New Interesting Property and Application of the Rectangular Hyperbola

Original Research Article

Abstract

This paper derives an interesting property of the rectangular hyperbola. On the branch of the first quadrant, the slope of a chord starting from the vertex of the hyperbola has an opposite sign with the slope of the line segment from the coordinate origin to the peak of the chord. An arbitrary another chord starting from the ending-point of the former one continues owning the stated property. With this property, hyperbola xy = N can be subdivided into a series of hyperbolic arcs to factorize N or to estimate the divisor-ratio q/p if N=pq is a semiprime. It is proven that a semiprime is easier to be factorized if it has a small divisor-ratio. The paper presents detail mathematical reasoning as well as an approach to realize the factorization or estimation.

Keywords: Rectangular hyperbola; subdivision; integer factorization divisor-ratio

2010 Mathematics Subject Classification:51N20/11A51

1 Introduction

The rectangular hyperbola is a conic curve that has been studied in every middle school for hundreds of years. Simple as it is, the curve is related many mathematical aspects. Except for that there are frequently new properties found on the curve itself, like those in [1][2] and [3], it is related with lattice geometry [4][5][6], Diophantine equations [7][8] and the integer factorization [9]. A recent study on the hyperbola $xy = N$ discovers several new interesting properties of the curve. This paper presents the results.

2 Preliminaries

In this whole paper, symbol $A \Rightarrow B$ means statement *A* can derive out statement *B*, symbol $|AB|$ means the length of line segment AB, symbol $P : (x, y)$ or $P = (x, y)$ means a point P with x and y being its coordinates; symbols $P.x$ and $P.y$ are to express P's x-coordinate and y-coordinate, respectively. $P : (x, y)$ is said to be an odd point if both x and y are odd integers. For a planar curve Γ, symbol $\widehat{AB} \in \Gamma$ or simply $\widehat{AB}$ means a convex part (or arc) of Γ starting at A and ending at B, or vise versa; the line segment connecting A and B is called the chord of $\widehat{AB}$; the point at which

the tangent line of $\overset{\frown}{AB}$ is parallel to AB is called the peak point of $\overset{\frown}{AB}$ or the peak of the chord AB. Symbol $< P_1P_2...P_n >$ means the polygon formed by points $P_1, P_2, ..., P_n$ and symbol H is to express the hyperbola $xy = N$ in Cartesian coordinate system; for an arbitrary real number $\alpha > 1$, the part of H between the line $y = \alpha x$ and the line $y = x$ is denoted with H_α, as the red part shown in Fig. 1. A point P is said to be over a line $y = \alpha x$ with $k \geq 0$ if the slope of OP is bigger than k. It should point out that, all the reasoning and deductions in this paper are done in the Cartesian coordinate system.

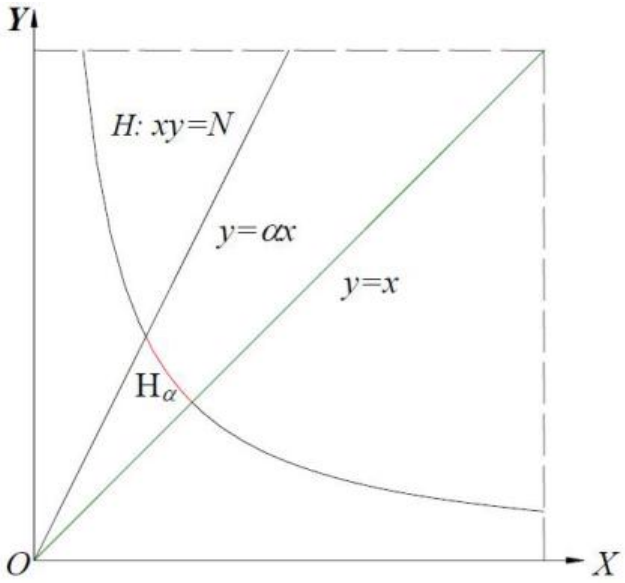

Figure 1: Hyperbola $xy = N$ and H_α

3 Main Results

Seen clockwise in Fig. 2, H_α starts at $P_r : (\sqrt{N}, \sqrt{N})$ and ends at $P_l : (\sqrt{\frac{N}{\alpha}}, \sqrt{\alpha N})$. Accordingly, the line segment P_rP_l is the chord of H_α. Related with the chord, the following theorems and propositions are proved.

Theorem 1. The slope of the chord P_rP_l is $-\sqrt{\alpha}$. The peak of $\overset{\frown}{P_rP_l}$ is $P_\alpha : (\frac{\sqrt{N}}{\sqrt[4]{\alpha}}, \sqrt[4]{\alpha}\sqrt{N})$. The slope of OP_α is $\sqrt{\alpha}$. The distance from P_α to P_rP_l is $d_\alpha = \frac{(\sqrt[4]{\alpha}-1)^2}{\sqrt{1+\alpha}} \times \sqrt{N}$.

Proof. Let k be the slope of the line segment P_rP_l. Direct calculation yields

$$k = \frac{\sqrt{\alpha N} - \sqrt{N}}{\sqrt{\frac{N}{\alpha}} - \sqrt{N}} = -\sqrt{\alpha}$$

Assume $T : (x_0, y_0)$ is the mentioned tangent point; then the slope of the tangent line at T is $-\frac{N}{x_0^2}$. As a result, $\frac{N}{x_0^2} = \sqrt{\alpha} \Rightarrow x_0 = \frac{\sqrt{N}}{\sqrt[4]{\alpha}} \Rightarrow y_0 = \frac{N}{x_0} = \sqrt[4]{\alpha}\sqrt{N}$. This directly yields the slope of OP_α is $\frac{y_0}{x_0} = \sqrt[4]{\alpha}\sqrt{N}/\frac{\sqrt{N}}{\sqrt[4]{\alpha}} = \sqrt{\alpha}$. Since the equation of the line containing P_rP_l is $\sqrt{\alpha}x+y-\sqrt{N}(\sqrt{\alpha}+1) = 0$,

the distance from P_α to P_rP_l is

$$d_\alpha = \frac{(\sqrt[4]{\alpha}-1)^2}{\sqrt{1+\alpha}} \times \sqrt{N}$$

□

The configuration of the lines and points mentioned in Theorem 1 are illustrated in Fig. 2.

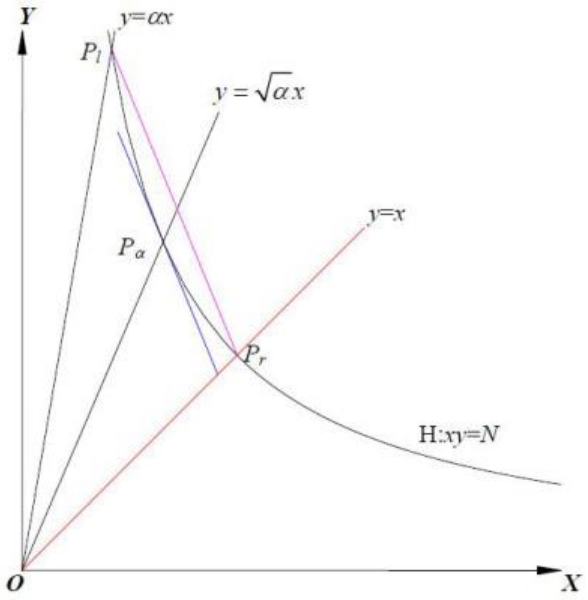

Figure 2: Configuration of the lines and points mentioned in Theorem 1

Proposition 1. Let P_α be that defined in Theorem 1 and denote it by another symbol P_m, namely $P_m = P_\alpha$; then the slopes of the chords P_lP_m and P_mP_r are $-\sqrt[4]{\alpha^3}$ and $-\sqrt[4]{\alpha}$, respectively ; the peaks of $\overset{\frown}{P_lP_l}$ (or P_lP_m) and $\overset{\frown}{P_mP_r}$ (or P_mP_r) are $P_{lm} : (\frac{\sqrt{N}}{\sqrt[8]{\alpha^3}}, \sqrt[8]{\alpha^3}\sqrt{N})$ and $P_{mr} : (\frac{\sqrt{N}}{\sqrt[8]{\alpha}}, \sqrt[8]{\alpha}\sqrt{N})$, respectively; the slopes of line segments OP_{lm} and OP_{mr} are $\sqrt[4]{\alpha^3}$ and $\sqrt[4]{\alpha}$, respectively; the distance from P_{lm} to P_lP_m is $d_{lm} = \frac{\sqrt[4]{\alpha}(\sqrt[8]{\alpha}-1)^2}{\sqrt{1+\alpha\sqrt{\alpha}}} \times \sqrt{N}$ and the distance from P_{mr} to P_mP_r is $d_{mr} = \frac{(\sqrt[8]{\alpha}-1)^2}{\sqrt{1+\sqrt{\alpha}}} \times \sqrt{N}$.

Proof. The slopes of the chords P_lP_m and P_mP_r are calculated respectively by

$$\frac{P_l.y - P_m.y}{P_l.x - P_m.x} = \frac{\sqrt{\alpha N} - \sqrt[4]{\alpha}\sqrt{N}}{\frac{\sqrt{N}}{\sqrt{\alpha}} - \frac{\sqrt{N}}{\sqrt[4]{\alpha}}} = -\sqrt[4]{\alpha^3}$$

and

$$\frac{P_r.y - P_m.y}{P_r.x - P_m.x} = \frac{\sqrt{N} - \sqrt[4]{\alpha}\sqrt{N}}{\sqrt{N} - \frac{\sqrt{N}}{\sqrt[4]{\alpha}}} = -\sqrt[4]{\alpha}$$

Accordingly, the peak points of P_lP_m and P_mP_r are respectively $P_{lm} : (\frac{\sqrt{N}}{\sqrt[8]{\alpha^3}}, \sqrt[8]{\alpha^3}\sqrt{N})$ and $P_{mr} : (\frac{\sqrt{N}}{\sqrt[8]{\alpha}}, \sqrt[8]{\alpha}\sqrt{N})$, which yield the slopes OP_{lm} and OP_{mr} are $\sqrt[4]{\alpha^3}$ and $\sqrt[4]{\alpha}$ respectively. Since

the equation of the line containing P_lP_m is $\sqrt[4]{\alpha^3}x+y-\sqrt[4]{\alpha}(\sqrt[4]{\alpha}+1)\sqrt{N}=0$, direct calculation shows the distance from P_{lm} to OP_{lm} is

$$d_{lm}=\frac{\sqrt[4]{\alpha}(\sqrt[8]{\alpha}-1)^2}{\sqrt{1+\alpha\sqrt{\alpha}}}\times\sqrt{N}$$

The equation of the line containing P_mP_r is $\sqrt[4]{\alpha}x+y-(\sqrt[4]{\alpha}+1)\sqrt{N}=0$; hence the distance from P_{mr} to P_mP_r is

$$d_{mr}=\frac{(\sqrt[8]{\alpha}-1)^2}{\sqrt{1+\sqrt{\alpha}}}\times\sqrt{N}$$

Note that α is the slope of OP_l and $\sqrt{\alpha}$ is the slope of OP_m, it demonstrates an interesting scenery, as shown in Fig. 3. L

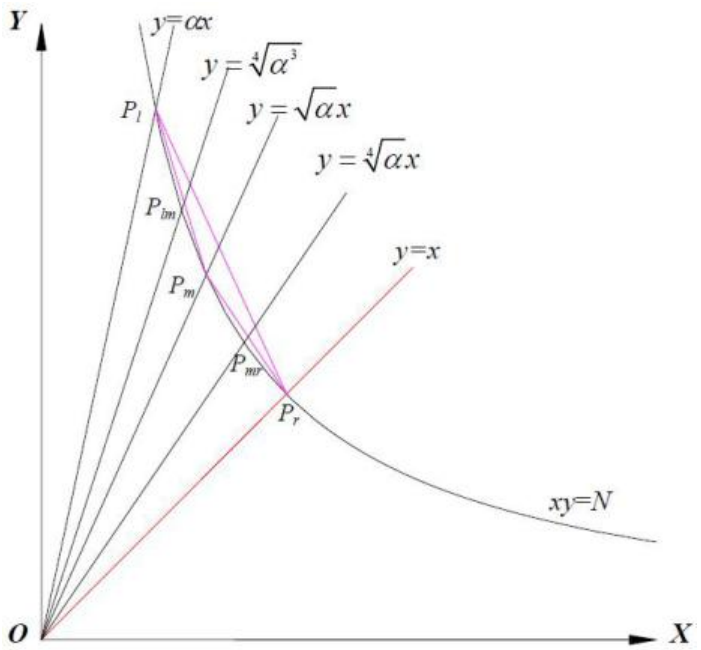

Figure 3: Configuration of the lines and points mentioned in Proposition 1

Remark 1. Calculations show that, the slopes of $P_rP_{mr}, P_{mr}P_m, P_mP_{lm}$ and $P_{lm}P_l$ are $-\sqrt[8]{\alpha}$, $-\sqrt[8]{\alpha^3}$, $-\sqrt[8]{\alpha^5}$ and $-\sqrt[8]{\alpha^7}$, respectively. The peaks of $P_rP_{mr}, P_{mr}P_m, P_mP_{lm}$ and $P_{lm}P_l$ are $(\frac{\sqrt{N}}{\sqrt[16]{\alpha}}, \sqrt[16]{\alpha}\sqrt{N})$, $(\frac{\sqrt{N}}{\sqrt[16]{\alpha^3}}, \sqrt[16]{\alpha^3}\sqrt{N})$, $(\frac{\sqrt{N}}{\sqrt[16]{\alpha^5}}, \sqrt[16]{\alpha^5}\sqrt{N})$ and $(\frac{\sqrt{N}}{\sqrt[16]{\alpha^7}}, \sqrt[16]{\alpha^7}\sqrt{N})$ respectively. Accordingly, the following Proposition 2.

Proposition 2. For an arbitrary positive integer $k\geq 1$, let $S=\{\sqrt[2^k]{\alpha}, \sqrt[2^k]{\alpha^3}, \sqrt[2^k]{\alpha^5},\cdots,\sqrt[2^k]{\alpha^{2j-1}},\cdots, \sqrt[2^k]{\alpha^{2^k-3}}, \sqrt[2^k]{\alpha^{2^k-1}}\}$ with integer $1\leq j\leq 2^{k-1}$; then term $\sqrt[2^k]{\alpha^{2j-1}}$ corresponds to peak P_j : $(\frac{\sqrt{N}}{\sqrt[2^{k+1}]{\alpha^{2j-1}}}, \sqrt[2^{k+1}]{\alpha^{2j-1}}\sqrt{N})$ whose chord is with a slope of $-\sqrt[2^k]{\alpha^{2j-1}}$; the two ending points of the chord are $(\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^{j-1}}}, \sqrt[2^k]{\alpha^{j-1}}\sqrt{N})$ and $(\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^{j}}}, \sqrt[2^k]{\alpha^{j}}\sqrt{N})$; the distance form P_j to its chord is

$\frac{\sqrt[2^k]{\alpha^{j-1}}(\sqrt[2^{k+1}]{\alpha}-1)^2}{\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}}}\sqrt{N}$ and the length of chord is $\sqrt{N}(\frac{\sqrt[2^k]{\alpha}-1}{\sqrt[2^k]{\alpha^j}})\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}}$.

Proof. Direct calculation knows the intersection of the line $y = \sqrt[2^k]{\alpha^{2j-1}}x$ with H is P_j : $(\frac{\sqrt{N}}{\sqrt[2^{k+1}]{\alpha^{2j-1}}}, \sqrt[2^{k+1}]{\alpha^{2j-1}}\sqrt{N})$. Accordingly, the slope of the tangent line at P_j is $k_j = -\frac{N}{(P_j.x)^2} = -\sqrt[2^k]{\alpha^{2j-1}}$, which is the slope of the chord of P_j. Next is to find out the chord.

For convenience, denote $Q_0 = (\sqrt{N}, \sqrt{N})$. Calculate $P_1 = (\frac{\sqrt{N}}{\sqrt[2^{k+1}]{\alpha}}, \sqrt[2^{k+1}]{\alpha}\sqrt{N})$ and $k_1 = -\sqrt[2^k]{\alpha}$. Assume Q_0Q_1 is the chord of P_1; then Q_0Q_1 has a slope $-\sqrt[2^k]{\alpha}$. Since it passes through Q_0 , it must be on the line

$$y - \sqrt{N} = k_1(x - \sqrt{N}) \Rightarrow y = -\sqrt[2^k]{\alpha}x + (\sqrt[2^k]{\alpha} + 1)\sqrt{N} = -\sqrt[2^k]{\alpha}x + \sqrt[2^k]{\alpha^0}(\sqrt[2^k]{\alpha} + 1)\sqrt{N}$$

Thereby Q_1 is calculated by $Q_1 : (\frac{\sqrt{N}}{\sqrt[2^k]{\alpha}}, \sqrt[2^k]{\alpha}\sqrt{N})$. The distance from P_1 to Q_0Q_1 is

$$d_{0,1} = \frac{\sqrt[2^k]{\alpha^0}(\sqrt[2^{k+1}]{\alpha} - 1)^2}{\sqrt{1+\sqrt[2^{k-1}]{\alpha}}}\sqrt{N}$$

The length of Q_0Q_1 is

$$|Q_0Q_1| = \sqrt{N}(\frac{\sqrt[2^k]{\alpha} - 1}{\sqrt[2^k]{\alpha}})\sqrt{1+\sqrt[2^{k-1}]{\alpha}}$$

Likewise, assume Q_1Q_2 is the chord of P_2; then it is on the line $y = -\sqrt[2^k]{\alpha^3}x + \sqrt[2^k]{\alpha}(\sqrt[2^k]{\alpha} + 1)\sqrt{N}$ because it passes through Q_1 and has a slope $-\sqrt[2^k]{\alpha^3}$. Q_2 is then calculated by Q_2 : $(\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^2}}, \sqrt[2^k]{\alpha^2}\sqrt{N})$ and the distance from P_2 to Q_1Q_2 is

$$d_{1,2} = \frac{\sqrt[2^k]{\alpha}(\sqrt[2^{k+1}]{\alpha} - 1)^2}{\sqrt{1+\sqrt[2^{k-1}]{\alpha^3}}}\sqrt{N}$$

The length of Q_1Q_2 is

$$|Q_1Q_2| = \sqrt{N}\frac{\sqrt[2^k]{\alpha} - 1}{\sqrt[2^k]{\alpha^2}}\sqrt{1+\sqrt[2^{k-1}]{\alpha^3}}$$

Assume Q_2Q_3 is the chord of P_3; then Q_2Q_3 is on the line $y = -\sqrt[2^k]{\alpha^5}x + \sqrt[2^k]{\alpha^2}(\sqrt[2^k]{\alpha} + 1)\sqrt{N}$ with $Q_3 = (\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^3}}, \sqrt[2^k]{\alpha^3}\sqrt{N})$ and the distance from P_3 to Q_2Q_3 is

$$d_{2,3} = \frac{\sqrt[2^k]{\alpha^2}(\sqrt[2^{k+1}]{\alpha} - 1)^2}{\sqrt{1+\sqrt[2^{k-1}]{\alpha^5}}}\sqrt{N}$$

The length of Q_2Q_3 is

$$|Q_2Q_3| = \sqrt{N}\frac{\sqrt[2^k]{\alpha} - 1}{\sqrt[2^k]{\alpha^3}}\sqrt{1+\sqrt[2^{k-1}]{\alpha^5}}$$

Now by principle of mathematical induction, the chord of P_j is $Q_{j-1}Q_j$ with $Q_{j-1} = (\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^{j-1}}}, \sqrt[2^k]{\alpha^{j-1}}\sqrt{N})$ and $Q_j = (\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^j}}, \sqrt[2^k]{\alpha^j}\sqrt{N})$; the distance form P_j to $Q_{j-1}Q_j$ is

$$d_{j-1,j} = \frac{\sqrt[2^k]{\alpha^{j-1}}(\sqrt[2^{k+1}]{\alpha} - 1)^2}{\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}}}\sqrt{N} \tag{3.1}$$

The length of $Q_{j-1}Q_j$ is

$$|Q_{j-1}Q_j| = \sqrt{N}(\frac{\sqrt[2^k]{\alpha}-1}{\sqrt[2^k]{\alpha^j}})\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}} \tag{3.2}$$

□

Remark 2. Seen from the proof of Proposition 2, points $Q_0, Q_1, ..., Q_{2^{k-1}}$ form an inscribed polygon $< Q_0Q_1...Q_{2^{k-1}} >$ of H_α while the tangent lines passing through the points $P_1, P_2, ..., P_{2^{k-1}}$ form a circumscribed polygon $< P_1P_2...P_{2^{k-1}} >$ of H_α. Note that $\sqrt[2^{k-1}]{\alpha^2} > 1$ and

$$\begin{aligned}&1+\sqrt[2^{k-1}]{\alpha^{2j+1}}-\sqrt[2^{k-1}]{\alpha}-\sqrt[2^{k-1}]{\alpha^{2j}} = 1-\sqrt[2^{k-1}]{\alpha}+(\sqrt[2^{k-1}]{\alpha}-1)\sqrt[2^{k-1}]{\alpha^{2j}}\\ &=(\sqrt[2^{k-1}]{\alpha}-1)(\sqrt[2^{k-1}]{\alpha^{2j}}-1)>0 \Rightarrow \frac{1+\sqrt[2^{k-1}]{\alpha^{2j+1}}}{\sqrt[2^{k-1}]{\alpha}+\sqrt[2^{k-1}]{\alpha^{2j}}}>1\end{aligned}$$

These yield

$$\frac{|Q_jQ_{j+1}|}{|Q_{j-1}Q_j|} = \frac{\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j+1}}}}{\sqrt[2^k]{\alpha}\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}}} = \sqrt{\frac{1+\sqrt[2^{k-1}]{\alpha^{2j+1}}}{\sqrt[2^{k-1}]{\alpha}+\sqrt[2^{k-1}]{\alpha^{2j}}}} > 1 \tag{3.3}$$

$$\frac{|Q_jQ_{j+1}|}{\sqrt[2^k]{\alpha}|Q_{j-1}Q_j|} = \frac{\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j+1}}}}{\sqrt[2^{k-1}]{\alpha}\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}}} = \sqrt{\frac{1+\sqrt[2^{k-1}]{\alpha^{2j+1}}}{\sqrt[2^{k-1}]{\alpha^2}+\sqrt[2^{k-1}]{\alpha^{2j+1}}}} < 1 \tag{3.4}$$

$$\frac{d_{j,j+1}}{d_{j-1,j}} = \sqrt[2^k]{\alpha}\frac{\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}}}{\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j+1}}}} = \sqrt{\frac{\sqrt[2^{k-1}]{\alpha}+\sqrt[2^{k-1}]{\alpha^{2j}}}{1+\sqrt[2^{k-1}]{\alpha^{2j+1}}}} < 1 \tag{3.5}$$

and

$$d_{j-1,j} \times |Q_{j-1}Q_j| = (\sqrt[2^{k+1}]{\alpha}-1)^2(1-\frac{1}{\sqrt[2^k]{\alpha}})N \tag{3.6}$$

saying $|Q_{j-1}Q_j| < |Q_jQ_{j+1}| < \sqrt[2^k]{\alpha}|Q_{j-1}Q_j|$, $d_{j,j+1} < d_{j-1,j}$ and $d_{j-1,j} \times |Q_{j-1}Q_j|$ is merely dependant of k, α and N. That is to say, the area of $\triangle Q_{j-1}P_jQ_j$ is independent of j. As a result, $\triangle Q_{j-1}P_jQ_j$ keeps a constant value for every j with $1 \le j \le 2^{k-1}$ if k , α and N are given.

Theorem 2. Given a rational number $\alpha > 1$ and a positive number N, let $l_{(N,\alpha,k,j)}$ be the length of $|Q_{j-1}Q_j|$ defined in 3.2, namely $l_{(N,\alpha,k,j)} = \sqrt{N}(\frac{\sqrt[2^k]{\alpha}-1}{\sqrt[2^k]{\alpha^j}})\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2j-1}}}$ with $1 \le j \le 2^{k-1}$; then there always exists an integer $k > \lfloor \log_2(\alpha-1) \rfloor$ such that $l_{(N,\alpha,k,j)}$ is limited within an expected value.

Proof. Let $\alpha = 1+\lambda$ with $\lambda > 0$; then the Bernoulli inequality $\sqrt[2^k]{\alpha} = (1+\lambda)^{\frac{1}{2^k}} \le 1+\frac{\lambda}{2^k}$ shows that $\frac{\lambda}{2^k} < 1$ and $\lim_{k\to\infty} \sqrt[2^k]{\alpha} = 1$ when $k > \log_2\lambda = \log_2(\alpha-1)$. As a result, there is always a k such that $\sqrt[2^k]{\alpha}-1$ is small enough to make $l_{(N,\alpha,k,j)}$ a small number no matter how big N is.L

4 Application in Estimation of Divisor-ratio of Semiprime

A semiprime is a composite integer having merely two distinct prime divisors. Let $N = pq$ be a semiprime with $2 < p < q$; then $\beta = \frac{q}{p}$ is the divisor-ratio of N. If β is known, N is surely factorized by $N = \beta p^2 \Rightarrow p = \sqrt{\frac{N}{\beta}} \otimes q = \frac{N}{p}$. Unfortunately, β is hardly known before N is factorized. Thereby, a valid estimation of β is helpful to know the distributions of p and q, as investigated in [10] and [12]. This section presents an estimation of β.

4.1 Theoretical Essences

Theorem 3. Let α be a rational number and $N = pq$ with $2 < p < q$ being primes be a semiprime whose divisor ratio is $\beta = \frac{q}{p}$; then $\beta \leq \alpha$ if and only if there is no odd point on H_α other than the point (p, q).

Proof. Referring to example 2 at page 5 of T Andreescu's book [12] as well as its followingremark at page 6.L

Theorem 4. Let α be a rational number, $N = pq$ with $2 < p < q$ being prime numbers and $\beta = \frac{q}{p}$; then $\beta \leq \sqrt{\alpha}$ if and only the peak of H_α is over the line $y = \beta x$.

Proof.Sufficiency. The peak of H_α is $P_\alpha : (\sqrt{\frac{N}{\sqrt{\alpha}}}, \sqrt{\sqrt{\alpha}N})$. $\beta \leq \sqrt{\alpha}$ yields $\sqrt{\frac{N}{\beta}} \geq \sqrt{\frac{N}{\sqrt{\alpha}}}$ and $\sqrt{\beta N} \leq \sqrt{\sqrt{\alpha}N}$. Since $(\sqrt{\frac{N}{\beta}}, \sqrt{\beta N})$ is an ending point of H_β and it is also the intersection of $y = \beta x$ with $xy = N$. Accordingly P_α is surely over the line $y = \beta x$. Now consider the necessity. Since P_α is over $y = \beta x$, the slope of OP_α is no smaller than β. Consequently $\sqrt{\alpha} \geq \beta$ because $\sqrt{\alpha}$ is the slope of OP_α.L

Proposition 3. Let $N = pq$ be a semiprime with $2 < p < q$ being primes and $\beta = \frac{q}{p}$; if there is not an odd point (u, v) such that $uv = N$ on $\overset{\frown}{Q_0Q_1}$,$\overset{\frown}{Q_1Q_2}$,$\cdots$,$\overset{\frown}{Q_{j-1}Q_j}$ for given α and k, then $\beta > \sqrt[2^k]{\alpha^{2^k-1}}$, where $Q_0, Q_1, ..., Q_{2^{k-1}}$ are points described in Remark 2.

Proof. The conclusion is directly from Proposition 2 and Theorem 3.L

Proposition 4. Let $N = pq$ be a semiprime with $2 < p < q$ being primes and $\beta = \frac{q}{p}$; then the closer β is to 1 the easier N is factorized.

Proof. By Theorems 3, 4 and Proposition 3, the odd point (p, q) can be found on H_β. By Theorem 2, the closer β is to 1 the shorter H_β is. Hence it takes less time to find (p, q).L

4.2 Realization

Assume N is a semiprime with a unknown small divisor-ratio β (the true value); here is to show a procedure to estimate β . The idea of the estimation is to set randomly an evaluated value α and check recursively by Proposition 3 if it is smaller or bigger than the true value β. Once β is smaller than α, N can be factorized in the checking process. Since there are might be huge number of computations for a big N, a maximal permissive computing number of times, denoted by $M_{permissive}$, is first set by Theorem 2. The procedure, whose Maple source codes are given in the appendix section, is described as follows.

Procedure Estimation

Step 1. Set an initial value α ;

Step 2. Calculate a minimal k such that $l_{(N,\alpha,k,2^{k-1})} \leq M_{permissive}$;

Step 3. For j from 1 to 2^{k-1} do

Calculate $Q_{j-1} = (\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^{j-1}}}, \sqrt[2^k]{\alpha^{j-1}}\sqrt{N})$ and $Q_j = (\frac{\sqrt{N}}{\sqrt[2^k]{\alpha^j}}, \sqrt[2^k]{\alpha^j}\sqrt{N})$;

Search on arc $\overset{\frown}{Q_{j-1}Q_j}$ the odd point (u, v) satisfying $uv = N$;

If (u, v) is found, terminate computing to output u, v and $\beta = \frac{v}{u}$.

end do

Step 4. Confirm $\beta > \sqrt[2^k]{\alpha^{2^k-1}}$.

End Procedure

Remark 3.

(1) k in Step 2 can be estimated as follows.

$$l_{(N,\alpha,k,2^{k-1})} = \sqrt{N}(\frac{\sqrt[2^k]{\alpha}-1}{\sqrt[2^k]{\alpha^{2^k-1}}})\sqrt{1+\sqrt[2^{k-1}]{\alpha^{2^k-1}}}$$
$$= \sqrt{N}(\frac{(\sqrt[2^k]{\alpha}-1)}{\sqrt{\alpha}})\sqrt{1+\frac{\alpha^2}{\sqrt[2^{k-1}]{\alpha}}} < \sqrt{N}(\frac{(\sqrt[2^k]{\alpha}-1)}{\sqrt{\alpha}})\sqrt{1+\alpha^2}$$

As a result,

$$\sqrt{N}(\frac{(\sqrt[2^k]{\alpha}-1)}{\sqrt{\alpha}})\sqrt{1+\alpha^2} \le M_{permissive} \Rightarrow \sqrt[2^k]{\alpha} \le 1+\frac{\sqrt{\alpha}M_{permissive}}{\sqrt{N}\sqrt{1+\alpha^2}}$$
$$\Rightarrow k \ge \left\lfloor \log_2 \frac{\ln\alpha}{\ln(1+\frac{\sqrt{\alpha}}{\sqrt{1+\alpha^2}}\frac{M_{permissive}}{\sqrt{N}})} \right\rfloor$$

(2) The procedure can surely be applied to parallel computing because the searching process in Step 3 is independent of one another. An efficient searching process is of course necessary.

Example 1. Let $N = 1333$; α is set to be 2 and $M_{permissive}$ is set to be 10. Then direct calculation yields $k = 2$; and then

$$Q_0 = (\frac{\sqrt{N}}{\sqrt[4]{\alpha^0}}, \sqrt[4]{\alpha^0}\sqrt{N}) \approx (36.51, 36.51)$$

$$Q_1 = (\frac{\sqrt{N}}{\sqrt[4]{\alpha}}, \sqrt[4]{\alpha}\sqrt{N}) \approx (30.7, 43.41)$$

and

$$Q_2 = (\frac{\sqrt{N}}{\sqrt[4]{\alpha^2}}, \sqrt[4]{\alpha^2}\sqrt{N}) \approx (25.57, 51.63)$$

Odd point $(u, v) = (31, 43)$, which satisfies $uv = N$, is found near Q_1 . And the divisor-ration of 1333 is $\beta = \frac{43}{31} \approx 1.3871$.

Example 2. Let $N = 4171$; α is set to be 2 and $M_{permissive}$ is set to be 10. Then $k = 2$ and thus

$$Q_0 = (\frac{\sqrt{N}}{\sqrt[4]{\alpha^0}}, \sqrt[4]{\alpha^0}\sqrt{N}) \approx (64.58, 64.58)$$

$$Q_1 = (\frac{\sqrt{N}}{\sqrt[4]{\alpha}}, \sqrt[4]{\alpha}\sqrt{N}) \approx (54.73, 76.204)$$

and

$$Q_2 = (\frac{\sqrt{N}}{\sqrt[4]{\alpha^2}}, \sqrt[4]{\alpha^2}\sqrt{N}) \approx (45.67, 91.32)$$

There is not an odd point on either $\overset{\frown}{Q_0Q_1}$ or $\overset{\frown}{Q_1Q_2}$. Accordingly $\beta > \sqrt[4]{8} \approx 1.68$.

Example 3. Let $N = 4171$; α is set to be 2.25 and $M_{permissive}$ is set to be 10. Then $k = 3$ and

$$Q_0 = (\frac{\sqrt{N}}{\sqrt[8]{\alpha^0}}, \sqrt[8]{\alpha^0}\sqrt{N}) \approx (64.583280, 64.583280)$$

$$Q_1 = (\frac{\sqrt{N}}{\sqrt[8]{\alpha}}, \sqrt[8]{\alpha}\sqrt{N}) \approx (58.357581, 71.473148)$$

$$Q_2 = (\frac{\sqrt{N}}{\sqrt[8]{\alpha^2}}, \sqrt[8]{\alpha^2}\sqrt{N}) \approx (52.732027, 79.098040)$$

$$Q_3 = (\frac{\sqrt{N}}{\sqrt[8]{\alpha^3}}, \sqrt[8]{\alpha^3}\sqrt{N}) \approx (47.648765, 87.536371)$$

and

$$Q_4 = (\frac{\sqrt{N}}{\sqrt[8]{\alpha^4}}, \sqrt[8]{\alpha^4}\sqrt{N}) \approx (43.055520, 96.874919)$$

There is not an odd point on either $\overset{\frown}{Q_0Q_1}$, $\overset{\frown}{Q_1Q_2}$, $\overset{\frown}{Q_2Q_3}$ or $\overset{\frown}{Q_3Q_4}$. Accordingly $\beta > \sqrt[8]{2.25^7} \approx 2.033$. In fact. the divisor ratio of 4171 is $\beta = \frac{97}{43} \approx 2.2558$.

5 Conclusions and Future Work

Estimating the divisor ratio of a semiprime is surely helpful for the factorization of the semiprime. The approach raised in this paper can limit an small interval containing the divisors of a semiprime with a small divisor ratio or not by predicting an initial divisor ratio. As is seen, the efficiency of the approach depends on that of the search on the hyperbolic arcs. Since a big semiprime such as the RSA numbers will generates a very large searching arc, fast searching algorithms are still in need. That is what the future work concerns. Hope more gougers join to perfect the work.

References

[1] Zvonko Čerin. (2001).On Properties of Rectangular Hyperbolas. Geometriae Dedicata, 84(1-3):41-47. https://doi.org/10.1023/A:1010396627915

[2] Pamfilos P. (2021). On Rectangular Hyperbolas Circumscribing a triangle. Global Journal of Advanced Research on Classical and Modern Geometries. 10(1),1-14.

[3] Wang X, Han M. (2022). New Fantastic Curves Discovered from Rectangular Hyperbola. Journal of Advances in Mathematics and Computer Science, 37(5), 10-31. https://doi.org/10.9734/jamcs/2022/v37i530450

[4] Cilleruelo J, J Jiménez-Urroz. (1997). Lattice Points on Hyperbolas. Journal of Number Theory, 63(2), 267-274. https://doi.org/10.1006/jnth.1997.2051

[5] Hansaem Ko, Yeonok Kim. (2013). A Note On The Integral Points on Some Hyperbolas. J. Korean Soc. Math. Educ. Ser. B: Pure Appl. Math., 20(3),137-148.http://dx.doi.org/10.7468/jksmeb.2013.20.3.137

[6] Goins E H , Mugo K . (2012). Points on Hyperbolas at Rational Distance. International Journal of Number Theory, 8(4),911–922.https://doi.org/10.1142/S1793042112500534

[7] MA Gopalan, S Vidhyalakshmi, N Thiruniraiselvi.(2013). A Study on the Hyperbola y2-8x2=31. International Journal of Latest Research in Science and Technology,2(1)454-456.

[8] Gilda Rech Bansimba, Regis Freguin Babindamana and Basile Guy Richard Bossoto. (2021). Some Arithmetical Properties of Hyperbola, JP Journal of Algebra, Number Theory and Applications.50(1),45-100. http://dx.doi.org/10.17654/NT050010045

[9] Babindamana R F , Bansimba G R , Bossoto B .(2022). Lattice Points on the Fermat Factorization Method. Journal of Mathematics. https://doi.org/10.1155/2022/6360264

[10] Wang X. (2018). Influence of Divisor-ratio to Distribution of Semiprime's Divisor. Journal of Mathematics Research. 10(4),54-61. https://doi.org/10.5539/jmr.v10n4p54

[11] Wang X, (2021). Bound Estimation for Divisors of RSA Modulus with Small Divisor-ratio. International Journal of Network Security. 23(3),412-425. http://ijns.jalaxy.com.tw/contents/ijns-v23-n3/ijns-v23-n3.pdf

[12] Andreescu T , Andrica D , Cucurezeanu I . (2010). An introduction to diophantine equations : a problem-based approach. Birkhäuser Boston.

Appendix: Maple source codes

This appendix section shows Maple source codes to perform the procedure in Section 4.2. In the procedure, the argument α is the randomly set initial value of the divisor ratio of N and the argument M is $M_{permissive}$.

```
Estimation:=proc(α, M, N)
local k, x, y, j, powr;
 k := floor(log2(ln(α)/ln(1 + sqrt(α)/sqrt(1+α^2) * M/sqrt(N))));
 printf("k=%d\n", k);
 powr := 2^k;
 for j from 1 to 2^(k-1) do
  x := evalf(sqrt(N)/(powr sqrt(α^(j-1))));
  y := evalf((powr sqrt(α^(j-1))) * sqrt(N));
  printf("Q(%d)=(%f , %f )\n", j, x, y);
  od;
  x := evalf(sqrt(N/α)); y := evalf(sqrt(α*N));
 printf("Q(%d)=(%f , %f )\n", j, x, y);
 printf("α might be bigger than %f\n", evalf((powr sqrt(α^(powr-1)))));
end proc
```