Journal of Integer Sequences, Vol. 23 (2020),
Article 20.6.5

The Number of Solutions to $ax + by + cz = n$ and its Relation to Quadratic Residues

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

Abstract

We develop a formula for the number of non-negative integer solutions (x, y, z) of the equation $ax + by + cz = n$, where a, b, c, and n are given positive integers. The formula leads us to a surprising connection between the number of non-negative integer 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 that are generally viewed as independent.

1 Introduction

Tripathi [7] used generating functions to obtain a formula for the number of non-negative integer solutions (x, y) of the equation $ax + by = n$, where a, b, and n are given positive integers. We generalize this procedure for three variables. Throughout this paper, by solutions of an equation, we mean non-negative integer solutions only. We let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x.

The purpose of this paper is to calculate the number of solutions $N(a, b, c; n)$ of the equation $ax + by + cz = n$ in non-negative integer triples (x, y, z), where a, b, c, and n are given positive integers. Note that if $\gcd(a, b, c)$ does not divide n, then the equation cannot have any solutions; 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 show that there is also no loss of generality in making the assumption that a, b, and c are pairwise coprime. This allows us to use generating functions to find an explicit formula for the number of solutions. Further, we establish the equivalence between the following well-known results of Gauss and Sylvester.

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

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

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

Gauss [3] proved Theorem 1 in 1808, which completed his third proof of the law of quadratic reciprocity. Eisenstein [2] gave a geometric proof of Theorem 1 in 1844. We refer the reader to Baumgart [1, pp. 15–20] for more information about these classical proofs. Sylvester [5] proved a more general version of Theorem 2 in 1882. In the general case, p and q need only be coprime natural numbers instead of being distinct odd primes. In 1883, Sylvester posed the general version of Theorem 2 as a recreational problem for which Curran [6] published a short proof based on generating functions.

We conclude the paper with some further applications of our formula and techniques, including a complete list of non-negative integer solutions of the equation $ax + by = n$.

2 The main theorem

2.1 Reduction to an equation with pairwise coprime coefficients

Let a, b, c, and n be positive integers and, as justified above, we assume that $\gcd(a, b, c) = 1$. 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 inverses 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 remainders 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 $C = \frac{c}{g_1 g_2}$.
- Let $N = \frac{n - an_1 - bn_2 - cn_3}{g_1 g_2 g_3}$. Note that N is an integer.

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

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. □

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.

Remark 4. We briefly describe the motivation behind this bijection. Reducing the equation $ax + by + cz = n$ modulo g_1, g_2, and g_3, gives the congruences $x \equiv n_1 \pmod{g_1}$, $y \equiv n_2 \pmod{g_2}$, and $z \equiv n_3 \pmod{g_3}$, respectively. Thus, we have the expressions $x = n_1 + g_1u$, $y = n_2+g_2v$, and $z = n_3+g_3w$, for some non-negative integers u, v, and w. Substituting these expressions back in the given equation $ax+by+cz = n$, yields the equation $Au+Bv+Cw = N$, which has pairwise coprime coefficients.

2.2 Statement of theorem and proof

As justified above, we may assume that $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1$. We introduce a few more 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 $1 \leq b'_3 \leq c$.
- Define $N_1 = n(n + a + b + c) + cbb'_1(a + 1 - c'_1(b'_1 - 1)) + acc'_2(b + 1 - a'_2(c'_2 - 1))$ $+baa'_3(c + 1 - b'_3(a'_3 - 1))$.

Theorem 5. *Let a, b, c, and n be given positive integers such that $\gcd(a, b) = \gcd(b, c) = \gcd(c, a) = 1$. With the notation above, the number of non-negative integer solutions of the equation $ax + by + cz = n$ 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 non-negative integer 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 ζ_m denote $e^{\frac{2\pi i}{m}}$. We know that

$$(1-x^a)(1-x^b)(1-x^c) = (1-x)^3 \prod_{k=1}^{a-1}(1-\zeta_a^{-k}x) \prod_{k=1}^{b-1}(1-\zeta_b^{-k}x) \prod_{k=1}^{c-1}(1-\zeta_c^{-k}x).$$

Since 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 partial fraction decomposition

$$\begin{aligned}\frac{1}{(1-x^a)(1-x^b)(1-x^c)} = \frac{d_1}{1-x} + \frac{d_2}{(1-x)^2} + \frac{d_3}{(1-x)^3} \\ + \sum_{k=1}^{a-1} \frac{A_k}{1-\zeta_a^{-k}x} + \sum_{k=1}^{b-1} \frac{B_k}{1-\zeta_b^{-k}x} + \sum_{k=1}^{c-1} \frac{C_k}{1-\zeta_c^{-k}x}.\end{aligned} \tag{1}$$

On comparing the coefficients of x^n on both sides of (1), we find

$$N(a,b,c;n) = d_1 + (n+1)d_2 + \frac{(n+2)(n+1)}{2}d_3 + \sum_{k=1}^{a-1} A_k\zeta_a^{-nk} + \sum_{k=1}^{b-1} B_k\zeta_b^{-nk} + \sum_{k=1}^{c-1} C_k\zeta_c^{-nk}. \tag{2}$$

If we substitute $x = 0$ in (1), we get

$$1 = d_1 + d_2 + d_3 + \sum_{k=1}^{a-1} A_k + \sum_{k=1}^{b-1} B_k + \sum_{k=1}^{c-1} C_k. \tag{3}$$

Upon subtracting (3) from (2), we get

$$\begin{aligned}N(a,b,c;n) - 1 = nd_2 + \frac{n(n+3)}{2}d_3 - \sum_{k=1}^{a-1} A_k(1-\zeta_a^{-nk}) \\ - \sum_{k=1}^{b-1} B_k(1-\zeta_b^{-nk}) - \sum_{k=1}^{c-1} C_k(1-\zeta_c^{-nk}).\end{aligned} \tag{4}$$

The usual procedure for finding coefficients of a partial fraction expansion gives the following

equations.

$$\begin{aligned} d_3 &= \frac{1}{abc}, \\ d_2 &= \frac{a+b+c-3}{2abc}, \\ A_k &= \frac{1}{a(1-\zeta_a^{bk})(1-\zeta_a^{ck})}, \\ B_k &= \frac{1}{b(1-\zeta_b^{ck})(1-\zeta_b^{ak})}, \\ C_k &= \frac{1}{c(1-\zeta_c^{ak})(1-\zeta_c^{bk})}. \end{aligned}$$

Substituting these back into (4), we have

$$N(a,b,c;n) = \frac{n(n+a+b+c)}{2abc} + 1 - \left(\frac{S_1}{a} + \frac{S_2}{b} + \frac{S_3}{c}\right), \tag{5}$$

where

$$\begin{aligned} S_1 &= \sum_{k=1}^{a-1} \frac{1-\zeta_a^{-nk}}{(1-\zeta_a^{bk})(1-\zeta_a^{ck})}, \\ S_2 &= \sum_{k=1}^{b-1} \frac{1-\zeta_b^{-nk}}{(1-\zeta_b^{ck})(1-\zeta_b^{ak})}, \end{aligned}$$

and

$$S_3 = \sum_{k=1}^{c-1} \frac{1-\zeta_c^{-nk}}{(1-\zeta_c^{ak})(1-\zeta_c^{bk})}.$$

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,

$$\begin{aligned} S_1 &= \sum_{k=1}^{a-1} \frac{1-\zeta_a^{bb_1'k}}{(1-\zeta_a^{bk})(1-\zeta_a^{ck})} \\ &= \sum_{k=1}^{a-1} \sum_{j=0}^{b_1'-1} \frac{\zeta_a^{jbk}}{1-\zeta_a^{ck}} \\ &= \sum_{k=1}^{a-1} \sum_{j=0}^{b_1'-1} \frac{1}{1-\zeta_a^{ck}} - \sum_{k=1}^{a-1} \sum_{j=0}^{b_1'-1} \frac{1-\zeta_a^{jbk}}{1-\zeta_a^{ck}}. \end{aligned} \tag{6}$$

It is well-known that

$$\sum_{k=1}^{a-1} \frac{1}{1-\zeta_a^{ck}} = \frac{a-1}{2},$$

and thus, changing the order of summations yields

$$\sum_{k=1}^{a-1}\sum_{j=0}^{b_1'-1}\frac{1}{1-\zeta_a^{ck}} = b_1'\left(\frac{a-1}{2}\right). \tag{7}$$

By definition of c_1', we have $cc_1' \equiv b \pmod a$, so $\zeta_a^{jbk} = \zeta_a^{jcc_1'k}$, and thus,

$$\begin{aligned}\sum_{k=1}^{a-1}\sum_{j=0}^{b_1'-1}\frac{1-\zeta_a^{jbk}}{1-\zeta_a^{ck}} &= \sum_{k=1}^{a-1}\sum_{j=1}^{b_1'-1}\frac{1-\zeta_a^{jbk}}{1-\zeta_a^{ck}} \\ &= \sum_{k=1}^{a-1}\sum_{j=1}^{b_1'-1}\frac{1-\zeta_a^{jcc_1'k}}{1-\zeta_a^{ck}} \\ &= \sum_{k=1}^{a-1}\sum_{j=1}^{b_1'-1}\sum_{l=0}^{jc_1'-1}\zeta_a^{lck}.\end{aligned} \tag{8}$$

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

$$S_1 = b_1'\left(\frac{a-1}{2}\right) - \sum_{k=1}^{a-1}\sum_{j=1}^{b_1'-1}\sum_{l=0}^{jc_1'-1}\zeta_a^{lck}. \tag{9}$$

Now,

$$\begin{aligned}\sum_{k=1}^{a-1}\sum_{j=1}^{b_1'-1}\sum_{l=0}^{jc_1'-1}\zeta_a^{lck} &= \sum_{j=1}^{b_1'-1}\sum_{l=0}^{jc_1'-1}\sum_{k=1}^{a-1}\zeta_a^{lck} \\ &= \sum_{j=1}^{b_1'-1}\sum_{l=0}^{jc_1'-1}\sum_{k=0}^{a-1}\zeta_a^{lck} - \frac{c_1'b_1'(b_1'-1)}{2}.\end{aligned} \tag{10}$$

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

$$\sum_{l=0}^{jc_1'-1}\sum_{k=0}^{a-1}\zeta_a^{lck} = a\left(\left\lfloor\frac{jc_1'-1}{a}\right\rfloor + 1\right).$$

Since $\gcd(a,c_1')=1$, and $j \leq b_1'-1 \leq a-1$, we have

$$\left\lfloor\frac{jc_1'-1}{a}\right\rfloor = \left\lfloor\frac{jc_1'}{a}\right\rfloor.$$

Hence,

$$\sum_{j=1}^{b_1'-1}\sum_{l=0}^{jc_1'-1}\sum_{k=0}^{a-1}\zeta_a^{lck} = a\sum_{j=1}^{b_1'-1}\left(\left\lfloor\frac{jc_1'}{a}\right\rfloor + 1\right). \tag{11}$$

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

$$\frac{S_1}{a} = b_1' \left(\frac{a-1}{2a}\right) + \frac{c_1' b_1' (b_1'-1)}{2a} - \sum_{j=1}^{b_1'-1} \left\lfloor \frac{jc_1'}{a} \right\rfloor - (b_1'-1).$$

We combine the first and last terms to get

$$\frac{S_1}{a} = \frac{c_1' b_1' (b_1'-1)}{2a} - \sum_{j=1}^{b_1'-1} \left\lfloor \frac{jc_1'}{a} \right\rfloor + 1 - b_1' \left(\frac{a+1}{2a}\right). \tag{12}$$

Symmetrically, we also have

$$\frac{S_2}{b} = \frac{a_2' c_2' (c_2'-1)}{2b} - \sum_{j=1}^{c_2'-1} \left\lfloor \frac{ja_2'}{b} \right\rfloor + 1 - c_2' \left(\frac{b+1}{2b}\right), \tag{13}$$

and

$$\frac{S_3}{c} = \frac{b_3' a_3' (a_3'-1)}{2c} - \sum_{j=1}^{a_3'-1} \left\lfloor \frac{jb_3'}{c} \right\rfloor + 1 - a_3' \left(\frac{c+1}{2c}\right). \tag{14}$$

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

Remark 6. Komatsu [4] obtained equations similar to (5) in the pairwise coprime case. He expressed these sums as summations of some very complicated expressions involving trigonometric functions, which can be solved for small values of a, b, and c. However, the summations become intractable as a, b or c become larger. In Theorem 5, we have expressed the number of solutions in terms of summations of floor functions that are easy to work with, particularly with the help of Lemma 7 below.

2.3 An algorithm to find $N(a, b, c; n)$

In this section, we describe an efficient way to find the sums in Theorem 5. Let us recall Theorem 1, which states that for distinct odd primes p and q,

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

It turns out that we can generalize Theorem 1 as follows:

Lemma 7. *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

$$\sum_{i=1}^{b} \left\lfloor \frac{ic}{a} \right\rfloor = \sum_{t=1}^{K} t n_t,$$

where n_t is the number of i such that $1 \leq i \leq b$ and $\left\lfloor \frac{ic}{a} \right\rfloor = t$. Clearly, if $t < K$, then

$$n_t = \left\lfloor \frac{(t+1)a}{c} \right\rfloor - \left\lfloor \frac{ta}{c} \right\rfloor;$$

if $t = K$, then

$$n_t = b - \left\lfloor \frac{Ka}{c} \right\rfloor.$$

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 cancelling terms and solving, we get the required result. □

Lemma 7 is helpful to calculate summations of the form $\sum_{i=1}^{b} \left\lfloor \frac{ic}{a} \right\rfloor$ because a summation can be reduced to another of the same form but with a smaller upper limit and a lesser denominator. In Section 2.5, we will see that after two applications of this lemma, the upper limit of summation and the denominator both get reduced to less than half of their original values while the numerator still remains less than the denominator.

Remark 8. Observe that if we take $a = p$, $b = \frac{p-1}{2}$, and $c = q$ in Lemma 7, then we get Theorem 1. Similar to Eisenstein's proof of Theorem 1 [1, pp. 19–20], we can also give a geometric proof of Lemma 7 by counting the number of points under the straight line $y = \frac{c}{a}x$.

Our algorithm for finding the number of non-negative integer solutions $N(a, b, c; n)$ of the equation $ax + by + cz = n$ is as follows:

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

2. Apply the formula in Theorem 5 to express the number of solutions in terms of the three summations involving floor functions.

3. Suppose the first summation has the form $\sum_{i=1}^{b_1} \left\lfloor \frac{ic_1}{a_1} \right\rfloor$ for some positive integers a_1,b_1, and c_1 such that $b_1 < a_1$, $c_1 < a_1$. Then, apply Lemma 7 to express 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. To calculate the sum $\sum_{i=1}^{K_1} \left\lfloor \frac{ia_1}{c_1} \right\rfloor$, we cannot apply Lemma 7 since $a_1 > c_1$. However, by the division algorithm, we have $a_1 = c_1 q + r$ for some quotient q and remainder r. Then,
$$\sum_{i=1}^{K_1} \left\lfloor \frac{ia_1}{c_1} \right\rfloor = \frac{qK_1(K_1+1)}{2} + \sum_{i=1}^{K_1} \left\lfloor \frac{ir}{c_1} \right\rfloor.$$
Since $r < c_1$, we can use Lemma 7 again to find this sum.

5. Keep repeating Steps 3 and 4 until the first summation in Step 2 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
$$4452x + 8030y + 9945z = 3857942.$$
For brevity, let N denote the number of non-negative integer solutions $N(4452, 8030, 9945; 3857942)$ of this equation. Firstly, we reduce this equation to an equation with pairwise coefficients. Note that $\gcd(4452, 8030) = 2$, $\gcd(4452, 9945) = 3$, and $\gcd(8030, 9945) = 5$. By Lemma 3, N is equal to the number of non-negative integer solutions of the equation
$$742x + 803y + 663z = 128598.$$
Next, we apply Theorem 5 to get
$$N = \sum_{i=1}^{129} \left\lfloor \frac{281i}{742} \right\rfloor + \sum_{i=1}^{539} \left\lfloor \frac{621i}{803} \right\rfloor + \sum_{i=1}^{335} \left\lfloor \frac{602i}{663} \right\rfloor - 166300. \tag{15}$$
In order to solve the first sum, we apply Lemma 7 to get
$$\sum_{i=1}^{129} \left\lfloor \frac{281i}{742} \right\rfloor = 6192 - \sum_{i=1}^{48} \left\lfloor \frac{742i}{281} \right\rfloor. \tag{16}$$
Then, by the division algorithm,
$$\begin{aligned} \sum_{i=1}^{48} \left\lfloor \frac{742i}{281} \right\rfloor &= \sum_{i=1}^{48} \left(2i + \left\lfloor \frac{180i}{281} \right\rfloor \right) \\ &= 2352 + \sum_{i=1}^{48} \left\lfloor \frac{180i}{281} \right\rfloor. \end{aligned} \tag{17}$$

Repeated applications of Lemma 7, followed by the division algorithm, give the following equations.

$$\begin{aligned}\sum_{i=1}^{48}\left\lfloor\frac{180i}{281}\right\rfloor &= 1440-\sum_{i=1}^{30}\left\lfloor\frac{281i}{180}\right\rfloor \\ &= 975-\sum_{i=1}^{30}\left\lfloor\frac{101i}{180}\right\rfloor,\end{aligned} \tag{18}$$

$$\begin{aligned}\sum_{i=1}^{30}\left\lfloor\frac{101i}{180}\right\rfloor &= 480-\sum_{i=1}^{16}\left\lfloor\frac{180i}{101}\right\rfloor \\ &= 344-\sum_{i=1}^{16}\left\lfloor\frac{79i}{101}\right\rfloor,\end{aligned} \tag{19}$$

$$\begin{aligned}\sum_{i=1}^{16}\left\lfloor\frac{79i}{101}\right\rfloor &= 192-\sum_{i=1}^{12}\left\lfloor\frac{101i}{79}\right\rfloor \\ &= 114-\sum_{i=1}^{12}\left\lfloor\frac{22i}{79}\right\rfloor,\end{aligned} \tag{20}$$

$$\begin{aligned}\sum_{i=1}^{12}\left\lfloor\frac{22i}{79}\right\rfloor &= 36-\sum_{i=1}^{3}\left\lfloor\frac{79i}{22}\right\rfloor \\ &= 18-\sum_{i=1}^{3}\left\lfloor\frac{13i}{22}\right\rfloor,\end{aligned} \tag{21}$$

and

$$\begin{aligned}\sum_{i=1}^{3}\left\lfloor\frac{13i}{22}\right\rfloor &= 3-\sum_{i=1}^{1}\left\lfloor\frac{22i}{13}\right\rfloor \\ &= 2.\end{aligned} \tag{22}$$

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 that $N = 22$, i.e., there are 22 solutions of the equation $4452x + 8030y + 9945z = 3857942$ in non-negative integer triples (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 non-negative integer solutions of the equation $ax + by + cz = n$. By a step, we mean a basic arithmetic operation on $O(\log r)$ bits where $r = \max(a, b, c)$. 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 3 of the algorithm, we need to apply Lemma 7 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 4 in the algorithm describes, we need to apply the division algorithm to obtain $a_1 = c_1 q_1 + a_2$, where $a_2 < c_1$. Since $\gcd(c_1, a_1) = 1$, we have $\gcd(a_2, c_1) = 1$. Thus, the sum $\sum_{i=1}^{K_1} \left\lfloor \frac{ia_1}{c_1} \right\rfloor$ can be obtained in terms of the sum $\sum_{i=1}^{K_1} \left\lfloor \frac{ia_2}{c_1} \right\rfloor$. Note that since $c_1 < a_1$, we have $q \geq 1$, and thus,

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

or equivalently $a_2 < \frac{a_1}{2}$.

According to Step 3 of the algorithm, we again apply Lemma 7 to get the sum $\sum_{i=1}^{K_1} \left\lfloor \frac{ia_2}{c_1} \right\rfloor$ in terms of the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ic_1}{a_2} \right\rfloor$ for some $K_2 < a_2$. Then, we again apply the division algorithm to obtain $c_1 = a_2 q_2 + c_2$ for some $c_2 < a_2$; we can then express the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ic_1}{a_2} \right\rfloor$ in terms of the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ic_2}{a_2} \right\rfloor$. Since a_2 is coprime to c_1, it is also coprime to c_2. Finally, since $K_2 < a_2$, $c_2 < a_2$, and $\gcd(c_2, a_2) = 1$, we return to Step 3 of the algorithm to find the sum $\sum_{i=1}^{K_2} \left\lfloor \frac{ic_2}{a_2} \right\rfloor$.

Thus, with two applications of Steps 3 and 4 of the algorithm (i.e., two applications of Lemma 7, with each one followed by an application of 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 $\sum_{i=1}^{K_2} \left\lfloor \frac{ic_2}{a_2} \right\rfloor$, where $a_2 < \frac{a_1}{2}$. It is also easy to see that $K_2 < \frac{b}{2}$. This ensures that the Steps 3, 4, and 5 of the algorithm terminate in $O(\log a)$ steps. Hence, the algorithm terminates in $O(\log t)$ steps, where $t = \max(a, b, c)$.

2.6 Relationship with quadratic residues

Let us recall Eisenstein's lemma, which states that for given distinct odd primes p and q, the Legendre symbol $\left(\frac{q}{p}\right)$ is given by

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

where

$$t = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor .$$

Remark 9. The Legendre symbol $\left(\frac{q}{p}\right)$ can be calculated in $O(\log s)$ steps, where $s = \max(p, q)$.

Thus, Eisenstein's lemma relates Legendre symbols to summations that we have been dealing with while attempting to solve the equation $ax + by + cz = n$. This suggests the existence of an equation whose number of solutions gives the Legendre symbol $\left(\frac{q}{p}\right)$.

Lemma 10. *The number of non-negative integer solutions of the equation* $px+qy+z = \frac{q(p-1)}{2}$ *is given by*

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

Proof. Clearly, one way of proving this is by applying Theorem 5. However, we could also prove it directly by fixing y and then calculating the number of possible values for x. For given x and y, z is automatically determined. □

Corollary 11. *The Legendre symbol* $\left(\frac{q}{p}\right)$ *is given by*

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

Proof. This follows directly from Eisenstein's lemma and Lemma 10. □

3 Equivalence between two well-known results

The aim of this section is to establish the equivalence between Theorems 1 and 2. Throughout this section, p and q denote distinct odd primes.

Lemma 12. *The number of non-negative integer 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 as* $px + qy$ *for some non-negative integers* x *and* y.

Proof. We first fix z and then calculate 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

$$\sum_{n=0}^{\frac{p(q-1)}{2}+\frac{q(p-1)}{2}} S_n,$$

where S_n is the number of solutions of the equation $px + qy = n$. Clearly, $S_0 = 1$. We would require the following well-known results which we would also reprove in Section 4.2 using the methods developed in Section 3.

(*i*) Whenever $1 \leq n \leq (p-1)(q-1)$, S_n is either 0 or 1.

(*ii*) Whenever $(p-1)(q-1) < n < pq$, $S_n = 1$.

Thus, by (*i*) and the definition of N_0,

$$\sum_{n=1}^{(p-1)(q-1)} S_n = (p-1)(q-1) - N_0.$$

Moreover, by (*ii*),

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

Therefore,

$$\begin{aligned}\sum_{n=0}^{\frac{p(q-1)}{2}+\frac{q(p-1)}{2}} S_n &= S_0 + \sum_{n=1}^{(p-1)(q-1)} S_n + \sum_{n=(p-1)(q-1)+1}^{\frac{p(q-1)}{2}+\frac{q(p-1)}{2}} S_n \\ &= \frac{p(q-1)}{2} + \frac{q(p-1)}{2} + 1 - N_0.\end{aligned}$$

□

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. Recall that $N_{p,q}$ denotes the number of non-negative solutions of the equation $px + qy + z = \frac{q(p-1)}{2}$.

Lemma 13. *The number of non-negative integer 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. $X \geq 0, Y < 0$, or
4. $X < 0$.

We define the following sets:

- Let S_1, S_2, S_3, and S_4 denote the set of non-negative integer solutions of $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ in Cases 1, 2, 3, and 4, respectively.
- Let T_1 denote the set of non-negative integer solutions of $px + qy + z = \frac{q(p-1)}{2}$.
- Let T_2 denote the set of non-negative integer solutions of $px + qy + z = \frac{p(q-1)}{2}$.
- Let U denote the set of solutions in T_2 that satisfy $z = 0$.
- Let V denote the set of solutions in T_2 that satisfy $y = 0$.
- Let W denote the set of solutions in T_1 that satisfy $x = 0$.

Clearly, $|T_1| = N_{p,q}$ and $|T_2| = N_{q,p}$. Moreover, it is straightforward to see that $|U| = 1$, $|V| = \frac{q+1}{2}$, and $|W| = \frac{p+1}{2}$. Next, we find the cardinalities of the sets S_1, S_2, S_3, and S_4 by defining the following maps from these sets to T_1 and T_2.

- Define $\phi_1 : S_1 \to T_1$ such that $(x, y, z) \mapsto (X, Y, Z)$.
- Define $\phi_2 : S_2 \to T_2$ such that $(x, y, z) \mapsto (x, y, -Z)$.
- Define $\phi_3 : S_3 \to T_2$ such that $(x, y, z) \mapsto (x, -Y, z)$.
- Define $\phi_4 : S_4 \to T_1$ such that $(x, y, z) \mapsto (-X, y, z)$.

It is easy to verify that ϕ_1, ϕ_2, ϕ_3, and ϕ_4 are well-defined injective maps and their images are given as follows:

- $\phi_1(S_1) = T_1$.
- $\phi_2(S_2) = T_2 \setminus U$.
- $\phi_3(S_3) = T_2 \setminus V$.
- $\phi_4(S_4) = T_1 \setminus W$.

Thus, $|S_1| = N_{p,q}$, $|S_2| = N_{q,p} - 1$, $|S_3| = N_{q,p} - \frac{q+1}{2}$, and $|S_4| = N_{p,q} - \frac{p+1}{2}$. Hence, the total number of non-negative integer solutions of the equation $px + qy + z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ is equal to $|S_1| + |S_2| + |S_3| + |S_4| = 2(N_{p,q} + N_{q,p}) - \left(\frac{p+1}{2} + \frac{q+1}{2} + 1\right)$. □

Upon comparing the number of non-negative integer solutions of the equation $px+qy+z = \frac{p(q-1)}{2} + \frac{q(p-1)}{2}$ obtained in Lemmas 12 and 13, and then using Lemma 10, we find

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

This establishes the required equivalence between Theorems 1 and 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 10, we counted the number of solutions of the equation $px + qy + z = \frac{q(p-1)}{2}$. Now, we count these in another way.

Lemma 14. *If p and q are distinct odd primes such that $q < p$, then the number of non-negative integer solutions of the equation $px + qy + z = \frac{q(p-1)}{2}$ is given by*

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

Proof. The 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 $x = 0$. The 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

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

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 10 and Lemma 14.

4.2 Solving the equation $ax + by = n$

It turns out that we can completely solve the equation $ax + by = n$ by modifying the technique used in Section 2.1. Note that if $\gcd(a, b)$ does not divide n, then there is no solution; otherwise we can divide both sides of the equation by $\gcd(a, b)$. Thus, without loss of generality, we can assume that $\gcd(a, b) = 1$.

We define the following symbols:

- Let a^{-1} and b^{-1} denote the modular inverses of a with respect to b and b with respect to a, respectively.
- Let a_1 and b_1 denote the remainders when na^{-1} is divided by b and nb^{-1} is divided by a, respectively.
- Let M denotes $\frac{n-aa_1-bb_1}{ab}$. Note that M is an integer.

We obtain a complete list of non-negative integer solutions of the equation $ax + by = n$.

Theorem 15. *Let a, b, and n be given positive integers such that $\gcd(a, b) = 1$. With the notation above, the non-negative integer solutions of the equation $ax + by = n$ are given as*

$$\{(bi + a_1, (M - i)a + b_1) : 0 \leq i \leq M\}.$$

Proof. Let S and T denote the solution sets of $ax + by = n$ and $x + y = M$, 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 with $\phi^{-1} : T \to S$ given by

$$(x, y) \mapsto (bx + a_1, ay + b_1).$$

Clearly, $T = \{(i, M - i) : 0 \leq i \leq M\}$. Then, ϕ^{-1} gives the required form for S. □

Remark 16. We briefly describe the motivation behind this bijection. Reducing the given equation $ax + by = n$ modulo b and a, gives the equations $x \equiv a_1 \pmod{b}$ and $y \equiv b_1 \pmod{a}$, respectively. Thus, we have the expressions $x = a_1 + bu$ and $y = b_1 + av$, for some non-negative integers u and v. Substituting these expressions back in the given equation $ax + by = n$ yields the equation $u + v = M$.

Corollary 17. *Let a, b, and n be given positive integers such that $\gcd(a, b) = 1$. With the notation above, the number of non-negative integer solutions of the equation $ax + by = n$ is given by*

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

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

Corollary 18. *The equation $ax + by = n$ has a unique non-negative integer 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 $b_1 \leq (a - 1)$, we have

$$N(a, b; n) \geq \frac{n + a + b - ab}{ab}.$$

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 that 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 18 gives another proof of the fact that the Frobenius number of the set $\{a, b\}$ such that $\gcd(a, b) = 1$ is equal to $ab - a - b$.

4.3 A by-product summation result

We can modify the proof of Lemma 14 to obtain the following result:

Theorem 19. *Let p and q be distinct odd primes such that $q > p$, then*

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

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

$$\sum_{i=354}^{369} \left\lfloor \frac{23i}{739} \right\rfloor = 176.$$

4.4 An application of Theorem 1

We want to show that Theorem 1 can be used to determine the parity of 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. Furthermore, let k denote the quantity $\left(\frac{p-1}{2}\right) + p\left(\frac{q-1}{2}\right)p^{-1}$.

Theorem 20. *The number of non-negative integer solutions of the equation*

$$px + qy + z = k$$

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 $t_1 = \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor$ and $t_2 = \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip^{-1}}{q} \right\rfloor$. Note that

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

Therefore, $\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor$ and $\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip^{-1}}{q} \right\rfloor$ have the same parity. The result now follows directly from Theorems 5 and 1. □

5 Acknowledgments

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 and A. Ganguli at IISER Mohali for helpful suggestions on 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, 2015.

[2] G. Eisenstein, Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste, *J. Reine Angew. Math.* **28** (1844), 246–248.

[3] C. F. Gauss, Theorematis arithmetici demonstratio nova, *Comment. Soc. regiae sci. Göttingen* **16** (1808), 69.

[4] T. Komatsu, On the number of solutions of the Diophantine equation of Frobenius—general case, *Math. Commun.* **8** (2003), 195–206.

[5] J. J. Sylvester, On subinvariants, i.e. semi-invariants to binary quantics of an unlimited order, *Amer. J. Math.* **5** (1882), 79–136.

[6] J. J. Sylvester, Problem 7382, *Mathematical Questions, with their Solutions, from the Educational Times* **41** (1884), 21.

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

2010 *Mathematics Subject Classification*: Primary 11D45; Secondary 05A15, 11A15, 11A05, 11A07, 11D04, 11D72.

Keywords: Frobenius coin problem, linear Diophantine equation, generating function, roots of unity, partial fraction, floor function, Eisenstein's lemma, Legendre symbol, quadratic reciprocity, Frobenius number.

Received December 21 2017; revised versions received September 25 2019; May 11 2020; May 18 2020. Published in *Journal of Integer Sequences*, June 11 2020. Minor revision fixing typos, February 1 2021.