Research Article

Lattice Points on the Fermat Factorization Method

Regis Freguin Babindamana, Gilda Rech Bansimba, and Basile Guy Richard Bosotto

Université Marien Ngouabi, Faculté des Sciences et Techniques, BP: 69, Brazzaville, Congo

Correspondence should be addressed to Regis Freguin Babindamana; regis.babindamana@umng.cg

Received 5 May 2021; Revised 17 August 2021; Accepted 6 December 2021; Published 28 January 2022

Academic Editor: Bibhas Ranjan Majhi

Copyright © 2022 Regis Freguin Babindamana et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we study algebraic properties of lattice points of the arc on the conics \( x^2 - dy^2 = N \) especially for \( d = 1 \), which is the Fermat factorization equation that is the main idea of many important factorization methods like the quadratic field sieve, using arithmetical results of a particular hyperbola parametrization. As a result, we present a generalization of the forms, the cardinal, and the distribution of its lattice points over the integers. In particular, we prove that if \( (N - 6) \equiv 0 \mod 4 \), Fermat’s method fails. Otherwise, in terms of cardinality, it has, respectively, 4, 8, 2 \( \alpha \), \( 1 \), \( 1 \), \( 2 \alpha + 1 \), and \( 2 \prod_{i=1}^{n} (a_i + 1) \) lattice points if \( N \) is an odd prime, \( N = N_a \times N_b \) with \( N_a \) and \( N_b \) being odd primes, \( N = N_a^2 \) with \( N_a \) being prime, \( N = \prod_{i=1}^{n} p_i \) with \( p_i \) being distinct primes, and \( N = \prod_{i=1}^{n} N_i \), with \( N_i \) being odd primes. These results are important since they provide further arithmetical understanding and information on the integer solutions revealing factors of \( N \). These results could be particularly investigated for the purpose of improving the underlying integer factorization methods.

1. Introduction

Diophantine equations have been for many decades a very important subject of research in number theory, and lattice points on curves have been studied in the literature particularly by Gauss, and bounds on arcs of conics have also been studied since then (see [1–6]). However, the necessity of representing an integer as difference of two squares, i.e., for a given \( N \in \mathbb{Z} \), finding nontrivial couples \( (x, y) \in \mathbb{Z}^2 \) such that \( x^2 - y^2 = N \), appears in the literature as the main idea of many factorization methods (see [7, 8]) as suggested by Fermat (see [9, 10]). While being not hard to observe, its lattice points are easily computable if one knows the factorization of \( N \), and in contrast, this gets exponentially harder when it comes to special cases of \( N \), mainly when \( N = \prod_{i=1}^{m} p_i \), where \( p_i \) are large primes, in which case this problem becomes equivalent to factoring the parameter \( N \).

For this reason, one of fundamental research problems on conics is to find integral solutions of particular hyperbola parametrizations mainly \( x^2 - y^2 = N \) over the integers, particularly when \( N \) is a large semiprime, in which case if a computationally efficient algorithm is found, cryptosystems like RSA [11] would no longer be secured.

Reviewing the literature, some results on various hyperbola parametrizations and their applications have been studied. Particularly in [1], Javier and Jorge used ideals in quadratic field \( \mathbb{Q}(\sqrt{d}) \) to find an upper bound for the number of lattice points on Pell’s equation \( x^2 - dy^2 = N \), while in [12], Jin et al. used results from the forms of integer solutions of the hyperbola \( bx^2 - abxy + ay^2 = k \) to solve the same equation where \( d \) is of the form \( p^2 - q > 0 \). In [13], the author studied a special case of hyperbola and presented the forms of its integral points over \( \mathbb{Z} \), and in [14], Yeonok investigated some behaviors of integral points on the hyperbola \( bx^2 - abxy + ay^2 = -bk \) \( (k \in \mathbb{Z}_{>0}) \) to the generalizations of Binet formula and Catalan’s identity, while in [15], the authors gave an application of group law on affine conics to cryptography. Still, in the previous works, algebraic properties and distribution of lattice points and cardinalities on Fermat’s equation are not presented. More recently, in [16], Gilda et al. investigated algebraic and arithmetical properties on the group structure \( \mathcal{B}_N(x, y) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} | y^2 = x^2 - N x \} \), mainly isomorphisms, integral solutions, and a description of a factorization method with no generalization to the Fermat factorization equation.
In this paper, we use the hyperbola parametrization introduced in [16] to study algebraic properties of lattice points and their distribution for Fermat’s factorization equation for which we find exact upper and lower bounds and we present the forms and cardinalities with a generalization of results for most of special cases of \( N \), using results from the particular hyperbola parametrization.

The article is organized as follows:

(i) In Section 1, we give an introduction
(ii) In Section 2, we present the particular hyperbola parametrization and related arithmetical results
(iii) In Section 3, we present the application of the hyperbola parametrization to the study of lattice points on the Fermat equation
(iv) In Section 4, we do a discussion on the likelihood of finding solutions to the Fermat factorization equation
(v) In Section 5, we finally conclude

Here is a list of the commonly used nomenclature in this paper:

\( \mathcal{B}_N(x, y)_{\mid \mathbb{Q}} = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} / y^2 = x^2 - 4Nx\} \): algebraic set of all rational points on \( \mathcal{B}_N(x, y) \).

\( \mathcal{B}_N(x, y)_{\mid \mathbb{Z}} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / y^2 = x^2 - 4Nx\} \): algebraic set of all integral points on \( \mathcal{B}_N(x, y) \).

\( \mathcal{B}_N(x, y)_{\mid Z_{\geq 4N}} = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / y^2 = x^2 - 4Nx\} \): algebraic set of integral points on \( \mathcal{B}_N(x, y) \) whose \( x \)-coordinates are greater or equal to \( 4N \).

\( X_N \to N \): an injective homomorphism from \( \mathcal{B}_N(x, y) \) to \( \mathcal{B}_{N'}(x, y) \).

\( \text{Card}(\mathcal{B}_N(x, y)) \): the cardinal of \( \mathcal{B}_N(x, y) \).

\( \text{Div}(N_a) \): set of divisors of \( N_a \).

\( \pi_2(n) \): the set of all prime divisors of \( n \).

\( H_N = \{(x, y) \in \mathbb{Z}^2 / x^2 - y^2 = N\} \): the Fermat factorization equation.

\( \delta_{ij} \): the Kronecker symbol.

2. BN Hyperbola Parametrization

A conic is an algebraic set satisfying an equation of the form \( a_1x^2 + 2a_2xy + a_3y^2 + 2a_4x + 2a_5y + a_6 = 0 \), \( (a_1, a_2, a_3, a_4, a_5, a_6) \in \mathbb{R}^5 \) where \( (a_1, a_2, a_3) \neq (0, 0, 0) \). Setting \( \mathcal{B}_N \) the parametrization defined by \( (x, y) \in \mathbb{Q} \times \mathbb{Q} / y^2 = x^2 - 4Nx \), in the projective space \( \mathbb{P}^2(\mathbb{Q}) \), we have \( \mathcal{B}_N(X, Y, Z) = \{(X: Y: Z) \in \mathbb{P}^2(\mathbb{Q}) / (Y^2/Z^2) = (X^2/Z^2) - 4N(X/Z)\} \). Setting \( \mathcal{B}_N(X, Y, Z) = \{(X: Y: Z) \in (\mathbb{P}^2(\mathbb{Q}) / Y^2) = (X^2 - 4NXZ)\} \).

At infinity, setting \( Z = 0 \) and considering \( X, Y > 0 \), we obtain \( Y^2 = X^2 \), and the equivalence class \( (X: Y: Z) \sim (X: X: 0) \sim X(1: 1: 0) \), and hence one of the points at infinity is \( P_{\infty} = (1: 1: 0) \).

From now on, \( \forall N \in \mathbb{Z}_{>0} \), \( \mathcal{B}_N(x, y) \) denotes \( \mathcal{B}_N(x, y) \) over the field \( \mathbb{Q} \), \( \mathcal{B}_N(x, y)_{\mid \mathbb{Z}} \) denotes \( \mathcal{B}_N(x, y) \) over \( \mathbb{Z} \), \( \mathcal{B}_N(x, y)_{\mid \mathbb{Z}_{\geq 4N}} \) denotes \( \mathcal{B}_N(x, y) \) over the integers, i.e., \( \mathcal{B}_N(x, y) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} / y^2 = x^2 - 4Nx\} \); and \( \mathcal{B}_N(x, y)_{\mid \mathbb{Z}^2} \) denotes \( \mathcal{B}_N(x, y) \) over the integers, i.e., \( \mathcal{B}_N(x, y) = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / y^2 = x^2 - 4Nx\} \).

\[ \text{Proposition 1. Consider the application} \]

\[ +: \mathcal{B}_N(x, y) \times \mathcal{B}_N(x, y) \to \mathcal{B}_N(x, y)(P, Q) \to P + Q. \]

\[ (1) \]

\[ P + Q \text{ is defined } \forall P = (x_p, y_p), Q = (x_q, y_q) \in \mathcal{B}_N(x, y), \begin{cases} x_{p+q} = \frac{1}{2N} \left[ (x_p - 2N)(x_q - 2N) + y_p y_q \right] + 2N, \\ y_{p+q} = \frac{1}{2N} \left[ y_p (x_q - 2N) + y_q (x_p - 2N) \right], \end{cases} \]

\[ (2) \]

\[ x_{2p} = \frac{1}{2N} \left[ (x_p - 2N)^2 + y_p^2 \right] + 2N, \quad y_{2p} = \frac{1}{N \cdot 2p} \left( y_p (x_p - 2N) \right). \]

Then, \( \mathcal{B}_N(x, y) + \) is an abelian group with neutral element \( \theta = (4N, 0) \).

\[ \text{Proof. Let us consider the affine space } \mathbb{Q}^2(x, y). \]

\( \mathcal{B}_N \) is a hyperbola of equation \( XY = 1 \), where \( X = (x - y - 2N/2N, Y = (x + y - 2N/2N) \), i.e., \( x - 2N/2N)^2 - (y/2N)^2 = 1 \), with \( N \in \mathbb{Z}_{>0} \). Set

\[ \begin{align*}
  x - 2N &= 2N \cosh(t) \\
  y &= 2N \sinh(t)
\end{align*} \quad \Rightarrow \quad \begin{cases} x = 2N \cosh(t) - 1 = \cosh(t) \\
  y = 2N \sinh(t)
\end{cases} \quad \text{since } \cosh^2(t) - \sinh^2(t) = 1,
\]

\[ t_1 + t_2 \in \{ t \in \mathbb{Z} / \cosh^2(t) - \sinh^2(t) = 1 \} \text{ where } \begin{cases} \cosh(t_1 + t_2) = \cosh(t_1) \cosh(t_2) + \sinh(t_1) \sinh(t_2) \\
  \sinh(t_1 + t_2) = \sinh(t_1) \cosh(t_2) + \cosh(t_1) \sinh(t_2).
\end{cases} \]
Given two points \( P = (x_p, y_p) \) and \( Q = (x_q, y_q) \) in \( \mathcal{B}_N(x, y) \),

\[
\begin{align*}
X_1 &= \frac{x_p}{2N} - 1 = \cosh(t_1), \\
Y_1 &= \frac{y_p}{2N} = \sinh(t_1), \\
X_2 &= \frac{x_q}{2N} - 1 = \cosh(t_2), \\
Y_2 &= \frac{y_q}{2N} = \sinh(t_2),
\end{align*}
\]

We then have:

\[
\begin{align*}
\cosh(t_1 + t_2) &= X_1X_2 + Y_1Y_2, \\
\sinh(t_1 + t_2) &= Y_1X_2 + X_1Y_2.
\end{align*}
\]

We easily verify that \((X_1X_2 + Y_1Y_2)^2 - (Y_1X_2 + X_1Y_2)^2 = 1\).

\[
\begin{align*}
\frac{x_{pq}}{2N} - 1 &= X_1X_2 + Y_1Y_2 = \frac{x_p - 2N}{2N} \left( x_q - 2N \right) + 1 = \frac{x_p - 2N}{2N} \left( x_q - 2N \right) + y_p y_q + 1, \\
\frac{y_{pq}}{2N} &= Y_1X_2 + X_1Y_2 = \frac{y_p}{2N} \left( x_q - 2N \right) + \frac{y_q}{2N} \left( x_p - 2N \right) = \frac{y_p}{2N} \left( x_q - 2N \right) + y_q \left( x_p - 2N \right),
\end{align*}
\]

We have both

\[
\begin{align*}
x_{pq} &= \frac{1}{2N} \left( (x_p - 2N)(x_q - 2N) + y_p y_q \right) + 2N, \\
y_{pq} &= \frac{1}{2N} \left[ y_p (x_q - 2N) + y_q (x_p - 2N) \right].
\end{align*}
\]

We denote \( + \) as the above defined additive law. This addition law is strongly unified since point doubling does exist and is well defined.
\[(P + Q) + T = \begin{cases} x_{(p+q)+t} = \frac{1}{2N} \left[ (x_{(p+q)} - 2N)(x_t - 2N) + y_{(p+q)}y_t \right] + 2N \\
y_{(p+q)+t} = \frac{1}{2N} \left[ y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right] \end{cases} \]

\[
\begin{align*}
&= \frac{1}{2N} \left[ \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \right] \left( x_t - 2N \right) + \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \left( x_t - 2N \right) + y_{(p+q)}y_t + 2N \\
&= \frac{1}{2N} \left[ \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \right] \left( x_t - 2N \right) + y_t \left( \frac{1}{2N} \right) \left( y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right) + 2N \\
&= \frac{1}{2N} \left[ \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \right] \left( x_t - 2N \right) + y_t \left( \frac{1}{2N} \right) \left( y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right) + 2N \tag{8} \\
&= \frac{1}{2N} \left[ \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \right] \left( x_t - 2N \right) + y_t \left( \frac{1}{2N} \right) \left( y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right) \tag{9} \end{align*} \]

Secondly we consider \(P + (Q + T) = \)

\[
\begin{align*}
x_{(p+q)+t} &= \frac{1}{2N} \left[ (x_{(p+q)} - 2N)(x_t - 2N) + y_{(p+q)}y_t \right] + 2N \\
y_{(p+q)+t} &= \frac{1}{2N} \left[ y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right] \end{align*} \]

\[
\begin{align*}
&= \frac{1}{2N} \left[ \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \right] \left( x_t - 2N \right) + y_t \left( \frac{1}{2N} \right) \left( y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right) + 2N \\
&= \frac{1}{2N} \left[ \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \right] \left( x_t - 2N \right) + y_t \left( \frac{1}{2N} \right) \left( y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right) + 2N \tag{10} \\
&= \frac{1}{2N} \left[ \left( \frac{1}{2N} \right) \left( x_{(p+q)} - 2N \right) \right] \left( x_t - 2N \right) + y_t \left( \frac{1}{2N} \right) \left( y_{(p+q)}(x_t - 2N) + y_t(x_{(p+q)} - 2N) \right) \tag{11} \end{align*} \]

We clearly see by identification that \(9 = 11\Rightarrow (P + Q) + T = P + (Q + T)\).
(i) Neutral element: \( \mathcal{O} = (4N, 0) \). It is obvious to see that \( \mathcal{O} = (4N, 0) \in \mathcal{B}_N(x, y) \). Given any point \( P = (x_p, y_p) \in \mathcal{B}(x, y) \), from (3), we have

\[
P + \mathcal{O} = \begin{cases} 
    x_{p+\mathcal{O}} = \frac{1}{2N} \left( (x_p - 2N)(4N - 2N) + y_p \times 0 \right) + 2N = \frac{1}{2N} \left[ 2N(x_p - 2N) \right] + 2N = x_p \\
y_{p+\mathcal{O}} = \frac{1}{2N} \left[ y_p(4N - 2N) + 0 \times (x_p - 2N) \right] = \frac{1}{2N} \left[ 2N y_p \right] = y_p,
\end{cases}
\]

\[
\mathcal{O} + P = \begin{cases} 
    x_{\mathcal{O}+p} = \frac{1}{2N} \left[ (4N - 2N)(x_p - 2N) + 0 \times y_p \right] + 2N = \frac{1}{2N} \left[ 2N(x_p - 2N) \right] + 2N = x_p \\
y_{\mathcal{O}+p} = \frac{1}{2N} \left[ 0 \times (x_p - 2N) + y_p(4N - 2N) \right] = \frac{1}{2N} \left[ 2N y_p \right] = y_p.
\end{cases}
\]

Hence, \( \forall P \in \mathcal{B}_N(x, y) \), \( P + \mathcal{O} = \mathcal{O} + P = P \).

(ii) Symmetric element: \( \forall P = (x_p, y_p) \in \mathcal{B}_N(x, y) \), \( P' = (x_p, -y_p) \) is the symmetric element of \( P \). It is obvious to see that \( (x_p, -y_p) \in \mathcal{B}_N(x, y) \). Then, we have

\[
P + P' = \begin{cases} 
    x_{p+p'} = \frac{1}{2N} \left( (x_p - 2N)^2 - y_p^2 \right) + 2N = \frac{1}{2N} \left[ x_p^2 - 4Nx_p + 4N^2 - y_p^2 \right] + 2N = \frac{1}{2N} \left[ 4N^2 \right] + 2N = 4N \\
y_{p+p'} = \frac{1}{2N} \left[ y_p(x_p - 2N) - y_p(x_p - 2N) \right] = \frac{1}{2N} \left[ 0 \right] = 0,
\end{cases}
\]

\[
P' + P = \begin{cases} 
    x_{p'+p} = \frac{1}{2N} \left( (x_p - 2N)^2 - y_p^2 \right) + 2N = \frac{1}{2N} \left[ x_p^2 - 4Nx_p + 4N^2 - y_p^2 \right] + 2N = \frac{1}{2N} \left[ 4N^2 \right] + 2N = 4N \\
y_{p'+p} = \frac{1}{2N} \left[ -y_p(x_p - 2N) + y_p(x_p - 2N) \right] = \frac{1}{2N} \left[ 0 \right] = 0.
\end{cases}
\]

Hence, \( \forall P = (x_p, y_p) \), \( P' = (x_p, -y_p) \in \mathcal{B}_N(x, y) \), \( P + P' = P' + P = \mathcal{O} \).

(iii) Commutativity:

\[
P + Q = \begin{cases} 
    x_{p+q} = \frac{1}{2N} \left[ (x_p - 2N)(x_q - 2N) + y_p y_q \right] + 2N = \frac{1}{2N} \left[ (x_q - 2N)(x_p - 2N) + y_q y_p \right] + 2N = x_{q+p}, \\
y_{p+q} = \frac{1}{2N} \left[ y_p(x_q - 2N) + y_q(x_p - 2N) \right] = \frac{1}{2N} \left[ y_q(x_p - 2N) + y_p(x_q - 2N) \right] = y_{q+p}.
\end{cases}
\]

Hence, \( \forall P, Q \in \mathcal{B}_N(x, y) \), \( P + Q = Q + P \). \( \Box \)

defines a group homomorphism.

Proposition 2. Let \( \mathcal{B}_{N_a}(x, y) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q}/y^2 = x^2 - 4N_a x \} \) and \( \mathcal{B}_{N_b}(x, y) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q}/y^2 = x^2 - 4N_b x \} \). Then, the following map:

\[
\chi: \mathcal{B}_{N_a}(x, y) \to \mathcal{B}_{N_b}(x, y) \to \left( \begin{array}{c} N_b \ \\
N_a \end{array} \right), \quad \left( \begin{array}{c} x \ \\
y \end{array} \right) \mapsto \left( \begin{array}{c} N_b \ \\
N_a \end{array} \right) \left( \begin{array}{c} x \ \\
y \end{array} \right),
\]

(15)

Proof. \( \forall P = (x_p, y_p) \in \mathcal{B}_{N_a}(x, y) \), \( \chi(P) = \chi(x_p, y_p) = \left( x_p(N_b/N_a), y_p(N_b/N_a) \right) \in \mathcal{B}_{N_b}(x, y) \), \( \left( x_p(N_b/N_a), y_p(N_b/N_a) \right) \in \mathcal{B}_{N_b}(x, y) \Rightarrow \left( y_p(N_b/N_a) \right)^2 = \left( x_p(N_b/N_a) \right)^2 - 4N_b(x_p(N_b/N_a)) = x_p(N_b^2/N_a^2)(x_p/N_a - 4) = N_b^2(x_p^2 - 4N_a x) \Rightarrow (y_p(N_b/N_a))^2 = N_b^2 y_p^2/N_a^2 = (y_p(N_b/N_a))^2 \). Thus, \( \left( x_p(N_b/N_a), y_p(N_b/N_a) \right) \in \mathcal{B}_{N_b}(x, y) \).
Consider $\mathcal{O}_{\mathcal{A}_N} = (4N_a, 0)$ and $\mathcal{O}_{\mathcal{A}_N} = (4N_b, 0)$.

$$\chi(\mathcal{O}_{\mathcal{A}_N}) = \chi((4N_a, 0)) = \left(\frac{N_b}{N_a} \right) = \left(4N_b, 0 \right) = \mathcal{O}_{\mathcal{A}_N} \Rightarrow \chi(\mathcal{O}_{\mathcal{A}_N}) = \mathcal{O}_{\mathcal{A}_N} \left(i_2\right).$$

Set $P'$ the inverse of $P$ in $\mathcal{B}_N(x, y)$; by definition, $P' = (x_p, -y_p)$.

$$\chi(P + Q) = \chi\left(\frac{(x_p - 2N_a)(x_q - 2N_a) + y_q y_q}{2N_a}\right),$$

$$\chi(P) + \chi(Q) = \left(\frac{N_b}{N_a}\right) \left(x_p, y_p + y_q\right)\left(y_p, y_q\right) + \left(2N_b, 0\right),$$

Then, $\chi(P') = \chi((x_p, -y_p)) = \chi(P) \Rightarrow \chi(P') = \chi(P)'(i_2).$

Consider (i) if $k_i, k_j \in \text{Div}(N)$ such that $k_i \times k_j = N$, then $(k_i, k_i + 1, k_j(k_j - 1)) \in \mathcal{B}_N(x, y)$. (ii) If $k_i, k_j \in \text{Div}(N) \setminus \{1, N\}$ with $k_i, k_j$ primes, then $k_i/k_j | N$ and $(k_i + 2k_j)N_a + k_i N_b, (k_i^2 - k_j^2)N_q \in \mathcal{B}_N(x, y)$ where $N_a = N/k_i, N_b = n/k_j, N_q = N/k_j$. (iii) More generally, if $k | N \Leftrightarrow \left((k + 2)N + (N/k), (k^2 - 1/N)\right) \in \mathcal{B}_N(x, y)$.

Example 1. $N = 18$: $\text{Div}(N) = \{1, 2, 3, 6, 9, 18\}; \forall N$ prime, $\text{Div}(N) = \{1, N\}$.

\[\text{Proposition 3}\]

(i) If $k_i, k_j \in \text{Div}(N)$ such that $k_i \times k_j = N$, then $(k_i + k_j)^3, (k_i^2 - k_j^2))$. (ii) If $k_i, k_j \in \text{Div}(N) \setminus \{1, N\}$ with $k_i, k_j$ primes, then $k_i/k_j | N$ and $(k_i + 2k_j)N_a + k_i N_b, (k_i^2 - k_j^2)N_q \in \mathcal{B}_N(x, y)$ where $N_a = N/k_i, N_b = n/k_j, N_q = N/k_j$. (iii) More generally, if $k | N \Leftrightarrow \left((k + 2)N + (N/k), (k^2 - 1/N)\right) \in \mathcal{B}_N(x, y)$.
Proposition 4. If \( P = (x_p, y_p) \in \mathcal{B}_N(x, y) \), then the following holds:

(i) \((x_p - y_p) \in \mathcal{B}_N(x, y)\).

(ii) \((-x_p + 4N, -y_p) \in \mathcal{B}_N(x, y)\).

(iii) \((-x_p + 4N, -y_p) \in \mathcal{B}_N(x, y)\).

Proof

(i) \((x_p - y_p) \in \mathcal{B}_N(x, y)\) is straightforward since it results from the symmetry of \(\mathcal{B}_N(x, y)\) with respect to the \((Ox)\) axis.

(ii) At the point \((-x_p + 4N, y_p)\), we have \(y_p^2 = (-x_p + 4N)^2 - 4N(-x_p + 4N) \Rightarrow y_p^2 = x_p^2 - 8Nx_p + 16N^2 + 4Nxp - 16N \Rightarrow y_p^2 = x_p^2 - 4Nxp \Rightarrow (-x_p + 4N, y_p) \in \mathcal{B}_N(x, y)\). (iii) From the symmetry of \(\mathcal{B}_N(x, y)\) with respect to the \((Ox)\) axis, we obtain \((-x_p + 4N, -y_p) \in \mathcal{B}_N(x, y)\). □

Lemma 1. \(\forall a \in \mathbb{Z}\), set \(x = (N + a)^2\); then, \((x, y) \in \mathcal{B}_N(x, y)\) if and only if \(a = 1\).

Proof. Set \(x = (N + a)^2\); then, \(y^2 = (N + a)^4 + 4N\) is square if and only if \(\delta = (a - 2)^2 - a^2 = 0\), which is impossible except for \(a = 1\), since \((a-2)^2 - a^2 = 0 \Rightarrow a = 4a = 4a = 1\). This yields that \(\forall a \in \mathbb{Z}\), \(x = (N + a)^2\) satisfies \(y^2 = x^2 - 4Nx\) if and only if \(a = 1\). □

Remark 1. Over \(\mathbb{Z}\), \(x^2 - 4Nx\) is square only if either \(x\) and \(x - 4N\) are squares or \(x - 4N\) such that \(x/(x - 4N) = k\), \(k \in \mathbb{Z}\).

Theorem 1. Consider \(\mathcal{B}_N\) over \(\mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0}\) denoted as \(\mathcal{B}_N(x, y)\). Then, \(\forall P = (x_p, y_p) \in \mathcal{B}_N(x, y)\), \((x_p, y_p) \in \{(x, y) \in \mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0} | x \leq (N + 1)^2\} \cap \{(x, y) \in \mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0} | y \leq (N + 1)^2\} \cap \{(x, y) \in \mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0} | x \geq (N + 1)^2\} \cap \{(x, y) \in \mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0} | y \geq (N + 1)^2\}\). Proof. It is not difficult to see that \(y^2 = x^2 - 4Nx \geq 0 \Rightarrow 0 \leq x \leq (N + 1)^2\); this holds if and only if \(a = 1\). Now assume there exists \(x > (N + 1)^2\); in this case, \(\exists b \in \mathbb{Z}_{\geq 0}\) such that \(x = (N + 1)^2 + b\). Then,
0 \Rightarrow N = 0, which is once more absurd since \( N \neq 0 \).

\[ \exists b \in \mathbb{Z}_{\geq 0}/x = (N + 1)^2 + b \text{ satisfying } y^2 = x^2 - 4Nx, \]
\[ \Rightarrow x \in [4N, (N + 1)^2]. \]

If \( x = 4N, y^2 = 16N^2 - 4N(4N) = 0, \Rightarrow y = 0. \) Also, if
\[ x = (N + 1)^2, \quad y^2 = (N + 1)^2[2(N + 1)^2 - 4N] = (N + 1)^2\]
\[ (N^2 + 2N + 1 - 4N) = (N + 1)^2(N - 1)^2 = (N^2 - 1)^2, \Rightarrow y = N^2 - 1, \text{ and thus } y \in [4N, (N + 1)^2]. \]

\[ \forall P = (x^p, y^p) \in \mathbb{R}_N(x, y)_{x \geq 0}, \quad (x^p, y^p) \in [4N, N(N + 2) + 1] \times [0, N^2 - 1]. \]

**Proposition 5**

\((p.1)\) If \( N = N_a \times N_b \), then there exists an injective homomorphism

\[ \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \]
\[ \forall (x_a, y_a), (x_b, y_b) \in \mathcal{R}_N(x, y), (x_a, y_a) \in \mathcal{R}_N(x, y), \]
\[ \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \]

(p.2) More generally, there is an injective homomorphism

\[ \prod_{\alpha = 1}^{z} \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \times \cdots \times \mathcal{R}_N(x, y) \]
\[ \forall (x^p, y^p, z^p) \in \mathcal{R}_N(x, y), \]
\[ \prod_{\alpha = 1}^{z} \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \]

Proof

\((p.1)\) Set \( N = N_a \times N_b \) and consider \( \mathcal{R}_{N_a}(x, y), \mathcal{R}_{N_b}(x, y) \) and \( \mathcal{R}_N(x, y) \) and consider the following morphism:

\[ \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \]
\[ \Rightarrow \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \]
\[ ((x_a, y_a), (x_b, y_b)) \Rightarrow \left( x_a N_{N_a}, y_a N_{N_a}, x_b N_{N_b}, y_b N_{N_b} \right). \]

We clearly see that it is a morphism since it splits into

\[ \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \]
\[ \forall (x^p, y^p, z^p) \in \mathcal{R}_N(x, y), \]
\[ \prod_{\alpha = 1}^{z} \mathcal{R}_N(x, y) \times \mathcal{R}_N(x, y) \]

\[(22)\]

\[ \left( x_a N_{N_a}, y_a N_{N_a}, x_b N_{N_b}, y_b N_{N_b} \right) = \left( x_a N_{N_a}, y_a N_{N_a}, x_b N_{N_b}, y_b N_{N_b} \right) \]
\[ \Rightarrow \left\{ \begin{array}{l}
 x_a N_{N_a} = x_a' N_{N_a}, \quad y_a N_{N_a} = y_a' N_{N_a} \\
 x_b N_{N_b} = x_b' N_{N_b}, \quad y_b N_{N_b} = y_b' N_{N_b}
 \end{array} \right. \]
\[ \Rightarrow \left\{ \begin{array}{l}
 x_a = x_a', \quad y_a = y_a' \\
 x_b = x_b', \quad y_b = y_b'
 \end{array} \right. \]

\[(23)\]
Hence, \( X_{N_a \times N_b} \to X_{N'}^{P_1, P_2} = X_{N_a \times N_b} \to X_{N'}^{P_1, P_2} \Leftrightarrow P_1 = P_1' \) and \( P_2 = P_2' \), hence the injection. 

(p.2) This comes straightforward from (p.1). □

Example 2. We consider the two hyperbolas plotted in Figure 1.

(i) \( N = 221 = N_a \times N_b = 13 \times 17 \):

\[
\begin{align*}
\mathcal{B}_{221}(x, y)_{|x| \geq 4N} &= \{(844, 0), (900, 120), (3332, 2856), (4212, 3744), (49284, 48840)\}, \\
\mathcal{B}_{13}(x, y)_{|x| \geq 2N} &= \{(52, 0), (196, 168)\}, \\
\mathcal{B}_{17}(x, y) &= \{(68, 0), (324, 288)\}, \\
\chi_{13 \times 17 \to 221} : \mathcal{B}_{13}(x, y)_{|x| \geq 2N} \times \mathcal{B}_{17}(x, y) \to \mathcal{B}_{221}(x, y)_{|x| \geq 4N} \\
&\cdot \left( (x, y, x_0, y_0) \right) \to \left( (17x_1, 17y_1), (13x_0, 13y_0) \right), \\
\chi_{13} \to 221(52, 0) &= (17 \times 52, 17 \times 0) = (884, 0) \in \mathcal{B}_{221}(x, y), \\
\chi_{13} \to 221(196, 168) &= (17 \times 196, 17 \times 168) = (3332, 2856) \in \mathcal{B}_{221}(x, y), \\
\chi_{17} \to 221(68, 0) &= (13 \times 68, 13 \times 0) = (884, 0) \in \mathcal{B}_{221}(x, y), \\
\chi_{17} \to 221(324, 288) &= (13 \times 324, 13 \times 288) = (4212, 3744) \in \mathcal{B}_{221}(x, y).
\end{align*}
\]

(ii) \( N = 210 = 2 	imes 3 \times 5 \times 7 \):

\[
\mathcal{B}_{210}(x, y)_{|x| \geq 2N} = \left\{ (840, 0), (841, 29), (845, 65), (847, 77), (864, 144), \\
(867, 153), (875, 175), (896, 224), (945, 315), (961, 341), (968, 352) \right\}, (1000, 400), \\
(1029, 441), (1083, 513), (1120, 560), (1183, 637), (1215, 675), \\
(1352, 832), (1369, 851), (1445, 935), (1512, 1008), (1681, 1189), (1715, 1225), \\
(1920, 1440), (2023, 1547), (2209, 1739), (2541, 2079), (2645, 2185), \\
(2888, 2432), (3375, 2925), (3584, 3136), (4107, 3663), (4840, 4400), (5329, 4891), \\
(6727, 6293), (7776, 7344), (9245, 8815), (11449, 11021), (15123, 14697) \\
, (22472, 22048), (44521, 44099) \right\}
\]

\[
\mathcal{B}_{2}(x, y)_{|x| \geq 2N} = \{(8, 0), (9, 3)\}, \\
\mathcal{B}_{3}(x, y) = \{(12, 0), (16, 8)\}, \\
\mathcal{B}_{5}(x, y) = \{(20, 0), (36, 24)\}, \\
\mathcal{B}_{7}(x, y) = \{(28, 0), (64, 48)\}, \\
\chi_{2 \times 3 \times 5 \times 7 \to 210} : \mathcal{B}_{2}(x, y) \times \mathcal{B}_{3}(x, y) \times \mathcal{B}_{5}(x, y) \times \mathcal{B}_{7}(x, y) \to \\
\prod_{i=1}^{4} \mathcal{B}_{210}(x, y) = \mathcal{B}_{210}(x, y) \times \cdots \times \mathcal{B}_{210}(x, y) \\
\cdot \left( (x, y, x_0, y_0) \right) \to \left( (105x_1, 105y_1), (70x_2, 70y_2), \\
(42x_3, 42y_3), (30x_4, 30y_4) \right), \\
\chi_{2} \to 210(8, 0) &= (105 \times 8, 105 \times 0) = (840, 0) \in \mathcal{B}_{210}(x, y), \\
\chi_{2} \to 210(9, 3) &= (105 \times 9, 105 \times 3) = (945, 315) \in \mathcal{B}_{210}(x, y), \\
\chi_{3} \to 210(12, 0) &= (70 \times 12, 70 \times 0) = (840, 0) \in \mathcal{B}_{210}(x, y), \\
\chi_{3} \to 210(16, 8) &= (70 \times 16, 70 \times 8) = (1120, 560) \in \mathcal{B}_{210}(x, y), \\
\chi_{5} \to 210(20, 0) &= (42 \times 20, 42 \times 0) = (840, 0) \in \mathcal{B}_{210}(x, y), \\
\chi_{5} \to 210(36, 24) &= (42 \times 36, 42 \times 24) = (1512, 1008) \in \mathcal{B}_{210}(x, y), \\
\chi_{7} \to 210(28, 0) &= (30 \times 28, 30 \times 0) = (840, 0) \in \mathcal{B}_{210}(x, y), \\
\chi_{7} \to 210(64, 48) &= (30 \times 64, 30 \times 48) = (1920, 1440) \in \mathcal{B}_{210}(x, y).
Definition 2. A prime divisor of an integer \( n \) is any prime number \( p \in \text{Div} (n) \). We denote \( \pi_p (n) \) as the set of all prime divisors of \( n \) and \( |\pi_p (n)| \) as the number of prime divisors of \( n \).

Example 3. 5 is a prime divisor of 40 since \( n \in \text{Div} (40) = \{1, 2, 4, 5, 8, 10, 20, 40\} \). \( \pi_p (40) = \{2, 5\} \) and \( |\pi_p (40)| = 2 \).

Proposition 6. Set \( N = \prod_{i=1}^{d} p_i \), \( p_i \) primes and consider \( B_N (x,y)_{x \geq 4N} = \{(x,y) \in \mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0} | x^2 = 4N y \} \). Set \( n = |\pi_p (N)| \) and \( U_n \) as the cardinal of \( B_N (x,y)_{x \geq 4N} \). Then, \( U_n = 3U_{n-1} - 1 \), \( n \geq 1 \) with \( U_0 = 1 \). In this case, we have the induction relation \( U_{n+2} = 2U_{n+1} + 3U_n - 2 \) and the sum of cardinals of \( B_N (x,y)_{x \geq 4N} \), given by the general term \( U_n \) is \( S_n = \sum_{i=1}^{n} U_i = (1/2)n - (3/4)(1 - 3^n) \).

Proof. \( n = |\pi_p (N)| \), \( U_n = \#B_N (x,y)_{x \geq 4N} = 3U_{n-1} - 1 \) with \( U_0 = 1 \), i.e., \( \#B_N (x,y)_{x \geq 4m} = U_{|\pi_p (m)|} = 3U_{|\pi_p (m)| - 1} - 1 \).

By induction on \( n \), we have

For \( n = 1 \), \( U_1 = 3U_0 - 1 = 2 \) (true).

For \( n = 2 \), \( U_2 = 3U_1 - 1 = 5 \) (true).

Assume the relation to be true for \( n \), i.e., \( U_n = 3U_{n-1} - 1 \), and let us show the relation to be true for \( n + 1 \).

\[
U_{|\pi_p (m)| + 1} = 3 \left( 3U_{|\pi_p (m)| - 1} - 1 \right) - 1 = 3U_{|\pi_p (m)|} - 1 = 3U_n - 1 = U_{n+1}.
\]

(26)

By the same,

\[
U_{n+1} = 3(U_n - 1) + 2 = 3U_n - 1,
\]

(27)

\[
U_{n+2} = 3(U_{n+1} - 1) + 2 = 3U_{n+1} - 1.
\]

(28)

By substituting (27) and (28), we obtain

\[
U_{n+2} + U_{n+1} = 3U_{n+1} - 1 + 3U_n - 1 = 3U_{n+1} + 3U_n - 2 \Rightarrow U_{n+2} = 2U_{n+1} + 3U_n - 2.
\]

(29)

For \( S_n \):
\[ U_5 = 3U_4 - 1 = 3(3^4U_0 - 3^3 - 3^2 - 3 - 1) - 1 = 3^5U_0 - 3^4 - 3^3 - 3^2 - 3 - 1, \]
\[ U_6 = 3U_5 - 1 = 3(3^5U_0 - 3^4 - 3^3 - 3^2 - 3 - 1) - 1 = 3^6U_0 - 3^5 - 3^4 - 3^3 - 3^2 - 3 - 1, \]
\[ \vdots \]
\[ U_n = 3U_{n-1} - 1 = 3^nU_0 - \sum_{i=0}^{n-1} 3^i = 3^n - \sum_{i=0}^{n-1} 3^i \text{ since } U_0 = 1 \]

\[ \sum_{j=1}^{n} U_j = \sum_{j=1}^{n} (3U_{j-1} - 1) = \sum_{j=1}^{n} \left( 3^j - \sum_{i=0}^{j-1} 3^i \right) \]
\[ = \sum_{j=1}^{n} 3^j - \sum_{j=1}^{n} \sum_{i=0}^{j-1} 3^i = \sum_{j=1}^{n} 3^j - \sum_{j=1}^{n} \frac{1 - 3^j}{1 - 3} = \sum_{j=1}^{n} 3^j + \frac{1}{2} \sum_{j=1}^{n} (1 - 3^j) = \sum_{j=1}^{n} 3^j + \frac{1}{2} n - \frac{1}{2} \sum_{j=1}^{n} 3^j \]
\[ = \frac{1}{2} n + \frac{1}{2} \sum_{j=1}^{n} 3^j = \frac{1}{2} n - \frac{3}{4} (1 - 3^n) \Rightarrow S_n = \sum_{j=1}^{n} U_j = \frac{1}{2} n - \frac{3}{4} (1 - 3^n). \]

**Example 4**

Verification:

(i) \( m = 253, \quad n = |\pi_p(m)| = 2, \quad \text{and} \quad U_2 = 3U_1 - 1, \)
knowing \( U_1 = 3U_0 - 1 = 3(1) - 1 = 2 \) since \( U_0 = 1. \)
Thus, \( U_2 = 3(2) - 1 = 5 \Rightarrow |R_{253}(x, y)_{|x \leq 4m}| = 5. \)

\[ R_{253}(x, y)_{|x \leq 4m} = \{(1012, 0), (1156, 408), (3312, 2760), (6336, 5808), (64, 516, 64, 008)\}, \]
\[ |R_{253}(x, y)_{|x \leq 4m}| = 5. \]

(ii) \( m = 30 \text{ and } n = |\pi_p(m)| = 3, U_3 = 3U_2 - 1 \)
knowing \( U_2 = 5, \quad \text{and thus} \quad U_3 = 3(5) - 1 = 14 \Rightarrow |R_{30}(x, y)_{|x \leq 4m}| = 14. \)

\[ R_{30}(x, y)_{|x \leq 4m} = \left\{ (120, 0), (121, 11), (125, 25), (128, 32), \right. \]
\[ \quad (135, 45), (147, 63), (160, 80), (169, 91), \]
\[ \left. (216, 144), (245, 175), (289, 221), (363, 297), (512, 448), (961, 899) \right\}, \]

and thus \( |R_{30}(x, y)_{|x \leq 4m}| = 14. \)

(iii) \( m = 2002, \quad n = |\pi_p(m)| = 4, \quad \text{and} \quad U_4 = 3U_3 - 1 \)
knowing \( U_3 = 14, \quad \text{and thus} \quad U_4 = 3(14) - 1 = 41 \Rightarrow |R_{2002}(x, y)_{|x \leq 4m}| = 41. \)

Verification:
and thus $|\mathcal{B}_{2002}(x, y)|_{x < 4m} = 41$.

**Theorem 2**

1. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 5$.

2. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 14$.

3. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 41$.

4. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 2$.

5. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 41$.

6. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 2$.

7. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 41$.

More generally, $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 4 \mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} + 1 \mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} - 2$.

**Proof**

(i) (2), (3), (6), and (9) come straightforwardly from the Proposition 6. Nevertheless, we give other proofs for (2) and (3) using injective homomorphisms.

1. Assume $\mathbb{P}$ prime; then, $\mathcal{B}(\mathbb{P}, 1) = \mathbb{P}$. The only injective homomorphisms in $\mathcal{B}(\mathbb{P}, 1)$ are $\chi_{1 \rightarrow \mathbb{P}}$, giving the point $(\mathbb{P}, 0)$ and the trivial automorphism $\chi_{\mathbb{P} \rightarrow \mathbb{P}}$, giving the point $(\mathbb{P}, 1)$.

2. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 2$.

3. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 41$.

4. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 2$.

5. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 41$.

6. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 2$.

7. If $N = \mathbb{P} \times \mathbb{P}$, where $\mathbb{P}$ and $\mathbb{P}$ are distinct primes, then $\mathcal{B}(\mathbb{P} \times \mathbb{P}, (x, y))_{\mathbb{P} \times \mathbb{P}} = 41$.
morphisms obtained with $\alpha$ from the induction hypothesis, there is now the new injective morphism got with the multiplication of $N$ by $N_a$. In this case, $|B_N(x, y)|_{N=4N} = \alpha + 1 = 1 + 2$. One deduces from (11) that $\text{Card}(B_N(x, y)_{N=4N}) = 4(\text{Card}(B_N(x, y)_{N=4N})) - 4(4(\alpha + 1) - 2 = 4\alpha + 2$.

(7) From Proposition 5, $\forall i \in \text{Div}(N), \exists k \in \mathbb{N}$: $B_N(x, y) \rightarrow B_N(x, y)$, it is clear that $\text{Card}(\text{Div}(N)) \leq \text{Card}(B_N(x, y)_{N=4N})$. By the same, we have injective homomorphisms obtained by composition $\forall i, j \in \text{Div}(N)$, $i + j = N = ((i + j)^2, i^2 - j^2) \in B_N(x, y)$ and we have the injective homomorphisms $\chi_{i,j} \rightarrow N$. Therefore, $\text{Card}(B_N(x, y)_{N=4N}) = \text{Card}(\text{Div}(N)) + \text{Card}(\{i, j \in \text{Div}(N) \mid i \cdot j = N\})$.

Then, for each $(i, j)$ verifying this condition, we can express this condition according to the Kronecker symbol. Indeed for the injective homomorphism $\chi_{i,j} \rightarrow N$, if $i = j$, there is no point since $i \cdot j = N$. If $i \neq j$, we have a point since $i \cdot j \in N$. Hence, $\text{Card}(B_N(x, y)_{N=4N}) = \text{Card}(\text{Div}(N)) + \sum_{i,j \in \text{Div}(N) \mid i \cdot j = N} (1 - \delta_{ij})$. From (11), we deduce that $\text{Card}(B_N(x, y)_{N=4N}) = 4\text{Card}(\text{Div}(N)) + \sum_{i,j \in \text{Div}(N) \mid i \cdot j = N} (1 - \delta_{ij}) = 4\text{Card}(\text{Div}(N)) + \sum_{i,j \in \text{Div}(N) \mid i \cdot j = N} (1 - \delta_{ij}) = 2$.

\section{Proposition 7.} The cardinal of $B_N$ over $\mathbb{Z}$ is given by the sequence $U_n^* = 6(2U_{n-1} - 1)$ and the sum of this sequence is $S_n^* = 2n - 3(1 - 3^n)$.

\textbf{Proof.} These results are straightforward from Theorem 2. $U_n^* = 4U_{n-1} - 2$ from the Proposition 6. Then, $U_n^* = 4(3U_{n-1} - 1) - 2 = 12U_{n-1} - 6 = 6(2U_{n-1} - 1)$. Also, $S_n^* = 4S_n = 4(1/2n - (3/4)(1 - 3^n)) = 2n - 3(1 - 3^n)$.

Plots of $U_n^*, S_n^*,$ and $S_n^*$ for different values of $n$ based on the data given by Table 1 for different distinct primes.

Comment on the plots in Figure 2 plotted with data from Table 1, from the first plot on the left corresponding to cardinals and sums of cardinals of $B_N(x, y)_{N=4N}$ we observe that the number of solutions grow quasi-exponentially with the number of distinct prime factors of $n$. In other words, the more distinct the prime factors of $n$, the bigger the algebraic set of $B_N$. Also, from the second plot (on the right), we observe that asymptotically $B_N(x, y)_{N=4N}$ and $B_N(x, y)_{N=4N}$ have the same behavior. In other words, knowing $B_N$ over positive integers gives as much information as knowing $B_N$ over the whole integers.

\section{Theorem 3.} If $N = N_a \times N_b$, $N_a$ and $N_b$ are primes, then $B_N(x, y)_{N=4N} = \langle P_1, P_2 \rangle = \langle P_a, P_1, P_2, P_3, P_4 \rangle$ with $P_3 = P_1 + P_2$, $P_4 = P_2 + P_1 = P_1 + 2P_2$ where $P_1 = ((N_a + N_b)^2, (N_a - N_b)^2), P_2 = (N_a(N_a + 1)^2, N_b(N_b^2 - 1)), P_3 = (N_a(N_a + 1)^2, N_a(N_a - 1)), P_4 = ((N + 1)^2, N^2 - 1)$.

\textbf{Proof.} $N = N_a \times N_b$, with $N_a$ and $N_b$ primes, then $\text{Div}(N) = \{1, N_a, N_b, N\} \text{ and } \text{Div}(N) = 4$. By Proposition 6 and Theorem 2, $\text{Card}(B_N(x, y)_{N=4N}) = U_2 = 5$.

$B_N(x, y)_{N=4N} = \{P_0, P_1, P_2, P_3, P_4\}$. Furthermore, from Theorem 3, $(N_a + N_b)^2, (N_a - N_b)^2), (N_a(N_a + 1)^2, N_b(N_b^2 - 1)), (N_a(N_a + 1)^2, N_a(N_a - 1)), (N + 1)^2, N^2 - 1 \in B_N(x, y)_{N=4N}$. Considering the addition law on $B_N(x, y)_{N=4N}$ given by Proposition 1 and setting $P_1 = \langle (N_a + N_b)^2, (N_a - N_b)^2 \rangle, P_2 = \langle (N_a(N_a + 1)^2, N_b(N_b^2 - 1) \rangle, P_3 = \langle (N_a(N_a + 1)^2, N_a(N_a - 1) \rangle, (N + 1)^2, N^2 - 1 \rangle$ one verifies as well in the polynomial ring $Q[N_a, N_b, N]$ that $P_1 + P_2 + P_3 + P_4 = P_1 + 2P_2 = P_a$.

Thus, $B_N(x, y)_{N=4N} = \{P_0, P_1\}$. It is not hard to see that $(B_N(x, y)_{N=4N}, +, \cdot)$ is a $2$-dimensional $Q$-vector space with basis $\{P_0, P_1\}$.

\section{3. Application of $B_N$ Parametrization to the Lattice Points on $x^2 - y^2 = N$ Fermat Equation}

In this section, we present results related to the lattice points on the arc of the hyperbola $x^2 - y^2 = N$ using results from $B_N$ parametrization.

\section{Theorem 4.} $\forall (a, b) \in B_N(x, y)_{N=4N}$, if $\exists x \in \mathbb{Z}$ such that $a = 4x^2$, then $x$ verifies $x^2 - y^2 = N$. In this case, for positive lattice points, $\sqrt{N}$ is the lower bound for $x$.

\textbf{Proof.} Consider $XY = N$, with $X = x + y$ and $Y = x - y$ which yields $x^2 - y^2 = N$.

\[
(x + y - (x - y))^2 = (x + y)^2 + (x - y)^2 - 2N = [(x + y + x - y)^2 - 2N] - 2N = (2x^2) - 4N.
\]

Set $(2x^2) = a; \text{ then, } 4x^2 = a; \text{ and } a = 4N$.

Then, there exists $b \in \mathbb{Z}/b^2 = a(a - 4N) = a^2 - 4Na = B_N(x, y)_{N=4N}$. Hence, $\forall (a, b) \in B_N(x, y)_{N=4N}$, if $\exists x \in \mathbb{Z}/a = 4x^2, \Rightarrow \exists y \in \mathbb{Z}/x^2 - y^2 = N$. Also, as $a \geq 4N$, then $4x^2 \geq 4N$, considering positive $x, \Rightarrow x \geq \sqrt{N}$.

From now on, we denote $H_N = \{x, y \in \mathbb{Z}/x^2 - y^2 = N\}$ and $S$ as the algebraic set of $H_N$ over the integers.

\section{Theorem 5.} $\forall (x, y) \in Z^2$, $(x, y) \in H_N$; then, $(x, y) \in [(N/\sqrt{2})^2, (1/2)(N + 1)]$.

\textbf{Proof.} Assume $(x, y) \in Z^2$, then $(x, y) \in H_N$.

From Theorem 1, $\forall (a, b) \in B_N(x, y)_{N=4N}$, $(a, b) \in [4N, N(N + 2) + 1] \times [0, N^2 - 1]$. From Theorem 4, $a = 4x^2$, where $(x, y)$ verifies $H_N$. If $a = 4N$, then $x^2 = N; \Rightarrow x = N/\sqrt{2}$, taking into account the assumption. Since we work over the integers, we take the ceiling for $x$. By the same, $y^2 = x^2 - N = 0; \Rightarrow y = 0$. If $a = (N + 1)^2$, then $x^2 = (1/4)(N + 1)^2; \Rightarrow x = (1/2)(N + 1)$. By the same, $y^2 = x^2 - N = (1/4)(N + 1)^2 - N = (1/4)(N - 1)^2; \Rightarrow y = (1/2)(N - 1)$ taking into account the assumption.
Lemma 2. Given the sequence
\[ N_k = \begin{cases} 
6 + 4k, & \text{if } k \geq 1, \\
4, & \text{if } k = 0.
\end{cases} \] (35)

Any term of this sequence and, respectively, any number of this form cannot be represented as difference of two squares.

Proof. If \( k = 0 \), \( N_0 = N = 4 \), as \( \text{Div}(4) = \{1, 2, 4\} \), we have from Proposition 5, the following homomorphisms \( X_1, X_2, X_N \). From Theorem 2, (17), Card \( (\mathcal{B}_4(x, y))_{x \in \{N/2\}} = 2 + 1 = 3 \), and considering Proposition 5, we have \( X_1, X_2, X_N \) (4N, 0) = (16, 0); \( X_2, X_N \) (9, 3) = 2 \times 9 \times 2 \times 3 = (18, 6), where \( 9, 3 \in \mathcal{B}_2(x, y) \) and \( X_N \) (16, 0, (18, 6), (25, 15)), \( \mathcal{B}(a, b) \in \mathcal{B}_4(x, y), a = 4^2, x \in \mathbb{Z} \). Hence, \( 4 \) cannot be written as difference of two squares.

For \( k > 0 \), \( N_k = N = 6 + 4k = 2(3 + 2k) \), and \( \text{Div}(N) = \{1, 2, 3 + 2k\} \cup \text{Div}(3 + 2k) \). By Proposition 3, since \( 2|N \), then \( (4N + 2)/3 \) (N/2) = \( (N + 3 + 2k)/2 \) \( \mathcal{B}_N(x, y) \). Also, as \( 3 + 2k|N \), then \( (3 + 2k)N + 2, 3(2 + k)^2 - 2 \) \( \mathcal{B}_N(x, y) \).

By induction, for \( k = 1, N_1 = N = 10 \), Div \( (N) = \{1, 2, 5, 10\} \). From Theorem 2, Card \( (\mathcal{B}_n(x, y))_{x \in \{N/2\}} = 5 \). We have from Proposition 5 the following homomorphisms: \( X_1, X_2, X_N \). From Theorem 2, Card \( (\mathcal{B}_N(x, y))_{x \in \{N/2\}} = 5 \). We have from Proposition 5 the following homomorphisms: \( X_1, X_2, X_N \), and from Proposition 3, the following points: \( 1|N \rightarrow (4N, 0) = (40, 0) \in \mathcal{B}_1(x, y), 2|N \rightarrow (4N + (N/2), 3(2)/2) = (45, 15) \in \mathcal{B}_2(x, y), \) \( 3|N \rightarrow (7N + (N/5), 225(N/5)) = (72, 48) \in \mathcal{B}_3(x, y) \), \( N|N \rightarrow (N + 2N + 1, N^2 - 1) = (121, 99) \in \mathcal{B}_N(x, y) \), and since \( 2 \times 5 = 10 \), then \( (5 + 2)^2, 2^2 - 2^2 = (49, 21) \in \mathcal{B}_N(x, y) \). Thus, \( \mathcal{B}_N(x, y)_{x \in \{0, 45, 49, 21, 72, 48, 121, 99\}} \). \( \mathcal{B}(a, b) \in \mathcal{B}_N(x, y), a = 4^2, x \in \mathbb{Z} \). Hence, \( 10 \) cannot be represented as difference of two squares.

For \( k = 2, N_2 = N = 14, 2|N \rightarrow (4N, 0) = (56, 0) \in \mathcal{B}_1(x, y), 2|N \rightarrow (4N + (N/2), 3(2)/2) = (63, 21) \in \mathcal{B}_2(x, y), \) \( 3|N \rightarrow (7N + (N/7), (7^2 - 1)/(7 - 1)) = (128, 96) \in \mathcal{B}_3(x, y) \), and since \( 2 \times 7 = 14 \), then \( (7 + 2)^2, 7^2 - 2^2 = (81, 45) \in \mathcal{B}_N(x, y) \). Thus, \( \mathcal{B}_N(x, y)_{x \in \{56, 0, 63, 21, 81, 45, 128, 96, 225, 195\}} \). \( \mathcal{B}(a, b) \in \mathcal{B}_N(x, y), a = 4^2, x \in \mathbb{Z} \). Hence, \( 10 \) cannot be represented as difference of two squares.

Assume the assumption to be true for \( k \), i.e., for the term \( N_k \), and let us show that it is true for \( k + 1 \).

\[ N_{k+1} = N = 6 + 4(k + 1) = 2(3 + 2(k + 1)) = 2(3 + 2k) + 2(2) = N_k + 4. \] (36)
Theorem 6. Consider the Fermat–Diophantine equation $x^2 - y^2 = N$. If $4|(N-6)$, i.e., $(N-6) \equiv 0 \mod 4$, then $S = \emptyset$.

Proof. If $N$ is prime, from Theorem 2,

1. $\text{Card}(B_N(x,y)_{x>N}) = 2$.

2. $\text{Card}(B_N(x,y)_{x=N}) = 4(2) - 2 = 6$. From Proposition 5, through injective homomorphisms, we have $B_N(x,y)_{x=N} = \{(4N,0),(N+1,2,N-2)\}$ (we first consider the possible values of $x$ and $y$) and as $x$ satisfies $x^2 - y^2 = N$, $y = (1/2)(N-1)$. Then, over $\mathbb{Z}$, $H_N = \{(1/2)(N+1),(1/2)(N-1)\}$. Taking into account symmetric properties of $H_N$, $(x,y) \in H_N \Rightarrow (-x,y)$, $(x,-y)$ and $(-x,-y) \in H_N$. Hence, $\text{Card}(H_N) = 4$ and

$S = \left\{ (-1/2)(N+1),(-1/2)(N-1),(-1/2)(N+1),(-1/2)(N-1) \right\}$.

Remark 2. If $N$ is an even prime, i.e., $N = 2$, then $\text{Card}(H_N) = 0$. This result is straightforward from Theorem 5, since $4|(N-6)$.

Proposition 9. If $N = N_a^\alpha$, $N_a$ is prime. Then, $\text{Card}(H_N) = 2(a+1)$. In this case,

$S = \left\{ \left( \frac{1}{2}(N_a^{\alpha+1} + N_a^i), \frac{1}{2}(N_a^{\alpha-i} - N_a^i) \right), \left( \frac{1}{2}(N_a^{\alpha+1} + N_a^i), \frac{1}{2}(N_a^{\alpha-i} - N_a^i) \right) \right\}_{\substack{\beta = 0,1,2, \ldots, \alpha \beta=0,1,2, \ldots, \alpha}}$

Proof. If $N = N_a^\alpha$, $N_a$ is prime, from Theorem 2,

1. $\text{Card}(B_N(x,y)_{x>N}) = \alpha + 1$.

2. $\text{Card}(B_N(x,y)_{x=N}) = 4a + 2$. From Proposition 5, through injective homomorphisms, we have $B_N(x,y)_{x=N} = \{(4N,0),(N+a^{\alpha-i} + N_a^i)^2, N_a^{(a-i)} - N_a^i, N_a^i(N_a^{(a-i)} + 1)^2, N_a^i(N_a^{(a-i)} - 1)\}_{i=0,1,2, \ldots, \alpha}$. It is obvious to see that $N_a^i(N_a^{(a-i)} + 1)^2$ is not square for all $i = 0, 1, \ldots, \alpha$. Now since $N_a$ is prime, then $N_a^{a-i}$ is a multiple of 4. From Theorem 4, for this case, $\exists x \in \mathbb{Z}$ such that $a = (N_a^{(a-i)} + N_a^i)^2 = 4x^2 \Rightarrow B_N(x,y)_{x=N}$ has a total of $\alpha + 1$ such terms since $i = 0, 1, \ldots, \alpha$. Now considering the redundant terms each time $i = \alpha - i$, since $i$ ranges from 0 to $\alpha$, then each term $N_a^{a-i} + N_a^i$ is the same as $N_a^i + N_a^{a-i}$ because of the commutativity of the additive law. Then, we have

\text{Proposition 10. Let } N = N_a \times N_b \text{ with } N_a, N_b \text{ odd primes. Then, } \text{Card}(H_N) = 8. \text{ In this case,}
Proof. Let \( N = N_a \times N_b \) with \( N_a, N_b \) odd primes, from Theorem 2,

1. \( \text{Card}(\mathcal{B}_N(x, y)_{|x| \leq 4N}) = 5. \)
2. \( \text{Card}(\mathcal{B}_N(x, y)_{|x| \leq 4N}) = 4(5) - 2 = 18. \)

From Proposition 5, through injective homomorphisms, we have

\[
\mathcal{B}_N(x, y)_{|x| \leq 4N} = \left\{ (4N, 0), (N_a, N_b), (N_a, N_b^2), (N_a^2, N_b), (N_b, N_a), (N_b, N_a^2), (N_a^2 - 1, N_b^2), (N_a^2, N_b^2 - 1) \right\}.
\]

Now since \( N_a, N_b, \) \( N = N_a N_b \) are an odd, \( N_a + N_b \) and \( N + 1 \) are even. Then, \( 4(N_a + N_b)^2 \) means 4 divides and \( 4(N + 1)^2. \) Set \( a_1 = (N_a + N_b)^2, \) \( a_2 = (N_a + N_b^2), \) \( a_3 = (N_a^2, N_b), \) \( a_4 = (N_a^2, N_b^2 - 1) \) and \( a_5 = (N_a^2, N_b^2, N_b^2 - 1) \) (we first consider the positive values of \( x \) and \( y \)), since \( x \) satisfies \( x^2 - y^2 = N, \) \( x \) satisfies \( x^2 - y^2 = N, \) \( x \) satisfies \( x^2 - y^2 = N, \) \( x \) satisfies \( x^2 - y^2 = N \) and \( x \) satisfies \( x^2 - y^2 = N. \)

Proposition 10. Let \( N = \prod_{i=1}^{n} p_i \) with, \( p_i \) odd primes, then 
\( \text{Card}(H_N) = U_{n-1} = 4U_{n-1} \), and let us prove it to be also true for \( n + 1. \)

For \( n + 1, \) \( \text{Card}(H_N) = U_{n+1} = 2U_{n}. \)

Proof. We give a proof by induction.

For \( n = 1, \) if \( p_1 = 2, \) \( \text{Card}(H_N) = 0 \) (true) from Remark 2

and if \( p_1 \neq 2, \) \( \text{Card}(H_N) = 4 \) (true) from Proposition 8.

Now assume the proposition is true for \( n, \) and let us prove it to be also true for \( n + 1. \)

For \( n + 1, \) \( \text{Card}(H_N) = U_{n+1} = 2U_{n}. \)

Remark 3. If \( N = N_a \times N_b, N_a, N_b \) primes Set \( N_a = 2, \) then \( S = \emptyset \) and \( \text{Card}(H_N) = 0. \)

Now, \( N - 6 = 2N_b = 2(2A) \) is even. Then, \( \exists A \in \mathbb{Z} \) such that \( N_b - 3 = 2A, \) \( N - 6 = 2(2A) = 4A. \) Since \( 4(1 - \delta_{2p_i}), \) \( \text{from Proposition 5, } S = \emptyset. \)

Proposition 11. Let \( N = \prod_{i=1}^{n} p_i \) with, \( p_i \) odd primes, then 
\( \text{Card}(H_N) = U_{n-1} = 2U_{n-1} \), and let us prove it to be also true for \( n + 1. \)

In this case, \( \text{Card}(H_N) = 2(1 + 1)(\beta + 1). \)
Proof. From Proposition 5, through injective homomorphisms, we have
\[ \mathcal{B}_N(x, y)_{|x^2 \leq 4N} = \left\{ \left( \prod_{i=1}^{\alpha} N_i^a + \prod_{i=j+1}^{n} N_i^b \right)^2, \prod_{i=1}^{\alpha} N_i^a + \prod_{i=j+1}^{n} N_i^b \right\}_{i \leq j \leq n}. \]

For each value of i, the value covers [0, β].

It is obvious to see that \( N_i^a N_i^b (N_i^a - N_i^b + 1)^2 \) is not square \( \forall i = 0, 1, \ldots, \alpha \) and \( j = 0, 1 \ldots, \beta \). Now since \( N_a \) and \( N_b \) are primes, then \( N_a^{-i} N_b^{-j} + N_i^a N_j^b \) is even \( \forall i = 0, 1, \ldots, \alpha \) and \( j = 0, 1, \ldots, \beta \), \( \Rightarrow (N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 \) is a multiple of 4. From Theorem 4, for this case, \( \exists x \in \mathbb{Z} \) such that \( a = (N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 \); then, considering the positive values of \( x \) and \( y \), \( x = (1/2)(N_a^{-i} N_b^{-j} + N_i^a N_j^b) \) and \( y^2 = x^2 - N = \left( (1/4)(N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 - N \right) = \left( (1/4)(N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 - N_a N_b \right) \).

Thus, over \( \mathbb{Z} \), Card \( (H_N) = (1/2)(\alpha + 1)(\beta + 1) \). Taking into account the symmetry of \( H_N \), \( (x, y) \in H_N \Rightarrow (-x, y), (x, -y) \) and \( (-x, -y) \in H_N \), then over \( \mathbb{Z} \), we have Card \( (H_N) = 4 \times (1/2)(\alpha + 1)(\beta + 1) \).

Since \( a = (N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 \), \( \Rightarrow x^2 = (1/4) (N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 \); then, considering the positive values of \( x \) and \( y \), \( x = (1/2)(N_a^{-i} N_b^{-j} + N_i^a N_j^b) \) and \( y^2 = x^2 - N = \left( (1/4)(N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 - N \right) = \left( (1/4)(N_a^{-i} N_b^{-j} + N_i^a N_j^b)^2 - N_a N_b \right) \).

Proposition 13. If \( N = \prod_{i=1}^{n} N_i^{\alpha_i} \), with \( N_i \) odd primes. Then, \( Card(H_N) = 2 \prod_{i=1}^{n} (\alpha_i + 1) \). In this case,

Now assume the assumption to be true for \( n \), and let us prove it to be true for \( n + 1 \).

\( N \cdot N_i^{\alpha_{i+1}} = \left( \prod_{i=1}^{n} N_i^{\alpha_i} \right) \cdot N_i^{\alpha_{i+1}} = \prod_{i=1}^{n+1} N_i^{\alpha_i} \), taking into account the assumption \( \Rightarrow Card(H_N) = 2 \prod_{i=1}^{n+1} (\alpha_i + 1) \). From Proposition 5, through injective homomorphisms, we have

It is obvious to see that \( \prod_{i=1}^{j} N_i^{\alpha_i} (\prod_{i=1}^{j} N_i^{\alpha_i} + 1)^2 \) is not square \( \forall i = 1, \ldots, n \) and \( j = 1, \ldots, n \). Now since \( N_i^{\alpha_i} \) is prime \( \forall i = 1, \ldots, n \), then \( \prod_{i=1}^{j} N_i^{\alpha_i} + \prod_{i=j+1}^{n} N_i^{\alpha_i} \) is even and \( (\prod_{i=1}^{j} N_i^{\alpha_i} + \prod_{i=j+1}^{n} N_i^{\alpha_i})^2 \) is a multiple of 4. From Theorem 4, for this case, \( \exists x \in \mathbb{Z} \) such that \( a = (\prod_{i=1}^{j} N_i^{\alpha_i} + \prod_{i=j+1}^{n} N_i^{\alpha_i})^2 = 4x^2 \). \( \Rightarrow x^2 = (1/4)(\prod_{i=1}^{j} N_i^{\alpha_i} + \prod_{i=j+1}^{n} N_i^{\alpha_i})^2 \).

Then
\[ y^2 = \frac{1}{4} \left( \prod_{i=1}^{j} N_i^{2\alpha_i} + \prod_{i=j+1}^{n} N_i^{2\alpha_i} + 2 \prod_{i=1}^{j} N_i^{\alpha_i} \prod_{i=j+1}^{n} N_i^{\alpha_i} - 4 \prod_{i=1}^{j} N_i^{\alpha_i} \prod_{i=j+1}^{n} N_i^{\alpha_i} \right) = \frac{1}{4} \left( \prod_{i=1}^{j} N_i^{\alpha_i} \prod_{i=j+1}^{n} N_i^{\alpha_i} \right)^2. \]
\[ y = (1/2) \left( \prod_{i=1}^{j} N_i^{n_i} - \prod_{i=j+1}^{n} N_i^{n_i} \right). \] Taking into account the symmetry of \( H_N \), \((x, y) \in H_N \Rightarrow (-x, y), (x, -y) \) and \((-x, -y) \in H_N \); then, over \( \mathbb{Z} \), we have

\[
S = \left\{ \left( \pm \frac{1}{2} \left( \prod_{i=1}^{j} N_i^{n_i} + \prod_{i=j+1}^{n} N_i^{n_i} \right) \right) \right\}
\]

\[ i \leq j \leq n. \] (45)

4. Discussion

We have exposed the forms of the Fermat equation \( x^2 - y^2 = N \), dependently on the different forms of \( N \), for which we have proved the cardinal over the integers to be 0, 4, and 8, of the form \( 2 \prod_{i=1}^{n} (a_i + 1) + 1 \) or \( (1 - \delta_{2p})2^{m+1} \).

Over \( \mathbb{Z}_{>0} \), \( x^2 - y^2 = N \) has only one nontrivial solution for a RSA modulus \( N \).

**Proposition 14.** \( \forall (x, y) \in \left[ \left( N^{1/2} \right), (1/2)(N + 1) \right] \times [0, (1/2) \left( N - 1 \right)] \), \((x, y) \in H_N \) with the probability \( P = \prod_{i=1}^{n} (a_i + 1)/N + 1 - 2 \left[ N^{1/2} \right] \).

**Proof.** Set \( N = \prod_{i=1}^{n} N_i^{n_i} \), with \( N_i \) odd primes. From Proposition 13, over \( \mathbb{Z}_{>0} \), Card \( (H_N) = (1/2) \prod_{i=1}^{n} (a_i + 1) \) and from Theorem 5, the length of the \( x \) interval is \( l = N + 1/2 - \left[ N^{1/2} \right] = N + 1 - 2 \left[ \sqrt{N} \right]/2 \). \( \Rightarrow P = \text{Card} (H_N) \left( \mathbb{Z}_{>0} / l \right) = \left( (1/2) \prod_{i=1}^{n} (a_i + 1)/N + 1 - 2 \left( \sqrt{N} \right)/2 \right) = \left( \prod_{i=1}^{n} (a_i + 1)/N + 1 - 2 \left( \sqrt{N} \right) \right). \) \( \square \)

5. Conclusion

In this paper, we have presented algebraic results on lattice points of the arc on the conics \( x^2 - dy^2 = N \) for \( d = 1 \), which is the Fermat factorization equation for which cardinals, forms of the algebraic set and exact upper and lower bounds are given using a particular hyperbola parametrization. These results provide further information on the structure of the algebraic set of this equation by exposing particularly the following.

(i) The general forms of lattice points.

(ii) The cardinals and the exact number of solutions.

(iii) The distribution of its lattice points over the integers.

As a future work, we shall apply these results in the square sieving methods of factorization (mainly the quadratic sieve) and evaluate any resulting impact and performance.

Data Availability

The algorithms were developed in Python, and the source codes are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References


