Journal of Combinatorics and Number Theory
Volume 6, Number 2, pp. 127–153
ISSN: 1942-5600


# DOUBLE GAUSS SUMS*

***Ayşe Alaca*, *Şaban Alaca*† and *Kenneth S. Williams*§**
School of Mathematics and Statistics, Carleton University,
Ottawa, Ontario, Canada

**Abstract**

We evaluate the double Gauss sum

$$G(a,b,c;m;p^n) := \sum_{x,y=0}^{p^n-1} e^{2\pi i m(ax^2+bxy+cy^2)/p^n},$$

where $a, b, c$ are integers such that $\gcd(a,b,c) = 1$ and $b^2 - 4ac \neq 0$, $p$ is a prime, $n$ is a positive integer, and $m$ is an integer not divisible by $p$. We apply the evaluation of this sum to the determination of the number of solutions of certain congruences of the form $ax^2 + bxy + cy^2 + dz^2 + ezt + ft^2 \equiv k \pmod{p^n}$, where $k$ is a nonzero integer.

**2010 Mathematics Subject Classification:** 11L03, 11L05, 11T23, 11E16, 11E25, 11D79

**Keywords and phrases:** Gauss sums, double Gauss sums, exponential sums, binary quadratic forms, sums of two binary quadratic forms, congruences

## 1. Introduction

Let $\mathbb{N}$ denote the set of positive integers and $\mathbb{Z}$ the set of all integers. Set $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For $p$ a prime, $n \in \mathbb{N}$ and $m \in \mathbb{Z}$, the (quadratic) Gauss sum $G(m;p^n)$ is defined by

$$G(m;p^n) := \sum_{x=0}^{p^n-1} e^{2\pi i m x^2/p^n}. \tag{1.1}$$

The value of this sum is well-known and goes back to Gauss. If $m \equiv 0 \pmod{p^n}$ then

$$G(m;p^n) = \sum_{x=0}^{p^n-1} 1 = p^n.$$

*The research of the first and second authors was supported by research grants from the Natural Sciences and Engineering Research Council of Canada.

†E-mail address: aalaca@math.carleton.ca
‡E-mail address: salaca@math.carleton.ca
§E-mail address: kwilliam@connect.carleton.ca

On the other hand if $m \not\equiv 0 \pmod{p^n}$ then for some $k \in \mathbb{N}_0$ with $k < n$ we have $p^k \mid\mid m$ so that

$$\sum_{x=0}^{p^n-1} e^{2\pi i m x^2/p^n} = \sum_{x=0}^{p^n-1} e^{2\pi i m_1 x^2/p^{n-k}} = p^k \sum_{x=0}^{p^{n-k}-1} e^{2\pi i m_1 x^2/p^{n-k}},$$

where $m_1 = m/p^k \in \mathbb{Z}$ and $p \nmid m_1$. Hence in this case we have

$$G(m; p^n) = p^k G(m_1; p^{n-k}).$$

Thus we may suppose that $p \nmid m$. For $p \neq 2$ and $p \nmid m$ we have

$$G(m; p^n) = \left(\frac{m}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} p^{n/2}, \tag{1.2}$$

where $\left(\frac{*}{p}\right)$ is the Legendre symbol, see for example [2, Theorem 1.5.2, p. 26]. For $p = 2$ and $2 \nmid m$ we have

$$G(m; 2^n) = \begin{cases} 0 & \text{if } n = 1, \\ \left(\frac{2}{m}\right)^n (1 + i^m) 2^{n/2} & \text{if } n \geq 2, \end{cases} \tag{1.3}$$

where

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

see for example [2, Theorem 1.5.1, Proposition 1.5.3, p. 26]. We note that for odd $p$ we have

$$i^{\left(\frac{p^n-1}{2}\right)^2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4, \\ & \text{or } p \equiv 3 \pmod 4, n \equiv 0 \pmod 2, \\ i & \text{if } p \equiv 3 \pmod 4, n \equiv 1 \pmod 2. \end{cases} \tag{1.4}$$

In this paper we consider the exponential sum formed by replacing $x^2$ in (1.1) by a primitive binary quadratic form $ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y]$ with a nonzero discriminant, that is, we consider the sum

$$G(a, b, c; m; p^n) = \sum_{x,y=0}^{p^n-1} e^{2\pi i m(ax^2+bxy+cy^2)/p^n}, \tag{1.5}$$

where

$$m \not\equiv 0 \pmod p, \quad \gcd(a, b, c) = 1, \quad b^2 - 4ac \neq 0.$$

We call such a sum a double (quadratic) Gauss sum.

We first evaluate the sum (1.5) when $p$ is an odd prime. We prove the following theorem in Section 2, where it is used to determine some double Gauss sums explicitly (Corollary

2.1). The underlying idea in the proof of Theorem 1.1 is the determination of integers $r, s, t$ and $u$ such that

$$\begin{aligned}&\begin{bmatrix} r & s \\ t & u \end{bmatrix}^T \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix} \\ &= \begin{bmatrix} ar^2+brt+ct^2 & (2ars+b(ru+st)+2ctu)/2 \\ (2ars+b(ru+st)+2ctu)/2 & as^2+bsu+cu^2 \end{bmatrix}\end{aligned}$$

is a diagonal matrix with integral entries and determinant not divisible by $p$ in order to express the double Gauss sum $G(a,b,c;m;p^n)$ as the product of two single Gauss sums. The proof is given in Section 2.

**Theorem 1.1.** *Let $p$ be an odd prime. Let $ax^2+bxy+cy^2 \in \mathbb{Z}[x,y]$ be such that*

$$\gcd(a,b,c) = 1 \tag{1.6}$$

*and*

$$b^2 - 4ac \neq 0. \tag{1.7}$$

*Let $A$ be any integer with $A \not\equiv 0 \pmod p$ represented by the binary quadratic form $ax^2+bxy+cy^2$. For example we can take*

$$A = \begin{cases} a & \text{if } p \nmid a \quad (\text{as } a = a\cdot 1^2 + b\cdot 1\cdot 0 + c\cdot 0^2), \\ c & \text{if } p \mid a,\ p \nmid c \quad (\text{as } c = a\cdot 0^2 + b\cdot 0\cdot 1 + c\cdot 1^2), \\ a+b+c & \text{if } p \mid a,\ p \mid c \quad (\text{as } a+b+c = a\cdot 1^2 + b\cdot 1\cdot 1 + c\cdot 1^2). \end{cases}$$

(*If $p \mid a$ and $p \mid c$ the condition* (1.6) *ensures that $p \nmid b$ so $p \nmid a+b+c$.*) *Define $l \in \mathbb{N}_0$ by*

$$p^l \mid\mid 4ac - b^2 \tag{1.8}$$

*and set*

$$h := \frac{4ac-b^2}{p^l} \in \mathbb{Z} \setminus \{0\} \tag{1.9}$$

*so $p \nmid h$. Let $n \in \mathbb{N}$. Let $m \in \mathbb{Z}$ be such that $m \not\equiv 0 \pmod p$. Then*

$$G(a,b,c;m;p^n) = \begin{cases} \left(\frac{Am}{p}\right)^n p^n \sqrt{(-1)^{(p^n-1)/2} p^n} & \text{if } l \geq n, \\ \left(\frac{-1}{p}\right)^{(l+1)n} \left(\frac{Am}{p}\right)^l \left(\frac{h}{p}\right)^{l+n} p^n \sqrt{(-1)^{(p^l-1)/2} p^l} & \text{if } l \leq n. \end{cases}$$

We remark that when $l = n$ the two expressions for $G(a,b,c;m;p^n)$ in Theorem 1.1 agree (as they should) as

$$\begin{aligned}&\left(\frac{-1}{p}\right)^{(n+1)n} \left(\frac{Am}{p}\right)^n \left(\frac{h}{p}\right)^{2n} p^n \sqrt{(-1)^{\frac{(p^n-1)}{2}} p^n} \\ &\qquad = \left(\frac{Am}{p}\right)^n p^n \sqrt{(-1)^{\frac{(p^n-1)}{2}} p^n}.\end{aligned} \tag{1.10}$$

We also note that the evaluation of $G(a,b,c;m;p^n)$ given in Theorem 1.1 is (as it should be) independent of the choice of the integer $A$. This follows from the theory of binary quadratic forms. We give a simple direct proof. It suffices to show that if $A$ and $A'$ are two integers represented by $ax^2+bxy+cy^2$ with $A \not\equiv 0 \pmod p$ and $A' \not\equiv 0 \pmod p$ then

$$\Big(\frac{A}{p}\Big) = \Big(\frac{A'}{p}\Big) \text{ when } l \geq 1. \tag{1.11}$$

(If $l = 0$ the independence is clear as

$$\Big(\frac{A}{p}\Big)^l = (\pm 1)^0 = 1, \ \ \Big(\frac{A'}{p}\Big)^l = (\pm 1)^0 = 1, \ \text{ so } \Big(\frac{A}{p}\Big)^l = \Big(\frac{A'}{p}\Big)^l .)$$

We now prove (1.11). As $A$ is represented by the binary quadratic form $ax^2+bxy+cy^2$ there are integers $u$ and $v$ such that

$$au^2 + buv + cv^2 = A.$$

Suppose first that $p \nmid a$. Then (as $p \mid 4ac - b^2$ since $l \geq 1$) we have

$$(2au + bv)^2 \equiv (2au + bv)^2 + (4ac - b^2)v^2 = 4a(au^2 + buv + cv^2) = 4aA \pmod p$$

so $\Big(\frac{4aA}{p}\Big) = 0$ or $1$. But $p \nmid 4aA$ so $\Big(\frac{4aA}{p}\Big) = 1$. Thus $\Big(\frac{A}{p}\Big) = \Big(\frac{a}{p}\Big)$. Similarly $\Big(\frac{A'}{p}\Big) = \Big(\frac{a}{p}\Big)$ and hence $\Big(\frac{A}{p}\Big) = \Big(\frac{A'}{p}\Big)$. Next suppose that $p \mid a$ and $p \nmid c$. Then, by the argument just given, we find that

$$\Big(\frac{A}{p}\Big) = \Big(\frac{c}{p}\Big) = \Big(\frac{A'}{p}\Big).$$

Finally suppose that $p \mid a$ and $p \mid c$. As $\gcd(a,b,c) = 1$ we have $p \nmid b$ and so $p \nmid a+b+c$. Let $z = u \in \mathbb{Z}$ and $w = v - u \in \mathbb{Z}$. Then

$$(a+b+c)z^2 + (b+2c)zw + cw^2 = au^2 + buv + cv^2 = A.$$

Hence, $A$ is represented by the binary quadratic form $(a+b+c)x^2 + (b+2c)xy + cy^2$ and, by the previous argument, we find

$$\Big(\frac{A}{p}\Big) = \Big(\frac{a+b+c}{p}\Big) = \Big(\frac{A'}{p}\Big).$$

This completes the proof of (1.11).

We will apply Theorem 1.1 to some specific binary quadratic forms in Corollary 2.1.

Regarding double Gauss sums (1.5) for $p = 2$, we begin by treating the case when $b$ is even. We prove the following result in Section 3 using the same method of proof as for Theorem 1.1.

**Theorem 1.2.** *Let* $ax^2+bxy+cy^2 \in \mathbb{Z}[x,y]$ *be such that*

$$\gcd(a,b,c)=1, \tag{1.12}$$

$$b^2-4ac \neq 0, \tag{1.13}$$

*and*

$$b \equiv 0 \pmod 2. \tag{1.14}$$

*From* (1.12) *and* (1.14) *we see that at least one of* $a$ *and* $c$ *is odd. As* $G(a,b,c;m;2^n) = G(c,b,a;m;2^n)$ *we may suppose without loss of generality that* $a$ *is odd. Define* $l \in \mathbb{N}_0$ *by*

$$2^l \mid\mid ac-(b/2)^2 \tag{1.15}$$

*and set*

$$h := \frac{ac-(b/2)^2}{2^l} \in \mathbb{Z}\setminus\{0\} \tag{1.16}$$

*so* $h \not\equiv 0 \pmod 2$. *Let* $n \in \mathbb{N}$. *Let* $m \in \mathbb{Z}$ *be such that* $m \not\equiv 0 \pmod 2$. *Then*

$$G(a,b,c;m;2^n) = \begin{cases} 0 & \text{if } n=1, \\ \left(\frac{2}{am}\right)^n (1+i^{am})2^{3n/2} & \text{if } 2 \le n \le l, \\ 0 & \text{if } n = l+1 \ge 2, \\ \left(\frac{2}{am}\right)^l \left(\frac{2}{h}\right)^{n+l} (1+i^{am})(1+i^{amh})2^{n+(l/2)} & \text{if } n \ge l+2. \end{cases}$$

Some numerical examples illustrating Theorem 1.2 are given in Corollary 3.1.

We now turn to the case when $p=2$ and $b$ is odd. In this case we cannot use the method, which was used to prove Theorems 1.1 and 1.2, to evaluate $G(a,b,c;m;p^n)$ since there are no integers $r$, $s$, $t$ and $u$ with $\det \begin{bmatrix} r & s \\ t & u \end{bmatrix} \not\equiv 0 \pmod 2$ such that

$$\begin{bmatrix} r & s \\ t & u \end{bmatrix}^T \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} r & s \\ t & u \end{bmatrix}$$

is a diagonal matrix. This is clear as $ru-st \equiv 1 \pmod 2$ implies $2ars+b(ru+st)+2ctu$ is odd and thus nonzero. Hence we must proceed differently. If $a=c=0$ we have

$$G(a,b,c;m;p^n) = \sum_{x=0}^{2^n-1} \Big( \sum_{y=0}^{2^n-1} e^{2\pi i (mbx)y/2^n} \Big) = \sum_{\substack{x=0 \\ 2^n \mid mbx}}^{2^n-1} 2^n = \sum_{\substack{x=0 \\ 2^n \mid x}}^{2^n-1} 2^n = 2^n.$$

Thus we may suppose that $(a,c) \neq (0,0)$. As $G(a,b,c;m;2^n) = G(c,b,a;m;2^n)$ we may assume without loss of generality that $a \neq 0$. Our approach involves multiplying both the numerator and the denominator in the exponent of $e$ in $G(a,b,c;m;2^n)$ by a suitable power $2^f$ so that we can complete the square in $2^f(ax^2+bxy+cy^2)$ modulo $2^{n+f}$. We prove the following result in Section 3.

**Theorem 1.3.** *Let* $ax^2+bxy+cy^2 \in \mathbb{Z}[x,y]$ *be such that*

$$\gcd(a,b,c)=1, \tag{1.17}$$

$$b \equiv 1 \pmod 2 \tag{1.18}$$

*and*

$$a \neq 0. \tag{1.19}$$

*Note that* (1.18) *ensures that*

$$b^2-4ac \neq 0. \tag{1.20}$$

*Let* $n \in \mathbb{N}$. *Let* $m \in \mathbb{Z}$ *be such that* $m \not\equiv 0 \pmod 2$. *Then*

$$G(a,b,c;m;2^n)=(-1)^{acn}\,2^n.$$

Some numerical examples illustrating Theorem 1.3 are given in Corollary 3.2.

Let $N_{p^n}(a,b,c,d,e,f;k)$ denote the number of solutions of the quadratic congruence

$$ax^2+bxy+cy^2+dz^2+ezw+fw^2 \equiv k \pmod{p^n},$$

where $a,b,c,d,e,f$ are integers, $k$ a nonzero integer, $p$ a prime and $n$ a positive integer. We use the results given in Corollary 2.1, Corollary 3.1 and Corollary 3.2 to determine explicit formulae for $N_{p^n}(a,b,c,d,e,f;k)$ for certain quaternary quadratic forms $ax^2+bxy+cy^2+dz^2+ezw+fw^2$ when $n \geq \alpha+1$, where $p^\alpha || k$. These formulae will be used in a forthcoming paper of the authors to determine formulae for the number of representations of a positive integer $k$ by each of these forms using the local densities method described in [1]. We prove the following theorems (Theorems 1.4–1.15) in Section 4.

**Important Note.** In Theorems 1.4 -1.15, $k$ is a nonzero integer, $p$ is a prime, $p^\alpha$ is the largest power of $p$ dividing $k$, $K=k/p^\alpha$ and $n$ is a positive integer with $n \geq \alpha+1$. For convenience, we also define $A_{p,\alpha}$ by

$$A_{p,\alpha}(*)=p^{3n-\alpha-2}\Big(p^2-\Big(\frac{*}{p}\Big)\Big)\frac{\Big(p^{\alpha+1}-\Big(\frac{*}{p}\Big)^{\alpha+1}\Big)}{p-\Big(\frac{*}{p}\Big)},$$

which is clearly an integer.

**Theorem 1.4.**

$$N_{p^n}(1,0,1,2,2,5;k)=\begin{cases}(p+1)(p^{3n-1}-p^{3n-\alpha-2}) & \text{if } p\neq 2,3,\\ 3^{3n}+3^{3n-1}\Big(\frac{k}{3}\Big) & \text{if } p=3,\alpha=0,\\ 4(3^{3n-1}-3^{3n-\alpha-1}) & \text{if } p=3,\alpha\geq 1,\\ 2^{3n} & \text{if } p=2,\alpha=0,\\ 3\cdot 2^{3n-\alpha} & \text{if } p=2,\alpha\geq 1.\end{cases}$$

**Theorem 1.5.**

$$N_{p^n}(1,0,3,2,2,3;k)=\begin{cases} A_{p,\alpha}(15) & \text{if } p\neq 2,3,5,\\ 5^{3n}+\Big(\dfrac{K}{5}\Big)(-1)^{\alpha}5^{3n-\alpha-1} & \text{if } p=5,\\ 3^{3n}+3^{3n-\alpha-1}\Big(\dfrac{K}{3}\Big) & \text{if } p=3,\\ 2^{3n}-2^{3n-\alpha-1}(-1)^{\frac{K-1}{2}} & \text{if } p=2. \end{cases}$$

**Theorem 1.6.**

$$N_{p^n}(1,0,1,5,2,5;k)$$
$$=\begin{cases} A_{p,\alpha}(6) & \text{if } p\neq 2,\ 3,\\ 3^{3n}+3^{3n-\alpha-1}\Big(\dfrac{K}{3}\Big) & \text{if } p=3,\\ 8 & \text{if } p=2,\alpha=0,n=1,\\ 2^5\big(2+(-1)^{\frac{K-1}{2}}\big) & \text{if } p=2,\alpha=0,n=2,\\ 2^{3n-2}\Big(4+2\Big(\dfrac{-1}{K}\Big)+\Big(\dfrac{2}{K}\Big)-\Big(\dfrac{-2}{K}\Big)\Big) & \text{if } p=2,\alpha=0,n\geq 3,\\ 3\cdot 2^{3n-1} & \text{if } p=2,\alpha=1,n\geq 2,\\ 2^{3n-1} & \text{if } p=2,(\alpha,n)=(2,3),(2,4),(3,4),\\ 2^{3n-1}+(-1)^{\alpha+1}2^{3n-\alpha-1}\Big(\dfrac{-2}{K}\Big) & \text{if } p=2,2\leq\alpha\leq n-3,n\geq 5,\\ 2^{3n-1} & \text{if } p=2,\alpha=n-2,n-1,n\geq 5. \end{cases}$$

**Theorem 1.7.**

$$N_{p^n}(1,0,5,2,2,3;k)=\begin{cases} (p+1)(p^{3n-1}-p^{3n-\alpha-2}) & \text{if } p\neq 2,5,\\ 2^{3n} & \text{if } p=2,\alpha=0,\\ 2^{3n+1}-3\cdot 2^{3n-\alpha} & \text{if } p=2,\ \alpha\geq 1,\\ 6\cdot 5^{3n-\alpha-1} & \text{if } p=5. \end{cases}$$

**Theorem 1.8.**

$$N_{p^n}(1,1,1,3,3,12;k)=\begin{cases} A_{p,\alpha}(5) & \text{if } p\neq 3,5,\\ 3^{3n}\Big(1+\Big(\dfrac{K}{3}\Big)\Big) & \text{if } p=3,\alpha=0,\\ \dfrac{1}{2}\Big(3^{3n}-(-1)^{\alpha}\cdot 5\cdot 3^{3n-\alpha}\Big) & \text{if } p=3,\alpha\geq 1,\\ 5^{3n}+5^{3n-\alpha-1}\Big(\dfrac{K}{5}\Big) & \text{if } p=5. \end{cases}$$

**Theorem 1.9.**

$$N_{p^n}(2,1,2,3,3,3;k)=\begin{cases} A_{p,\alpha}(5) & \text{if } p\neq 3,5,\\ 3^{3n}\big(1-\big(\frac{K}{3}\big)\big) & \text{if } p=3,\alpha=0,\\ \frac{1}{2}\big(3^{3n}-(-1)^{\alpha}5\cdot 3^{3n-\alpha}\big) & \text{if } p=3,\alpha\geq 1,\\ 5^{3n}+\big(\frac{K}{5}\big)5^{3n-\alpha-1} & \text{if } p=5.\end{cases}$$

**Theorem 1.10.**

$$N_{p^n}(1,0,3,2,2,5;k)=\begin{cases} A_{p,\alpha}(3) & \text{if } p\neq 2,3,\\ 2\cdot 3^{3n-1} & \text{if } p=3,\alpha=0,\\ 5\cdot 3^{3n-1}-(-1)^{\alpha}3^{3n-\alpha}\big(\frac{K}{3}\big) & \text{if } p=3,\alpha\geq 1,\\ 2^{3n}-(-1)^{\alpha+\frac{K+1}{2}}2^{3n-\alpha-1} & \text{if } p=2.\end{cases}$$

**Theorem 1.11.**

$$N_{p^n}(1,0,2,3,2,5;k)=\begin{cases} A_{p,\alpha}(7) & \text{if } p\neq 2,7,\\ 7^{3n}+(-1)^{\alpha}7^{3n-\alpha-1}\big(\frac{K}{7}\big) & \text{if } p=7,\\ 2^{3n} & \text{if } p=2,\alpha=0,\\ 2^{3n}-2^{3n-\alpha}(-1)^{\frac{K-1}{2}} & \text{if } p=2,\alpha\geq 1.\end{cases}$$

**Theorem 1.12.**

$$N_{p^n}(1,0,2,6,4,6;k)=\begin{cases} (p+1)(p^{3n-1}-p^{3n-\alpha-2}) & \text{if } p\neq 2,\\ 2^{3n}+2^{3n-1}\big(\frac{2}{K}\big)\big(1+(-1)^{\frac{K-1}{2}}\big) & \text{if } p=2,\ \alpha=0,\\ 2^{3n} & \text{if } p=2,\ \alpha=1,\\ 2^{3n}-2^{3n-1}(-1)^{\frac{K-1}{2}} & \text{if } p=2,\ \alpha=2,\\ 3\cdot 2^{3n-1} & \text{if } p=2,\ \alpha=3,\\ 2^{3n-1} & \text{if } p=2,\ \alpha=4,\\ 3\cdot 2^{3n-\alpha+3} & \text{if } p=2,\ \alpha\geq 5.\end{cases}$$

**Theorem 1.13.**

$$N_{p^n}(1,1,4,5,5,5;k)=\begin{cases} A_{p,\alpha}(5) & \text{if } p\neq 3,5,\\ \frac{1}{2}\big(3^{3n+1}-(-1)^{\alpha}5\cdot 3^{3n-\alpha-1}\big) & \text{if } p=3,\\ 5^{3n}+\big(\frac{K}{5}\big)5^{3n-\alpha} & \text{if } p=5.\end{cases}$$

**Theorem 1.14.**

$$N_{p^n}(2,1,2,5,5,5;k)=\begin{cases} A_{p,\alpha}(5) & \text{if } p\neq 3,5,\\ \frac{3^{3n}}{2}\Big(1+(-1)^{\alpha}5\cdot 3^{-\alpha-1}\Big) & \text{if } p=3,\\ 5^{3n}-\Big(\frac{K}{5}\Big)5^{3n-\alpha} & \text{if } p=5.\end{cases}$$

**Theorem 1.15.**

$$N_{p^n}(2,2,5,3,0,3;k)=\begin{cases} (p+1)(p^{3n-1}-p^{3n-\alpha-2}) & \text{if } p\neq 2,3,\\ 3^{3n}\big(1-\big(\frac{K}{3}\big)\big) & \text{if } p=3,\ \alpha=0,\\ 4\cdot 3^{3n-\alpha} & \text{if } p=3,\ \alpha\geq 1,\\ 2^{3n} & \text{if } p=2,\ \alpha=0,\\ 2^{3n+1}-3\cdot 2^{3n-\alpha} & \text{if } p=2,\ \alpha\geq 1.\end{cases}$$

We conclude this introduction by recording a few easily-proved elementary identities that we will use in this paper.

Let $n_1, n_2 \in \mathbb{N}$. Let $p$ be an odd prime. Then

$$(-1)^{(p^{n_1}-1)(p^{n_2}-1)/4}=\Big(\frac{-1}{p}\Big)^{n_1n_2}. \tag{1.21}$$

Taking $n_1=n_2=n\in\mathbb{N}$ in (1.21) we deduce that

$$(-1)^{(p^n-1)^2/4}=\Big(\frac{-1}{p}\Big)^{n}. \tag{1.22}$$

Let $k, l$ be odd integers. Then

$$i^{((k-1)/2)^2+((l-1)/2)^2}=(-1)^{(k-1)(l-1)/4}\,i^{((kl-1)/2)^2} \tag{1.23}$$

and

$$(1+i^k)(1+i^l)=\begin{cases}\big(\frac{-1}{k}\big)\,2i & \text{if } k\equiv l \pmod 4,\\ 2 & \text{if } k\not\equiv l \pmod 4.\end{cases} \tag{1.24}$$

## 2. Proof of Theorem 1.1

In this section we prove Theorem 1.1, which gives the evaluation of the double Gauss sum $G(a,b,c;m;p^n)$ when $p$ is an odd prime.

**Proof of Theorem 1.1.** Let $A$ be any integer not divisible by $p$ which is represented by the binary quadratic form $ax^2+bxy+cy^2$. Then there exist integers $r$ and $t$ such that

$$A=ar^2+brt+ct^2\not\equiv 0 \pmod p. \tag{2.1}$$

Define integers $s$ and $u$ by

$$s := -br - 2ct, \quad u := 2ar + bt. \tag{2.2}$$

Then we have

$$as^2 + bsu + cu^2 = (4ac - b^2)(ar^2 + brt + ct^2) = p^l hA, \tag{2.3}$$

$$2ars + b(ru + st) + 2ctu = 0, \tag{2.4}$$

and

$$ru - st = 2(ar^2 + brt + ct^2) = 2A \not\equiv 0 \pmod{p}. \tag{2.5}$$

Let $\mathbb{Z}_{p^n}$ denote the ring of residue classes modulo $p^n$. We write $\bar{k}$ for the residue class $(\mathrm{mod}\ p^n)$ containing the integer $k$. The mapping $\lambda : \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n} \to \mathbb{Z}_{p^n} \times \mathbb{Z}_{p^n}$ given by $\lambda((\bar{x}, \bar{y})) = (\overline{rx + sy}, \overline{tx + uy})$ is well-defined. It is both injective and surjective in view of (2.5). Hence it is a bijection. As $e^{2\pi ix/p^n}$ is a periodic function of $x \in \mathbb{Z}$ with period $p^n$, we have by (2.3) and (2.4)

$$\begin{aligned} G(a,b,c;m;p^n) &= \sum_{x,y=0}^{p^n-1} e^{2\pi im(a(rx+sy)^2+b(rx+sy)(tx+uy)+c(tx+uy)^2)/p^n} \\ &= \sum_{x,y=0}^{p^n-1} e^{2\pi im(Ax^2+p^l hAy^2)/p^n} \\ &= \sum_{x=0}^{p^n-1} e^{2\pi iAmx^2/p^n} \sum_{y=0}^{p^n-1} e^{2\pi iAmhy^2/p^{n-l}}. \end{aligned}$$

If $l \geq n$ we obtain by (1.2)

$$\begin{aligned} G(a,b,c;m;p^n) &= p^n \sum_{x=0}^{p^n-1} e^{2\pi iAmx^2/p^n} \\ &= p^n \Big(\frac{Am}{p}\Big)^n i^{(p^n-1)^2/4} p^{n/2} \\ &= p^n \Big(\frac{Am}{p}\Big)^n \sqrt{(-1)^{(p^n-1)/2}\, p^n}. \end{aligned}$$

If $l < n$ we obtain by (1.2), (1.21) and (1.23)

$$\begin{aligned} G(a,b,c;m;p^n) &= p^l \sum_{x=0}^{p^n-1} e^{2\pi iAmx^2/p^n} \sum_{y=0}^{p^{n-l}-1} e^{2\pi iAmhy^2/p^{n-l}} \\ &= p^l \Big(\frac{Am}{p}\Big)^n i^{(p^n-1)^2/4}\, p^{n/2} \Big(\frac{Amh}{p}\Big)^{n-l} i^{(p^{n-l}-1)^2/4}\, p^{(n-l)/2} \\ &= \Big(\frac{Am}{p}\Big)^l \Big(\frac{h}{p}\Big)^{n+l} i^{(p^n-1)^2/4+(p^{n-l}-1)^2/4} p^{n+(l/2)} \end{aligned}$$

$$\begin{aligned}
&= \Big(\frac{Am}{p}\Big)^l \Big(\frac{h}{p}\Big)^{n+l} (-1)^{(p^n-1)(p^{n-l}-1)/4}\, i^{(p^{2n-l}-1)^2/4}\, p^{n+(l/2)} \\
&= \Big(\frac{Am}{p}\Big)^l \Big(\frac{h}{p}\Big)^{n+l} \Big(\frac{-1}{p}\Big)^{n(n-l)}\, p^n\, i^{(p^l-1)^2/4}\, p^{l/2} \\
&= \Big(\frac{-1}{p}\Big)^{(l+1)n} \Big(\frac{Am}{p}\Big)^l \Big(\frac{h}{p}\Big)^{l+n} p^n \sqrt{(-1)^{(p^l-1)/2}\, p^l}.
\end{aligned}$$

This completes the proof in view of (1.10). ∎

We now illustrate Theorem 1.1 by applying it to some specific binary quadratic forms $ax^2 + bxy + cy^2$.

**Corollary 2.1.** *Let $p$ be an odd prime and let $n \in \mathbb{N}$. Let $m \in \mathbb{Z}$ satisfy $m \not\equiv 0 \pmod p$. Then*

$$\text{(i)}\ \ G(1,1,1;m;p^n) = \begin{cases} \Big(\frac{m}{3}\Big) 3^n \sqrt{-3} & \text{if } p = 3, \\ \Big(\frac{-3}{p}\Big)^n p^n & \text{if } p \neq 3; \end{cases}$$

$$\text{(ii)}\ \ G(1,1,2;m;p^n) = \begin{cases} \Big(\frac{m}{7}\Big) 7^n \sqrt{-7} & \text{if } p = 7, \\ \Big(\frac{-7}{p}\Big)^n p^n & \text{if } p \neq 7; \end{cases}$$

$$\text{(iii)}\ \ G(1,1,3;m;p^n) = \begin{cases} \Big(\frac{m}{11}\Big) 11^n \sqrt{-11} & \text{if } p = 11, \\ \Big(\frac{-11}{p}\Big)^n p^n & \text{if } p \neq 11; \end{cases}$$

$$\text{(iv)}\ \ G(1,1,4;m;p^n) = \begin{cases} (-1)^{n+1}\Big(\frac{m}{3}\Big) 3^n \sqrt{-3} & \text{if } p = 3, \\ (-1)^{n+1}\Big(\frac{m}{5}\Big) 5^n \sqrt{5} & \text{if } p = 5, \\ \Big(\frac{-15}{p}\Big)^n p^n & \text{if } p \neq 3, 5; \end{cases}$$

$$\text{(v)}\ \ G(2,1,2;m;p^n) = \begin{cases} (-1)^{n}\Big(\frac{m}{3}\Big) 3^n \sqrt{-3} & \text{if } p = 3, \\ (-1)^{n}\Big(\frac{m}{5}\Big) 5^n \sqrt{5} & \text{if } p = 5, \\ \Big(\frac{-15}{p}\Big)^n p^n & \text{if } p \neq 3, 5; \end{cases}$$

$$\text{(vi)}\ \ G(2,2,3;m;p^n) = \begin{cases} -\Big(\frac{m}{5}\Big) 5^n \sqrt{5} & \text{if } p = 5, \\ \Big(\frac{-5}{p}\Big)^n p^n & \text{if } p \neq 5; \end{cases}$$

$$\text{(vii)}\ \ G(2,2,5;m;p^n)=\begin{cases} -\Big(\dfrac{m}{3}\Big)3\sqrt{-3} & \text{if } p=3,\ n=1,\\ (-1)^n 3^{n+1} & \text{if } p=3,\ n\geq 2,\\ \Big(\dfrac{-1}{p}\Big)^n p^n & \text{if } p\neq 3;\end{cases}$$

$$\text{(viii)}\ \ G(3,2,3;m;p^n)=\Big(\frac{-2}{p}\Big)^n p^n;$$

$$\text{(ix)}\ \ G(3,2,5;m;p^n)=\begin{cases} -\Big(\dfrac{m}{7}\Big)7^n\sqrt{-7} & \text{if } p=7,\\ \Big(\dfrac{-14}{p}\Big)^n p^n & \text{if } p\neq 7;\end{cases}$$

$$\text{(x)}\ \ G(4,4,5;m;p^n)=\Big(\frac{-1}{p}\Big)^n p^n;$$

$$\text{(xi)}\ \ G(5,2,5;m;p^n)=\begin{cases} (-1)^n\Big(\dfrac{m}{3}\Big)3^n\sqrt{-3} & \text{if } p=3,\\ \Big(\dfrac{-6}{p}\Big)^n p^n & \text{if } p\neq 3.\end{cases}$$

**Proof.** Throughout this proof $p$ denotes an odd prime and $m$ is an integer not divisible by $p$.
(i) Here $(a,b,c)=(1,1,1)$ and $4ac-b^2=3$. The binary quadratic form $x^2+xy+y^2$ represents 1 so we may take $A=1$. We have

$$\begin{cases} l=1,\ h=1 & \text{if } p=3,\\ l=0,\ h=3 & \text{if } p\neq 3.\end{cases}$$

Theorem 1.1 with $p=3$ gives

$$G(1,1,1;m;3^n)=\Big(\frac{m}{3}\Big)3^n\sqrt{-3}$$

and for $p\neq 3$

$$G(1,1,1;m;p^n)=\Big(\frac{-1}{p}\Big)^n\Big(\frac{3}{p}\Big)^n p^n=\Big(\frac{-3}{p}\Big)^n p^n.$$

(ii) Here $(a,b,c)=(1,1,2)$ and $4ac-b^2=7$. We may take $A=1$. We have

$$\begin{cases} l=1,\ h=1 & \text{if } p=7,\\ l=0,\ h=7 & \text{if } p\neq 7.\end{cases}$$

Theorem 1.1 with $p=7$ gives

$$G(1,1,2;m;7^n)=\Big(\frac{m}{7}\Big)7^n\sqrt{-7}$$

and for $p \neq 7$

$$G(1,1,2;m;p^n) = \Big(\frac{-1}{p}\Big)^n \Big(\frac{7}{p}\Big)^n p^n = \Big(\frac{-7}{p}\Big)^n p^n.$$

(iii) The proof is similar to that of (i) (and (ii)).
(iv) Here $(a,b,c) = (1,1,4)$ and $4ac - b^2 = 15$. We may take $A = 1$. We have

$$\begin{cases} l = 1,\ h = 5 & \text{if } p = 3, \\ l = 1,\ h = 3 & \text{if } p = 5, \\ l = 0,\ h = 15 & \text{if } p \neq 3, 5. \end{cases}$$

Theorem 1.1 gives

$$G(1,1,4;m;3^n) = \Big(\frac{m}{3}\Big)\Big(\frac{5}{3}\Big)^{n+1} 3^n\sqrt{-3} = (-1)^{n+1}\Big(\frac{m}{3}\Big)3^n\sqrt{-3},$$
$$G(1,1,4;m;5^n) = \Big(\frac{m}{5}\Big)\Big(\frac{3}{5}\Big)^{n+1} 5^n\sqrt{5} = (-1)^{n+1}\Big(\frac{m}{5}\Big)5^n\sqrt{5},$$
$$G(1,1,4;m;p^n) = \Big(\frac{-1}{p}\Big)^n \Big(\frac{15}{p}\Big)^n p^n = \Big(\frac{-15}{p}\Big)^n p^n \quad \text{if } p \neq 3, 5.$$

(v) Here $(a,b,c) = (2,1,2)$ and $4ac - b^2 = 15$. We may take $A = 2$. We have

$$\begin{cases} l = 1,\ h = 5 & \text{if } p = 3, \\ l = 1,\ h = 3 & \text{if } p = 5, \\ l = 0,\ h = 15 & \text{if } p \neq 3, 5. \end{cases}$$

Theorem 1.1 gives

$$G(2,1,2;m;3^n) = \Big(\frac{2m}{3}\Big)\Big(\frac{5}{3}\Big)^{n+1} 3^n\sqrt{-3} = (-1)^n\Big(\frac{m}{3}\Big)3^n\sqrt{-3},$$
$$G(2,1,2;m;5^n) = \Big(\frac{2m}{5}\Big)\Big(\frac{3}{5}\Big)^{n+1} 5^n\sqrt{5} = (-1)^n\Big(\frac{m}{5}\Big)5^n\sqrt{5},$$
$$G(2,1,2;m;p^n) = \Big(\frac{-1}{p}\Big)^n \Big(\frac{15}{p}\Big)^n p^n = \Big(\frac{-15}{p}\Big)^n p^n \quad \text{if } p \neq 3, 5.$$

(vi) Here $(a,b,c) = (2,2,3)$ and $4ac - b^2 = 20$. We may take $A = 2$. We have

$$\begin{cases} l = 1,\ h = 4 & \text{if } p = 5, \\ l = 0,\ h = 20 & \text{if } p \neq 5. \end{cases}$$

Theorem 1.1 gives

$$G(2,2,3;m;5^n) = \Big(\frac{2m}{5}\Big)5^n\sqrt{5} = -\Big(\frac{m}{5}\Big)5^n\sqrt{5},$$
$$G(2,2,3;m;p^n) = \Big(\frac{-1}{p}\Big)^n \Big(\frac{20}{p}\Big)^n p^n = \Big(\frac{-20}{p}\Big)^n p^n = \Big(\frac{-5}{p}\Big)^n p^n \quad \text{if } p \neq 5.$$

(vii) Here $(a,b,c)=(2,2,5)$ and $4ac-b^2=36$. We may take $A=2$. We have

$$\begin{cases} l=2,\ h=4 & \text{if } p=3,\\ l=0,\ h=36 & \text{if } p\neq 3.\end{cases}$$

With $p=3$ Theorem 1.1 gives

$$G(2,2,5;m;3^n)=\begin{cases} \Big(\dfrac{2m}{3}\Big)3\sqrt{-3}=-\Big(\dfrac{m}{3}\Big)3\sqrt{-3} & \text{if } n=1,\\ \Big(\dfrac{-1}{3}\Big)^n 3^{n+1}=(-1)^n 3^{n+1} & \text{if } n\geq 2.\end{cases}$$

For $p\neq 3$ Theorem 1.1 gives

$$G(2,2,5;m;p^n)=\Big(\frac{-1}{p}\Big)^n p^n.$$

(viii) Here $(a,b,c)=(3,2,3)$ and $4ac-b^2=32$. We may take $A=8$. We have $l=0$ and $h=32$. Theorem 1.1 gives

$$G(3,2,3;m;p^n)=\Big(\frac{-1}{p}\Big)^n\Big(\frac{32}{p}\Big)^n p^n=\Big(\frac{-2}{p}\Big)^n p^n.$$

(ix) Here $(a,b,c)=(3,2,5)$ and $4ac-b^2=56$. We may take

$$A=\begin{cases} 5 & \text{if } p=3,\\ 3 & \text{if } p\neq 3.\end{cases}$$

We have

$$\begin{cases} l=1,\ h=8 & \text{if } p=7,\\ l=0,\ h=56 & \text{if } p\neq 7.\end{cases}$$

Theorem 1.1 gives

$$\begin{aligned} G(3,2,5;m;3^n)&=\Big(\frac{-1}{3}\Big)^n\Big(\frac{56}{3}\Big)^n 3^n=\Big(\frac{-14}{3}\Big)^n 3^n,\\ G(3,2,5;m;7^n)&=\Big(\frac{3m}{7}\Big)\Big(\frac{8}{7}\Big)^{n+1}7^n\sqrt{-7}=-\Big(\frac{m}{7}\Big)7^n\sqrt{-7},\\ G(3,2,5;m;p^n)&=\Big(\frac{-1}{p}\Big)^n\Big(\frac{56}{p}\Big)^n p^n=\Big(\frac{-14}{p}\Big)^n p^n \quad \text{if } p\neq 3,7.\end{aligned}$$

(x) Here $(a,b,c)=(4,4,5)$ and $4ac-b^2=64$. We can take $A=4$. We have $l=0$ and $h=64$. Theorem 1.1 gives

$$G(4,4,5;m;p^n)=\Big(\frac{-1}{p}\Big)^n p^n.$$

(xi) Here $(a,b,c)=(5,2,5)$ and $4ac-b^2=96$. We can take $A=8$. We have

$$\begin{cases} l=1,\ h=32 & \text{if } p=3,\\ l=0,\ h=96 & \text{if } p\neq 3.\end{cases}$$

Theorem 1.1 gives

$$G(5,2,5;m;3^n) = \Big(\frac{8m}{3}\Big)\Big(\frac{32}{3}\Big)^{n+1} 3^n\sqrt{-3} = (-1)^n\Big(\frac{m}{3}\Big)3^n\sqrt{-3},$$
$$G(5,2,5;m;p^n) = \Big(\frac{-1}{p}\Big)^n\Big(\frac{96}{p}\Big)^n p^n = \Big(\frac{-6}{p}\Big)^n p^n \quad \text{if } p \neq 3.$$

## 3. Proofs of Theorems 1.2 and 1.3

We begin by proving Theorem 1.2, which evaluates the double Gauss sum $G(a,b,c;m;p^n)$ when $p = 2$ and $b$ is even.

**Proof of Theorem 1.2.** Define the integers $r$, $s$, $t$ and $u$ by

$$r = 1,\ s = -\frac{b}{2},\ t = 0,\ u = a.$$

Then

$$ar^2 + brt + ct^2 = a \equiv 1 \pmod 2, \tag{3.1}$$
$$2ars + b(ru + st) + 2ctu = 0, \tag{3.2}$$
$$as^2 + bsu + cu^2 = a\big(ac - \frac{b^2}{4}\big) = 2^l ah, \tag{3.3}$$
$$ru - st = a \equiv 1 \pmod 2, \tag{3.4}$$

where we appealed to (1.16) for (3.3).

Let $\mathbb{Z}_{2^n}$ denote the ring of residue classes modulo $2^n$. We write $\bar{k}$ for the residue class $(\mathrm{mod}\ 2^n)$ containing the integer $k$. The mapping $\lambda : \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n}$ given by $\lambda((\bar{x},\bar{y})) = (\overline{rx+sy}, \overline{tx+uy})$ is well-defined. It is both injective and surjective in view of (3.4). Hence it is a bijection. As $e^{2\pi ix/2^n}$ is a periodic function of $x \in \mathbb{Z}$ with period $2^n$, we have by (3.1)-(3.3)

$$\begin{aligned} G(a,b,c;m;2^n) &= \sum_{x,y=0}^{2^n-1} e^{2\pi im(a(rx+sy)^2+b(rx+sy)(tx+uy)+c(tx+uy)^2)/2^n} \\ &= \sum_{x,y=0}^{2^n-1} e^{2\pi im(ax^2+2^l ahy^2)/2^n} \\ &= \sum_{x=0}^{2^n-1} e^{2\pi iamx^2/2^n} \sum_{y=0}^{2^n-1} e^{2\pi iamhy^2/2^{n-l}}. \end{aligned}$$

If $n = 1$ the first sum in this product is 0 by (1.3) so we have

$$G(a,b,c;m;2^n) = 0 \text{ if } n = 1.$$

Now suppose $n \geq 2$. If $n \leq l$ the second sum in the product is $2^n$ and we have by (1.3)

$$G(a,b,c;m;2^n) = \Big(\frac{2}{am}\Big)^n (1 + i^{am})\, 2^{n/2} \cdot 2^n$$

so

$$G(a,b,c;m;2^n)=\Big(\frac{2}{am}\Big)^n(1+i^{am})\,2^{3n/2}\quad\text{if } 2\le n\le l.$$

If $n=l+1$ the second sum is

$$\sum_{y=0}^{2^{l+1}-1}e^{2\pi iamhy^2/2}=2^l\sum_{y=0}^{1}e^{2\pi iamhy^2/2}=0$$

so

$$G(a,b,c;m;2^n)=0\quad\text{if } n=l+1\ge 2.$$

Finally if $n\ge l+2$ we have by (1.3)

$$\begin{aligned}G(a,b,c;m;2^n)&=\Big(\frac{2}{am}\Big)^n(1+i^{am})\,2^{n/2}\cdot 2^l\Big(\frac{2}{amh}\Big)^{n-l}(1+i^{amh})\,2^{(n-l)/2}\\&=\Big(\frac{2}{am}\Big)^l\Big(\frac{2}{h}\Big)^{n+l}(1+i^{am})\,(1+i^{amh})\,2^{n+(l/2)}.\end{aligned}$$

This completes the proof of Theorem 1.2. ∎

We now apply Theorem 1.2 to the binary quadratic forms $ax^2+bxy+cy^2$ considered in Corollary 2.1 having $b$ even.

**Corollary 3.1.** *Let $n\in\mathbb{N}$. Let $m$ be an odd integer. Then*

$$\text{(i)}\quad G(2,2,3;m;2^n)=\begin{cases}0 & \text{if } n=1,\\ (-1)^{n+1}\Big(\dfrac{-1}{m}\Big)2^{n+1}i & \text{if } n\ge 2;\end{cases}$$

$$\text{(ii)}\quad G(2,2,5;m;2^n)=\begin{cases}0 & \text{if } n=1,\\ \Big(\dfrac{-1}{m}\Big)2^{n+1}i & \text{if } n\ge 2;\end{cases}$$

$$\text{(iii)}\quad G(3,2,3;m;2^n)=\begin{cases}0 & \text{if } n=1,4,\\ 8\Big(1-\Big(\dfrac{-1}{m}\Big)i\Big) & \text{if } n=2,\\ -16\sqrt{2}\Big(\dfrac{2}{m}\Big)\Big(1-\Big(\dfrac{-1}{m}\Big)i\Big) & \text{if } n=3,\\ \Big(\dfrac{-2}{m}\Big)2^{n+2}i\sqrt{2} & \text{if } n\ge 5;\end{cases}$$

$$\text{(iv)}\quad G(3,2,5;m;2^n)=\begin{cases}0 & \text{if } n=1,2,\\ -\Big(\dfrac{2}{m}\Big)2^{n+1}\sqrt{2} & \text{if } n\ge 3;\end{cases}$$

$$\text{(v)}\ \ G(4,4,5;m;2^n)=\begin{cases}0 & \text{if } n=1,5,\\ 8\Big(1+\Big(\dfrac{-1}{m}\Big)i\Big) & \text{if } n=2,\\ -16\sqrt{2}\Big(\dfrac{2}{m}\Big)\Big(1+\Big(\dfrac{-1}{m}\Big)i\Big) & \text{if } n=3,\\ 64\Big(1+\Big(\dfrac{-1}{m}\Big)i\Big) & \text{if } n=4,\\ \Big(\dfrac{-1}{m}\Big)2^{n+3}i & \text{if } n\geq 6;\end{cases}$$

$$\text{(vi)}\ \ G(5,2,5;m;2^n)=\begin{cases}0 & \text{if } n=1,4,\\ 8\Big(1+\Big(\dfrac{-1}{m}\Big)i\Big) & \text{if } n=2,\\ -16\sqrt{2}\Big(\dfrac{2}{m}\Big)\Big(1+\Big(\dfrac{-1}{m}\Big)i\Big) & \text{if } n=3,\\ (-1)^n\Big(\dfrac{2}{m}\Big)2^{n+2}\sqrt{2} & \text{if } n\geq 5.\end{cases}$$

**Proof.** (i) Here we choose $(a,b,c)=(3,2,2)$ so $ac-(b/2)^2=5$. Thus $l=0$ and $h=5$. By Theorem 1.2 we have

$$G(2,2,3;m;2^n)=\begin{cases}0 & \text{if } n=1,\\ \Big(\dfrac{2}{5}\Big)^n(1+i^{3m})(1+i^{15m})2^n & \text{if } n\geq 2.\end{cases}$$

Now by (1.24) we have

$$(1+i^{3m})(1+i^{15m})=\Big(\frac{-1}{3m}\Big)2i=-\Big(\frac{-1}{m}\Big)2\sqrt{-1}$$

so

$$\begin{aligned}G(2,2,3;m;2^n) &= \Big(\frac{2}{5}\Big)^n(1+i^{3m})(1+i^{15m})\,2^n\\ &= (-1)^{n+1}\Big(\frac{-1}{m}\Big)2^{n+1}\sqrt{-1}\ \text{ for }\ n\geq 2.\end{aligned}$$

(ii) Here we choose $(a,b,c)=(5,2,2)$ so $ac-(b/2)^2=9$. Thus $l=0$ and $h=9$. By Theorem 1.2 we have

$$G(2,2,5;m;2^n)=\begin{cases}0 & \text{if } n=1,\\ \Big(\dfrac{2}{9}\Big)^n(1+i^{5m})(1+i^{45m})2^n & \text{if } n\geq 2.\end{cases}$$

Now by (1.24) we have

$$(1+i^{5m})(1+i^{45m})=\Big(\frac{-1}{5m}\Big)2i=\Big(\frac{-1}{m}\Big)2\sqrt{-1}$$

so

$$G(2,2,5;m;2^n)=\Big(\frac{-1}{m}\Big)2^{n+1}\sqrt{-1}\ \text{ for }\ \ n\ge 2.$$

(iii) Here we choose $(a,b,c)=(3,2,3)$ so $ac-(b/2)^2=8$. Thus $l=3$ and $h=1$. By Theorem 1.2 we have

$$G(3,2,3;m;2^n) = \begin{cases} 0 & \text{if } n=1,4,\\ (1+i^{3m})2^3 & \text{if } n=2,\\ \Big(\frac{2}{3m}\Big)(1+i^{3m})\,2^{9/2} & \text{if } n=3,\\ \Big(\frac{2}{3m}\Big)(1+i^{3m})^2\,2^{n+(3/2)} & \text{if } n\ge 5,\end{cases}$$

$$= \begin{cases} 0 & \text{if } n=1,4,\\ 8\Big(1-\Big(\frac{-1}{m}\Big)\sqrt{-1}\Big) & \text{if } n=2,\\ -16\Big(\frac{2}{m}\Big)\Big(\sqrt{2}-\Big(\frac{-1}{m}\Big)\sqrt{-2}\Big) & \text{if } n=3,\\ \Big(\frac{-2}{m}\Big)2^{n+2}\sqrt{-2} & \text{if } n\ge 5.\end{cases}$$

(iv) Here we choose $(a,b,c)=(3,2,5)$ so $ac-(b/2)^2=14$. Thus $l=1$ and $h=7$. By Theorem 1.2 we have

$$G(3,2,5;m;2^n) = \begin{cases} 0 & \text{if } n=1,2,\\ \Big(\frac{2}{3m}\Big)\Big(\frac{2}{7}\Big)^{n+1}(1+i^{3m})(1+i^{21m})\,2^{n+(1/2)} & \text{if } n\ge 3,\end{cases}$$

$$= \begin{cases} 0 & \text{if } n=1,2,\\ -\Big(\frac{2}{m}\Big)\,2^{n+(3/2)} & \text{if } n\ge 3,\end{cases}$$

$$= \begin{cases} 0 & \text{if } n=1,2,\\ -\Big(\frac{2}{m}\Big)\,2^{n+1}\sqrt{2} & \text{if } n\ge 3.\end{cases}$$

(v) Here we take $(a,b,c)=(5,4,4)$ so $ac-(b/2)^2=16$. Thus $l=4$ and $h=1$. By Theorem 1.2 we have

$$G(4,4,5;m;2^n) = \begin{cases} 0 & \text{if } n=1,5,\\ 8(1+i^m) & \text{if } n=2,\\ -16\Big(\frac{2}{m}\Big)(1+i^m)\sqrt{2} & \text{if } n=3,\\ 64(1+i^m) & \text{if } n=4,\\ (1+i^m)^2\,2^{n+2} & \text{if } n\ge 6,\end{cases}$$

$$= \begin{cases} 0 & \text{if } n = 1, 5, \\ 8\Big(1 + \Big(\frac{-1}{m}\Big)\sqrt{-1}\Big) & \text{if } n = 2, \\ -16\Big(\frac{2}{m}\Big)\Big(\sqrt{2} + \Big(\frac{-1}{m}\Big)\sqrt{-2}\Big) & \text{if } n = 3, \\ 64\Big(1 + \Big(\frac{-1}{m}\Big)\sqrt{-1}\Big) & \text{if } n = 4, \\ \Big(\frac{-1}{m}\Big)\, 2^{n+3}\sqrt{-1} & \text{if } n \geq 6. \end{cases}$$

(vi) Here we take $(a, b, c) = (5, 2, 5)$ so $ac - (b/2)^2 = 24$. Thus $l = 3$ and $h = 3$. By Theorem 1.2 we have

$$G(5, 2, 5; m; 2^n) = \begin{cases} 0 & \text{if } n = 1, 4, \\ 8(1 + i^{5m}) & \text{if } n = 2, \\ \Big(\frac{2}{5m}\Big)(1 + i^{5m})\, 2^{9/2} & \text{if } n = 3, \\ \Big(\frac{2}{5m}\Big)\Big(\frac{2}{3}\Big)^{n+1}(1 + i^{5m})(1 + i^{15m})\, 2^{n+(3/2)} & \text{if } n \geq 5, \end{cases}$$

$$= \begin{cases} 0 & \text{if } n = 1, 4, \\ 8\Big(1 + \Big(\frac{-1}{m}\Big)\sqrt{-1}\Big) & \text{if } n = 2, \\ -16\Big(\frac{2}{m}\Big)\Big(\sqrt{2} + \Big(\frac{-1}{m}\Big)\sqrt{-2}\Big) & \text{if } n = 3, \\ (-1)^n\Big(\frac{2}{m}\Big)\, 2^{n+2}\sqrt{2} & \text{if } n \geq 5. \end{cases}$$

■

Next we turn to the evaluation of the double Gauss sum $G(a, b, c; m; p^n)$ when $p = 2$ and $b$ is odd. We begin with a lemma.

**Lemma 3.1.** *Let $n, k \in \mathbb{N}$. Let $m \in \mathbb{Z}$ be odd. Let $a \in \mathbb{Z}$. If $n \geq 2k + 2$ then*

$$\sum_{\substack{x = 0 \\ x \equiv 0 \pmod{2^k}}}^{2^n - 1} e^{2\pi i m x^2/2^n} = \Big(\frac{2}{m}\Big)^n (1 + i^m)\, 2^{n/2}$$

*and*

$$\sum_{\substack{x = 0 \\ x \equiv a \pmod{2^k}}}^{2^n - 1} e^{2\pi i m x^2/2^n} = 0 \text{ for } a \not\equiv 0 \pmod{2^k}.$$

**Proof.** We have

$$\sum_{\substack{x = 0 \\ x \equiv 0 \pmod{2^k}}}^{2^n - 1} e^{2\pi i m x^2/2^n} = \sum_{y=0}^{2^{n-k} - 1} e^{2\pi i m y^2/2^{n-2k}}$$

$$\begin{aligned} &= 2^k \sum_{y=0}^{2^{n-2k}-1} e^{2\pi i m y^2/2^{n-2k}} \\ &= 2^k \left(\frac{2}{m}\right)^{n-2k} (1+i^m)\, 2^{(n-2k)/2} \\ &= \left(\frac{2}{m}\right)^n (1+i^m)\, 2^{n/2}, \end{aligned}$$

by (1.3) as $n-2k \geq 2$.

Now let $a \in \mathbb{Z}$ be such that $a \not\equiv 0 \pmod{2^k}$. We have

$$\begin{aligned} \sum_{\substack{x=0 \\ x \equiv a \pmod{2^k}}}^{2^n-1} e^{2\pi i m x^2/2^n} &= \frac{1}{2^k} \sum_{x=0}^{2^n-1} e^{2\pi i m x^2/2^n} \sum_{t=0}^{2^k-1} e^{2\pi i t(x-a)/2^k} \\ &= \frac{1}{2^k} \sum_{t=0}^{2^k-1} e^{-2\pi i a t/2^k} \sum_{x=0}^{2^n-1} e^{\frac{2\pi i m x^2}{2^n} + \frac{2\pi i t x}{2^k}}. \end{aligned}$$

Now

$$\sum_{x=0}^{2^n-1} e^{\frac{2\pi i m x^2}{2^n} + \frac{2\pi i t x}{2^k}} = \sum_{x=0}^{2^n-1} e^{\frac{2\pi i (m x^2 + 2^{n-k} t x)}{2^n}}.$$

As $m$ is odd there is an integer $s$ such that

$$ms \equiv 1 \pmod{2^n}.$$

Hence

$$\begin{aligned} \sum_{x=0}^{2^n-1} e^{2\pi i (m x^2 + 2^{n-k} t x)/2^n} &= \sum_{x=0}^{2^n-1} e^{2\pi i m (x^2 + 2^{n-k} s t x)/2^n} \\ &= \sum_{x=0}^{2^n-1} e^{2\pi i m ((x + 2^{n-k-1} st)^2 - 2^{2n-2k-2} s^2 t^2)/2^n} \\ &= \sum_{x=0}^{2^n-1} e^{2\pi i m (x + 2^{n-k-1} st)^2/2^n} \qquad (\text{as } n \geq 2k+2) \\ &= \sum_{y=0}^{2^n-1} e^{2\pi i m y^2/2^n} \\ &= \left(\frac{2}{m}\right)^n (1+i^m)\, 2^{n/2} \end{aligned}$$

by (1.3). Finally

$$\sum_{\substack{x=0\\ x\equiv a \pmod{2^k}}}^{2^n-1} e^{2\pi i m x^2/2^n} = \left(\frac{2}{m}\right)^n (1+i^m)\, 2^{(n/2)-k} \sum_{t=0}^{2^k-1} e^{-2\pi i a t/2^k} = 0,$$

as $a \not\equiv 0 \pmod{2^k}$. ∎

We now make use of Lemma 3.1 to prove Theorem 1.3.

**Proof of Theorem 1.3.** Define $\alpha \in \mathbb{N}_0$ and $a_1 \in \mathbb{Z}$ with $a_1 \equiv 1 \pmod 2$ by $a = 2^\alpha a_1$. As $a_1 \equiv b \equiv 1 \pmod 2$ there exists an odd integer $w$ such that

$$b \equiv a_1 w \pmod{2^n}$$

so that

$$G(a,b,c;m;2^n) = \sum_{x,y=0}^{2^n-1} e^{2\pi i m(2^\alpha a_1 x^2 + a_1 wxy + cy^2)/2^n}. \tag{3.5}$$

Case (i): $n \le \alpha$. (Here, as $n \in \mathbb{N}$, $\alpha \ge 1$). From (3.5) we obtain

$$\begin{aligned} G(a,b,c;m;2^n) &= \sum_{y=0}^{2^n-1} \Big( \sum_{x=0}^{2^n-1} e^{2\pi i m y(a_1 wx+cy)/2^n} \Big) \\ &= \sum_{y=0}^{2^n-1} \Big( \sum_{z=0}^{2^n-1} e^{2\pi i m y z/2^n} \Big) \quad (\text{as } a_1 w \equiv 1 \pmod 2) \\ &= \sum_{\substack{y=0\\ y\equiv 0 \pmod{2^n}}}^{2^n-1} 2^n \\ &= 2^n = (-1)^{acn} 2^n. \end{aligned}$$

Case (ii): $n = \alpha + 1$. (Here $\alpha \ge 0$). We have from (3.5)

$$\begin{aligned} G(a,b,c;m;2^n) &= \sum_{x,y=0}^{2^{\alpha+1}-1} e^{2\pi i m(2^\alpha a_1 x^2 + a_1 wxy + cy^2)/2^{\alpha+1}} \\ &= \sum_{y=0}^{2^{\alpha+1}-1} \sum_{x=0}^{2^{\alpha+1}-1} (-1)^x e^{2\pi i m y(a_1 wx+cy)/2^{\alpha+1}} \quad (\text{as } a_1 m \equiv 1 (\text{mod } 2)) \\ &= 2 \sum_{y=0}^{2^{\alpha+1}-1} \sum_{\substack{x=0\\ x\equiv 0 \pmod 2}}^{2^{\alpha+1}-1} e^{2\pi i m y(a_1 wx+cy)/2^{\alpha+1}} \\ &\quad - \sum_{y=0}^{2^{\alpha+1}-1} \sum_{x=0}^{2^{\alpha+1}-1} e^{2\pi i m y(a_1 wx+cy)/2^{\alpha+1}} \end{aligned}$$

$$
\begin{aligned}
&= 2\sum_{y=0}^{2^{\alpha+1}-1}\sum_{x=0}^{2^{\alpha}-1} e^{2\pi imy(2a_1wx+cy)/2^{\alpha+1}} \\
&- \sum_{y=0}^{2^{\alpha+1}-1}\sum_{z=0}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} \quad (\text{as } a_1w \equiv 1 (\mathrm{mod}\ 2)) \\
&= 2\sum_{y=0}^{2^{\alpha+1}-1} \sum_{\substack{z=0 \\ z \equiv cy\ (\mathrm{mod}\ 2)}}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} - \sum_{\substack{y=0 \\ y \equiv 0\ (\mathrm{mod}\ 2^{\alpha+1})}}^{2^{\alpha+1}-1} 2^{\alpha+1} \\
&= \begin{cases} 2\displaystyle\sum_{y=0}^{2^{\alpha+1}-1} \sum_{\substack{z=0 \\ z \equiv 0\ (\mathrm{mod}\ 2)}}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} - 2^{\alpha+1} & \text{if } c \equiv 0\ (\mathrm{mod}\ 2), \\ 2\displaystyle\sum_{y=0}^{2^{\alpha+1}-1} \sum_{\substack{z=0 \\ z \equiv y\ (\mathrm{mod}\ 2)}}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} - 2^{\alpha+1} & \text{if } c \equiv 1\ (\mathrm{mod}\ 2). \end{cases}
\end{aligned}
$$

Now,

$$
\sum_{\substack{z=0 \\ z \equiv 0\ (\mathrm{mod}\ 2)}}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} = \sum_{t=0}^{2^{\alpha}-1} e^{2\pi imyt/2^{\alpha}} = \begin{cases} 2^{\alpha} & \text{if } y \equiv 0\ (\mathrm{mod}\ 2^{\alpha}), \\ 0 & \text{if } y \not\equiv 0\ (\mathrm{mod}\ 2^{\alpha}), \end{cases}
$$

and

$$
\begin{aligned}
\sum_{\substack{z=0 \\ z \equiv 1\ (\mathrm{mod}\ 2)}}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} &= \sum_{z=0}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} - \sum_{\substack{z=0 \\ z \equiv 0\ (\mathrm{mod}\ 2)}}^{2^{\alpha+1}-1} e^{2\pi imyz/2^{\alpha+1}} \\
&= \left\{ \begin{array}{ll} 2^{\alpha+1} & \text{if } y \equiv 0\ (\mathrm{mod}\ 2^{\alpha+1}) \\ 0 & \text{if } y \not\equiv 0\ (\mathrm{mod}\ 2^{\alpha+1}) \end{array} \right\} \\
&\quad - \left\{ \begin{array}{ll} 2^{\alpha} & \text{if } y \equiv 0\ (\mathrm{mod}\ 2^{\alpha}) \\ 0 & \text{if } y \not\equiv 0\ (\mathrm{mod}\ 2^{\alpha}) \end{array} \right\} \\
&= \begin{cases} 2^{\alpha} & \text{if } y \equiv 0\ (\mathrm{mod}\ 2^{\alpha+1}), \\ -2^{\alpha} & \text{if } y \equiv 2^{\alpha}\ (\mathrm{mod}\ 2^{\alpha+1}), \\ 0 & \text{if } y \not\equiv 0\ (\mathrm{mod}\ 2^{\alpha}). \end{cases}
\end{aligned}
$$

Thus if $c \equiv 0\ (\mathrm{mod}\ 2)$ we have

$$
\begin{aligned}
G(a,b,c;m;2^n) &= 2 \sum_{\substack{y=0 \\ y \equiv 0\ (\mathrm{mod}\ 2^{\alpha})}}^{2^{\alpha+1}-1} 2^{\alpha} - 2^{\alpha+1} \\
&= 2\big(2^{\alpha}+2^{\alpha}\big) - 2^{\alpha+1}
\end{aligned}
$$

$$= \quad 2^{\alpha+1} = 2^n = (-1)^{acn}\, 2^n;$$

if $c \equiv 1 \pmod 2$ and $\alpha \geq 1$ we have

$$\begin{aligned} G(a,b,c;m;2^n) &= 2 \sum_{\substack{y=0 \\ y \equiv 0 \pmod 2}}^{2^{\alpha+1}-1} \left\{ \begin{array}{ll} 2^\alpha & \text{if } y \equiv 0 \pmod{2^\alpha} \\ 0 & \text{if } y \not\equiv 0 \pmod{2^\alpha} \end{array} \right\} \\ &\quad +2 \sum_{\substack{y=0 \\ y \equiv 1 \pmod 2}}^{2^{\alpha+1}-1} \left\{ \begin{array}{ll} 2^\alpha & \text{if } y \equiv 0 \pmod{2^{\alpha+1}} \\ -2^\alpha & \text{if } y \equiv 2^\alpha \pmod{2^{\alpha+1}} \\ 0 & \text{if } y \not\equiv 0 \pmod{2^\alpha} \end{array} \right\} \\ &\quad -2^{\alpha+1} \\ &= 2 \sum_{\substack{y=0 \\ y \equiv 0 \pmod{2^\alpha}}}^{2^{\alpha+1}-1} 2^\alpha + 2 \cdot 0 - 2^{\alpha+1} \\ &= 2\big(2^\alpha + 2^\alpha\big) - 2^{\alpha+1} \\ &= 2^{\alpha+1} = 2^n = (-1)^{acn}\, 2^n; \end{aligned}$$

and if $c \equiv 1 \pmod 2$ and $\alpha = 0$ (so that $n = 1$) we have

$$G(a,b,c;m;2^n) = 2(1) + 2(-1) - 2 = -2 = (-1)^{acn}\, 2^n.$$

Case (iii): $n \geq \alpha + 2$. (Here $\alpha \geq 0$). Appealing to (3.5) we obtain

$$\begin{aligned} &G(a,b,c;m;2^n) \\ &\quad = \sum_{x,y=0}^{2^n-1} e^{2\pi i m(2^\alpha a_1 x^2 + a_1 wxy + cy^2)/2^n} \\ &\quad = \frac{1}{2^{\alpha+3}} \sum_{y=0}^{2^{n+\alpha+2}-1} \sum_{x=0}^{2^{n+1}-1} e^{2\pi i m(2^\alpha a_1 x^2 + a_1 wxy + cy^2)/2^n} \\ &\quad = \frac{1}{2^{\alpha+3}} \sum_{y=0}^{2^{n+\alpha+2}-1} \sum_{x=0}^{2^{n+1}-1} e^{2\pi i m(2^{2\alpha+2} a_1 x^2 + 2^{\alpha+2} a_1 wxy + 2^{\alpha+2} cy^2)/2^{n+\alpha+2}} \\ &\quad = \frac{1}{2^{\alpha+3}} \sum_{y=0}^{2^{n+\alpha+2}-1} \sum_{x=0}^{2^{n+1}-1} e^{2\pi i m(a_1(2^{\alpha+1}x + wy)^2 + (2^{\alpha+2}c - a_1 w^2)y^2)/2^{n+\alpha+2}} \\ &\quad = \frac{1}{2^{\alpha+3}} \sum_{y=0}^{2^{n+\alpha+2}-1} e^{2\pi i m(2^{\alpha+2}c - a_1 w^2)y^2/2^{n+\alpha+2}} \sum_{x=0}^{2^{n+1}-1} e^{2\pi i m a_1 (2^{\alpha+1}x + wy)^2/2^{n+\alpha+2}}, \end{aligned}$$

that is

$$G(a,b,c;m;2^n)$$

$$= \frac{1}{2^{\alpha+3}} \sum_{y=0}^{2^{n+\alpha+2}-1} e^{2\pi i m(2^{\alpha+2}c - a_1 w^2)y^2/2^{n+\alpha+2}} \sum_{\substack{z=0 \\ z \equiv wy \pmod{2^{\alpha+1}}}}^{2^{n+\alpha+2}-1} e^{2\pi i m a_1 z^2/2^{n+\alpha+2}}. \quad (3.6)$$

In this case $n \geq \alpha + 2$ so that $n + \alpha + 2 \geq 2(\alpha + 1) + 2$. Hence

$$\sum_{\substack{z=0 \\ z \equiv wy \pmod{2^{\alpha+1}}}}^{2^{n+\alpha+2}-1} e^{2\pi i m a_1 z^2/2^{n+\alpha+2}} = 0 \text{ for } y \not\equiv 0 \pmod{2^{\alpha+1}},$$

by Lemma 3.1. Thus, by Lemma 3.1 again, we obtain

$$\begin{aligned}
&G(a,b,c;m;2^n)\\
&= \frac{1}{2^{\alpha+3}} \sum_{\substack{y=0 \\ y \equiv 0 \pmod{2^{\alpha+1}}}}^{2^{n+\alpha+2}-1} e^{2\pi i m(2^{\alpha+2}c - a_1 w^2)y^2/2^{n+\alpha+2}} \Big(\frac{2}{ma_1}\Big)^{n+\alpha+2} (1 + i^{ma_1})\, 2^{(n+\alpha+2)/2}\\
&= \Big(\frac{2}{ma_1}\Big)^{n+\alpha} (1 + i^{ma_1})\, 2^{\frac{n-\alpha}{2}-2} \sum_{z=0}^{2^{n+1}-1} e^{2\pi i m(2^{\alpha+2}c - a_1 w^2)z^2/2^{n-\alpha}}\\
&= \Big(\frac{2}{ma_1}\Big)^{n+\alpha} (1 + i^{ma_1})\, 2^{\frac{n+\alpha}{2}-1} \sum_{z=0}^{2^{n-\alpha}-1} e^{2\pi i m(2^{\alpha+2}c - a_1 w^2)z^2/2^{n-\alpha}}\\
&= \Big(\frac{2}{ma_1}\Big)^{n+\alpha} (1 + i^{ma_1})\, 2^{\frac{n+\alpha}{2}-1} \Big(\frac{2}{m(2^{\alpha+2}c - a_1 w^2)}\Big)^{n-\alpha}\\
&\quad \times (1 + i^{m(2^{\alpha+2}c - a_1 w^2)})\, 2^{(n-\alpha)/2}.
\end{aligned}$$

Now

$$\Big(\frac{2}{m(2^{\alpha+2}c - a_1 w^2)}\Big)^{n-\alpha} = \begin{cases} \Big(\frac{2}{m(a_1 - 4c)}\Big)^n & \text{if } \alpha = 0, \\ \Big(\frac{2}{ma_1}\Big)^{n+\alpha} & \text{if } \alpha \geq 1, \end{cases}$$

and

$$i^{m(2^{\alpha+2}c - a_1 w^2)} = i^{-a_1 m} = -\Big(\frac{-1}{ma_1}\Big)\sqrt{-1}.$$

Thus for $\alpha = 0$ and $n \geq 2$ we have

$$\begin{aligned}
&G(a,b,c;m;2^n)\\
&= \Big(\frac{2}{ma}\Big)^n \Big(1 + \Big(\frac{-1}{ma}\Big)\sqrt{-1}\Big) 2^{(n/2)-1} \Big(\frac{2}{m(a-4c)}\Big)^n \Big(1 - \Big(\frac{-1}{ma}\Big)\sqrt{-1}\Big)\, 2^{n/2}\\
&= \Big(\frac{2}{a(a-4c)}\Big)^n 2^n = \Big(\frac{2}{1+4ac}\Big)^n 2^n = (-1)^{acn}\, 2^n,
\end{aligned}$$

and for $\alpha \geq 1$ and $n \geq \alpha + 2$ we have

$$\begin{aligned} G(a,b,c;m;2^n) &= \Big(\frac{2}{ma_1}\Big)^{n+\alpha}\big(1+\Big(\frac{-1}{ma_1}\Big)\sqrt{-1}\,\big)2^{(n+\alpha)/2-1}\Big(\frac{2}{ma_1}\Big)^{n+\alpha} \\ &\quad \times\big(1-\Big(\frac{-1}{ma_1}\Big)\sqrt{-1}\,\big)\,2^{(n-\alpha)/2} \\ &= 2^n = (-1)^{acn}\,2^n. \end{aligned}$$

This completes the proof of Theorem 1.3. ∎

We conclude this section by determining $G(a,b,c;m;2^n)$ for those binary quadratic forms in Corollary 2.1 with $b$ odd.

**Corollary 3.2.** *Let $n \in \mathbb{N}$. Let $m$ be an odd integer. Then*

$$\begin{aligned} &\text{(i)}\ \ G(1,1,1;m;2^n) = (-1)^n 2^n, \\ &\text{(ii)}\ \ G(1,1,2;m;2^n) = 2^n, \\ &\text{(iii)}\ \ G(1,1,3;m;2^n) = (-1)^n 2^n, \\ &\text{(iv)}\ \ G(1,1,4;m;2^n) = 2^n, \\ &\text{(v)}\ \ G(2,1,2;m;2^n) = 2^n. \end{aligned}$$

**Proof.** This follows immediately from Theorem 1.3. ∎

## 4. Proofs of Theorems 1.4–1.15

We just prove Theorem 1.4 as the remaining theorems can be proved similarly. We first observe that

$$\begin{aligned} N_{p^n}(a,b,c,d,e,f;k) &= \frac{1}{p^n}\sum_{x,y,z,w=0}^{p^n-1}\sum_{m=0}^{p^n-1} e^{2\pi i m(ax^2+bxy+cy^2+dz^2+ezw+fw^2-k)/p^n} \\ &= p^{3n} + \frac{1}{p^n}\sum_{x,y,z,w=0}^{p^n-1}\sum_{m=1}^{p^n-1} e^{2\pi i m(ax^2+bxy+cy^2+dz^2+ezw+fw^2-k)/p^n} \\ &= p^{3n} + \frac{1}{p^n}\sum_{x,y,z,w=0}^{p^n-1}\sum_{r=0}^{n-1}\sum_{\substack{M=1\\ p\nmid M}}^{p^{n-r}-1} e^{2\pi i\, p^r M(ax^2+bxy+cy^2+dz^2+ezw+fw^2-k)/p^n} \\ &= p^{3n} + \frac{1}{p^n}\sum_{r=0}^{n-1}\sum_{\substack{M=1\\ p\nmid M}}^{p^{n-r}-1} e^{-2\pi i M k/p^{n-r}}\sum_{x,y=0}^{p^n-1} e^{2\pi i M(ax^2+bxy+cy^2)/p^{n-r}} \\ &\qquad \times \sum_{z,w=0}^{p^n-1} e^{2\pi i M(dz^2+ezw+fw^2)/p^{n-r}} \end{aligned} \tag{4.1}$$

$$= p^{3n} + \frac{1}{p^n}\sum_{r=0}^{n-1} p^{4r} \sum_{\substack{M=1\\ p\nmid M}}^{p^{n-r}-1} e^{-2\pi iMk/p^{n-r}} G(a,b,c;M;p^{n-r})G(d,e,f;M;p^{n-r}).$$

Noting that $k = p^\alpha K$ with $p \nmid K$, (4.1) becomes

$$N_{p^n}(a,b,c,d,e,f;k) \tag{4.2}$$
$$= p^{3n} + \frac{1}{p^n}\sum_{r=0}^{n-1} p^{4r} \sum_{\substack{M=1\\ p\nmid M}}^{p^{n-r}-1} e^{-2\pi iMK/p^{n-r-\alpha}} G(a,b,c;M;p^{n-r})G(d,e,f;M;p^{n-r}).$$

We need the following two formulas from [1, pp. 1670, 1675].

$$\sum_{\substack{M=1\\ p\nmid M}}^{p^{n-r}-1} e^{-2\pi iMK/p^{n-r-\alpha}} = \begin{cases} p^{n-r} - p^{n-r-1} & \text{if } r \geq n-\alpha, \\ -p^\alpha & \text{if } r = n-\alpha-1, \\ 0 & \text{if } r \leq n-\alpha-2, \end{cases} \tag{4.3}$$

$$\sum_{\substack{M=1\\ 3\nmid M}}^{3^{n-r}-1} \Big(\frac{M}{3}\Big) e^{-2\pi iMK/3^{n-r-\alpha}} = \begin{cases} 0 & \text{if } r \geq n-\alpha, \\ -\Big(\frac{K}{3}\Big)3^\alpha\sqrt{-3} & \text{if } r = n-\alpha-1, \\ 0 & \text{if } r \leq n-\alpha-2. \end{cases} \tag{4.4}$$

First we prove the theorem when $p \neq 2, 3$. By (4.2), (1.2) and Corollary 2.1(vii), we obtain

$$N_{p^n}(1,0,1,2,2,5;k) = p^{3n} + \frac{1}{p^n}\sum_{r=0}^{n-1} p^{4r} \sum_{\substack{M=1\\ p\nmid M}}^{p^{n-r}-1} e^{-2\pi iMK/p^{n-r-\alpha}}$$
$$\times \Big(\Big(\frac{M}{p}\Big)^{n-r} i^{\left(\frac{p^{n-r}-1}{2}\right)^2} p^{\frac{n-r}{2}}\Big)^2 p^{n-r}\Big(\frac{-1}{p}\Big)^{n-r}$$
$$= p^{3n} + p^n\Big(\frac{-1}{p}\Big)^n \sum_{r=0}^{n-1} p^{2r}\Big(\frac{-1}{p}\Big)^r (-1)^{\left(\frac{p^{n-r}-1}{2}\right)^2} \sum_{\substack{M=1\\ p\nmid M}}^{p^{n-r}-1} e^{-2\pi iMK/p^{n-r-\alpha}} \tag{4.5}$$

By substituting (4.3) into (4.5), we obtain

$$N_{p^n}(1,0,1,2,2,5;k) = (p+1)\big(p^{3n-1} - p^{3n-\alpha-2}\big),$$

which is the asserted result.

We now prove the theorem when $p = 3$ and $\alpha = 0$. From (4.2), (1.2) and Corollary 2.1(vii) we obtain

$$N_{3^n}(1,0,1,2,2,5;k) = 3^{3n} + 3^{3n-2}\sqrt{-3}\sum_{M=1}^{2}\Big(\frac{M}{3}\Big)e^{-2\pi iMK/3}. \tag{4.6}$$

By (4.4) and (4.6) we obtain

$$N_{3^n}(1,0,1,2,2,5;k) = 3^{3n} + 3^{3n-1}\Big(\frac{K}{3}\Big),$$

which is the asserted result. Now let $p = 3$ and $\alpha \geq 1$. From (4.2), (1.2) and Corollary 2.1(vii) we obtain

$$N_{3^n}(1,0,1,2,2,5;k) = \quad 3^{3n} + 3^{n+1}\sum_{r=0}^{n-2} 3^{2r} \sum_{\substack{M=1 \\ 3 \nmid M}}^{3^{n-r}-1} e^{-2\pi i MK/3^{n-r-\alpha}}. \tag{4.7}$$

By (4.3) and (4.7) we obtain

$$N_{3^n}(1,0,1,2,2,5;k) = 4(3^{3n-1} - 3^{3n-1-\alpha}),$$

which is the asserted result.

We now prove the theorem when $p = 2$ and $\alpha = 0$. From (4.2), (1.3) and Corollary 3.1(ii) we obtain

$$N_{2^n}(1,0,1,2,2,5;k) = 2^{3n} - 2^{n+2}\sum_{r=0}^{n-2} 2^{2r} \sum_{\substack{M=1 \\ 2 \nmid M}}^{2^{n-r}-1} e^{-2\pi i MK/2^{n-r}}. \tag{4.8}$$

By (4.3) and (4.8) we obtain

$$N_{2^n}(1,0,1,2,2,5;k) = 2^{3n},$$

which is the asserted result. Now let $p = 2$ and $\alpha \geq 1$. From (4.2), (1.3) and Corollary 3.1(ii) we obtain

$$N_{2^n}(1,0,1,2,2,5;k) = 2^{3n} - 2^{n+2}\sum_{r=0}^{n-2} 2^{2r} \sum_{\substack{M=1 \\ 2 \nmid M}}^{2^{n-r}-1} e^{-2\pi i MK/2^{n-r-\alpha}}. \tag{4.9}$$

By (4.3) and (4.9) we obtain

$$N_{2^n}(1,0,1,2,2,5;k) = 3 \cdot 2^{3n-\alpha},$$

which is the asserted result.

## References


[1] 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 $2x^2 + 3y^2 + 6z^2 + 6t^2$, *Int. J. Number Theory* 8 (2012), no. 7, 1661–1686.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, Gauss and Jacobi Sums, *Canad. Math. Soc. Ser. of Monographs and Adv. Texts*, John Wiley & Sons, Inc., New York, 1998.