where $\alpha_2 - 2$ corresponds to l in [1, p. 69].

Suppose now that b is odd and we recall that $(a, b, c) = 1$ so that $m_2 = 4ac - b^2 = A_2$ is

odd. In particular, we see that $A_2 \equiv 3 \pmod 4$. Theorem 1.3 of Alaca, et al. states

$$G(Q_2; S; 2^n) = (-1)^{acn} 2^n. \tag{5.12}$$

It's clear that if $\alpha \geq n > 1$, Theorem 5.2 will agree with (5.12). If $\alpha = n = 1$, then a is odd so $(-1)^a = (-1)$ and as b is odd we have $\mathbb{O}(m_2 + 1) = 1$. Thus, from Theorem 5.2, we have $G(Q_2; S; 2) = 2(-1)^c$, which agrees with (5.12). Otherwise, for $\alpha < n$, along with Theorem 3.1, Theorem 5.2 yields

$$\begin{aligned} G(Q_2; S; 2^n) &= \frac{1}{4} \left(\frac{2}{SA}\right)^{n+1+\alpha} (1 + i^{SA}) 2^{\frac{n+1-\alpha}{2}} \cdot \left(\frac{2}{SAA_2}\right)^{n+\alpha+1} (1 + i^{SAA_2}) 2^{\frac{n+1+\alpha}{2}} \\ &= 2^{n-1} \left(\frac{2}{A_2}\right)^{n+\alpha+1} (1 + i^{SA})(1 - i^{SA}) \\ &= 2^n \left(\frac{2}{A_2}\right)^{n+\alpha+1}. \end{aligned} \tag{5.13}$$

If both a and c are odd, then modulo 8 we have $A_2 \equiv 4ac - b^2 \equiv 3 \pmod 8$. As a is odd, $\alpha = 1$ and thus $\left(\frac{2}{A_2}\right)^{n+\alpha+1} = (-1)^n$, which shows that (5.13) agrees with (5.12). Otherwise, if at least one of a or c is even, $A_2 \equiv 7 \pmod 8$ and $\left(\frac{2}{A_2}\right) = 1$. We see that (5.12) and (5.13) will yield the same expression. Hence, regardless of parity of our coefficients, Theorem 5.2 will yield the results of Alaca, et al. We will determine explicit expressions similar to (5.13) in Corollary 5.2 below.

We provide a brief example to demonstrate our method. Set $Q_2 = x_1^2 + x_1 x_2 + x_2^2$. To evaluate any quadratic form Gauss sum we first look at the minors of the associated symmetric matrix. The symmetric matrix associated with Q_2 is given by $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Thus, $m_1 = 2$ and $m_2 = 3$. We now proceed by specifying the prime p and express our minors using prime power notation. As usual, S will be an arbitrary integer coprime to p.

Suppose first p is odd. Write $m_1 = p^\alpha A$ and we see that $\alpha = 0$ and $m_1 = A$ in this case.

Hence, for $n \in \mathbb{N}$, Theorem 5.1 yields

$$\begin{aligned} G(Q_2; S; p^n) &= G(2Sm_1; p^n) \cdot G(2Sm_1m_2; p^n) = G(2^2S; p^n) \cdot G(2^2 \cdot 3S; p^n) \\ &= G(S; p^n) \cdot G(3S; p^n), \end{aligned}$$

where we have used Proposition 3.13 to simplify as needed. If we expand this using Theorem 3.1, we find that

$$\begin{aligned} G(3S; p^n) \cdot G(S; p^n) &= \begin{cases} 3 \cdot G(S; 3^{n-1}) \cdot G(S; 3^n) & \text{if } p = 3 \\ G(3S; p^n) \cdot G(S; p^n) & \text{if } p > 3 \end{cases} \\ &= \begin{cases} 3^{n+\frac{1}{2}} \left(\dfrac{S}{3}\right) i & \text{if } p = 3 \\ \left(\dfrac{-3}{p}\right)^n p^n & \text{if } p > 3. \end{cases} \end{aligned}$$

Note that this is exactly the statement of Corollary 2.1(i) of Alaca, et al. [1, p. 75].

For Theorem 5.2, we observe that as $m_1 = 2$, we have $\alpha = 1$ and $A = 1$ in this case. Assume for the sake of discussion that $n > 1$. Thus, Theorem 5.2 yields

$$G(Q_2; S; 2^n) = \frac{1}{4} G(SA; 2^{n+1-\alpha}) \cdot G(SAm_2; 2^{n+2}) = \frac{1}{4} G(S; 2^n) \cdot G(3S; 2^{n+2}).$$

As before, if we expand this using Theorem 3.1, we have that

$$\begin{aligned} \frac{1}{4} G(S; 2^n) \cdot G(3S; 2^{n+2}) &= \frac{1}{4} \left(\frac{2}{S}\right)^n (1 + i^S) 2^{\frac{n}{2}} \cdot \left(\frac{2}{3S}\right)^n (1 + i^{3S}) 2^{\frac{n+2}{2}} \\ &= 2^{n-1} \left(\frac{2}{3}\right)^n (1 + i^S)(1 - i^S) = 2^n (-1)^n. \end{aligned}$$

This agrees with Corollary 3.2(i) of Alaca, et al. [1, p. 89]. One can recover the remaining cases of Corollary 3.2 given by Alaca, et al. using Theorem 5.2.

Continuing in this manner, we now use Theorem 3.1 to derive exact formulas for the

binary quadratic form Gauss sums.

Corollary 5.1. *Let p be an odd prime. Let $\delta \in \mathbb{N}_0$ and $D \in \mathbb{Z}$ be such that $(D,p)=1$ and $p^\delta D \equiv m_2 \pmod{p^{n+\alpha}}$. Then for $\alpha < n$, we have*

$$G(Q_2;S;p^n) = \begin{cases} p^{\frac{3n+\alpha}{2}} \left(\frac{2SA}{p}\right)^{n+\alpha} i^{\left(\frac{p^{n+\alpha}-1}{2}\right)^2} & \text{if } \delta = n+\alpha \\ p^{n+\frac{\delta}{2}} \left(\frac{2SA}{p}\right)^{\delta} \left(\frac{D}{p}\right)^{n+\alpha+\delta} \left(\frac{-1}{p}\right)^{(\delta+1)(n+\alpha)} i^{\left(\frac{p^{\delta}-1}{2}\right)^2} & \text{if } \delta < n+\alpha. \end{cases}$$

Proof. By Theorem 3.1 and Theorem 5.1, we have that $G(Q_2;S;p^n)$ is given by

$$G(2SADp^\delta;p^{n+\alpha}) \cdot G(2SA;p^{n-\alpha}) = G(2SADp^\delta;p^{n+\alpha}) \cdot \left(\frac{2SA}{p}\right)^{n+\alpha} i^{\left(\frac{p^{n+\alpha}-1}{2}\right)^2} p^{\frac{n-\alpha}{2}}. \quad (5.14)$$

If $\delta = n+\alpha$, then by Proposition 3.2, (5.14) will simplify to

$$p^{\frac{3n+\alpha}{2}} \left(\frac{2SA}{p}\right)^{n+\alpha} i^{\left(\frac{p^{n+\alpha}-1}{2}\right)^2}.$$

Otherwise, if $\delta < n+\alpha$, by Proposition 3.2 and Theorem 3.1, we have

$$\begin{aligned} G(2SADp^\delta;p^{n+\alpha}) &= p^\delta G(2SAD;p^{n+\alpha-\delta}) \\ &= p^\delta \left(\frac{2SAD}{p}\right)^{n+\alpha+\delta} i^{\left(\frac{p^{n+\alpha+\delta}-1}{2}\right)^2} p^{\frac{n+\alpha-\delta}{2}} \\ &= p^{\frac{n+\alpha+\delta}{2}} \left(\frac{2SAD}{p}\right)^{n+\alpha+\delta} i^{\left(\frac{p^{n+\alpha+\delta}-1}{2}\right)^2}. \end{aligned} \quad (5.15)$$

We substitute (5.15) into (5.14), which yields

$$p^{n+\frac{\delta}{2}} \left(\frac{2SA}{p}\right)^{\delta} \left(\frac{D}{p}\right)^{n+\alpha+\delta} i^{\left(\frac{p^{n+\alpha}-1}{2}\right)^2} i^{\left(\frac{p^{n+\alpha+\delta}-1}{2}\right)^2}. \quad (5.16)$$

Thus, with Proposition 2.16, (5.16) will simplify to the statement of the corollary. □

As mentioned previously, this agrees with Theorem 1.1 given by Alaca, et al. [1, p. 67]

under the condition that $\alpha = 0$. Further, under the conditions that $n = 1$ and $\alpha = \delta = 0$, the statement of the corollary agrees with the results given by Weber [111, p. 26].

Corollary 5.2. *Let $\delta \in \mathbb{N}_0$ and $D \in \mathbb{Z}$ be such that D is odd and $2^\delta D \equiv m_2 \pmod{2^{n+\alpha+1}}$. Then for $\alpha < n$, we have*

$$G(Q_2; S; 2^n) = \begin{cases} 2^{\frac{3n+\alpha-1}{2}} \left(\frac{2}{SA}\right)^{n+\alpha+1} (1 + i^{SA}) & \text{if } \delta = n + \alpha + 1 \\ 0 & \text{if } \delta = n + \alpha \\ 2^{n+\frac{\delta}{2}} \left(\frac{2}{SA}\right)^{\delta} \left(\frac{2}{D}\right)^{n+\alpha+\delta+1} i^{SA\left(\frac{D+1}{2}\right)^2} & \text{if } \delta < n + \alpha. \end{cases}$$

Proof. By Theorems 3.1 and 5.2, we have

$$\begin{aligned} G(Q_2; S; 2^n) &= \frac{1}{4} G(SA; 2^{n+1-\alpha}) \cdot G(SAm_2; 2^{n+1+\alpha}) \\ &= 2^{\frac{n-\alpha-3}{2}} \left(\frac{2}{SA}\right)^{n+1+\alpha} (1 + i^{SA}) \cdot G(SAD2^\delta; 2^{n+1+\alpha}). \end{aligned} \tag{5.17}$$

Subsequently, by Theorem 3.1 and Proposition 3.2, we have

$$G(SAD2^\delta; 2^{n+1+\alpha}) = \begin{cases} 2^{n+1+\alpha} & \text{if } \delta = n + 1 + \alpha \\ 0 & \text{if } \delta = n + \alpha \\ 2^{\frac{n+1+\alpha+\delta}{2}} \left(\frac{2}{SAD}\right)^{n+1+\alpha+\delta} (1 + i^{SAD}) & \text{if } \delta < n + \alpha. \end{cases} \tag{5.18}$$

Combining (5.17) and (5.18) for $\delta = n + 1 + \alpha$ or $\delta = n + \alpha$ will clearly yield the statements of the corollary. Hence, suppose $\delta < n + \alpha$, and combining (5.17) and (5.18), along with Proposition 2.19 yields

$$2^{n+\frac{\delta}{2}} \left(\frac{2}{SA}\right)^{\delta} \left(\frac{2}{D}\right)^{n+1+\alpha+\delta} i^{SA\left(\frac{D+1}{2}\right)^2},$$

which agrees with the remaining statement of the corollary. □

As mentioned above, Corollary 5.2 will agree with Theorems 1.2 and 1.3 [1, pp. 69-70] of Alaca, et al. depending on the parity of b. Observe as well that the results of Weber [111, p. 49] agree with Corollary 5.2.

5.2 Ternary Quadratic Form Gauss Sums

For this section, we let

$$Q_3 = t_1x_1^2 + t_2x_2^2 + t_3x_3^2 + t_{12}x_1x_2 + t_{13}x_1x_3 + t_{23}x_2x_3,$$

for $t_i, t_{ij} \in \mathbb{Z}$ which are mutually relatively prime, that is, no prime divides every coefficient t_i, t_{ij}. With this notation, we have $m_1 = 2t_1$ and $m_2 = 4t_1t_2 - t_{12}^2$, and we assume that $\Delta = m_1m_2 \neq 0$. Due to our assumptions, there exist $\alpha_1, \alpha_2 \in \mathbb{N}_0$ and $A_1, A_2 \in \mathbb{Z}$ such that $(A_1A_2, p) = 1$ and $m_1 = p^{\alpha_1}A_1, m_2 = p^{\alpha_2}A_2$ and $\Delta = p^{\alpha}A = p^{\alpha_1+\alpha_2}A_1A_2$.

Our aim in this section is to introduce a method which can generalize to quadratic forms of an arbitrary number of variables. For notational convenience for this section and the next, we set

$$\overline{\alpha_{ij}} = \max(\alpha_i - \alpha_{ij}, 0),$$

for $1 \leq i < j \leq r$. In this fashion, we have $0 \leq \overline{\alpha_{ij}} \leq \alpha_i$. Similarly, for $i = 1, \ldots, r$, we set $\alpha_{0i} = 0$ for convenience. Recall from section 4.2 that m_{ij} denotes an integer obtained in diagonalizing our quadratic form, which we refer to as a mixed minor.

Theorem 5.3. *Let p be an odd prime. Let $\alpha_3 \in \mathbb{N}_0$ and $A_3 \in \mathbb{Z}$ be such that $(A_3, p) = 1$ and $p^{\alpha_3}A_3 \equiv m_3 \pmod{p^{n+\alpha}}$. Similarly, for $1 \leq i < j \leq 3$ we let $\alpha_{ij} \in \mathbb{N}_0$ and $A_{ij} \in \mathbb{Z}$ satisfy $(A_{ij}, p) = 1$ and $p^{\alpha_{ij}}A_{ij} \equiv m_{ij} \pmod{p^{n+\alpha}}$. Without loss of generality, we may assume that*

$\alpha_{12} \leq \alpha_{13}$. *If* $n \geq \alpha$ *and* $n \geq \alpha_3 - \alpha_2 + 2(\max(\overline{\alpha_{23}}, \overline{\alpha_{13}}))$ *we have*

$$G(Q_3; S; p^n) = \frac{1}{p^{3\alpha}} \prod_{i=1}^{3} G(2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}}; p^{n+\alpha}).$$

Proof. By Theorem 4.3, we have that

$$p^{\alpha}Q_3 \equiv \sum_{i=1}^{2}(2A_iA_{i-1})^{-1}p^{\alpha-\alpha_i-\alpha_{i-1}}y_i^2 + (2A_2)^{-1}m_3p^{\alpha-\alpha_2}x_3^2 \pmod{p^{n+\alpha}}.$$

Hence, by (5.1) and in light of Proposition 3.13, we have that

$$\begin{aligned} G(Q_3; S; p^n) =& \frac{1}{p^{3\alpha}} \sum_{x_3=0}^{p^{n+\alpha}-1} e\left(\frac{2SA_3A_2p^{\alpha_3+\alpha_1}x_3^2}{p^{n+\alpha}}\right) \sum_{x_2=0}^{p^{n+\alpha}-1} e\left(\frac{2SA_2A_1y_2^2}{p^{n+\alpha}}\right) \\ & \times \sum_{x_1=0}^{p^{n+\alpha}-1} e\left(\frac{2SA_1p^{\alpha_2}y_1^2}{p^{n+\alpha}}\right). \end{aligned} \tag{5.19}$$

By (4.3), it follows that

$$y_1 \equiv p^{\alpha_1}A_1x_1 + p^{\alpha_{12}}A_{12}x_2 + p^{\alpha_{13}}A_{13} \pmod{p^{n+\alpha}}.$$

As $n \geq \alpha \geq \alpha_1$, by Proposition 3.7, the sum indexed by x_1 in (5.19) will be non-zero if and only if

$$\begin{aligned} p^{\alpha_{12}}A_{12}x_2 + p^{\alpha_{13}}A_{13} &\equiv 0 \pmod{p^{\alpha_1}} \\ p^{\alpha_{12}}x_2 &\equiv -A_{12}^{-1}A_{13}p^{\alpha_{13}}x_3 \pmod{p^{\alpha_1}} \\ x_2 &\equiv -A_{12}^{-1}A_{13}p^{\alpha_{13}-\alpha_{12}}x_3 \pmod{p^{\overline{\alpha_{12}}}}. \end{aligned}$$

Thus, (5.19) will simplify to

$$\frac{1}{p^{3\alpha}}p^{\alpha}G(2SA_1; p^{n+\alpha_1}) \sum_{x_3=0}^{p^{n+\alpha}-1} e\left(\frac{2SA_3A_2p^{\alpha_3+\alpha_1}x_3^2}{p^{n+\alpha}}\right)$$

$$\times \sum_{\substack{x_2=0 \\ x_2 \equiv -A_{12}^{-1}A_{13}p^{\alpha_{13}-\alpha_{12}}x_3 \pmod{p^{\overline{\alpha_{12}}}}}}^{p^{n+\alpha}-1} e\left(\frac{2SA_2A_1y_2^2}{p^{n+\alpha}}\right). \tag{5.20}$$

Note that $y_2 \equiv p^{\alpha_2}A_2x_2 + p^{\alpha_{23}}A_{23}x_3 \pmod{p^{n+\alpha}}$. If $\alpha_1 \leq \alpha_{12}$, then as $n \geq \alpha_2 - \alpha_1$, we may use Proposition 3.7 to evaluate the sum indexed by x_2 in (5.20). Otherwise, if $\overline{\alpha_{12}} \neq 0$, as $n \geq \alpha - 2\alpha_{12}$, we may use Proposition 3.9 to evaluate (5.20). Further, Proposition 3.7 can be seen as a special case of Proposition 3.9, so we may use this latter proposition unreservedly.

In order for the sum indexed by x_2 in (5.20) to be non-zero, x_3 must satisfy the congruence conditions

$$p^{\alpha_{23}}A_{23}x_3 \equiv 0 \pmod{p^{\alpha_2}} \rightarrow x_3 \equiv 0 \pmod{p^{\overline{\alpha_{23}}}}$$

and

$$-A_{12}^{-1}A_{13}p^{\alpha_{13}-\alpha_{12}}x_3 \equiv 0 \pmod{p^{\overline{\alpha_{12}}}} \rightarrow x_3 \equiv 0 \pmod{p^{\overline{\alpha_{13}}}}, \tag{5.21}$$

where we have used the fact that $\overline{\alpha_{12}} - (\alpha_{13} - \alpha_{12}) = \overline{\alpha_{13}}$. Hence, by Proposition 3.9 and (5.21), (5.20) can be written as

$$\frac{1}{p^{3\alpha}} \cdot p^{\alpha}G(2SA_1; p^{n+\alpha_1}) \cdot p^{2\alpha_2}G(2SA_2A_1; p^{n+\alpha-2\alpha_2}) \times \sum_{\substack{x_3=0 \\ x_3 \equiv 0 \pmod{p^{\max(\overline{\alpha_{23}},\overline{\alpha_{13}})}}}}^{p^{n+\alpha}-1} e\left(\frac{2SA_2A_3p^{\alpha+\alpha_3-\alpha_2}x_3^2}{p^{n+\alpha}}\right). \tag{5.22}$$

Finally, due to our assumption that $n \geq \alpha_3 - \alpha_2 + \max(\overline{\alpha_{23}}, \overline{\alpha_{13}})$, by Corollary 3.1, (5.22) will simplify to

$$\frac{1}{p^{3\alpha}} \cdot p^{\alpha}G(2SA_1; p^{n+\alpha_1}) \cdot p^{2\alpha_2}G(2SA_2A_1; p^{n+\alpha-2\alpha_2}) \cdot p^{\alpha+\alpha_3-\alpha_2}G(2SA_2A_3; p^{n-(\alpha_3-\alpha_2)}). \tag{5.23}$$

To achieve the statement of the theorem, we simplify the Gauss sums given in (5.23) by Proposition 3.11. Hence, we have that

$$\begin{aligned} p^{\alpha}G(2SA_1; p^{n+\alpha_1}) &= p^{\alpha+\alpha_1}G(2SA; p^{n-\alpha_1}) = G(2SAp^{\alpha+\alpha_1}; p^{n+\alpha}), \\ p^{2\alpha_2}G(2SA_1A_2; p^{n+\alpha-2\alpha_2}) &= p^{\alpha+\alpha_2-\alpha_1}G(2SA_1A_2; p^{n+\alpha-(\alpha+\alpha_2-\alpha_1)}) \\ &= G(2SA_1A_2p^{\alpha+\alpha_2-\alpha_1}; p^{n+\alpha}), \\ p^{\alpha+\alpha_3-\alpha_2}G(2SA_2A_3; p^{n+\alpha-(\alpha_3+\alpha_1)}) &= G(2SA_2A_3p^{\alpha+\alpha_3-\alpha_2}; p^{n+\alpha}), \end{aligned}$$

so that (5.23) will simplify to the statement of the theorem. □

We mention that Theorem 5.3 will be valid for $m_3 = 0$ under certain conditions. Suppose $m_3 = 0$. By convention, we have $\alpha_3 = n + \alpha$. Thus, the condition of the theorem pertaining to n and α_3 will simplify to

$$\begin{aligned} n &\geq \alpha_3 - \alpha_2 + 2\max(\overline{\alpha_{23}}, \overline{\alpha_{13}}) \\ 0 &\geq \alpha_1 + 2\max(\overline{\alpha_{23}}, \overline{\alpha_{13}}). \end{aligned}$$

Hence, Theorem 5.3 will be valid for a ternary quadratic form with zero determinant if $\alpha_1 = 0$ and $\alpha_2 \leq \alpha_{23}$. We provide an example of such a case.

Let $Q_3 = x_1^2 + 2x_2^2 + x_3^2 + x_1x_2 + 2x_1x_3 + x_2x_3$ which has associated symmetric integral matrix $\begin{pmatrix} 2 & 1 & 2 \\ 1 & 4 & 1 \\ 2 & 1 & 2 \end{pmatrix}$. It follows that $m_1 = 2, m_2 = 7$ and $m_3 = 0$. From Theorem 4.2, we see that $m_{12} = 1$ and $m_{13} = 2$. Recall that m_{23} is the determinant of the 2×2 leading principal submatrix of the matrix with columns 2 and 3 interchanged. Hence, $m_{23} = 0$. Suppose $p = 7$ and $n \in \mathbb{N}$. Writing $m_i \equiv 7^{\alpha_i}A_i \pmod{7^{n+\alpha}}$ and $m_{ij} \equiv 7^{\alpha_{ij}}A_{ij} \pmod{7^{n+\alpha}}$ we see that

$$\alpha_1 = 0, \quad \alpha_2 = \alpha = 1, \quad \alpha_3 = n + \alpha = n + 1, \quad \alpha_{23} = n + \alpha = n + 1,$$

and

$$A_1 = 2, \quad A_2 = 1, \quad A_3 = 1.$$

In particular, we have $\alpha_2 \leq \alpha_{23}$ and $\alpha_1 = 0$ which satisfies the conditions of Theorem 5.3. Hence, Theorem 5.3 yields

$$\begin{aligned} G(Q_3; S; 7^n) &= \frac{1}{7^3} G(2S \cdot 7^{n+1}; 7^{n+1}) \cdot G(2^2 S \cdot 7^2; 7^{n+1}) \cdot G(2^2 S \cdot 7^1; 7^{n+1}) \\ &= 7^{n-2} \cdot 7^2 G(S; 7^{n-1}) \cdot 7 G(S; 7^n) \\ &= 7^{n+1} G(S; 7^{n-1}) G(S; 7^n). \end{aligned}$$

If we expand this using Theorem 3.1, we find that

$$\begin{aligned} G(Q_3; S; 7^n) &= 7^{n+1} \cdot \left(\frac{S}{7}\right)^{n+1} \imath^{\left(\frac{7^{n-1}-1}{2}\right)^2} 7^{\frac{n-1}{2}} \cdot \left(\frac{S}{7}\right)^{n} \imath^{\left(\frac{7^{n}-1}{2}\right)^2} 7^{\frac{n}{2}} \\ &= 7^{2n+\frac{1}{2}} \imath = 7^{2n} \sqrt{-7}. \end{aligned}$$

For p odd and $p \neq 7$, we can not evaluate $G(Q_3; S; p^n)$ using Theorem 5.3.

Next, we have a similar theorem for the even prime case.

Theorem 5.4. *Let $\alpha_3 \in \mathbb{N}_0$ and $A_3 \in \mathbb{Z}$ be such that $(A_3, 2) = 1$ and $2^{\alpha_3} A_3 \equiv m_3 \pmod{2^{n+\alpha+1}}$. Similarly, for $1 \leq i < j \leq 3$ we let $\alpha_{ij} \in \mathbb{N}_0$ and $A_{ij} \in \mathbb{Z}$ satisfy $(2, A_{ij}) = 1$ and $2^{\alpha_{ij}} A_{ij} \equiv m_{ij} \pmod{2^{n+\alpha+1}}$. Without loss of generality, we may assume that $\alpha_{12} \leq \alpha_{13}$. Then for $n \geq \alpha + 1$ and $n \geq \alpha_3 - \alpha_2 + 2\max(\overline{\alpha_{13}}, \overline{\alpha_{23}}) + 1$, we have*

$$G(Q_3; S; 2^n) = \frac{1}{2^{3(\alpha+1)}} \prod_{i=1}^{3} G(S A_i A_{i-1} 2^{\alpha + \alpha_i - \alpha_{i-1}}; 2^{n+\alpha+1}).$$

Proof. The proof follows in the same manner as in the proof of Theorem 5.4. From Theorem

4.3 and Proposition 3.14, we deduce that

$$G(Q_3;S;2^n) = \frac{1}{2^{3(\alpha+1)}} \sum_{x_3=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA_3A_2 2^{\alpha_3+\alpha_1}x_3^2}{2^{n+\alpha+1}}\right) \sum_{x_2=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA_2A_1y_2^2}{2^{n+\alpha+1}}\right) \times \sum_{x_1=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA_1 2^{\alpha_2}y_1^2}{2^{n+\alpha+1}}\right). \tag{5.24}$$

We now simplify these sums using Proposition 3.8, Proposition 3.10 and Corollary 3.2, respectively, in the same manner as we did in Theorem 5.3. In order to use these propositions, we note that

$$n \geq \alpha + 1$$

which allows us to use Proposition 3.8. Next, the condition on n necessary for Proposition 3.10 is

$$n + \alpha + 1 \geq 2(\overline{\alpha_{12}} + \alpha_2) + 2.$$

Thus, we see that

$$n \geq \alpha + 1 \geq \max(\alpha_2 - \alpha_1 + 1, \alpha + 1 - 2\alpha_{12}),$$

so we may use Proposition 3.10. Finally, our last condition on n will be given by

$$n + \alpha + 1 \geq \alpha_3 + \alpha_1 + 2\max(\overline{\alpha_{13}}, \overline{\alpha_{23}}) + 2$$

which simplifies to the assumption given in the statement of the theorem. Hence, (5.24) will

simplify to

$$\frac{1}{2^{3(\alpha+1)}} \cdot 2^{\alpha} G(SA_1; 2^{n+\alpha_1+1}) \cdot 2^{2\alpha_2} G(SA_2A_1; 2^{n+\alpha_1-\alpha_2+1}) \cdot 2^{\alpha_3+\alpha_1} G(SA_3A_2; 2^{n+1-(\alpha_3-\alpha_2)}). \tag{5.25}$$

Finally, with Proposition 3.12, we simplify the Gauss sums in (5.25). We have that

$$\begin{aligned} 2^{\alpha} G(SA_1; 2^{n+\alpha_1+1}) &= 2^{\alpha+\alpha_1} G(SA_1; 2^{n-\alpha_1+1}) = G(SA_1 2^{\alpha+\alpha_1}; 2^{n+\alpha+1}), \\ 2^{2\alpha_2} G(SA_2A_1; 2^{n+\alpha_1-\alpha_2+1}) &= G(SA_2A_1 2^{\alpha+\alpha_2-\alpha_1}; 2^{n+\alpha+1}), \\ 2^{\alpha_3+\alpha_1} G(SA_3A_2; 2^{n+1-(\alpha_3-\alpha_2)}) &= G(SA_3A_2 2^{\alpha+\alpha_3-\alpha_2}; 2^{n+\alpha+1}), \end{aligned}$$

so (5.25) will simplify to the statement of the theorem. □

We end this section with a curious example. Let $Q_3 = x_1^2 + 2x_2^2 + x_3^2 + 2x_1x_2$ which has associated matrix $\begin{pmatrix} 2 & 2 & 0 \\ 2 & 4 & 0 \\ 0 & 0 & 2 \end{pmatrix}$. It follows that

$$m_1 = 2, \quad m_2 = 4, \quad m_3 = 8, \quad m_{12} = 2 \quad \text{and} \quad m_{13} = m_{23} = 0.$$

Hence, for any odd prime p and $n \in \mathbb{N}$, the conditions of Theorem 5.3 are trivially satisfied so that

$$G(Q_3; S; p^n) = G(2^6 S; p^n) \cdot G(2^4 S; p^n) \cdot G(2^2 S; p^n) = G(S; p^n)^3.$$

Suppose now $p = 2$. Writing $m_i = 2^{\alpha_i} A_i$ and $m_{ij} \equiv 2^{\alpha_{ij}} A_{ij} \pmod{2^{n+\alpha+1}}$ we have

$$\begin{aligned} &\alpha_1 = 1, \quad \alpha_2 = 2, \quad \alpha_3 = 3, \quad \alpha = \alpha_1 + \alpha_2 = 3, \\ &\alpha_{12} = 1, \quad \alpha_{13} = n + \alpha + 1 = n + 4, \quad \alpha_{23} = n + \alpha + 1 = n + 4, \end{aligned}$$

and

$$A_1 = A_2 = A_3 = 1.$$

Observe that we have $\alpha_{12} \leq \alpha_{13}$. Further, we have

$$\overline{\alpha_{23}} = \max(\alpha_2 - \alpha_{23}, 0) = 0 = \max(\alpha_1 - \alpha_{13}, 0) = \overline{\alpha_{13}}.$$

Thus, if $n \geq 4$, the conditions of Theorem 5.4 are satisfied, so that

$$G(Q_3; S; 2^n) = \frac{1}{2^{12}} G(2^4 S; 2^{n+4}) \cdot G(2^4 S; 2^{n+4}) \cdot G(2^4 S; 2^{n+4}) = G(S; 2^n)^3.$$

It is interesting to note that in this case, for p arbitrary, $G(Q_3; S; p^n) = G(S; p^n)^3$.

5.3 General Quadratic Form Gauss Sums

For this section, we let

$$Q_r = \sum_{i=1}^{r} t_i x_i^2 + \sum_{1 \leq i < j \leq r} t_{ij} x_i x_j \tag{5.26}$$

denote an r-dimensional quadratic form. Further, we may assume that the coefficients of Q_r are mutually relatively prime. Recall that m_i denotes the i^{th} leading principal minor of the integral symmetric matrix associated with Q_r, and the associated minor product of Q_r is given by $\Delta = \prod_{i=1}^{r-1} m_i$. Finally, we assume that the associated minor product Δ is non-zero. As $\Delta \neq 0$, there exist $\alpha_i \in \mathbb{N}_0$ and $A_i \in \mathbb{Z}$ such that $(A_i, p) = 1$ and $p^{\alpha_i} A_i = m_i$, for each $i = 1, \ldots, r-1$. We set

$$\Delta = p^{\alpha} A = p^{\alpha_1 + \alpha_2 + \cdots + \alpha_{r-1}} \left(\prod_{i=1}^{r-1} A_i \right).$$

We extend this notation to the determinant m_r and the mixed minors m_{ij}, so that

$$m_r \equiv \left\{ \begin{array}{ll} p^{\alpha_r} A_r & (\text{mod } p^{n+\alpha}) \\ 2^{\alpha_r} A_r & (\text{mod } 2^{n+\alpha+1}) \end{array} \right\} \quad \text{and} \quad m_{ij} \equiv \left\{ \begin{array}{ll} p^{\alpha_{ij}} A_{ij} & (\text{mod } p^{n+\alpha}) \\ 2^{\alpha_{ij}} A_{ij} & (\text{mod } 2^{n+\alpha+1}) \end{array} \right\}.$$

From the previous section, we see that the divisibility of the coefficients will affect how we can evaluate the quadratic form Gauss sum. We present our main results repeatedly, with an increasing number of conditions on the coefficients.

Theorem 5.5. *Let p be an odd prime. If $(\Delta, p) = 1$ then*

$$G(Q_r; S; p^n) = G(2Sm_r A_{r-1}; p^n) \prod_{i=1}^{r-1} G(2SA_i A_{i-1}; p^n).$$

Proof. If $(\Delta, p) = 1$, this means $\alpha_i = 0$ and $m_i = A_i$ for each i. Hence, Theorem 4.3 states that

$$Q_r \equiv \sum_{i=1}^{r-1} (2A_i A_{i-1})^{-1} y_i^2 + (2A_{r-1})^{-1} m_r x_r^2 \ (\text{mod } p^n).$$

In light of Proposition 3.13, it follows that

$$G(Q_r; S; p^n) = \sum_{x_r=0}^{p^n-1} e\left(\frac{2Sm_r A_{r-1} x_r^2}{p^n}\right) \cdots \sum_{x_1=0}^{p^n-1} e\left(\frac{2SA_1 A_0 y_1^2}{p^n}\right). \tag{5.27}$$

Consider $y_1 = A_1 x_1 + \sum_{j=2}^{r} A_{1j} x_j$. By Proposition 2.5, as x_1 runs through a complete residue system modulo p^n, so does y_1. This means the sum indexed by x_1 in (5.27) will resolve to $G(2SA_1 A_0; p^n)$. By similar reasoning, the sums indexed by $x_2, \ldots, x_{r-1}$ in (5.27) will simplify in the same manner. Finally, the sum indexed by x_r in (5.27) is a quadratic Gauss

sum, so that (5.27) becomes

$$G(2Sm_rA_{r-1};p^n)\prod_{i=1}^{r-1}G(2SA_iA_{i-1};p^n).$$

□

Corollary 5.3. *Let p be an odd prime. If $(\Delta m_r, p) = 1$ then*

$$G(Q_r;S;p^n)=\prod_{i=1}^{r}G(2SA_iA_{i-1};p^n).$$

Proof. If $(m_r, p) = 1$ then $m_r \neq 0$ and $m_r \equiv A_r \pmod{p^n}$. Hence, the corollary follows from Theorem 5.5. □

We emphasize that Corollary 5.3 agrees with the results of Weber [111] as stated by Cohen [22, p. 14] for $S = 1$ and Q_r a Gaussian form. Indeed, this implies $2^r \mid m_r$. Hence, under these assumptions, Corollary 5.3 states

$$\prod_{i=1}^{r}\left(\frac{2A_iA_{i-1}}{p}\right)G(1;p^n)=\left(\frac{2^rm_r}{p}\right)G(1;p^n)^r,$$

which corresponds to (2.16) of [22]. Further, one can use the multiplicative properties of quadratic Gauss sums to arrive at a similar expression for arbitrary odd positive modulus. We will discuss this further in Chapter 7.

We have a similar theorem for the even prime case. However, as $2 \mid \Delta$, this theorem is conditional upon every mixed term of Q_r being even. Hence, for the following theorem, we assume Q_r is of the form

$$Q_r=\sum_{i=1}^{r}t_ix_i^2+2\sum_{1\leq i<j\leq r}t'_{ij}x_ix_j. \tag{5.28}$$

Note that (5.26) and (5.28) agree under the notation $t'_{ij} = \dfrac{t_{ij}}{2}$. These types of quadratic

forms are sometimes called *Gaussian forms* [83].

Consider the matrix M representing the integral matrix associated with Q_r. As every non-diagonal term is divisible by 2, we can extract 2 as a scalar factor. Thus, we have

$$M = 2M'.$$

We emphasize that M' is an integral matrix. As $\Delta \neq 0$, there exists non-zero integers m'_i, such that

$$m_i = \det(M_i) = \det(2M'_i) = 2^i \det(M'_i) = 2^i m'_i$$

for each $i = 1, \ldots, r-1$. We modify our notation in this fashion, so that

$$m_{ij} \equiv 2^i m'_{ij} \pmod{2^{n+\alpha+1}}$$

and $2^r m'_r \equiv m_r \pmod{2^{n+\alpha+1}}$. We define

$$\Delta' = \prod_{i=1}^{r-1} m'_i$$

and we may refer to Δ' as the *associated Gaussian minor product.*

Theorem 5.6. *If Δ' is odd, then*

$$G(Q_r; S; 2^n) = G(Sm'_r A_{r-1}; 2^n) \prod_{i=1}^{r} G(SA_i A_{i-1}; 2^n).$$

Proof. As Δ' is odd, we have that

$$\Delta = \prod_{i=1}^{r-1} m_i = \prod_{i=1}^{r-1} 2^{\alpha_i} A_i = \prod_{i=1}^{r-1} 2^i m'_i = 2^{1+2+\cdots+r-1} \Delta' = 2^\alpha A.$$

Thus, $\alpha_i = i$ for $i = 1, \ldots, r-1$ and $\alpha = \dfrac{r(r-1)}{2}$. Further, this means that $A_i = m_i'$ for $i = 1, \ldots, r-1$. By Theorem 4.3, we have

$$2^{\alpha+1}Q_r \equiv \sum_{i=1}^{r-1}(A_iA_{i-1})^{-1}2^{\alpha-i-(i-1)}y_i^2 + (A_{r-1})^{-1}m_r'2^{\alpha+r-(r-1)}x_r^2 \pmod{2^{n+\alpha+1}}.$$

In light of Proposition 3.14, it follows that

$$G(Q_r; S; 2^n) = \frac{1}{2^{r(\alpha+1)}} \sum_{x_r=0}^{2^{n+\alpha+1}-1} e\left(\frac{Sm_r'A_{r-1}2^{\alpha+1}x_r^2}{2^{n+\alpha+1}}\right) \cdots \sum_{x_1=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA_1 2^{\alpha-1}y_1^2}{2^{n+\alpha+1}}\right). \quad (5.29)$$

For $i = 1, \ldots, r-1$, we have that

$$y_i \equiv m_ix_i + \sum_{j=i+1}^{r} m_{ij}x_j \equiv 2^i\left(A_ix_i + \sum_{j=i+1}^{r} m_{ij}'x_j\right) \equiv 2^iy_i' \pmod{2^{n+\alpha+1}}.$$

By Proposition 2.5, as x_i runs over a complete residue system modulo $2^{n+\alpha+1}$, so does y_i'. Hence, with Proposition 3.2, the summands of (5.29) indexed by $x_1, \ldots, x_{r-1}$ will simplify to

$$\begin{aligned}\sum_{x_i=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA_iA_{i-1}2^{\alpha-i-(i-1)}y_i}{2^{n+\alpha+1}}\right) &= \sum_{x_i=0}^{2^{n+\alpha+1}-1} e\left(\frac{SA_iA_{i-1}2^{\alpha+1}y_i'}{2^{n+\alpha+1}}\right) \\ &= G(SA_iA_{i-1}2^{\alpha+1}; 2^{n+\alpha+1}) \\ &= 2^{\alpha+1}G(SA_iA_{i-1}; 2^n). \quad (5.30)\end{aligned}$$

With Proposition 3.2, the sum indexed by x_r in (5.29) is given by

$$G(SA_{r-1}m_r'2^{\alpha+1}; 2^{n+\alpha+1}) = 2^{\alpha+1}G(SA_{r-1}m_r'; 2^n). \quad (5.31)$$

Thus, with (5.30) and (5.31), (5.29) becomes

$$\frac{1}{2^{r(\alpha+1)}}\left(\prod_{i=1}^{r-1}2^{\alpha+1}G(SA_iA_{i-1};2^n)\right)2^{\alpha+1}G(SA_{r-1}m_r';2^n)$$
$$= G(SA_{r-1}m_r';2^n)\prod_{i=1}^{r-1}G(SA_iA_{i-1};2^n).$$

□

We note that an equivalent condition to Δ' being odd is that $\alpha_i = i$, for each $i = 1,\ldots,r-1$. Similarly, it would be sufficient to require $2^i \mid\mid m_i$ for each such i.

Corollary 5.4. *If $2^i \mid\mid m_i$ for $i = 1,\ldots,r$, then*

$$G(Q_r;S;2^n) = \prod_{i=1}^{r}G(SA_iA_{i-1};2^n).$$

Proof. If $2^r \mid\mid m_r$, then $m_r' = A_r$ and the corollary follows from Theorem 5.6. □

The previous two theorems have what could be called the best divisibility conditions. That is, each minor is coprime to the given modulus, or has a favorable divisibility, depending on the parity. The following two theorems will relax these divisibility conditions somewhat, but not completely.

Theorem 5.7. *Let p be an odd prime. Suppose that $\alpha_i \le \alpha_{ij}$ for all $1 \le i < j \le r$. Then*

$$G(Q_r;S;p^n) = \frac{1}{p^{r\alpha}}\prod_{i=1}^{r}G(2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}};p^{n+\alpha}).$$

Proof. By Theorem 4.3, (5.1) and considering Proposition 3.13 we have

$$G(Q_r;S:p^n) = \frac{1}{p^{r\alpha}}\sum_{x_r=0}^{p^{n+\alpha}-1}e\left(\frac{2SA_rA_{r-1}p^{\alpha+\alpha_r-\alpha_{r-1}}x_r^2}{p^{n+\alpha}}\right)\cdots\sum_{x_1=0}^{p^{n+\alpha+1}-1}e\left(\frac{2SA_1p^{\alpha-\alpha_1}y_1^2}{p^{n+\alpha}}\right). \tag{5.32}$$

For each $i = 1, \ldots, r-1$ we have

$$y_i \equiv p^{\alpha_i} A_i x_i + \sum_{j=i+1}^{r} p^{\alpha_{ij}} A_{ij} x_j \equiv p^{\alpha_i} \left(A_i x_i + \sum_{j=i+1}^{r} p^{\alpha_{ij}-\alpha_i} A_{ij} x_j \right) \equiv p^{\alpha_i} y_i' \pmod{p^{n+\alpha}}.$$

By Proposition 2.5, as x_i runs through a complete residue system, so does y_i'. Hence, each of the sums indexed by $x_1, \ldots, x_{r-1}$ in (5.32) will be given by

$$\sum_{x_i=0}^{p^{n+\alpha}-1} e\left(\frac{2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}}y_i'^2}{p^{n+\alpha}} \right) = G(2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}}; p^{n+\alpha}).$$

As the sum indexed by x_r in (5.32) is a quadratic Gauss sum, we arrive at the statement of our theorem. □

Theorem 5.8. *Suppose that $\alpha_i \leq \alpha_{ij}$ for all $1 \leq i < j \leq r$. Then*

$$G(Q_r; S; 2^n) = \frac{1}{2^{r(\alpha+1)}} \prod_{i=1}^{r} G(SA_iA_{i-1}2^{\alpha+\alpha_i-\alpha_{i-1}}; 2^{n+\alpha+1}).$$

Proof. The proof will follow entirely in the same manner as Theorem 5.10. We mention that we will use Theorem 4.3, (5.1) and Propositions 3.14 and 2.5. □

In light of Theorems 5.3 and 5.4, it is clear that we can achieve our results, regardless of the coefficients of Q_r, for sufficiently large n. Hence, for notational convenience in the remaining theorems, we will assume the coefficients of Q_r satisfy favorable divisibility conditions.

Theorem 5.9. *Let p be an odd prime. Suppose that we may permute the coefficients of Q_r so that for each $i = 1, \ldots, r-1$ we have*

$$\overline{\alpha_{i(i+1)}} \geq \overline{\alpha_{(i-1)i}},$$

and for every i, j, k satisfying $1 \leq i < j \leq k \leq r$ we have

$$\alpha_{ij} \leq \alpha_{ik}.$$

If $n \geq 2\overline{\alpha_{(i-1)i}} + \alpha_i - \alpha_{i-1}$ for each $i = 1, \ldots, r$, then

$$G(Q_r; S; p^n) = \frac{1}{p^{r\alpha}} \prod_{i=1}^{r} G(2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}}; p^{n+\alpha}).$$

Proof. By assumption, $\Delta \neq 0$, and so by Theorem 4.3 we have

$$\begin{aligned} G(Q_r; S; p^n) =& \frac{1}{p^{r\alpha}} \sum_{x_r=0}^{p^{n+\alpha}-1} e\left(\frac{S(2A_{r-1})^{-1}A_r p^{\alpha+\alpha_r-\alpha_{r-1}}x_r^2}{p^{n+\alpha}}\right) \times \cdots \\ &\times \sum_{x_i=0}^{p^{n+\alpha}-1} e\left(\frac{S(2A_iA_{i-1})^{-1}p^{\alpha-\alpha_i-\alpha_{i-1}}y_i^2}{p^{n+\alpha}}\right) \times \cdots \\ &\times \sum_{x_1=0}^{p^{n+\alpha}-1} e\left(\frac{S(2A_1A_0)^{-1}p^{\alpha-\alpha_1-\alpha_0}y_1^2}{p^{n+\alpha}}\right). \end{aligned} \tag{5.33}$$

Observe that $y_1 = p^{\alpha_1}A_1x_1 + \sum_{j=2}^{r} m_{1j}x_j$. By Proposition 3.7, as $n \geq \alpha_1$, the sum indexed by x_1 in (5.33) is non-zero if

$$\sum_{j=2}^{r} p^{\alpha_{1j}}A_{1j}x_j \equiv 0 \pmod{p^{\alpha_1}}. \tag{5.34}$$

For convenience, we set

$$C_i \equiv -A_{(i-1)i}^{-1}\left(\sum_{j=i+1}^{r} p^{\alpha_{(i-1)j}-\alpha_{(i-1)i}}A_{(i-1)j}x_j\right) \pmod{p^{\overline{\alpha_{(i-1)i}}}},$$

for $i = 2, \ldots, r-1$. Thus, the congruence given by (5.34) becomes

$$x_2 \equiv -A_{12}^{-1}\left(\sum_{j=3}^{r} p^{\alpha_{1j}-\alpha_{12}}A_{1j}x_j\right) \pmod{p^{\overline{\alpha_{12}}}}$$

$$x_2 \equiv C_2 \pmod{p^{\overline{\alpha_{12}}}}. \tag{5.35}$$

If we suppose that $x_2, \ldots, x_r$ satisfy the congruence given by (5.35), by Propositions 3.2, 3.7 and 3.11, the sum indexed by x_1 in (5.33) will simplify to

$$p^{\alpha} G(2SA_1; p^{n+\alpha_1}) = p^{\alpha+\alpha_1} G(2SA_1; p^{n-\alpha_1}) = G(2SA_1 p^{\alpha+\alpha_1}; p^{n+\alpha}). \tag{5.36}$$

It follows that (5.33) is non-zero whenever $x_2, \ldots, x_r$ satisfy the congruence conditions given in (5.35). Hence, we may write the sum indexed by x_2 in (5.33) as

$$\sum_{\substack{x_2=0 \\ x_2 \equiv C_2 \pmod{p^{\overline{\alpha_{12}}}}}}^{p^{n+\alpha}-1} e\left(\frac{S(2A_2A_1)^{-1} p^{\alpha-\alpha_2-\alpha_1} y_2^2}{p^{n+\alpha}}\right). \tag{5.37}$$

Regardless of the congruence condition imposed on the index of x_2 in (5.37), by Proposition 3.9, as

$$n \geq 2\overline{\alpha_{12}} + \alpha_2 - \alpha_1,$$

if the sum given in (5.37) is non-zero, it must happen that $y_2 \equiv 0 \pmod{p^{\alpha_2}}$. This means we must have

$$\begin{aligned} \sum_{j=3}^{r} p^{\alpha_{2j}} A_{2j} x_j &\equiv 0 \pmod{p^{\alpha_2}} \\ x_3 &\equiv -A_{23}^{-1} \left(\sum_{j=4}^{r} p^{\alpha_{2j}-\alpha_{23}} A_{2j} x_j\right) \pmod{p^{\overline{\alpha_{23}}}} \\ x_3 &\equiv C_3 \pmod{p^{\overline{\alpha_{23}}}}. \end{aligned}$$

We continue in this fashion. As we have

$$n \geq 2\overline{\alpha_{(i-1)i}} + \alpha_i - \alpha_{i-1},$$

for each $i = 2, \ldots, r$, we may use Proposition 3.9 to deduce that for $i = 2, \ldots, r-1$, the i^{th} term will be given by

$$\sum_{\substack{x_i=0 \\ x_i \equiv C_i \pmod{p^{\overline{\alpha_{(i-1)i}}}}}}^{p^{n+\alpha}-1} e\left(\frac{S(2A_iA_{i-1})^{-1}p^{\alpha-\alpha_i-\alpha_{i-1}}y_i^2}{p^{n+\alpha}}\right), \tag{5.38}$$

and the final term will be given by

$$\sum_{\substack{x_r=0 \\ x_r \equiv 0 \pmod{p^{\overline{\alpha_{(r-1)r}}}}}}^{p^{n+\alpha}-1} e\left(\frac{S(2A_{r-1})^{-1}A_rp^{\alpha+\alpha_r-\alpha_{r-1}}x_r^2}{p^{n+\alpha}}\right). \tag{5.39}$$

We now move back up our series of nested sums. Hence, suppose $x_r \equiv 0 \pmod{p^{\overline{\alpha_{(r-1)r}}}}$ and we write $x_r = p^{\overline{\alpha_{(r-1)r}}}x_r'$. We see then that as $\overline{\alpha_{(r-1)r}} \geq \overline{\alpha_{(r-2)(r-1)}}$, C_{r-1} can be written as

$$x_{r-1} \equiv -A_{(r-2)(r-1)}^{-1}\left(p^{\alpha_{(r-2)r}-\alpha_{(r-2)(r-1)}}A_{(r-2)r}(p^{\overline{\alpha_{(r-1)r}}}x_r')\right) \pmod{p^{\overline{\alpha_{(r-2)(r-1)}}}}$$
$$x_{r-1} \equiv 0 \pmod{p^{\overline{\alpha_{(r-2)(r-1)}}}}.$$

Continuing in this manner, as we have assumed $\overline{\alpha_{i(i+1)}} \geq \overline{\alpha_{(i-1)i}}$ for $i = 2, \ldots, r-1$, for each such i the condition C_i will be given by

$$C_i \equiv 0 \pmod{p^{\overline{\alpha_{(i-1)i}}}},$$

and so each of the sums given in (5.38) can be written as

$$\sum_{\substack{x_i=0 \\ x_i \equiv 0 \pmod{p^{\overline{\alpha_{(i-1)i}}}}}}^{p^{n+\alpha}-1} e\left(\frac{S(2A_iA_{i-1})^{-1}p^{\alpha-\alpha_i-\alpha_{i-1}}y_i^2}{p^{n+\alpha}}\right). \tag{5.40}$$

But as $n \geq 2\overline{\alpha_{(i-1)i}} + \alpha_i - \alpha_{i-1}$ for $i = 2, \ldots, r-1$, by Propositions 3.9 and 3.11, each sum

in (5.40) is given by

$$\begin{aligned} p^{\alpha-\alpha_i-\alpha_{i-1}+2\alpha_i} & G(2SA_iA_{i-1}; p^{n+\alpha-(\alpha-\alpha_i-\alpha_{i-1})-2\alpha_i}) \\ &= p^{\alpha+\alpha_i-\alpha_{i-1}} G(2SA_iA_{i-1}; p^{n+\alpha-(\alpha+\alpha_i-\alpha_{i-1})}) \\ &= G(2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}}; p^{n+\alpha}). \end{aligned} \tag{5.41}$$

We note that we evaluate these sums in the nested manner as seen in (5.33), so that the sum indexed by x_2 is considered first, and subsequently x_3, and so on in this manner until we arrive at the final sum indexed by x_{r-1}. Thus, remaining now in (5.33) is the final sum given in (5.39). As $n \geq 2\overline{\alpha_{(r-1)r}} + \alpha_r - \alpha_{r-1}$, by Corollary 3.1, (5.39) is given by

$$\begin{aligned} p^{\alpha+\alpha_r-\alpha_{r-1}} & G(2SA_rA_{r-1}; p^{n+\alpha-(\alpha+\alpha_r-\alpha_{r-1})}) \\ &= G(2SA_rA_{r-1}p^{\alpha+\alpha_r-\alpha_{r-1}}; p^{n+\alpha}). \end{aligned} \tag{5.42}$$

Hence, with (5.36), (5.41) and (5.42), (5.33) is given by

$$\frac{1}{p^{r\alpha}} \prod_{i=1}^{r} G(2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}}; p^{n+\alpha}).$$

□

The even prime case will follow in a similar manner.

Theorem 5.10. *Suppose that we may permute the coefficients of Q_r so that for all $1 \leq i < j \leq k \leq r$ we have*

$$\alpha_{ij} \leq \alpha_{ik}$$

and for each $i = 2, \ldots, r-1$ we have

$$\overline{\alpha_{i(i+1)}} \geq \overline{\alpha_{(i-1)i}}.$$

If $n \geq 2\overline{\alpha_{(i-1)i}} + \alpha_i - \alpha_{i-1} + 1$ *for* $i = 1, \ldots, r$, *then*

$$G(Q_r; S; 2^n) = \frac{1}{2^{r(\alpha+1)}} \prod_{i=1}^{r} G(SA_iA_{i-1}2^{\alpha+\alpha_i-\alpha_{i-1}}; 2^{n+\alpha+1}).$$

Proof. The proof is conducted in the same manner as in the proof of Theorem 5.10, where our conditions on n are given by Propositions 3.8, 3.10. and Corollary 3.2. This requires, respectively,

$$\begin{aligned} &n \geq \alpha_1 + 1, \\ &n \geq 2\overline{\alpha_{(i-1)i}} + \alpha_i - \alpha_{i-1} + 1 \text{ for } i = 2, \ldots, r-1, \\ &n \geq 2\overline{\alpha_{(r-1)r}}\alpha_r - \alpha_{r-1} + 1, \end{aligned}$$

which will be satisfied given the requirements of n in the statement of the theorem. □

Given a quadratic form Q_r, one can determine which theorem to use to evaluate the quadratic form Gauss sum based on the minors of Q_r. Let M be the integral symmetric matrix associated with Q_r, with leading principal minors $m_1, \ldots, m_r$ and associated minor product $\Delta = \prod_{i=1}^{r-1} m_i$. Further, for $1 \leq i < j \leq r$, we recall the mixed minors m_{ij}, which can be shown to be the determinant of the $i \times i$ leading principal submatrix of the matrix obtained by interchanging columns i and j in M. The evaluation of $G(Q_r; S; p^n)$ will depend on the parity of p and the divisibility of the minors m_i and m_{ij}.

Suppose that p is an odd prime. If we have $(\Delta, p) = 1$ then we use Theorem 5.5 to evaluate $G(Q_r; S; p^n)$. If, in addition, we have also $(m_r, p) = 1$, then $G(Q_r; S; p^n)$ is given by Corollary 5.3. Suppose that at least one minor m_i is divisible by p, for some $i = 1, \ldots, r-1$. In this case, we consider the divisibility of each mixed minor $m_{ij} \equiv p^{\alpha_{ij}} A_{ij} \pmod{p^{n+\alpha}}$. If, for each such divisible minor m_i, we have $\alpha_i \leq \alpha_{ij}$ for each $j = i+1, \ldots, r$, then we can evaluate $G(Q_r; S; p^n)$ using Theorem 5.7. Otherwise, one must be able to permute the coefficients in such a fashion that, given n sufficiently large, we may appeal to Theorem 5.9

to evaluate $G(Q_r; S; p^n)$.

Suppose now that $p = 2$. If each mixed coefficient of Q_r is divisible by 2, and $2^i \,||\, m_i$ for each $i = 1, \ldots, r-1$, then $G(Q_r; S; 2^n)$ is given by Theorem 5.6. Additionally, if we also have $2^r \,||\, m_r$, then $G(Q_r; S; 2^n)$ is given by Corollary 5.4. If instead we have, say, $2^{i+1} \mid m_i$, we must determine the greatest prime power of 2 dividing $m_{ij} \equiv 2^{\alpha_{ij}} A_{ij} \pmod{2^{n+\alpha+1}}$. Similar to the odd prime case, if we have $\alpha_i \leq \alpha_{ij}$ for every such minor m_i, then we evaluate $G(Q_r; S; 2^n)$ using Theorem 5.8. If for some i and j satisfying $1 \leq i < j \leq r$, we have $\alpha_i > \alpha_{ij}$, then assuming a favorable permutation of the coefficients, we may evaluate $G(Q_r; S; 2^n)$ using Theorem 5.10, taking n sufficiently large.

We present an example to emphasize the algorithmic nature of determining which theorem to use to evaluate $G(Q_r; S; p^n)$. For what follows, we mention that we use Propositions 3.13 and 3.14 to simplify the expression of various quadratic Gauss sums. Let

$$Q_4 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_1 x_2.$$

This has associated symmetric matrix $\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$, from which we may determine that

$$\begin{aligned} &m_1 = 2, \quad m_{12} = 1, \quad m_{13} = m_{14} = 0, \\ &m_2 = 3, \quad m_{23} = m_{24} = 0, \\ &m_3 = 6, \quad m_{34} = 0, \\ &m_4 = 12 \quad \text{and} \quad \Delta = m_1 \cdot m_2 \cdot m_3 = 36. \end{aligned}$$

For $p > 3$ prime, we have that $(\Delta m_4, p) = 1$, which satisfies the conditions of Corollary 5.3.

Thus, for $n \in \mathbb{N}$, we obtain

$$\begin{aligned} G(Q_4; S; p^n) &= G(2Sm_4m_3; p^n) \cdot G(2Sm_3m_2; p^n) \cdot G(2Sm_2m_1; p^n) \cdot G(2Sm_1; p^n) \\ &= G(144S; p^n) \cdot G(36S; p^n) \cdot G(12S; p^n) \cdot G(4S; p^n) \\ &= G(S; p^n)^3 \cdot G(3S; p^n). \end{aligned}$$

One can then determine a specific formula using Theorem 3.1.

Suppose now $p = 3$ and write $m_i = 3^{\alpha_i} A_i$ and $m_{ij} \equiv 3^{\alpha_{ij}} A_{ij} \pmod{3^{n+\alpha}}$. We see that

$$\begin{aligned} &\alpha_1 = 0, \quad \alpha_{12} = 0, \quad \alpha_{13} = n + \alpha, \quad \alpha_{14} = n + \alpha, \\ &\alpha_2 = 1, \quad \alpha_{23} = \alpha_{24} = n + \alpha, \\ &\alpha_3 = 1, \quad \alpha_{34} = n + \alpha, \\ &\alpha_4 = 1, \quad \text{and} \quad A_1 = 2, \quad A_2 = 1, \quad A_3 = 2, \quad A_4 = 4. \end{aligned}$$

Note also that $\alpha = 2$ in this case and we have $\alpha_i \leq \alpha_{ij}$ for all $1 \leq i < j \leq 4$. Therefore, by Theorem 5.7, we have

$$\begin{aligned} G(Q_4; S; 3^n) =& \frac{1}{3^8} G(2SA_4A_3 \cdot 3^{2+\alpha_4-\alpha_3}; 3^{n+2}) \cdot G(2SA_3A_2 \cdot 3^{2+\alpha_3-\alpha_2}; 3^{n+2}) \\ & \times G(2SA_2A_1 \cdot 3^{2+\alpha_2-\alpha_1}; 3^{n+2}) \cdot G(2SA_1 \cdot 3^{2+\alpha_1}; 3^{n+2}) \\ =& \frac{1}{3^8} G(16S \cdot 3^2; 3^{n+2}) \cdot G(4S \cdot 3^2; 3^{n+2}) \cdot G(4S \cdot 3^3; 3^{n+2}) \cdot G(4S \cdot 3^2; 3^{n+2}) \\ =& 3G(S; 3^n)^3 \cdot G(S; 3^{n-1}), \end{aligned}$$

where we have used Proposition 3.2 to simplify prime powers.

Finally, suppose $p = 2$. Write $m_i = 2^{\alpha_i} A_i$ and $m_{ij} \equiv 2^{\alpha_{ij}} A_{ij} \pmod{2^{n+\alpha+1}}$. Hence, we have

$$\alpha_1 = 1, \quad \alpha_{12} = 0, \quad \alpha_{13} = n + \alpha + 1, \quad \alpha_{14} = n + \alpha + 1,$$

$$\alpha_2 = 0, \quad \alpha_{23} = 1, \quad \alpha_{24} = n + \alpha + 1,$$
$$\alpha_3 = 1, \quad \alpha_{34} = n + \alpha + 1,$$
$$\alpha_4 = 2, \quad \text{and } A_1 = 1, \quad A_2 = 3, \quad A_3 = 3, \quad A_4 = 3.$$

Observe also that in this case $\alpha = 2$. Hence, as $\alpha_1 > \alpha_{12}$, we must look to Theorem 5.10 to evaluate $G(Q_4; S; 2^n)$. First, note that $\alpha_{ij} \geq \alpha_{ik}$ for all $1 \leq i < j \leq k \leq 4$. Recall that $\overline{\alpha_{ij}} = \max(\alpha_i - \alpha_{ij}, 0)$ and for convenience $\overline{\alpha_{0j}} = 0$. We see that

$$\overline{\alpha_{12}} = 1 \quad \text{and} \quad \overline{\alpha_{ij}} = 0 \quad \text{otherwise.}$$

Thus, the condition $\overline{\alpha_{i(i+1)}} \geq \overline{\alpha_{(i-1)i}}$ is not satisfied for $i = 2$. Hence, we look to permute the coefficients of the quadratic form to obtain more favorable divisibility properties. Consider instead

$$Q_4' = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_3x_4,$$

obtained by, say, $x_1 \leftrightarrow x_3$ and $x_2 \leftrightarrow x_4$. This has associated symmetric matrix $\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$, and thus we have that

$$m_1 = 2, \quad m_{12} = m_{13} = m_{14} = 0,$$
$$m_2 = 4, \quad m_{23} = m_{24} = 0,$$
$$m_3 = 8, \quad m_{34} = 4, \quad \text{and} \quad m_4 = 12.$$

Writing $m_i = 2^{\alpha_i} A_i$ and $m_{ij} \equiv 2^{\alpha_{ij}} A_{ij} \pmod{2^{n+\alpha+1}}$ as before yields

$$\begin{aligned}
&\alpha_1 = 1, \quad \alpha_{12} = \alpha_{13} = \alpha_{14} = n + \alpha + 1, \\
&\alpha_2 = 2, \quad \alpha_{23} = \alpha_{24} = n + \alpha + 1, \\
&\alpha_3 = 3, \quad \alpha_{34} = 2, \\
&\alpha_4 = 2 \quad \text{and} \quad A_1 = A_2 = A_3 = 1, A_4 = 3.
\end{aligned}$$

Observe that $\alpha = 6$ in this case. Note also that with this notation, we have $\alpha_{ij} \leq \alpha_{ik}$ as before as well as

$$\overline{\alpha_{1j}} = 0, \quad \overline{\alpha_{2j}} = 0, \quad \overline{\alpha_{34}} = 1.$$

Thus, $\overline{\alpha_{i(i+1)}} \geq \overline{\alpha_{(i-1)i}}$ for $i = 2, 3$ which means that the conditions of Theorem 5.10 are satisfied for n sufficiently large. We require that n satisfies $n \geq 2\overline{\alpha_{(i-1)i}} + \alpha_i - \alpha_{i-1} + 1$ for $i = 1, \ldots, 4$. Hence, we have that

$$\begin{aligned}
2\overline{\alpha_{34}} + \alpha_4 - \alpha_3 + 1 &= 2, \\
2\overline{\alpha_{23}} + \alpha_3 - \alpha_2 + 1 &= 2, \\
2\overline{\alpha_{12}} + \alpha_2 - \alpha_1 + 1 &= 2, \\
2\overline{\alpha_{01}} + \alpha_1 - \alpha_0 + 1 &= 2,
\end{aligned}$$

where $\alpha_0 = 0$. Thus, if $n \geq 2$, Theorem 5.10 states

$$\begin{aligned}
G(Q_4'; S; 2^n) =& \frac{1}{2^{28}} G(SA_4A_3 \cdot 2^{6+\alpha_4-\alpha_3}; 2^{n+7}) \cdot G(SA_3A_2 \cdot 2^{6+\alpha_3-\alpha_2}; 2^{n+7}) \\
&\times G(SA_2A_1 \cdot 2^{6+\alpha_2-\alpha_1}; 2^{n+7}) \cdot G(SA_1 \cdot 2^{6+\alpha_1}; 2^{n+7}) \\
=& \frac{1}{2^{28}} G(3S \cdot 2^5; 2^{n+7}) \cdot G(S \cdot 2^7; 2^{n+7})^3 \\
=& \frac{1}{2^2} G(3S; 2^{n+2}) \cdot G(S; 2^n)^3,
\end{aligned}$$

where as before we have used Proposition 3.2 for simplification. This re-indexing method suggests that the coefficient conditions as stated in Theorem 5.10 can be improved.

5.4 Explicit Formula for General Quadratic Form Gauss Sums

We would like to give a general expression for $G(Q_r; S; p^n)$. We will use Theorems 5.5-5.11 to deduce these formulas. We begin with the odd prime cases first, and subsequently the even prime case.

Theorem 5.11. *Let p be an odd prime and Q_r satisfy the conditions of Theorem 5.5. Then*

$$G(Q_r; S; p^n) = \left(\frac{2S}{p}\right)^{nr+\alpha_r} \left(\frac{A_{r-1}}{p}\right)^{\alpha_r} \left(\frac{A_r}{p}\right)^{n+\alpha_r} p^{\frac{nr+\alpha_r}{2}} i^{(r-1)\left(\frac{p^n-1}{2}\right)^2} i^{\left(\frac{p^{n+\alpha_r}-1}{2}\right)^2}.$$

Proof. From Theorems 3.1 and 5.5, we have

$$\begin{aligned} G(Q_r; S; p^n) &= G(2Sm_rA_{r-1}; p^n) \prod_{i=1}^{r-1} G(2SA_iA_{i-1}; p^n) \\ &= G(2SA_rA_{r-1}p^{\alpha_r}; p^n) \prod_{i=1}^{r-1} \left(\frac{2SA_iA_{i-1}}{p}\right)^n p^{\frac{n}{2}} i^{\left(\frac{p^n-1}{2}\right)^2} \\ &= G(2SA_rA_{r-1}p^{\alpha_r}; p^n) \left(\frac{2S}{p}\right)^{(r-1)n} \left(\frac{A_{r-1}}{p}\right)^n p^{\frac{(r-1)n}{2}} i^{(r-1)\left(\frac{p^n-1}{2}\right)^2}. \end{aligned} \tag{5.43}$$

If $\alpha_r < n$, from Theorem 3.1 and Proposition 3.2, we have

$$G(2SA_{r-1}A_rp^{\alpha_r}; p^n) = p^{\alpha_r} G(2SA_{r-1}A_r; p^{n-\alpha_r}) = p^{\frac{n+\alpha_r}{2}} \left(\frac{2SA_{r-1}A_r}{p}\right)^{n+\alpha_r} i^{\left(\frac{p^{n+\alpha}-1}{2}\right)^2}. \tag{5.44}$$

Combining (5.43) and (5.44) will yield the statement of the theorem. Otherwise, if $\alpha_r = n$,

$G(2SA_{r-1}A_rp^{\alpha_r};p^n)=p^n$ and in this case (5.43) becomes

$$\left(\frac{2S}{p}\right)^{(r-1)n}\left(\frac{A_{r-1}}{p}\right)^n p^{\frac{(r+1)n}{2}}i^{(r-1)\left(\frac{p^n-1}{2}\right)^2},$$

which will simplify to the statement of the theorem.

□

If the determinant of the quadratic form is non-zero and coprime to p, we have the following obvious corollary.

Corollary 5.5. *Let p be an odd prime and Q_r satisfy the conditions of Theorem 5.5. Then if $(m_r,p)=1$ we have*

$$G(Q_r;S;p^n)=\left(\frac{(2S)^rA_r}{p}\right)^n p^{\frac{nr}{2}}i^{r\left(\frac{p^n-1}{2}\right)^2}.$$

Proof. This follows from Theorem 5.14 with $\alpha_r=0$. □

Theorem 5.12. *Let p be an odd prime and let Q_r satisfy the conditions of Theorem 5.10. Then if $n\geq\alpha_i-\alpha_{i-1}$ for each $i=1,\ldots,r$, $G(Q_r;S;p^n)$ is given by*

$$p^{\frac{rn+\alpha_r}{2}}\left(\frac{2S}{p}\right)^{rn+\alpha_r}\left(\frac{A_r}{p}\right)^{n+\alpha_r+\alpha_{r-1}}\prod_{i=1}^{r-1}\left(\frac{A_i}{p}\right)^{\alpha_{i-1}+\alpha_{i+1}}$$
$$\times\left(\frac{-1}{p}\right)^{\sum_{1\leq i\leq r-1}\alpha_i(1+\alpha_{i+1})}\begin{cases}\left(\frac{-1}{p}\right)^{n(\alpha_r+\frac{r}{2})}i^{\left(\frac{p^{\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 0 \pmod 2\\ \left(\frac{-1}{p}\right)^{n(\frac{r-1}{2})}i^{\left(\frac{p^{n+\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 1 \pmod 2.\end{cases}$$

Proof. From Theorem 3.1, Proposition 3.2 and Theorem 5.10, we have that

$$\begin{aligned}G(Q_r;s;p^n)=&\frac{1}{p^{r\alpha}}\prod_{i=1}^{r}G(2SA_iA_{i-1}p^{\alpha+\alpha_i-\alpha_{i-1}};p^{n+\alpha})\\ =&\frac{1}{p^{r\alpha}}\prod_{i=1}^{r}p^{\alpha+\alpha_i-\alpha_{i-1}}G(2SA_iA_{i-1};p^{n-(\alpha_i-\alpha_{i-1})})\end{aligned}$$

$$
\begin{aligned}
&= \prod_{i=1}^{r} p^{\frac{n+\alpha_i-\alpha_{i-1}}{2}} \left(\frac{2SA_iA_{i-1}}{p}\right)^{n+\alpha_i+\alpha_{i-1}} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2} \\
&= p^{\frac{rn+\alpha_r}{2}} \prod_{i=1}^{r} \left(\frac{2SA_iA_{i-1}}{p}\right)^{n+\alpha_i+\alpha_{i-1}} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2}. \qquad (5.45)
\end{aligned}
$$

Thus, we examine in turn the factors in the product expression of (5.45). First, observe that

$$
\begin{aligned}
\prod_{i=1}^{r} \left(\frac{2SA_iA_{i-1}}{p}\right)^{n+\alpha_i+\alpha_i} &= \left(\prod_{i=1}^{r} \left(\frac{2SA_iA_{i-1}}{p}\right)^{n}\right) \left(\prod_{i=1}^{r} \left(\frac{2SA_iA_{i-1}}{p}\right)^{\alpha_i+\alpha_{i-1}}\right) \\
&= \left(\frac{2S}{p}\right)^{nr} \left(\frac{A_r}{p}\right)^{n} \left(\frac{2S}{p}\right)^{\alpha_r} \left(\frac{A_r}{p}\right)^{\alpha_r+\alpha_{r-1}} \prod_{i=1}^{r-1} \left(\frac{A_i}{p}\right)^{\alpha_{i-1}+\alpha_{i+1}} \\
&= \left(\frac{2S}{p}\right)^{rn+\alpha_r} \left(\frac{A_r}{p}\right)^{n+\alpha_r+\alpha_{r-1}} \prod_{i=1}^{r-1} \left(\frac{A_i}{p}\right)^{\alpha_{i-1}+\alpha_{i+1}}. \qquad (5.46)
\end{aligned}
$$

It remains to evaluate $\prod_{i=1}^{r} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2}$. We assume that r is sufficiently large so we may deduce a pattern from this expression. Using Proposition 2.16, we have that

$$
\begin{aligned}
\prod_{i=1}^{r} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2} &= i^{\left(\frac{p^{n+\alpha_1}-1}{2}\right)^2} i^{\left(\frac{p^{n+\alpha_1+\alpha_2}-1}{2}\right)^2} \prod_{i=3}^{r} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2} \\
&= \left(\frac{-1}{p}\right)^{n(\alpha_2+1)+\alpha_1(\alpha_2+1)} i^{\left(\frac{p^{\alpha_2}-1}{2}\right)^2} i^{\left(\frac{p^{n+\alpha_3+\alpha_2}-1}{p}\right)^2} \prod_{i=4}^{r} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2} \\
&= \left(\frac{-1}{p}\right)^{n+\sum_{1\le i\le 2}\alpha_i(\alpha_{i+1}+1)} i^{\left(\frac{p^{n+\alpha_3}-1}{2}\right)^2} i^{\left(\frac{p^{n+\alpha_3+\alpha_4}-1}{2}\right)^2} \prod_{i=5}^{r} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2} \\
&= \left(\frac{-1}{p}\right)^{n\alpha_4+\sum_{1\le i\le 3}\alpha_i(\alpha_{i+1}+1)} i^{\left(\frac{p^{\alpha_4}-1}{2}\right)^2} i^{\left(\frac{p^{n+\alpha_4+\alpha_5}-1}{2}\right)^2} \prod_{i=6}^{r} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2} \\
&= \left(\frac{-1}{p}\right)^{\sum_{1\le i\le 4}\alpha_i(\alpha_{i+1}+1)} i^{\left(\frac{p^{n+\alpha_5}-1}{2}\right)^2} i^{\left(\frac{p^{n+\alpha_5+\alpha_6}-1}{2}\right)^2} \prod_{i=7}^{r} i^{\left(\frac{p^{n+\alpha_i+\alpha_{i-1}}-1}{2}\right)^2}.
\end{aligned} \qquad (5.47)
$$

Continuing in this fashion we see that this product will depend on the residue class of r

modulo 4. Hence, we see that (5.47) is given by

$$\begin{aligned}
&\left(\frac{-1}{p}\right)^{\sum_{1\le i\le r-1}\alpha_i(\alpha_{i+1}+1)}\begin{cases}\left(\frac{-1}{p}\right)^{n(\alpha_r+1)} i^{\left(\frac{p^{\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 2 \pmod 4\\ \left(\frac{-1}{p}\right)^{n} i^{\left(\frac{p^{n+\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 3 \pmod 4\\ \left(\frac{-1}{p}\right)^{n\alpha_r} i^{\left(\frac{p^{\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 0 \pmod 4\\ i^{\left(\frac{p^{n+\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 1 \pmod 4.\end{cases}\\
&=\left(\frac{-1}{p}\right)^{\sum_{1\le i\le r-1}\alpha_i(\alpha_{i+1}+1)}\begin{cases}\left(\frac{-1}{p}\right)^{n(\frac{r-1}{2})} i^{\left(\frac{p^{n+\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 1 \pmod 2\\ \left(\frac{-1}{p}\right)^{n(\alpha_r+\frac{r}{2})} i^{\left(\frac{p^{\alpha_r}-1}{2}\right)^2} & \text{if } r\equiv 0 \pmod 2.\end{cases}
\end{aligned}\tag{5.48}$$

Hence, with (5.45), (5.46) and (5.48) we arrive at the statement of the theorem. □

Finally, we have similar theorems for the even prime cases.

Theorem 5.13. *Let Q_r satisfy the conditions of Theorem 5.6 and let $m_r \equiv 2^r \cdot 2^{\alpha'_r} A'_r \pmod{2^{n+\alpha+1}}$. If $\alpha'_r \ge n$, then $G(Q_r; S; 2^n)$ is given by*

$$2^{\frac{(r+1)n}{2}}\left(\frac{2}{S}\right)^{(r-1)n}\left(\frac{2}{A_{r-1}}\right)^{n}\begin{cases}\displaystyle\prod_{i=1}^{\frac{r-1}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r\equiv 1 \pmod 2\\ \displaystyle(1+i^{SA_{r-1}A_{r-2}})\prod_{i=1}^{\frac{r-2}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r\equiv 0 \pmod 2\end{cases}$$

If $\alpha'_r < n$, then $G(Q_r; S; 2^n)$ is given by

$$\begin{aligned}
&2^{\frac{nr+\alpha'_r}{2}}\left(\frac{2}{S}\right)^{rn+\alpha'_r}\left(\frac{2}{A_{r-1}}\right)^{\alpha'_r}\left(\frac{2}{A_r}\right)^{n+\alpha'_r}\\
&\qquad\times\begin{cases}\displaystyle\prod_{i=1}^{\frac{r}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r\equiv 0 \pmod 2\\ \displaystyle(1+i^{SA_rA_{r-1}})\prod_{i=1}^{\frac{r-1}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r\equiv 1 \pmod 2.\end{cases}
\end{aligned}$$

Proof. We write $\alpha_r = \alpha'_r + r$. In this fashion, we have

$$m_r \equiv 2^r m'_r \equiv 2^{r+\alpha'_r} A_r \equiv 2^{\alpha_r} A_r \pmod{2^{n+\alpha+1}}.$$

Hence, by Theorem 5.6, we have

$$\begin{aligned} G(Q_r; S; 2^n) &= G(SA_{r-1}A_r 2^{\alpha'_r}; 2^n) \prod_{i=1}^{r-1} G(SA_iA_{i-1}; 2^n) \\ &= G(SA_{r-1}A_r 2^{\alpha'_r}; 2^n) \prod_{i=1}^{r-1} \left(\frac{2}{SA_iA_{i-1}}\right)^n (1 + i^{SA_iA_{i-1}}) 2^{\frac{n}{2}} \\ &= G(SA_{r-1}A_r 2^{\alpha'_r}; 2^n) 2^{\frac{(r-1)n}{2}} \left(\frac{2}{S}\right)^{(r-1)n} \left(\frac{2}{A_{r-1}}\right)^n \prod_{i=1}^{r-1} (1 + i^{SA_iA_{i-1}}). \end{aligned} \tag{5.49}$$

If $\alpha'_r \geq n$, then $G(SA_{r-1}A_r 2^{\alpha'_r}; 2^n) = 2^n$. By Proposition 2.20, we have that

$$\begin{aligned} &\prod_{i=1}^{r-1} \left(1 + i^{SA_iA_{i-1}}\right) \\ &= \begin{cases} \displaystyle\prod_{i=1}^{\frac{r-1}{2}} \left(1 + i^{SA_{2i-1}A_{2i-2}}\right)\left(1 + i^{SA_{2i-1}A_{2i}}\right) & \text{if } r \equiv 1 \pmod 2 \\ \left(1 + i^{SA_{r-1}A_{r-2}}\right) \displaystyle\prod_{i=1}^{\frac{r-2}{2}} \left(1 + i^{SA_{2i-1}A_{2i-2}}\right)\left(1 + i^{SA_{2i-1}A_{2i}}\right) & \text{if } r \equiv 0 \pmod 2. \end{cases} \\ &= \begin{cases} \displaystyle\prod_{i=1}^{\frac{r-1}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r \equiv 1 \pmod 2 \\ \left(1 + i^{SA_{r-1}A_{r-2}}\right) \displaystyle\prod_{i=1}^{\frac{r-2}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r \equiv 0 \pmod 2. \end{cases} \end{aligned} \tag{5.50}$$

Thus, with (5.49) and (5.50), we arrive at the first statement of the theorem in this case. Otherwise, for $\alpha'_r < n$, by Theorem 3.1 and Proposition 3.2, we have

$$\begin{aligned} G(SA_{r-1}A_r 2^{\alpha'_r}; 2^n) &= 2^{\alpha'_r} G(SA_{r-1}A_r; 2^{n-\alpha'_r}) \\ &= 2^{\frac{n+\alpha'_r}{2}} \left(\frac{2}{SA_{r-1}A_r}\right)^{n+\alpha'_r} \prod_{i=1}^{r} (1 + i^{SA_iA_{i-1}}). \end{aligned} \tag{5.51}$$

By similar reasoning to (5.50), it follows that

$$\prod_{i=1}^{r}(1+i^{SA_iA_{i-1}}) = \begin{cases} \displaystyle\prod_{i=1}^{\frac{r}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r \equiv 0 \pmod 2 \\ (1+i^{SA_rA_{r-1}}) \displaystyle\prod_{i=1}^{\frac{r-1}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r \equiv 1 \pmod 2. \end{cases} \tag{5.52}$$

We combine (5.49), (5.51) and (5.52) to arrive at the remaining statement of the theorem. □

Corollary 5.6. *Let Q_r be a quadratic form satisfying the conditions of Theorem 5.6 and suppose $2^r \,||\, m_r$. Then*

$$G(Q_r;S;2^n) = 2^{\frac{nr}{2}}\left(\frac{2}{(S)^rA_r}\right)^n \begin{cases} \displaystyle\prod_{i=1}^{\frac{r}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \textit{if } r \equiv 0 \pmod 2 \\ (1+i^{SA_rA_{r-1}}) \displaystyle\prod_{i=1}^{\frac{r-1}{2}} 2i^{SA_{2i-1}A_{2i}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \textit{if } r \equiv 1 \pmod 2. \end{cases}$$

Proof. This will follow from Theorem 5.16 with $\alpha_r' = 0$. □

Theorem 5.14. *Let Q_r be a quadratic form satisfying the conditions of Theorem 5.11. If $n \geq \alpha_i - \alpha_{i-1} + 1$ for $i = 1, \ldots, r$, then $G(Q_r; s; 2^n)$ is given by*

$$2^{\frac{r(n-1)+\alpha_r}{2}}\left(\frac{2}{S}\right)^{r(n+1)+\alpha_r}\left(\frac{2}{A_r}\right)^{n+1+\alpha_r+\alpha_{r-1}}\prod_{i=1}^{r-1}\left(\frac{2}{A_i}\right)^{\alpha_{i-1}+\alpha_{i+1}} \times \begin{cases} \displaystyle\prod_{i=1}^{\frac{r}{2}} 2i^{SA_{2i-1}A_{2i-2}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \textit{if } r \textit{ even} \\ (1+i^{SA_rA_{r-1}}) \displaystyle\prod_{i=1}^{\frac{r-1}{2}} 2i^{SA_{2i-1}A_{2i-2}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \textit{if } r \textit{ odd.} \end{cases}$$

Proof. Observe that as $n \geq \alpha_i - \alpha_{i-1} + 1$, none of the Gauss sums in the statement of Theorem 5.11 will have a modulus congruent to 2 (mod 4). Thus, from Theorem 3.1, Proposition 3.2

and Theorem 5.11 we have

$$\begin{aligned} G(Q_r;S;2^n) &= \frac{1}{2^{r(\alpha+1)}}\prod_{i=1}^{r} G(SA_iA_{i-1}2^{\alpha+\alpha_i-\alpha_{i-1}};2^{n+\alpha+1}) \\ &= \frac{1}{2^{r(\alpha+1)}}\prod_{i=1}^{r} 2^{\alpha+\alpha_i-\alpha_{i-1}} G(SA_iA_{i-1};2^{n+1-\alpha_i+\alpha_{i-1}}) \\ &= \frac{1}{2^r}\prod_{i=1}^{r} 2^{\frac{n+\alpha_i-\alpha_{i-1}+1}{2}} \left(\frac{2}{SA_iA_{i-1}}\right)^{n+\alpha_i+\alpha_{i-1}+1} (1+i^{SA_iA_{i-1}}) \\ &= 2^{\frac{r(n-1)+\alpha_r}{2}}\prod_{i=1}^{r} \left(\frac{2}{SA_iA_{i-1}}\right)^{n+\alpha_i+\alpha_{i-1}+1} (1+i^{SA_iA_{i-1}}). \end{aligned} \tag{5.53}$$

We examine the factors of (5.53) individually. First, we have

$$\begin{aligned} &\prod_{i=1}^{r} \left(\frac{2}{SA_iA_{i-1}}\right)^{n+\alpha_i+\alpha_{i-1}+1} \\ &\quad= \left(\frac{2}{S}\right)^{r(n+1)} \prod_{i=1}^{r} \left(\frac{2}{S}\right)^{\alpha_i+\alpha_{i-1}} \prod_{i=1}^{r} \left(\frac{2}{A_iA_{i-1}}\right)^{n+1} \prod_{i=1}^{r} \left(\frac{2}{A_iA_{i-1}}\right)^{\alpha_i+\alpha_{i-1}} \\ &\quad= \left(\frac{2}{S}\right)^{r(n+1)+\alpha_r} \left(\frac{2}{A_r}\right)^{n+1+\alpha_r+\alpha_{r-1}} \prod_{i=1}^{r-1} \left(\frac{2}{A_i}\right)^{\alpha_{i-1}+\alpha_{i+1}}. \end{aligned} \tag{5.54}$$

Finally, by Proposition 2.20 and similar to the proof of Theorem 5.16, we deduce that

$$\prod_{i=1}^{r}(1+i^{SA_iA_{i-1}}) = \begin{cases} \displaystyle\prod_{i=1}^{\frac{r}{2}} 2i^{SA_{2i-1}A_{2i-2}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r \text{ even} \\ \displaystyle(1+i^{SA_rA_{r-1}})\prod_{i=1}^{\frac{r-1}{2}} 2i^{SA_{2i-1}A_{2i-2}\left(\frac{A_{2i-2}+A_{2i}}{2}\right)^2} & \text{if } r \text{ odd.} \end{cases} \tag{5.55}$$

Hence, with (5.53), (5.54) and (5.55) we arrive at the statement of the theorem. □

Chapter 6

Applications

In this chapter, we will use our results for the binary quadratic form Gauss sum to determine the number of solutions to a binary quadratic form congruence. Thus, for this chapter, we let $a, b, c \in \mathbb{Z}$ be such that $a \neq 0$ and $(a, b, c) = 1$. For now, we let p denote an arbitrary prime, $S \in \mathbb{Z}$ will be coprime to p and we let $n \in \mathbb{N}$ arbitrarily. We emphasize that S is coprime to the modulus, as we will use s for indexing. For $k \in \mathbb{Z}$, we will determine the number of solutions to the congruence

$$ax^2 + bxy + cy^2 \equiv k \pmod{p^n}. \tag{6.1}$$

If we let $N_{p^n}(a, b, c; k)$ denote the number of solutions to the congruence given in (6.1), then we have

$$N_{p^n}(a, b, c; k) = \frac{1}{p^n} \sum_{s=0}^{p^n-1} \sum_{x,y=0}^{p^n-1} e\left(\frac{s(ax^2 + bxy + cy^2 - k)}{p^n}\right). \tag{6.2}$$

By evaluating the sum given in (6.2) we can determine the values of $N_{p^n}(a, b, c; k)$. We have the following theorem to aid in this evaluation.

Theorem 6.1. *Let p be any prime and $n \in \mathbb{N}$. Then for $k \in \mathbb{Z}$ we have that*

$$N_{p^n}(a,b,c;k) = p^n \left(1 + \sum_{t=1}^{n} \frac{1}{p^{2t}} \sum_{\substack{S<p^t \\ (S,p)=1}} e\left(\frac{S(-k)}{p^t}\right) G(Q_2;S;p^t) \right).$$

Proof. From (6.2), we have

$$N_{p^n}(a,b,c;k) = \frac{1}{p^n} \sum_{s=0}^{p^n-1} \sum_{x,y=0}^{p^n-1} e\left(\frac{s(ax^2+bxy+cy^2-k)}{p^n}\right). \tag{6.3}$$

We break up this sum by isolating the index position $s = 0$, and hence (6.3) becomes

$$\begin{aligned}
&\frac{1}{p^n} \sum_{x,y=0}^{p^n-1} 1 + \frac{1}{p^n} \sum_{s=1}^{p^n-1} \sum_{x,y=0}^{p^n-1} e\left(\frac{s(ax^2+bxy+cy^2-k)}{p^n}\right) \\
&\qquad = p^n + \frac{1}{p^n} \sum_{s=1}^{p^n-1} e\left(\frac{s(-k)}{p^n}\right) G(Q_2;s;p^n) \\
&\qquad = p^n + \frac{1}{p^n} \sum_{t=0}^{n-1} \sum_{\substack{s=1 \\ p^t||s}}^{p^n-1} e\left(\frac{s(-k)}{p^n}\right) G(Q_2;s;p^n) \\
&\qquad = p^n + \frac{1}{p^n} \sum_{t=0}^{n-1} \sum_{\substack{p^tS=1 \\ (S,p)=1}}^{p^n-1} e\left(\frac{p^tS(-k)}{p^n}\right) G(Q_2;Sp^t;p^n) \\
&\qquad = p^n + \frac{1}{p^n} \sum_{t=0}^{n-1} \sum_{\substack{S<p^{n-t} \\ (S,p)=1}} e\left(\frac{S(-k)}{p^{n-t}}\right) p^{2t} G(Q_2;S;p^{n-t}).
\end{aligned}$$

We re-index this sum by sending $t \mapsto n-t$ and collect the common factor p^n to arrive at the statement of the theorem.

□

From now on, p will denote an odd prime. We proceed to determine the number of solutions to the congruence given by (6.1) by considering the odd prime case and subsequently the even prime case. We will have some preliminary results for both cases to aid in these

evaluations.

6.1 Sums of Legendre Symbols

Evaluating the number of solutions $N_{2^n}(a,b,c;k)$ will depend on the value of the quadratic Gauss sum. Each non-zero quadratic Gauss sum with prime power modulus will contain a Legendre symbol in its explicit formula. By Theorem 6.1, we see that we will need to consider sums of Legendre symbols. We have various propositions to aid in this evaluation.

Proposition 6.1. *We have* $G(1;p) = \sum_{x=1}^{p-1} e\left(\frac{x}{p}\right)\left(\frac{x}{p}\right)$.

Proof. We have that

$$\begin{aligned} G(1;p) &= \sum_{x=0}^{p-1} e\left(\frac{x^2}{p}\right) = 1 + \sum_{x=1}^{p-1} e\left(\frac{x^2}{p}\right) = 1 + 2 \sum_{\substack{x=1 \\ x \text{ is a quadratic residue}}}^{p-1} e\left(\frac{x}{p}\right) \\ &= 1 + 2\sum_{x=1}^{p-1} e\left(\frac{x}{p}\right) \cdot \frac{1}{2}\left(1 + \left(\frac{x}{p}\right)\right) \\ &= 1 + \sum_{x=1}^{p-1} e\left(\frac{x}{p}\right) + \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) \cdot e\left(\frac{x}{p}\right) \\ &= \sum_{x=0}^{p-1} e\left(\frac{x}{p}\right) + \sum_{x=1}^{p-1} e\left(\frac{x}{p}\right)\left(\frac{x}{p}\right) = \sum_{x=1}^{p-1} e\left(\frac{x}{p}\right)\left(\frac{x}{p}\right). \end{aligned}$$

□

The preceding proposition is a common generalization of the quadratic Gauss sum, which we will need in our evaluation of $N_{p^n}(a,b,c;k)$. We now turn to sums of Legendre symbols. We must differentiate between the even and odd prime cases.

Definition 6.2. Let $u, v \in \mathbb{N}_0$. For p an odd prime and $S \in \mathbb{Z}$ coprime to p, we define

$$H_p(S;u,v) = \sum_{x=u}^{v} \left(\frac{S}{p}\right)^x.$$

The following sums occur quite frequently in our evaluation of the number of solutions for the odd prime case.

Proposition 6.2. *Let $u, v \in \mathbb{N}_0$ be such that $u \leq v$. Then*

$$H_p(S; u, v) = \begin{cases} \left[\frac{v-u+1}{2}\right] + \left(\frac{S}{p}\right)\left[\frac{v-u+2}{2}\right] & \text{if } u \text{ odd} \\ \left[\frac{v-u+2}{2}\right] + \left(\frac{S}{p}\right)\left[\frac{v-u+1}{2}\right] & \text{if } u \text{ even.} \end{cases}$$

Proof. By Definition 6.2,

$$H_p(S; u, v) = \sum_{x=u}^{v} \left(\frac{S}{p}\right)^x = \sum_{\substack{x=u \\ x \text{ even}}}^{v} 1 + \left(\frac{S}{p}\right) \sum_{\substack{x=u \\ x \text{ odd}}}^{v} 1. \tag{6.4}$$

If u is even, then we map $x \mapsto x + u$ in each sum given in (6.4) to obtain

$$\sum_{\substack{x=0 \\ x \text{ even}}}^{v-u} 1 + \left(\frac{S}{p}\right) \sum_{\substack{x=0 \\ x \text{ odd}}}^{v-u} 1.$$

Subsequently, we map $x \mapsto 2y$ in our first sum, and $x \mapsto 2y + 1$ in our second sum, which yields

$$\sum_{y=0}^{\left[\frac{v-u}{2}\right]} 1 + \left(\frac{S}{p}\right) \sum_{y=0}^{\left[\frac{v-u-1}{2}\right]} 1 = \left[\frac{v-u}{2}\right] + 1 + \left(\frac{S}{p}\right)\left(\left[\frac{v-u-1}{2}\right] + 1\right),$$

which will simplify to the statement of the proposition. If u is odd, we map $x \mapsto x + u - 1$ in each sum in (6.4) as before to get

$$\sum_{\substack{x=1 \\ x \text{ even}}}^{v-u+1} 1 + \left(\frac{S}{p}\right) \sum_{\substack{x=1 \\ x \text{ odd}}}^{v-u+1} 1.$$

We map $x \mapsto 2y$ and $x \mapsto 2y+1$ as before and our sum becomes

$$\sum_{y=1}^{\left[\frac{v-u+1}{2}\right]} 1 + \left(\frac{S}{p}\right) \sum_{y=0}^{\left[\frac{v-u}{2}\right]} 1 = \left[\frac{v-u+1}{2}\right] + \left(\frac{S}{p}\right)\left(\left[\frac{v-u}{2}\right]+1\right),$$

which simplifies to the statement of the proposition. □

It will be convenient to establish the following proposition.

Proposition 6.3. *For $u, v \in \mathbb{N}_0$ the following hold:*

(a) $H_p(S; u, v) = 0$ *if* $u > v$,

(b) $H_p(S; u, v) = \left(\frac{v-u+1}{2}\right)\left(1 + \left(\frac{S}{p}\right)\right)$ *if* $u \not\equiv v \pmod 2$ *and* $u \leq v$,

(c) $H_p(S; u, v) = \left(\frac{v-u}{2}\right)\left(1 + \left(\frac{S}{p}\right)\right) + \left(\frac{S}{p}\right)^u$ *if* $u \equiv v \pmod 2$ *and* $u \leq v$,

(d) $H_p(S; u, v) \geq -1$ *if* $u \leq v$.

Proof. For part (a), as $u > v$ we have $v - u \leq -1$ which means

$$0 \leq \left[\frac{v-u+1}{2}\right] \leq \left[\frac{v-u+2}{2}\right] \leq \left[\frac{1}{2}\right] = 0.$$

Thus, by Proposition 6.2 we will deduce our result for (a).

For (b), by Proposition 6.2, regardless of the parity of u, if $u \not\equiv v \pmod 2$ we have

$$H_p(S; u, v) = \left(\frac{v-u+1}{2}\right)\left(1 + \left(\frac{S}{p}\right)\right).$$

Next, for (c), assume that $u \equiv v \pmod 2$. By Proposition 6.2, if u is odd we have that

$$H_p(S; u, v) = \left(\frac{v-u}{2}\right)\left(1 + \left(\frac{S}{p}\right)\right) + \left(\frac{S}{p}\right).$$

Otherwise, if u is even we have

$$H_p(S;u,v) = 1 + \left(\frac{v-u}{2}\right)\left(1 + \left(\frac{S}{p}\right)\right).$$

Based on the parity of u we arrive at the expression for (c). Finally, for (d), we note that $\left(1 + \left(\frac{S}{p}\right)\right) \geq 0$. Hence, from (c) we have $H_p(S;u,v) \geq \left(\frac{S}{p}\right) \geq -1$. □

The above proposition will not only be notationally convenient, but will also allow us to show that the expressions for the number of solutions yield non-negative integer values. We introduce similar notation for the even prime case.

Definition 6.3. Let $u, v \in \mathbb{N}_0$. Then for $S \in \mathbb{Z}$ odd we define

$$P_S(u,v) = \sum_{t=u}^{v} \left(\frac{2}{S}\right)^t$$

We have some propositions to aid in evaluation of this expression.

Proposition 6.4. *Let $u, v \in \mathbb{N}_0$ be such that $u \leq v$. Then*

$$P_S(u,v) = \left\lceil \frac{v+2}{2} \right\rceil - \left\lceil \frac{u+1}{2} \right\rceil + \left(\frac{2}{S}\right)\left(\left\lceil \frac{v+1}{2} \right\rceil + \left\lfloor \frac{u}{2} \right\rfloor\right).$$

Proof. By Definition 6.3, we have

$$\begin{aligned}
P_S(u,v) = \sum_{t=u}^{v} \left(\frac{2}{S}\right)^t &= \sum_{\substack{t=u \\ t \text{ even}}}^{v} 1 + \left(\frac{2}{S}\right) \sum_{\substack{t=u \\ t \text{ odd}}}^{v} 1 \\
&= \sum_{t=\left\lceil \frac{u+1}{2} \right\rceil}^{\left\lceil \frac{v}{2} \right\rceil} 1 + \left(\frac{2}{S}\right) \sum_{t=\left\lceil \frac{u}{2} \right\rceil}^{\left\lceil \frac{v-1}{2} \right\rceil} 1 \\
&= \left\lceil \frac{v}{2} \right\rceil - \left\lceil \frac{u+1}{2} \right\rceil + 1 + \left(\frac{2}{S}\right)\left(\left\lceil \frac{v-1}{2} \right\rceil + \left\lceil \frac{u}{2} \right\rceil + 1\right) \\
&= \left\lceil \frac{v+2}{2} \right\rceil - \left\lceil \frac{u+1}{2} \right\rceil + \left(\frac{2}{S}\right)\left(\left\lceil \frac{v+1}{2} \right\rceil + \left\lfloor \frac{u}{2} \right\rfloor\right).
\end{aligned}$$

□

Proposition 6.5. *For $u, v \in \mathbb{N}_0$, the following hold:*

(a) $P_S(u,v) = 0$ *if* $u > v$,

(b) $P_S(u,v) = \left(\frac{2}{S}\right)^v + \left(\frac{v-u}{2}\right)\left(1+\left(\frac{2}{S}\right)\right)$ *if* $u \equiv v \pmod 2$, $u \leq v$,

(c) $P_S(u,v) = \left(\frac{v-u+1}{2}\right)\left(1+\left(\frac{2}{S}\right)\right)$ *if* $u \not\equiv v \pmod 2$, $u \leq v$,

(d) $P_S(u,v) \geq -1$.

Proof. For (a), as $u > v$, by Definition 6.3 this will be an empty sum. Thus, we may assume now that $u \leq v$. Next, for (b), suppose first that $u \equiv v \pmod 2$ and u is even. Then from Proposition 6.4, we have

$$P_S(u,v) = \frac{v+2}{2} - \left(\frac{u}{2}\right) + \left(\frac{2}{S}\right)\left(\frac{v}{2} - \frac{u}{2}\right) = 1 + \left(\frac{v-u}{2}\right)\left(1+\left(\frac{2}{S}\right)\right).$$

Otherwise, for $u \equiv v \pmod 2$ and v odd, we have

$$\begin{aligned} P_S(u,v) &= \frac{v+1}{2} - \left(\frac{u+1}{2}\right) + \left(\frac{2}{S}\right)\left(\frac{v+1}{2} - \left(\frac{u-1}{2}\right)\right) \\ &= \left(\frac{2}{S}\right) + \left(\frac{v-u}{2}\right)\left(1+\left(\frac{2}{S}\right)\right). \end{aligned}$$

Due to the parity of v, the statement of the proposition for (b) will hold.

Suppose now that $u \not\equiv v \pmod 2$. If v is even, we have

$$P_S(u,v) = \frac{v+2}{2} - \left(\frac{u+1}{2}\right) + \left(\frac{2}{S}\right)\left(\frac{v}{2} - \left(\frac{u-1}{2}\right)\right) = \left(\frac{v-u+1}{2}\right)\left(1+\left(\frac{2}{S}\right)\right).$$

Otherwise, for v odd and u even we have

$$P_S(u,v) = \frac{v+1}{2} - \left(\frac{u}{2}\right) + \left(\frac{2}{S}\right)\left(\frac{v+1}{2} - \left(\frac{u}{2}\right)\right) = \left(\frac{v-u+1}{2}\right)\left(1+\left(\frac{2}{S}\right)\right),$$

which is given by case (c). Finally, from (b) and (c) we may deduce that

$$P_S(u,n) \geq \left(\frac{2}{S}\right) \geq -1.$$

□

6.2 Number of Solutions: Odd Prime

Let $Q_2 = ax^2 + bxy + cy^2$. With respect to the symmetric integral matrix associated with Q_2, we have $m_1 = 2a$ and $m_2 = 4ac - b^2$. Let $\alpha \in \mathbb{N}_0$ and $A \in \mathbb{Z}$ be such that $2a = p^\alpha A$. Similarly, we let $\delta, \omega \in \mathbb{N}_0$ and $D, K \in \mathbb{Z}$ be such that $(DK, p) = 1$ and

$$m_2 \equiv p^\delta D \pmod{p^{n+\alpha}},$$
$$k \equiv p^\omega K \pmod{p^n}.$$

Further, we may permute a and c as necessary so that without loss of generality we may assume that $p^\alpha \mid c$. In particular, as $(a,b,c) = 1$ if $\alpha \geq 1$ we have $\delta = 0$.

Theorem 6.4. *The numbers of solutions $N_{p^n}(a,b,c;k)$ are given according to the following cases.*

Case 1: *If $\alpha = 0$ and $\delta = n$,*

$$N_{p^n}(a,b,c;k) = \begin{cases} p^{n+\left[\frac{n}{2}\right]} & \text{if } \omega = n \\ p^{n+\frac{\omega}{2}}\left(1 + \left(\frac{2AK}{p}\right)\right) & \text{if } \omega < n,\ \omega \equiv 0 \pmod 2 \\ 0 & \text{if } \omega < n,\ \omega \equiv 1 \pmod 2. \end{cases}$$

Case 2*:If $\alpha = 0$ and $\delta < \omega = n$,*

$$N_{p^n}(a,b,c;k) = \begin{cases} p^{n+\frac{\delta-1}{2}} & \text{if } \delta \equiv 1 \pmod 2 \\ p^{n+\frac{\delta}{2}-1}\left(p + (p-1)H_p(-D;\delta+1,n)\right) & \text{if } \delta \equiv 0 \pmod 2. \end{cases}$$

Case 3*: If $\alpha = 0$ and $\omega < n$,*

$$N_{p^n}(a,b,c;k)$$
$$= p^n \begin{cases} 0 & \text{if } \omega < \delta,\ \omega \equiv 1 \pmod 2 \\ p^{\frac{\omega}{2}}\left(1 + \left(\frac{2AK}{p}\right)\right) & \text{if } \omega < \delta,\ \omega \equiv 0 \pmod 2 \\ p^{\frac{\delta-1}{2}}\left(1 + \left(\frac{2AK}{p}\right)\left(\frac{D}{p}\right)^{\omega}\right) & \text{if } \omega \geq \delta,\ \delta \equiv 1 \pmod 2 \\ p^{\frac{\delta}{2}-1}\left(p - \left(\frac{-D}{p}\right)^{\omega+1} + (p-1)H_p(-D;\delta+1,\omega)\right) & \text{if } \omega \geq \delta,\ \delta \equiv 0 \pmod 2. \end{cases}$$

Case 4*: If $\alpha \neq 0$,*

$$N_{p^n}(a,b,c;k)$$
$$= p^{n-1} \begin{cases} p + (p-1)(\alpha + H_p(-D;1,n-\alpha)) & \text{if } \omega = n, \\ (\omega+1)(p-1) & \text{if } \omega < \alpha \leq n \\ p - \left(\frac{-D}{p}\right)^{\omega+\alpha+1} + (p-1)(\alpha + H_p(-D;1,\omega-\alpha)) & \text{if } \alpha \leq \omega < n. \end{cases}$$

Proof. By Theorem 6.1, we have

$$N_{p^n}(a,b,c;k) = p^n\Big\{1 + \sum_{t=1}^{n} \frac{1}{p^{2t}} \sum_{\substack{S<p^t \\ (S,p)=1}} e\left(\frac{S(-k)}{p^t}\right) G(Q_2;S;p^t)\Big\}. \tag{6.5}$$

We will proceed by evaluating the sum indexed by t in (6.5) for the following three cases:

1. $\alpha = 0$, $\delta = n$,

2. $\alpha = 0$, $\delta < n$,

3. $\alpha \neq 0$.

First, let us assume that $\alpha = 0$. From Theorem 5.1 and Corollary 5.1, for a positive integer t, we have that

$$\begin{aligned} G(Q_2; S; p^t) &= G(2SA; p^t)G(2SADp^\delta; p^t) \\ &= \left(\frac{2SA}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} p^{\frac{t}{2}} G(2SADp^\delta; p^t) \\ &= \begin{cases} p^{\frac{3t}{2}} \left(\frac{2SA}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} & \text{if } \delta \geq t \\ p^{t+\frac{\delta}{2}} \left(\frac{2SA}{p}\right)^\delta \left(\frac{D}{p}\right)^{t+\delta} \left(\frac{-1}{p}\right)^{t(\delta+1)} i^{\left(\frac{p^\delta-1}{2}\right)^2} & \text{if } \delta < t. \end{cases} \end{aligned} \tag{6.6}$$

Thus, we proceed first under the assumption that $\delta = n$. We substitute the appropriate value from (6.6) into the sum indexed by t in (6.5), which yields the expression

$$\begin{aligned} &\sum_{t=1}^{n} \frac{1}{p^{2t}} \sum_{\substack{S<p^t \\ (S,p)=1}} e\left(\frac{-Sk}{p^t}\right) \left(\frac{2SA}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} p^{\frac{3t}{2}} \\ &\quad = \sum_{t=1}^{n} p^{-\frac{t}{2}} \left(\frac{-2A}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} \sum_{\substack{S<p^t \\ (S,p)=1}} e\left(\frac{Sk}{p^t}\right) \left(\frac{S}{p}\right)^t, \end{aligned} \tag{6.7}$$

where by Proposition 2.5 we may map $S \mapsto -S$ without altering the index of summation. We now re-index the inner sum by mapping $S \mapsto u + pv$ where u runs from 1 to $p-1$ and v runs from 0 to $p^{t-1} - 1$. Thus, our expression given in (6.7) becomes

$$\begin{aligned} &= \sum_{t=1}^{n} p^{\frac{-t}{2}} \left(\frac{-2A}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} \sum_{u=1}^{p-1} \sum_{v=0}^{p^{t-1}-1} e\left(\frac{(u+pv)k}{p^t}\right) \left(\frac{u+pv}{p}\right)^t \\ &= \sum_{t=1}^{n} p^{\frac{-t}{2}} \left(\frac{-2A}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} \sum_{u=1}^{p-1} e\left(\frac{p^\omega Ku}{p^t}\right) \left(\frac{u}{p}\right)^t \sum_{v=0}^{p^{t-1}-1} e\left(\frac{p^\omega Kv}{p^{t-1}}\right) \end{aligned} \tag{6.8}$$

We now evaluate this sum based on the size of ω.

Assume first that $\omega = n$. Then with Proposition 2.9 (e), (6.8) will reduce to

$$\sum_{t=1}^{n} p^{\frac{-t}{2}} \left(\frac{-2A}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} \sum_{u=1}^{p-1} \left(\frac{u}{p}\right)^t \sum_{v=0}^{p^{t-1}-1} 1 = (p-1) \sum_{\substack{t=1 \\ t\equiv 0 \pmod 2}}^{n} p^{\frac{t}{2}-1}$$

$$= \frac{(p-1)}{p} \sum_{t=1}^{\left[\frac{n}{2}\right]} p^t = p^{\left[\frac{n}{2}\right]} - 1. \tag{6.9}$$

Suppose now that $\omega < n$. From Corollary 2.2, the sum indexed by v in (6.8) will be non-zero if and only if $\omega \geq t-1$. Hence, with Propositions 2.1, 2.5, 2.9(e), 2.10 and 6.1, and Theorem 3.1, we see that (6.8) can be written as

$$\begin{aligned}
&\sum_{t=1}^{\omega+1} p^{\frac{-t}{2}} \left(\frac{-2A}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} \sum_{u=1}^{p-1} e\left(\frac{p^\omega K u}{p^t}\right) \left(\frac{u}{p}\right)^t p^{t-1} \\
&= \sum_{t=1}^{\omega} p^{\frac{t}{2}-1} \left(\frac{-2A}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2} \sum_{u=1}^{p-1} \left(\frac{u}{p}\right)^t + p^{\frac{\omega-1}{2}} \left(\frac{-2A}{p}\right)^{\omega+1} i^{\left(\frac{p^{\omega+1}-1}{2}\right)^2} \sum_{u=1}^{p-1} e\left(\frac{uK}{p}\right) \left(\frac{u}{p}\right)^{\omega+1} \\
&= \sum_{\substack{t=1 \\ t\equiv 0 \pmod 2}}^{\omega} p^{\frac{t}{2}-1}(p-1) + p^{\frac{\omega-1}{2}} \left(\frac{-2AK}{p}\right)^{\omega+1} i^{\left(\frac{p^{\omega+1}-1}{2}\right)^2} \sum_{u=1}^{p-1} e\left(\frac{uK}{p}\right) \left(\frac{uK}{p}\right)^{\omega+1} \\
&= p^{\left[\frac{\omega}{2}\right]} - 1 + \begin{cases} p^{\frac{\omega-1}{2}} \sum_{u=1}^{p-1} e\left(\frac{uK}{p}\right) & \text{if } \omega \equiv 1 \pmod 2 \\ p^{\frac{\omega-1}{2}} \left(\frac{-2AK}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} G(1;p) & \text{if } \omega \equiv 0 \pmod 2 \end{cases} \\
&= p^{\left[\frac{\omega}{2}\right]} - 1 + \begin{cases} -p^{\frac{\omega-1}{2}} & \text{if } \omega \equiv 1 \pmod 2 \\ p^{\frac{\omega}{2}} \left(\frac{2AK}{p}\right) & \text{if } \omega \equiv 0 \pmod 2. \end{cases} \\
&= \begin{cases} -1 & \text{if } \omega \equiv 1 \pmod 2 \\ p^{\frac{\omega}{2}}(1 + \left(\frac{2AK}{p}\right)) - 1 & \text{if } \omega \equiv 0 \pmod 2. \end{cases}
\end{aligned} \tag{6.10}$$

Hence, (6.5) along with (6.9) and (6.10) will allow us to deduce the statement of the theorem for case 1.

Next, we assume that $\delta < n$. We see that with (6.6), the sum indexed by t in (6.5) becomes

$$\begin{aligned}=&\sum_{t=1}^{\delta}\frac{1}{p^{2t}}\sum_{\substack{S<p^t\\(S,p)=1}}e\left(\frac{-Sk}{p^t}\right)\left(\frac{2SA}{p}\right)^t i^{\left(\frac{p^t-1}{2}\right)^2}p^{\frac{3t}{2}}\\&+\sum_{t=\delta+1}^{n}\frac{1}{p^{2t}}\sum_{\substack{S<p^t\\(S,p)=1}}e\left(\frac{-Sk}{p^t}\right)p^{t+\frac{\delta}{2}}\left(\frac{2SA}{p}\right)^{\delta}\left(\frac{D}{p}\right)^{t+\delta}\left(\frac{-1}{p}\right)^{t(\delta+1)}i^{\left(\frac{p^\delta-1}{2}\right)^2}.\end{aligned}\tag{6.11}$$

From (6.7)-(6.10), we deduce that the first term of (6.11) can be written as

$$\begin{cases}p^{\left[\frac{\delta}{2}\right]}-1 & \text{if } \omega\geq\delta\\ p^{\frac{\omega}{2}}\left(1+\left(\frac{2AK}{p}\right)\right)-1 & \text{if } \omega<\delta,\ \omega \text{ even}\\ -1 & \text{if } \omega<\delta,\ \omega \text{ odd.}\end{cases}\tag{6.12}$$

We now look to examine the second term of (6.11). By Proposition 2.5 we may re-index by $S\mapsto -S$, and subsequently we map $S\mapsto u+pv$ as before so that the second term of (6.11) becomes

$$\begin{aligned}&=\left(\frac{-2AD}{p}\right)^{\delta}i^{\left(\frac{p^\delta-1}{2}\right)^2}\sum_{t=\delta+1}^{n}p^{\frac{\delta}{2}-t}\left(\frac{D}{p}\right)^t\left(\frac{-1}{p}\right)^{t(\delta+1)}\sum_{\substack{S<p^t\\(S,p)=1}}e\left(\frac{Sk}{p^t}\right)\left(\frac{S}{p}\right)^{\delta}\\&=\left(\frac{-2AD}{p}\right)^{\delta}i^{\left(\frac{p^\delta-1}{2}\right)^2}\sum_{t=\delta+1}^{n}p^{\frac{\delta}{2}-t}\left(\frac{D}{p}\right)^t\left(\frac{-1}{p}\right)^{(\delta+1)t}\sum_{u=1}^{p-1}e\left(\frac{p^\omega uK}{p^t}\right)\left(\frac{u}{p}\right)^{\delta}\sum_{v=0}^{p^{t-1}-1}e\left(\frac{p^\omega vK}{p^{t-1}}\right).\end{aligned}\tag{6.13}$$

From here we proceed by making assumptions on the prime divisibility of k.

Suppose $\omega = n$. Then with Proposition 2.9(e), (6.13) becomes

$$=\left(\frac{-2AD}{p}\right)^{\delta}i^{\left(\frac{p^\delta-1}{2}\right)^2}\sum_{t=\delta+1}^{n}p^{\frac{\delta}{2}-t}\left(\frac{D}{p}\right)^t\left(\frac{-1}{p}\right)^{(\delta+1)t}\sum_{u=1}^{p-1}\left(\frac{u}{p}\right)^{\delta}p^{t-1}$$

$$
\begin{aligned}
&= \begin{cases} 0 & \text{if } \delta \equiv 1 \pmod 2 \\ \displaystyle\sum_{t=\delta+1}^{n} p^{\frac{\delta}{2}-1} \left(\frac{-D}{p}\right)^t (p-1) & \text{if } \delta \equiv 0 \pmod 2 \end{cases} \\
&= \begin{cases} 0 & \text{if } \delta \equiv 1 \pmod 2 \\ p^{\frac{\delta}{2}-1}(p-1) \displaystyle\sum_{t=\delta+1}^{n} \left(\frac{-D}{p}\right)^t & \text{if } \delta \equiv 0 \pmod 2 \end{cases} \\
&= \begin{cases} 0 & \text{if } \delta \equiv 1 \pmod 2 \\ p^{\frac{\delta}{2}-1}(p-1) H_p(-D; \delta+1, n) & \text{if } \delta \equiv 0 \pmod 2. \end{cases}
\end{aligned} \tag{6.14}
$$

Suppose now that $\omega < n$. From Corollary 2.2, the sum indexed by v in (6.13) will be non-zero if and only if $\omega \geq t-1$. As $\delta \leq t-1 \leq n-1$, we see that (6.13) will reduce to zero if $\omega < \delta$. Hence, suppose $\delta \leq \omega$ and so by Corollary 2.2, (6.13) will simplify to

$$
\begin{aligned}
&= \left(\frac{-2AD}{p}\right)^{\delta} i^{\left(\frac{p^\delta-1}{2}\right)^2} p^{\frac{\delta}{2}-1} \sum_{t=\delta+1}^{\omega+1} \left(\frac{D}{p}\right)^t \left(\frac{-1}{p}\right)^{(\delta+1)t} \sum_{u=1}^{p-1} e\left(\frac{uK}{p^{t-\omega}}\right) \left(\frac{u}{p}\right)^{\delta} \\
&= \left(\frac{-2ADK}{p}\right)^{\delta} i^{\left(\frac{p^\delta-1}{2}\right)^2} p^{\frac{\delta}{2}-1} \left(\sum_{t=\delta+1}^{\omega} \left(\frac{D}{p}\right)^t \left(\frac{-1}{p}\right)^{(\delta+1)t} \sum_{u=1}^{p-1} \left(\frac{uK}{p}\right)^{\delta} \right. \\
&\quad \left. + \left(\frac{D}{p}\right)^{\omega+1} \left(\frac{-1}{p}\right)^{(\delta+1)(\omega+1)} \sum_{u=1}^{p-1} e\left(\frac{uK}{p}\right) \left(\frac{uK}{p}\right)^{\delta} \right)
\end{aligned} \tag{6.15}
$$

If δ is odd, then with Propositions 2.5, 2.9(e), 2.10 and 6.1, and Theorem 3.1, (6.15) resolves to

$$
\left(\frac{-2ADK}{p}\right) i^{\left(\frac{p-1}{2}\right)^2} p^{\frac{\delta}{2}-1} \left(\frac{D}{p}\right)^{\omega+1} G(1;p) = p^{\frac{\delta-1}{2}} \left(\frac{2AK}{p}\right) \left(\frac{D}{p}\right)^{\omega}. \tag{6.16}
$$

Otherwise, for even δ, with Proposition 2.1, (6.15) is given by

$$
p^{\frac{\delta}{2}-1} \left((p-1) \sum_{t=\delta+1}^{\omega} \left(\frac{-D}{p}\right)^t - \left(\frac{-D}{p}\right)^{\omega+1} \right)
$$

$$= p^{\frac{\delta}{2}-1}\left((p-1)H_p(-D;\delta+1,\omega) - \left(\frac{-D}{p}\right)^{\omega+1}\right). \tag{6.17}$$

Hence, with (6.5) and (6.11)-(6.14), if $\delta < \omega = n$, then $N_{p^n}(a,b,c;k)$ is given by

$$\begin{aligned} & p^n\left(p^{\left[\frac{\delta}{2}\right]} + \begin{cases} 0 & \text{if } \delta \equiv 1 \pmod 2 \\ p^{\frac{\delta}{2}-1}(p-1)H_p(-D;\delta+1,n) & \text{if } \delta \equiv 0 \pmod 2 \end{cases}\right) \\ & = p^n \begin{cases} p^{\frac{\delta-1}{2}} & \text{if } \delta \equiv 1 \pmod 2 \\ p^{\frac{\delta}{2}-1}\left(p + (p-1)H_p(-D;\delta+1,n)\right) & \text{if } \delta \equiv 0 \pmod 2. \end{cases} \end{aligned} \tag{6.18}$$

It's clear that (6.18) corresponds to the statement of case 2.

Next, if $\omega < n$, then with (6.5), (6.12), (6.13) and (6.15)-(6.17), $N_{p^n}(a,b,c;k)$ is given by

$$\begin{aligned} & p^n\left(\begin{cases} p^{\left[\frac{\delta}{2}\right]} & \text{if } \omega \geq \delta \\ p^{\frac{\omega}{2}}\left(1+\left(\frac{2AK}{p}\right)\right) & \text{if } \omega < \delta, \omega \equiv 0 \pmod 2 \\ 0 & \text{if } \omega < \delta, \omega \equiv 1 \pmod 2 \end{cases}\right. \\ & \left. + \begin{cases} 0 & \text{if } \omega < \delta \\ p^{\frac{\delta-1}{2}}\left(\frac{2AK}{p}\right)\left(\frac{D}{p}\right)^{\omega} & \text{if } \omega \geq \delta, \delta \equiv 1 \pmod 2 \\ p^{\frac{\delta}{2}-1}((p-1)H_p(-D;\delta+1,\omega) - \left(\frac{-D}{p}\right)^{\omega+1}) & \text{if } \omega \geq \delta, \delta \equiv 0 \pmod 2 \end{cases}\right) \\ & = p^n \begin{cases} 0 & \text{if } \omega < \delta, \omega \equiv 1 \pmod 2 \\ p^{\frac{\omega}{2}}\left(1+\left(\frac{2AK}{p}\right)\right) & \text{if } \omega < \delta, \omega \equiv 0 \pmod 2 \\ p^{\frac{\delta-1}{2}}\left(1+\left(\frac{2AK}{p}\right)\left(\frac{D}{p}\right)^{\omega}\right) & \text{if } \omega \geq \delta, \delta \equiv 1 \pmod 2 \\ p^{\frac{\delta}{2}-1}\left(p - \left(\frac{-D}{p}\right)^{\omega+1} + (p-1)H_p(-D;\delta+1,\omega)\right) & \text{if } \omega \geq \delta, \delta \equiv 0 \pmod 2. \end{cases} \end{aligned}$$

It's clear these values correspond to case 3 of the theorem.

Finally, we deal with the case where $\alpha \neq 0$. Observe that as $(a,b,c) = 1$ we must have

$\delta = 0$. Hence, from Theorem 5.1 and Corollary 5.1, for $t \in \mathbb{N}$ we have that

$$G(Q_2; S; p^t) = \begin{cases} p^t & \text{if } \alpha \geq t \\ G(2SA; p^{t-\alpha})G(2SAD; p^{t+\alpha}) & \text{if } \alpha < t \end{cases}$$
$$= \begin{cases} p^t & \text{if } \alpha \geq t \\ p^t \left(\frac{-D}{p}\right)^{t+\alpha} & \text{if } \alpha < t. \end{cases} . \tag{6.19}$$

Thus, with (6.19), and following the mappings $-S \mapsto S \mapsto u + pv$ as before, we see that the sum indexed by t in (6.5) becomes

$$\sum_{t=1}^{\alpha} \frac{1}{p^{2t}} \sum_{\substack{S<p^t \\ (S,p)=1}} e\left(\frac{-Sk}{p^t}\right) p^t + \sum_{t=\alpha+1}^{n} \frac{1}{p^{2t}} \sum_{\substack{S<p^t \\ (S,p)=1}} e\left(\frac{-Sk}{p^t}\right) \left(\frac{-D}{p}\right)^{t+\alpha} p^t$$
$$= \sum_{t=1}^{\alpha} p^{-t} \sum_{u=1}^{p-1} e\left(\frac{up^\omega K}{p^t}\right) \sum_{v=0}^{p^{t-1}-1} e\left(\frac{vp^\omega K}{p^{t-1}}\right)$$
$$+ \sum_{t=\alpha+1}^{n} p^{-t} \left(\frac{-D}{p}\right)^{t+\alpha} \sum_{u=0}^{p-1} e\left(\frac{up^\omega K}{p^t}\right) \sum_{v=0}^{p^{t-1}-1} e\left(\frac{vp^\omega K}{p^{t-1}}\right). \tag{6.20}$$

As before, we now specify the prime divisibility of k. If $\omega = n$, then with Proposition 6.3 (a) and by mapping $t \mapsto t + \alpha$ in the second term, (6.20) will simplify to

$$= \sum_{t=1}^{\alpha} p^{-t} \sum_{u=1}^{p-1} \sum_{v=0}^{p^{t-1}-1} 1 + \sum_{t=\alpha+1}^{n} p^{-t} \left(\frac{-D}{p}\right)^{t+\alpha} \sum_{u=1}^{p-1} \sum_{v=0}^{p^{t-1}-1} 1$$
$$= \frac{(p-1)}{p} \sum_{t=1}^{\alpha} 1 + \frac{(p-1)}{p} \sum_{t=1}^{n-\alpha} \left(\frac{-D}{p}\right)^t$$
$$= \frac{(p-1)}{p} \begin{cases} \alpha & \text{if } \alpha = n \\ \alpha + H_p(-D; 1, n-\alpha) & \text{if } \alpha < n. \end{cases}$$
$$= \frac{(p-1)}{p} \left(\alpha + H_p(-D; 1, n-\alpha)\right). \tag{6.21}$$

Suppose now that $\omega < n$. Observe that by Corollary 2.2, the sum indexed by v in each

term of (6.20) will be non-zero if $\omega \geq t-1$. In other words, the index t will reach a maximum value of $\omega+1$ and the rest of this expression will vanish.

Suppose first that $\alpha = n$. Then with Proposition 2.1, (6.20) will be given by

$$\begin{aligned}\sum_{t=1}^{n} p^{-t} \sum_{u=1}^{p-1} e\left(\frac{up^{\omega}K}{p^t}\right) \sum_{v=0}^{p^{t-1}-1} e\left(\frac{vp^{\omega}K}{p^{t-1}}\right) &= \frac{1}{p} \sum_{t=1}^{\omega+1} \sum_{u=1}^{p-1} e\left(\frac{up^{\omega}K}{p^t}\right) \\ &= \frac{1}{p} \sum_{t=1}^{\omega} (p-1) + \frac{1}{p} \sum_{u=1}^{p-1} e\left(\frac{uK}{p}\right) \\ &= \frac{\omega(p-1)}{p} - \frac{1}{p} = \frac{\omega(p-1)-1}{p}. \end{aligned} \tag{6.22}$$

Hence, suppose now that $\alpha < n$. We proceed to evaluate (6.20) based on the relation of ω to α. If we first assume that $\omega < \alpha$, then with Corollary 2.2, (6.20) becomes

$$\begin{aligned}\sum_{t=1}^{\omega+1} p^{-t} \sum_{u=1}^{p-1} e\left(\frac{up^{\omega}K}{p^t}\right) p^{t-1} &= \frac{1}{p} \sum_{t=1}^{\omega} \sum_{u=1}^{p-1} 1 + \frac{1}{p} \sum_{u=1}^{p-1} e\left(\frac{uK}{p}\right) \\ &= \frac{1}{p} \left(\omega(p-1)-1\right) \\ &= \frac{\omega(p-1)-1}{p}. \end{aligned} \tag{6.23}$$

Next, if $\omega = \alpha$, then with Proposition 2.1 and Corollary 2.2, (6.20) becomes

$$\begin{aligned}&= \sum_{t=1}^{\omega} p^{-t} \sum_{u=1}^{p-1} e\left(\frac{up^{\omega}K}{p^t}\right) p^{t-1} + p^{-(\omega+1)} \left(\frac{-D}{p}\right) \sum_{u=1}^{p-1} e\left(\frac{uK}{p}\right) p^{\omega} \\ &= \frac{1}{p} \sum_{t=1}^{\alpha} (p-1) - \frac{1}{p} \left(\frac{-D}{p}\right) = \frac{1}{p} \left(\alpha(p-1) - \left(\frac{-D}{p}\right)\right). \end{aligned} \tag{6.24}$$

Finally, if $\omega > \alpha$ then with Proposition 2.1 and Corollary 2.2, we find that (6.20) simplifies to

$$= \sum_{t=1}^{\alpha} p^{-t} \sum_{u=1}^{p-1} e\left(\frac{up^{\omega}K}{p^t}\right) p^{t-1} + \sum_{t=\alpha+1}^{\omega+1} p^{-t} \left(\frac{-D}{p}\right)^{t+\alpha} \sum_{u=1}^{p-1} e\left(\frac{up^{\omega}K}{p^t}\right) p^{t-1}$$

$$
\begin{aligned}
=&\frac{(p-1)\alpha}{p}+\frac{(p-1)}{p}\sum_{t=\alpha+1}^{\omega}\left(\frac{-D}{p}\right)^{t+\alpha}-\frac{1}{p}\left(\frac{-D}{p}\right)^{\omega+1+\alpha}\\
=&\frac{(p-1)}{p}\left(\alpha+\sum_{t=1}^{\omega-\alpha}\left(\frac{-D}{p}\right)^{t}\right)-\frac{1}{p}\left(\frac{-D}{p}\right)^{\omega+\alpha+1}\\
=&\frac{(p-1)}{p}\left(\alpha+H_p(-D;1,\omega-\alpha)\right)-\frac{1}{p}\left(\frac{-D}{p}\right)^{\omega+1+\alpha}. \qquad (6.25)
\end{aligned}
$$

Hence, with (6.5), (6.20) and (6.21), if $\omega = n$ then $N_{p^n}(a,b,c;k)$ is given by

$$
p^{n-1}\left(p+(p-1)(\alpha+H_p(-D;1,n-\alpha))\right). \qquad (6.26)
$$

As $\alpha \geq 1$ from Proposition 6.3(d), we see $N_{p^n}(a,b,c;k) \geq 0$ for $\omega = n$.

Otherwise, if $\omega < n$, from (6.5), (6.20) and (6.22)-(6.25), and with Proposition 6.3(a), $N_{p^n}(a,b,c;k)$ is given by

$$
\begin{aligned}
p^{n-1}&\begin{cases}
p+\omega(p-1)-1 & \text{if } \omega<\alpha\\
p+\alpha(p-1)-\left(\frac{-D}{p}\right) & \text{if } \omega=\alpha\\
p+(p-1)(\alpha+H_p(-D;1,\omega-\alpha))-\left(\frac{-D}{p}\right)^{\omega+1+\alpha} & \text{if } \omega>\alpha
\end{cases}\\
&=p^{n-1}\begin{cases}
(\omega+1)(p-1) & \text{if } \omega<\alpha\\
p+(p-1)(\alpha+H_p(-D;1,\omega-\alpha))-\left(\frac{-D}{p}\right)^{\omega+1+\alpha} & \text{if } \omega\geq\alpha.
\end{cases}
\end{aligned} \qquad (6.27)
$$

Hence, we see that (6.26) and (6.27) will yield case 4 of the theorem.

□

6.3 Preliminary Results: Powers of 2

We now proceed in a similar manner to determine the number of solutions for a power of 2. By Theorem 6.1, the number of solutions to the congruence

$$ax^2 + bxy + cy^2 \equiv k \pmod{2^n}$$

is given by

$$N_{2^n} = 2^n \left(1 + \sum_{t=1}^{n} \frac{1}{2^{2t}} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-kS}{2^t}\right) G(Q_2; S; 2^t) \right). \tag{6.28}$$

By Theorem 5.2, for any $t \in \mathbb{N}$, we have

$$G(Q_2; S; 2^t) = \begin{cases} 2^n & \text{if } \alpha \geq t > 1 \\ 2(-1)^c \mathbb{O}(m_2 + 1) & \text{if } \alpha = t = 1 \\ \dfrac{1}{4} G(SA; 2^{t+1-\alpha}) G(SAm_2; 2^{t+1+\alpha}) & \text{if } \alpha < t. \end{cases} \tag{6.29}$$

This means the sum in (6.28) will depend on two cases of α. Either we have $\alpha = 1$ or $\alpha > 1$. Regardless, for the remainder of this chapter, we let $\delta, \omega \in \mathbb{N}_0$ and $D, K \in \mathbb{Z}$ be such that $(DK, 2) = 1$ and

$$2^\delta D \equiv m_2 \pmod{2^{n+\alpha+1}},$$
$$2^\omega K \equiv k \pmod{2^n}.$$

By Theorem 3.1 and Proposition 2.3 we have

$$G(SAD2^{\delta};2^{t+1+\alpha}) = \begin{cases} 2^{t+1+\alpha} & \text{if } \delta \geq t+1+\alpha \\ 0 & \text{if } \delta = t+\alpha \\ 2^{\delta}G(SAD;2^{t+1+\alpha-\delta}) & \text{if } \delta \leq t+\alpha-1 \end{cases} \tag{6.30}$$

Suppose for the moment that $\alpha = 1$. With (6.29) and (6.30), the bracketed expression in (6.28) is given by

$$\begin{aligned} &1 + \frac{1}{2^2} e\left(\frac{-k}{2}\right) G(Q_2;1;2) + \sum_{t=2}^{\delta-2} \frac{1}{2^t} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-kS}{2^t}\right) G(SA;2^t) \\ &+ \sum_{t=\max(2,\delta)}^{n} \frac{2^{\delta}}{2^{2t+2}} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-kS}{2^t}\right) G(SA;2^t)G(SAD;2^{t+2-\delta}). \end{aligned} \tag{6.31}$$

Otherwise, if $\alpha > 1$ we have $\delta = 0$. In this case, the bracketed expression in (6.28) is given by

$$\begin{aligned} &1 + \sum_{t=1}^{\alpha} \frac{1}{2^t} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-kS}{2^t}\right) \\ &+ \sum_{t=\alpha+1}^{n} \frac{1}{2^{2t+2}} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-kS}{2^t}\right) G(SA;2^{t+1-\alpha})G(SAD;2^{t+1+\alpha}). \end{aligned} \tag{6.32}$$

This necessitates the following definitions.

Definition 6.5. Let A, D and K be arbitrary odd integers and let α, ω and $\delta \in \mathbb{N}_0$. Then for $t \in \mathbb{N}$, $t \geq 2$ we define

$$E(A, 2^{\omega}K; t) = \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^{\omega}KS}{2^t}\right) G(SA;2^t).$$

Further, if $\alpha < t$ and $\delta \leq t$, we define

$$F(2^\alpha A, 2^\delta D, 2^\omega K; t) = \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right) G(SA; 2^{t+1-\alpha}) G(SAD; 2^{t+1+\alpha-\delta}).$$

When the contexts of our variables are clear, we may simplify our notation by writing $E(A, 2^\omega K; t) = E(t)$ and $F(2^\alpha A, 2^\delta D, 2^\omega K; t) = F(t)$. Thus, with Definition 6.5 and (6.31), if $\alpha = 1$, $N_{2^n}(a, b, c; k)$ is given by

$$2^n \left\{ 1 + \frac{1}{2^2} e\left(\frac{k}{2}\right) G(Q_2; 1; 2) + \sum_{t=2}^{\delta-2} \frac{1}{2^t} E(t) + \sum_{t=\max(2,\delta)}^{n} \frac{2^\delta}{2^{2t+2}} F(t) \right\}, \tag{6.33}$$

and for $\alpha > 1$, with (6.32), $N_{2^n}(a, b, c; k)$ is given by

$$2^n \left\{ 1 + \sum_{t=1}^{\alpha} \frac{1}{2^t} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-kS}{2^t}\right) + \sum_{t=\alpha+1}^{n} \frac{1}{2^{2t+2}} F(t) \right\}. \tag{6.34}$$

We now look to evaluate these sums.

Proposition 6.6. *If $\alpha = 1$, we have that*

$$\frac{1}{4} e\left(\frac{k}{2}\right) G(Q_2; 1; 2) = \begin{cases} 0 & \text{if } \delta \geq 1 \\ \dfrac{(-1)^{c+2^\omega}}{2} & \text{if } \delta = 0. \end{cases}$$

Proof. From Theorem 5.2, when $\alpha = 1$, we have $G(Q_2; 1; 2) = 2(-1)^c \mathbb{O}(2^\delta D + 1)$. In particular, this is non-zero if and only if $\delta = 0$. Thus, if $\delta = 0$, we multiply $G(Q_2; 1; 2)$ by $\dfrac{(-1)^{2^\omega K}}{4}$ to yield the statement of the proposition. □

Proposition 6.7. *We have*

$$E(2) = \begin{cases} 2^2(-1)^{\frac{A-K}{2}} & \text{if } \omega = 0 \\ -2^2 & \text{if } \omega = 1 \\ 2^2 & \text{if } \omega \geq 2. \end{cases}$$

Proof. By Definition 6.5 and Theorem 3.1, we have

$$\begin{aligned} E(A, 2^\omega K; 2) &= 2 \sum_{\substack{S<4 \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{4}\right)\left(\frac{2}{SA}\right)^2 (1+i^{SA}) \\ &= 2 \sum_{\substack{S<4 \\ S\equiv 1 \pmod 2}} e\left(\frac{2^\omega KS}{4}\right)(1-i^{SA}) \\ &= 2\left(e\left(\frac{2^\omega K}{4}\right)(1-i^A) + e\left(\frac{3\cdot 2^\omega K}{4}\right)(1+i^A)\right) \\ &= 2i^{2^\omega K}\left(1-i^A+(-1)^{2^\omega}(1+i^A)\right) \\ &= 2i^{2^\omega K}\begin{cases} -2i^A & \text{if } \omega = 0 \\ 2 & \text{if } \omega \geq 1 \end{cases} = \begin{cases} -2^2(-1)^{\frac{A+K}{2}} & \text{if } \omega = 0 \\ -2^2 & \text{if } \omega = 1 \\ 2^2 & \text{if } \omega \geq 2. \end{cases} \end{aligned}$$

We see that the $\omega = 0$ case will simplify to the statement of the proposition. □

Proposition 6.8. *Suppose $t \geq 3$. Then*

$$E(t) = \begin{cases} 0 & \text{if } \omega + 3 < t \\ 2^{\frac{3\omega}{2}+4}\left(\frac{2}{AK}\right)\mathbb{O}(\omega)\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega + 3 = t \\ 2^{\frac{3\omega}{2}+2}\mathbb{O}(\omega)(-1)^{\frac{A-K}{2}} & \text{if } \omega + 2 = t \\ -2^{\frac{3\omega+1}{2}}\mathbb{O}(\omega+1) & \text{if } \omega + 1 = t \\ 2^{\frac{3t}{2}-1}\mathbb{O}(t) & \text{if } \omega \geq t. \end{cases}$$

Proof. By Theorem 3.1, we have

$$\begin{aligned} E(t) &= \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right)\left(\frac{2}{SA}\right)^t (1+i^{SA})2^{\frac{t}{2}} \\ &= 2^{\frac{t}{2}}\left(\frac{2}{A}\right)^t \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{2^\omega KS}{2^t}\right)\left(\frac{2}{S}\right)^t (1-i^{SA}). \end{aligned} \tag{6.35}$$

As $t \geq 3$, we may break up the sum in (6.35) according to its residues modulo 8. This yields

$$\begin{aligned} 2^{\frac{t}{2}}\left(\frac{2}{A}\right)^t \Bigg\{ &\sum_{\substack{S<2^t \\ S\equiv 1 \pmod 8}} e\left(\frac{2^\omega SK}{2^t}\right)(1-i^A) + (-1)^t \sum_{\substack{S<2^t \\ S\equiv 3 \pmod 8}} e\left(\frac{2^\omega SK}{2^t}\right)(1+i^A) \\ &+(-1)^t \sum_{\substack{S<2^t \\ S\equiv 5 \pmod 8}} e\left(\frac{2^\omega SK}{2^t}\right)(1-i^A) + \sum_{\substack{S<2^t \\ S\equiv 7 \pmod 8}} e\left(\frac{2^\omega SK}{2^t}\right)(1+i^A) \Bigg\} \end{aligned} \tag{6.36}$$

Each of these sums in (6.36) can be re-indexed by $S \mapsto 8u+\zeta$, where $u = 0, \ldots, 2^{t-3}-1$ and ζ is the corresponding odd residue modulo 8. Hence, (6.36) becomes

$$\begin{aligned} &2^{\frac{t}{2}}\left(\frac{2}{A}\right)^t \sum_{u=0}^{2^{t-3}-1} e\left(\frac{2^\omega Ku}{2^{t-3}}\right)\left\{ e\left(\frac{2^\omega K}{2^t}\right)(1-i^A) + (-1)^t e\left(\frac{2^\omega 3K}{2^t}\right)(1+i^A) \right. \\ &\qquad \left. +(-1)^t e\left(\frac{2^\omega 5K}{2^t}\right)(1-i^A) + e\left(\frac{2^\omega 7K}{2^t}\right)(1+i^A)\right\} \\ &= 2^{\frac{t}{2}}\left(\frac{2}{A}\right)^t \sum_{u=0}^{2^{t-3}-1} e\left(\frac{2^\omega Ku}{2^{t-3}}\right)\left\{ (1-i^A) e\left(\frac{2^\omega K}{2^t}\right)\left(1+(-1)^t e\left(\frac{2^\omega K}{2^{t-2}}\right)\right)\right. \\ &\qquad \left. +(1+i^A) e\left(\frac{2^\omega 3K}{2^t}\right)\left(e\left(\frac{2^\omega K}{2^{t-2}}\right)+(-1)^t\right)\right\} \\ &= 2^{\frac{t}{2}}\left(\frac{2}{A}\right)^t \sum_{u=0}^{2^{t-3}-1} e\left(\frac{2^\omega Ku}{2^{t-3}}\right) e\left(\frac{2^\omega K}{2^t}\right)\left(1+(-1)^t e\left(\frac{2^\omega K}{2^{t-2}}\right)\right) \\ &\qquad \times \left(1-i^A+(-1)^t e\left(\frac{2^\omega K}{2^{t-1}}\right)(1+i^A)\right). \end{aligned} \tag{6.37}$$

We now simplify based on ω. By Proposition 2.1, whenever $\omega < t-3$, the sum indexed by

u in (6.37) will vanish. Hence, suppose now $\omega = t-3$. Substituting this into (6.37) yields

$$\begin{aligned}
&2^{\frac{\omega+3}{2}}\left(\frac{2}{A}\right)^{\omega+1}2^{\omega}e\left(\frac{K}{8}\right)\left(1+(-1)^{\omega+1}e\left(\frac{K}{2}\right)\right)\left(1-i^{A}+(-1)^{\omega+1}e\left(\frac{K}{4}\right)(1+i^{A})\right)\\
&\quad=2^{\frac{3\omega+3}{2}}\left(\frac{2}{A}\right)^{\omega+1}i^{\frac{K}{2}}\left(1+(-1)^{\omega}\right)\left(1-i^{A}-i^{K}-i^{A+K}\right)\\
&\quad=2^{\frac{3\omega+5}{2}}\left(\frac{2}{A}\right)\mathbb{O}(\omega)\left(2^{\frac{-1}{2}}\left(\frac{2}{K}\right)(1+i^{K})\right)\left(2\mathbb{O}(\frac{A-K}{2})(1-i^{K})\right)\\
&\quad=2^{\frac{3\omega}{2}+4}\left(\frac{2}{AK}\right)\mathbb{O}(\omega)\mathbb{O}(\frac{A-K}{2}),
\end{aligned}$$

where we have used Propositions 2.18 and 2.21 in this evaluation.

Suppose now that $\omega = t-2$. We substitute this into (6.37) which gives the expression

$$\begin{aligned}
&2^{\frac{\omega+2}{2}}\left(\frac{2}{A}\right)^{\omega}2^{\omega-1}e\left(\frac{K}{4}\right)(1+(-1)^{\omega})\left(1-i^{A}+(-1)^{\omega}e\left(\frac{K}{2}\right)(1+i^{A})\right)\\
&\quad=2^{\frac{3\omega}{2}+1}\mathbb{O}(\omega)i^{K}(1-i^{A}-(1+i^{A}))\\
&\quad=-2^{\frac{3\omega}{2}+2}\mathbb{O}(\omega)(-1)^{\frac{A+K}{2}}=2^{\frac{3\omega}{2}+2}\mathbb{O}(\omega)(-1)^{\frac{A-K}{2}}.
\end{aligned}$$

Next, if $\omega = t-1$, substituting this into (6.37) yields

$$\begin{aligned}
&2^{\frac{\omega+1}{2}}\left(\frac{2}{A}\right)^{\omega+1}2^{\omega-2}e\left(\frac{K}{2}\right)\left(1+(-1)^{\omega+1}\right)\left(1-i^{A}+(-1)^{\omega+1}(1+i^{A})\right)\\
&\quad=2^{\frac{3\omega-3}{2}}(-1)^{K}\cdot 2\mathbb{O}(\omega+1)\cdot 2\\
&\quad=-2^{\frac{3\omega+1}{2}}\mathbb{O}(\omega+1).
\end{aligned}$$

Finally, for $\omega \geq t$, the expression in (6.37) becomes

$$2^{\frac{t}{2}}\left(\frac{2}{A}\right)^{t}2^{t-3}(1+(-1)^{t})(1-i^{A}+1+i^{A})=2^{\frac{3t}{2}-1}\mathbb{O}(t).$$

□

Proposition 6.9. *For $\alpha = 1$ and $\delta \leq 2$, we have*

$$F(2) = F(2A, 2^\delta D, 2^\omega K; 2) = \begin{cases} 2^{5-\frac{\delta}{2}}(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 0 \\ -2^{5-\frac{\delta}{2}}\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega = 1 \\ 2^{5-\frac{\delta}{2}}\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega \geq 2. \end{cases}$$

Proof. By Definition 6.5, Theorem 3.1 and Proposition 2.19,

$$\begin{aligned} &F(2A, 2^\delta D, 2^\omega K; 2) \\ &= \sum_{\substack{S<4 \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{4}\right) G(SA; 2^2) G(SAD; 2^{4-\delta}) \\ &= \sum_{\substack{S<4 \\ S\equiv 1 \pmod 2}} \left(\frac{2^\omega KS}{4}\right) \cdot \left(\frac{2}{SA}\right)^2 (1 - i^{SA}) 2 \cdot \left(\frac{2}{SAD}\right)^{4-\delta} (1 - i^{SAD}) 2^{\frac{4-\delta}{2}} \\ &= 2^{3-\frac{\delta}{2}} \left(\frac{2}{AD}\right)^\delta \left(i^{2^\omega K} \prod_{j=1,D} (1 - i^{Aj}) + (-1)^\delta i^{2^\omega 3K} \prod_{j=1,D} (1 + i^{Aj}) \right) \\ &= 2^{4-\frac{\delta}{2}} \left(\frac{2}{AD}\right)^\delta i^{A\left(\frac{D+1}{2}\right)^2} i^{2^\omega K} \left((-1)^{\frac{D+1}{2}} + (-1)^{2^\omega + \delta} \right). \end{aligned} \tag{6.38}$$

As $\delta \leq 2$, we must have that δ is even. Hence, (6.38) simplifies to

$$2^{4-\frac{\delta}{2}} i^{A\left(\frac{D+1}{2}\right)^2} i^{2^\omega K} (-1)^{\frac{D+1}{2}} \left(1 + (-1)^{2^\omega + \frac{D+1}{2}}\right). \tag{6.39}$$

When $\omega = 0$, (6.39) becomes

$$\begin{aligned} &2^{4-\frac{\delta}{2}} i^{A\left(\frac{D+1}{2}\right)^2} i^K (-1)^{\frac{D+1}{2}} (1 + (-1)^{\frac{D-1}{2}}) \\ &\quad = 2^{5-\frac{\delta}{2}} \mathbb{O}(\frac{D-1}{2})(-1) i^{A+K} = 2^{5-\frac{\delta}{2}} (-1)^{\frac{A-K}{2}} \mathbb{O}(\frac{D-1}{2}). \end{aligned}$$

When $\omega = 1$, (6.39) simplifies to

$$2^{4-\frac{\delta}{2}} i^{A\left(\frac{D+1}{2}\right)^2} (-1)^K (-1)^{\frac{D+1}{2}} (1 + (-1)^{\frac{D+1}{2}}) = -2^{5-\frac{\delta}{2}} \mathbb{O}(\frac{D+1}{2}).$$

Finally, for $\omega \geq 2$, (6.39) becomes

$$2^{4-\frac{\delta}{2}} i^{A\left(\frac{D+1}{2}\right)^2} (-1)^{\frac{D+1}{2}} (1 + (-1)^{\frac{D+1}{2}}) = 2^{5-\frac{\delta}{2}} \mathbb{O}(\frac{D+1}{2}).$$

□

Proposition 6.10. *Suppose $t \geq 3$. Then for $\alpha < t$ and $\delta \leq t$, we have*

$$F(t) = \begin{cases} 0 & \text{if } \omega + 3 < t \\ 2^{2(\omega+3)+\frac{1-\delta}{2}} \mathbb{O}(\delta+1) \left(\frac{2}{ADK}\right) \left(\frac{2}{D}\right)^{\omega+\alpha} (-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \omega + 3 = t \\ 2^{2\omega+5-\frac{\delta}{2}} \mathbb{O}(\delta) \mathbb{O}(\frac{D-1}{2}) \left(\frac{2}{D}\right)^{\omega+\alpha+1} (-1)^{\frac{A-K}{2}} & \text{if } \omega + 2 = t \\ -2^{2\omega+3-\frac{\delta}{2}} \mathbb{O}(\delta) \mathbb{O}(\frac{D+1}{2}) \left(\frac{2}{D}\right)^{\omega+\alpha} & \text{if } \omega + 1 = t \\ 2^{2t+1-\frac{\delta}{2}} \mathbb{O}(\delta) \mathbb{O}(\frac{D+1}{2}) \left(\frac{2}{D}\right)^{t+1+\alpha} & \text{if } \omega \geq t. \end{cases}$$

Proof. From Definition 6.5 and Theorem 3.1,

$$\begin{aligned} &F(2^\alpha A; 2^\delta D; 2^\omega K; t) \\ &= \sum_{\substack{S < 2^t \\ S \equiv 1 \pmod 2}} e\left(\frac{2^\omega KS}{2^t}\right) \left(\frac{2}{SA}\right)^{t+1+\alpha} (1 - i^{SA}) 2^{\frac{t+1-\alpha}{2}} \left(\frac{2}{SAD}\right)^{t+1+\alpha+\delta} (1 - i^{SAD}) 2^{\frac{t+1+\alpha-\delta}{2}} \\ &= 2^{t+1-\frac{\delta}{2}} \left(\frac{2}{AD}\right)^\delta \left(\frac{2}{D}\right)^{t+1+\alpha} \sum_{\substack{S < 2^t \\ S \equiv 1 \pmod 2}} e\left(\frac{2^\omega KS}{2^t}\right) \left(\frac{2}{S}\right)^\delta \prod_{j=1,D} (1 - i^{SAj}). \end{aligned} \tag{6.40}$$

Similar to the proof of Proposition 6.8, we re-index this sum according to its residue modulo 8 and map $S \mapsto 8u + \zeta$ for $u = 0, \ldots, 2^{t-3} - 1$ and ζ the corresponding odd residue. Hence,

we write (6.40) as

$$2^{t+1-\frac{\delta}{2}}\left(\frac{2}{AD}\right)^{\delta}\left(\frac{2}{D}\right)^{t+1+\alpha}\sum_{u=0}^{2^{t-3}-1}e\left(\frac{2^{\omega}Ku}{2^{t-3}}\right)$$
$$\times\left\{e\left(\frac{2^{\omega}K}{2^{t}}\right)\prod_{j=1,D}(1-i^{Aj})+(-1)^{\delta}e\left(\frac{2^{\omega}3K}{2^{t}}\right)\prod_{j=1,D}(1+i^{Aj})\right.$$
$$\left.+(-1)^{\delta}e\left(\frac{2^{\omega}5K}{2^{t}}\right)\prod_{j=1,D}(1-i^{Aj})+e\left(\frac{2^{\omega}7K}{2^{t}}\right)\prod_{j=1,D}(1+i^{Aj})\right\}. \tag{6.41}$$

We look to simplify the bracketed expression in (6.41). By Proposition 2.19, this expression becomes

$$\begin{aligned}
&e\left(\frac{2^{\omega}K}{2^{t}}\right)\prod_{j=1,D}(1-i^{Aj})\left(1+(-1)^{\delta}e\left(\frac{2^{\omega}K}{2^{t-2}}\right)\right)\\
&+e\left(\frac{2^{\omega}3K}{2^{t}}\right)\prod_{j=1,D}(1+i^{A}j)\left(e\left(\frac{2^{\omega}K}{2^{t-2}}\right)+(-1)^{\delta}\right)\\
&=e\left(\frac{2^{\omega}K}{2^{t}}\right)\left(1+(-1)^{\delta}e\left(\frac{2^{\omega}K}{2^{t-2}}\right)\right)\left(\prod_{j=1,D}(1-i^{Aj})+(-1)^{\delta}e\left(\frac{2^{\omega}K}{2^{t-1}}\right)\prod_{j=1,D}(1+i^{Aj})\right)\\
&=e\left(\frac{2^{\omega}K}{2^{t}}\right)\left(1+(-1)^{\delta}e\left(\frac{2^{\omega}K}{2^{t-2}}\right)\right)\cdot 2i^{A\left(\frac{D+1}{2}\right)^{2}}(-1)^{\frac{D+1}{2}}\left(1+(-1)^{\delta+\frac{D+1}{2}}e\left(\frac{2^{\omega}K}{2^{t-1}}\right)\right)
\end{aligned} \tag{6.42}$$

Combining (6.41) and (6.42) means that $F(t)$ can be written as

$$2^{t+2-\frac{\delta}{2}}\left(\frac{2}{AD}\right)^{\delta}\left(\frac{2}{D}\right)^{t+1+\alpha}\sum_{u=0}^{2^{t-3}-1}e\left(\frac{2^{\omega}Ku}{2^{t-3}}\right)$$
$$\times e\left(\frac{2^{\omega}K}{2^{t}}\right)\left(1+(-1)^{\delta}e\left(\frac{2^{\omega}K}{2^{t-2}}\right)\right)i^{A\left(\frac{D+1}{2}\right)^{2}}(-1)^{\frac{D+1}{2}}\left(1+(-1)^{\delta+\frac{D+1}{2}}e\left(\frac{2^{\omega}K}{2^{t-1}}\right)\right) \tag{6.43}$$

Due to the geometric sum indexed by u in (6.43), this expression vanishes for $\omega+3<t$.

Thus, we take $\omega + 3 = t$ in (6.43). With Proposition 2.18, we see that $F(\omega + 3)$ is given by

$$\begin{aligned}
&2^{\omega+5-\frac{\delta}{2}}\left(\frac{2}{AD}\right)^{\delta}\left(\frac{2}{D}\right)^{\omega+\alpha} 2^{\omega} i^{\frac{K}{2}}(1+(-1)^{\delta+1}) i^{A\left(\frac{D+1}{2}\right)^2}(-1)^{\frac{D+1}{2}}(1+(-1)^{\delta+\frac{D+1}{2}} i^K) \\
&\quad = 2^{2\omega+6-\frac{\delta}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{AD}\right)\left(\frac{2}{D}\right)^{\omega+\alpha} 2^{-\frac{1}{2}}\left(\frac{2}{K}\right)(1+i^K) i^{A\left(\frac{D+1}{2}\right)^2}(-1)^{\frac{D+1}{2}} \\
&\quad \times (1+(-1)^{\frac{D-1}{2}} i^K) \\
&\quad = 2^{2\omega+6-\frac{(\delta+1)}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{ADK}\right)\left(\frac{2}{D}\right)^{\omega+\alpha} i^{A\left(\frac{D+1}{2}\right)^2}(-1)^{\frac{D+1}{2}} \\
&\quad \times (1+(-1)^{\frac{D-1}{2}} i^K). \qquad (6.44)
\end{aligned}$$

If $\mathbb{O}(\frac{D+1}{2}) = 1$, then (6.44) becomes

$$\begin{aligned}
&2^{2\omega+6-\frac{(\delta+1)}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{ADK}\right)\left(\frac{2}{D}\right)^{\omega+\alpha}(1+i^K)(1-i^K) \\
&\qquad = 2^{\omega+6+\frac{1-\delta}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{ADK}\right)\left(\frac{2}{D}\right)^{\omega+\alpha}. \qquad (6.45)
\end{aligned}$$

Otherwise, for $\mathbb{O}(\frac{D-1}{2}) = 1$, (6.44) is given by

$$\begin{aligned}
&2^{2\omega+6-\frac{(\delta+1)}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{ADK}\right)\left(\frac{2}{D}\right)^{\omega+\alpha}(-1) i^A (1+i^K)^2 \\
&\qquad = -2^{2\omega+6+\frac{1+\delta}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{ADK}\right)\left(\frac{2}{D}\right)^{\omega+\alpha} i^{A+K} \\
&\qquad = 2^{2\omega+6+\frac{1+\delta}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{ADK}\right)\left(\frac{2}{D}\right)^{\omega+\alpha}(-1)^{\frac{A-K}{2}}. \qquad (6.46)
\end{aligned}$$

Hence, with (6.45) and (6.46) we have

$$F(\omega+3) = 2^{2(\omega+3)+\frac{1-\delta}{2}}\mathbb{O}(\delta+1)\left(\frac{2}{ADK}\right)\left(\frac{2}{D}\right)^{\omega+\alpha}(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)}.$$

Next, suppose $\omega + 2 = t$. Substituting this into (6.43) yields

$$\begin{aligned}
&2^{\omega+4-\frac{\delta}{2}}\left(\frac{2}{AD}\right)^{\delta}\left(\frac{2}{D}\right)^{\omega+\alpha+1}2^{\omega-1}e\left(\frac{K}{4}\right)(1+(-1)^{\delta})i^{A\left(\frac{D+1}{2}\right)^2}(-1)^{\frac{D+1}{2}}\\
&\quad\times(1+(-1)^{\frac{D+1}{2}}e\left(\frac{K}{2}\right))\\
&\quad=2^{2\omega+4-\frac{\delta}{2}}\mathbb{O}(\delta)\left(\frac{2}{D}\right)^{\omega+\alpha+1}i^{K}i^{A\left(\frac{D+1}{2}\right)^2}(-1)^{\frac{D+1}{2}}(1+(-1)^{\frac{D-1}{2}})\\
&\quad=-2^{2\omega+5-\frac{\delta}{2}}\mathbb{O}(\delta)\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha+1}i^{A+K}\\
&\quad=2^{2\omega+5-\frac{\delta}{2}}\mathbb{O}(\delta)\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha+1}(-1)^{\frac{A-K}{2}}.
\end{aligned}$$

Continuing, we let $\omega + 1 = t$ and substitute this into (6.43). Hence, $F(\omega + 1)$ is given by

$$\begin{aligned}
&2^{\omega+3-\frac{\delta}{2}}\left(\frac{2}{AD}\right)^{\delta}\left(\frac{2}{D}\right)^{\omega+\alpha}2^{\omega-2}e\left(\frac{K}{2}\right)(1+(-1)^{\delta})i^{A\left(\frac{D+1}{2}\right)^2}(-1)^{\frac{D+1}{2}}(1+(-1)^{\frac{D+1}{2}})\\
&\quad=-2^{2\omega+3-\frac{\delta}{2}}\mathbb{O}(\delta)\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha}.
\end{aligned}$$

Finally, for $\omega \geq t$, (6.43) becomes

$$\begin{aligned}
&2^{t+2-\frac{\delta}{2}}\left(\frac{2}{AD}\right)^{\delta}\left(\frac{2}{D}\right)^{t+1+\alpha}2^{t-3}(1+(-1)^{\delta})(1+(-1)^{\frac{D+1}{2}})\\
&\quad=2^{2t+1-\frac{\delta}{2}}\mathbb{O}(\delta)\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{t+1+\alpha}.
\end{aligned}$$

□

Proposition 6.11. *Let $t \in \mathbb{N}$. Then*

$$\sum_{\substack{S<2^t\\ S\equiv 1 \pmod 2}} e\left(\frac{-2^{\omega}KS}{2^t}\right) = \begin{cases} 0 & \text{if } \omega < t-1\\ -2^{\omega} & \text{if } \omega = t-1\\ 2^{t-1} & \text{if } \omega > t-1. \end{cases}$$

Proof. By Proposition 2.5, we have

$$\begin{aligned}\sum_{\substack{S<2^t\\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right) &= \sum_{\substack{S<2^t\\ S\equiv 1 \pmod 2}} e\left(\frac{2^\omega KS}{2^t}\right)\\ &= \sum_{u=0}^{2^{t-1}-1} e\left(\frac{2^\omega K(2u+1)}{2^t}\right) = e\left(\frac{2^\omega K}{2^t}\right)\sum_{u=0}^{2^{t-1}-1} e\left(\frac{2^\omega K}{2^{t-1}}\right)\\ &= \begin{cases} 0 & \text{if } \omega < t-1\\ e\left(\frac{2^\omega K}{2^t}\right)\sum_{u=0}^{2^{t-1}-1} 1 & \text{if } \omega \le t-1\end{cases}\\ &= \begin{cases} 0 & \text{if } \omega < t-1\\ -2^\omega & \text{if } \omega = t-1\\ 2^{t-1} & \text{if } \omega > t-1.\end{cases}\end{aligned}$$

□

Proposition 6.12. *For $\alpha > 1$,*

$$\sum_{t=1}^{\alpha}\frac{1}{2^t}\sum_{\substack{S<2^t\\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right) = \begin{cases}\frac{\alpha}{2} & \textit{if } \omega+1>\alpha\\ \frac{\omega-1}{2} & \textit{if } \omega+1\le\alpha.\end{cases}$$

Proof. From Proposition 6.11, we have

$$\sum_{t=1}^{\alpha}\frac{1}{2^t}\sum_{\substack{S<2^t\\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right) = \sum_{t=1}^{\alpha}\frac{1}{2^t}\begin{cases} 0 & \text{if } \omega < t-1\\ -2^\omega & \text{if } \omega = t-1\\ 2^{t-1} & \text{if } \omega > t-1.\end{cases} \tag{6.47}$$

Hence, if $\omega+1>\alpha$, then (6.47) is given by

$$\sum_{t=1}^{\alpha}\frac{1}{2^t}(2^{t-1}) = \frac{\alpha}{2}.$$

Otherwise, for $\omega + 1 \leq \alpha$, (6.47) resolves to

$$\sum_{t=1}^{\omega} \frac{1}{2^t}(2^{t-1}) + \frac{1}{2^{\omega+1}}(-2^{\omega}) = \frac{1}{2}(\omega - 1).$$

□

From (6.33) and (6.34), to complete the evaluation of $N_{2^n}(a, b, c; k)$, we must examine the sums $\sum_{t=2}^{\delta-2} \frac{E(t)}{2^t}$ and $\sum \frac{2^\delta F(t)}{2^{2t+2}}$. The following corollaries all follow from the previous propositions, and will be used in the evaluation of $N_{2^n}(a, b, c; k)$.

Corollary 6.1. *We have that*

$$\frac{E(2)}{4} = \begin{cases} (-1)^{\frac{A-K}{2}} & \text{if } \omega = 0 \\ -1 & \text{if } \omega = 1 \\ 1 & \text{if } \omega \geq 2. \end{cases}$$

Proof. The result is immediate upon multiplying the statement of Proposition 6.7 by $\frac{1}{4}$. □

Corollary 6.2. *We have, for $t \geq 3$,*

$$\frac{E(t)}{2^t} = \begin{cases} 0 & \text{if } \omega + 3 < t \\ 2^{\frac{\omega}{2}+1}\left(\frac{2}{AK}\right)\mathbb{O}(\omega)\mathbb{O}(\frac{A-K}{2}) & \text{if } t = \omega + 3 \\ 2^{\frac{\omega}{2}}\mathbb{O}(\omega)(-1)^{\frac{A-K}{2}} & \text{if } t = \omega + 2 \\ -2^{\frac{\omega-1}{2}}\mathbb{O}(\omega + 1) & \text{if } t = \omega + 1 \\ 2^{\frac{t}{2}-1}\mathbb{O}(t) & \text{if } t \leq \omega. \end{cases}$$

Proof. We obtain our results by multiplying Proposition 6.8 by $\frac{1}{2^t}$ and considering the various cases. □

We introduce some notation to aid in our evaluation.

Definition 6.6. Suppose $t \geq 3$. Then we set

$$\begin{aligned} U_1(\omega) &= \frac{E(\omega+3)}{2^t} + \frac{E(\omega+2)}{2^t} \\ U_2(\omega) &= \frac{E(\omega+2)}{2^t} + \frac{E(\omega+1)}{2^t} \\ U_3(\omega) &= \frac{E(\omega+3)}{2^t} + \frac{E(\omega+2)}{2^t} + \frac{E(\omega+1)}{2^t}. \end{aligned}$$

Corollary 6.3. *For $t \geq 3$, we have*

$$\begin{aligned} U_1(\omega) &= 2^{\frac{\omega}{2}}\mathbb{O}(\omega)\left[2\left(\frac{2}{AK}\right)\mathbb{O}(\frac{A-K}{2}) + (-1)^{\frac{A-K}{2}}\right], \\ U_2(\omega) &= 2^{\left[\frac{\omega}{2}\right]}\left[\mathbb{O}(\omega)(-1)^{\frac{A-K}{2}} - \mathbb{O}(\omega+1)\right], \\ U_3(\omega) &= 2^{\left[\frac{\omega}{2}\right]}\left[\mathbb{O}(\omega)\left(2\left(\frac{2}{AK}\right)\mathbb{O}(\frac{A-K}{2}) + (-1)^{\frac{A-K}{2}}\right) - \mathbb{O}(\omega+1)\right]. \end{aligned}$$

Proof. We group together the appropriate terms using Corollary 6.2. □

Corollary 6.4. *For ω and $\delta - 2 \geq 3$, we have*

$$\sum_{t=3}^{\omega} \frac{E(t)}{2^t} = 2^{\left[\frac{\omega}{2}\right]} - 2 \quad \text{and} \quad \sum_{t=3}^{\delta-2} \frac{E(t)}{2^t} = 2^{\left[\frac{\delta-2}{2}\right]} - 2.$$

Proof. From Corollary 6.2, we have

$$\begin{aligned} \sum_{t=3}^{\omega} \frac{E(t)}{2^t} = \sum_{t=2}^{\omega} 2^{\frac{t}{2}-1}\mathbb{O}(t) = \frac{1}{2}\sum_{\substack{t=3 \\ 2|t}}^{\omega} 2^{\frac{t}{2}} = \sum_{\substack{t=1 \\ 2|t}}^{\omega-2} 2^{\frac{t}{2}} = \sum_{t=1}^{\left[\frac{\omega-2}{2}\right]} 2^t \\ = 2\sum_{t=0}^{\left[\frac{\omega-2}{2}\right]-1} 2^t = 2\left(2^{\left[\frac{\omega-2}{2}\right]} - 1\right) \\ = 2^{\left[\frac{\omega}{2}\right]} - 2. \end{aligned}$$

By similar reasoning we deduce the result for $\sum_{t=3}^{\delta-2} \frac{E(t)}{2^t}$. □

Thus, the evaluation of $\sum_{t=2}^{\delta-2} \frac{E(t)}{2^t}$ will vary based on the choice of ω. We deduce similar corollaries now for $\sum \frac{2^\delta F(t)}{2^{2t+2}}$. The expression for F contains additional terms, and will be dependent on both ω and δ.

Corollary 6.5. *For $\alpha = 1$ and $\delta \leq 2$, we have*

$$\frac{2^\delta F(2)}{2^6} = 2^{\frac{\delta}{2}-1} \begin{cases} (-1)^{\frac{A-K}{2}} \mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 0 \\ -\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega = 1 \\ \mathbb{O}(\frac{D+1}{2}) & \text{if } \omega \geq 2. \end{cases}$$

Proof. The results are obtained by multiplying the statement of Proposition 6.9 by $2^{\delta-6}$. □

Corollary 6.6. *Let $t \geq 3$. Then for $\alpha < t$ and $\delta \leq t$ we have*

$$2^{\delta-2}\frac{F(t)}{2^{2t}} = \begin{cases} 0 & \text{if } \omega + 3 < t \\ 2^{\frac{\delta-3}{2}} \mathbb{O}(\delta+1) \left(\frac{2}{ADK}\right) \left(\frac{2}{D}\right)^{\omega+\alpha} (-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \omega + 3 = t \\ 2^{\frac{\delta}{2}-1} \mathbb{O}(\delta) \mathbb{O}(\frac{D-1}{2}) \left(\frac{2}{D}\right)^{\omega+\alpha+1} (-1)^{\frac{A-K}{2}} & \text{if } \omega + 2 = t \\ -2^{\frac{\delta}{2}-1} \mathbb{O}(\delta) \mathbb{O}(\frac{D+1}{2}) \left(\frac{2}{D}\right)^{\omega+\alpha} & \text{if } \omega + 1 = t \\ 2^{\frac{\delta}{2}-1} \mathbb{O}(\delta) \mathbb{O}(\frac{D+1}{2}) \left(\frac{2}{D}\right)^{t+1+\alpha} & \text{if } \omega \geq t. \end{cases}$$

Proof. The proof results from multiplying Proposition 6.10 by $2^{\delta-(2t+2)}$ and simplifying according to each case. □

We introduce some notation to keep track of these sums.

Definition 6.7. For $t \geq 3$ and $\delta \leq t$ we let

$$T_1(\omega, \delta) = \frac{2^\delta F(\omega+3)}{2^{2t+2}} + \frac{2^\delta F(\omega+2)}{2^{2t+2}},$$

$$T_2(\omega,\delta) = \frac{2^\delta F(\omega+2)}{2^{2t+2}} + \frac{2^\delta F(\omega+1)}{2^{2t+2}},$$
$$T_3(\omega,\delta) = \frac{2^\delta F(\omega+3)}{2^{2t+2}} + \frac{2^\delta F(\omega+2)}{2^{2t+2}} + \frac{2^\delta F(\omega+1)}{2^{2t+2}}.$$

Corollary 6.7. *For $t \geq 3$,*

$$T_1(\omega,\delta) = 2^{\left[\frac{\delta-3}{2}\right]}\left(\frac{2}{D}\right)^{\omega+\alpha+1}\left(\mathbb{O}(\delta+1)\left(\frac{2}{AK}\right)(-1)^{(\frac{A-K}{2})(\frac{D+1}{2})} + \mathbb{O}(\delta)(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\right)$$
$$T_2(\omega,\delta) = 2^{\frac{\delta}{2}-1}\mathbb{O}(\delta)\left(\frac{2}{D}\right)^{\omega+\alpha+1}\left(\mathbb{O}(\frac{D-1}{2})(-1)^{\frac{A-K}{2}} - \left(\frac{2}{D}\right)\mathbb{O}(\frac{D+1}{2})\right)$$
$$T_3(\omega,\delta) = 2^{\left[\frac{\delta-3}{2}\right]}\left(\frac{2}{D}\right)^{\omega+\alpha+1}\left(\mathbb{O}(\delta+1)\left(\frac{2}{AK}\right)(-1)^{(\frac{A-K}{2})(\frac{D+1}{2})}\right.$$
$$\left. + \mathbb{O}(\delta)\left[\mathbb{O}(\frac{D-1}{2})(-1)^{\frac{A-K}{2}} - \mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)\right]\right).$$

Proof. We combine the appropriate sums using Corollary 6.6. □

Corollary 6.8. *Let $u, v \in \mathbb{N}$ be such that $3 \leq u \leq v$. Then,*

$$\sum_{t=u}^{v} \frac{2^\delta}{2^{2t+2}} F(t) = 2^{\frac{\delta}{2}-1}\left(\frac{2}{D}\right)^{\alpha+1} P_D(u,v)\mathbb{O}(\delta)\mathbb{O}(\frac{D+1}{2}).$$

Proof. With Corollary 6.6 and Definition 6.3, we have

$$\begin{aligned}\sum_{t=u}^{v} \frac{2^\delta}{2^{2t+2}} F(t) &= \sum_{t=u}^{v} 2^{\frac{\delta}{2}-1}\mathbb{O}(\delta)\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{t+1+\alpha} \\ &= 2^{\frac{\delta}{2}-1}\mathbb{O}(\delta)\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{\alpha+1}\sum_{t=u}^{v}\left(\frac{2}{D}\right)^{t} \\ &= 2^{\frac{\delta}{2}-1}\left(\frac{2}{D}\right)^{\alpha+1} P_D(u,v)\mathbb{O}(\delta)\mathbb{O}(\frac{D+1}{2}).\end{aligned}$$

□

6.4 Number of Solutions: Even Prime

With the preliminary steps out of the way, in order to evaluate $N_{2^n}(a,b,c;k)$, we must consider various cases with respect to α, δ, ω and n. We divide our cases according to α. Hence, we proceed first under the assumption that $\alpha = 1$. We consider $N_{2^n}(a,b,c;k)$ under the cases

(I) $n = 1$,

(II) $n \geq 2$, $\delta \leq 2$,

(III) $n \geq 2$, $\delta = 3$,

(IV) $4 \leq \delta \leq n$,

(V) $4 \leq n+1 \leq \delta \leq n+2$.

In light of (6.33) and Proposition 6.6, we have that

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \mathbb{O}(2^\delta + 1)\frac{(-1)^{2^\omega + c}}{2} + \sum_{t=2}^{\delta-2} \frac{E(t)}{2^t} + \sum_{t=\max(2,\delta)}^{n} \frac{2^\delta F(t)}{2^{2t+2}} \right\}. \tag{6.48}$$

Hence, we use (6.48) to give similar expressions for our five cases.

Case I: $n = 1$**;**

$$N_{2^n}(a,b,c;k) = 2 \left\{ 1 + \mathbb{O}(2^\delta + 1)\frac{(-1)^{2^\omega + c}}{2} \right\}. \tag{6.49}$$

Case II: $n \geq 2$**,** $\delta \leq 2$**;**

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \mathbb{O}(2^\delta + 1)\frac{(-1)^{2^\omega + c}}{2} + \sum_{t=2}^{n} \frac{2^\delta F(t)}{2^{2t+2}} \right\}. \tag{6.50}$$

Case III: $n \geq 2$, $\delta = 3$;

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \sum_{t=3}^{n} \frac{2^\delta F(t)}{2^{2t+2}} \right\}. \tag{6.51}$$

Case IV: $4 \leq \delta \leq n$;

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \sum_{t=2}^{\delta-2} \frac{E(t)}{2^t} + \sum_{t=\delta}^{n} \frac{2^\delta F(t)}{2^{2t+2}} \right\}. \tag{6.52}$$

Case V: $4 \leq n+1 \leq \delta \leq n+2$;

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \sum_{t=2}^{\delta-2} \frac{E(t)}{2^t} \right\}. \tag{6.53}$$

We now proceed to evaluate these sums using the material from the previous section. These sums will be broken up into further cases depending on certain variables. However, the first case is straightforward.

Theorem 6.8 (**Case I**). *Let $\alpha = n = 1$. Then*

$$N_2(a,b,c;k) = 2 + (-1)^{2^\omega + c}\mathbb{O}(2^\delta + 1) = \begin{cases} 2 & \text{if } \delta \geq 1 \\ 2 + (-1)^{2^\omega + c} & \text{if } \delta = 0. \end{cases}$$

Proof. This is easily deduced from the equation given in (6.49). □

Theorem 6.9 (**Case II**). *Let $\alpha = 1$, $n \geq 2$ and $\delta \leq 2$. If $n = 2$, then $N_4(a,b,c;k)$ is given by*

$$4 + 2(-1)^{2^\omega + c}\mathbb{O}(2^\delta + 1) + 2^{\frac{\delta}{2}+1} \begin{cases} (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 0 \\ -\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega = 1 \\ \mathbb{O}(\frac{D+1}{2}) & \text{if } \omega \geq 2. \end{cases}$$

If $n \geq 3$, $N_{2^n}(a,b,c;k)$ is given by

$$2^n + 2^{n-1}(-1)^{2^\omega+c}\mathbb{O}(2^\delta+1)$$
$$+ 2^{n-1+\frac{\delta}{2}} \begin{cases} (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 0, n \geq 3 \\ -\mathbb{O}(\frac{D+1}{2}) + \mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)(-1)^{\frac{A-K}{2}} & \text{if } \omega = 1, n = 3 \\ \mathbb{O}(\frac{D+1}{2})\left(1 - \left(\frac{2}{D}\right)\right) & \text{if } \omega = 2, n = 3 \\ \mathbb{O}(\frac{D+1}{2})\left(1 - \left(\frac{2}{D}\right)\right) + (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 2, n \geq 4 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(3,n)+1\right) & \text{if } \omega \geq n \geq 3 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(3,\omega)+1-\left(\frac{2}{D}\right)^{\omega+1}\right) & \text{if } 3 \leq \omega = n-1 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(3,\omega)+1-\left(\frac{2}{D}\right)^{\omega+1}\right) + (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } 3 \leq \omega \leq n-2. \end{cases}$$

Proof. From (6.50), we see that

$$N_{2^n}(a,b,c;k) = 2^n\left\{1 + \frac{(-1)^{2^\omega+c}}{2}\mathbb{O}(2^\delta+1) + \frac{2^\delta F(2)}{2^6} + \sum_{t=3}^{n}\frac{2^\delta F(t)}{2^{t+2}}\right\}. \tag{6.54}$$

From (6.54) and Corollary 6.5, the first three terms in the bracketed expression of (6.54) are given by

$$1 + \frac{(-1)^{2^\omega+c}}{2}\mathbb{O}(2^\delta+1) + 2^{\frac{\delta}{2}-1}\begin{cases} (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 0 \\ -\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega = 1 \\ \mathbb{O}(\frac{D+1}{2}) & \text{if } \omega \geq 2. \end{cases} \tag{6.55}$$

Hence, when $n = 2$, $N_{2^n}(a,b,c;k)$ is given by (6.55).

Suppose now that $n \geq 3$. We consider $\displaystyle\sum_{t=3}^{n}\frac{2^\delta F(t)}{2^{t+2}}$ for various n and ω. Observe that as

$\delta \leq 2$, we must have δ even. By Proposition 6.10 and Definition 6.7, we have

$$\sum_{t=3}^{n} \frac{2^\delta F(t)}{2^{2t+2}} = \begin{cases} 0 & \text{if } \omega = 0, n \geq 3 \\ \dfrac{2^\delta F(\omega+2)}{2^{2(3)+2}} & \text{if } \omega = 1, n \geq 3 \\ \dfrac{2^\delta F(\omega+1)}{2^{2(3)+2}} & \text{if } \omega = 2, n = 3 \\ T_2(2,\delta) & \text{if } \omega = 2, n \geq 4 \\ \displaystyle\sum_{t=3}^{n} \frac{2^\delta F(t)}{2^{2t+2}} & \text{if } \omega \geq n \geq 3 \\ \displaystyle\sum_{t=3}^{\omega} \frac{2^\delta F(t)}{2^{2t+2}} + \frac{2^\delta F(\omega+1)}{2^{2(\omega+1)+2}} & \text{if } 3 \leq \omega, n = \omega+1 \\ \displaystyle\sum_{t=3}^{\omega+1} \frac{2^\delta F(t)}{2^{2t+2}} + T_2(\omega,\delta) & \text{if } 3 \leq \omega \leq n-2. \end{cases} \tag{6.56}$$

Combining (6.55) and (6.56) and using Corollaries 6.6, 6.7 and 6.8, we see the bracketed term of (6.54) is given by

$$1 + \frac{(-1)^{2^\omega + c}}{2}\mathbb{O}(2^\delta + 1) + 2^{\frac{\delta}{2}-1} \begin{cases} (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 0, n \geq 3 \\ -\mathbb{O}(\frac{D+1}{2}) + \mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)(-1)^{\frac{A-K}{2}} & \text{if } \omega = 1, n = 3 \\ \mathbb{O}(\frac{D+1}{2})\left(1 - \left(\frac{2}{D}\right)\right) & \text{if } \omega = 2, n = 3 \\ \mathbb{O}(\frac{D+1}{2})\left(1 - \left(\frac{2}{D}\right)\right) + (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \omega = 2, n \geq 4 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(3,n) + 1\right) & \text{if } \omega \geq n \geq 3 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(3,\omega) + 1 - \left(\frac{2}{D}\right)^{\omega+1}\right) & \text{if } 3 \leq \omega = n-1 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(3,\omega) + 1 - \left(\frac{2}{D}\right)^{\omega+1}\right) + (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } 3 \leq \omega \leq n-2. \end{cases} \tag{6.57}$$

Hence, we multiply (6.57) by 2^n and simplify to arrive at the statement of the theorem. $\square$

Theorem 6.10 (Case III). *Let $\alpha = 1$, $n \geq 2$ and $\delta = 3$. Then $N_{2^n}(a, b, c; k)$ is given by*

$$2^n \begin{cases} 1 & \text{if } \omega + 3 > n \\ 1 + \left(\frac{2}{D}\right)^{\omega} \left(\frac{2}{AK}\right) (-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \omega + 3 \leq n. \end{cases}$$

Proof. From (6.51), we have that

$$N_{2^n}(a, b, c; k) = 2^n \left\{ 1 + \sum_{t=3}^{n} \frac{2^\delta F(t)}{2^{2t+2}} \right\}. \tag{6.58}$$

We look for a similar expression to that in (6.56), except now we have that δ is odd. Hence, by Proposition 6.10 and Definition 6.7, we have

$$\sum_{t=3}^{n} \frac{2^\delta F(t)}{2^{2t+2}} = \begin{cases} 0 & \text{if } n = 2 \\ \dfrac{2^\delta F(\omega+3)}{2^{2t+2}} & \text{if } \omega = 0, n \geq 3 \\ \dfrac{2^\delta F(\omega+2)}{2^{2t+2}} & \text{if } \omega = 1, n = 3 \\ T_1(1, \delta) & \text{if } \omega = 1, n \geq 4 \\ \dfrac{2^\delta F(\omega+1)}{2^{2t+2}} & \text{if } \omega = 2, n = 3 \\ T_2(2, \delta) & \text{if } \omega = 2, n = 4 \\ T_3(2, \delta) & \text{if } \omega = 2, n \geq 5 \\ \displaystyle\sum_{t=3}^{n} \frac{2^\delta F(t)}{2^{2t+2}} & \text{if } 3 \leq n \leq \omega \\ \displaystyle\sum_{t=3}^{\omega} \frac{2^\delta F(t)}{2^{2t+2}} + \frac{2^\delta F(\omega+1)}{2^{2t+2}} & \text{if } 3 \leq \omega = n - 1 \\ \displaystyle\sum_{t=3}^{\omega} \frac{2^\delta F(t)}{2^{2t+2}} + T_2(\omega, \delta) & \text{if } 3 \leq \omega = n - 2 \\ \displaystyle\sum_{t=3}^{\omega} \frac{2^\delta F(t)}{2^{2t+2}} + T_3(\omega, \delta) & \text{if } 3 \leq \omega \leq n - 3. \end{cases} \tag{6.59}$$

As δ is odd, with Corollaries 6.6-6.8, (6.59) simplifies to

$$\begin{cases} 0 & \text{if } n = 2 \\ \left(\frac{2}{AK}\right)(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \omega = 0, n \geq 3 \\ 0 & \text{if } \omega = 1, n = 3 \\ \left(\frac{2}{AK}\right)\left(\frac{2}{D}\right)^{\omega}(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \omega = 1, n \geq 4 \\ 0 & \text{if } \omega = 2, n = 3, 4 \\ \left(\frac{2}{AK}\right)(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \omega = 2, n \geq 5 \\ 0 & \text{if } 3 \leq n-2 \leq \omega \\ \left(\frac{2}{D}\right)^{\omega}\left(\frac{2}{AK}\right)(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } 3 \leq \omega \leq n-3. \end{cases} \tag{6.60}$$

Hence, with (6.58) and (6.60), when $\omega + 3 \leq n$, we have

$$N_{2^n}(a, b, c; k) = 2^n \left\{1 + \left(\frac{2}{D}\right)^{\omega}\left(\frac{2}{AK}\right)(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)}\right\},$$

and when $\omega + 3 > n$, we have

$$N_{2^n}(a, b, c; k) = 2^n.$$

□

Theorem 6.11 (Case IV). *Let $\alpha = 1$ and $4 \leq \delta \leq n$. Then $N_{2^n}(a, b, c; k)$ is given according to the following cases.*

If $\omega \equiv \delta \equiv 0 \pmod 2$ *and* $D \equiv 1 \pmod 4$,

$$N_{2^n}(a,b,c;k) = 2^n \begin{cases} 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega+5 \le \delta \\ 2^{\frac{\delta}{2}-1}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega+4=\delta \\ 2^{\frac{\delta}{2}}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega+2=\delta \\ 2^{\frac{\delta}{2}-1} & \text{if } \delta \le n-1 \le \omega \\ 2^{\frac{\delta}{2}}\mathbb{O}(\frac{A-K}{2}) & \text{if } \delta \le \omega \le n-2. \end{cases}$$

If $\omega \equiv \delta \equiv 0 \pmod 2$ *and* $D \equiv 3 \pmod 4$,

$$N_{2^n}(a,b,c;k) = 2^n \begin{cases} 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega+5 \le \delta \\ 2^{\frac{\delta}{2}-1}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega+4=\delta \\ 2^{\frac{\delta}{2}-1} & \text{if } \omega+2=\delta \\ 2^{\frac{\delta}{2}-1}\left(1+P_D(\delta,n)\right) & \text{if } \delta \le n \le \omega \\ 2^{\frac{\delta}{2}-1}\left(2-\left(\frac{2}{D}\right)+\left(\frac{\omega-\delta}{2}\right)\left(1+\left(\frac{2}{D}\right)\right)\right) & \text{if } \delta \le \omega \le n-1. \end{cases}$$

If $\omega \equiv 1 \pmod 2$, $\delta \equiv 0 \pmod 2$ *and* $D \equiv 1 \pmod 4$,

$$N_{2^n}(a,b,c;k) = 2^{n+\frac{\delta}{2}-1} \begin{cases} 0 & \text{if } \omega+3 \le \delta \\ 1 & \text{if } \delta \le n-1 \le \omega \text{ or } \delta=\omega+1=n \\ 1+(-1)^{\frac{A-K}{2}}\left(\frac{2}{D}\right) & \text{if } \delta \le \omega \le n-2 \text{ or } \delta=\omega+1 \le n-1. \end{cases}$$

If $\omega \equiv 1 \pmod 2$, $\delta \equiv 0 \pmod 2$ *and* $D \equiv 3 \pmod 4$,

$$N_{2^n}(a,b,c;k) = 2^{n+\frac{\delta}{2}-1} \begin{cases} 0 & \text{if } \omega+1 \le \delta \\ \left(\frac{\omega-\delta+1}{2}\right)\left(1+\left(\frac{2}{D}\right)\right) & \text{if } \delta \le \omega \le n-1 \\ 1+P_D(\delta,n) & \text{if } \delta \le n \le \omega. \end{cases}$$

If $\omega \equiv 0 \pmod 2$ *and* $\delta \equiv 1 \pmod 2$,

$$N_{2^n}(a,b,c;k) = 2^n \begin{cases} 2^{\frac{\omega}{2}+1}\mathbb{O}\left(\frac{A-K}{2}\right)\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega+5 \le \delta \\ 2^{\frac{\delta-3}{2}}\left(1+(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)}\left(\frac{2}{AK}\right)\right) & \text{if } 5 \le \delta \le \omega+3 \le n \\ 2^{\frac{\delta-3}{2}} & \text{if } n < \omega+3. \end{cases}$$

If $\omega \equiv \delta \equiv 1 \pmod 2$,

$$N_{2^n}(a,b,c;k) = 2^{n+\frac{\delta-3}{2}} \begin{cases} 0 & \text{if } \omega+3 < \delta \\ 1+\left(\frac{2}{AKD}\right)(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \delta < \omega+3 \le n \\ 1 & \text{if } \omega+3 > n. \end{cases}$$

Proof. From (6.52), we have

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1+\frac{E(2)}{4}+\sum_{t=3}^{\delta-2}\frac{E(t)}{2^t}+\sum_{t=\delta}^{n}\frac{2^\delta F(t)}{2^{2t+2}} \right\}. \tag{6.61}$$

From Corollary 6.1, we see that the first two terms of the terms inside the brackets in (6.61)

are given by

$$1+\begin{Bmatrix}(-1)^{\frac{A-K}{2}} & \text{if } \omega=0\\ -1 & \text{if } \omega=1\\ 1 & \text{if } \omega\geq 2\end{Bmatrix}=\begin{cases}2\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega=0\\ 0 & \text{if } \omega=1\\ 2 & \text{if } \omega\geq 2.\end{cases} \tag{6.62}$$

From Proposition 6.8, the third term within the brackets of (6.61) is given by

$$\sum_{t=3}^{\delta-2}\frac{E(t)}{2^t}=\begin{cases}0 & \text{if } \delta=4\\ \dfrac{E(\omega+3)}{2^t} & \text{if } \omega=0,\delta\geq 5\\ \dfrac{E(\omega+2)}{2^t} & \text{if } \omega=1,\delta=5\\ U_1(\omega) & \text{if } \omega=1,\delta\geq 6\\ \dfrac{E(\omega+1)}{2^t} & \text{if } \omega=2,\delta=5\\ U_2(\omega) & \text{if } \omega=2,\delta=6\\ U_3(\omega) & \text{if } \omega=2,\delta\geq 7\\ \displaystyle\sum_{t=3}^{\delta-2}\frac{E(t)}{2^t} & \text{if } 3\leq\delta-2\leq\omega\\ \displaystyle\sum_{t=3}^{\omega}\frac{E(t)}{2^t}+\frac{E(\omega+1)}{2^{\omega+1}} & \text{if } 3\leq\omega=\delta-3\\ \displaystyle\sum_{t=3}^{\omega}\frac{E(t)}{2^t}+U_2(\omega) & \text{if } 3\leq\omega=\delta-4\\ \displaystyle\sum_{t=3}^{\omega}\frac{E(t)}{2^t}+U_3(\omega) & \text{if } 3\leq\omega\leq\delta-5.\end{cases} \tag{6.63}$$

From Corollaries 6.2, 6.3 and 6.4, (6.63) will simplify to

$$\begin{cases} 0 & \text{if } \delta = 4 \\ 2\left(\frac{2}{AK}\right)\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = 0, \delta \geq 5 \\ 0 & \text{if } \omega = 1, \delta \geq 5 \\ 0 & \text{if } \omega = 2, \delta = 5 \\ 2(-1)^{\frac{A-K}{2}} & \text{if } \omega = 2, \delta = 6 \\ 2\left(2\left(\frac{2}{AK}\right)\mathbb{O}(\frac{A-K}{2}) + (-1)^{\frac{A-K}{2}}\right) & \text{if } \omega = 2, \delta \geq 7 \\ 2^{\left[\frac{\delta-2}{2}\right]} - 2 & \text{if } 3 \leq \delta - 2 \leq \omega \\ 2^{\left[\frac{\omega}{2}\right]} - 2 - 2^{\frac{\omega-1}{2}}\mathbb{O}(\omega+1) & \text{if } 3 \leq \omega = \delta - 3 \\ 2^{\left[\frac{\omega}{2}\right]} - 2 + 2^{\left[\frac{\omega}{2}\right]}\left(\mathbb{O}(\omega)(-1)^{\frac{A-K}{2}} - \mathbb{O}(\omega+1)\right) & \text{if } 3 \leq \omega = \delta - 4 \\ 2^{\left[\frac{\omega}{2}\right]} - 2 + 2^{\left[\frac{\omega}{2}\right]}\mathbb{O}(\omega)\left(2\left(\frac{2}{AK}\right)\mathbb{O}(\frac{A-K}{2}) + (-1)^{\frac{A-K}{2}}\right) - 2^{\left[\frac{\omega}{2}\right]}\mathbb{O}(\omega+1) & \text{if } 3 \leq \omega \leq \delta - 5. \end{cases} \tag{6.64}$$

Thus, by combining (6.62) and (6.64), the first three terms of (6.61) are given by

$$\begin{cases} 2\mathbb{O}\left(\frac{A-K}{2}\right) & \text{if } \delta = 4, \omega = 0 \\ 0 & \text{if } \delta = 4, \omega = 1 \\ 2 & \text{if } \delta = 4, \omega = 2 \\ 2\mathbb{O}(\frac{A-K}{2})\left(1 + \left(\frac{2}{AK}\right)\right) & \text{if } \omega = 0, \delta \geq 5 \\ 0 & \text{if } \omega = 1, \delta \geq 5 \\ 2 & \text{if } \omega = 2, \delta = 5 \\ 2^2\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = 2, \delta = 6 \\ 2^2\mathbb{O}(\frac{A-K}{2})\left(1 + \left(\frac{2}{AK}\right)\right) & \text{if } \omega = 2, \delta \geq 7 \\ 2^{\left[\frac{\delta-2}{2}\right]} & \text{if } 3 \leq \delta - 2 \leq \omega \\ 2^{\left[\frac{\omega}{2}\right]}\left(1 - \mathbb{O}(\omega+1)\right) & \text{if } 3 \leq \omega = \delta - 3 \\ 2^{\left[\frac{\omega}{2}\right]}\left(1 + \mathbb{O}(\omega)(-1)^{\frac{A-K}{2}} - \mathbb{O}(\omega+1)\right) & \text{if } 3 \leq \omega = \delta - 4 \\ 2^{\left[\frac{\omega}{2}\right]}\left[1 + \mathbb{O}(\omega)\left((-1)^{\frac{A-K}{2}} + 2\left(\frac{2}{AK}\right)\mathbb{O}(\frac{A-K}{2})\right) - \mathbb{O}(\omega+1)\right] & \text{if } 3 \leq \omega \leq \delta - 5. \end{cases} \tag{6.65}$$

It is clear that if ω is odd and satisfies $\omega \leq \delta - 3$, the first three terms of (6.61) will be zero. Further, from (6.65), we see that if ω is even, the first three terms of (6.61) are given by

$$\begin{cases} 2^{\left[\frac{\delta-2}{2}\right]} & \text{if } \omega \geq \delta - 2 \geq 2 \\ 2^{\frac{\omega}{2}} & \text{if } \omega = \delta - 3 \\ 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = \delta - 4 \\ 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1 + \left(\frac{2}{AK}\right)\right) & \text{if } \omega \leq \delta - 5. \end{cases} \tag{6.66}$$

Next, we look at $\sum_{t=\delta}^{n} \frac{2^\delta F(t)}{2^{2t+2}}$. From Proposition 6.8 and Definition 6.4, we have that

$$\sum_{t=\delta}^{n} \frac{2^\delta F(t)}{2^{2t+2}} = \begin{cases} 0 & \text{if } \omega+3 < \delta \\ \dfrac{2^\delta F(\omega+3)}{2^t} & \text{if } \omega+3 = \delta \\ \dfrac{2^\delta F(\omega+2)}{2^t} & \text{if } \omega+2 = \delta = n \\ T_1(\omega,\delta) & \text{if } \omega+2 = \delta \leq n-1 \\ \dfrac{2^\delta F(\omega+1)}{2^t} & \text{if } \omega+1 = \delta = n \\ T_2(\omega,\delta) & \text{if } \omega+1 = \delta = n-1 \\ T_3(\omega,\delta) & \text{if } \omega+1 = \delta \leq n-2 \\ \displaystyle\sum_{t=\delta}^{n} \frac{2^\delta F(t)}{2^{2t+2}} & \text{if } \delta \leq n \leq \omega \\ \displaystyle\sum_{t=\delta}^{\omega} \frac{2^\delta F(t)}{2^{2t+2}} + \frac{2^\delta F(t)}{2^{2t+2}} & \text{if } \delta \leq \omega = n-1 \\ \displaystyle\sum_{t=\delta}^{\omega} \frac{2^\delta F(t)}{2^{2t+2}} + T_2(\omega,\delta) & \text{if } \delta \leq \omega = n-2 \\ \displaystyle\sum_{t=\delta}^{\omega} \frac{2^\delta F(t)}{2^{2t+2}} + T_3(\omega,\delta) & \text{if } \delta \leq \omega \leq n-3. \end{cases} \tag{6.67}$$

We now simplify (6.67) based on the parity of δ. First, suppose δ is even. Then by Corollaries

6.6, 6.7 and 6.8, (6.67) simplifies to

$$2^{\frac{\delta}{2}-1}\begin{cases} 0 & \text{if } \omega+3\leq\delta \\ \mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega}(-1)^{\frac{A-K}{2}} & \text{if } \omega+2=\delta \\ -\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{\omega+1} & \text{if } \omega+1=\delta=n \\ \left(\frac{2}{D}\right)^{\omega}\mathbb{O}(\frac{D-1}{2})(-1)^{\frac{A-K}{2}}-\left(\frac{2}{D}\right)^{\omega+1}\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega+1=\delta\leq n-1 \\ P_D(\delta,n)\mathbb{O}(\frac{D+1}{2}) & \text{if } \delta\leq n\leq\omega \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(\delta,\omega)-\left(\frac{2}{D}\right)^{\omega+1}\right) & \text{if } \delta\leq\omega=n-1 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(\delta,\omega)-\left(\frac{2}{D}\right)^{\omega+1}\right)+\left(\frac{2}{D}\right)^{\omega}(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2}) & \text{if } \delta\leq\omega\leq n-2. \end{cases} \tag{6.68}$$

Otherwise, if δ is odd, with Corollaries 6.6, 6.7 and 6.8, (6.67) reduces to

$$\begin{cases} 0 & \text{if } \omega+3<\delta \text{ or } \omega+3>n \\ 2^{\frac{\delta-3}{2}}\left(\frac{2}{AK}\right)\left(\frac{2}{D}\right)^{\omega}(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \delta\leq\omega+3\leq n. \end{cases} \tag{6.69}$$

Hence, we see that $N_{2^n}(a,b,c;k)$ will depend on the parity of both δ and ω. Suppose first that $\delta\equiv\omega\equiv 0 \pmod 2$. By combining (6.66) and (6.68), we see that the bracketed expression in (6.61) is given by

$$\begin{cases} 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega+5\leq\delta \\ 2^{\frac{\delta}{2}-1}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega+4=\delta \\ 2^{\frac{\delta}{2}-1}\left(1+(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\right) & \text{if } \omega+2=\delta \\ 2^{\frac{\delta}{2}-1}\left(1+\mathbb{O}(\frac{D+1}{2})P_D(\delta,n)\right) & \text{if } \delta\leq n\leq\omega \\ 2^{\frac{\delta}{2}-1}\left(1+\mathbb{O}(\frac{D+1}{2})\left[P_D(\delta,\omega)-\left(\frac{2}{D}\right)\right]\right) & \text{if } \delta\leq\omega=n-1 \\ 2^{\frac{\delta}{2}-1}\left(1+\mathbb{O}(\frac{D+1}{2})\left[P_D(\delta,\omega)-\left(\frac{2}{D}\right)\right]+(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\right) & \text{if } \delta\leq\omega\leq n-2. \end{cases} \tag{6.70}$$

We proceed by considering the residues of D modulo 4. If $D \equiv 1 \pmod 4$, then by (6.61) and (6.70), $N_{2^n}(a,b,c;k)$ is given by

$$2^n \begin{cases} 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega+5 \le \delta \\ 2^{\frac{\delta}{2}-1}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega+4=\delta \\ 2^{\frac{\delta}{2}}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega+2=\delta \\ 2^{\frac{\delta}{2}-1} & \text{if } \delta \le n-1 \le \omega \\ 2^{\frac{\delta}{2}}\mathbb{O}(\frac{A-K}{2}) & \text{if } \delta \le \omega \le n-2. \end{cases} \tag{6.71}$$

Otherwise, for $D \equiv 3 \pmod 4$, by (6.61), (6.70) and Proposition 6.5(b), we have that $N_{2^n}(a,b,c;k)$ is

$$2^n \begin{cases} 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega+5 \le \delta \\ 2^{\frac{\delta}{2}-1}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega+4=\delta \\ 2^{\frac{\delta}{2}-1} & \text{if } \omega+2=\delta \\ 2^{\frac{\delta}{2}-1}\left(1+P_D(\delta,n)\right) & \text{if } \delta \le n \le \omega \\ 2^{\frac{\delta}{2}-1}\left(2-\left(\frac{2}{D}\right)+\left(\frac{\omega-\delta}{2}\right)\left(1+\left(\frac{2}{D}\right)\right)\right) & \text{if } \delta \le \omega \le n-1. \end{cases} \tag{6.72}$$

Both (6.71) and (6.72) agree with the statement of the theorem.

Suppose now that ω is even and δ is odd. Then with (6.61), (6.66) and (6.69), we see that $N_{2^n}(a,b,c;k)$ is given by

$$2^n \begin{cases} 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega+5 \le \delta \\ 2^{\frac{\delta-3}{2}}\left(1+(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)}\left(\frac{2}{AK}\right)\right) & \text{if } 5 \le \delta \le \omega+3 \le n \\ 2^{\frac{\delta-3}{2}} & \text{if } n < \omega+3. \end{cases} \tag{6.73}$$

Finally, when ω is odd, from (6.65), the first three terms of the bracketed expression in

(6.61) are given by

$$\begin{cases} 0 & \text{if } \omega+3 \le \delta \\ 2^{\left[\frac{\delta-2}{2}\right]} & \text{if } \delta-2 \le \omega. \end{cases} \tag{6.74}$$

Hence, we combine (6.68), (6.69) and (6.74), depending on the parity of δ, and multiply by 2^n to arrive at an expression for $N_{2^n}(a,b,c;k)$. Note that by Proposition 6.5(c), if ω odd and δ even, we have

$$P_D(\delta,\omega) = \left(\frac{\omega-\delta+1}{2}\right)\left(1+\left(\frac{2}{D}\right)\right). \tag{6.75}$$

Hence, for ω odd and δ even, and with (6.75), $N_{2^n}(a,b,c;k)$ is given by

$$2^{n+\frac{\delta}{2}-1}\begin{cases} 0 & \text{if } \omega+3 \le \delta \\ 1-\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega+1=\delta=n \\ 1+(-1)^{\frac{A-K}{2}}\left(\frac{2}{D}\right)\mathbb{O}(\frac{D-1}{2})-\mathbb{O}(\frac{D+1}{2}) & \text{if } \omega+1=\delta\le n-1 \\ 1+P_D(\delta,n)\mathbb{O}(\frac{D+1}{2}) & \text{if } \delta\le n\le\omega \\ 1+\mathbb{O}(\frac{D+1}{2})\left[\left(\frac{\omega-\delta+1}{2}\right)\left(1+\left(\frac{2}{D}\right)\right)-1\right] & \text{if } \delta\le\omega=n-1 \\ 1+\mathbb{O}(\frac{D+1}{2})\left[\left(\frac{\omega-\delta+1}{2}\right)\left(1+\left(\frac{2}{D}\right)\right)-1\right] & \\ \quad +(-1)^{\frac{A-K}{2}}\left(\frac{2}{D}\right)\mathbb{O}(\frac{D-1}{2}) & \text{if } \delta\le\omega\le n-2. \end{cases} \tag{6.76}$$

We simplify based on the residue class of D modulo 4. For $D \equiv 1 \pmod 4$, (6.76) simplifies to

$$2^{n+\frac{\delta}{2}-1}\begin{cases} 0 & \text{if } \omega+3\le\delta \\ 1 & \text{if } \delta\le n-1\le\omega \text{ or } \delta=\omega+1=n \\ 1+(-1)^{\frac{A-K}{2}}\left(\frac{2}{D}\right) & \text{if } \delta\le\omega\le n-2 \text{ or } \delta=\omega+1\le n-1. \end{cases} \tag{6.77}$$

Otherwise, for $D \equiv 3 \pmod 4$, (6.76) reduces to

$$2^{n+\frac{\delta}{2}-1}\begin{cases} 0 & \text{if } \omega+1 \leq \delta \\ \left(\frac{\omega-\delta+1}{2}\right)\left(1+\left(\frac{2}{D}\right)\right) & \text{if } \delta \leq \omega \leq n-1 \\ 1+P_D(\delta,n) & \text{if } \delta \leq n \leq \omega. \end{cases} \tag{6.78}$$

Finally, for $\delta \equiv \omega \equiv 1 \pmod 2$, from (6.61), (6.69) and (6.74), $N_{2^n}(a,b,c;k)$ is given by

$$2^{n+\frac{\delta-3}{2}}\begin{cases} 0 & \text{if } \omega+3 < \delta \\ 1+\left(\frac{2}{AKD}\right)(-1)^{\left(\frac{A-K}{2}\right)\left(\frac{D+1}{2}\right)} & \text{if } \delta < \omega+3 \leq n \\ 1 & \text{if } \omega+3 > n. \end{cases} \tag{6.79}$$

We see that (6.77), (6.78) and (6.79) agree with the statement of the theorem. □

Theorem 6.12 (Case V). *Let $\alpha = 1$, $\delta \geq 4$ and either $\delta = n+1$ or $\delta = n+2$. Then $N_{2^n}(a,b,c;k)$ is given according to the following cases.*

If $\delta = n+1$ and $\omega \equiv 0 \pmod 2$,

$$N_{2^n}(a,b,c;k) = 2^n\begin{cases} 2\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = 0, n = 2 \\ 2 & \text{if } \omega = 2, n = 2 \\ 2^{\left[\frac{n-1}{2}\right]} & \text{if } \omega \geq n-1 \geq 2 \\ 2^{\frac{n-2}{2}} & \text{if } \omega = n-2 \geq 2 \\ 2^{\frac{n-1}{2}}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = n-3 \geq 0 \\ 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } 0 \leq \omega \leq n-4. \end{cases}$$

If $\delta = n+2$ *and* $\omega \equiv 0 \pmod 2$,

$$N_{2^n}(a,b,c;k) = 2^n \begin{cases} 2^{\frac{n}{2}} & \text{if } \omega = n \geq 2 \\ 2^{\frac{n-1}{2}} & \text{if } \omega = n-1 \geq 2 \\ 2^{\frac{n}{2}} \mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = n-2 \geq 0 \\ 2^{\frac{\omega}{2}+1} \mathbb{O}(\frac{A-K}{2}) \left(1 + \left(\frac{2}{AK}\right)\right) & \text{if } 0 \leq \omega \leq n-3. \end{cases}$$

If $\delta = n+1$ *and* $\omega \equiv 1 \pmod 2$,

$$N_{2^n}(a,b,c;k) = 2^n \begin{cases} 2^{\left[\frac{n-1}{2}\right]} & \text{if } 3 \leq n-1 \leq \omega \\ 0 & \text{if } \omega \leq n-2. \end{cases}$$

If $\delta = n+2$ *and* $\omega \equiv 1 \pmod 2$,

$$N_{2^n}(a,b,c;k) = 2^n \begin{cases} 2^{\left[\frac{n-1}{2}\right]} & \text{if } \omega = n \\ 0 & \text{if } \omega \leq n-1. \end{cases}$$

Proof. From (6.53), we have that

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \frac{E(2)}{4} + \sum_{t=3}^{\delta-2} \frac{E(t)}{2^t} \right\}. \tag{6.80}$$

From the proof of Theorem 6.11, we see that the bracketed expression of (6.80) is given by (6.65) and (6.66). We proceed by considering the parity of ω and by specifying the value of δ. First suppose $n = 2$. Then $\delta - 2 < 3$ regardless, and from (6.80) we have

$$N_{2^2}(a,b,c;k) = 2^2 \left\{ 1 + \frac{E(2)}{4} \right\} = \begin{cases} 2^3 \mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = 0 \\ 0 & \text{if } \omega = 1 \\ 2^3 & \text{if } \omega = 2. \end{cases} \tag{6.81}$$

Thus, we may assume $n \geq 3$ for the remaining cases. If $\delta = n+1$ and ω is even, from (6.66) and (6.80), $N_{2^n}(a,b,c;k)$ is given by

$$2^n \begin{cases} 2^{\left[\frac{n-1}{2}\right]} & \text{if } \omega \geq n-1 \geq 2 \\ 2^{\frac{n-2}{2}} & \text{if } \omega = n-2 \geq 2 \\ 2^{\frac{n+1}{2}-1}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega = n-3 \geq 0 \\ 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } 0 \leq \omega \leq n-4. \end{cases} \tag{6.82}$$

Combining (6.81) and (6.82) will yield the statement of the theorem in this case. Otherwise, for ω odd, from (6.65) we deduce that

$$N_{2^n}(a,b,c;k) = 2^n \begin{cases} 2^{\left[\frac{n-1}{2}\right]} & \text{if } 3 \leq n-1 \leq \omega \\ 0 & \text{if } \omega \leq n-2. \end{cases} \tag{6.83}$$

Now suppose that $\delta = n+2$. By (6.66) and (6.80), if $\delta = n+2$ and ω is even, $N_{2^n}(a,b,c;k)$ is given by

$$2^n \begin{cases} 2^{\left[\frac{n}{2}\right]} & \text{if } \omega = n \geq 3 \\ 2^{\frac{n-1}{2}} & \text{if } \omega + 1 = n \\ 2^{\frac{n}{2}}\mathbb{O}(\frac{A-K}{2}) & \text{if } \omega + 2 = n \\ 2^{\frac{\omega}{2}+1}\mathbb{O}(\frac{A-K}{2})\left(1+\left(\frac{2}{AK}\right)\right) & \text{if } \omega + 3 \leq n. \end{cases} \tag{6.84}$$

We combine (6.81) and (6.84) to arrive at the statement of the theorem in this case. Otherwise, for ω odd, with (6.81) and (6.65), $N_{2^n}(a,b,c;k)$ is given by

$$2^n \begin{cases} 2^{\left[\frac{n-1}{2}\right]} & \text{if } \omega = n \\ 0 & \text{if } \omega \leq n-1. \end{cases} \tag{6.85}$$

□

It now remains to consider the cases when $\alpha > 1$. Recall that we must have $\delta = 0$ in this case. We consider $N_{2^n}(a, b, c; k)$ under the cases

(VI) $1 < \alpha < n$,

(VII) $1 < \alpha = n$.

By (6.34), we see our cases are given by the following sums.

Case VI: $1 < \alpha < n$**;**

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \sum_{t=1}^{\alpha} \frac{1}{2^t} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right) + \sum_{t=\alpha+1}^{n} \frac{F(t)}{2^{2t+2}} \right\}. \tag{6.86}$$

Case VII: $\alpha = n > 1$**;**

$$N_{2^n}(a,b,c;k) = 2^n \left\{ 1 + \sum_{t=1}^{n} \frac{1}{2^t} \sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right) \right\}. \tag{6.87}$$

Theorem 6.13 (Case VI). *Let $1 < \alpha < n$. Then $N_{2^n}(a, b, c; k)$ is given according to the following cases.*

If $D \equiv 1 \pmod 4$,

$$N_{2^n}(a,b,c;k) = 2^{n-1} \begin{cases} \omega + 1 & \text{if } \omega + 2 \le \alpha \\ \alpha + (-1)^{\frac{A-K}{2}} & \text{if } \omega + 1 = \alpha \le n-1 \\ \alpha + 2 & \text{if } \omega = \alpha = n-1 \\ \alpha + 2 + (-1)^{\frac{A-K}{2}} \left(\frac{2}{D}\right) & \text{if } \omega = \alpha \le n-2 \\ \alpha + 2 & \text{if } \alpha + 1 \le n-1 \le \omega \\ \alpha + 2 + (-1)^{\frac{A-K}{2}} \left(\frac{2}{D}\right)^{\omega+\alpha+1} & \text{if } \alpha + 1 \le \omega \le n-2. \end{cases}$$

If $D \equiv 3 \pmod 4$,

$$N_{2^n}(a,b,c;k) = 2^{n-1} \begin{cases} \omega + 1 & \text{if } \omega + 2 \leq \alpha \\ \omega + 1 & \text{if } \omega + 1 = \alpha \leq n-1 \\ \alpha + 1 & \text{if } \omega = \alpha \leq n-1 \\ \alpha + 2 + \left(\frac{2}{D}\right)^{\alpha+1} P_D(\alpha_1, n) & \text{if } \alpha + 1 \leq n \leq \omega \\ \alpha + 2 + \left(\frac{2}{D}\right)^{\alpha+1} \left(P_D(\alpha+1,\omega) - \left(\frac{2}{D}\right)^{\omega+1}\right) & \text{if } \alpha + 1 \leq \omega \leq n-1. \end{cases}$$

Proof. From Proposition 6.12, we have that

$$1 + \sum_{t=1}^{\alpha} \frac{1}{2^t} \sum_{\substack{S < 2^t \\ S \equiv 1 \pmod 2}} e\left(\frac{-2^\omega KS}{2^t}\right) = \begin{cases} \frac{\alpha}{2} + 1 & \text{if } \omega \geq \alpha \\ \frac{\omega+1}{2} & \text{if } \omega \leq \alpha - 1. \end{cases} \tag{6.88}$$

Subsequently, as $\alpha + 1 \geq 3$, from Proposition 6.10 and Definition 6.7, we have that

$$\sum_{t=\alpha+1}^{n} \frac{F(t)}{2^{2t+2}} = \begin{cases} 0 & \text{if } \omega + 3 < \alpha + 1 \\ \dfrac{F(\omega+3)}{2^{2t+2}} & \text{if } \omega + 3 = \alpha + 1 \\ \dfrac{F(\omega+2)}{2^{2t+2}} & \text{if } \omega + 2 = \alpha + 1 = n \\ T_1(\omega, 0) & \text{if } \omega + 2 = \alpha + 1 \leq n - 1 \\ \dfrac{F(\omega+1)}{2^{2t+2}} & \text{if } \omega + 1 = \alpha + 1 = n \\ T_2(\omega, 0) & \text{if } \omega + 1 = \alpha + 1 = n - 1 \\ T_3(\omega, 0) & \text{if } \omega + 1 = \alpha + 1 \leq n - 2 \\ \displaystyle\sum_{t=\alpha+1}^{n} \frac{F(t)}{2^{2t+2}} & \text{if } \alpha + 1 \leq n \leq \omega \\ \displaystyle\sum_{t=\alpha+1}^{n} \frac{F(t)}{2^{2t+2}} + \frac{F(\omega+1)}{2^{2t+2}} & \text{if } \alpha + 1 \leq \omega = n - 1 \\ \displaystyle\sum_{t=\alpha+1}^{n} \frac{F(t)}{2^{2t+2}} + T_2(\omega, 0) & \text{if } \alpha + 1 \leq \omega = n - 2 \\ \displaystyle\sum_{t=\alpha+1}^{n} \frac{F(t)}{2^{2t+2}} + T_3(\omega, 0) & \text{if } \alpha + 1 \leq \omega \leq n - 3. \end{cases} \tag{6.89}$$

Hence, from Corollaries 6.6, 6.7 and 6.8, and as $\delta = 0$, (6.89) simplifies to

$$\frac{1}{2}\left(\frac{2}{D}\right)^{\alpha+1}\begin{cases} 0 & \text{if } \omega+3 \le \alpha+1 \\ (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega} & \text{if } \omega+2=\alpha+1\le n \\ -\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{\omega+1} & \text{if } \omega+1=\alpha+1=n \\ (-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega}-\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{\omega+1} & \text{if } \omega+1=\alpha+1\le n-1 \\ P_D(\alpha+1,n)\mathbb{O}(\frac{D+1}{2}) & \text{if } \alpha+1\le n\le\omega \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(\alpha+1,\omega)-\left(\frac{2}{D}\right)^{\omega+1}\right) & \text{if } \alpha+1\le\omega=n-1 \\ \mathbb{O}(\frac{D+1}{2})\left(P_D(\alpha+1,\omega)-\left(\frac{2}{D}\right)^{\omega+1}\right) & \\ \quad +(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega} & \text{if } \alpha+1\le\omega\le n-2. \end{cases} \tag{6.90}$$

Thus, with (6.86), (6.88) and (6.90), we have that $N_{2^n}(a,b,c;k)$ is given by

$$2^{n-1}\begin{cases} \omega+1 & \text{if } \omega+2\le\alpha \\ \omega+1+(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha+1} & \text{if } \omega+1=\alpha\le n-1 \\ \alpha+2-\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha} & \text{if } \omega=\alpha=n-1 \\ \alpha+2+(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha+1}-\mathbb{O}(\frac{D+1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha} & \text{if } \omega=\alpha\le n-2 \\ \alpha+2+\left(\frac{2}{D}\right)^{\alpha+1}\mathbb{O}(\frac{D+1}{2})P_D(\alpha+1,n) & \text{if } \alpha+1\le n\le\omega \\ \alpha+2+\left(\frac{2}{D}\right)^{\alpha+1}\mathbb{O}(\frac{D+1}{2})\left(P_D(\alpha+1,\omega)-\left(\frac{2}{D}\right)^{\omega+1}\right) & \text{if } \alpha+1\le\omega=n-1 \\ \alpha+2+\left(\frac{2}{D}\right)^{\alpha+1}\mathbb{O}(\frac{D+1}{2})\left(P_D(\alpha+1,\omega)-\left(\frac{2}{D}\right)^{\omega+1}\right) & \\ \quad +(-1)^{\frac{A-K}{2}}\mathbb{O}(\frac{D-1}{2})\left(\frac{2}{D}\right)^{\omega+\alpha+1} & \text{if } \alpha+1\le\omega\le n-2. \end{cases} \tag{6.91}$$

By simplifying (6.91) according to the residue class of D modulo 4, we arrive at the statement of the theorem.

□

Theorem 6.14 (**Case VII**). *Suppose* $\alpha = n \geq 2$. *Then*

$$N_{2^n}(a,b,c;k) = 2^{n-1}\begin{cases} n+2 & \text{if } \omega \geq n \\ \omega+1 & \text{if } \omega \leq n-1. \end{cases}$$

Proof. Similar to the proof of Theorem 6.13, from Proposition 6.12, we see that

$$1+\sum_{t=1}^{n}\frac{1}{2^t}\sum_{\substack{S<2^t \\ S\equiv 1 \pmod 2}} e\left(\frac{-2^{\omega}KS}{2^t}\right) = \begin{cases} \frac{n}{2}+1 & \text{if } \omega \geq n \\ \frac{\omega+1}{2} & \text{if } \omega \leq n-1. \end{cases} \tag{6.92}$$

Hence, by (6.87) and (6.92), we deduce that

$$N_{2^n}(a,b,c;k) = 2^{n-1}\begin{cases} n+2 & \text{if } \omega \geq n \\ \omega+1 & \text{if } \omega \leq n-1. \end{cases}$$

□

Chapter 7

Conclusion

7.1 Future Reseach

For the sake of discussion, for this chapter we let Q_r be a non-singular r-dimensional integral quadratic form. We recall the notation introduced in Chapter 4, where M denotes the $r \times r$ symmetric integral matrix associated with Q_r, and m_i denotes the i^{th} leading principal minor of M, for $i = 1, \ldots, r$. Let $q \in \mathbb{N}$ be an arbitrary integer, and let $S \in \mathbb{Z}$ be co-prime to q. We may use the methods developed to evaluate $G(Q_r; S; q)$. As Q_r is non-singular, we can follow the steps leading up to Theorem 4.3 to deduce the equation

$$Q_r = \sum_{i=1}^{r} \frac{y_i^2}{2m_{i-1}m_i}.$$

For this discussion we set $\Delta = \prod_{i=1}^{r} m_i$. If q is odd and $(\Delta, q) = 1$ it follows that

$$\begin{aligned} G(Q_r; S; q) &= \sum_{x_1,\ldots,x_n=0}^{q-1} e\left(\frac{S}{q}\sum_{i=1}^{r}(2m_{i-1}m_i)^{-1}y_i^2\right) = \prod_{i=1}^{r} G(2Sm_{i-1}m_i; q) \\ &= \left(\frac{2S}{q}\right)^r \left(\frac{m_r}{q}\right) G(1; q)^r. \end{aligned}$$

Note that as $2^r \mid m_r$, the formula above agrees with the results of Weber [22, p. 14], [111, p. 23], when $S = 1$.

As the quadratic Gauss sum possesses certain multiplicative properties, we can deduce some multiplicative properties of $G(Q_r; S; q)$. Suppose $q = p_1p_2$ for two odd, distinct primes and $(\Delta, p_1p_2) = 1$. Then by Proposition 3.1, we have

$$G(2Sm_{i-1}m_i; p_1p_2) = G(2sm_{i-1}m_ip_1; p_2)G(2sm_{i-1}m_ip_2; p_1).$$

This means,

$$G(Q_r; S; p_1p_2) = \prod_{i=1}^{r} G(2sm_{i-1}m_ip_1; p_2)G(2sm_{i-1}m_ip_2; p_1) = G(Q_r; p_1S; p_2)G(Q_r; p_2S; p_1).$$

Suppose now that $q = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, for distinct odd primes $p_1, \ldots, p_n$ and positive integers $\alpha_1, \ldots, \alpha_n$. Set $P_i = \dfrac{q}{p_i^{\alpha_i}}$ for $i = 1, \ldots, n$. By similar reasoning to the above, if $(\Delta, q) = 1$, we can deduce that

$$G(Q_r; S; q) = \prod_{i=1}^{n} G(Q_r; P_iS; p_i^{\alpha_i}).$$

This shows we can describe $G(Q_r; S; q)$ for all odd positive integers q, provided that $(\Delta, q) = 1$.

Evaluating $G(Q_r; S; 2^\sigma q)$, for $\sigma \in \mathbb{N}$ will require more study. Even given favorable divisibility properties, there will be a factor of 2 which prevents the use of Proposition 3.1. Suppose for the moment that $m_i = 2^i m_i'$ for $i = 1, \ldots, r$ and m_i' coprime to q. Then by Corollaries 5.3 and 5.4, and with Proposition 3.12, we have

$$\begin{aligned} G(Q_r; qS; 2^\sigma)G(Q_r; 2^\sigma S; q) &= \prod_{i=1}^{r} G(qSm_i'm_{i-1}'; 2^\sigma)G(2^\sigma Sm_im_{i-1}; q) \\ &= \prod_{i=1}^{r} \frac{1}{2^{i+1}} G(qSm_i'm_{i-1}'; 2^{\sigma+2i+2})G(2^\sigma Sm_im_{i-1}; q) \\ &= \prod_{i=1}^{r} \frac{1}{2^{i+1}} G(2qSm_im_{i-1}; 2^\sigma)G(2^\sigma Sm_im_{i-1}; q). \end{aligned}$$

However, this suggests that similar multiplicative properties exist for the quadratic form

Gauss sum with even modulus, up to a factor of a power of 2. The challenge when evaluating $G(Q_r; S; 2^\sigma q)$ is in detecting those cases where the modulus is congruent to 2 (mod 4). Because of this difficulty, one must consider various cases in the evaluation of $G(Q_r; S; 2^\sigma q)$. These results seem attainable, but still require further study. We add that a translation of the papers of Weber [111] and Jordan [61] into English would be very valuable with regards to this question.

Extending our main results is the most obvious next step. However, we mention that in the development of $G(Q_r; S; p^n)$, we did not use any particularly noteworthy theorems pertaining to quadratic forms. Our diagonalization of Q_r needed only the existence of an LDL^T decomposition. The decomposition itself used basic linear algebra. In particular, we did not use the idea of equivalent quadratic forms.

Roughly speaking, two quadratic forms Q_r and Q'_r are equivalent if one is obtained from the other by a linear, invertible change of variables over $\mathbb{Z}$. One can show that equivalent forms represent the same integers. Assume for the sake of discussion that p is an odd prime and $m_i = p^{\alpha_i} A_i$. If we are to consider our original diagonalization, it is of the form

$$\begin{aligned} Q_r(x_1, \ldots, x_r) &= \sum_{i=1}^{r} \frac{m_i X_i^2}{2m_{i-1}} = Q'_r(X_1, \ldots, X_r) \\ \rightarrow p^\alpha Q_r &\equiv \sum_{i=1}^{r} 2A_i A_{i-1} p^{\alpha+\alpha_i-\alpha_{i-1}} X_i^2 \pmod{p^{n+\alpha}}. \end{aligned}$$

If the forms Q_r and Q'_r are equivalent, one can show that as x_i runs over a complete residue system, so does X_i and hence it is immediate that

$$G(Q_r; S; p^n) = \frac{1}{p^{r\alpha}} \prod_{i=1}^{r} G(2SA_iA_{i-1}p^{\alpha+\alpha_r-\alpha_{r-1}}; p^{n+\alpha}).$$

Observe that the change of variables $x_i \mapsto X_i$ is described by the i^{th} row of L. Hence, L describes the change of variables from Q_r to Q'_r, and this map is invertible over $\mathbb{Z}$. However, as we are evaluating Q_r modulo $p^{n+\alpha}$, we must have Q_r and Q'_r equivalent over $\mathbb{Z}_{p^{n+\alpha}}$, which

means we must have L invertible over $\mathbb{Z}_{p^{n+\alpha}}$. This is equivalent to $(\Delta, p) = 1$ or $p^{\alpha_i} \mid m_{ij}$ for all $i < j$. These conditions are given in Corollary 5.3 and Theorem 5.7, respectively. We have similar conclusions for p even. Due to the vastness of the field, one might be able to use various ideas from the theory of quadratic forms to extend this approach.

Our approach when the minors of Q_r were divisible by p, was to consider Gauss sums of the form

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{p^m}}}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right), \tag{7.1}$$

for $n \geq 2m$. These restrictions will necessitate the size restrictions on n in the statement of Theorems 5.9 and 5.10. For this reason, we would like to study these Gauss sums for small n. For example, consider the sum in (7.1) for $m \in \mathbb{N}$ satisfying $m < n < 2m$, and $w \in \mathbb{Z}$. It can be shown that

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{p^m}}}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right) = \frac{G(S;p^n)}{p^m} \sum_{y=0}^{p^m-1} e\left(\frac{-p^{n-m}ST^2y^2 - wy}{p^m}\right), \tag{7.2}$$

where T is an integer such that $2ST \equiv 1 \pmod{p^n}$. Hence, if $w \equiv 0 \pmod{p^m}$, (7.1) will reduce to

$$\begin{aligned}\frac{1}{p^m} G(S;p^n)G(-St^2p^{n-m};p^m) &= \frac{p^{n-m}}{p^m} G(S;p^n)G(-S;p^{2m-n}) \\ &= \frac{p^{n-m}}{p^m} \left(\frac{S}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{n}{2}} \left(\frac{-S}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{\frac{2m-n}{2}} = p^{n-m}.\end{aligned}$$

Thus, we deduce that

$$\sum_{\substack{x=0 \\ x \equiv 0 \pmod{p^m}}}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right) = \begin{cases} 1 & \text{if } m \geq n \\ p^{n-m} & \text{if } m < n < 2m \cdot \\ G(S;p^n) & \text{if } 2m \leq n. \end{cases} \tag{7.3}$$

For arbitrary w, the evaluation of (7.2) will mean considering sums of the form

$$\sum_{x=0}^{p^n-1} e\left(\frac{x^2+x}{p^n}\right).$$

For p odd, we have

$$\sum_{x=0}^{p^n-1} e\left(\frac{x^2+x}{p^n}\right) = e\left(\frac{-1}{4p^n}\right)\sum_{x=0}^{p^n-1} e\left(\frac{(x-2^{-1})^2}{p^n}\right) = e\left(\frac{-1}{4p^n}\right) G(1;p^n).$$

Preliminary research suggests that the sum indexed by y in (7.2) will be of the form

$$\epsilon\left(S,w,p^n\right) G(1;p^n), \text{ where } |\epsilon\left(\cdot\right)| = 1;$$

see [49], [92]. Hence, (7.1) will behave similarly to the quadratic Gauss sum, with a root of unity as a factor. As such, further investigation is required. Additionally, similar study is needed for sums of the form $\sum_{\substack{x=0 \\ x\equiv w \pmod{2^m}}}^{2^n-1} e\left(\frac{Sx^2}{2^n}\right)$.

7.2 Possible Applications of the Quadratic Form Gauss Sum

In light of Chapter 6, it's clear that one may use the quadratic form Gauss sum to determine the number of solutions to a congruence of the form

$$Q_r \equiv k \pmod{p^n}, \tag{7.4}$$

given that Q_r satisfies certain conditions with respect to p^n. Similar to Theorem 6.1, one can show that the number of solutions to the congruence given in (7.4) is given by

$$p^{(r-1)n}\left\{1+\sum_{t=1}^{n}\frac{1}{p^{rt}}\sum_{\substack{S<p^t\\(S,p)=1}}e\left(\frac{-kS}{p^t}\right)G(Q_r;S;p^t)\right\}. \tag{7.5}$$

If we suppose for convenience that p is an odd prime, r is even and $k\equiv 0 \pmod{p^n}$, then by Corollary 5.5, we deduce that (7.5) can be written as

$$p^{(r-1)n-1}\left\{p+(p-1)\sum_{t=1}^{n}\left(\frac{-\Delta}{p}\right)^t p^{t\left(1-\frac{r}{2}\right)}\right\}. \tag{7.6}$$

The sum $\displaystyle\sum_{t=1}^{n}\left(\frac{-\Delta}{p}\right)^t p^{t\left(1-\frac{r}{2}\right)}$ will be straightforward to evaluate, similar to Definition 6.2. Hence, the expression in (7.6) is a tractable expression to determine the number of solutions to $Q_r\equiv 0 \pmod{p^n}$. Current research is directed towards estimates of the number of such solutions within a certain range; see, e.g. [20], [50], [51]. One might be able to use these results along with symmetric arguments to achieve similar results.

We turn now to more abstract applications. As mentioned in the introduction, the quadratic Gauss sum is a generalization of a particular exponential sum. We present the following definition to highlight some different types of Gauss sums. For what follows, let $q\in\mathbb{N}$ be a positive integer, and $S\in\mathbb{Z}$ is coprime to q.

Definition 7.1. Let χ be a Dirichlet character defined on $\mathbb{Z}_q$ (see, e.g. [5, p. 138]). Then we define the Gauss character sum by

$$G_\chi(S;q)=\sum_{x=0}^{q-1}\chi(x)e\left(\frac{Sx}{q}\right).$$

Suppose for q odd, we let χ denote a quadratic character modulo q. Then it can be shown

that

$$G_\chi(S;q) = \sum_{\substack{x=0 \\ (x,q)=1}}^{q-1} \chi(x) e\left(\frac{Sx}{q}\right) = \sum_{x=0}^{q-1} e\left(\frac{Sx^2}{q}\right) = G(S;q).$$

This is shown for q an odd prime in Proposition 6.1. Thus, a Gauss character sum can be seen as a generalization of the quadratic Gauss sum. One can view the exponential term with modulus q of $G_\chi(S;q)$ as an additive character. In this fashion, the Gauss character sum is related to both multiplicative and additive number theory. In particular, Gauss character sums are of great interest due to their connections with Dirichlet L-functions; see, e.g. [5, pp. 262-263].

Definition 7.2. Let $q = p^n$ be a prime power, and let χ be a multiplicative character defined on $\mathbb{F}_q$ (see, e.g. [78, p. 191]) and let $\sigma \in \mathbb{F}_q$. The finite field Gauss sum with respect to χ is given by

$$\mathbb{G}_\chi(\sigma;q) = \sum_{x \in \mathbb{F}_q} \chi(x) e\left(\frac{T(\sigma x)}{p}\right),$$

where T is the field trace from $\mathbb{F}_q$ onto $\mathbb{F}_p$ and the character χ has been extended to all of $\mathbb{F}_q$ by setting

$$\chi(0) = \begin{cases} 1 & \text{if } \chi \text{ is trivial,} \\ 0 & \text{otherwise.} \end{cases}$$

Similarly, for $q = p^n$, for a positive integer m and $\sigma \in \mathbb{F}_q$, the sum given by

$$\mathbb{G}_m(\sigma;q) = \sum_{x \in \mathbb{F}_q} e\left(\frac{T(\sigma x^m)}{p}\right)$$

is called an m^{th} power Gauss sum over the finite field $\mathbb{F}_q$.

We emphasize that we use the terms principal character and trivial character interchangeably. These two finite field Gauss sums are related by the formula

$$G_m(\sigma, q) = \sum_{j=1}^{m-1} \mathbb{G}_{\chi^j}(\sigma; q),$$

where χ is a character of order m on $\mathbb{F}_q$ and $\sigma \in \mathbb{F}_q^*$ [12, p. 11]. Moreover, the finite field character sum and the Gauss character sum are equivalent in a certain case. When $q = p$ is an odd prime, the trace function on $\mathbb{F}_q$ will be the identity map. Thus, for χ a non-trivial character, we have that

$$\mathbb{G}_\chi(\sigma; p) = \sum_{x \in \mathbb{F}_p} \chi(x) e\left(\frac{\sigma x}{p}\right) = G_\chi(\sigma; p).$$

Given these generalizations of the quadratic Gauss sum, one naturally wonders if such generalizations exist for the quadratic form Gauss sum. As it happens, such a generalization will be difficult to obtain. The Gauss character sum has, as summand, the product of an additive character and a multiplicative character. When the multiplicative character is quadratic, the Gauss character sum will simplify to a sum of additive characters. This simplification will not hold in general for an arbitrary character χ of order greater than 2. Indeed, the product of two Gauss character sums is difficult to evaluate. If χ and ψ are two characters modulo q, then

$$G_\chi(1; q) \cdot G_\psi(1; q) = \sum_{x \in \mathbb{Z}_q^*} \chi(x) e\left(\frac{x}{q}\right) \sum_{y \in \mathbb{Z}_q^*} \psi(y) e\left(\frac{y}{q}\right) = \sum_{x,y \in \mathbb{Z}_q^*} \chi(x)\psi(y) e\left(\frac{x+y}{q}\right). \quad (7.7)$$

Suppose that Q_2 is a binary quadratic form such that m_1 and m_2 are coprime to $q = p^n$. Then for p odd we have

$$G(Q_2; S; q) = G(2Sm_1; q)G(2Sm_1m_2; q).$$

We may consider a product of Gauss character sums with similar coefficients. For χ and ψ modulo q, we have

$$\begin{aligned} G_\chi(2Sm_1;q)G_\psi(2Sm_1m_2;q) &= \sum_{x\in\mathbb{Z}_q^*}\chi(x)e\left(\frac{2Sm_1x}{q}\right)\sum_{y\in\mathbb{Z}_q*}\psi(y)e\left(\frac{2Sm_1m_2y}{q}\right) \\ &= \sum_{x,y\in\mathbb{Z}_q^*}\chi((2Sm_1)^{-1}x)\psi((2Sm_1m_2)^{-1}y)e\left(\frac{x+y}{q}\right) \\ &= \chi\psi((2Sm_1)^{-1})\psi(m_2^{-1})\sum_{x,y\in\mathbb{Z}_q*}\chi(x)\psi(y)e\left(\frac{x+y}{q}\right), \end{aligned}$$

where we have used the fact that $G_\chi(S;q) = \chi^{-1}(S)G(1;q)$. Hence, evaluating the product of the Gauss character sum will require studying sums of the form seen in (7.7).

There is current research containing products of Gauss character sums where an exact formula would be valuable. Consider the generalized Gauss character sum, for $k \in \mathbb{N}$, given by

$$G_k(S,\chi;q) = \sum_{x=0}^{q-1}\chi(x)e\left(\frac{Sx^k}{q}\right),$$

where χ is a Dirichlet character modulo q. Historically, research efforts have been focused on determining upper bounds for $|G_k(S,\chi;q)|$. Famously, A. Weil [112] showed that for p an odd prime,

$$|G_k(S,\chi;p)| \leq \overline{S}p^{\frac{1}{2}},$$

where $\overline{S}$ denotes the positive integer residue of S modulo p. More recently, Cochrane and Zheng [21] have shown that for any positive integer $q \geq 3$ and $(S,q) = 1$, we have

$$|G_k(S,\chi;q)| \leq (4k)^{\omega(q)}q^{1-\frac{1}{k+1}}, \tag{7.8}$$

where $\omega(q)$ denotes the number of distinct prime divisors of q.

Current research has focused on exact formulas for the $2m^{th}$ power mean of the generalized Gauss character sum, given by

$$\sum_{\chi \mod q} |G_k(S, \chi; q)|^{2m}. \tag{7.9}$$

Determining an exact expression for (7.9) was first investigated by Zhang [121], in 2002. Zhang determined exact expressions for

$$\sum_{\chi \mod p} |G_2(S, \chi; p)|^4 \quad \text{and} \quad \sum_{\chi \mod p} |G_2(S, \chi; p)|^6,$$

where p is an odd prime. These expressions determined by Zhang arose as a byproduct of his investigation into sums of the form given in (7.9) weighted by Dirichlet L-functions [121, pp. 305-306]. Subsequently, in 2005, W. Zhang and H. Liu [124] investigated the sum (7.9) directly. They determined exact expressions for $\sum_{\chi \mod p} |G_3(S, \chi; p)|^4$ for $p \equiv 1 \pmod 3$, and $\sum_{\chi \mod q} |G_k(S, \chi; q)|^4$, for $q \geq 3$ a square-full number, and $(Sk, q) = 1$. In 2009, Yuan He and Q. Liao [56] determined formulas for $\sum_{\chi \mod p} |G_2(S, \chi; p)|^6$ and $\sum_{\chi \mod p} |G_2(S, \chi; p)|^8$. In a similar vein, in 2011, Yanfeng He and W. Zhang [55] have determined formulas for $\sum_{\chi \mod q} |G_2(S, \chi; q)|^6$ and $\sum_{\chi \mod q} |G_2(S, \chi; q)|^8$, where q is a square-full number and $(S, q) = 1$. Most recently, in 2012, F. Liu and Q. H. Yang [79] have shown that

$$\sum_{\chi \mod q} |G_2(S, \chi; q)|^{2m} = 4^{(m-1)\omega(q)} q^{m-1} \phi^2(q), \tag{7.10}$$

for $q \geq 2$ odd and square-full. This formula can be compared with the upper bound of Cochrane and Zheng given in (7.8).

We emphasize that these results take advantage of the property

$$|G_k(S, \chi; q)|^2 = G_k(S, \chi; q)\overline{G_k(S, \chi; q)}.$$

Thus, this research is preoccupied with the product of Gauss character sums. Given an exact formula for a product of such sums, one might be able to deduce a formula for

$$\sum_{\chi \mod q} |G_k(S, \chi; q)|^{2m}.$$

Given that a majority of efforts have been to find upper bounds of $G_k(S, \chi; q)$, this is likely a very difficult problem. The current use of these $2m^{th}$ power mean formulas is to determine asymptotic formula for weighted sums, mostly involving L-fuctions; see, e.g., [81], [94], [118], [120], [122], [123]. Hence, such an exact formula would likely lead to improvements in these asymptotic formulas, and may yield interesting connections with the given weighted sum.

Our emphasis has been on the generalization of the quadratic form Gauss sum to an expression involving Gauss character sums. Both the quadratic Gauss sum and the Gauss character sum run over a ring of integers, which leads to the natural generalization question. However, one would also like to generalize the quadratic form Gauss sum to the finite field Gauss sum. Similar difficulties will exist with this generalization, as our Gauss sum is with respect to a multiplicative character χ. However, we would be interested in such a generalization, as there is a well known exponential sum which makes use of a product of finite field Gauss sums. Let q be a prime power and consider the so-called Jacobi sum, given by $\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\psi(1-\alpha)$ for characters χ, ψ defined on $\mathbb{F}_q$. It can be shown that if the character given by $\chi\psi$ is nontrivial, then

$$\sum_{\alpha \in \mathbb{F}_q} \chi(\alpha)\psi(1-\alpha) = \frac{\mathbb{G}_\chi(1;q)\mathbb{G}_\psi(1;q)}{\mathbb{G}_{\chi\psi}(1;q)},$$

see, e.g. [12, p. 59]. One notes that the restriction of $\chi\psi$ nontrivial, means the above equation will not hold for two quadratic characters. Thus, one would expect to generalize the Gauss character sum before attempting a similar generalization for the finite field case.

7.3 Current Applications

Finally, we mention briefly the usage of Gauss sums in the current literature. This list is not exhaustive, but serves to demonstrate the wide variety of applications of Gauss sums.

As mentioned in the previous section, the Gauss character sum has various connections with Dirichlet L-functions [4], [125]. As well, this Gauss sum can be used to estimate various character sums [33], [53], [58], [80], [108]; estimate the number of solutions for certain congruences [52], [109]; and has applications for the number of representations of an integer as a sum of primes [72].

The finite field Gauss sum has applications in many finite field problems. One sees their use in coding theory [37], [116]; point counting on elliptic curves [97], [117]; determining the number of solutions to polynomial equations [7], [95]; determining the value of cyclotomic numbers [114]; constructing difference sets [39]; and the evaluation of various related functions [85]. In particular, the finite field Gauss sums are widely used in the construction of Cayley graphs [38], [40], [43], [87], [88], [113], [115].

In addition, Gauss sums have been generalized over various algebraic structures, including various types of groups [46], [64], [76], [77] [82] ; rings [36], [105], [119]; and fields [14], [57], [84], [90]. Regardless of the generalization, the Gauss sum can be used for additive or multiplicative problems.

Due to the wide variety of Gauss sums, its generalizations and applications, it seems likely that the quadratic form Gauss sum will have other, unforseen applications. The quadratic Gauss sum possesses a very interesting structure, with many deep connections to other branches of mathematics. Due to the similarity in structure in the quadratic form Gauss sum, it is certain that this sum will contain many deep connections as well. As the results of Weber and Jordan have been forgotten over time, we hope to see further study of the quadratic form Gauss sum.

Bibliography

[1] A. Alaca, S. Alaca, and K. S. Williams. Double Gauss Sums. *Journal of Combinatorics and Number Theory*, 6(2):65–92, 2014.

[2] A. Alaca, S. Alaca, and K. S. Williams. Representation numbers of a certain quaternary quadratic forms in a genus consisting of a single class. *Preprint*, 2015.

[3] A. Alaca and K. S. Williams. On the quaternary forms $x^2+y^2+2z^2+3t^2$, $x^2+2y^2+2z^2+6t^2$, $x^2+3y^2+3z^2+6t^2$ and $2x^2+3y^2+6z^2+6t^2$. *International Journal of Number Theory*, 8(7):1661–1686, 2012.

[4] E Alkan. On linear combinations of special values of L-functions. *Manuscripta Mathematica*, 139:473–494, 2012.

[5] T. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, 1976.

[6] J. Araujo and L. Fernández. Contando con Sumas de Gauss. *Divulgaciones Matemáticas*, 12(2):171–180, 2004.

[7] R. Barman and G. Kalita. On the polynomial x^d+ax+b over $\mathbb{F}_q$ and Gaussian hypergeometric series. *International Journal of Number Theory*, 9(7):1753–1763, 2013.

[8] R. Bellman. *A Brief Introduction to Theta Functions*. Dover Publications, 1961.

[9] B. C. Berndt. On Gaussian sums and other exponential sums with periodic coefficients. *Duke Mathematical Journal*, 40:145–156, 1973.

[10] B. C. Berndt. What is a q-series? In *Ramanujan Rediscovered*, volume 14, pages 31–51. Ramanujan Math. Soc. Lec. Notes Ser., 2010.

[11] B. C. Berndt and R. J. Evans. The Determination of Gauss Sums. *Bulletin of the American Mathematical Society*, 5(2), 1981.

[12] B. C. Berndt, R. J. Evans, and K. S. Williams. *Gauss and Jacobi Sums*. John Wiley and Sons, Inc., 1998.

[13] B. C. Berndt and L. Schoenfeld. Periodic analogues of the Euler-Maclaurin and Poisson summation formulas with applications to number theory. *Acta Arithmetica*, 28(1):23–68, 1975.

[14] H. Boylan and N. Skoruppa. A quick proof of reciprocity for Hecke Gauss sums. *Journal of Number Theory*, 133:110–114, 2013.

[15] D. M. Bressoud. On the value of Gaussian sums. *Journal of Number Theory*, 13(1):88–94, 1981.

[16] L. Carlitz. A Note on Gauss' Sum. *Proceedings of the American Mathematical Society*, 7(5):910–911, 1966.

[17] B. Casselman. Dirichlet's calculation of Gauss sums. *L'Enseignement Mathématiques*, 57:281–301, 2011.

[18] A. Cauchy. Méthode simple et nouvelle pour la détermination complète des sommes alternées, formées avec les racines primitives des éequations binomes. *Comptes rendus hebdomadaires des sances de l'Acadmie des sciences*, 10:560–572, 1840.

[19] K. Chandrasekharan. *Elliptic Functions*. Springer-Verlag, 1985.

[20] T. Cochrane and A. H. Hakami. Small zeros of quadratic forms mod p^2. *Proc. Amer. M. Soc.*, 140(12):4041–4052, 2012.

[21] T. Cochrane and Z. Zheng. A Survey on Pure and Mixed Exponential Sums Modulo Prime Powers. In *Number Theory for the Millenium, I*, pages 273–300. A. K. Peters, 2000.

[22] E. Cohen. Rings of arithmetic functions. II: The number of solutions of quadratic congruences. *Duke Mathematical Journal*, 21(1):9–28, 1954.

[23] G. Danas. Note on the quadratic Gauss sums. *International Journal of Mathematics and Mathematical Sciences*, 25(3):167–173, 2001.

[24] H. Davenport. *Multiplicative Number Theory*. Springer-Verlag, Third edition, 2000.

[25] F. Deloup. A reciprocity formula for Gauss sums and invariants of 3-manifolds. *Comptes Rendus de l'Académie des Sciences. Series I*, 326(1):69–73, 1998.

[26] F. Deloup. Linking forms, reciprocity for Gauss sums and invariants of 3-manifolds. *Transactions of the American Mathematical Society*, 351(5):1895–1918, 1999.

[27] L. E. Dickson. *Modern Algebraic Theories*. Benj. H. Sanborn and Co., 1926.

[28] P. G. L. Dirichlet. Über eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen. *Abhandlungen der Köniiglich Preussischen Akademie der Wissenschaften*, pages 391–407, 1835.

[29] P. G. L. Dirichlet. Sur l'usage des intégrales définies dans la sommation des séries finies ou infinies. *Journal für die reine und angewandte Mathematik*, 17, 1837.

[30] P. G. L. Dirichlet. Recherches sure diverses applications de l'Analyse infinitésimale à la Théorie des Nombres. *Journal für die reine und angewandte Mathematik*, 21:1–12, 1840.

[31] P. G. L. Dirichlet. *Vorlesungen Über Zahlentheorie*. Friedrich Vieweg und Sohn, 1871. Edited and provided with additives from R. Dedekind.

[32] F. M. Dopico, C. R. Johnson, and J. M. Molera. Multiple LU Factorizations of a Singular Matrix. *Linear Algebra and its Applications*, 419(1):24–36, 2006.

[33] Y. Du and H Lui. On the mean value of the mixed exponential sums with Dirichlet characters and general Gauss sum. *Czechoslovak Mathematical Journal*, 63(2):461–473, 2013.

[34] M Eichler. *Introduction to the Theory of Algebraic Numbers and Functions*. Academic Press Inc., 1966.

[35] T. Estermann. On the sign of the Gaussian sum. *Journal of the London Mathematical Society*, 20:66–67, 1945.

[36] K. Feng, J. Li, and S. Zhu. The Gauss sums and Jacobi sums over Galois ring $GR(p^2, r)$. *Science China Mathematics*, 56(7):1457–1465, 2013.

[37] T. Feng and K. Momihara. Evaluation of the weight distribution of a class of cyclic codes based on index 2 Gauss sums. *IEEE Transactions on Information Theory*, 59(9):5980–5984, 2013.

[38] T. Feng, F. Wu, and Q. Xiang. Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes. *Designs, Codes and Cryptography*, 65:247–257, 2012.

[39] T. Feng and Q. Xiang. Cyclotomic constructions of skew Hadamard difference sets. *Journal of Combinatorial Theory, Series A*, 119:245–256, 2012.

[40] T. Feng and Q. Xiang. Strongly regular graphs from unions of cyclotomic classes. *Journal of Combinatorial Theory, Series B*, 102:982–995, 2012.

[41] C. F. Gauss. Summatio Quarumdam Serierum Singularium. *Societas Regia Scientiarum Gottingensis*, 1811.

[42] C. F. Gauss. *Mathematisches Tagebuch 1796-1814*. Ostwalds Klassiker der exakten Wissenschaften, 256. Akademische Verlagsgesellschaft Geest und Portig, Leipzig, 1976.

[43] G. Ge, Q. Xiang, and T. Yuan. Constructions of strongly regular Cayley graphs using index four Gauss sums. *Journal of Algebraic Combinatorics*, 37:313–329, 2013.

[44] A Genocchi. Sulla formula sommatoria di Eulero, e sulla teorica de'residui quadratici. *Ann. Sci. Mat. Fis. (Roma)*, 3:406–436, 1852.

[45] G Golub and C. F. Van Loan. *Matrix Computations*. Johns Hopkins University Press, 1983.

[46] Y. Gomi, T. Maeda, and K. Shinoda. Gauss Sums on Finite Groups. *Tokyo J. Math*, 35(1), 2012.

[47] D. Grant. The Quadratic Gauss Sum Redux. *The American Mathematical Monthly*, 121(2):145–149, 2014.

[48] S. Gurevich, R. Hadani, and R. Howe. Quadratic Reciprocity and the Sign of the Gauss Sum via the Finite Weil Representation. *International Mathematics Research Notices*, 2010(19):3729–3745, 2010.

[49] A. H. Hakami. Weighted Quadratic Partitions Modulo p^m a New Formula and a New Demonstration. *Tamkang Journal of Mathematics*, 43(1):11–19, 2012.

[50] A. H. Hakami. Estimates for lattice points of quadratic forms with integral coefficients modulo a prime number square. *Journal of Inequalities and Applications*, 2014, 2014. `http://journalofinequalitiesandapplications.springeropen.com/articles/10.1186/1029-242X-2014-290`.

[51] A. H. Hakami. Estimates for lattice points of quadratic forms with integral coefficients modulo a prime number square (ii). *Journal of Inequalities and Applications*, 2015, 2015. `http://journalofinequalitiesandapplications.springeropen.com/articles/10.1186/s13660-015-0637-0`.

[52] D. Han and J. Li. Some estimate of character sums and its applications. *Journal of Inequalities and Applications*, 2013, 2013. `http://www.journalofinequalitiesandapplications.com/content/2013/1/328`.

[53] D. Han and Y. Li. A sum analogous to the high-dimensional Kloosterman sums and its upper bound estimate. *Journal of Inequalities and Applications*, 2013(130), 2013. `http://www.journalofinequalitiesandapplications.com/content/2013/1/130`.

[54] G. H. Hardy. On the representation of a number as the sum of any number of squares, and in particular of five. *Transactions of the American Mathematical Society*, 21:255–284, 1920.

[55] Yanfeng He and W. Zhang. On the $2k^{th}$ power mean value of the generalized quadratic Gauss sums. *Bull. Korean Math. Soc.*, 48(1):9–15, 2011.

[56] Yuan He and Q. Liao. On an identity associated with Weil's estimate and its applications. *Journal of Number Theory*, 129:1075–1089, 2009.

[57] E. Hecke. Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. *Mathematische Zeitschrift*, 1:357–376, 1918.

[58] S. Jakubec. A connection between sums of binomial coefficients and Gross-Koblitz formula. *Mathematica Slovaca*, 62(1):13–16, 2012.

[59] C. Jordan. Sur les congruences du second degré. *Comptes Rendus*, 62, 1866.

[60] C. Jordan. *Traité des substitutions et des équations algébriques.* Gauthiers-Villars, Paris, 1870.

[61] C. Jordan. Sur les sommes de Gauss à plusieurs variables. *Comptes rendus hebdomadaires des séances de l'Académie des sciences*, 73:1316–1319, 1871.

[62] C. Jordan. Sur la forme canonique des congruences du second degré et le nombre de leurs solutions. *Journal de mathematiques pures et appliquees*, 17:368–402, 1872.

[63] C. Jordan. *Notice sur les travaux de M. Camille Jordan*. Gauthier-Villars, Paris, 1881.

[64] D. S. Kim. Codes Associated with $\mathcal{O}^+(2n, 2^r)$ and Power Moments of Kloosterman Sums. *Integers*, 12:237–257, 2012.

[65] A. Krazer. *Lehrbuch der Thetafunktionen*. B. G. Teubner, 1903.

[66] A. Krazer. Zur Theorie der mehrfachen Gaußschen Summen. In *Festschrift Heinrich Weber zu seinem siebzigsten Geburtstag am 5. März 1912*. AMS Chelsea Publishing, 1971.

[67] L. Kronecker. Sur une formule de Gauss. *Journal de mathématiques pures et appliquées, série 2*, 1:392–395, 1856.

[68] L. Kronecker. Über den bierten Gaußschen Beweis des Reziprozitätsgesetzes für die quadratischen Reste. *Königlische Akademie der Wissenschaften*, pages 686–698, 854–860, 1880.

[69] L. Kronecker. Summirung der Gausschen Reihen $\sum_{h=0}^{h=n-1} e^{\frac{2h^2\pi\imath}{n}}$. *Journal für die reine und angewandte Mathematik*, 105:267–268, 1889.

[70] L. Kronecker. Über die Dirichletsche Methode der Wertbestimmung der Gaußsschen Reihen. *Mitteilungen der Mathematischen Gesellschaft in Hamburg*, 2:32–36, 1890.

[71] E. Landau. *Elementary Number Theory*. AMS Chelsea Publishing, 1999.

[72] A. Languasco and A. Zaccagnini. Sums of many primes. *Journal of Number Theory*, 132:1265–1283, 2012.

[73] F. Lemmermeyer. Proofs of the Quadratic Reciprocity Law. `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html`. [Online; accessed 6-February-2016].

[74] F. Lemmermeyer. *Reciprocity laws: from Euler to Eisenstein*. Springer-Verlag, 2000.

[75] M. Lerch. Zur Theorie der Gaußschen Summen. *Mathiematische Annalen*, 57(4):554–567, 1903.

[76] M. Lewko, A. O'Neill, and A. Smith. Regularity of Lossy RSA on Subdomains and Its Applications. In *Lecture Notes in Computer Science*, volume 7881. Springer, Heidelberg, 2013.

[77] Y. Li and S. Hu. Gauss sums over some matrix groups. *Journal of Number Theory*, 132:2967–2976, 2012.

[78] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge University Press, 1997.

[79] F. Liu and Q. Yang. An identity on the $2m$-th power mean value of the generalized Gauss sums. *Bulletin of the Korean Mathematical Society*, 49(6):1327–1334, 2012.

[80] H. Liu and J. Gao. On the Gauss sums and generalized Bernoulli numbers. *Ukranian Mathematical Journal*, 64(6):971–978, 2012.

[81] H. Liu and X. Zhang. On the mean value of $\frac{L'}{L}(1,\chi)$. *J. Math. Anal. Appl.*, 320:562–577, 2006.

[82] T. Maeda. Gauss sums on $GL_2(\mathbb{Z}/p^l\mathbb{Z})$. *Journal of Algebra*, 396:98–116, 2013.

[83] A. V. Malyshev. Quadratic form. In *Encyclopedia of Mathematics*. Springer, 2011. `http://www.encyclopediaofmath.org/index.php?title=Quadratic_form`.

[84] O. D. Mbodj. Quadratic Gauss Sums. *Finite Fields and their Applications*, 4:347–361, 1998.

[85] D. McCarthy. Transformations of well-poised hypergeometric functions over finite fields. *Finite Fields and Their Applications*, 18:1133–1147, 2012.

[86] F. Mertens. Über die gaußschen Summen. *Sitz. Berlin Akad.*, pages 217–219, 1896.

[87] K. Momihara. Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums. *European Journal of Combinatorics*, 34:706–723, 2013.

[88] K. Momihara. Certain strongly regular Cayley graphs on $\mathbb{F}_{2^{2(2s+1)}}$ from cyclotomy. *Finite Fields and their Applications*, 25:280–292, 2014.

[89] L. J. Mordell. On a simple summation of the series $\sum_{s=0}^{n-1} e^{2s^2\pi\imath/n}$. *Messenger of Mathematics*, 48:54–56, 1918.

[90] L. J. Mordell. On the Reciprocity Formula for the Gauss's Sums in the Quadratic Field. *Proceedings of the London Mathematical Society*, S2-20:289–296, 1922.

[91] L. J. Mordell. The sign of the Gaussian sum. *Illnois Journal of Mathematics*, 6:177–180, 1960.

[92] L. J. Mordell. Some Exponential Sums in Several Variables. *Monatshefte für Mathematik*, 73:348–353, 1969.

[93] T. Nagell. *Introduction to Number Theory*. Chelsea Publishing Company, 1964.

[94] X. Pan and H. Zhang. An hybrid mean value of quadratic Gauss sums and a sum analogous to Kloosterman sums. *Journal of Inequalities and Applications*, 2014(129), 2014. `http://www.journalofinequalitiesandapplications.com/content/2014/1/129`.

[95] X. Pan, X. Zhao, and W. Cao. A Problem of Carlitz and its generalizations. *Archiv der Mathematik*, 102(4):337–343, 2014.

[96] A. Polishchuk. *Abelian Varieties, Theta Functions and the Fourier Transform*. Cambridge University Press, 2004.

[97] A. Salerno. Counting points over finite fields and hypergeometric functions. *Functiones et Approximatio*, 49(1):137–157, 2013.

[98] M. Schaar. Mémoire sure une formule d'analyse. *Mémoires couronnés et mémoires des savants étrangers, l'Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique*, 23, 1848-1850.

[99] M. Schaar. Mémoire sur la théorie des résidus quadratique. *Mémoires de l'Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique*, 24:1–14, 1850.

[100] J. Schur. Über die Gaußschen Summen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 1921:147–153, 1921.

[101] R Sczech. Gaussian sums, Dedekind sums and the Jacobi triple product identity. *Kyushu Journal of Mathematics*, 49(2):233–241, 1995.

[102] D. Shanks. Two theorems of Gauss. *Pacific Journal of Mathematics*, 8(3), 1958.

[103] C. L. Siegel. Über die analystische Theorie der quadratischen Formen. *Annals of Mathematics*, 36(3):527–606, 1935.

[104] C. L. Siegel. Über das quadratische Reziprozitätsgesetz in algebraischen Zahlkörpern. *Nachrichten der Akademie der Wissenschaften zu Göttingen. II. Mathematisch-Physikalische Klasse*, 1:1–16, 1960.

[105] F. Szechtman. Quadratic Gauss Sums over Finite Commutative Rings. *Journal of Number Theory*, 95:1–13, 2002.

[106] M. E. Taylor. Multivariate Gauss sums. `http://www.unc.edu/math/Faculty/met/gausum2.pdf`. [Online; accessed 3-August-2015].

[107] V. Turaev. Reciprocity for Gauss sums on finite abelian groups. *Math. Proc. Camb. Phil. Soc.*, 124:205–215, 1998.

[108] T. Wang and W. Zhang. On the mean value of Dedekind sum weighted by the quadratic Gauss sum. *Czechoslovak Mathematical Journal*, 63(138):357–367, 2013.

[109] W. Wang and W. Zhang. A Mean Value Related to Primitive Roots and Golomb's Conjecture. *Abstract and Applied Analysis*, 2014, 2014. Article ID 908273.

[110] W. Waterhouse. The sign of the Gaussian sum. *Journal of Number Theory*, 2(3):363, 1970.

[111] H. Weber. Über die mehrfachen Gaussischen summen. *Journal für die reine und angewandte Mathematik*, 74:14–56, 1872.

[112] A. Weil. On Some Exponential Sums. *Proc. Nat. Acad. Sci. U. S. A.*, 34:204–207, 1948.

[113] F. Wu. Constructions of strongly regular Cayley graphs using even index Gauss sums. Published online 21 December 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/jcd.21339.

[114] L. Xia and J. Yang. Cyclotomic problem, Gauss sums and Legendre curve. *Science China Mathematics*, 56(7):1485–1508, 2013.

[115] Q. Xiang. Cyclotomy, Gauss Sums, Difference Sets and Strongly Regular Cayley Graphs. In *Lecture Notes in Computer Science*, volume 7280. Springer, Heidelberg, 2012.

[116] M. Xiong. The weight distributions of a class of cyclic codes. *Finite Fields and Their Applications*, 18:933–945, 2012.

[117] M. Xiong. The weight distributions of a class of cyclic codes II. *Designs, Codes and Cryptography*, 72:511–528, 2014.

[118] Z. Xu, T. Zhang, and W. Zhang. On the mean value of the two-term exponential sums with Dirichlet characters. *Journal of Number Theory*, 123:352–362, 2007.

[119] M. Yamada. Difference sets over Galois rings with odd extension degrees and characteristic an even power of 2. *Designs, Codes and Cryptography*, 67:37–57, 2013.

[120] T. Zhang. On the general quadratic Gauss sums weighted by character sums over a short interval. *Bull. Korean Math. Soc.*, 50(3):873–883, 2013.

[121] W. Zhang. Moments of Generalized Quadratic Gauss Sums Weighted by L-Functions. *Journal of Number Theory*, 92:304–314, 2002.

[122] W. Zhang. The First Power Mean of the Inversion of L-Functions Weighted by Quadratic Gauss Sums. *Acta Mathematica Sinica, English Series*, 20(2):283–292, 2004.

[123] W. Zhang and Y. Deng. A hybrid mean value of the inversion of L-functions and general quadratic Gauss sums. *Nagoya Math. J.*, 167:1–15, 2002.

[124] W. Zhang and Liu Huaning. On the general Gauss sums and their fourth power mean. *Osaka J. Math*, 1:189–199, 2005.

[125] M. Zhu and W. Cao. Invariant factors of degree matrices and L-functions of certain exponential sums. *Finite Fields and their Applications*, 28:188–198, 2014.