Number of Non-negative Integer Solutions of the Equation $ax + by + cz = n$
and its Relation with Quadratic Residues

Damanvir Singh Binner
Department of Mathematics, Simon Fraser University
8888 University Dr, Burnaby, BC V5A 1S6
dbinner@sfu.ca

Abstract
In 2000, A. Tripathi [7] used generating functions to obtain a formula for the number of non-negative solutions $(x, y)$ of the equation $ax + by = n$ where $a$, $b$ and $n$ are given positive integers. We generalize this procedure for the number of solutions of the equation $ax + by + cz = n$. The formula leads us to a surprising connection between the number of solutions of the equation $ax + by + cz = n$ and quadratic residues. As a consequence of our work, we are able to prove the equivalence between two fundamental results by Gauss and Sylvester in the nineteenth century which are generally viewed to be independent.

1 Introduction
Let $a, b, c$ and $n$ be given positive integers. The purpose of this note is to calculate the number of solutions $N(a, b, c; n)$ of the equation $ax + by + cz = n$ in non-negative integer tuples $(x, y, z)$. Note that if gcd$(a, b, c)$ does not divide $n$, then the equation cannot have any solutions and if it does divide $n$, then we can divide both sides of the equation by this common factor. Thus without loss of generality, we can assume that gcd$(a, b, c) = 1$. We will first show that there is also no loss of generality in making the assumption that $a$, $b$ and $c$ are pairwise coprime. This will allow us to use generating functions to find an explicit formula for the number of solutions. In Section 3 of this note, we establish the equivalence between two well-known results of Gauss and Sylvester which are as follows:

**Theorem 1** (Gauss (1808)). For distinct odd primes $p$ and $q$,

$$
\sum_{i=1}^{\lfloor p-1 \rfloor} \lfloor \frac{iq}{p} \rfloor + \sum_{i=1}^{\lfloor q-1 \rfloor} \lfloor \frac{ip}{q} \rfloor = \frac{(p-1)(q-1)}{4},
$$

**Theorem 2** (Sylvester (1882)). If $p$ and $q$ are distinct odd prime numbers, the number of natural numbers which cannot be expressed in the form $px + qy$ for non-negative integers $x$ and $y$ is equal to $\frac{(p-1)(q-1)}{2}$.

Theorem 1 was proved in [3]. Gauss used it to give his third proof of the law of quadratic reciprocity. Eisenstein [2] gave a geometric proof of Theorem 1 in 1844. For more information about these classical proofs, see [1]. Theorem 2 is a special case of a result proved in [3]. In the general case, $p$ and $q$ just need to be coprime natural numbers instead of distinct odd primes. An easy proof can be found in [6].

Throughout this note, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to $x$. 


2 The Main Theorem

2.1 Reduction to pairwise coprime case

Let \( a, b, c \) and \( n \) be positive integers and as justified above, assume \( \gcd(a, b, c) = 1 \). We define the following symbols:

- Let \( g_1, g_2 \) and \( g_3 \) denote \( \gcd(b, c), \gcd(c, a) \) and \( \gcd(a, b) \) respectively. Note that \( \gcd(g_1, g_2) = \gcd(g_2, g_3) = \gcd(g_3, g_1) = 1 \).
- Let \( a_1, b_2 \) and \( c_3 \) denote the modular inverse of \( a \) with respect to the modulus \( g_1 \), \( b \) with respect to the modulus \( g_2 \) and \( c \) with respect to the modulus \( g_3 \) respectively.
- Let \( n_1, n_2 \) and \( n_3 \) denote the remainder upon dividing \( na_1 \) by \( g_1 \), \( nb_2 \) by \( g_2 \) and \( nc_3 \) by \( g_3 \) respectively.
- Let \( A = \frac{a}{g_2 g_3}, B = \frac{b}{g_3 g_1} \) and \( C = \frac{c}{g_1 g_2} \).
- Define \( N = \frac{n-a_1 c_3 b_2 - b_1 c_2 n_3}{g_1 g_2 g_3} \). Note that \( N \) is an integer.

**Lemma 3.** With the above notation, the number of solutions of the equation \( ax+by+cz = n \) in non-negative integer tuples \((x, y, z)\) is equal to the number of solutions of the equation \( Ax+By+Cz = N \).

**Proof.** Let \( S \) and \( T \) denote the solution sets of \( ax+by+cz = n \) and \( Ax+By+Cz = N \) respectively. Then the function \( \phi : S \to T \) such that

\[
(x, y, z) \mapsto \left(\frac{x - n_1}{g_1}, \frac{y - n_2}{g_2}, \frac{z - n_3}{g_3}\right)
\]

provides the required bijection. \(\square\)

Since \( A, B \) and \( C \) are pairwise coprime positive integers, Lemma 3 shows that there is no loss of generality in making the assumption that \( a, b \) and \( c \) are pairwise coprime.

2.2 Statement of Theorem and Proof

As justified above, we assume \( \gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1 \). We define a few other symbols:

- Define \( b'_1 \) such that \( b'_1 \equiv -nb^{-1} \pmod{a} \) with \( 1 \leq b'_1 \leq a \). Moreover define \( c'_1 \) such that \( c'_1 \equiv bc^{-1} \pmod{a} \) with \( 1 \leq c'_1 \leq a \).
- Define \( c'_2 \) such that \( c'_2 \equiv nc^{-1} \pmod{b} \) with \( 1 \leq c'_2 \leq b \). Moreover define \( a'_2 \) such that \( a'_2 \equiv ca^{-1} \pmod{b} \) with \( 1 \leq a'_2 \leq b \).
- Define \( a'_3 \) such that \( a'_3 \equiv -na^{-1} \pmod{c} \) with \( 1 \leq a'_3 \leq c \). Moreover define \( b'_3 \) such that \( b'_3 \equiv ab^{-1} \pmod{c} \) with \( 1 \leq b'_3 \leq c \).
- \( N_1 = n(n+a+b+c)+abb'_1(a+1-c'_1(b'_1-1))+acc'_2(b+1-a'_2(c'_2-1))+baa'_3(c+1-b'_3(a'_3-1)) \).

**Theorem 4.** With the notation above, the number of solutions of the equation \( ax+by+cz = n \) with \( \gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1 \) is given by

\[
N(a, b, c; n) = \frac{N_1}{2abc} + \sum_{i=1}^{b'_1-1} \left\lfloor \frac{ic'_1}{a} \right\rfloor + \sum_{i=1}^{c'_2-1} \left\lfloor \frac{ia'_2}{b} \right\rfloor + \sum_{i=1}^{a'_3-1} \left\lfloor \frac{ib'_3}{c} \right\rfloor - 2.
\]
Proof. By elementary combinatorics, we know that the number of solutions of \(ax + by + cz = n\) is equal to the coefficient of \(x^n\) in
\[
\frac{1}{(1 - x^a)(1 - x^b)(1 - x^c)}.
\]
Let \(\zeta_m\) denote \(e^{\frac{2\pi i}{m}}\). We know that
\[
(1 - x^a)(1 - x^b)(1 - x^c) = (1 - x)^3 \prod_{k=1}^{a-1} (1 - \zeta_a^{-k} x) \prod_{k=1}^{b-1} (1 - \zeta_b^{-k} x) \prod_{k=1}^{c-1} (1 - \zeta_c^{-k} x).
\]
Note that because \(a, b\) and \(c\) are pairwise coprime, \(1 - \zeta_a^{-k} x, 1 - \zeta_b^{-k} x\) and \(1 - \zeta_c^{-k} x\) are distinct for all values of \(k\). Thus we obtain the following partial fraction decomposition:
\[
\frac{1}{(1 - x^a)(1 - x^b)(1 - x^c)} = \frac{c_1}{1 - x} + \frac{c_2}{(1 - x)^2} + \frac{c_3}{(1 - x)^3} + \sum_{k=1}^{a-1} A_k (1 - \zeta_a^{-k} x) + \sum_{k=1}^{b-1} B_k (1 - \zeta_b^{-k} x) + \sum_{k=1}^{c-1} C_k (1 - \zeta_c^{-k} x).
\]
On comparing the coefficients of \(x^n\) on both sides of (1), we find
\[
N(a, b, c; n) = c_1 + (n + 1)c_2 + \frac{(n + 2)(n + 1)}{2} c_3 + \sum_{k=1}^{a-1} A_k \zeta_a^{-nk} + \sum_{k=1}^{b-1} B_k \zeta_b^{-nk} + \sum_{k=1}^{c-1} C_k \zeta_c^{-nk}.
\]
If we substitute \(x = 0\) in (1), we get
\[
1 = c_1 + c_2 + c_3 + \sum_{k=1}^{a-1} A_k + \sum_{k=1}^{b-1} B_k + \sum_{k=1}^{c-1} C_k.
\]
Upon subtracting (3) from (2) to cancel \(c_1\) and thus simplify our calculation, we get
\[
N(a, b, c; n) - 1 = nc_2 + \frac{n(n + 3)}{2} c_3 - \sum_{k=1}^{a-1} A_k (1 - \zeta_a^{-nk}) - \sum_{k=1}^{b-1} B_k (1 - \zeta_b^{-nk}) - \sum_{k=1}^{c-1} C_k (1 - \zeta_c^{-nk}).
\]
The usual procedure for finding coefficients of partial fraction gives
\[
c_3 = \frac{1}{abc}, c_2 = \frac{a + b + c - 3}{2abc},
\]
\[
A_k = \frac{1}{a(1 - \zeta_a^{-bk})(1 - \zeta_a^{ck})}, B_k = \frac{1}{b(1 - \zeta_b^{-ck})(1 - \zeta_b^{ak})} \text{ and } C_k = \frac{1}{c(1 - \zeta_c^{-ak})(1 - \zeta_c^{bk})}.
\]
Substituting these back in (4), we have
\[
N(a, b, c; n) = \frac{n(n + a + b + c)}{2abc} + 1 - \left( \frac{S_1}{a} + \frac{S_2}{b} + \frac{S_3}{c} \right),
\]
where
\[
S_1 = \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{-nk}}{(1 - \zeta_a^{-bk})(1 - \zeta_a^{ck})}, S_2 = \sum_{k=1}^{b-1} \frac{1 - \zeta_b^{-nk}}{(1 - \zeta_b^{-ck})(1 - \zeta_b^{ak})} \text{ and } S_3 = \sum_{k=1}^{c-1} \frac{1 - \zeta_c^{-nk}}{(1 - \zeta_c^{-ak})(1 - \zeta_c^{bk})}.
\]
Equations similar to (5) have been known before in the pairwise coprime case (see, for example [1]). They do not solve these sums explicitly but express them as summations of some complicated...
sums, products and quotients of trigonometric functions which could be solved for small values of \(a, b\) and \(c\). However, the summations become intractable as \(a, b\) or \(c\) become slightly large. In this paper, we would express the number of solutions in terms of summations of floor functions which are quite easy to work with, particularly with the help of Lemma 5 that we would describe in the next section.

Next, we find \(S_1, S_2\) and \(S_3\). By definition of \(b'_1\), we have \(bb'_1 \equiv -n \pmod{a}\), so \(\zeta_a^{-nk} = \zeta_a^{bb'_1 k}\), and thus

\[
S_1 = \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{bb'_1 k}}{(1 - \zeta_a^k)(1 - \zeta_a^{ck})} = \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{bb'_1 k}}{(1 - \zeta_a^k) \zeta_a^{ck}} = \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{bb'_1 k}}{(1 - \zeta_a^k) \zeta_a^{ck}} - \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{bb'_1 k}}{(1 - \zeta_a^{ck}) \zeta_a^k}.
\]  

(6)

It is well known that

\[
\sum_{k=1}^{a-1} \frac{1}{1 - \zeta_a^k} = \frac{a - 1}{2},
\]

and thus changing the order of summations yields

\[
\sum_{k=1}^{a-1} \frac{1}{1 - \zeta_a^k} = b'_1 \left(\frac{a - 1}{2}\right).
\]  

(7)

By definition of \(c'_1\), we have \(cc'_1 \equiv b \pmod{a}\), so \(\zeta_a^{-nk} = \zeta_a^{jcc'_1 k}\) and thus

\[
\sum_{k=1}^{a-1} \frac{1 - \zeta_a^{jcc'_1 k}}{(1 - \zeta_a^k)(1 - \zeta_a^{ck})} = \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{jcc'_1 k}}{(1 - \zeta_a^k) \zeta_a^{ck}} = \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{jcc'_1 k}}{(1 - \zeta_a^{ck}) \zeta_a^k} = \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{jcc'_1 k}}{(1 - \zeta_a^{ck}) \zeta_a^k} - \sum_{k=1}^{a-1} \frac{1 - \zeta_a^{jcc'_1 k}}{(1 - \zeta_a^{ck}) \zeta_a^k}.
\]  

(8)

From (6), (7) and (8), we get that

\[
S_1 = b'_1 \left(\frac{a - 1}{2}\right) - \sum_{k=1}^{a-1} \sum_{j=1}^{b'_1 - 1} \sum_{l=0}^{c'_1 - 1} \zeta_a^l.
\]

(9)

Now,

\[
\sum_{k=1}^{a-1} \sum_{j=1}^{b'_1 - 1} \sum_{l=0}^{c'_1 - 1} \zeta_a^l = \sum_{j=1}^{b'_1 - 1} \sum_{l=0}^{c'_1 - 1} \sum_{k=1}^{a-1} \zeta_a^l = \sum_{j=1}^{b'_1 - 1} \sum_{l=0}^{c'_1 - 1} \sum_{k=1}^{a-1} \sum_{l=0}^{c'_1 - 1} \zeta_a^l - \frac{c'_1 b'_1 (b'_1 - 1)}{2}.
\]  

(10)

We know that \(\sum_{k=0}^{a-1} \zeta_a^l \neq 0\) only if \(a\) divides \(l\) in which case the sum is \(a\). Note that here we have again used the fact that \(\gcd(a, c) = 1\). Therefore,

\[
\sum_{k=0}^{a-1} \sum_{l=0}^{c'_1 - 1} \zeta_a^l = a \left(\left\lfloor \frac{jc'_1 - 1}{a} \right\rfloor + 1\right) = a \left(\left\lfloor \frac{jc'_1}{a} \right\rfloor + 1\right).
\]

In the last step we have used that \(\gcd(a, c'_1) = 1\) and that \(j \leq b'_1 - 1 \leq a - 1\). Hence,

\[
\sum_{j=1}^{b'_1 - 1} \sum_{l=0}^{c'_1 - 1} \sum_{k=0}^{a-1} \zeta_a^l = a \sum_{j=1}^{b'_1 - 1} \left(\left\lfloor \frac{jc'_1}{a} \right\rfloor + 1\right).
\]  

(11)
From (9), (10) and (11), we have

\[
S_1 = b_1' \left( \frac{a - 1}{2a} \right) + \frac{c_1' b_1'(b_1' - 1)}{2a} - \sum_{j=1}^{b_1' - 1} \left\lfloor \frac{j c_1'}{a} \right\rfloor - (b_1' - 1).
\]

We combine the first and the last terms to get

\[
S_1 = c_1' b_1' \left( b_1' - 1 \right) 2a - b_1' - 1 - \sum_{j=1}^{b_1' - 1} \left\lfloor \frac{j c_1'}{a} \right\rfloor + 1.
\] (12)

Symmetrically, we also have

\[
S_2 = a_2' a_2' \left( a_2' - 1 \right) 2b - a_2' - 1 - \sum_{j=1}^{a_2' - 1} \left\lfloor \frac{j a_2'}{b} \right\rfloor + 1 - a_2' \left( b + 1 \right) 2b,
\] (13)

and

\[
S_3 = b_3' a_3' \left( a_3' - 1 \right) 2c - b_3' - 1 - \sum_{j=1}^{a_3' - 1} \left\lfloor \frac{j b_3'}{c} \right\rfloor + 1 - a_3' \left( c + 1 \right) 2c.
\] (14)

The result now follows from (5), (12), (13) and (14).

### 2.3 An algorithm to find these sums

To be able to calculate the number of solutions faster, we need better methods to calculate these summations involving floor functions. Let us recall Theorem 1 which states that for distinct odd primes \( p \) and \( q \),

\[
\sum_{i=1}^{p-1} \left\lfloor \frac{i q}{p} \right\rfloor + \sum_{i=1}^{q-1} \left\lfloor \frac{i p}{q} \right\rfloor = (p-1)(q-1)/4.
\]

It turns out that we can generalize this result for arbitrary numerator and denominator.

**Lemma 5.** Let \( a, b, c \) and \( K \) be positive integers such that \( b < a, c < a, \gcd(a,c) = 1 \) and \( K = \left\lfloor \frac{bc}{a} \right\rfloor \). Then

\[
\sum_{i=1}^{b} \left\lfloor \frac{ic}{a} \right\rfloor + \sum_{i=1}^{K} \left\lfloor \frac{ia}{c} \right\rfloor = bK.
\]

**Proof.** We have

\[
\sum_{i=1}^{b} \left\lfloor \frac{ic}{a} \right\rfloor = \sum_{i=1}^{K} tn_i,
\]

where \( n_i \) is the number of \( i \) such that \( 1 \leq i \leq b \) and \( \left\lfloor \frac{ic}{a} \right\rfloor = t \). Clearly \( n_t = \left\lfloor \frac{(t+1)a}{c} \right\rfloor - \left\lfloor \frac{ta}{c} \right\rfloor \) if \( t < K \) and \( n_K = b - \left\lfloor \frac{Ka}{c} \right\rfloor \). Therefore,

\[
\sum_{i=1}^{b} \left\lfloor \frac{ic}{a} \right\rfloor = \sum_{t=1}^{K-1} \left( \left\lfloor \frac{(t+1)a}{c} \right\rfloor - \left\lfloor \frac{ta}{c} \right\rfloor \right) t + \left( b - \left\lfloor \frac{Ka}{c} \right\rfloor \right) K.
\]
We rearrange the terms and solve the summation using telescoping sums to obtain
\[
\sum_{i=1}^{b} \left\lfloor \frac{ic}{a} \right\rfloor = \sum_{t=1}^{K-1} \left( \left\lfloor \frac{(t+1)a}{c} \right\rfloor (t+1) - \left\lfloor \frac{ta}{c} \right\rfloor t \right) - \sum_{t=1}^{K-1} \left\lfloor \frac{(t+1)a}{c} \right\rfloor + bK - K \left\lfloor \frac{Ka}{c} \right\rfloor.
\]
By canceling terms and solving, we get the required result.

Lemma 5 is helpful to calculate summations of the form \( \sum_{i=1}^{b} \left\lfloor \frac{ic}{a} \right\rfloor \) because it reduces to a summation of the same form with a lower upper limit of summation and a lower denominator. We shall see in Section 2.5 that after two applications of this lemma, the upper limit of summation and the denominator both reduce to less than half while the numerator is still less than the denominator.

Remark 6. Observe that if we take \( a = p, b = \frac{p-1}{2} \) and \( c = q \) in Lemma 5, then we get Theorem 1. Similarly to Eisenstein’s proof of Theorem 1 (see [2] or [1] for details), we can also give a geometric proof of Lemma 5 by counting the number of points under the straight line \( y = cax \).

Let us describe the algorithm for finding the number of solutions \( N(a, b, c; n) \) of the equation \( ax + by + cz = n \).

1. Reduce the given equation to an equation with \( \gcd(a, b, c) = 1 \) as described in Section 1. Then reduce it to the pairwise coprime case as described in Section 2.1.

2. Apply the formula in Theorem 4 to get the number of solutions in terms of the three summations involving floor functions.

3. Suppose the first summation looks like \( \sum_{i=1}^{b_1} \left\lfloor \frac{ia}{c_1} \right\rfloor \) for some positive integers \( a_1, b_1 \) and \( c_1 \) such that \( b_1 < a_1, c_1 < a_1 \). Then we apply Lemma 5 to get the summation in terms of the summation \( \sum_{i=1}^{K_1} \left\lfloor \frac{ia_1}{c_1} \right\rfloor \), where \( K_1 = \left\lfloor \frac{b_1 c_1}{a_1} \right\rfloor \).

4. Now we have the summation \( \sum_{i=1}^{K_1} \left\lfloor \frac{ia_1}{c_1} \right\rfloor \). Note that we cannot apply Lemma 5 again to find this sum since \( a_1 > c_1 \). However, by division algorithm, we have \( a_1 = c_1 q + r \) for some quotient \( q \) and remainder \( r \). Then \( \sum_{i=1}^{K} \left\lfloor \frac{ia_1}{c_1} \right\rfloor = \frac{qK(K+1)}{2} + \sum_{i=1}^{K} \left\lfloor \frac{ir}{c_1} \right\rfloor \). Since \( r < c_1 \), we can use Lemma 5 again to find this sum.

5. Keep repeating Steps 4 and 5 till the first summation in Step 3 is fully solved. Then follow the same procedure to find the other two summations and hence the number of solutions.

2.4 An example

Let us apply this algorithm to an example. Consider the equation
\[
4452x + 8030y + 9945z = 3857942.
\]
Let \( N \) denote the number of solutions of this equation. Note that \( \gcd(4452, 8030) = 2, \gcd(4452, 9945) = 3 \) and \( \gcd(8030, 9945) = 5 \). If we apply the reduction to coprime case as in Lemma 3 we get that the number of solutions of the above equation is equal to the number of solutions of the equation
\[
742x + 803y + 663z = 128598.
\]
Now we apply the formula of Theorem 4 to get

\[ N = 129 \sum_{i=1}^{129} \left\lfloor \frac{281i}{742} \right\rfloor + 539 \sum_{i=1}^{539} \left\lfloor \frac{621i}{803} \right\rfloor + 335 \sum_{i=1}^{335} \left\lfloor \frac{602i}{663} \right\rfloor - 166300. \] (15)

In order to solve the first sum, we apply Lemma 5 to get

\[ 129 \sum_{i=1}^{129} \left\lfloor \frac{281i}{742} \right\rfloor = 6192 - 48 \sum_{i=1}^{48} \left\lfloor \frac{742i}{281} \right\rfloor. \] (16)

Now,

\[ 48 \sum_{i=1}^{48} \left\lfloor \frac{742i}{281} \right\rfloor = \sum_{i=1}^{48} \left( 2i + \left\lfloor \frac{180i}{281} \right\rfloor \right) = 2352 + \sum_{i=1}^{48} \left\lfloor \frac{180i}{281} \right\rfloor. \] (17)

Another application of Lemma 5 gives

\[ 48 \sum_{i=1}^{48} \left\lfloor \frac{180i}{281} \right\rfloor = 1440 - \sum_{i=1}^{30} \left\lfloor \frac{281i}{180} \right\rfloor = 975 - \sum_{i=1}^{30} \left\lfloor \frac{101i}{180} \right\rfloor. \] (18)

Repeating the above procedure, we have

\[ 30 \sum_{i=1}^{30} \left\lfloor \frac{101i}{180} \right\rfloor = 480 - \sum_{i=1}^{16} \left\lfloor \frac{180i}{101} \right\rfloor = 344 - \sum_{i=1}^{16} \left\lfloor \frac{79i}{101} \right\rfloor, \] (19)

\[ 16 \sum_{i=1}^{16} \left\lfloor \frac{79i}{101} \right\rfloor = 192 - \sum_{i=1}^{12} \left\lfloor \frac{101i}{79} \right\rfloor = 114 - \sum_{i=1}^{12} \left\lfloor \frac{22i}{79} \right\rfloor, \] (20)

\[ 12 \sum_{i=1}^{12} \left\lfloor \frac{22i}{79} \right\rfloor = 36 - \sum_{i=1}^{3} \left\lfloor \frac{79i}{22} \right\rfloor = 18 - \sum_{i=1}^{3} \left\lfloor \frac{13i}{22} \right\rfloor, \] (21)

and

\[ 3 \sum_{i=1}^{3} \left\lfloor \frac{13i}{22} \right\rfloor = 3 - \sum_{i=1}^{1} \left\lfloor \frac{22i}{13} \right\rfloor = 3 - 1 = 2. \] (22)

From (16) to (22), we get

\[ \sum_{i=1}^{129} \left\lfloor \frac{281i}{742} \right\rfloor = 3111. \]

Repeating the same procedure with the other two summations leads to

\[ \sum_{i=1}^{539} \left\lfloor \frac{621i}{803} \right\rfloor = 112277, \]

and

\[ \sum_{i=1}^{335} \left\lfloor \frac{602i}{663} \right\rfloor = 50934. \]

Substituting these values back in (15), we find \( N = 22 \), i.e., there are 22 solutions for the equation \( 4452x + 8030y + 9945z = 3857942 \) in non-negative tuples \((x, y, z)\).
2.5 Efficiency of the algorithm

We want to find an upper bound for the number of steps required to calculate the number of solutions of the equation $ax + by + cz = n$. Suppose we want to find the sum $\sum_{i=1}^{b} \left\lfloor \frac{ic_1}{a_1} \right\rfloor$ for some positive integers $a_1$, $b$ and $c_1$ such that $b < a_1, c_1 < a_1$ and $\gcd(c_1, a_1) = 1$.

According to Step 4 of the algorithm, we need to apply Lemma 2 to get $\sum_{i=1}^{b} \left\lfloor \frac{ic_1}{a_1} \right\rfloor$ in terms of the sum $\sum_{i=1}^{K_1} \left\lfloor \frac{ia_1}{c_1} \right\rfloor$ for some $K_1 < c_1$. Then as step 5 in the algorithm describes, we need to apply the division algorithm $a_1 = c_1 q_1 + a_2$ where $a_2 < c_1$. Since $\gcd(c_1, a_1) = 1$, so $\gcd(a_2, c_1) = 1$. Note that since $c_1 < a_1$, so $q \geq 1$ and thus

$$a_1 \geq c_1 + a_2 > 2a_2,$$

or equivalently $a_2 < \frac{a_1}{2}$. With the help of this division algorithm, the sum $\sum_{i=1}^{K_1} \left\lfloor \frac{ia_1}{c_1} \right\rfloor$ can be obtained in terms of the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ia_2}{c_2} \right\rfloor$.

According to step 5 of the algorithm, we again apply Lemma 5 to get the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ia_2}{c_2} \right\rfloor$ in terms of the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ia_2}{c_2} \right\rfloor$ for some $K_2 < a_2$. Then we again apply division algorithm $c_1 = a_2 q_2 + c_2$ for some $c_2 < a_2$ to get the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ia_2}{c_2} \right\rfloor$ in terms of the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ia_2}{c_2} \right\rfloor$. Since $\gcd(a_2, c_1) = 1$, so $\gcd(c_2, a_2) = 1$. Finally, since $K_2 < a_2, c_2 < a_2$ and $\gcd(c_2, a_2) = 1$, we return to Step 4 of the algorithm to find the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ia_2}{c_2} \right\rfloor$.

Thus with one application of the Steps 4 and 5 of the algorithm (i.e. two applications of both Lemma 5 and the division algorithm), we can obtain the sum $\sum_{i=1}^{b} \left\lfloor \frac{ic_1}{a_1} \right\rfloor$ in terms of the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ia_2}{c_2} \right\rfloor$ where $a_2 < \frac{a_1}{2}$. It is also easy to see that $K_2 < \frac{b}{2}$. This makes sure that the Steps 4 and 5 of the algorithm terminate in $O(\log a)$ steps and hence the algorithm terminates in $O(\log t)$ steps where $t = \max(a, b, c)$.

2.6 Relationship with quadratic residues

Let us recall the Eisenstein’s Lemma which states that for given odd distinct primes $p$ and $q$, the quadratic residue is given by $\left( \frac{a}{p} \right) = (-1)^t$, where $t = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{aq}{p} \right\rfloor$.

Thus the quadratic residues are related to some summations with which we have been dealing while attempting to solve the equation $ax + by + cz = n$. This suggests that we might be able to find an equation whose number of solutions gives the quadratic residues.

**Lemma 7.** The number of solutions of the equation $px + qy + z = \frac{q(p-1)}{2}$ is equal to

$$N_{p,q} = \frac{p-1}{2} + \sum_{i=1}^{p-1} \left\lfloor \frac{iq}{p} \right\rfloor.$$

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

**Proof.** Clearly, one way of proving this is by applying Theorem 3. However we could also prove it directly by fixing a $y$ and then calculating the number of possibilities for $x$. For a given $x$ and $y, z$ is automatically determined. \(\Box\)
3 Equivalence between two well-known results

The aim of this section is to establish the equivalence between Theorem 1 and Theorem 2. Throughout this section, \( p \) and \( q \) would denote distinct odd primes.

**Lemma 8.** The number of solutions of the equation \( px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} \) is equal to \( \frac{p(q-1)}{2} + \frac{q(p-1)}{2} + 1 - N_0 \) where \( N_0 \) is the number of natural numbers which cannot be expressed in the form \( px + qy \) such that \( x \) and \( y \) are non-negative integers.

**Proof.** We first fix a \( z \) and then look for the number of solutions of the equation \( px + qy = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} - z \).

Thus the number of solutions of the equation \( px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} \) is equal to

\[
\sum_{n=0}^{p(q-1)\over 2 + q(p-1)\over 2} S_n,
\]

where \( S_n \) is the number of solutions of the equation \( px + qy = n \). Clearly \( S_0 = 1 \). Furthermore, it is well known that whenever \( 1 \leq n \leq (p-1)(q-1) \), \( S_n \) could either be 0 or 1 and whenever \((p-1)(q-1) < n < pq \), \( S_n = 1 \). We also prove these facts in Section 4 using the methods developed in Section 3. Thus by the definition of \( N_0 \),

\[
\sum_{n=1}^{(p-1)(q-1)} S_n = (p-1)(q-1) - N_0,
\]

and,

\[
\sum_{n=(p-1)(q-1)+1}^{p(q-1)\over 2 + q(p-1)\over 2} S_n = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} - (p-1)(q-1).
\]

Therefore,

\[
\sum_{n=0}^{p(q-1)\over 2 + q(p-1)\over 2} S_n = S_0 + \sum_{n=0}^{(p-1)(q-1)} S_n + \sum_{n=(p-1)(q-1)+1}^{p(q-1)\over 2 + q(p-1)\over 2} S_n = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} + 1 - N_0.
\]

\[ \square \]

We calculate the number of solutions of the equation \( px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} \) in another way by considering four separate cases. We recall that \( N_{p,q} \) denotes the number of solutions of the equation \( px + qy + z = \frac{q(p-1)}{2} \).

**Lemma 9.** The number of solutions of the equation \( px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} \) is equal to \( 2(N_{p,q} + N_{q,p}) - \left( \frac{p+1}{2} + \frac{q+1}{2} + 1 \right) \).

**Proof.** Let \( X, Y \) and \( Z \) denote \( \frac{q-1}{2} - x, \frac{p-1}{2} - y \) and \( \frac{q(p-1)}{2} - z \) respectively. We split our calculation into four different cases according to:
1. $X \geq 0, Y \geq 0, Z \geq 0$.
2. $X \geq 0, Y \geq 0, Z < 0$.
3. $X \geq 0, Y < 0$.
4. $X < 0$.

Case 1: Let

$$X \geq 0, Y \geq 0, Z \geq 0.$$ 

Let $S_1$ denote the set of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ in Case 1, and let $T_1$ denote the set of solutions of $px + qy + z = \frac{q(p-1)}{2}$. Then the function $\phi_1 : S_1 \rightarrow T_1$ such that

$$(x, y, z) \mapsto (X, Y, Z)$$

is a bijection. Thus the number of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ in Case 1 is equal to $N_{p,q}$.

Case 2: Let

$$X \geq 0, Y \geq 0, Z < 0.$$ 

Let $S_2$ denote the set of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ such that $X \geq 0$, $Y \geq 0$ and $Z \leq 0$, and let $T_2$ denote the set of solutions of $px + qy + z = \frac{p(q-1)}{2}$. Then the function $\phi_2 : S_2 \rightarrow T_2$ such that

$$(x, y, z) \mapsto (x, y, -Z)$$

is a bijection. However, to calculate the number of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ in Case 2, we need to subtract the solutions in which $Z = 0$, but if $Z = 0$, then the equation becomes $px + qy = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ which has a unique solution $x = \frac{q-1}{2}$ and $y = 0$ because $p$ divides $y$ and $y < p$ together imply $y = 0$. Thus the number of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ in Case 2 is equal to $N_{q,p} - 1$.

Case 3: Let

$$X \geq 0, Y < 0.$$ 

Let $S_3$ denote the set of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ such that $X \geq 0$ and $Y \leq 0$, and let $T_3$ denote the set of solutions of $px + qy + z = \frac{p(q-1)}{2}$. Then the function $\phi_3 : S_3 \rightarrow T_3$ such that

$$(x, y, z) \mapsto (x, -Y, z)$$

is a bijection. However, to calculate the number of solutions of the equation in Case 3, one has to subtract the number of solutions with $Y = 0$, but if $Y = 0$, then the equation becomes $px + z = \frac{p(q-1)}{2}$ which clearly has $\frac{q-1}{2}$ possible values for $x$ and for a given $x$, $z$ is automatically determined. Thus the number of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ in Case 3 is equal to $N_{q,p} - \frac{q-1}{2}$.

Case 4: Let

$$X < 0.$$ 

Let $S_4$ denote the set of solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ such that $X \leq 0$, and let $T_4$ denote the set of solutions of $px + qy + z = \frac{p(q-1)}{2}$. Then the function $\phi_4 : S_4 \rightarrow T_4$ such that

$$(x, y, z) \mapsto (-X, y, z)$$

is a bijection. However, to calculate the number of solutions of the equation in Case 4, one has to subtract the number of solutions with $X = 0$, but if $X = 0$, then the equation becomes $qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$.
which clearly has \( \frac{p+1}{2} \) solutions. Thus the number of solutions of \( px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} \) in Case 4 is equal to \( N_{p,q} - \frac{p+1}{2} \).

Adding up the solutions in all the above cases, we get the required result.

Upon comparing the number of solutions of the equation \( px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2} \) obtained in Lemma 8 and Lemma 9, and then using Lemma 7, we get

\[
N_0 + 2 \left( \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor + \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor \right) = (p-1)(q-1).
\]

This establishes the required equivalence between Theorem 1 and Theorem 2.

4 Some applications of techniques developed in this paper

4.1 Another proof of Theorem 1

In this section, we prove Theorem 1 by counting the number of solutions of an equation in two different ways. Without loss of generality, we can assume \( q < p \). Recall that in Lemma 7 we counted the number of solutions of the equation \( px + qy + z = \frac{q(p-1)}{2} \) with \( q < p \). Now we will count these in another way.

**Lemma 10.** If \( p \) and \( q \) are distinct odd primes such that \( q < p \), then the number of solutions of the equation \( px + qy + z = \frac{q(p-1)}{2} \), with \( q < p \), is given by

\[
N_{p,q} = p + 1 + \frac{(p-1)(q-1)}{4} - \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor.
\]

**Proof.** Maximum possible value for \( x \) is

\[
\left\lfloor \frac{q(p-1)}{2p} \right\rfloor = \left\lfloor \frac{(q-1)}{2} + \frac{p-q}{2p} \right\rfloor = \frac{q-1}{2}.
\]

Now we consider two cases:

Case 1: Let \( x = 0 \). Number of solutions in Case 1 is equal to \( \frac{p+1}{2} \).

Case 2: Let \( x \geq 1 \). Fix \( x = i \). Then the number of possible values for \( y \) is equal to

\[
1 + \left\lfloor \frac{q(p-1)}{2} - \frac{ip}{q} \right\rfloor = \frac{p-1}{2} - \left\lfloor \frac{ip}{q} \right\rfloor.
\]

Hence the total number of solutions in Case 2 is equal to

\[
\sum_{i=1}^{\frac{q-1}{2}} \left( \frac{p-1}{2} - \left\lfloor \frac{ip}{q} \right\rfloor \right) = \frac{(p-1)(q-1)}{4} - \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor.
\]

Adding up the number of solutions in both the cases, we get the required result.

Theorem 1 now easily follows from Lemma 7 and Lemma 10.
4.2 Solving the equation \( ax + by = n \)

If we modify the techniques used in Section 2.1 to reduce the equation \( ax + by + cz = n \) to the pairwise coprime case, we can completely solve the equation \( ax + by = n \). Note that if \( \gcd(a, b) \) does not divide \( n \), then there is no solution and if it does, then we can divide out both sides of the equation by \( \gcd(a, b) \). Thus without loss of generality, we can assume \( \gcd(a, b) = 1 \).

Let \( a^{-1} \) and \( b^{-1} \) denote the modular inverse of \( a \) with respect to \( b \) and \( b^{-1} \) with respect to \( a \) respectively. Further, let \( a_1 \) and \( b_1 \) denote the remainder when \( na^{-1} \) is divided by \( b \) and \( nb^{-1} \) is divided by \( a \) respectively.

**Theorem 11.** Let \( a \) and \( b \) be coprime positive integers and \( n \) is some positive integer. Then the number of solutions of the equation \( ax + by = n \) is given by

\[
N(a, b; n) = 1 + \frac{n - aa_1 - bb_1}{ab}
\]

**Proof.** Let \( S \) and \( T \) denote the solution sets of \( ax + by = n \) and \( x + y = \frac{n - aa_1 - bb_1}{ab} \) respectively. Then the function \( \phi : S \to T \) such that

\[
(x, y) \mapsto \left( \frac{x - a_1}{b}, \frac{y - b_1}{a} \right)
\]

is a bijection. \( \square \)

This formula is equivalent to the one given in [7].

**Corollary 12.** \( ax + by = n \) has a unique solution if \( (a - 1)(b - 1) \leq n < ab \).

**Proof.** If \( n < ab \), then clearly \( N(a, b; n) < 2 \). Moreover, since \( a_1 \leq (b - 1) \) and \( b_1 \leq (a - 1) \), so \( N(a, b; n) \geq \frac{n - a + b - ab}{ab} \). Therefore, if \( (a - 1)(b - 1) \leq n \), then \( N(a, b; n) > 0 \). Thus whenever \( (a - 1)(b - 1) \leq n < ab \), \( N(a, b; n) = 1 \).

Recall that the Frobenius number of a set \( \{a_1, a_2, \ldots, a_l\} \) such that \( \gcd(a_1, a_2, \ldots, a_l) = 1 \) is defined as the largest integer which cannot be expressed in the form

\[
k_1a_1 + k_2a_2 + \cdots + k_la_l
\]

where \( k_1, k_2, \ldots, k_l \) are non-negative integers.

Corollary [12] gives another proof of the fact that the Frobenius number of the set \( \{a, b\} \) such that \( \gcd(a, b) = 1 \) is equal to \( (a - 1)(b - 1) \). For more information about Frobenius numbers and the formula for three variables, see [8].

4.3 A by-product summation result

We can modify the proof of Lemma [10] to obtain the following result:

**Theorem 13.** Let \( p \) and \( q \) be distinct odd primes such that \( p < q \), then

\[
\sum_{i=\frac{q}{2}+\frac{p}{2p}}^{\frac{q}{2}} \left\lfloor \frac{ip}{q} \right\rfloor = \left( \frac{p - 1}{2} \right) \left( \left\lfloor \frac{q - p}{2p} \right\rfloor + 1 \right).
\]

For example, if we take \( p = 23 \) and \( q = 739 \), then \( \left\lfloor \frac{q - p}{2p} \right\rfloor = 15 \), and we get

\[
\sum_{i=354}^{369} \frac{23i}{739} = 176.
\]
4.4 An application of Theorem 1

We want to show that Theorem 1 can be used to determine the parity of the number of solutions of a particular linear equation. Let $p$ and $q$ be distinct odd primes, and let $p^{-1}$ denote the modular inverse of $p$ with respect to $q$. Further, let $k$ denote the quantity \( \left( \frac{p^t}{2} \right) + p \left( \frac{q^t}{2} \right) p^{-1} \).

**Theorem 14.** The number of solutions of the equation

\[
p x + q y + z = k
\]

has the same parity as

\[
(k + 1) \left( \frac{k + p + q}{2} \right) + \left( \frac{q^2 - 1}{8} \right)(1 + p^{-1}) + \frac{(p - 1)(q - 1)}{4}.
\]

**Proof.** By Eisenstein’s Lemma, \( \left( \frac{p}{q} \right) = (-1)^{t_1} \) and \( \left( \frac{p^{-1}}{q} \right) = (-1)^{t_2} \) where \( t_1 = \sum_{i=1}^{q-1} \left\lfloor \frac{ip}{q} \right\rfloor \) and \( t_2 = \sum_{i=1}^{q-1} \left\lfloor \frac{ip^{-1}}{q} \right\rfloor \). Note that

\[
\left( \frac{p}{q} \right) = \left( \frac{p^{-1}}{q} \right).
\]

Therefore, \( \sum_{i=1}^{q-1} \left\lfloor \frac{ip}{q} \right\rfloor \) and \( \sum_{i=1}^{q-1} \left\lfloor \frac{ip^{-1}}{q} \right\rfloor \) have the same parity. The result now follows directly from Theorem 4 and Theorem 1.

5 Acknowledgements

I am highly grateful to A. Tripathi at IIT Delhi who asked me to try to extend his work for 3 variables. Section 2.2 of this note heavily uses the techniques developed in his paper. I also want to thank my friend A. Jain for verifying the reduction process by running a computer program and also for simplifying the expression of $N$ in Section 2.1. I am highly indebted to A. Rattan at SFU Burnaby, J. O. Shallit at the University of Waterloo and A. Ganguli at IISER Mohali for helping me with the presentation of this paper. I also wish to express my gratitude to D. Prasad at TIFR, Mumbai for listening to my work very patiently and giving me encouraging remarks.

References

[1] O. Baumgart. *The Quadratic Reciprocity Law: A Collection of Classical Proofs*. Springer International Publishing, Cham, 2015 edition, 2015.

[2] G. Eisenstein. Geometrischer Beweis des Fundamental theorems für die quadratischen reste. *J. Reine Angew. Math.*, 28:246–248, 1844.

[3] C. F. Gauss. Theorematis arithmetici demonstratio nova. *Comment. Soc. regiae sci. Göttingen*, XVI(69), 1808.

[4] T. Komatsu. On the number of solutions of the Diophantine equation of Frobenius-general case. *Mathematical Communications*, 8(2):195–206, 2003.

[5] J. J. Sylvester. On subvariants, ie semi-invariants to binary quantics of an unlimited order. *American Journal of Mathematics*, 5(1):79–136, 1882.
[6] J. J. Sylvester. Mathematical questions with their solutions. *Educational times*, 41(21):6, 1884.

[7] A. Tripathi. The number of solutions to $ax+by=n$. *Fibonacci Quarterly*, 38(4):290–293, 2000.

[8] A. Tripathi. Formulae for the Frobenius number in three variables. *Journal of Number Theory*, 170:368–389, 2017.