Hindawi
Journal of Mathematics
Volume 2022, Article ID 6360264, 18 pages
https://doi.org/10.1155/2022/6360264

Research Article

Lattice Points on the Fermat Factorization Method

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

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 $(N - 6) \equiv 0 \bmod 4$, Fermat's method fails. Otherwise, in terms of cardinality, it has, respectively, 4, 8, $2(\alpha + 1)$, $(1 - \delta_{2p_i})2^{n+1}$, and $2\prod_{i=1}^{n}(\alpha_i + 1)$ lattice pointts if N is an odd prime, $N = N_a \times N_b$ with N_a and N_b being odd primes, $N = N_a^{\alpha}$ with N_a being prime, $N = \prod_{i=1}^{n} p_i$ with p_i being distinct primes, and $N = \prod_{i=1}^{n} N_i^{\alpha_i}$ 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 $N = \prod_{i=1}^{j} p_i$, 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 integral 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 $\mathscr{B}_N(x, y) = \{(x, y) \in \mathbb{Q} \times \mathbb{Q}/y^2 = x^2 - 4Nx\}$, 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, 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:

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

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

$\mathscr{B}_N(x,y)_{|x\geq 4N} = \{(x,y) \in \mathbb{Z}_{\geq 4N}\times\mathbb{Z}_{\geq 0}/y^2 = x^2 - 4Nx\}$: algebraic set of integral points on $\mathscr{B}_N(x,y)$ whose x–coordinates are greater or equal to $4N$.

$\chi_{N_a\longrightarrow N_b}$: an injective homomorphism from $\mathscr{B}_{N_a}(x,y)$ to $\mathscr{B}_{N_b}(x,y)$.

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

Div(N_a): set of divisors of N_a.

$\pi_p(n)$: 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.

δ_{ij}: the Kronecker symbol.

2. BN Hyperbola Parametrization

A conic is an algebraic set satisfying an equation of the form $\alpha_1 x^2 + 2\alpha_2 xy + \alpha_2 y^2 + 2\alpha_3 x + 2\alpha_4 y + \alpha_5 = 0$, $(\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5) \in \mathbb{R}^5$ where $(\alpha_1,\alpha_2,\alpha_3) \neq (0,0,0)$. Setting $\mathscr{B}_N$ 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 $\mathscr{B}_n(X,Y,Z) = \{(X\colon Y\colon Z) \in \mathbb{P}^2(\mathbb{Q})/(Y^2/Z^2) = (X^2/Z^2) - 4N(X/Z)\} \Leftrightarrow \mathscr{B}_N(X,Y,Z) = \{(X\colon Y\colon Z) \in (\mathbb{P}^2(\mathbb{Q})/\,Y^2) = X^2 - 4NXZ\}$.

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

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

Proposition 1. *Consider the application*

$$+\colon \mathscr{B}_N(x,y)\times\mathscr{B}_N(x,y) \longrightarrow \mathscr{B}_N(x,y)(P,Q)\mapsto P+Q. \tag{1}$$

$P+Q$ is defined $\forall P = (x_p, y_p)$, $Q = (x_q, y_q) \in \mathscr{B}_N(x,y)$, by

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

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

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

$\mathscr{B}_N$ 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

$$\begin{cases} x - 2N = 2N\cosh(t) \\ y = 2N\sinh(t) \end{cases} \Rightarrow \begin{cases} \dfrac{x}{2N} - 1 = \cosh(t) \\ \dfrac{y}{2N} = \sinh(t) \end{cases} \quad \sin ce \quad \cosh^2(t) - \sinh^2(t) = 1,$$
$$t_1 + t_2 \in \left\{t \in \mathbb{Z}/\cosh^2(t) - \sinh^2(t) = 1\right\} where \begin{cases} \cosh(t_1 + t_2) = \cosh(t_1)\cosh(t_2) + \sinh(t_1)\sinh(t_2), \\ \sinh(t_1 + t_2) = \sinh(t_1)\cosh(t_2) + \cosh(t_1)\sinh(t_2). \end{cases} \tag{3}$$

Given two points $P = (x_p, y_p)$ and $Q = (x_q, y_q) \in \mathscr{B}_N(x, y)$,

$$\text{Set}\begin{cases} X_1 = \dfrac{x_p}{2N} - 1 = \cosh(t_1), \\ Y_1 = \dfrac{y_p}{2N} = \sinh(t_1), \end{cases} \qquad \begin{cases} X_2 = \dfrac{x_q}{2N} - 1 = \cosh(t_2), \\ Y_2 = \dfrac{y_q}{2N} = \sinh(t_2), \end{cases} \quad \text{We then have}\begin{cases} \cosh(t_1 + t_2) = X_1X_2 + Y_1Y_2, \\ \sinh(t_1 + t_2) = Y_1X_2 + X_1Y_2. \end{cases} \tag{4}$$

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

$$\begin{cases} \dfrac{x_{p+q}}{2N} - 1 = X_1X_2 + Y_1Y_2 \\ \dfrac{y_{p+q}}{2N} = Y_1X_2 + X_1Y_2 \end{cases} \Rightarrow \begin{cases} \dfrac{x_{p+q}}{2N} = X_1X_2 + Y_1Y_2 + 1 \\ \dfrac{y_{p+q}}{2N} = Y_1X_2 + X_1Y_2 \end{cases} \Rightarrow \begin{cases} x_{p+q} = 2N(X_1X_2 + Y_1Y_2 + 1) \\ y_{p+q} = 2N(Y_1X_2 + X_1Y_2) \end{cases},$$

$$\begin{aligned} X_1X_2 + Y_1Y_2 + 1 &= \left(\frac{x_p}{2N} - 1\right)\left(\frac{x_q}{2N} - 1\right) + \left(\frac{y_p}{2N}\right)\left(\frac{y_q}{2N}\right) + 1 = \frac{(x_p - 2N)(x_q - 2N) + y_py_q}{4N^2} + 1, \\ &\Rightarrow x_{p+q} = 2N(X_1X_2 + Y_1Y_2 + 1) = \frac{1}{2N}\left[(x_p - 2N)(x_q - 2N) + y_py_q\right] + 2N, \\ Y_1X_2 + X_1Y_2 &= \left(\frac{y_p}{2N}\right)\left(\frac{x_q}{2N} - 1\right) + \left(\frac{y_q}{2N}\right)\left(\frac{x_p}{2N} - 1\right) = \frac{1}{4N^2}\left[y_p(x_q - 2N) + y_q(x_p - 2N)\right] \\ &\Rightarrow y_{p+q} = 2N(Y_1X_2 + X_1Y_2) = \frac{1}{2N}\left[y_p(x_q - 2N) + y_q(x_p - 2N)\right]. \end{aligned} \tag{5}$$

We have both

$$\begin{cases} x_{p+q} = \dfrac{1}{2N}\left[(x_p - 2N)(x_q - 2N) + y_py_q\right] + 2N, \\ y_{p+q} = \dfrac{1}{2N}\left[y_p(x_q - 2N) + y_q(x_p - 2N)\right], \end{cases} \qquad \begin{cases} x_{2p} = \dfrac{1}{2N}\left[(x_p - 2N)^2 + y_p^2\right] + 2N, \\ y_{2p} = \dfrac{1}{N}\left(y_p(x_p - 2N)\right). \end{cases} \tag{6}$$

We denote + as the above defined additive law. This addition law is strongly unified since point doubling does exist and is well defined.

Now let us consider the application

$$\begin{aligned} + : \mathscr{B}_N(x, y) \times \mathscr{B}_N(x, y) &\longrightarrow \mathscr{B}_N(x, y) \\ (P, Q) &\mapsto P + Q. \end{aligned} \tag{7}$$

This application is an internal composition law since $P + Q \in \mathscr{B}_N(x, y)$, $(y^2_{p+q} = x^2_{p+q} - 4Nx_{p+q})$.

(i) Associativity: given 3 points $P = (x_p, y_p), Q = (x_q, y_q), T = (x_t, y_t) \in \mathscr{B}_N(x, y)$, here we show that $(P + Q) + T = P + (Q + T)$.

Note that this can be shown either geometrically or analytically, but here we give just the analytic proof.

Consider $(P + Q) + T$.

$$(P+Q)+T=\begin{cases} x_{(p+q)+t}=\frac{1}{2N}\left[\left(x_{(p+q)}-2N\right)\left(x_t-2N\right)+y_{(p+q)}y_t\right]+2N \\ y_{(p+q)+t}=\frac{1}{2N}\left[y_{(p+q)}\left(x_t-2N\right)+y_t\left(x_{(p+q)}-2N\right)\right] \end{cases}$$

$$=\begin{cases} x_{(p+q)+t}=\frac{1}{2N}\left[\left(\frac{1}{2N}\left[\left(x_p-2N\right)\left(x_q-2N\right)+y_py_q\right]+2N-2N\right)\left(x_t-2N\right)+\left(\frac{1}{2N}\left[y_p\left(x_q-2N\right)+y_q\left(x_p-2N\right)\right]\right)y_t\right]+2N \\ y_{(p+q)+t}=\frac{1}{2N}\left[\left(\frac{1}{2N}\left[y_p\left(x_q-2N\right)+y_q\left(x_p-2N\right)\right]\right)\left(x_t-2N\right)+y_t\left(\frac{1}{2N}\left[\left(x_p-2N\right)\left(x_q-2N\right)+y_py_q\right]+2N-2N\right)\right] \end{cases}$$

$$=\begin{cases} x_{(p+q)+t}=\frac{1}{2N}\left[\left(\frac{1}{2N}\left[\left(x_p-2N\right)\left(x_q-2N\right)+y_py_q\right]\right)\left(x_t-2N\right)+\left(\frac{1}{2N}\left[y_p\left(x_q-2N\right)+y_q\left(x_p-2N\right)\right]\right)y_t\right]+2N \\ y_{(p+q)+t}=\frac{1}{2N}\left[\left(\frac{1}{2N}\left[y_p\left(x_q-2N\right)+y_q\left(x_p-2N\right)\right]\right)\left(x_t-2N\right)+y_t\left(\frac{1}{2N}\left[\left(x_p-2N\right)\left(x_q-2N\right)+y_py_q\right]\right)\right]. \end{cases} \tag{8}$$

$$(9)=\begin{cases} x_{(p+q)+t}=\frac{1}{2N}\left[\frac{1}{2N}\left(x_p-2N\right)\left(x_q-2N\right)\left(x_t-2N\right)+\frac{1}{2N}y_py_q\left(x_t-2N\right)+\frac{1}{2N}y_py_t\left(x_q-2N\right)+\frac{1}{2N}y_qy_t\left(x_p-2N\right)\right]+2N, \\ y_{(p+q)+t}=\frac{1}{2N}\left[\frac{1}{2N}y_p\left(x_q-2N\right)\left(x_t-2N\right)+\frac{1}{2N}y_q\left(x_p-2N\right)\left(x_t-2N\right)+\frac{1}{2N}y_t\left(x_p-2N\right)\left(x_q-2N\right)+\frac{1}{2N}y_py_qy_t\right], \end{cases} \tag{9}$$

Secondly we consider $P+(Q+T)=\begin{cases} x_{p+(q+t)}=\frac{1}{2N}\left[\left(x_p-2N\right)\left(x_{(q+t)}-2N\right)+y_py_{(q+t)}\right]+2N \\ y_{p+(q+t)}=\frac{1}{2N}\left[y_p\left(x_{(q+t)}-2N\right)+y_{(q+t)}\left(x_p-2N\right)\right] \end{cases}$

$$=\begin{cases} x_{p+(q+t)}=\frac{1}{2N}\left[\left(x_p-2N\right)\left(\frac{1}{2N}\left[\left(x_q-2N\right)\left(x_t-2N\right)+y_qy_t\right]+2N-2N\right)+y_p\frac{1}{2N}\left[y_q\left(x_t-2N\right)+y_t\left(x_q-2N\right)\right]\right]+2N \\ y_{p+(q+t)}=\frac{1}{2N}\left[y_p\left(\frac{1}{2N}\left[\left(x_q-2N\right)\left(x_t-2N\right)+y_qy_t\right]+2N-2N\right)+\frac{1}{2N}\left[y_q\left(x_t-2N\right)+y_t\left(x_q-2N\right)\right]\left(x_p-2N\right)\right] \end{cases}$$

$$=\begin{cases} x_{p+(q+t)}=\frac{1}{2N}\left[\left(x_p-2N\right)\left(\frac{1}{2N}\left[\left(x_q-2N\right)\left(x_t-2N\right)+y_qy_t\right]\right)+y_p\frac{1}{2N}\left[y_q\left(x_t-2N\right)+y_t\left(x_q-2N\right)\right]\right]+2N \\ y_{p+(q+t)}=\frac{1}{2N}\left[y_p\left(\frac{1}{2N}\left[\left(x_q-2N\right)\left(x_t-2N\right)+y_qy_t\right]\right)+\frac{1}{2N}\left[y_q\left(x_t-2N\right)+y_t\left(x_q-2N\right)\right]\left(x_p-2N\right)\right], \end{cases} \tag{10}$$

$$(11)=\begin{cases} x_{p+(q+t)}=\frac{1}{2N}\left[\frac{1}{2N}\left(x_p-2N\right)\left(x_q-2N\right)\left(x_t-2N\right)+\frac{1}{2N}y_qy_t\left(x_p-2N\right)+\frac{1}{2N}y_py_q\left(x_t-2N\right)+\frac{1}{2N}y_py_t\left(x_q-2N\right)\right]+2N \\ y_{p+(q+t)}=\frac{1}{2N}\left[\frac{1}{2N}y_p\left(x_q-2N\right)\left(x_t-2N\right)+\frac{1}{2N}y_py_qy_t+\frac{1}{2N}y_q\left(x_t-2N\right)\left(x_p-2N\right)+\frac{1}{2N}y_t\left(x_q-2N\right)\left(x_p-2N\right)\right]. \end{cases} \tag{11}$$

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

$$P + \mathcal{O} = \begin{cases} x_{p+\mathcal{O}} = \dfrac{1}{2n}\left[\left(x_p - 2N\right)(4N - 2N) + y_p \times 0\right] + 2N = \dfrac{1}{2N}\left[2N\left(x_p - 2N\right)\right] + 2N = x_p \\ y_{p+\mathcal{O}} = \dfrac{1}{2N}\left[y_p(4N - 2N) + 0 \times \left(x_p - 2N\right)\right] = \dfrac{1}{2N}\left[2Ny_p\right] = y_p, \end{cases}$$
$$\mathcal{O} + P = \begin{cases} x_{\mathcal{O}+p} = \dfrac{1}{2N}\left[(4N - 2N)\left(x_p - 2N\right) + 0 \times y_p\right] + 2N = \dfrac{1}{2N}\left[2N\left(x_p - 2N\right)\right] + 2N = x_p \\ y_{\mathcal{O}+p} = \dfrac{1}{2N}\left[0 \times \left(x_p - 2N\right) + y_p(4N - 2N)\right] = \dfrac{1}{2N}\left[2Ny_p\right] = y_p. \end{cases} \tag{12}$$

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

(ii) Symmetric element: $\forall P = (x_p, y_p) \in \mathcal{B}(x, y), P' = (x_p, -y_p)$ 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

$$P + P' = \begin{cases} x_{p+p'} = \dfrac{1}{2N}\left[\left(x_p - 2N\right)^2 - y_p^2\right] + 2N = \dfrac{1}{2N}\left[x_p^2 - 4Nx_p + 4N^2 - y_p^2\right] + 2N = \dfrac{1}{2N}\left[4N^2\right] + 2N = 4N \\ y_{p+p'} = \dfrac{1}{2N}\left[y_p\left(x_p - 2N\right) - y_p\left(x_p - 2N\right)\right] = \dfrac{1}{2N}[0] = 0, \end{cases}$$
$$P' + P = \begin{cases} x_{p'+p} = \dfrac{1}{2N}\left[\left(x_p - 2N\right)^2 - y_p^2\right] + 2N = \dfrac{1}{2N}\left[x_p^2 - 4Nx_p + 4N^2 - y_p^2\right] + 2N = \dfrac{1}{2N}\left[4N^2\right] + 2N = 4N \\ y_{p'+p} = \dfrac{1}{2N}\left[-y_p\left(x_p - 2N\right) + y_p\left(x_p - 2N\right)\right] = \dfrac{1}{2N}[0] = 0. \end{cases} \tag{13}$$

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:

$$P + Q = \begin{cases} x_{p+q} = \dfrac{1}{2N}\left[\left(x_p - 2N\right)\left(x_q - 2N\right) + y_p y_q\right] + 2N = \dfrac{1}{2N}\left[\left(x_q - 2N\right)\left(x_p - 2N\right) + y_q y_p\right] + 2N = x_{q+p}, \\ y_{p+q} = \dfrac{1}{2N}\left[y_p\left(x_q - 2N\right) + y_q\left(x_p - 2N\right)\right] = \dfrac{1}{2N}\left[y_q\left(x_p - 2N\right) + y_p\left(x_q - 2N\right)\right] = y_{q+p}. \end{cases} \tag{14}$$

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

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:*

$$\chi\colon \mathcal{B}_{N_a}(x, y) \longrightarrow \mathcal{B}_{N_b}(x, y)(x, y) \mapsto \left(x\frac{N_b}{N_a}, y\frac{N_b}{N_a}\right), \tag{15}$$

defines a group homomorphism.

Proof. $\forall P = (x_p, y_p) \in \mathcal{B}_{N_a}(x, y)$, $\chi(P) = \chi(x_p, y_p) = (x_p(N_b/N_a), y_p(N_b/N_a)) \overset{?}{\in} \mathcal{B}_{N_b}(x, y)$. $(x_p(N_b/N_a), y_p(N_b/N_a)) \in \mathcal{B}_{N_b}(x, y) \Leftrightarrow (y_p(N_b/N_a))^2 = (x_p(N_b/N_a))^2 - 4N_b(x_p(N_b/N_a)) = x_p(N_b^2/N_a)((x_p/N_a) - 4) = N_b^2(x_p^2 - 4N_a x_p)/N_a^2 \Rightarrow (y_p(N_b/N_a))^2 = N_b^2 y_p^2/N_a^2 = (y_p(N_b/N_a))^2$. Thus, $(x_p(N_b/N_a), y_p(N_b/N_a)) \in \mathcal{B}_{N_b}(x, y)$.

Consider $\mathcal{O}_{\mathcal{B}_{N_a}} = (4N_a, 0)$ and $\mathcal{O}_{\mathcal{B}_{N_b}} = (4N_b, 0)$.

$$\chi\left(\mathcal{O}_{\mathcal{B}_{N_a}}\right) = \chi((4N_a, 0)) = \left(4N_a\frac{N_b}{N_a}, 0\frac{N_b}{N_a}\right) = (4N_b, 0) = \mathcal{O}_{\mathcal{B}_{N_b}} \Rightarrow \chi\left(\mathcal{O}_{\mathcal{B}_{N_a}}\right) = \mathcal{O}_{\mathcal{B}_{N_b}}\,(i_1). \tag{16}$$

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

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

$$\begin{aligned}
\chi(P+Q) &= \chi\begin{pmatrix} \dfrac{1}{2N_a}\left[\left(x_p - 2N_a\right)\left(x_q - 2N_a\right) + y_p y_q\right] + 2N_a, \\ \dfrac{1}{2N_a}\left[y_p\left(x_q - 2N_a\right) + y_q\left(x_p - 2N_a\right)\right] \end{pmatrix}, \\
&= \left(\frac{N_b}{2N_a^2}\left[\left(x_p - 2N_a\right)\left(x_q - 2N_a\right) + y_p y_q\right] + 2N_b, \frac{N_b}{2N_a^2}\left[y_p\left(x_q - 2N_a\right) + y_q\left(x_p - 2N_a\right)\right]\right).
\end{aligned} \tag{17}$$

$$\begin{aligned}
\chi(P) + \chi(Q) &= \left(x_p\frac{N_b}{N_a}, y_p\frac{N_b}{N_a}\right) + \left(x_q\frac{N_b}{N_a}, y_q\frac{N_b}{N_a}\right) \\
&= \begin{pmatrix} \dfrac{1}{2N_b}\left[\left(x_p\dfrac{N_b}{N_a} - 2N_b\right)\left(x_q\dfrac{N_b}{N_a} - 2N_b\right) + \dfrac{N_b^2}{N_a^2}y_p y_q\right] + 2N_b, \\ \dfrac{1}{2N_b}\left[y_p\dfrac{N_b}{N_a}\left(x_q\dfrac{N_b}{N_a} - 2N_b\right) + y_q\dfrac{N_b}{N_a}\left(x_p\dfrac{N_b}{N_a} - 2N_a\right)\right] \end{pmatrix} \\
&= \begin{pmatrix} \dfrac{1}{2N_b}\left[\dfrac{N_b}{N_a}\left(x_p - 2N_a\right)\dfrac{N_b}{N_a}\left(x_q - 2N_a\right) + \dfrac{N_b^2}{N_a^2}y_p y_q\right] + 2N_b, \\ \dfrac{1}{2N_b}\left[y_p\dfrac{N_b^2}{N_a^2}\left(x_q - 2N_a\right) + y_q\dfrac{N_b^2}{N_a^2}\left(x_p - 2N_a\right)\right] \end{pmatrix} \\
&= \begin{pmatrix} \dfrac{N_b}{N_a^2}\left[\left(x_p - 2N_a\right)\left(x_q - 2N_a\right) + y_p y_q\right] + 2N_b, \\ \dfrac{N_b}{N_a^2}\left[y_p\left(x_q - 2N_a\right) + y_q\left(x_p - 2N_a\right)\right] \end{pmatrix}.
\end{aligned} \tag{18}$$

$\chi(P+Q) = \chi(P) + \chi(Q)\,(i_3)$, (it is the relation (i_3)). Then, relations (i_1), (i_2), and $((i_3))$ imply that X is a group morphism

Furthermore,

$\text{Ker}(\chi) = \left\{(x, y) \in \mathcal{B}_{N_a}(x, y)/\chi(x, y) = \mathcal{O}_{\mathcal{B}_{N_b}}\right\} = \left\{\mathcal{O}_{\mathcal{B}_{N_a}}\right\}$.

χ is then injective and $\text{Im}(\chi) = \left\{(x', y') \in \mathcal{B}_{N_b}(x, y)/(x', y') = \chi(x, y)\forall(x, y) \in \mathcal{B}_{N_a}(x, y)\right\} = \mathcal{B}_{N_b}(x, y)$ since $\forall(x', y') \in \mathcal{B}_{N_b}(x, y), \exists(x, y) \in \mathcal{B}_{N_a}(x, y)$ such that $(x', y') = \chi(x, y)$. χ is also surjective. $\Rightarrow \chi$ is bijective.

Since χ is a homomorphism of group and bijective, then χ defines an isomorphism of groups. Thus, $\mathcal{B}_{N_a}(x, y)$ and $\mathcal{B}_{N_b}(x, y)$ are isomorphic. □

Definition 1. Given an integer N, we define $\text{Div}(N)$ as the set of all divisors of N. That is to say, $\text{Div}(N) = \{x \in \mathbb{Z}/x \mid N\}$.

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

Proposition 3

(i) If k_i, $k_j \in Div(N)$ such that $k_i \times k_j = N$, then $((k_i + k_j)^2, (k_i^2 - k_j^2))$, $(k_i(k_j + 1)^2, k_i(k_j^2 - 1)) \in \mathcal{B}_N(x, y)$.

(ii) If k_i, $k_j \in Div(N)\smallsetminus\{1, N\}$ with k_i, k_j primes, then $k_j/k_i|N$ and $((k_j + 2k_i)N_\alpha + k_i N_\beta, (k_j^2 - k_i^2)N_\gamma) \in \mathcal{B}_N(x, y)$ where $N_\alpha = N/k_i$, $N_\beta = n/k_j$, $N_\gamma = N/k_i k_j$.

(iii) More generally, if $k|N \Leftrightarrow ((k + 2)N + (N/k), (k^2 - 1/k)N) \in \mathcal{B}_N(x, y)$.

Proof

(i) If k_i, $k_j \in \mathrm{Div}(N)$, $k_i \times k_j = N$. $((k_i + k_j)^2, (k_i^2 - k_j^2)) \in \mathscr{B}_N(x, y)((k_i^2 - k_j^2))^2 = ((k_i + k_j)^2)^2 - 4N((k_i + k_j)^2) = (k_i + k_j)^2(k_i^2 + k_j^2 + 2N - 4N) = (k_i + k_j)^2(k_i - k_j)^2 = (k_i^2 - k_j^2)^2$. Also, $(k_i(k_j + 1)^2, k_i(k_j^2 - 1)) \in \mathscr{B}_N(x, y) \Leftrightarrow (k_i(k_j^2 - 1))^2 = (k_i(k_j + 1)^2)^2 - 4N(k_i(k_j + 1)^2) = k_i^2(k_j + 1)^2[(k_j + 1)^2 - 4(N/k_i)] = k_i^2(k_j + 1)^2[(k_j + 1)^2 - 4k_j] = k_i^2(k_j + 1)^2[k_j^2 + 2k_j - 4k_j + 1] = k_i^2(k_j + 1)^2(k_j - 1)^2 = k_i^2(k_j^2 - 1)^2 = (k_i(k_j^2 - 1))^2$.

(ii) If $k_i, k_j \in \mathrm{Div}(n) \setminus \{1, N\}, k_j/k_i | N \Rightarrow ((k_j + 2k_i)N_\alpha + k_i N_\beta, (k_j^2 - k_i^2)N_\gamma) \in \mathscr{B}_N(x, y)$ where $N_\alpha = N/k_i$, $N_\beta = N/k_j$, $N_\gamma = N/k_i k_j$. It comes to verify that $((k_j + 2k_i)N_\alpha + k_i n_\beta, (k_j^2 - k_i^2)N_\gamma)$ verifies the equation $y^2 = x^2 - 4Nx$. As $N = k_j \times k_i$, k_j, k_i being prime and $\mathrm{Div}(N) = \{1, k_j, k_i, N\}$, then $N_\alpha = N/k_i = k_j$, $N_\beta = N/k_j = k_i$, $N_\gamma = N/k_j k_i = 1$. We have $((k_j + 2k_i)N_\alpha + k_i N_\beta, (k_j^2 - k_i^2)N_\gamma) = ((k_j + 2k_i)N_\alpha + k_i N_\beta, (k_j^2 - k_i^2)N_\gamma) = ((k_j + 2k_i)k_j + k_i^2, (k_j^2 - k_i^2) \times 1) = ((k_j + k_i)^2, (k_j^2 - k_i^2)) \in \mathscr{B}_N(x, y) \Leftrightarrow (k_j^2 - k_i^2)^2 = ((k_j + k_i)^2)^2 - 4N((k_j + k_i)^2) = (k_j + k_i)^4 - 4N(k_j + k_i)^2 = (k_j + k_i)^2((k_j + k_i)^2 - 4N) = (k_j + k_i)^2(k_j^2 + k_i^2 + 2N - 4N) = (k_j + k_i)^2(k_j^2 + k_i^2 - 2N) = (k_j + k_i)^2(k_j - k_i)^2 = (k_j^2 - k_i^2)^2((k_j + 2k_i)k_j + k_i^2, (k_j^2 - k_i^2) \times 1) = ((k_j + k_i)^2, (k_j^2 - k_i^2)) \in \mathscr{B}_N(x, y) \Leftrightarrow (k_j^2 - k_i^2)^2 = ((k_j + k_i)^2)^2 - 4N((k_j + k_i)^2) = (k_j + k_i)^4 - 4N(k_j + k_i)^2 = (k_j + k_i)^2((k_j + k_i)^2 - 4N) = (k_j + k_i)^2(k_j^2 + k_i^2 + 2N - 4N) = (k_j + k_i)^2(k_j^2 + k_i^2 - 2N) = (k_j + k_i)^2(k_j - k_i)^2 = (k_j^2 - k_i^2)^2$. Hence, $((k_j + 2k_i)N_\alpha + k_i N_\beta, (k_j^2 - k_i^2)N_\gamma) \in \mathscr{B}_N(x, y)$.

(iii) More generally, if $k|N$,

$$
\begin{aligned}
&((k + 2)N + (N/k), (k^2 - 1/k)N) \in \mathscr{B}_N(x, y) \Leftrightarrow ((k^2 - 1/k)N)^2 = ((k + 2)N + (N/k))^2 - 4N((k + 2)N + (N/k))\\
&\Leftrightarrow ((k^2 - 1/k)N)^2 = ((k^2 + 2k + 1/k)N)^2 - 4N((k^2 + 2k + 1/k)N) \Leftrightarrow ((k^2 - 1/k)N)^2\\
&= (k^2 + 2k + 1/k)N((k^2 + 2k + 1/k)N - 4N) \Leftrightarrow ((k^2 - 1/k)N)^2 = (k^2 + 2k + 1/k)N((k^2 + 2k + 1 - 4k/k)N) \Leftrightarrow (k^2 - 1/k)^2 \cdot\\
&= (k^2 + 2k + 1/k)N((k^2 - 2k + 1/k)N) = (k + 1)^2/kN(k - 1)^2/kN = (k^2 - 1)^2/k^2N^2 = ((k^2 - 1/k)N)^2
\end{aligned}
$$

□

Proposition 4. *If $P = (x_p, y_p) \in \mathscr{B}_N(x, y)|_{x \geq 4N}$, then the following holds:*

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

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

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

Proof

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

(ii) At the point $(-x_p + 4n, y_p)$, we have $y_p^2 = (-x_p + 4N)^2 - 4N(-x_p + 4N) \Leftrightarrow y_p^2 = x_p^2 - 8Nx_p + 16N^2 + 4Nx_p - 16N^2 \Leftrightarrow$ $y_p^2 = x_p^2 - 4Nx_p$, $\Rightarrow (-x_p + 4N, y_p) \in \mathscr{B}_N(x, y)$.

(iii) From the symmetry of $\mathscr{B}_N(x, y)$ with respect to the (Ox) axis, we obtain $(-x_p + 4N, -y_p) \in \mathscr{B}_N(x, y)$. □

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

Proof. Set $x = (N + a)^2$; then, $y^2 = (N + a)^4 + 4N(N + a)^2 = (N + a)^2[(N + a)^2 - 4N] = (N + a)^2[N^2 + 2(a - 2)N + a^2]$ which is square if and only if $\delta' = (a - 2)^2 - a^2 = 0$, which is impossible except for $a = 1$, since $(a - 2)^2 - a^2 = 0 \Leftrightarrow a^2 - 4a + 4 - a^2 = 0 \Leftrightarrow 4a = 4 \Leftrightarrow a = 1$. 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 $x - 4N | x$ such that $x/(x - 4N) = k^2$, $k \in \mathbb{Z}$.

Theorem 1. *Consider $\mathscr{B}_N$ over $\mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0}$ denoted as $\mathscr{B}_N(x, y)|_{x \geq 4N}$. Then, $\forall P = (x_p, y_p) \in \mathscr{B}_N(x, y)|_{x \geq 4N}$, $(x_p, y_p) \in [4N, N(N + 2) + 1] \times [0, N^2 - 1]$.*

Proof. It is not difficult to see that $y^2 = x^2 - 4Nx \geq 0 \Leftrightarrow x \in]-\infty, 0] \cup [4N, \infty[$. From the Remark 1, a given x satisfies the condition only if either both x and $x - 4N$ are squares or $(x - 4N)|x$ with $x/(x - 4N) = k^2$, $k \in \mathbb{Z}$. Considering the fact that any integer i can be written as a function of N, that is to say $i = N + a$, where $a = i - N$, if x is square, then $\exists a \in \mathbb{Z}$ such that $x = (N + a)^2$. From Lemma 1, 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,

$$
\begin{aligned}
x(x - 4N) &= \left[(N + 1)^2 + b\right]\left[(N + 1)^2 + b - 4N\right] = (N + 1)^4 + 2(b - 2N)(N + 1)^2\\
&\quad + b(b - 4N)\\
&= b^2 + \left[2(N + 1)^2 - 4N\right]b + (N + 1)^4 - 4N(N + 1)^2,
\end{aligned}
\tag{19}
$$

and (19) is a square if and only if $\delta' = (b - 2N)^2 - b(b - 4N) = 0 \Leftrightarrow b^2 - 4Nb + 4N^2 - b^2 + 4Nb = 0 \Leftrightarrow 4N^2 = 0 \Leftrightarrow N = 0$, which is absurd since $N \neq 0$.

Also, (19) is a square if and only if $\delta' = [(N + 1)^2 - 2N]^2 - (N + 1)^4 + 4N(N + 1)^2 = 0 \Leftrightarrow (N + 1)^4 - 4N(N + 1)^2 + 4N^2 - (N + 1)^4 + 4N(N + 1)^2 = 0 \Leftrightarrow 4N^2$

$= 0 \Leftrightarrow N = 0$, which is once more absurd since $N \neq 0$. $\Rightarrow \nexists b \in \mathbb{Z}_{\geq 0} / x = (N+1)^2 + b$ 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 $x = (N+1)^2$, $y^2 = (N+1)^2[(N+1)^2 - 4N] = (N+1)^2 (N^2 + 2N + 1 - 4N) = (N+1)^2 (N-1)^2 = (N^2-1)^2$, $\Rightarrow y = N^2 - 1$, and thus $y \in [4N, (N+1)^2]$.

Hence, $\forall P = (x_p, y_p) \in \mathscr{B}_N(x,y)_{|_{x \geq 4N}}$, $(x_p, y_p) \in [4N, N(N+2)+1] \times [0, N^2 - 1]$. □

Proposition 5

(p_1) If $N = N_a \times N_b$, then there exists an injective homomorphism

$$
\begin{aligned}
&\chi_{N_a \times N_b \longrightarrow N^2} \colon \mathscr{B}_{N_a}(x,y) \times \mathscr{B}_{N_b}(x,y) \longrightarrow \frac{\mathscr{B}_N(x,y) \times \mathscr{B}_N(x,y)}{\forall (x_a, y_a) \in \mathscr{B}_{N_a}(x,y), (x_b, y_b) \in \mathscr{B}_{N_b}(x,y)},\\
&\chi_{N_a \longrightarrow N}(x_a, y_a) = (N_b x_a, N_b y_a) \in \mathscr{B}_N,\\
&\chi_{N_b \longrightarrow N}(x_b, y_b) = (N_a x_b, N_a y_b) \in \mathscr{B}_N.
\end{aligned}
\tag{20}
$$

(p_2) More generally, there is an injective homomorphism

$$
\begin{aligned}
&\chi_{\prod_{i=1}^{z} N \longrightarrow N^z} \colon \mathscr{B}_{N_a}(x,y) \times \mathscr{B}_{N_b}(x,y) \times \cdots \times \mathscr{B}_{N_z}(x,y) \longrightarrow \frac{\prod_{i=1}^{z} \mathscr{B}_N(x,y)}{\forall \left(x_{N_i}, y_{N_i}\right) \in \mathscr{B}_{N_i}(x,y)},\\
&\chi_{\prod_{i=1}^{z} N_i \longrightarrow n^z}\left(x_{N_i}, y_{N_i}\right) = \prod_{i=1,\widehat{j}}^{z} N_i\left(x_{N_i}, y_{N_i}\right).
\end{aligned}
\tag{21}
$$

Proof

(p_1) Set $N = N_a \times N_b$ and consider $\mathscr{B}_{N_a}(x,y)$, $\mathscr{B}_{N_b}(x,y)$ and $\mathscr{B}_N(x,y)$ and consider the following morphism:

$$
\begin{aligned}
&\chi_{N_a \times N_b \longrightarrow N^2} \colon \mathscr{B}_{N_a}(x,y) \times \mathscr{B}_{N_b}(x,y)\\
&\quad \longrightarrow \mathscr{B}_N(x,y) \times \mathscr{B}_N(x,y)\\
&\quad ((x_a, y_a), (x_b, y_b)) \mapsto \left(\left(x_a \frac{N}{n_a}, y_a \frac{N}{N_a} \right), \left(x_b \frac{N}{N_b}, y_b \frac{N}{N_b} \right) \right).
\end{aligned}
\tag{22}
$$

We clearly see that it is a morphism since it splits into morphisms $\chi_{N_a \longrightarrow N}$ and $\chi_{N_a \longrightarrow N}$ that are already known to be group morphisms from Proposition 2. It stays now to prove the injection. Given $(P_1, P_2) \in \mathscr{B}_{N_a}(x,y) \times \mathscr{B}_{N_b}(x,y)$, $(P_1', P_2') \in \mathscr{B}_{N_a}(x,y) \times \mathscr{B}_{N_b}(x,y)$ such that $\chi_{N_a \times N_b \longrightarrow N^2}(P_1, P_2) = \chi_{N_a \times N_b \longrightarrow N^2}(P_1', P_2')$ where $P_1 = (x_a, y_a), P_2 = (x_b, y_b), P_1' = (x_a', y_a')$ and $P_2' = (x_b', y_b')$. Then,

$$
\begin{aligned}
&\left(\left(x_a \frac{N}{N_a}, y_a \frac{N}{N_a} \right), \left(x_b \frac{N}{N_b}, y_b \frac{N}{N_b} \right) \right) = \left(\left(x_a' \frac{N}{N_a}, y_a' \frac{N}{N_a} \right), \left(x_b' \frac{N}{N_b}, y_b' \frac{N}{N_b} \right) \right)\\
&\Rightarrow \begin{cases} \left(x_a \dfrac{N}{N_a}, y_a \dfrac{N}{N_a} \right) = \left(x_a' \dfrac{N}{N_a}, y_a' \dfrac{N}{N_a} \right) \\ \left(x_b \dfrac{N}{N_b}, y_b \dfrac{N}{N_b} \right) = \left(x_b' \dfrac{N}{N_b}, y_b' \dfrac{N}{N_b} \right) \end{cases} \Leftrightarrow \begin{cases} x_a \dfrac{N}{N_a} = x_a' \dfrac{N}{N_a} \\ x_b \dfrac{N}{N_b} = x_b' \dfrac{N}{N_b} \end{cases}, \begin{cases} y_a \dfrac{N}{N_a} = y_a' \dfrac{N}{N_a} \\ y_b \dfrac{N}{N_b} = y_b' \dfrac{N}{n_b} \end{cases}\\
&\Rightarrow \begin{cases} x_a = x_a', \quad y_a = y_a', \\ x_b = x_b', \quad y_b = y_b'. \end{cases}
\end{aligned}
\tag{23}
$$

Hence, $\chi_{N_a\times N_b\longrightarrow N^2}(P_1,P_2)=\chi_{N_a\times N_b\longrightarrow N^2}(P_1',P_2')\Leftrightarrow P_1=P_1'$ 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) $N=221=N_a\times N_b=13\times 17$:

$$\begin{aligned}
\mathscr{B}_{221}(x,y)_{|x\geq 4N}&=\{(884,0),(900,120),(3332,2856),(4212,3744),(49284,48840)\},\\
\mathscr{B}_{13}(x,y)_{|x\geq 4N}&=\{(52,0),(196,168)\},\\
\mathscr{B}_{17}(x,y)&=\{(68,0),(324,288)\},\\
\chi_{13\times 17\longrightarrow 221^2}&:\mathscr{B}_{13}(x,y)_{|x\geq 4N}\times\mathscr{B}_{17}(x,y)_{|x\geq 4N}\longrightarrow\mathscr{B}_{221}(x,y)_{|x\geq 4N}\times\mathscr{B}_{221}(x,y)_{|x\geq 4N}\\
&\cdot\left((x_a,y_a),(x_b,y_b)\right)\mapsto\left((17x_1,17y_1),(13x_b,13y_b)\right),\\
\chi_{13\longrightarrow 221}(52,0)&=(17\times 52,17\times 0)=(884,0)\in\mathscr{B}_{221}(x,y),\\
\chi_{13\longrightarrow 221}(196,168)&=(17\times 196,17\times 168)=(3332,2856)\in\mathscr{B}_{221}(x,y),\\
\chi_{17\longrightarrow 221}(68,0)&=(13\times 68,13\times 0)=(884,0)\in\mathscr{B}_{221}(x,y),\\
\chi_{17\longrightarrow 221}(324,288)&=(13\times 324,13\times 288)=(4212,3744)\in\mathscr{B}_{221}(x,y).
\end{aligned}\tag{24}$$

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

$$\begin{aligned}
\mathscr{B}_{210}(x,y)_{|x\geq 4N}&=\left\{\begin{array}{c}
(840,0),(841,29),(845,65),(847,77),(864,144),\\
(867,153),(875,175),(896,224),(945,315),(961,341),(968,352)(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)
\end{array}\right\}\\
\mathscr{B}_{2}(x,y)_{|x\geq 4N}&=\{(8,0),(9,3)\},\\
\mathscr{B}_{3}(x,y)&=\{(12,0),(16,8)\},\\
\mathscr{B}_{5}(x,y)&=\{(20,0),(36,24)\}\\
\mathscr{B}_{7}(x,y)&=\{(28,0),(64,48)\},\\
\chi_{2\times 3\times 5\times 7\longrightarrow 210^4}&:\mathscr{B}_{2}(x,y)\times\mathscr{B}_{3}(x,y)\times\mathscr{B}_{5}(x,y)\times\mathscr{B}_{7}(x,y)\longrightarrow\\
\prod_{i=1}^{4}\mathscr{B}_{210}(x,y)&=\mathscr{B}_{210}(x,y)\times\cdots\times\mathscr{B}_{210}(x,y)\\
&\cdot\left((x_a,y_a),(x_b,y_b),(x_c,y_c),(x_d,y_d)\right)\mapsto\begin{pmatrix}(105x_1,105y_1),(70x_2,70y_2),\\(42x_3,42y_3),(30x_4,30y_4)\end{pmatrix},\\
\chi_{2\longrightarrow 210}(8,0)&=(105\times 8,105\times 0)=(840,0)\in\mathscr{B}_{210}(x,y),\\
\chi_{2\longrightarrow 210}(9,3)&=(105\times 9,105\times 3)=(945,315)\in\mathscr{B}_{210}(x,y),\\
\chi_{3\longrightarrow 210}(12,0)&=(70\times 12,70\times 0)=(840,0)\in\mathscr{B}_{210}(x,y),\\
\chi_{3\longrightarrow 210}(16,8)&=(70\times 16,70\times 8)=(1120,560)\in\mathscr{B}_{210}(x,y),\\
\chi_{5\longrightarrow 210}(20,0)&=(42\times 20,42\times 0)=(840,0)\in\mathscr{B}_{210}(x,y),\\
\chi_{5\longrightarrow 210}(36,24)&=(42\times 36,42\times 24)=(1512,1008)\in\mathscr{B}_{210}(x,y),\\
\chi_{7\longrightarrow 210}(28,0)&=(30\times 28,30\times 0)=(840,0)\in\mathscr{B}_{210}(x,y),\\
\chi_{7\longrightarrow 210}(64,48)&=(30\times 64,30\times 48)=(1920,1440)\in\mathscr{B}_{210}(x,y).
\end{aligned}\tag{25}$$

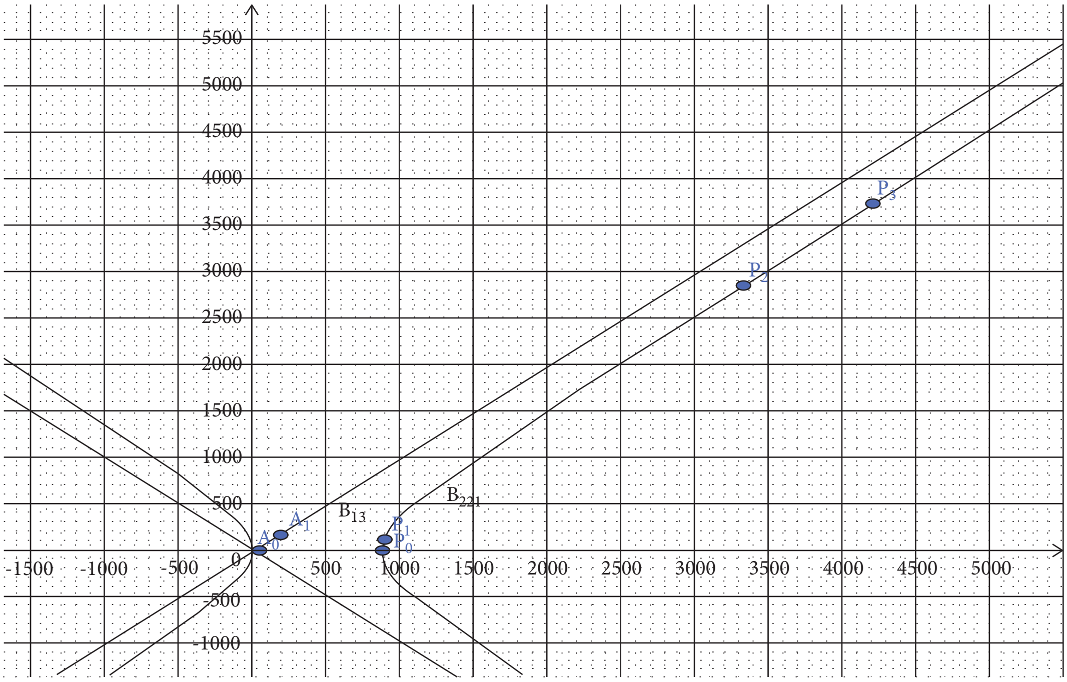


Figure 1: $\mathscr{B}_{13}(x,y)_{|x\geq 52}$ and $\mathscr{B}_{221}(x,y)_{|x\geq 884}$.

Definition 2. A prime divisor of an integer n is any prime number $p \in \mathrm{Div}(n)$. 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 $5 \in \mathrm{Div}(40) = \{1,2,4,5,8,10,20,40\}$. $\pi_p(40) = \{2,5\}$ and $|\pi_p(40)| = 2$.

Proposition 6. *Set $N = \prod_{i=1}^{\delta} p_i$, p_i primes and consider $\mathscr{B}_N(x,y)_{|x\geq 4N} = \{(x,y) \in \mathbb{Z}_{\geq 4N} \times \mathbb{Z}_{\geq 0} / y^2 = x^2 - 4Nx\}$. Set $n = |\pi_p(N)|$ and U_n as the cardinal of $\mathscr{B}_N(x,y)_{|x\geq 4N}$. Then, $U_n = 3U_{n-1} - 1 \forall n \geq 1$ 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 $\mathscr{B}_{N_i}(x,y)_{x\geq 4N_i}$ 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. $n = |\pi_p(N)|$, $U_n = |\mathscr{B}_N(x,y)_{|x\geq 4N}| = 3U_{n-1} - 1$ where $U_0 = 1$, i.e., $|\mathscr{B}_m(x,y)_{|x\geq 4m}| = U_{|\pi_p(m)|} = 3U_{|\pi_p(m)|-1} - 1$.

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 $n+1$.

$$U_{|\pi_p(m)|+1} = 3\left(3U_{|\pi_p(m)|-1} - 1\right) - 1 = 3U_{|\pi_p(m)|} - 1 = 3U_n - 1 = U_{n+1}. \tag{26}$$

By the same,

$$U_{n+1} = 3\left(U_n - 1\right) + 2 = 3U_n - 1, \tag{27}$$

$$U_{n+2} = 3\left(U_{n+1} - 1\right) + 2 = 3U_{n+1} - 1. \tag{28}$$

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

$$\begin{gathered} U_{n+2} + U_{n+1} = 3U_{n+1} - 1 + 3U_n - 1 = 3U_{n+1} + 3U_n - 2 \\ \Rightarrow U_{n+2} = 2U_{n+1} + 3U_n - 2. \end{gathered} \tag{29}$$

For S_n:

$$\begin{aligned}
&U_1 = 3U_0 - 1, \\
&U_2 = 3U_1 - 1 = 3\left(3U_0 - 1\right) - 1 = 3^2U_0 - 3 - 1, \\
&U_3 = 3U_2 - 1 = 3\left(3^2U_0 - 3 - 1\right) - 1 = 3^3U_0 - 3^2 - 3 - 1, \\
&U_4 = 3U_3 - 1 = 3\left(3^3U_0 - 3^2 - 3 - 1\right) - 1 = 3^4U_0 - 3^3 - 3^2 - 3 - 1,
\end{aligned}$$

$$U_5 = 3U_4 - 1 = 3\left(3^4U_0 - 3^3 - 3^2 - 3 - 1\right) - 1 = 3^5U_0 - 3^4 - 3^3 - 3^2 - 3 - 1,$$

$$U_6 = 3U_5 - 1 = 3\left(3^5U_0 - 3^4 - 3^3 - 3^2 - 3 - 1\right) - 1 = 3^6U_0 - 3^5 - 3^4 - 3^3 - 3^2 - 3 - 1,$$

$$\vdots$$

$$U_n = 3U_{n-1} - 1 = 3^nU_0 - \sum_{i=0}^{n-1} 3^i = 3^n - \sum_{i=0}^{n-1} 3^i \text{ since } U_0 = 1$$

$$\begin{aligned}\sum_{j=1}^{n} U_j &= \sum_{j=1}^{n}\left(3U_{j-1} - 1\right) = \sum_{j=1}^{n}\left(3^j - \sum_{i=0}^{j-1} 3^i\right)\\ &= \sum_{j=1}^{n} 3^j - \sum_{j=1}^{n}\sum_{i=0}^{j-1} 3^i = \sum_{j=1}^{n} 3^j - \sum_{j=1}^{n} \frac{1-3^j}{1-3} = \sum_{j=1}^{n} 3^j + \frac{1}{2}\sum_{j=1}^{n}\left(1 - 3^j\right) = \sum_{j=1}^{n} 3^j + \frac{1}{2}n - \frac{1}{2}\sum_{j=1}^{n} 3^j\\ &= \frac{1}{2}n + \frac{1}{2}\sum_{j=1}^{n} 3^j = \frac{1}{2}\left[n - \frac{3}{2}\left(1 - 3^n\right)\right] \Rightarrow S_n = \sum_{j=1}^{n} U_j = \frac{1}{2}n - \frac{3}{4}\left(1 - 3^n\right).\end{aligned} \tag{30}$$

□

Example 4

(i) $m = 253$, $n = |\pi_p(m)| = 2$, and $U_2 = 3U_1 - 1$, knowing $U_1 = 3U_0 - 1 = 3(1) - 1 = 2$ since $U_0 = 1$. Thus, $U_2 = 3(2) - 1 = 5 \Rightarrow |\mathscr{B}_{253}(x, y)_{|x\geq 4m}| = 5$.

Verification:

$$\begin{aligned}&\mathscr{B}_{253}(x, y)_{|x\geq 4m} = \{(1012, 0), (1156, 408), (3312, 2760), (6336, 5808), (64\quad 516, 64\quad 008)\},\\ &\left|\mathscr{B}_{253}(x, y)_{|x\geq 4m}\right| = 5.\end{aligned} \tag{31}$$

(ii) $m = 30$ and $n = |\pi_p(m)| = 3$, $U_3 = 3U_2 - 1$ knowing $U_2 = 5$, and thus $U_3 = 3(5) - 1 = 14 \Rightarrow |\mathscr{B}_{30}(x, y)_{|x\geq 4m}| = 14$.

Verification:

$$\mathscr{B}_{30}(x, y)_{|x\geq 4m} = \left\{\begin{array}{c}(120, 0), (121, 11), (125, 25), (128, 32),\\ (135, 45), (147, 63), (160, 80), (169, 91),\\ (216, 144), (245, 175), (289, 221), (363, 297), (512, 448), (961, 899)\end{array}\right\}, \tag{32}$$

and thus $|\mathscr{B}_{30}(x, y)_{|x\geq 4m}| = 14$.

(iii) $m = 2002$, $n = |\pi_p(m)| = 4$, and $U_4 = 3U_3 - 1$ knowing $U_3 = 14$, and thus $U_4 = 3(14) - 1 = 41 \Rightarrow |\mathscr{B}_{2002}(x, y)_{|x\geq 4m}| = 41$.

Verification:

$$\mathscr{B}_{2002}(x,y)_{|x\geq 4m}=\left\{\begin{array}{c}(8008,0),(8019,297),(8064,672),(8125,975),(8424,1872),\\(8575,2205),(8800,2640),(9009,3003),(9583,3885),\\(10609,5253),(10933,5655),(11583,6435),(11979,6897),\\(12769,7797),(15379,10647),(16200,11520),(17325,12705),\\(18304,13728),(20808,16320),(24649,20253),(26208,21840),\\(27889,23547),(30184,25872),(32175,27885),(37249,33003),\\(45000,40800),(48139,43953),(56133,51975),(81133,77025),\\(85849,81747),(95139,91047),(147175,143115),(158184,154128),\\(186208,182160),(290304,286272),(312325,308295),\\(368379,364353),(576583,572565),(1006009,1001997),\\(2008008,2004000),(4012009,4008003)\end{array}\right\}, \tag{33}$$

and thus $|\mathscr{B}_{2002}(x,y)_{|x\geq 4m}|=41$.

Theorem 2

(1) N is prime if and only if $|\mathscr{B}_N(x,y)_{|x\geq 4N}|=2$.

(2) If $N=N_a\times N_b$ where N_a and N_b are distinct primes, then $Card(\mathscr{B}_N(x,y)_{|x\geq 4N})=5$.

(3) If $N=N_a\times N_b\times N_c$ where N_a, N_b and N_c are distinct primes, then $Card(\mathscr{B}_N(x,y)_{|x\geq 4N})=14$.

(4) If $N=N_a\times N_b\times N_c\times N_d$ where N_a, N_b, N_c, and N_d are distinct primes, then $Card(\mathscr{B}_N(x,y)_{|x\geq 4N})=41$.

(5) $Card(\mathscr{B}_N(x,y)_{|x\in\mathbb{Z}})=4(Card(\mathscr{B}_N(x,y)_{|x\geq 4N})-1)+1_{(4N,0)}+1_{(0,0)}=4(Card(\mathscr{B}_N(x,y)_{|x\geq 4N}))-2$.

(6) Set N_a as a prime number, and $\alpha\in\mathbb{Z}_{\geq 0}$ such that $N=N_a^\alpha$. Then, $Card(\mathscr{B}_N(x,y)_{|x\geq 4N})=\alpha+1$, and $Card(\mathscr{B}_N(x,y)_{|x\in\mathbb{Z}})=4\alpha+2$.

(7) If $N\neq N_a^\alpha$, $(p,\alpha)\in\mathbb{Z}^2_{\geq 0}$, $Card(\mathscr{B}_N(x,y)_{|x\geq 4N})=Card(Div(N))+\sum_{i,j\in Div(N)\smallsetminus\{1,N\}/i\times j=N}(1-\delta_{ij})$.

More generally, $Card(\mathscr{B}_N(x,y)_{|x\in\mathbb{Z}})=4(Card(Div(N))+\sum_{i,j\in Div(N)\smallsetminus\{1,N\}/i\times j=N}(1-\delta_{ij}))-2$.

Proof

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

(1) Assume N_a prime; then, $\mathrm{Div}(N_a)=\{1,N_a\}$. The only injective homomorphisms in $\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}$ are $\chi_{1\longrightarrow N_a}$ giving the point $(4N_a,0)$ and the trivial automorphism $\chi_{N_a\longrightarrow N_a}$ giving the point $(N_a(N_a+2)+1,N_a^2-1)$ from Proposition 3. As $1|N_a$ and $N_a|N_a\Rightarrow\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}=\{(4N_a,0),(N_a(N_a+2)+1,N_a^2-1)\}$, $|\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}|=2$. Now assume $|\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}|=2$, and we know that $(4N_a,0)$ and $((N_a+1)^2,N_a^2-1)\in\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}$; that is to say, $\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}=\{(4N_a,0),((N_a+1)^2,N_a^2-1)\}$. From Proposition 6, $U_n=3U_{n-1}-1\forall n\geq 1$ with $U_0=1$, and since the cardinal $U_n=2$, $\Rightarrow n=1$, i.e., $U_n=3U_0-1=2$, N_a is prime.

(2) If $N=N_a\times N_b$ where N_a and N_b are distinct primes, then $\mathrm{Div}(N)=\{1,N_a,N_b,N\}$. We then have the following injective morphisms $\chi_{1\longrightarrow N}$, $\chi_{N_a\longrightarrow N}$, $\chi_{N_b\longrightarrow N}$ and the trivial automorphism $\chi_{N\longrightarrow N}$. As $\mathrm{Div}(N_a)=\{1,N_a\}$ and $\mathrm{Div}(N_b)=\{1,N_b\}$, then $|\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}|=2$ and $|\mathscr{B}_{N_b}(x,y)_{|x\geq 4N_b}|=2$; in this case, $\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}=\{(4N_a,0),(N_a(N_a+2)+1,N_a^2-1)=P_{N_a}\}$, $\mathscr{B}_{N_b}(x,y)_{|x\geq 4N_b}=\{(4N_b,0),(N_b(N_b+2)+1,N_b^2-1)=P_{N_b}\}$. $\chi_{N\longrightarrow N}(x,y)=(N(N+2)+1,N^2-1)=P_N$, $\chi_{1\longrightarrow N}(x,y)=\chi_{N_a\longrightarrow N}(4N_a,0)=\chi_{N_b\longrightarrow N}(4N_b,0)=(4N,0)=P_0$, $\chi_{N_a\longrightarrow N}(P_{N_a})=P_1$, $\chi_{N_b\longrightarrow N}(P_{N_b})=P_2$, and from the Proposition 3, $P_{N_a+N_b}=((N_a+N_b)^2,N_a^2-N_b^2)=P_3\Rightarrow\mathscr{B}_N(x,y)_{|x\geq 4N}=\{P_0,P_1,P_2,P_3,P_N\}$. Hence, $\mathrm{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N})=5$.

(5) From Proposition 4, $\forall P=(x_p,y_p)\in\mathbb{Z}_{\geq 4N^2}\times\mathbb{Z}_{\geq 0}$, $P\in\mathscr{B}_N(x,y)$; then, $((x_p,-y_p),(-x_p+4N,y_p),(-x_p+4N,-y_p))\in\mathscr{B}_N^3(x,y)$; as $\forall x_p\geq 4N$, $-x_p+4N\leq 0$ except for the point $(4N,0)$ which gives the point itself and the point $(0,0)$, then each point on $\mathscr{B}_N(x,y)_{|x\geq 4N}\smallsetminus\{(4N,0)\}$ leads to 4 points on $\mathscr{B}_N(x,y)_{|\mathbb{Z}}\Rightarrow\mathrm{Card}(\mathscr{B}_N(x,y)_{|x\in\mathbb{Z}})=4(\mathrm{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N})-1_{(4N,0)})+1_{(4N,0)}+1_{(0,0)}$, i.e., $\mathrm{Card}(\mathscr{B}_N(x,y)_{|x\in\mathbb{Z}})=4(\mathrm{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N}))-2$.

(6) By induction: if $\alpha=1$, $N=N_a$, then from (2), $|\mathscr{B}_{N_a}(x,y)_{|x\geq 4N_a}|=2=\alpha+1$ (true). If $\alpha=2$, $N=N_a^2$, from Proposition 3, since $\mathrm{Div}(N)=\mathrm{Div}(N_a^\alpha)=\{1,N_a,N\}$, we have the following injective morphisms $\chi_{1\longrightarrow N}$, $\chi_{N_a\longrightarrow N}$ and the trivial automorphism $\chi_{N\longrightarrow N}$ yielding to respectively 3 points $(4N,0)$, $(N_a(N_a+1)^2,N_a(N_a^2-1))$, and $((N+1)^2,N^2-1)$. Thus, $|\mathscr{B}_N(x,y)_{|x\geq 4N}|=3=\alpha+1$ (true). Now assume the assumption to be true for α, i.e., for $N=N_a^\alpha$ with $\mathrm{Div}(N)=\{1,N_a,\ldots,N_a^{\alpha-1},N\}$, $|\mathscr{B}_N(x,y)_{|x\geq 4N}|=\alpha+1$. Let us prove that to be also true for $\alpha+1$. If $N=N_a^\alpha\Rightarrow N\cdot N_a=N_a^{\alpha+1}$. In this case, $\mathrm{Div}(N)=\{1,N_a,\ldots,N_a^{\alpha-1},N_a^\alpha,N\}$. To the injective

morphisms obtained with α from the induction hypothesis, there is now the new injective homomorphism got with the multiplication of N by N_a. In this case, $|\mathscr{B}_N(x,y)_{|x\geq 4N}| = \alpha+1+1 = \alpha+2$. One deduces from (11) that $\text{Card}(\mathscr{B}_N(x,y)_{|x\in\mathbb{Z}}) = 4(\text{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N})) - 2 = 4(\alpha+1)-2 = 4\alpha+2$.

(7) From Proposition 5, $\forall i \in \text{Div}(N), \exists \chi_{i\longrightarrow N}$: $\mathscr{B}_i(x,y) \longrightarrow \mathscr{B}_N(x,y)$, it is clear that $\text{Card}(\text{Div}(N)) \leq \text{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N})$. By the same, we have injective homomorphisms obtained by composition $\forall i,j \in \text{Div}(N)\setminus\{1,N\}, i\times j = N \Rightarrow ((i+j)^2, i^2-j^2) \in \mathscr{B}_N(x,y)$ and we have the injective homomorphisms $\chi_{i\times j\longrightarrow N}$ for each case. Therefore, $\text{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N}) = \text{Card}(\text{Div}(N)) + \text{Card}(\{(i,j)\in \text{Div}(N)^2/i\cdot j = N\})$.

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

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

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

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

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

Theorem 3. *If $N = N_a\times N_b$, N_a and N_b are primes, then $\mathscr{B}_N(x,y)_{|x\geq 4N} = \langle P_1, P_2\rangle = \{P_0, P_1, P_2, P_3, P_4\}$ with $P_3 = P_1 + P_2$, $P_4 = P_2 + P_3 = P_1 + 2P_2$ where $P_1 = ((N_a + N_b)^2, (N_a^2 - N_b^2))$, $P_2 = (N_b(N_a+1)^2, N_b(N_a^2-1))$, $P_3 = (N_a(N_b+1)^2, N_a(N_b^2-1))$, $P_4 = ((N+1)^2, N^2-1)$.*

Proof. $N = N_a\cdot N_b$, with N_a and N_b primes, then $\text{Div}(N) = \{1, N_a, N_b, N\}$ and $|\text{Div}(N)| = 4$. By Proposition 6 and Theorem 2, $\text{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N}) = U_2 = 5 \Rightarrow \mathscr{B}_N(x,y)_{|x\geq 4N} = \{P_0, P_1, P_2, P_3, P_4\}$. Furthermore, from Proposition 3, $((N_a+N_b)^2, N_a^2 - N_b^2)$, $(N_b(N_a+1)^2, N_b(N_a^2-1))$, $(N_a(N_b+1)^2, N_a(N_b^2-1))$, $((N+1)^2, N^2-1) \in \mathscr{B}_N(x,y)_{|x\geq 4N}$. Considering the addition law on $\mathscr{B}_N(x,y)_{|x\geq 4N}$ given by Proposition 1 and setting $P_1 = ((N_a+N_b)^2, (N_a^2-N_b^2))$, $P_2 = (N_b(N_a+1)^2, N_b(N_a^2-1))$, $P_3 = (N_a(N_b+1)^2, N_a(N_b^2-1))$, $P_4 = ((N+1)^2, N^2-1)$, one verifies as well in the polynomial ring $Q[N_a, N_b, N]$ that $P_1 + P_2 = P_3$, $P_2 + P_3 = P_1 + 2P_2 = P_4$.

Thus, $\mathscr{B}_N(x,y)_{|x\geq 4N} = \langle P_1, P_2\rangle$. It is not hard to see that $(\mathscr{B}_N(x,y)_{|x\geq 4N}, +, \cdot)$ is then a 2–dimensional $\mathbb{Q}$–vector space with basis $\{P_1, P_2\}$. □

3. Application of $\mathscr{B}_N$ 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 $\mathscr{B}_N$ parametrization.

Theorem 4. *$\forall (a,b) \in \mathscr{B}_N(x,y)_{|x\geq 4N}$, 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.*

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

$$\begin{aligned}(x+y-(x-y))^2 &= (x+y)^2 + (x-y)^2 - 2N \\ &= \left[(x+y+x-y)^2 - 2N\right] - 2N \\ &= (2x)^2 - 4N.\end{aligned} \tag{34}$$

Set $(2x)^2 = a$; then, $4x^2 = a$.

$a - 4N$ and a are squares, yielding $a(a-4N)$ to be also a square.

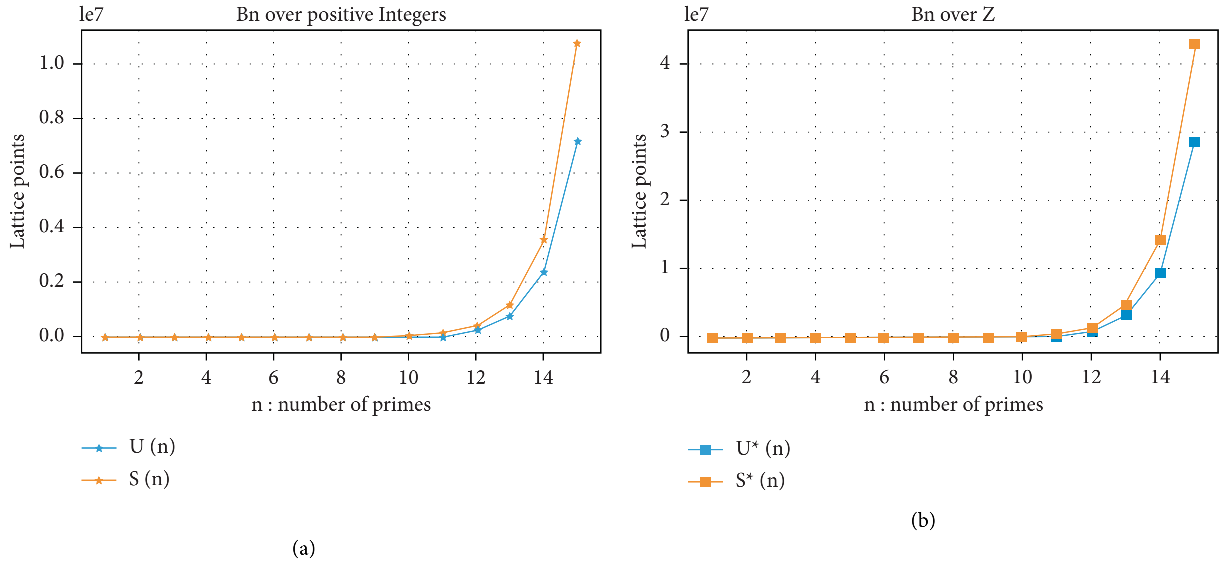
Then, there exists $b\in\mathbb{Z}/b^2 = a(a-4N) = a^2 - 4Na = \mathscr{B}_N(x,y)_{|x\geq 4N}$. Hence, $\forall (a,b)\in\mathscr{B}_N(x,y)_{|x\geq 4N}$, if $\exists x\in\mathbb{Z}/a = 4x^2$, $\Rightarrow \exists y\in\mathbb{Z}/x^2 - y^2 = N$. Also, as $a \geq 4N$, then $4x^2 \geq 4N$, considering positive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

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

Theorem 5. *$\forall (x,y)\in\mathbb{Z}_{\geq 0}^2$, $(x,y)\in H_N$; then, $(x,y)\in[\lceil N^{1/2}\rceil, (1/2)(N+1)]\times[0, (1/2)(N-1)]$.*

Proof. Assume $(x,y)\in\mathbb{Z}_{\geq 0}^2$ and $(x,y)\in H_N$.

From Theorem 1, $\forall (a,b)\in\mathscr{B}_N(x,y)_{|x\geq 4N}$, $(a,b)\in [4N,\ N(N+2)+1]\times[0, N^2-1]$. From Theorem 4, $a = 4x^2$, where (x,y) verifies H_N. If $a = 4N$, then $x^2 = N$, $\Rightarrow x = N^{1/2}$ 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.



(a)

(b)

Figure 2: Card$(\mathscr{B}_n(x, y)_{|x\geq 4n})$ (a) and Card$(\mathscr{B}_n(x, y)_{|x\in\mathbb{Z}})$ (b) over a sample of n's up to a product of 15 distinct primes.

Table 1: $U_n, S_n; U_n^*, S_n^*$ based on a dataset of up to 15 distinct prime factors.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
U_n	2	5	14	41	122	365	1094	3281	9842	29 525	88 574	265 721	797 162	2391 485	7174 454
S_n	2	7	21	62	184	549	1643	4924	14 766	44 291	132 865	398 586	1195 748	3587 233	10 761 687
U_n^*	8	20	56	164	488	1460	4376	13 124	39 368	118 100	354 296	1062 884	3188 648	9565 940	28 697 816
S_n^*	8	28	84	248	736	2196	6572	19 696	59 064	177 164	531 460	1594 344	4782 992	14 348 932	43 046 748

Hence, the bounds for (x, y), $(x, y) \in [\lceil N^{(1/2)} \rceil, (1/2)(N + 1)] \times [0, (1/2)(N - 1)]$. □

Lemma 2. *Given the sequence*

$$N_k = \begin{cases} 6 + 4k, & \text{if } k \geq 1, \\ 4, & \text{if } k = 0. \end{cases} \tag{35}$$

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 $\chi_{1\longrightarrow N}, \chi_{2\longrightarrow N}, \chi_{N\longrightarrow N}$. From Theorem 2, (17), Card$(\mathscr{B}_4(x, y)_{|x\geq 4N}) = 2 + 1 = 3$, and considering Proposition 5, we have $\chi_{1\longrightarrow N} \longrightarrow (4N, 0) = (16, 0)$; $\chi_{2\longrightarrow N}$: $\mathscr{B}_2(x, y) \longrightarrow \mathscr{B}_N(x, y)$, $(9, 3) \mapsto (2 \times 9, 2 \times 3) = (18, 6)$ where $(9, 3) \in \mathscr{B}_2(x, y)$ and $\chi_{N\longrightarrow N} \longrightarrow ((N + 1)^2, N^2 - 1) = (25, 15) \Rightarrow \mathscr{B}_4(x, y)_{|x\geq 16} = \{(16, 0), (18, 6), (25, 15)\}$, $\nexists (a, b) \in \mathscr{B}_4(x, y)_{|x\geq 16}/a = 4x^2, x \in \mathbb{Z}$. Hence, 4 cannot be written as difference of two squares.

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

By induction, for $k = 1, N_1 = N = 10, \text{Div}(N) = \{1, 2, 5, 10\}$. From Theorem 2, Card$(\mathscr{B}_n(x, y)_{|x\geq 4n}) = 5$. We have from Proposition 5 the following homomorphisms: $\chi_{1\longrightarrow N}, \chi_{2\longrightarrow N}, \chi_{5\longrightarrow N}, \chi_{10\longrightarrow N}$, and from Proposition 3, the following points: $1|N \longrightarrow (4N, 0) = (40, 0) \in \mathscr{B}_{10}(x, y)$, $2|N \longrightarrow (4N + (N/2), 3(N/2)) = (45, 15) \in \mathscr{B}_{10}(x, y)$, $5|N \longrightarrow (7N + (N/5), 24(N/5)) = (72, 48) \in \mathscr{B}_{10}(x, y)$, $N|N \longrightarrow ((N + 2)N + 1, N^2 - 1) = (121, 99) \in \mathscr{B}_{10}(x, y)$, and since $2 \times 5 = 10$, then $((5 + 2)^2, 5^2 - 2^2) = (49, 21) \in \mathscr{B}_{10}(x, y)$. Thus, $\mathscr{B}_{10}(x, y)_{|x\geq 40} = \{(40, 0), (45, 15), (49, 21), (72, 48), (121, 99)\}$. $\nexists (a, b) \in \mathscr{B}_{10}(x, y)_{|x\geq 16}/a = 4x^2, x \in \mathbb{Z}$. Hence, 10 cannot be represented as difference of two squares.

For $k = 2, N_2 = N = 14, \text{Div}(N) = \{1, 2, 7, 14\}$. From Theorem 2, Card$(\mathscr{B}_N(x, y)_{|x\geq 4N}) = 5$. We have from Proposition 5 the following homomorphisms: $\chi_{1\longrightarrow N}$, $\chi_{2\longrightarrow N}$, $\chi_{7\longrightarrow N}, \chi_{14\longrightarrow N}$, and from Proposition 3, the following points: $1|N \longrightarrow (4N, 0) = (56, 0) \in \mathscr{B}_{14}(x, y)$, $2|N \longrightarrow (4N + (N/2), 3(N/2)) = (63, 21) \in \mathscr{B}_{14}(x, y)$, $7|N \longrightarrow (9N + (N/7), (7^2 - 1)(N/7)) = (128, 96) \in \mathscr{B}_{14}(x, y)$, $N|N \longrightarrow ((N + 2)N + 1, N^2 - 1) = (225, 195) \in \mathscr{B}_{14}(x, y)$, and since $2 \times 7 = 14$, then $((7 + 2)^2, 7^2 - 2^2) = (81, 45) \in \mathscr{B}_{14}(x, y)$. Thus, $\mathscr{B}_{14}(x, y)_{|x\geq 56} = \{(56, 0), (63, 21), (81, 45), (128, 96), (225, 195)\}$. $\nexists (a, b) \in \mathscr{B}_{14}(x, y)_{|x\geq 56}/a = 4x^2, x \in \mathbb{Z}$. Hence, 14 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 $k + 1$.

$$\begin{aligned} N_{k+1} &= N = 6 + 4(k + 1) = 2(3 + 2(k + 1)) \\ &= 2(3 + 2k) + 2(2) = N_k + 4. \end{aligned} \tag{36}$$

Since $N_k = 6 + 4k \Rightarrow N_{k+1} = 6 + 4k + 4 = 6 + 4(k + 1)$. Set $k' = k + 1$; then, $N_{k'} = 6 + 4k'$ (true by assumption).

Hence, $\nexists x \in \mathbb{Z}/(4x^2, y) \in \mathscr{B}_{N_{k+1}}(x, y)_{|x \geq N_{k+1}}$. □

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 $S = \varnothing$.*

Proof. This result is straightforward from Lemma 2. □

Proposition 8. *If N is an odd prime, then $Card(H_N) = 4$. In this case,*

$$S = \left\{ \begin{array}{c} \left(\frac{1}{2}(N+1), \frac{1}{2}(N-1)\right), \left(-\frac{1}{2}(N+1), -\frac{1}{2}(N-1)\right), \\ \left(-\frac{1}{2}(N+1), \frac{1}{2}(N-1)\right), \left(\frac{1}{2}(N+1), -\frac{1}{2}(N-1)\right) \end{array} \right\}. \tag{37}$$

Proof. If N is prime, from Theorem 2,

(1) $\text{Card}(\mathscr{B}_N(x, y)_{|x \geq 4N}) = 2$.

(2) $\text{Card}(\mathscr{B}_N(x, y)_{|\mathbb{Z}}) = 4(2) - 2 = 6$. From Proposition 5, through injective homomorphisms, we have $\mathscr{B}_N(x, y)_{|x \geq 4N} = \left\{(4N, 0), ((N + 1)^2, N^2 - 1)\right\}$.

Now since N is an odd prime, $N + 1$ is even, and $4|(N + 1)^2$. Setting $a = (N + 1)^2$, $\exists x \in \mathbb{Z}/a = 4x^2 \Leftrightarrow x = (1/2)(N + 1)$ (we first consider the positive values of x and y), and as x satisfies $x^2 - y^2 = N, \Rightarrow y = (1/2)(N - 1)$. 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 $S = \left\{ \begin{array}{c} ((1/2)(N + 1), (1/2)(N - 1)), (-(1/2)(N + 1), -(1/2)(N - 1)), \\ (-(1/2)(N + 1), (1/2)(N - 1)), ((1/2)(N + 1), -(1/2)(N - 1)) \end{array} \right\}$. □

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, $Card(H_N) = 2(\alpha + 1)$. In this case,*

$$S = \left\{ \begin{array}{c} \left(\frac{1}{2}\left(N_a^{\alpha-i} + N_a^i\right), \frac{1}{2}\left(N_a^{\alpha-i} - N_a^i\right)\right), -\left(\frac{1}{2}\left(N_a^{\alpha-i} + N_a^i\right), \frac{1}{2}\left(N_a^{\alpha-i} - N_a^i\right)\right), \\ \left(\frac{1}{2}\left(N_a^{\alpha-i} + N_a^i\right), -\frac{1}{2}\left(N_a^{\alpha-i} - N_a^i\right)\right), \left(-\frac{1}{2}\left(N_a^{\alpha-i} + N_a^i\right), -\frac{1}{2}\left(N_a^{\alpha-i} - N_a^i\right)\right) \end{array} \right\}_{|i=\overline{0,1\ldots\alpha}}. \tag{38}$$

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

(1) $\text{Card}(\mathscr{B}_N(x, y)_{|x \geq 4N}) = \alpha + 1$.

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

Then, over $\mathbb{Z}_+$, $\text{Card}(H_N) = (1/2)(\alpha + 1)$. 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 $\text{Card}(H_N) = 4 \times (1/2)(\alpha + 1) = 2(\alpha + 1)$.

Since $a = (N_a^{\alpha-i} + N_a^i)^2 = 4x^2$, $\Rightarrow x^2 = (1/4)(N_a^{\alpha-i} + N_a^i)^2$, then considering the positive values of x and y, $x = (1/2)(N_a^{\alpha-i} + N_a^i)$ and $y^2 = x^2 - N = (1/4)(N_a^{\alpha-i} + N_a^i)^2 - N_a^\alpha = (1/4) \quad (N_a^{2(\alpha-i)} + 2N_a^\alpha - 4N_a^\alpha + N_a^{2i}) = \quad (1/4)(N_a^{\alpha-i} - N_a^i)^2$, $y = (1/2)(N_a^{\alpha-i} - N_a^i)$.

Hence, $S = \left\{ \begin{array}{c} ((1/2)(N_a^{\alpha-i} + N_a^i), (1/2)(N_a^{\alpha-i} - N_a^i)), (-(1/2)(N_a^{\alpha-i} + N_a^i), (1/2)(N_a^{\alpha-i} - N_a^i)), \\ ((1/2)(N_a^{\alpha-i} + N_a^i), -(1/2)(N_a^{\alpha-i} - N_a^i)), (-(1/2)(N_a^{\alpha-i} + N_a^i), -(1/2)(N_a^{\alpha-i} - N_a^i)) \end{array} \right\}_{|i=\overline{0,1\ldots\alpha}}$. □

Proposition 10. *Let $N = N_a \times N_b$, with N_a, N_b odd primes. Then, $Card(H_N) = 8$. In this case,*

$$S=\left\{\begin{array}{c}\left(\frac{1}{2}(N_a+N_b),\frac{1}{2}(N_a-N_b)\right),\left(-\frac{1}{2}(N_a+N_b),\frac{1}{2}(N_a-N_b)\right),\\ \left(\frac{1}{2}(N_a+N_b),-\frac{1}{2}(N_a-N_b)\right),\left(-\frac{1}{2}(N_a+N_b),-\frac{1}{2}(N_a-N_b)\right),\\ \left(\frac{1}{2}(N+1),\frac{1}{2}(N-1)\right),\left(-\frac{1}{2}(N+1),-\frac{1}{2}(N-1)\right),\\ \left(-\frac{1}{2}(N+1),\frac{1}{2}(N-1)\right),\left(\frac{1}{2}(N+1),-\frac{1}{2}(N-1)\right)\end{array}\right\}. \tag{39}$$

Proof. Let $N=N_a\times N_b$ with N_aN_b odd primes, from Theorem 2,

(1) $\mathrm{Card}(\mathscr{B}_N(x,y)_{|x\geq 4N})=5$.

(2) $\mathrm{Card}(\mathscr{B}_N(x,y)_{|\mathbb{Z}})=4(5)-2=18$.

From Proposition 5, through injective homomorphisms, we have $\mathscr{B}_N(x,y)_{|x\geq 4N}=\left\{\begin{array}{c}(4N,0),((N_a+N_b)^2,N_a^2-N_b^2),(N_a(N_b+1)^2,N_a(N_b^2-1),)\\ ,(N_b(N_a+1)^2,N_b(N_a^2-1),),((N+1)^2,N^2-1)\end{array}\right\}$.

Now since N_a, N_b, $N=N_aN_b$ 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 $a_1=(N_a+N_b)^2$, $\exists x\in\mathbb{Z}/a_1=4x^2\Leftrightarrow x=(1/2)(N_a+N_b)$, since x satisfies $x^2-y^2=N$, $\Rightarrow y=(1/2)(N_a-N_b)$ and $a_2=(N+1)^2$, $\exists x\in\mathbb{Z}/a_2=4x^2\Leftrightarrow x=(1/2)(N+1)$ (we first consider the positive values of x and y), since x satisfies $x^2-y^2=N$, $\Rightarrow y=(1/2)(N-1)$. Then, over $\mathbb{Z}_+$, $H_N=\{((1/2)(N_a+N_b),(1/2)(N_a-N_b)),((1/2)(N+1),(1/2)(N-1))\}$. 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, $\mathrm{Card}(H_N)=8$ and $S=\left\{\begin{array}{c}((1/2)(N_a+N_b),(1/2)(N_a-N_b)),(-(1/2)(N_a+N_b),(1/2)(N_a-N_b)),\\ ((1/2)(N_a+N_b),-(1/2)(N_a-N_b)),(-(1/2)(N_a+N_b),-(1/2)(N_a-N_b)),\\ ((1/2)(N+1),(1/2)(N-1)),(-(1/2)(N+1),-(1/2)(N-1),\\ (-(1/2)(N+1),(1/2)(N-1)),((1/2)(N+1),-(1/2)(N-1))\end{array}\right\}$. □

Proposition 11. *Let $N=\prod_{i=1}^{n}p_i$ with, p_i odd primes, then $Card(H_N)=U_n=2U_{n-1}=2^{n+1}$, and more generally, $Card(H_N)=(1-\delta_{2p_i})2^{n+1}$ for all distinct primes p_i, with δ_{2p_i} being the Kronecker symbol which is given by*

$$\delta_{2p_i}=\begin{cases}1, & \text{if } p_i=2\\ 0, & \text{else,}\end{cases}\quad\forall i=\overline{1\ldots n}. \tag{40}$$

Proof. We give a proof by induction.

For $n=1$, if $p_1=2$, $\mathrm{Card}(H_N)=0$ (true) from Remark 2 and if $p_1\neq 2$, $\mathrm{Card}(H_N)=4$ (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 $n+1$, $\mathrm{Card}(H_N)=U_{n+1}=2U_n$. From the recurrence hypothesis, $U_n=2U_{n-1}=(1-\delta_{2p_i})2^{n+1}$; then, $\mathrm{Card}(H_N)=U_{n+1}=4U_{n-1}=2(1-\delta_{2p_i})2^{n+1}=(1-\delta_{2p_i})2^{n+2}$, hence the result. □

Remark 3. If $N=N_a\times N_b$, N_a, N_b primes Set $N_a=2$, then $S=\varnothing$ and $\mathrm{Card}(H_N)=0$. Indeed, $N-6=2N_b-6=2(N_b-3)$. Since N_b is prime, $\Rightarrow N_b-3$ is even. Then, $\exists A\in\mathbb{Z}$ such that $N_b-3=2A$, $\Rightarrow N-6=2(2A)=4A$. Since $4|(N-6)$, From Theorem 5, $S=\varnothing$.

Example 5. Solve $x^2-y^2=352706$. Here, $N=352706=2\cdot 176353$. From Proposition 11, $\mathrm{Card}(H_N)=(1-\delta_{2p_i})2^{n+1}$. Here, $\delta_{2p_i}=1$ since $\exists p_i$: $p_i=2$. In this case, $\mathrm{Card}(H_N)=(1-1)2^{2+1}=0$. This algebraic set is empty over the integers.

Proposition 12. *Let $N=N_a^{\alpha}\times N_b^{\beta}$ with N_a and N_b odd primes Then, $Card(H_N)=2(\alpha+1)(\beta+1)$. In this case,*

$$S=\left\{\begin{array}{c}\left(\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j\right),\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j\right)\right),\\ \left(\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j\right)-\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j\right)\right),\\ \left(\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j\right),-\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j\right)\right),\\ \left(-\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j\right),-\frac{1}{2}\left(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j\right)\right)\end{array}\right\}_{|i=0,\ldots,\alpha j=0,\ldots,\beta}. \tag{41}$$

Proof. From Proposition 5, through injective homomorphisms, we have $\mathscr{B}_N(x,y)_{|x\geq 4N} = \left\{\begin{matrix}(4N,0),((N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)^2, N_a^{2(\alpha-i)}N_b^{2(\beta-j)}-N_a^{2i}N_b^{2j})\\ ,(N_a^iN_b^j(N_a^{\alpha-i}N_b^{\beta-j}+1)^2, N_a^iN_b^j(N_a^{2(\alpha-i)}N_b^{2(\beta-j)}-1))\end{matrix}\right\}_{|i=0,\ldots,\alpha;j=0,\ldots,\beta}.$ For each value of i, the value of j covers $[0,\beta]$.

It is obvious to see that $N_a^iN_b^j(N_a^{\alpha-i}N_b^{\beta-j}+1)^2$ is not square $\forall i=\overline{0,1,\ldots,\alpha}$ and $j=\overline{0,1\ldots\beta}$. Now since N_a and N_b are primes, then $N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j$ is even $\forall i=\overline{0,1\ldots\alpha}$ and $j=\overline{0,1\ldots\beta}$, $\Rightarrow (N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)^2$ is a multiple of 4. From Theorem 4, for this case, $\exists x\in\mathbb{Z}$ such that $a=(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)^2=4x^2$. $\Rightarrow\mathscr{B}_N(x,y)_{|x\geq 4N}$ has a total of $(\alpha+1)(\beta+1)$ such terms since $i=\overline{0,1\ldots\alpha}$ and $j=\overline{0,1\ldots\beta}$. Now, considering the redundant terms each time $i=\alpha-i$ and $j=\beta-j$ then this leads each term $N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j$ to be the same as $N_a^iN_b^j+N_a^{\alpha-i}N_b^{\beta-j}$, which is the same due to the commutativity of the common addition law, and then we have exactly $(1/2)(\alpha+1)(\beta+1)$ such terms without any redundancy, since all of the $(\alpha+1)(\beta+1)$ terms represent all terms together with their doublet.

Then, over $\mathbb{Z}_+$, $\text{Card}(H_N)=(1/2)(\alpha+1)(\beta+1)$. 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 $\text{Card}(H_N)=4\times(1/2)(\alpha+1)\ (\beta+1)=2(\alpha+1)(\beta+1)$.

Since $a=(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)^2=4x^2$, $\Rightarrow x^2=(1/4)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)^2$; then, considering the positive values of x and y, $x=(1/2)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)$ and $y^2=x^2-N=(1/4)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)^2-N=(1/4)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j)^2-N_a^{\alpha}N_b^{\beta}=(1/4)(N_a^{2(\alpha-i)}N_b^{2(\beta-j)}+N_a^{2i}N_b^{2j}-2N_a^{\alpha}N_b^{\beta})=(1/4)(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j)^2$, $y=(1/2)(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j)$. Hence, $S=\left\{\begin{matrix}((1/2)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j),(1/2)(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j)),\\ ((1/2)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j),-(1/2)(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j)),\\ ((1/2)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j),-(1/2)(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j)),\\ (-(1/2)(N_a^{\alpha-i}N_b^{\beta-j}+N_a^iN_b^j),-(1/2)(N_a^{\alpha-i}N_b^{\beta-j}-N_a^iN_b^j))\end{matrix}\right\}_{|i=0,\ldots,\alpha;j=0,\ldots,\beta}$ □

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,*

$$S=\left\{\left(\pm\frac{1}{2}\left(\prod_{i=1}^{j}N_i^{\alpha_i}+\prod_{i=j+1}^{n}N_i^{\alpha_i}\right),\pm\frac{1}{2}\left(\prod_{i=1}^{j}N_i^{\alpha_i}-\prod_{i=j+1}^{n}N_i^{\alpha_i}\right)\right)\right\}_{i\leq j\leq n}. \tag{42}$$

Proof. We prove this by induction.

For $n=1$, $N=\prod_{i=1}^1 N_i^{\alpha_i}=N_1^{\alpha_1}=2\prod_{i=1}^1(\alpha_i+1)=2(\alpha_1+1)$ which is true, since from Proposition 9, $\text{Card}(H_N)=2(\alpha_1+1)$.

For $n=2$, $N=\prod_{i=1}^2 N_i^{\alpha_i}=N_1^{\alpha_1}N_2^{\alpha_2}=2\prod_{i=1}^2(\alpha_i+1)=2(\alpha_1+1)(\alpha_2+1)$ which is also true, since from Proposition 8, $\text{Card}(H_N)=2(\alpha_1+1)(\alpha_2+1)$.

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

$N\cdot N_{n+1}^{\alpha_{n+1}}=(\prod_{i=1}^n N_i^{\alpha_i})\cdot N_{n+1}^{\alpha_{n+1}}=\prod_{i=1}^{n+1}N_i^{\alpha_i}$, taking into account the assumption $\Rightarrow\text{Card}(H_N)=2\prod_{i=1}^{n+1}(\alpha_i+1)$.

From Proposition 5, through injective homomorphisms, we have

$$\mathscr{B}_N(x,y)_{|x\geq 4N}=\left\{\left(\left(\left(\prod_{i=1}^{j}N_i^{\alpha_i}+\prod_{i=j+1}^{n}N_i^{\alpha_i}\right)^2,\prod_{i=1}^{j}N_i^{2\alpha_i}-\prod_{i=j+1}^{n}N_i^{2\alpha_i}\right),\left(\prod_{i=1}^{j}N_i^{\alpha_i}\left(\prod_{i=j+1}^{n}N_i^{\alpha_i}+1\right)^2,\prod_{i=1}^{j}N_i^{\alpha_i}\left(\prod_{i=j+1}^{n}N_i^{2\alpha_i}-1\right)\right)\right\}_{i\leq j\leq n}. \tag{43}$$

It is obvious to see that $\prod_{i=1}^j N_i^{\alpha_i}(\prod_{i=1}^n N_i^{\alpha_i}+1)^2$ is not square $\forall i=\overline{1,\ldots n}$ and $j=\overline{1,\ldots n}$. Now since $N_i^{\alpha_i}$ is prime $\forall i=\overline{1,\ldots n}$, 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, considering the positive values of x and y, $x=(1/2)(\prod_{i=1}^j N_i^{\alpha_i}+\prod_{i=j+1}^n N_i^{\alpha_i})$ and $y^2=x^2-N=(1/4)(\prod_{i=1}^j N_i^{\alpha_i}+\prod_{i=1}^n N_i^{\alpha_i})^2-\prod_{i=1}^n N_i^{\alpha_i}$. Since $\prod_{i=1}^n N_i^{\alpha_i}=\prod_{i=1}^j N_i^{\alpha_i}+\prod_{i=j+1}^n N_i^{\alpha_i}$, then

$$y^2=\frac{1}{4}\left(\prod_{i=1}^{j}N_i^{2\alpha_i}+\prod_{i=j+1}^{n}N_i^{2\alpha_i}+2\prod_{i=1}^{j}N_i^{\alpha_i}\prod_{i=j+1}^{n}N_i^{\alpha_i}-4\prod_{i=1}^{j}N_i^{\alpha_i}\prod_{i=j+1}^{n}N_i^{\alpha_i}\right)=\frac{1}{4}\left(\prod_{i=1}^{j}N_i^{\alpha_i}-\prod_{i=j+1}^{n}N_i^{\alpha_i}\right)^2. \tag{44}$$

$y = (1/2)(\prod_{i=1}^{j} N_i^{\alpha_i} - \prod_{i=j+1}^{n} N_i^{\alpha_i})$. 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

$$S = \left\{\left(\pm\frac{1}{2}\left(\prod_{i=1}^{j} N_i^{\alpha_i} + \prod_{i=j+1}^{n} N_i^{\alpha_i}\right), \pm\frac{1}{2}\left(\prod_{i=1}^{j} N_i^{\alpha_i} - \prod_{i=j+1}^{n} N_i^{\alpha_i}\right)\right)\right\}_{i \leq j \leq n}. \tag{45}$$

□

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 $2\prod_{i=1}^{n}(\alpha_i + 1)$ or $(1 - \delta_{2p_i})2^{n+1}$.

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

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

Proof. Set $N = \prod_{i=1}^{n} N_i^{\alpha_i}$, with N_i odd primes. From Proposition 13, over $\mathbb{Z}_{\geq 0}$, $\mathrm{Card}(H_N) = (1/2)\prod_{i=1}^{n}(\alpha_i + 1)$ and from Theorem 5, the length of the x interval is $l = N + 1/2 - \lceil N^{1/2}\rceil = N + 1 - 2\lceil\sqrt{N}\rceil/2$. $\Rightarrow P = (\mathrm{Card}(H_N)_{|\mathbb{Z}\geq 0}/l) = ((1/2)\prod_{i=1}^{n}(\alpha_i + 1)/N + 1 - 2\lceil\sqrt{N}\rceil/2) = (\prod_{i=1}^{n}(\alpha_i + 1)/N + 1 - 2\lceil\sqrt{N}\rceil)$. □

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

[1] J. Cilleruelo and J. Jiménez-Urroz, "Lattice points on hyperbolas," *Journal of Number Theory*, vol. 63, no. 2, pp. 267–274, 1997.

[2] J. Cilleruelo and J. Jimenez-Urroz, "The Hyperbola $xy = N$," *Journal de Théorie des Nombres de Bordeaux, Tome*, vol. 12, no. 1, pp. 87–92, 2000.

[3] J. Cilleruelo and A. Cordoba, "Trigonometric polynomials and lattice points," *Proceeding of the American Mathematical Society*, vol. 115, no. 4, 1992.

[4] J. John Brillhart, R. Blecksmith, and M. Decaro, "Using conic sections to factor integers," *The American Mathematical Monthly*, vol. 123, no. 2, pp. 168–174, 2016.

[5] B. Emanuele, M. Nadir, J. Antonio, and E. Michele, "Point-groups over singular cubics," 2020, https://arxiv.org/pdf/2001.04288.pdf.

[6] R. Taton, "L' essay pour les coniques de pascal," *Revue d'Histoire des Sciences et de Leurs Applications*, vol. 8, no. 1, pp. 1–18, 1955.

[7] A. K. Lenstra, H. W. Lenstra, M. Manasse, and J. M. Pollard, "Carl pomerance the number field sieve," *Proceedings of Symposia in Applied Mathematics*, vol. 48, 1994.

[8] C. Pomerance, "The quadratic sieve factoring algorithm," in *Proceedings of the Advances in Cryptology, Proceeding of EUROCRYPT'84', LNCS 209*, pp. 169–182, Springer-Verlag, Berlin, Germany, 1985.

[9] Fermat, *Oeuvres de Fermat*, vol. 2, p. 256, 1894.

[10] J. McKee, "Speeding Fermat's factoring method," *Mathematics of Computation*, vol. 68, no. 228, pp. 1729–1737, 1999.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[12] H. Jin, K. Jeong, and J.-H. Kwon, "Integral points on hyperbolas," *Journal of the Korean Mathematical Society*, vol. 34, no. 1, pp. 149–157, 1997.

[13] K. Zelator, "Integral points on hyperbolas over *Z*: a special case," 2009, https://arxiv.org/abs/0907.3675.

[14] Y. Kim, "On some Behavior of integral points on a Hyperbola," *Bulletin of the Korean Mathematical Society*, vol. 50, no. 4, pp. 1243–1259, 2013.

[15] B. Emanuele, N. Murru, J. Antonio, Di Scala, and E. Michele, "Group law on affine conics and applications to cryptography," *Journal of Applied Mathematics and Computation*, Elsevier, 2020.

[16] G. R. Bansimba, R. F. Babindamana, and B. G. R. Bossoto, "Some arithmetical properties on hyperbola," *JP Journal of Algebra, Number Theory and Applications*, vol. 50, no. 1, pp. 45–100, 2021.