Global Journal of Advanced Research
on Classical and Modern Geometries
ISSN: 2284-5569, Vol.12, (2023), Issue 2, pp.316-330

A BI-PARAMETER ELLIPSE AVAILABLE FOR STUDYING INTEGERS

XINGBO WANG, LI MA, AND MIAN JIANG

ABSTRACT. This paper first defines a bi-parameter ellipse and then place it together with the rectangular hyperbola $xy = N$ to study their intersections. The study reveals several new properties of the intersections that are merely dependent on the two parameters that determine the ellipse. It is also shown that the new properties are available for studying integers and are helpful to develop new method to factorizing integers. Mathematical reasoning is presented in detail for each conclusion and each conclusion is demonstrated with Geogebra software.

1. INTRODUCTION AND MOTIVATIONS

Factorization of a composite integer N is geometrically to find integer points on the hyperbola $xy = N$ in Cartesian coordinate system. That is why people have kept researching new methods to factorize integers with conic sections (see [1],[2],[3],[4],and [5]). For a composite integer $N = pq$ with $1 < p < q$ being integers, it is sure that N can be easily factorized if the divisor ratio $k = q/p$ were known. Since k is hardly known before N is factorized, its evaluation becomes a research topic. Wang investigated the influence of the divisor-ratio to the distribution of a semiprime's divisor([6]); he also investigated rectangular hyperbola and ellipse to find a way to evaluate the divisor ratio of a semiprime by means of constructing certain arcs on the hyperbola and ellipse (see [7] and [8]). Following the previous study, this paper investigates a family of ellipses that can derive more properties relevant to k and N. By defining an ellipse whose equation contains k and N as parameters, and placing the ellipse together with the hyperbola $xy = N$, k's change and N's change exhibit very interesting traits that can derive new method to factorize integers.

The paper consists of five sections. Except for this introductory section, section 2 lists symbols and proves several lemmas necessary for the mathematical deductions in later sections, section 3 presents main results, section 4 introduces potential applications of the study, and section 5 gives the conclusion content.

2010 *Mathematics Subject Classification.* 51N20;11A51.
Key words and phrases. Ellipse, Hyperbola, Intersection, Discriminant, Integer factorization.

2. PRELIMINARIES

This section presents necessary symbols, notations, and the fundamental knowledge for later investigation. Subsection 2.1 introduces the symbols and notations; subsection 2.2 proves several lemmas relevant to the cubic algebraic equation that is utilized in Section 3.

2.1. **Symbols and Notations.** In this whole paper, symbol $A \Rightarrow B$ means statement A can derive out statement B. Symbol $P : (x, y)$ or $P = (x, y)$ means a point P with x and y being its coordinates. P is an integer point means both its x-coordinate and y-coordinate are integers. Symbol $\Gamma : f(x, y) = 0$ means the curve Γ is defined by the equation $f(x, y) = 0$. The hyperbola $H : xy = N$ is restricted with $x > 0$, $y > 0$, and $N > 0$ being real numbers unless particularly commented.

2.2. **Lemmas.** The following lemmas are necessary for analyzing the roots of a cubic algebraic equation, which frequently occurs in finding the intersections of two conic sections.

Lemma 2.1. *Assume $\alpha \neq 0$ is a root of the cubic equation $ax^3 + bx^2 + cx + d = 0$ with $a \neq 0$ and $d \neq 0$; then $\frac{1}{\alpha}$ is a root of $dx^3 + cx^2 + bx + a = 0$.*

Proof. Since $a\alpha^3 + b\alpha^2 + c\alpha + d = \alpha^3(a + \frac{b}{\alpha} + \frac{c}{\alpha^2} + \frac{d}{\alpha^3})$, it yields

$$a\alpha^3 + b\alpha^2 + c\alpha + d = 0 \Leftrightarrow \alpha^3(a + \frac{b}{\alpha} + \frac{c}{\alpha^2} + \frac{d}{\alpha^3}) = 0$$

which confirms the lemma. □

Lemma 2.2. *Assume $\alpha \neq 0$ is a repeated root of the cubic equation $ax^3 + 3bx^2 + 3cx + d = 0$ with $a \neq 0$ and $d \neq 0$. Let $\delta_1 = ac - b^2$, $\delta_2 = ad - bc$, and $\delta_3 = bd - c^2$; then $\alpha = -\frac{\delta_2}{2\delta_1}$ and $\alpha^2 = \frac{\delta_3}{\delta_1}$ provided that $\delta_1 \neq 0$, $\delta_2 \neq 0$, and $\delta_3 \neq 0$. Another root of the equation is $\beta = -\frac{3b}{a} + \frac{\delta_2}{\delta_1} = \frac{a^2d - 4abc + 3b^3}{a(ac - b^2)}$.*

Lemma 2.2*. Assume $\alpha \neq 0$ is a repeated root of the cubic equation $ax^3 + bx^2 + cx + d = 0$ with $a \neq 0$ and $d \neq 0$. Let $\delta_1 = 3ac - b^2$, $\delta_2 = 9ad - bc$, and $\delta_3 = 3bd - c^2$; then $\alpha = -\frac{\delta_2}{2\delta_1}$ and $\alpha^2 = \frac{\delta_3}{\delta_1}$ provided that $\delta_1 \neq 0$, $\delta_2 \neq 0$, and $\delta_3 \neq 0$. Another root of the equation is $\beta = -\frac{b}{a} + \frac{\delta_2}{\delta_1}$.

Proof. Only prove Lemma 2.2 only because Lemma 2.2* is proven in the same way. Let $g(x) = ax^3 + 3bx^2 + 3cx + d$ and $h(x) = dx^3 + 3cx^2 + 3bx + a$; then $g'(\alpha) = 0$ and $h'(\frac{1}{\alpha}) = 0$, which lead to

$$\begin{cases} 3a\alpha^2 + 6b\alpha + 3c = 0 \\ \frac{3d}{\alpha^2} + \frac{6c}{\alpha} + 3b = 0 \end{cases} \Rightarrow \begin{cases} 3a\alpha^2 + 6b\alpha + 3c = 0 \\ 3b\alpha^2 + 6c\alpha + 3d = 0 \end{cases}$$
$$\Rightarrow \begin{cases} 2(ac - b^2)\alpha + ad - bc = 0 \Rightarrow \alpha = -\frac{ad - bc}{2(ac - b^2)} = -\frac{\delta_2}{2\delta_1} \\ (ac - b^2)\alpha^2 + c^2 - bd = 0 \Rightarrow \alpha^2 = \frac{bd - c^2}{ac - b^2} = \frac{\delta_3}{\delta_1} \end{cases}$$

The Vieta's formula $2\alpha + \beta = -\frac{3b}{a}$ immediately leads to $\beta = -\frac{3b}{a} + \frac{\delta_2}{\delta_1}$. □

Lemma 2.3. *For given real numbers a, b, c and d with $a \neq 0$ and $d \neq 0$, assume $\delta_1 = ac - b^2 \neq 0$, $\delta_2 = ad - bc \neq 0$, and $D = a^2d^2 - 6abcd + 4ac^3 + 4b^3d - 3b^2c^2$; then $\alpha = -\frac{\delta_2}{2\delta_1}$ is a repeated root of the cubic equation $ax^3 + 3bx^2 + 3cx + d = 0$ if and only if $D = 0$.*

Lemma 2.3*. For given real numbers a, b, c and d with $a \neq 0$ and $d \neq 0$, assume $\delta_1 = 3ac - b^2 \neq 0$, $\delta_2 = 9ad - bc \neq 0$, and $D = 27a^2d^2 - 18abcd + 4ac^3 + 4b^3d - b^2c^2$; then $\alpha = -\frac{\delta_2}{2\delta_1}$ is a repeated root of the cubic equation $ax^3 + bx^2 + cx + d = 0$ if and only if $D = 0$.

Proof. Only prove Lemma 2.3 only because Lemma 2.3* can be simply proven by substituting b with $\frac{b}{3}$ and c with $\frac{c}{3}$ in Lemma 3. Let $f(x) = ax^3 + 3bx^2 + 3cx + d$. By Lemma 2, $\beta = -\frac{3b}{a} + \frac{\delta_2}{\delta_1}$ is a root of $f(x) = 0$. Calculations of division with remainder show

$$f(x) = a(x-\beta)((x + \frac{\delta_2}{2\delta_1})^2 + \frac{3D}{4\delta_1^2}) + (a\delta_2 - 2b\delta_1)D$$

and

$$f(x) = a(x-\alpha)^2(x + \frac{3b}{a} - \frac{\delta_2}{\delta_1}) + \frac{3aDx}{4(ac-b^2)^2} + \frac{(a^2d - b^3)D}{4(ac-b^2)^3}$$

These two formulas immediately approve the Lemma. □

3. MAIN RESULTS

In subsection 3.1, we define an ellipse Γ that is with two parameters k and N, and then investigate its basic properties. In subsections 3.2 to 3.4, we place the hyperbola $H : xy = N$ together with Γ and investigate the influence of each parameter to the intersections of H intersecting Γ.

3.1. **An Ellipse with Two Parameters.**

Let $k > 0$ and $N > 0$ be real numbers; define in the Cartesian coordinate system a planar curve Γ by

$$\begin{aligned}\Gamma : 6\sqrt{2}k(24+k^2)x^2 + 276\sqrt{2}k^2xy + 6\sqrt{2}k(24k^2+1)y^2 - (288(k^2+1)\sqrt{2k} + 35k^2\sqrt{k^2+1})\sqrt{N}x \\ -(288(k^2+1)\sqrt{2k} - 35\sqrt{k^2+1})k\sqrt{N}y + 144\sqrt{2}(k^2+1)^2N = 0\end{aligned} \tag{3.1}$$

Then the following Theorem 3.1 holds.

Theorem 3.1. *Γ is an ellipse having the following properties.*
(P1). It is tangent to the line $T_P : y = kx$ at point $P : (\sqrt{\frac{N}{k}}, \sqrt{kN})$ and the line $T_Q : y = k^*x$ with

$$k^* = k - \frac{20160\sqrt{2}\sqrt{k(k^2+1)}(k^2+1)}{20160\sqrt{2}k\sqrt{k(k^2+1)} + 6912k^2 - 1225k + 6912}$$

(P2). Its center $C : (x_c, y_c)$ is given by

$$\begin{cases} x_c = (\frac{1}{\sqrt{k}} + \frac{35\sqrt{2}}{24} \cdot \frac{k}{\sqrt{k^2+1}})\sqrt{N} \\ y_c = (\sqrt{k} - \frac{35\sqrt{2}}{24} \cdot \frac{1}{\sqrt{k^2+1}})\sqrt{N} \end{cases}$$

and two loci, $F_1 : (x_1, y_1)$ and $F_2 : (x_2, y_2)$, are calculated by

$$\begin{cases} x_1 = (\frac{1}{\sqrt{k}} + \frac{(35\sqrt{69}+210\sqrt{2})}{144} \cdot \frac{k}{\sqrt{k^2+1}})\sqrt{N} \\ y_1 = (\sqrt{k} - \frac{(35\sqrt{69}+210\sqrt{2})}{144} \cdot \frac{1}{\sqrt{k^2+1}})\sqrt{N} \end{cases}$$

and

$$\begin{cases} x_2 = (\frac{1}{\sqrt{k}} - \frac{(35\sqrt{69}-210\sqrt{2})}{144} \cdot \frac{k}{\sqrt{k^2+1}})\sqrt{N} \\ y_2 = (\sqrt{k} + \frac{(35\sqrt{69}-210\sqrt{2})}{144} \cdot \frac{1}{\sqrt{k^2+1}})\sqrt{N} \end{cases}$$

Proof. First prove (P1). Assume the equation of the tangent line is $y = sx$. Substituting this into the equation of Γ yields

$$(6\sqrt{2}k((k^2+24)+46ks+(24k^2+1)s^2))x^2 - ((288k^2+288)\sqrt{2}\sqrt{kN}+35k^2\sqrt{k^2+1}\sqrt{N} \\ +((288k^2+288)\sqrt{2}\sqrt{k^3N}-35k\sqrt{k^2+1}\sqrt{N})s)x + 144\sqrt{2}(k^2+1)^2N = 0$$

Denote

$$\begin{cases} a = 6\sqrt{2}k((k^2+24)+46ks+(24k^2+1)s^2) \\ b = (288k^2+288)\sqrt{2}\sqrt{kN}+35k^2\sqrt{k^2+1}\sqrt{N}+((288k^2+288)\sqrt{2}\sqrt{k^3N}-35k\sqrt{k^2+1}\sqrt{N})s \\ c = 144\sqrt{2}(k^2+1)^2N \end{cases}$$

Solving the quadratic equation $b^2 - 4ac = 0$ with respect to s yields $s_1 = k$ and

$$s_2 = k - \frac{20160\sqrt{2}\sqrt{k(k^2+1)}(k^2+1)}{20160\sqrt{2}k\sqrt{k(k^2+1)}+6912k^2-1225k+6912}$$

Thereby, Γ is tangent to $T_P : y = kx$ and $T_Q : y = k^*x$. Direct calculation shows that T_P is tangent to Γ at $P : (\sqrt{\frac{N}{k}}, \sqrt{kN})$.
To prove (P2), let

$$\begin{cases} A = 6\sqrt{2}k(24+k^2) \\ B = 276\sqrt{2}k^2 \\ C = 6\sqrt{2}k(24k^2+1) \\ D = -(288(k^2+1)\sqrt{2k}+35k^2\sqrt{k^2+1})\sqrt{N} \\ E = -(288(k^2+1)\sqrt{2k}-35\sqrt{k^2+1})k\sqrt{N} \\ F = 144\sqrt{2}(k^2+1)^2N \end{cases} \tag{3.2}$$

then it follows

$$B^2 - 4AC = -6912k^2(k^2+1)^2 < 0$$

Referring to page 63 in Lawrence's book [9] and Ayoub's paper [10], Γ is known to be an ellipse whose center is calculated by

$$\begin{cases} x_c = \frac{BE-2CD}{4AC-B^2} \\ y_c = \frac{BD-2AE}{4AC-B^2} \end{cases}$$

and whose majoraxis α and minoraxis β are respectively given by

$$\alpha, \beta = -\frac{2\sqrt{2(AE^2+CD^2-BDE+(B^2-4AC)F)((A+C)\pm\sqrt{(A-C)^2+B^2})}}{B^2-4AC}$$

Direct calculations yield

$$\begin{cases} x_c = (\frac{1}{\sqrt{k}} + \frac{35\sqrt{2}}{24} \cdot \frac{k}{\sqrt{k^2+1}})\sqrt{N} \\ y_c = (\sqrt{k} - \frac{35\sqrt{2}}{24} \cdot \frac{1}{\sqrt{k^2+1}})\sqrt{N} \end{cases}$$

$$\alpha = \frac{35\sqrt{2N}}{12} \text{ and } \beta = \frac{35\sqrt{3N}}{72}$$

Meanwhile the equation of the line T_P^* that is perpendicular to T_P and passes the point P is given by

$$y - \sqrt{kN} = -\frac{1}{k}(x - \sqrt{\frac{N}{k}})$$

This shows the center C is on T_P^* and therefore the majoraxis coincides with T_P^* because T_P^* intersects Γ at $P^* : (x^*, y^*)$, which is calculated by

$$\begin{cases} x^* = \sqrt{\frac{N}{k}} + \frac{35\sqrt{2N}}{12} \cdot \frac{k}{\sqrt{k^2+1}} \\ y^* = \sqrt{kN} - \frac{35\sqrt{2N}}{12} \cdot \frac{1}{\sqrt{k^2+1}} \end{cases}$$

As a result, the two loci are calculated as the theorem claims. □

Remark 1. The area of Γ is N-dependent because $\alpha = \frac{35\sqrt{2N}}{12}$ and $\beta = \frac{35\sqrt{3N}}{72}$. The eccentricity of Γ is $e = \sqrt{1 - (\frac{\beta}{\alpha})^2} = \sqrt{\frac{69}{72}} = \approx 0.9789450100$, meaning Γ is quite flat, as shown in Figure 1, in which T_P, T_P^*, and T_Q are also exhibited. Note that T_Q is tangent to Γ at Q; hence O is the pole of the polar line PQ.

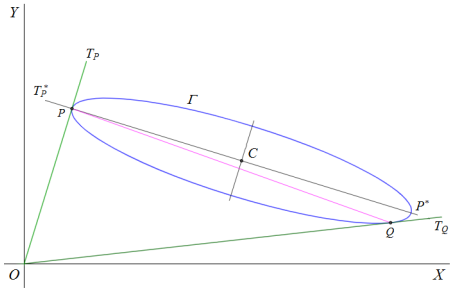


Figure 1. Γ, T_P, T_P^*, and T_Q

Place the hyperbola $H : xy = N$ together with Γ, T_P, and T_P^*, as shown in Figure 2; it is seen that H, Γ, T_P, and T_P^* are concurrent at P because $P : (\sqrt{\frac{N}{k}}, \sqrt{kN})$ is also the intersection of H and T_P.

3.2. **The Parameter k.** By definition and Remark 1, Γ changes its position and direction with the change of k for a fixed N, as illustrated in Figure 3. In the figure, Γ_1, Γ_2, and Γ_3 are respectively matching to the cases of $k = k_1$, $k = k_2$, and $k = k_3$. In later sections, symbol Γ_k is to stand for the configuration of Γ under a specific k for a fixed N.
k's change affects not only the position and direction of Γ but also the number of intersections between H and Γ, as the following Theorem 3.2 states.

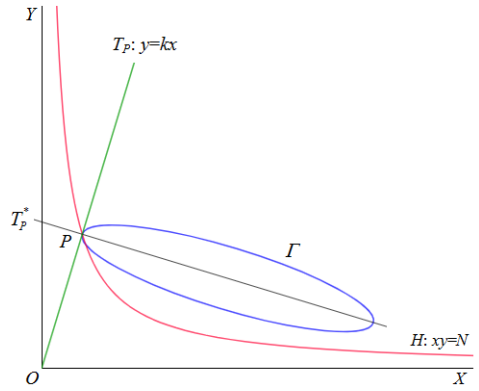


Figure 2. H,Γ, T_P, T_P^*, and T_Q are concurrent at P

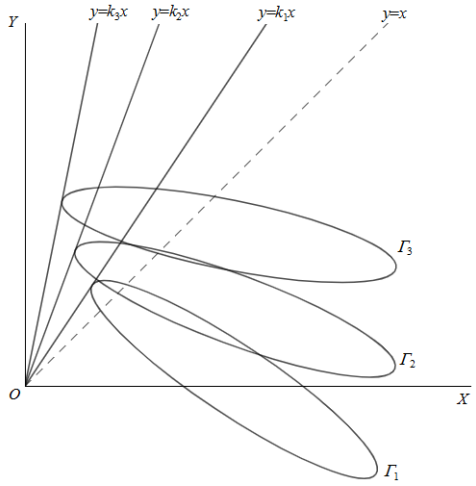


Figure 3. Γ changes its position and direction with k

Theorem 3.2. *If $k > 1$, H and Γ might have 2, 3, or 4 intersections. There are two values of k, say k_s and k_b with $k_s < k_b$, such that $k = k_s$ or $k = k_b$ yields H and Γ have 3 intersections, $k_s < k < k_b$ yields H and Γ have 4 intersections and the other cases yield H and Γ have 2 intersections.*

Proof. Putting $y = \frac{N}{x}$ into (3.1) obtains the following quartic equation from which the x-coordinates of the intersections can be solved by

$$\begin{aligned} 6\sqrt{2}k(24+k^2)x^4 - (288(k^2+1)\sqrt{2k}+35k^2\sqrt{k^2+1})\sqrt{N}x^3 + 12\sqrt{2}(12k^4+47k^2+12)Nx^2 \\ -(288(k^2+1)\sqrt{2k}-35\sqrt{k^2+1})kN\sqrt{N}x + 6\sqrt{2}k(24k^2+1)N^2 = 0 \end{aligned} \tag{3.3}$$

Referring to the proof of Theorem 3.5, it is sure equation (3.3) might have 2, 3, or 4 real solutions when $k > 1$. Let $G_4(x)$ be the left side of (3.3), namely,

$$\begin{aligned} G_4(x) = 6\sqrt{2}k(24+k^2)x^4 - (288(k^2+1)\sqrt{2k}+35k^2\sqrt{k^2+1})\sqrt{N}x^3 + 12\sqrt{2}(12k^4+47k^2+12)Nx^2 \\ -(288(k^2+1)\sqrt{2k}-35\sqrt{k^2+1})kN\sqrt{N}x + 6\sqrt{2}k(24k^2+1)N^2 \end{aligned}$$

then (3.3) is equivalent to $G_4(x) = 0$. Direct calculations show

$$G_4(x) = (x - \sqrt{\frac{N}{k}})G_3(x) \tag{3.4}$$

where $G_3(x)$ is

$$G_3(x) = g_3x^3 + 3g_2x^2 + 3g_1x + g_0 \tag{3.5}$$

with

$$\begin{cases} g_3 = 6\sqrt{2}k(k^2+24) \\ g_2 = -\frac{(282k^2\sqrt{2k}+35k^2\sqrt{k^2+1}+144\sqrt{2k})\sqrt{N}}{3} \\ g_1 = \frac{(144\sqrt{2}k^4-35k\sqrt{k(k^2+1)}+282\sqrt{2}k^2)N}{3} \\ g_0 = -6\sqrt{2}\left(24k^2+1\right)kN\sqrt{kN} \end{cases} \tag{3.6}$$

Obviously, $k > 1$ yields

$$\begin{cases} g_3 > 0 \\ g_2 < 0 \\ g_1 > 0 \\ g_0 < 0 \end{cases} \tag{3.7}$$

Note that

$$G_3(x) = (x - \sqrt{\frac{K}{k}})G_2(x) + R_2(x)$$

where

$$G_2(x) = g_3x^2 - (35\sqrt{k^2+1} + 276\sqrt{2k})k^2\sqrt{N}x - (70k\sqrt{k(k^2+1)} - 6\sqrt{2}k^2(24k^2+1))N$$

and

$$R_2(x) = -70k\sqrt{k^2+1} \cdot N\sqrt{N}$$

It is known that $x_0 = \sqrt{\frac{N}{k}}$ is a root of $G_4(x) = 0$ but not a root of $G_3(x) = 0$; thus $G_3(x)$ might be one of the following four forms

$$G_3(x) = g_3(x - x_1)^3, x_1 \in \mathbf{R} \tag{3.8}$$

$$G_3(x) = g_3(x - x_1)^2(x - x_2), x_1, x_2 \in \mathbf{R} \tag{3.9}$$

$$G_3(x) = g_3(x - x_1)(x - x_2)(x - x_3) = 0, x_1, x_2, x_3 \in \mathbf{R} \tag{3.10}$$

or

$$G_3(x) = g_3(x - x_1)(x - z_0)(x - \bar{z}_0) = 0, z_0 \in \mathbf{C}, x_1 \in \mathbf{R} \tag{3.11}$$

where z_0 and $\bar{z}_0$ are conjugated complex numbers, $x_1 \neq \sqrt{\frac{N}{k}}$ in (3.8) and (3.11), $x_1 \neq x_2 \neq \sqrt{\frac{N}{k}}$ in (3.9), $x_1 \neq x_2 \neq x_3 \neq \sqrt{\frac{N}{k}}$ in (3.10).

It can be proven that $G_3(x)$ cannot be of the form (3.8). In fact, assume $G_3(x) = g_3(x - x_1)^3 = g_3x^3 - 3g_3x^2x_1 + 3g_3xx_1^2 - g_3x_1^3$; then compared with (3.5) and by (3.6), x_1 must simultaneously satisfies the following 3 equalities

$$\begin{cases} x_1 = -\frac{g_2}{g_3} = \frac{(282k^2\sqrt{2k}+35k^2\sqrt{k^2+1}+144\sqrt{2k})\sqrt{N}}{18\sqrt{2k}(k^2+24)} \\ x_1^2 = \frac{g_1}{g_3} = \frac{(144\sqrt{2}k^4-35k\sqrt{k(k^2+1)}+282\sqrt{2}k^2)N}{18\sqrt{2}k(k^2+24)} \\ x_1^3 = -\frac{g_0}{g_3} = \frac{\left(24k^2+1\right)N\sqrt{kN}}{(k^2+24)} \end{cases}$$

These immediately lead to contradictions because the 3 equalities can hardly simultaneously hold. Consequently, $G_3(x)$ might be of the form (3.9), (3.10) or (3.11).
Now let

$$\begin{cases} \delta_1 = g_3 g_1 - g_2^2 \\ \delta_2 = g_3 g_0 - g_2 g_1 \\ \delta_3 = g_2 g_0 - g_1^2 \\ \Delta = 4\delta_1\delta_3 - \delta_2^2 \end{cases} \tag{3.12}$$

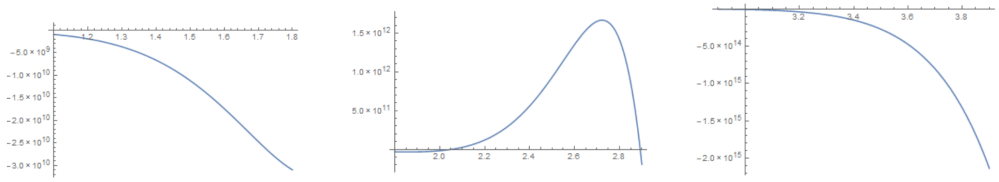
then according to Blinn's method [11], the case $\delta_1 = \delta_2 = \delta_3 = 0$ is impossible because $G_3(x)$ is impossible to be of the form (3.8). Thereby, there are 3 cases left to investigate:
Case 1. $\Delta = 0$. It means $G_3(x)$ is of the form (3.9) and $G_4(x) = 0$ have 3 distinct real solutions; and thus Γ and H have 3 intersections.
Case 2. $\Delta > 0$. It means $G_3(x)$ is of the form (3.10) and $G_4(x) = 0$ has 4 distinct real solutions ; and thus Γ and H have 4 intersections.
Case 3. $\Delta < 0$. It means $G_3(x)$ is of the form (3.11) and $G_4(x) = 0$ has 2 real solutions; and thus Γ and H have 2 intersections.
Direct calculations yield

$$\Delta = g(k)N^3 \tag{3.13}$$

where

$$\begin{aligned} g(k) = -10616832(k^{10} - \frac{1225}{6912}k^9 - \frac{8}{3}k^8 + \frac{52675}{10368}k^7 + \frac{484219439}{286654464}k^6 + \frac{9818375}{995328}k^5 \\ + \frac{484219439}{286654464}k^4 + \frac{52675}{10368}k^3 - \frac{8}{3}k^2 - \frac{1225}{6912}k + 1)k^3(k^2+1) + 39997440\sqrt{2}(k^8 - \frac{1225k^7}{35712} \\ - \frac{157k^6}{186} - \frac{1225k^5}{35712} + \frac{1225k^3}{35712} + \frac{157k^2}{186} + \frac{1225k}{35712} - 1)k^4\sqrt{k(k^2+1)} \end{aligned} \tag{3.14}$$

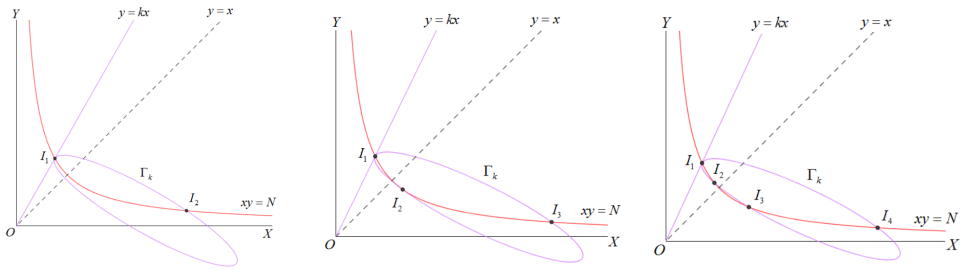
With Mathematica software, $g(k)$ is drawn for $1 < k \leq 1.8$, $1.8 < k \leq 2.9$, and $k > 2.9$, as demonstrated respectively in Figures 4(a), 4(b), and 4(c). It is seen from Figure 4(b) that $g(k) = 0$ has merely two zero-points in $2 < k < 2.9$. In fact, directly calculations show $g(2.0) \approx -1.69016 \times 10^{10}$, $g(2.05) \approx 1.72031 \times 10^8$, $g(2.89) \approx -6.78311 \times 10^{10}$, and $g(2.9) \approx 1.93021 \times 10^{11}$. It is known that $2 < k_s < k_b < 2.9$. Seen in (13), the roots of $\Delta = 0$ is N-independent. That is to say, k_s and k_b are fixed values no matter how N changes. Roughly calculated, they are around $2.04959862 + \frac{1}{300000000}$ and 2.8927390012, respectively. □



(a) $g(k)$ *for* $1 < k \leq 1.8$ (b) $g(k)$ *for* $1.8 < k \leq 2.9$ (c) $g(k)$ *for* $k > 2.9$

Figure 4. Graph of $g(k)$ in different intervals

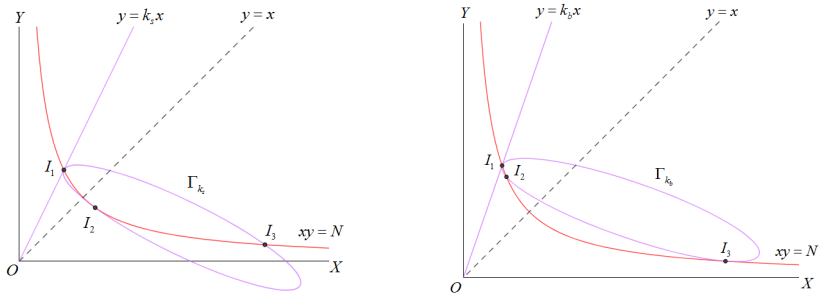
Remark 2. Theorem 3.2 can easily be demonstrated with dynamic geometry software GeoGebra. For example, taking $N = 1333$ and letting k change from 1.05 to 3 demonstrate with Geogebra that there are true cases of 2,3 and 4 intersections from Γ intersecting H, as shown in Figure 5.



(a) Two intersections (b) Three intersections (c) Four intersections

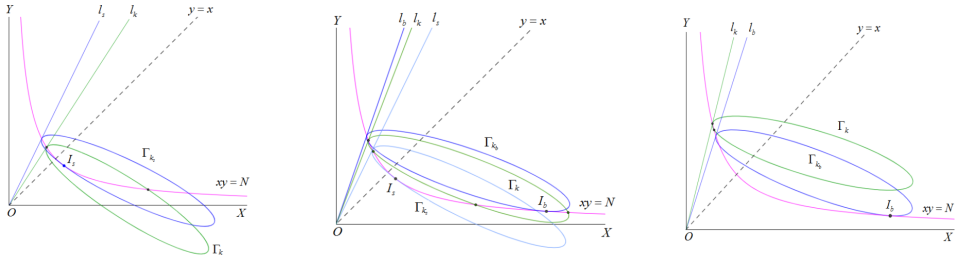
Figure 5. Different number of intersections from Γ intersecting H

Geogebra also shows that, there are two values of k, say k_s and k_b with $k_s < k_b$, at each of which Γ and H have 3 intersections, as demonstrated with Figure 6. In the figure, the intersections are marked by small dots. Geometrically seen, the case that Γ and H have 3 intersections occurs when Γ is tangent to H.
It is also seen that $k < k_s$ or $k > k_b$ brings 2 intersections while $k_s < k < k_b$ brings 4 intersections, as shown in Figure 7. In the figure, l_b is the line $y = k_b x$, l_s is the line $y = k_s x$, and l_k is the line $y = kx$; the small dots are intersections among which I_s and I_b are respectively intersections of l_s and l_b intersecting $H : xy = N$.



(a) Three intersections at $k = k_s$ (b) Three intersections at $k = k_b$

Figure 6. Two cases of three intersections from Γ intersecting H



(a) Case $k < k_s$ (b) Case $k_s < k < k_b$ (c) Case $k > k_b$

Figure 7. Different number of intersections from Γ_k intersecting H

Theorem 3.2 establishes the relationship between k's distribution and the number of intersections from H intersecting Γ. The next Theorem 3.3 describes more traits of the intersections.

Theorem 3.3. *Let $G_3(x)$ be defined by (3.5), g_i ($i = 0,1,2,3$) be defined by (3.6), Δ and δ_j ($j = 1,2,3$) be defined by (3.12); denote x_1, x_2, and x_3 to be the roots of $G_3(x) = 0$; assume k_s and k_b are those stated in Theorem 3.2. Then*
(C31). $\Delta = 0$ results in a repeated real root $x_1 = -\frac{\delta_2}{2\delta_1} = \xi(k)\sqrt{N}$ plus another real root $x_2 = \zeta(k)\sqrt{N}$ such that $x_1|_{k=k_s} > \sqrt{N}$, $x_2|_{k=k_s} > 3\sqrt{N}$, $x_1|_{k=k_b} > 4\sqrt{N}$, and $x_2|_{k=k_b} < \frac{2}{3}\sqrt{N}$, where $\xi(k)$ and $\zeta(k)$ are k-related real numbers.
(C32). $\Delta > 0$ results in 3 distinct real roots $x_1 = \phi(k)\sqrt{N} > 0$, $x_2 = \varphi(k)\sqrt{N} > 0$, and $x_3 = \gamma(k)\sqrt{N} > 0$, where $\phi(k)$, $\varphi(k)$, and $\gamma(k)$ are k-related real numbers.
(C33). $\Delta < 0$ results in one real root $x_1 = \omega(k)\sqrt{N} > 0$, where $\omega(k)$ is a k-related real number.

Proof. First prove (C31). $\Delta = 0$ means $G_3(x)$ is of the form (3.9). By Lemma 2, x_1 is calculated by

$$x_1|_{\Delta=0} = -\frac{\delta_2}{2\delta_1} = \frac{g_1g_2 - g_0g_3}{2(g_2^2 - g_1g_3)}$$

Direct calculations obtain

$$x_1 = \frac{(65664k^4 - 1225k^3 - 173376k^2 - 1225k + 65664)k\sqrt{k} + 5040\sqrt{2}k\sqrt{k^2+1}(k^4-1)}{420\sqrt{2}\,(97k^2+120)\,k\sqrt{k}\sqrt{k^2+1} - 10368k^6 + 2450k^5 + 48960k^4 + 2450k^3 - 162432k^2 + 82944}\sqrt{N} \tag{3.15}$$

which indicates $x_1|_{k=k_s} \approx 1.15848\sqrt{N}$, $x_1|_{k=k_b} \approx 4.027\sqrt{N}$, and thus

$$x_1|_{\Delta=0,k=k_s} > \sqrt{N} \tag{3.16}$$

and

$$x_1|_{\Delta=0,k=k_b} > 4\sqrt{N} \tag{3.17}$$

Meanwhile, by Vieta's formula,

$$x_1^2x_2 = -\frac{g_0}{g_3} = \frac{\left(24k^2+1\right)N\sqrt{kN}}{(k^2+24)} \Rightarrow x_2 = \frac{\left(24k^2+1\right)N\sqrt{kN}}{(k^2+24)x_1^2} \tag{3.18}$$

This yields

$$x_2|_{k=k_s} = \frac{\left(24k^2+1\right)N\sqrt{kN}}{(k^2+24)x_1^2}|_{k=k_s} \approx 3.851503713\sqrt{N} > 3\sqrt{N} \tag{3.19}$$

and

$$x_2|_{k=k_b} = \frac{\left(24k^2+1\right)N\sqrt{kN}}{(k^2+24)x_1^2}|_{k=k_b} \approx 0.6628365784\sqrt{N} < \frac{2}{3}\sqrt{N} \tag{3.20}$$

These results match to Fig. 6 very well, showing x_2 is relatively small when $\Delta = 0$ and $k = k_b$. Now seen in (3.15) and (3.18), x_1 and x_2 are surely of the form

$$\begin{cases} x_1 = \xi(k)\sqrt{N} \\ x_2 = \zeta(k)\sqrt{N} \end{cases}$$

which validates (C31).

To prove (C32) and (C33), let $U = \frac{2g_2^3 - 3g_1g_2g_3 + g_0g_3^2}{2g_3^3}$, $V = \frac{g_2^2 - g_1g_3}{g_3^2}$, $D = U^2 - V^3$, $S = \sqrt[3]{-U + \sqrt{D}}$, and $T = \sqrt[3]{-U - \sqrt{D}}$ according to Adewumi's technique [12]. Direct calculations shows $U = u(k)N$ and $V = v(k)N$, where $u(k)$ and $v(k)$ are k-related real numbers. Thus S and T are of the form $S = s(k)\sqrt{N}$ and $T = t(k)\sqrt{N}$ with $s(k)$ and $t(k)$ being k-related real numbers.

For the case $\Delta > 0$, it holds $U^2 < V^3$. Letting $\theta = \arccos(\frac{U}{\sqrt{V^3}})$ leads to the three real roots by

$$\begin{cases} x_1 = -2\sqrt{V}\cos(\frac{\theta}{3}) - \frac{g_2}{g_3} \\ x_2 = -2\sqrt{V}\cos(\frac{\theta+2\pi}{3}) - \frac{g_2}{g_3} \\ x_3 = -2\sqrt{V}\cos(\frac{\theta-2\pi}{3}) - \frac{g_2}{g_3} \end{cases} \tag{3.21}$$

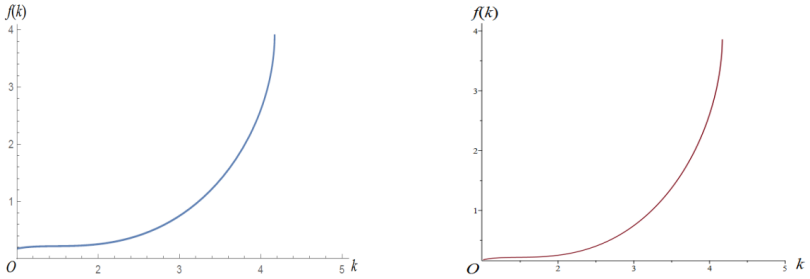
Since

$$\frac{g_2}{g_3} = -\frac{(282k^2\sqrt{2k} + 35k^2\sqrt{k^2+1} + 144\sqrt{2k})\sqrt{N}}{18\sqrt{2}k(k^2+24)}$$

and

$$V = \frac{g_2^2 - g_1g_3}{g_3^2} = \frac{N}{648k(k^2+24)^2}(\sqrt{2}(25200 + 20370k^2)k\sqrt{k(k^2+1)} \\ -5184k^6 + 1225k^5 + 24480k^4 + 1225k^3 - 81216k^2 + 41472)$$

x_1, x_2, and x_3 are surely of the forms $x_1 = \phi(k)\sqrt{N}$, $x_2 = \varphi(k)\sqrt{N}$, and $x_3 = \gamma(k)\sqrt{N}$. Let $f(k) = \frac{1}{\sqrt{N}}(-2\sqrt{V} - \frac{g_2}{g_3})$. Using Mathematica to plot $f(k)$ obtains Figure 8(a) ; Using Maple to plot it obtains Figure 8(b). Either one shows $f(k) > 0$. Seen in (3.21), $x_i \geq f(k)$. As a result, (C32) is established.



(a) Mathematica plot (b) Maple plot

Figure 8. Graphs of $f(k)$ plotted by Mathematica and Maple

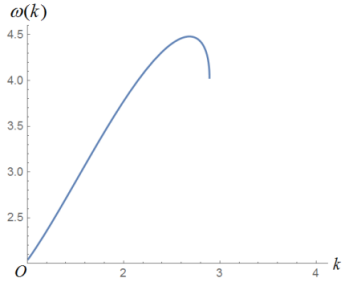
For the case $\Delta < 0$, it holds $U^2 > V^3$. The unique real root x_1 is calculated by

$$x_1 = S + T - \frac{g_2}{g_3}$$

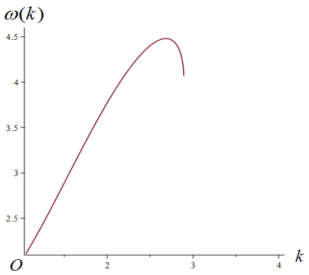
which is sure to be of the form

$$x_1 = \omega(k)\sqrt{N}$$

where $\omega(k)$ is a k-related real number.



(a) Mathematica plot



(b) Maple plot

Figure 9. Graphs of $\omega(k)$ plotted by Mathematica and Maple

$\omega(k)$ has a very complicated mathematical expression that is hardly analyzed manually; its graph is plotted with Mathematica or Maple, as seen in Figure 9, showing it is a positive function in its domain. Accordingly,(C33) is established.

□

3.3. **The Parameter** N**.** By Theorem 3.1 and Remark 1, for a fixed k, N's change makes Γ become larger or smaller. Except for this trait, there are other interesting properties described by the following Theorem 3.4.

Theorem 3.4. *Let $k > 1$, N_1, N_2, and N_3 be positive real numbers; denote E_1, E_2, and E_3 respectively to be the ellipses defined by (3.1) when fixing k and taking N by N_1, N_2, and N_3. Let H_1, H_2, and H_3 be respectively the hyperbolas $xy = N_1$, $xy = N_2$, and $xy = N_3$. Assume O is the coordinate origin. Then*
(C41). The line $y = kx$ is a common tangent line of E_1, E_2, and E_3; it tangents E_i at point $(x_0^i, y_0^i) = (\sqrt{\frac{N_i}{k}}, \sqrt{kN_i})$, where $i = 1, 2, 3$. The line $y = k^*x$ stated in Theorem 3.1 is also a common tangent line of E_1, E_2, and E_3.
(C42). When E_i and H_i ($i = 1, 2, 3$) have two intersections $I_0^i : (x_0^i, y_0^i)$ and $I_1^i : (x_1^i, y_1^i)$, the 4 points $I_0^1 : (x_0^1, y_0^1)$, $I_0^2 : (x_0^2, y_0^2)$, $I_0^3 : (x_0^3, y_0^3)$ and O are collinear and so it is with $I_1^1 : (x_1^1, y_1^1)$, $I_1^2 : (x_1^2, y_1^2)$, $I_1^3 : (x_1^3, y_1^3)$, and O. When E_i and H_i have 3 intersections, $I_0^i : (x_0^i, y_0^i)$ plus O are collinear, $I_1^i : (x_1^i, y_1^i)$ plus O are collinear, and $I_2^i : (x_2^i, y_2^i)$ plus O are collinear. When E_i and H_i have 4 intersections, $I_0^i : (x_0^i, y_0^i)$ plus O are collinear , $I_1^i : (x_1^i, y_1^i)$ plus O are collinear , $I_2^i : (x_2^i, y_2^i)$ plus O are collinear, and $I_3^i : (x_3^i, y_3^i)$ plus O are collinear.

Proof. By Theorem 3.1, the lines $y = kx$ and $y = k^*x$ tangent the ellipse (3.1) no matter how N changes. It is also know that $(x_0^i, y_0^i) = (\sqrt{\frac{N_i}{k}}, \sqrt{kN_i})$ is the tangent point of the line $y = kx$ tangent to E_i. Hence (C41) holds.
Now is to prove that $I_1^1 : (x_1^1, y_1^1)$, $I_1^2 : (x_1^2, y_1^2)$, $I_1^3 : (x_1^3, y_1^3)$, and O are collinear if they exist. By Theorem 3.3, for a fixed k, it holds

$$x_1^i = X_1(k)\sqrt{N_i} \Rightarrow y_1^i = \frac{N_i}{X_1(k)\sqrt{N_i}} = \frac{\sqrt{N_i}}{X_1(k)} \Rightarrow \frac{y_1^i}{x_1^i} = \frac{1}{(X_1(k))^2}$$

saying that $y = \frac{x}{(X_1(k))^2}$ passes through I_1^1, I_1^2 and I_1^3. The other cases are proved in the same way. □

With Geogebra, Figure 10 shows what Theorem 3.4 states. The figure demonstrates the case E_i and H_i have 4 intersections.

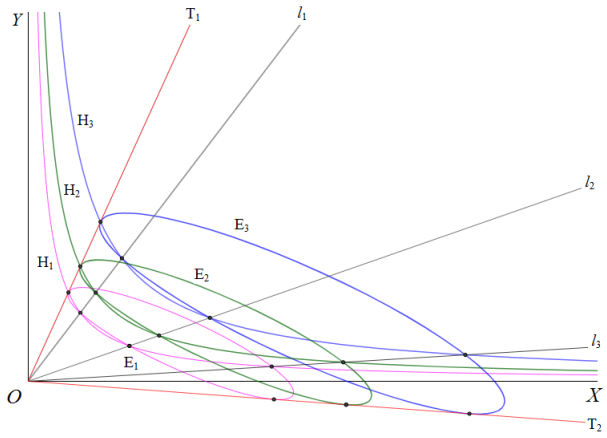


Figure 10. Collinear intersections and tangent points(Drawn with Geogebra)

3.4. **The Part of H Inside Γ.** H's intersecting Γ results in a part of H is inside Γ, as the following Theorem 3.5 describes.

Theorem 3.5. *Let Δ be that defined by (3.12); denote the intersections of Γ intersecting H by $I_0(x_0, y_0)$, $I_1(x_1, y_1)$,$I_2(x_2, y_2)$ and $I_3(x_3, y_3)$ ordered by $x_0 < x_1 < x_2 < x_3$. Then*
(C51). If $\Delta < 0$, Γ and H have 2 intersections, I_0 and I_1; the part of H between I_0 and I_1 lies inside Γ.
(C52). If $\Delta = 0$, Γ and H have 3 intersections, I_0, I_1 and I_2; the part of H between I_0 and I_1 lies inside Γ.
(C53). If $\Delta > 0$, Γ and H have 4 intersections, I_0, I_1, I_2 and I_3; the part of H between I_0 and I_1 lies inside Γ.

Proof. The first part of each statement is established in the proof of Theorem 3.2. Here merely show the second part. By statement (1) of Theorem 3.1, Γ is tangent to the line $y = kx$ at $I_0 = (\sqrt{\frac{N}{k}}, \sqrt{kN})$. The slope of the tangent line to H at I_0 is $k_H = -\frac{N}{x_0^2} = -k$, meaning H crosses into Γ at I_0 and the part between I_0 and I_1 lies inside Γ . □

4. Application to Study of Integers

Theorems 3.4 and 3.5 can have their applications in studying integers, as the following Theorems 4.1 and 4.2 state.

4.1. **Application To Integer Factorization.** By Theorem 3.4 one can see that factorization of integer $N = pq$ can be alternatively done by factoring another number $N_1 = p_1 q_1$, as the following Theorem 4.1 says.

Theorem 4.1. *Let $N = pq$ be a semiprime with $1 < p < q$ being odd primes. Assume $k = \frac{q}{p}$; then factorization of N can be done by the following steps.*
Step 1. Find a real number N_1 such that $N_1 = p_1 q_1$ with $0 < p_1 < q_1$ being real numbers and $k = \frac{q_1}{p_1}$.

Step 2. Calculate $\frac{N}{N_1} = \alpha$.
Step 3. If $p_1\sqrt{\alpha}$ *and* $q_1\sqrt{\alpha}$ *are integers, then* $p = p_1\sqrt{\alpha}$ *and* $q = q_1\sqrt{\alpha}$ *are the divisors of* N*; otherwise repeat Step 1 and Step 2 to select and calculate until the factorization is accomplished.*

Proof. Direct calculations know $p = \sqrt{\frac{N}{k}}$, $q = \sqrt{kN}$, $p_1 = \sqrt{\frac{N_1}{k}}$, and $q_1 = \sqrt{kN_1}$. Consider (p, q) is a point on the hyperbola $xy = N$ and (p_1, q_1) is a point on the hyperbola $xy = N_1$. Then by Theorem 3.4, the two points,(p, q) and (p_1, q_1), are on the line $y = kx$. Therefore the integers $p = p_1\sqrt{\alpha}$ and $q = q_1\sqrt{\alpha}$ surely satisfy $pq = \alpha p_1 q_1 = \alpha N_1 = N$. □

Remark 3. To enable Theorem 6 practicable, N_1 is selected to be a terminating decimal satisfying $\frac{N}{N_1} = \beta^2$ so that $p = p_1\beta$ and $q = q_1\beta$ can be integers. Readers can refer section 4 of Wang's paper [13] for more details.

4.2. **Application To Evaluation of Divisor Ratio.** With H and Γ, the divisor ratio can be evaluated as Theorem 4.2 states.

Theorem 4.2. *Let* H_Γ *be the part of* H *inside* Γ, $k > 1$ *be a rational number, and* $N = pq$ *be a composite integer with* $1 < p < q$ *being integers. If there is not an integer point on* H_Γ *restricted with* $1 < x \leq \sqrt{N} \leq y$*; then* $\frac{q}{p} > k$.

Proof. Consider (p, q) is an integer point on H; then it is an integer solution of the following inequalities

$$\begin{cases} xy = N \\ 1 < x \leq \sqrt{N} \leq y \\ 6\sqrt{2k}(24 + k^2)x^2 + 276\sqrt{2}k^2xy + 6\sqrt{2k}(24k^2+1)y^2 - (288(k^2+1)\sqrt{2k} + 35k^2\sqrt{k^2+1})\sqrt{N}x \\ -(288(k^2+1)\sqrt{2k} - 35\sqrt{k^2+1})k\sqrt{N}y + 144\sqrt{2}(k^2+1)^2N \leq 0 \end{cases}$$

By Theorems 3.4 and 3.5, Theorem 4.2 holds. □

5. Conclusion and Future Work

My initial motivation to define and research the ellipse (3.1) was to find a way to describe how the divisor ratio k of a semiprime N changes because my research interest has been on integer factorization. After nearly one year's study, I finished this paper. As readers can see, this paper does not achieve my initial goal because I could not obtain a good result to set up a relationship between k and N although I proved a related Theorem 4.2, which looks like something to evaluate k but is hardly applied for a big semiprime N. Fortunately, I gained Theorems 3.4 and 4.1. These two theorems enable us to convert the factorization of a big semiprime into that of a small or another big number which is easily factorized. This happened to coincident with what I had mentioned in one of my previously published paper [13]. Therefore, my future work is to develop the new method.

Acknowledgments. The research work is supported by project of Guangdong Universities Newinformation Field under No.2021ZDZX1057 and projects of Guangdong Natural Science Foundation for Basic and Applied Basic Research under No. 2022A1515140096 and No. 2022A1515140156. The authors thank them. Thanks also to Geogebra, which helps me draw excellent figures.

REFERENCES

[1] Gilda Rech Bansimba, Regis Freguin Babindamana, Basile Guy R Bossoto.(2023). A New Hyperbola based Approach to factoring Integers. arXiv:2304.07474.
doi: 10.48550/arXiv.2304.07474

[2] Crasmareanu, Mircea.(2021). Magic conics, their integer points and complementary ellipses. An Ştiinţ. Univ. Al. I. Cuza Iaşi, Ser. Nouă, Mat. 67(1): 129-148
doi:10.47743/ anstim.2021.00010

[3] Dmitry I. Khomovsky, et al. (2018). A geometric approach to integer factorization. arXiv:1802.03658.
doi: 10.48550/arXiv.1802.03658

[4] John Brillhart, Richard Blecksmith, Mike Decaro. (2016). Using Conic Sections to Factor Integers. The American Mathematical Monthly. 123 (2): 168-174.
doi: 10.4169/ amer.math.monthly.123.2.168

[5] Hong J, Jeong K, Kwon J H. (1997). Integral points on hyperbolas. Journal of the Korean Mathematical Society, 34(1):149-157.

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

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

[8] Wang, X. (2022). New Interesting Property and Application of the Rectangular Hyperbola, Journal of Advances in Mathematics and Computer Science,37(12): 1-11.
doi:10.9734/jamcs/2022/v37i121724

[9] Lawrence J Dennis. (1972). A Catalog of Special Plane Curves, Dover.

[10] Ayoub A B. (1993). The central conic sections revisited, Mathematics Magazine. 66(5): 322-325
doi:10.1080/0025570x.1993.11996157

[11] James F. Blinn.(2006). How to Solve a Cubic Equation, Part 1: The Shape of the Discriminant. IEEE Computer Graphics and Applications. 26(3): 84-93.
doi: 10.1109/MCG.2006.60

[12] Adewumi M. (2022). Solution techniques for cubic expressions and root finding. Penn State University Courseware Module . https://www.e-education.psu.edu/png520/m11_p6.html [Online; accessed 22-10-2022]

[13] Wang X. (2023). Number of Digits in Fractional Part of Arithmetic Operations of Two Terminating Decimals. Asian Research Journal of Mathematics.19(7): 47-55.
doi:10.9734/arjom/2023/v19i7678

DEPARTMENT OF MECHATRONIC ENGINEERING,FOSHAN UNIVERSITY,FOSHAN,CHINA
DEPARTMENT OF ARTIFICIAL INTELLIGENCE,GUANGZHOU COLLEGE OF APPLIED SCIENCE AND TECHNOLOGY,ZHAOQING, CHINA
E-mail address: wxbmail@msn.com; 153668@qq.com

DEPARTMENT OF MECHATRONIC ENGINEERING,FOSHAN UNIVERSITY,FOSHAN,CHINA
E-mail address: molly_917@fosu.edu.cn

DEPARTMENT OF MECHATRONIC ENGINEERING,FOSHAN UNIVERSITY,FOSHAN,CHINA
E-mail address: mjiang@fosu.edu.cn