

Triangle Conics, Cubics and Possible Applications in Cryptography

Veronika Starodub^{1,*}, Ruslan V. Skuratovskii², Sergii S. Podpriatov³

¹American University in Bulgaria, Bulgaria

²Interregional Academy of Personnel Management, Kiev and The National Technical University of Ukraine,

Igor Sikorsky Kyiv Polytechnic Institute, Ukraine

³MD, Kyiv, Ukraine

Received May 23, 2021; Revised July 20, 2021; Accepted August 21, 2021

Cite This Paper in the following Citation Styles

(a): [1] Veronika Starodub, Ruslan V. Skuratovskii, Sergii S. Podpriatov, "Triangle Conics, Cubics and Possible Applications in Cryptography," *Mathematics and Statistics*, Vol.9, No.5, pp. 749-759, 2021. DOI: 10.13189/ms.2021.090515

(b): Veronika Starodub, Ruslan V. Skuratovskii, Sergii S. Podpriatov, (2021). *Triangle Conics, Cubics and Possible Applications in Cryptography*. *Mathematics and Statistics*, 9(5), 749-759. DOI: 10.13189/ms.2021.090515

Copyright ©2021 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

Abstract We research triangle cubics and conics in classical geometry with elements of projective geometry. In recent years, N.J. Wildberger has actively dealt with this topic using an algebraic perspective. Triangle conics were also studied in detail by H.M. Cundy and C.F. Parry recently. The main task of the article is development of a method for creating curves that pass through triangle centers. During the research, it was noticed that some different triangle centers in distinct triangles coincide. The simplest example: an incenter in a base triangle is an orthocenter in an excentral triangle. This is the key for creating an algorithm. Indeed, we can match points belonging to one curve (base curve) with other points of another triangle. Therefore, we get a new fascinating geometrical object. During the research number of new triangle conics and cubics are derived, their properties in Euclidian space are considered. In addition, it is discussed corollaries of the obtained theorems in projective geometry, which proves that all of the discovered results could be transferred to the projective plane. It is well known that many modern cryptosystems can be naturally transformed into elliptic curves. We investigate the class of curves applicable in cryptography.

Keywords Triangle Cubics, Conics, Curves, Projective Geometry, Euclidian Space

1 Introduction

Centers of triangle and central triangles were studied by Clark Kimberling [1]. We considered number of curves that pass through base triangle centers, as incenter, orthocenter, circumcenter, mittenpunkt, Bevan point, and others. Namely, Jarabek, Yff, Thomson, Darboux, Lucas curves were discussed. In addition, their connection in different triangles was established, and as a result new curves were constructed. Derived curve classes include elliptic ones, as well as hyper curves, therefore, some of them could be applied in the elliptic cryptography [10]. For constructing a cryptosystem based on an elliptic curve, it is important to firstly analyze the order of a group of elliptic curve (EC) points. We provide an approach to construct Edwards curves of determined order, which are important within the cryptography and coding theory domains.

We note, that it was accepted in 1999 as an ANSI standard and in 2000 as an IEEE and NIST standard. One of the fundamental problems in EC cryptography regards the generation of cryptographically secure ECs over prime fields [18], suitable for use in various cryptographic applications. Since supersingular elliptic curves as part of one of the classes of obtained curves, are vulnerable to pairing-based attacks then we find a criterion for Edwards curve supersingularity in our previous works [11, 12]. In this work we try to improve ECDSA (Elliptic Curve Digital Signature Algorithm) by coding elliptic curve in terms of private geometrical parameters. These parameters can be used as components of private key. The part of medical modeling belongs to S. S. Podpriatov. Mathematical part of this investigation belongs to V. Starodub and R. Skuratovskii.

2 Preliminaries

Let us recall the shared secret concept.

Definition 1. Access group is a non-empty subset A of the members of the set P , who, having gathered together, have the right to recover the secret; access structure Γ will be called the non-empty set of all access groups.

There are n participants in the secret sharing protocol. Let in our case the access group consists of members that are nodes of a certain community in the block-chain. In the secret distribution algorithm, the access group consists of 9 representatives of the access structure Γ , each representative knows only one component of the secret key. In our case, these will be triangular centers, and their special belonging to the curve. The entire block chain is divided into access groups. Each access group has its own dealer who is responsible for distributing barbed components to the group. The dealer in the group, according to the Proof-of-stake (PoS) requirement, is chosen by the representative who owns such a number of tokens or, if the significance is proved, the number of cryptocurrency units on the balance sheet (significant for PoI are balances more than the specified number of units, for example, at least 10 thousand NEM); which is not less than the threshold percentage of the total number of tokens in this group. In our case, these parameters are directly the points of the curve or the points of the excentral, median or other triangles. By knowing them one of the points of the curve is uniquely restored, as well as the curve itself is uniquely defined. As known from analytical geometry, one needs to know only 9 points of a cubic (or conic) in order to unambiguously restore it. The base point of the curve can also be added to the key components. After they have gathered together with the whole group, they will be able to reconstruct the curve of its base point and check whether the ECDSA EDS was made correctly (on an elliptical curve), or, on the contrary, create a digital signature of a message created by one of the group members. Thus, this is a distributed signature using an elliptic curve, in a block chain, where only a person who owns at least a critical number of tokens from the number of tokens of the entire group has the right to sign. The principle of distributed signature in a group. Any subset with at least 9 nodes had to have a unique key for multisignature. But the right to distribute the components of the key for signing on behalf of the group also had a part of the nodes that collectively satisfy certain conditions. In the simplest case, a certain percentage of tokens from the total number of tokens of the entire group. But the main task of our research is not the application but the self-construction of the above curves.

3 Main result

Firstly, we will consider excentral triangle. Correspondence between points of the excentral and base triangles will give us significant results in developing new triangle curves. Below you may observe correspondence table between points of the base and excentral triangles. All of the above facts could be easily proved by basic principles of classical geometry [1].

Proof. Correspondence I-H. Incenter of the base triangle ABC is orthocenter of the excentral triangle $\triangle I_1I_2I_3$. Let $\triangle ABC$ be base triangle. Centers of excircles, which are tangents to BC, AC, AB , of the $\triangle ABC$ are I_1, I_2, I_3 respectively. Then $\angle CBI = \angle IBA$, because BI is bisector. Line BI_1 splits adjacent angle to the angle $\angle ABC$ in halves (exbisector). Therefore, $\angle CBI_1$ is half of the exterior angle, and $\angle CBI$ is half of the interior angle. Half of the adjacent angles sum up to 90° . Thus, I_2B is perpendicular to the I_2I_3 , so I_2B is altitude of the excentral triangle. Analogically, I_1A and I_3C are altitudes as well, therefore, I (incenter of $\triangle ABC$) is orthocenter in the excentral triangle $\triangle I_1I_2I_3$.

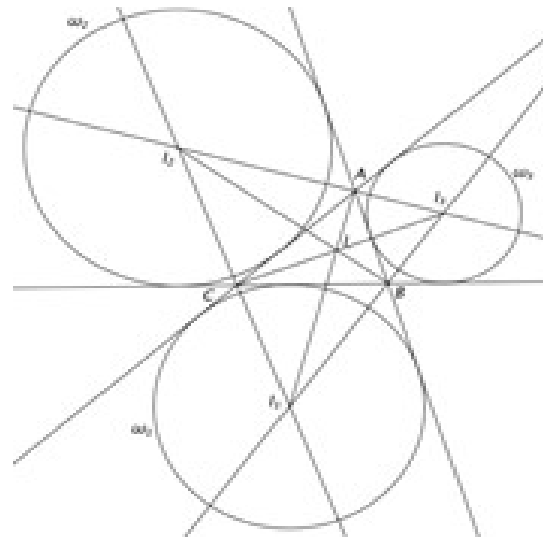


Figure 1. Correspondence $I - H$ for excentral triangle

□

Proof. Correspondence O - E. Base triangle $\triangle ABC$ is orthic for the excentral triangle. Euler circle passes through bases of the altitudes in the triangle, thus, Euler circle is circumcircle of the orthic triangle, therefore, Euler circle of the excentral triangle is circumcircle of the base triangle $\triangle ABC$. Hence, their centers coincide.

□

Proof. Correspondence Be - O. Bevan point in the triangle ABC is circumcenter in the excentral triangle $\triangle I_1I_2I_3$. Since, lines I_1A_1, I_2B_1, I_3C_1 pass through centers of the circles and tangent points of this circles to the triangle sides, I_1A_1, I_2B_1, I_3C_1 are perpendicular to the BC, AC, AB , respectively (radius is always perpendicular to the tangent). Since sides of the triangle $\triangle ABC$ are nonparallel to the sides of the excentral triangle (ABC is orthic triangle for the triangle $I_1I_2I_3$), perpendicular I_1A_1 to BC is isogonal conjugate to the perpendicular drawn from I_1 to the I_2I_3 . However, isogonal conjugate line to the altitude is line that passes through vertex and circumcenter of the triangle, it is known fact from geometry of the triangle. Similar conclusions we could make about lines I_2B_1 and I_3C_1 . Therefore, all three lines I_1A_1, I_2B_1, I_3C_1 pass through circumcenter of the triangle $\triangle I_1I_2I_3$. So we proved that Bevan point of $\triangle ABC$ is circumcenter in excentral triangle $\triangle I_1I_2I_3$.

□

Table 1. Correspondence table between points of the base and excentral triangles.

Base triangle	Excentral triangle
I (incenter)	H (orthocenter)
O (circumcenter)	E (nine-point center)
Be (Bevan point)	O (circumcenter)
Mi (mittenpunkt)	Sy (Lemoine point)
Mi' (isogonal conjugate of the mittenpunkt)	M (centroid)
Sp (Speaker point)	Ta (Taylor point)
Sy (Lemoine point)	$Sy(H_1H_2H_3)$ (Lemoine point of the orthic triangle)
Mi'' (isogonal conjugate point of the mittenpunkt with respect to the excentral triangle)	GOT (homothetic center of the orthic and tangent triangles)

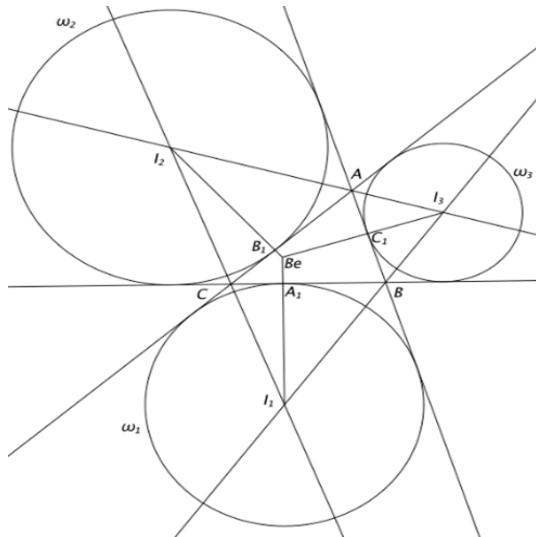


Figure 2. Correspondence $Be - O$ for excentral triangle

Proof. Correspondence $Mi - Sy$. Mittenpunkt point in $\triangle ABC$ is centroid in excentral triangle $\triangle I_1I_2I_3$. Since the lines I_1M_1, I_2M_2, I_3M_3 are straight lines that connect the centers of the circles and the midpoints of the sides of the triangle, then I_1M_1, I_2M_2, I_3M_3 are medians in the triangles I_1BC, I_2AC, I_3AB , respectively. Since the sides of the $\triangle ABC$ are antiparallel to the sides of the excentral triangle ($\triangle ABC$ is the orthic triangle for $\triangle I_1I_2I_3$), the median I_1M_1 drawn to BC is isogonal conjugate to the median drawn to I_2I_3 . It is known that a straight line isogonal conjugate to a median is the symmedian. Similarly for lines I_2M_2 and I_3M_3 . Lines I_1M_1, I_2M_2, I_3M_3 intersect at one point, that is the point of intersection of the symmedians in the excentral triangle. □

Proof. Correspondence $Sp - Ta$. The Speaker point of $\triangle ABC$ is Taylor point for the excentral triangle $\triangle I_1I_2I_3$. From vertex A we draw the perpendicular to side I_1I_3 to get the point Q , extend AQ to the intersection with BC at point P . The triangle $\triangle ABP$ is isosceles (BP is the external bisector in triangle ABC , hence the bisector of angle $\angle ABP$, since AP is perpendicular to I_1I_3, BP is height, bisector in the triangle $\triangle ABQ$), therefore BP is the median in $\triangle ABQ$, i.e. P is the middle of AQ . Similarly, the base of the perpendicular K drawn from A to side I_1I_2 is the middle of the side AT , where T is the intersection point of AK and BC . Therefore, RK is the mid-line in $\triangle AQT$. Since QT coincides with the line BC ,

PK coincides with the middle line of $\triangle ABC$. Similarly, the straight lines FW and RU , connect the bases of the perpendiculars drawn from the vertices of the original triangle to the excentral triangle sides, pass through M_1M_3 and M_1M_2 .

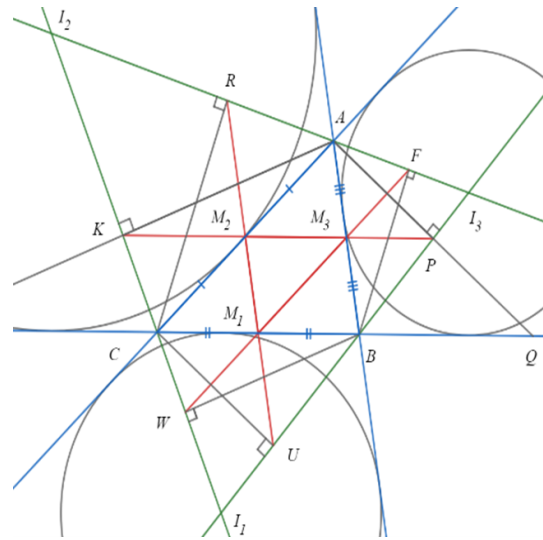


Figure 3. Correspondence $Be - O$ for excentral triangle

Shpeaker point for $\triangle ABC$ is the center of the inscribed circle in $\triangle M_1M_2M_3$, and the Taylor point for the excentral triangle is the center of the circle passing through the points R, F, P, U, W, K . Let us prove that the centers of these circles coincide. Draw the bisector perpendicular to the segment RF . It is parallel to the lines BF and CR , therefore, by the Thales theorem, it passes through the middle of the side $BC \ni M_1$. Then we can conclude that $\triangle RM_1F$ is an isosceles triangle. Then the middle perpendicular to RF coincides with the bisector of the angle $\angle RM_1F$. Similarly, the middle perpendicular to UP and to WK coincides with the bisectors of the angles $\angle UM_2P, \angle KM_3W$. Therefore, the intersection point of the bisectors of the triangle $\triangle M_1M_2M_3$ coincides with the intersection point of the middle perpendiculars to the segments RF, UP, WK , i.e. with the center of the circumscribed circle around the hexagon $RFPUWK$. □

Proof. Correspondence $Sy - Sy(H_1H_2H_3)$. The Lemoine point in the ABC triangle coincides with Lemoine point for the orthic triangle of the excentral triangle. Since the original ABC triangle is orthic for excentral, the above statement is valid.

Proof. Correspondence $Mi'' - GOT$. The isogonally conjugate point to the point Mittenpunkt, in the base triangle, with respect to the excentral triangle is homotetic center of the orthic and tangential triangle in excentral triangle. For the excentral triangle orthic triangle is simply base triangle, as was proved above. Tangential triangle for excentral triangle is triangle with parallel sides to the sides of the base triangle, which are drawn through excenters. Therefore, GOT is point of intersection of lines drawn through vertices of the base triangle and tangential triangle to the excentral triangle. Mittenpunkt is the point of intersection of the points that pass through vertices of the excentral triangle and through middles of the base triangle. Due to antiparallelity of the sides of the excentral and base triangle, and homotetic properties of the tangential and base triangles, isogonal conjugacy of the Mittenpunkt and GOT , which respect to the excentral triangle, is obvious.

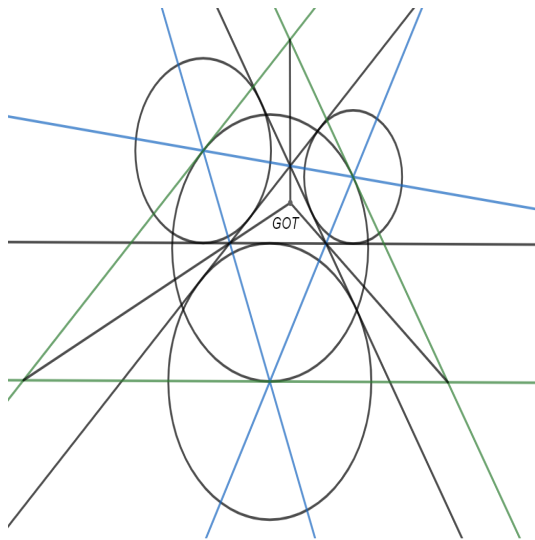


Figure 4. Correspondence $Mi'' - GOT$ for excentral triangle

Hence, we may apply derived results for creating new triangle cubics and conics. Firstly Jerabek hyperbola was considered.

Definition 2. Jerabek hyperbola is a curve that passes through vertices of triangle, circumcenter, orthocenter, Lemoine point, isogonal conjugate of the de Longchamps point [5].

We may observe that Jerabek hyperbola for the excentral triangle has number of points that correspond to other ones in the base triangle. The study of such matches gave us significant results.

Therefore, we got new triangle hyperbola 5 that passes through centers of the excircles, Bevan point, incenter, mittenpunkt and de Longchamps point. It is still rectangular as Jerabek hyperbola is. Known fact about Jerabek hyperbola is that its center is center of the Euler circle. However, Euler circle of the excentral triangle is circumscribed circle for the base triangle. In addition, Jerabek Hyperbola is the isogonal

conjugate to the Euler line. Meanwhile, Euler line for the excentral triangle is line $(I$ (incenter), O (circumcenter), Be (Bevan point), Mi' (isogonal conjugate for the mittenpunkt with respect to the extriangle), Mi'' (isogonal conjugate for the mittenpunkt with respect to the base triangle)). Therefore, we can conclude, that our new hyperbola is isogonal conjugate to the line (I, O, Be, Mi', Mi'') and its center is the circumcenter.

Theorem 1. New hyperbola passes through excenters, Bevan point, incenter, mittenpunkt, de Longchamps point. It is isogonal conjugate to the line (I, O, Be, Mi', Mi'') , and its center is circumcircle.

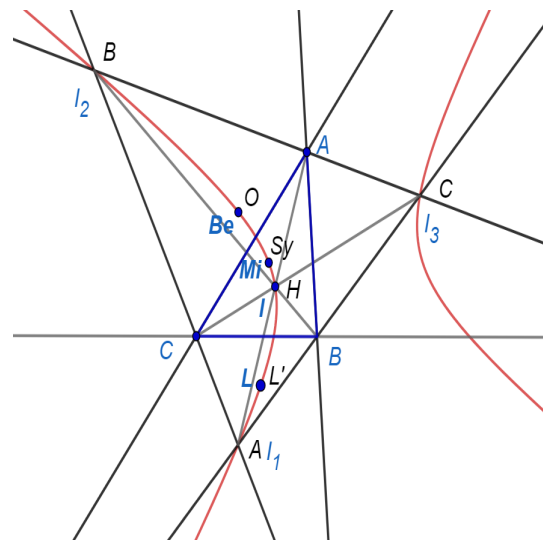


Figure 5. New triangle conic based on Jerabek hyperbola for the excentral triangle

If we consider in the triangle under Jerabek hyperbola on Fig. 5 domain bounded by A, H, C, O, B, C , where point C has blue color, then it can be contracted under the uniform deformation of hyperbola. Then we identify the area of the triangle between A, H, S, O, B , in modeling with missing skin area as a result of damage and surgical removal.

As line of skin fixation before stretching, we can choose the sides BC, CA of the triangle, where the letters B, C, A are black. Therefore, with directional deformation, the above region can be tightened by an implicit skin between the Jerabek hyperbola and a part of the triangle A, H, S, O, B, C , where point C has black color on Fig. 5.

Similarly we studied Thomson cubic [20] for the base triangle and matched its points with ones in the excentral triangle.

Definition 3. Thomson cubic is a curve that passes through vertices of the triangle, middles of the triangle sides, centers of the excircles, incenter, centroid, circumcenter, Lemoine point, mittenpunkt, isogonal conjugate of the mittenpunkt [1].

By applying correspondence table between points of the base and excentral triangles 1 to the points of Thomson cubic we obtain a new triangle cubic.

According to the table, we got new cubic.

Theorem 2. New triangle cubic 6 passes through vertices of the triangle, bases of the altitudes, middles of the triangle sides

Table 2. Matching points for Jerabek hyperbola.

Jerabek hyperbola for excentral triangle	New hyperbola for the base triangle
A, B, C (vertices of the base triangle)	I_1, I_2, I_3 (excenters)
O (circumcenter)	Be (Bevan point)
H (orthocenter)	I (incenter)
Sy (Lemoine point)	Mi (mittenpunkt)
L' (isogonal conjugate of the de Longchamps point)	L (de Longchamps point)

Table 3. Mtaching points for Thomson cubic.

Thomson cubic for the base triangle	New cubic for the excentral triangle
A, B, C (vertices of the base triangle)	H_1, H_2, H_3 (bases of the altitudes)
M_a, M_b, M_c (middles of the base triangle sides)	M_{ha}, M_{hb}, M_{hc} (middles of orthic triangle's sides)
I_1, I_2, I_3 (excenters)	A, B, C (vertices)
I (incenter)	H (orthocenter)
M (centroid)	$M(H_1H_2H_3)$ (centroid in the orthic triangle)
O (circumcenter)	E (nine-point center)
Sy (Lemoine point)	$Sy(H_1H_2H_3)$ (Lemoine point of the orthic triangle)
Mi (mittenpunkt)	Sy (Lemoine point)
Mi'' (isogonal conjugate of the mittenpunkt with respect to the excentral triangle)	GOT (gomotetic center of the orthic and tangent triangles)

in the orthic triangle, orthocenter; Euler point, centroid in orthic triangle, Lemoine point, and gomotetic center of the orthic and tangent triangles.

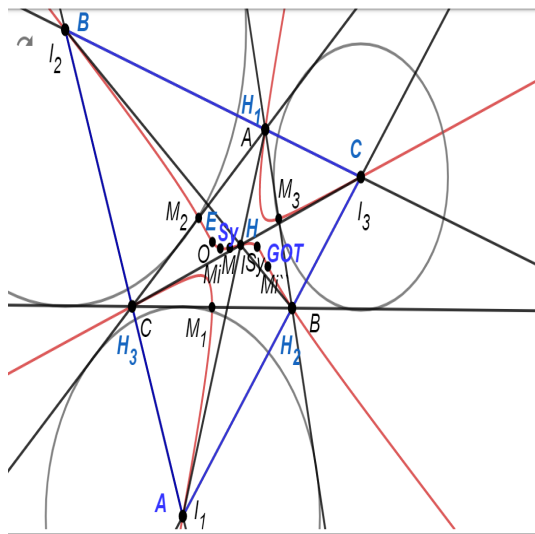


Figure 6. New triangle conic based on Thomson hyperbola for the excentral triangle

Analogically new triangle cubic based on the Darboux cubic and correspondence of its points with triangle centers in the excentral triangle was derived.

Definition 4. Darboux cubic is a curve that passes through vertices of the triangle, centers of the excircles, incenter, circumcenter, Bevan point [3].

Triangle centers of the Darboux cubic in the base triangle were matched with points in the excentral triangle.

Theorem 3. Therefore, we got a new cubic 7 that passes through vertices of the triangle, bases of the altitudes, orthocenter, Euler center, and circumcenter.

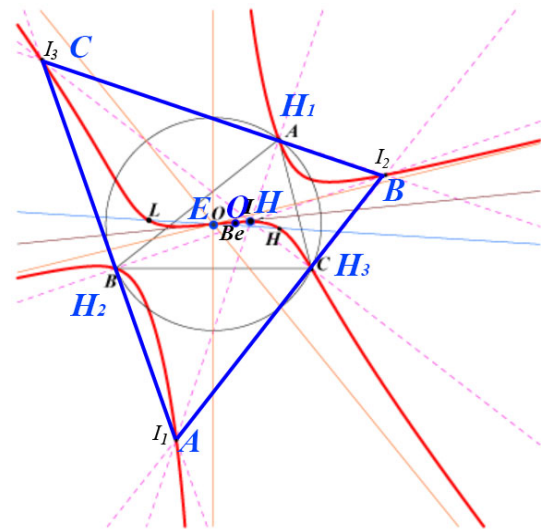


Figure 7. New triangle conic based on Darboux cubic for the base triangle in correspondence with excentral triangle

The discussed above results were obtained from considering excentral triangle, its triangle centers and correspondence between points in the excentral and basic triangle. As a result, were derived three new triangle curves that were not discovered before. However, to get wider results were applied the same idea to other triangles. Namely, medial triangle was consider. In the same way as before, was proven the fact that some points in the medial triangle match with some points in the base triangle [1].

Definition 5. Medial triangle is a triangle with vertices in the middles of the base triangle sides.

Proof. Correspondence $I - Sp$. Speaker point is an incenter in the median triangle by the definition. \square

Table 4. Matching points for Darboux cubic.

Darboux cubic for the base triangle	New cubic for the excentral triangle
A, B, C (vertices of the base triangle)	H_1, H_2, H_3 (bases of the altitudes)
I_1, I_2, I_3 (excenters)	A, B, C (vertices)
I (incenter)	H (orthocenter)
O (circumcenter)	E (nine-point center)
Be (Bevan point)	O (circumcenter)

Table 5. Correspondence table between points of the medial and base triangles.

Points in the medial triangle	Point in the base triangle
I (incenter)	Sp (Speaker point)
M (centroid)	M (centroid)
O (circumcenter)	E (nine-point center)
H (orthocenter)	O (circumcenter)
L (de Longchamps point)	H (orthocenter)
Be (Bevan point)	$Be(M_1M_2M_3)$ (Bevan point of the medial triangle)
Na (Nagel point)	I (incenter)
G (Gergonne point)	Mi (mittenpunkt)
Sy_A (Lemoine point of the anticomplementary triangle)	Sy (Lemoine point)
B_3 (third Brocard point)	M_B (Brocard midpoint)

Proof. Correspondence $M - M$. The centroid in the base triangle coincide with the centroid in the median triangle. The centroid of any triangle is its center of mass. Since the vertices of the median triangle are in the middle of the sides of the base, their centers of mass must coincide. Therefore, their centroids coincide. \square

Proof. Correspondence $O - E$. Circumcenter of the medial triangle is the center of the Euler circle in the base triangle. The Euler circle passes through the bases of the medians of the triangle, which means that the Euler circle is the circumscribed circle of the median triangle. Therefore, the circumcenter of the median triangle is the center of the Euler circle of the base triangle. \square

Proof. Correspondence $H - O$. The orthocenter of the medial triangle is the circumcenter of the base triangle. The altitude in the median triangle is the middle perpendicular to the side of the base triangle. Since it is drawn from the middle of the side and perpendicular to the base (perpendicular to the side of the median triangle, which is parallel to the side of the base triangle). Therefore, the point of intersection of the altitudes of the median triangle is the point of intersection of the middle perpendiculars of the base triangle, and therefore it is the center of its circumscribed circle. \square

Proof. Correspondence $L - H$. De Longchamps point in the medial triangle is orthocenter in the base triangle. By the definition of de Longchamps point is a point that is symmetric to the orthocenter with respect to the circumcircle. The orthocenter of the median triangle is the circumcenter of the base triangle, as was proved above, and the circumcenter of the median triangle is the center of the Euler circle. Due to the properties of the Euler line, the fact that the circumcenter is symmetric to the orthocenter with respect to the Euler center, we can conclude that de Longchamps is the point of the median triangle and is the orthocenter in the base triangle. \square

Proof. Correspondence $Be - Be(M_1M_2M_3)$. The correspondence is straight forward from the definition. \square

Proof. Correspondence $Na - I$. Nagel point in the medial triangle is incenter in the base triangle. Given parallelogram $ABCD$ below, M and N are located such that $AM = CN$. Prove that DQ bisects angle D of the parallelogram.

First we extend CM and DA to intersect at point Z as shown below.

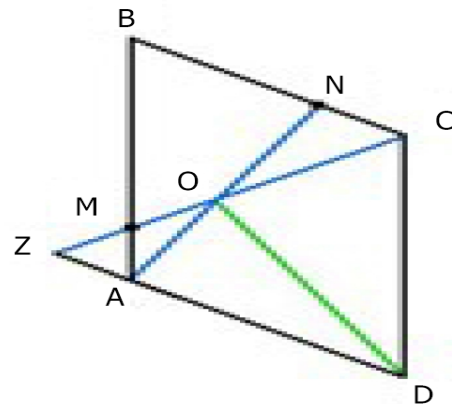


Figure 8. Correspondence $Na - I$ for medial triangle (a)

Since BC and DZ are parallel, angles Z and ZCB are congruent. The vertical angles at Q make triangle AZQ similar to triangle NCQ . Furthermore, since AB and DC are parallel, triangle AZM is obviously similar to $\triangle DZC$. The first similarity gives the first equality below; the stated condition that $AM = NC$ gives the second, and the second similarity gives the third:

$$\frac{ZQ}{QC} = \frac{AZ}{NC} = \frac{AZ}{AM} = \frac{DZ}{DC} \tag{1}$$

Thus consider point Q in triangle DZC . Q divides CZ in the same ratio as the other two sides of that triangle precisely the configuration for the angle bisector theorem. Since only one point on the segment CZ can have that property, the angle bisector theorem guarantees that DQ bisects angle D of the parallelogram, which is what we wanted to prove. To prove that Nagel point of the medial triangle is the incenter of the base one, we first reveal a larger diagram (in red below) that includes the original problem:

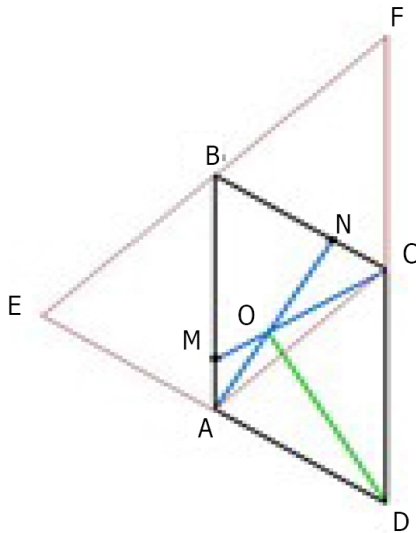


Figure 9. Correspondence $N_a - I$ for medial triangle (b)

Consider triangle ABC as the original triangle, with three parallelograms ($ABCD$, $ABFC$, $ACBE$) built around it. This makes triangle DEF anticomplementary triangle of ABC , or, we can state equivalently with different vocabulary, ABC is the medial triangle of DEF . Now let M and N are the points halfway around the perimeter of ABC from C and A , respectively. Then $AM = CN$ (both are the semi-perimeter of ABC minus side AC), and the theorem above applies, and thus DQ is an angle bisector of $\triangle DEF$. This proof could, of course, be repeated for any of the three vertices of DEF . But when M and N are semi-perimeter points in $\triangle ABC$, then Q is the Nagel point. And since Q lies on the angle bisectors of DEF , it is the incenter of that triangle. Thus, we have the result we were seeking for: the incenter of a triangle is also the Nagel point of its medial triangle. \square

Proof. Correspondence $G - Mi$. Gergonne point in the medial triangle is mittenpunkt for the base triangle. Line that passes through the center of the excircle and middle of the side of the triangle coincide with the line that passes through the middle of the triangle side and tangent point of the inscribed circle in the medial triangle, due to the triangle similarity. Intersection of this lines is mittenpunkt for the base triangle and Gergonne point for the medial triangle, respectively. Since, these lines coincide, this triangle centers coincide as well. \square

Proof. Correspondence $Sy_A - Sy$. Lemoine point of the anticomplementary triangle is Lemoine point of the medial triangle. \square

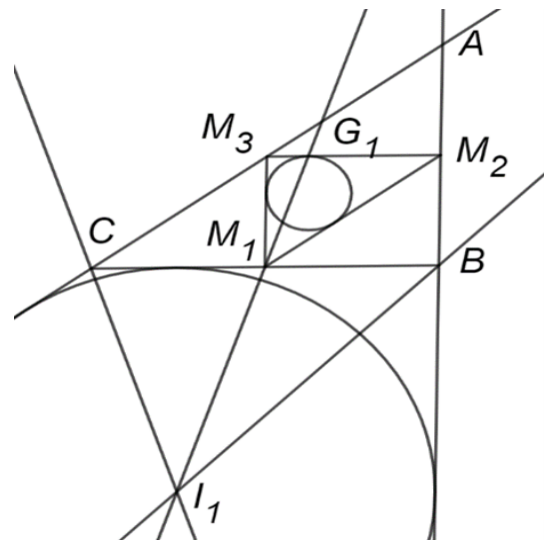


Figure 10. Correspondence G_{Mi} for medial triangle

By the definition anticomplementary triangle for the medial triangle is the base triangle. Therefore, the fact does not need a proof. \square

Definition 6. *Yff hyperbola is a triangle curve that passes through centroid, orthocenter, circumcenter, and Euler center.*

We have considered Yff hyperbola for the base triangle and matched its point with triangle centers of the medial triangle, applying correspondence table.

We got a new conic that has vertices in the centroid and de Longchaps point, focus in the orthocenter. Directrix of the Yff hyperbola is perpendicular to the Euler line and passes through center of the Euler circle. Euler line for the medial and base triangles coincide. However, center of the Euler circle of the base triangle is circumcenter for the medial. Therefore, directrix of the new hyperbola is perpendicular to the Euler line and passes through circumcenter.

Theorem 4. *New conic I_1 is a curve that has vertices in the centroid and de Longchaps point, focus in the orthocenter. Directrix of the new hyperbola is perpendicular to the Euler line and passes through its circumcenter.*

Let's go further in our research and create more triangle curves with the help of correspondences between triangle centers in medial and base triangles.

We observed the transformation of the Darboux cubic under the correspondence. It led us to a new cubic.

Theorem 5. *We got new cubic I_2 that passes through Speaker point, center of the Euler circle, circumcenter, orthocenter, complementary conjugate of the orthocenter, middles of the triangle side, and antipodes of the medial triangle.*

Similarly, we may take Lucas cubic for the base cubic and match it with points of the medial triangle.

Definition 7. *Lucas cubic is a curve that passes through triangle vertices, orthocenter, Gergone point, centroid, Nagel point, Lemoine point of the anticomplementary triangle, and vertices of th anticomplementary triangle.*

Table 6. Matching points for the Yff hyperbola and medial triangle.

Yff hyperbola for the base triangle	New hyperbola for the medial triangle
M (centroid)	M (centroid)
H (orthocenter)	L (de Longchaps point)
O (circumcenter)	H (orthocenter)
E (nine-point center)	O (circumcenter)

Table 7. Matching points for the Darboux cubic and medial triangle.

Darboux cubic for the medial triangle	New cubic for the base triangle
A, B, C (triangle vertices)	M_1, M_2, M_3 (middles of the triangle sides)
A_1, B_2, C_3 (antipods of the triangle)	Antipods of the medial triangle
I (incenter)	Sp (Speaker point)
O (circumcenter)	E (nine-point center)
H (orthocenter)	O (circumcenter)
L (de Longchaps point)	H (orthocenter)
L' (isogonal conjugate of the de Longchaps point)	H_A (complementary conjugate of the orthocnter)

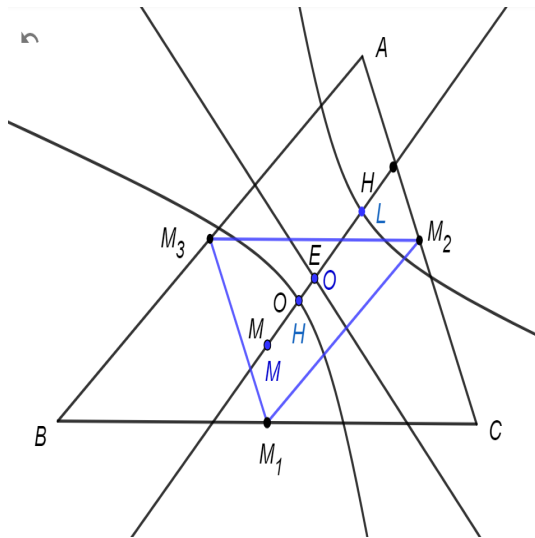


Figure 11. New conic based on Yff hyperbola

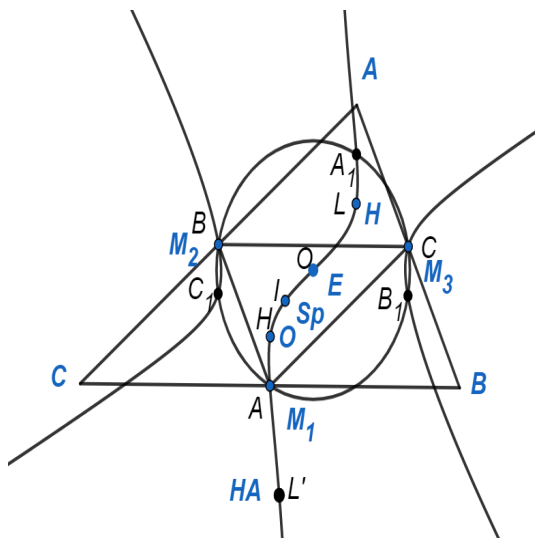


Figure 12. New cubic based on Darboux cubic for the medial triangle

We make the correspondence between points of the Lucas cubic in the medial triangle with triangle centers in the base triangle. As a result we obtain the following table.

Theorem 6. *New cubic 13 that passes through Lemoine point, centroid, circumcenter, mittenpunkt, incenter, orthocenter, triangle vertices, and middles of the triangle sides.*

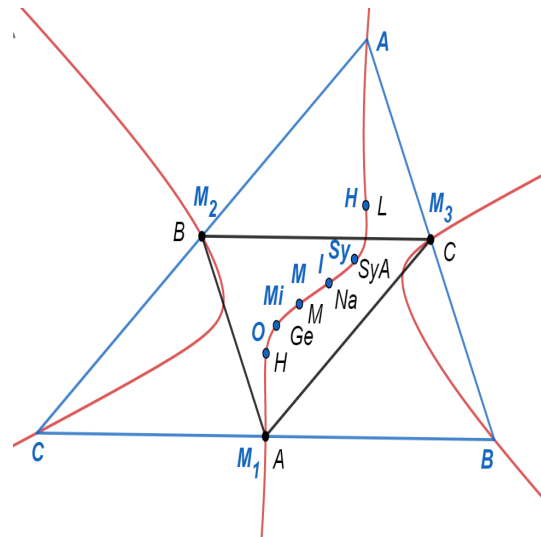


Figure 13. New cubic based on Lucas cubic for the medial triangle

Therefore, while we were applying correspondence method to the medial triangle we derived one new conic and two new cubics. In addition, we observed Euler and mid-arc triangles as correspondence base, one can also consider application of the derived method on other triangle constructions.

Definition 8. *Euler triangle is triangle with vertices in the intersection points of the triangle altitudes and the nine-point circle.*

Definition 9. *Mid-arc triangle is a triangle with vertices in the middles of the arcs of the circumcircle.*

Let's firstly consider correspondence of points between Euler and base triangles.

Table 8. Mtaching points for the Lucas cubic and medial triangle.

Lucas cubic for the medial triangle	New cubic for the base triangle
Sy_A (Lemoine point of the anticomplementary triangle)	Si (Lemoine point)
M (centroid)	M (centroid)
H (orthocenter)	O (circumcenter)
Ge (Gergonne point)	Mi (mittenpunkt)
Na (Nagel point)	I (incenter)
L (de Longchamps point)	H (orthocenter)

Table 9. Correspondence table between points in the Euler and base triangles.

Points in the Euler triangle	Points in the base triangle
I (incenter)	M_{IH} (midpoint of incener and orthocenter)
M (centroid)	M_{MH} (midpoint of centroid and orthocenter)
O (circumcenter)	E (nine-point center)
H (orthocenter)	H (orthocenter)
N (Nagel point)	F (Furhman point)
L (de Longchamps point)	O (circumcenter)

According to the above table we have built the correspondence between points of the Darboux cubic for the Euler triangle and triangle centers of the base triangle.

Theorem 7. *New cubic 14 passes through circumcenter, orthocenter, Euler center, midpoint of the incenter and the orthocenter, vertices of the Euler triangle and middles of the triangle sides.*

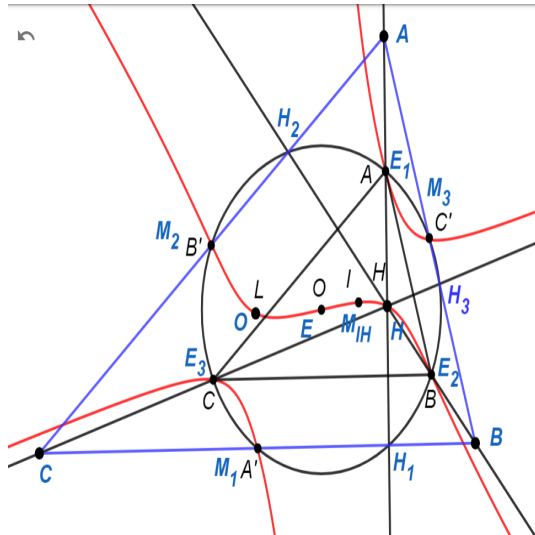


Figure 14. New cubic based on Darboux cubic in the Euler triangle

Finally, we observe correspondence of triangle centers between mid-arc and base triangle.

Based on the correspondence between point of the mid-arc and base triangles we discovered new cubic which is based on Jerabek hyperbola.

Theorem 8. *New conic fig. 15 is rectangular and passes through circumcenter, incenter, midpoint of mittenpunkt and incenter, Schiffler point, and isogonal conjugate point to the Bevan point.*

Therefore, during the research of the triangle curves were derived three new triangle conics and five new triangle cubics.

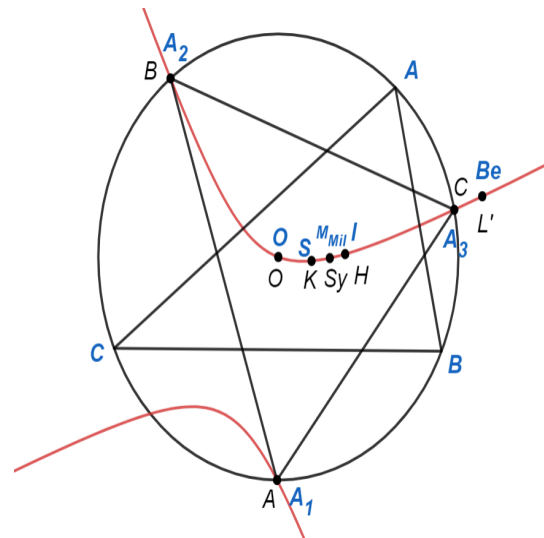


Figure 15. New conic based on the Jerabek hyperbola for the mid-arc triangle

This is a significant result and leaves a room for new investigations.

Since, geometry of conic sections and other triangle curves are broadly used in the projective geometry we looked on the obtained result through the prism of the projective geometry.

According to the Pascal's theorem if six arbitrary points are chosen on a conic and joined by line segments in any order to form a hexagon, then the three pairs of opposite sides of the hexagon meet at three points that belong to a straight line.

Let's consider the first derived triangle curve based on Jerabek hyperbola for the excentral triangle. New hyperbola passes though excenters, Bevan point, incenter, mittenpunkt, de Longchamps point. We built a hexagon with verices in the given triangle centers and apply Pascal's theorem.

Let I_1, I_2 be excenters, and Be, Mi, L be Bevan point, Mi mittenpunkt, de Longchamps point, respectively. We get the following results:

Corollary 1. *Concurrent points of I_2Be and $LI, BeMi$ and I_1L, MiI and I_2I_1 belong to one line.*

Corollary 2. *Concurrent points of segments I_2Mi and $BeI_1,$*

Table 10. Matching points for the Darboux cubic and Euler triangle.

Darboux cubic in the Euler triangle	New cubic for the base triangle
A, B, C (vertices)	E_1, E_2, E_3 (vertices of the Euler triangle)
A', B', C' (antipodes of the triangle vertices)	M_1, M_2, M_3 (middles of the triangle sides)
I (incenter)	M_{IH} (midpoint of incenter and orthocenter)
O (circumcenter)	E (nine-point center)
H (orthocenter)	H (orthocenter)
L (de Longchamps point)	O (circumcenter)

Table 11. Correspondence table between points in the mid-arc and base triangles.

Points for the mid-arc triangle	Points for the base triangle
O (circumcenter)	O (circumcenter)
H (orthocenter)	I (incenter)
S_y (Lemoine center)	M_{MiI} (midpoint of mittenpunkt and incenter)
L (de Longchamps point)	Be (Bevan point)
K (Kosnita point)	S (Schiffler point)

BeL and II_2 , MiL and II_2 lie on one line.

Similarly, we have applied the same idea for the hexagon inscribed in the new hyperbola derived from the Jerabek hyperbola for the mid-arc triangle.

Let A_2, A_3 be middles of the arcs of the circumcircle, and Be, I, S, O be Bevan point, incenter, Speaker point, circumcenter, respectively. The following facts were discovered:

Corollary 3. *Points of intersection of lines A_2Be and SI, IA_3 and OA_2, BeA_3 and OS belong to one line.*

Corollary 4. *Points of intersection of line segments BeO and A_3A_2, BeS and IA_2, A_3S and IA_2 belong to a straight line.*

Moreover, the combination of two of the discovered triangle cubics gives us significant results as well. Let's consider new cubic derived from the Darboux cubic for the excentral triangle and new cubic constructed with the base on Darboux cubic with respect to the medial triangle. The first mentioned new cubic passes through bases of altitudes, vertices, orthocenter, nine-point center, circumcenter, let's name it $P(x, y)$. The second mentioned new cubic passes through middles of the triangle sides, Speaker point, nine-point center, circumcenter, orthocenter, let's name it $Q(x, y)$. We may notice that this two cubics pass through three common points, that are nine-point center, circumcenter and orthocenter. Moreover, this three points belong to Euler line, let it has an equation $ax + by + c = 0$. Since, we have two cubics which pass through points which belong to one line, there exists such integer t such that the following holds: $P(x, y) - tQ(x, y) : ax + by + c$. Therefore, Euler line is linear component of the composition of two new cubics. In addition, points of intersection of the linear component with the curve are inflection points [4, 7, 23].

Corollary 5. *Euler line is a linear component of the composition of new triangle cubic (passes through bases of altitudes, vertices, orthocenter, nine-point center, circumcenter) and new triangle cubic (passes through middles of the triangle sides, Speaker point, nine-point center, circumcenter, orthocenter). Moreover, orthocenter, circumcenter, and nine-point center are inflection point of the composition of these two curves.*

The above corollaries prove that the discovered in the research new triangle curves could be applied in different geometric areas and studied in advanced.

Remark 1. *A further continue of our research consists in the same analysis of singularities as provided by second author in [6, 17, 13, 23] for cubic obtained by us in the presented work.*

4 Discussions

The method we have proposed, significantly simplifies creation the curves that pass through triangular centers. Beyond that, our projective method opens up a number of 3D possibilities, as well as for graphic, as for natural biologic objects too. To get the right answer, we have to distinguish the new curves topological nature and its properties according to different objects and fields.

5 Conclusions

During the research were discovered three new triangle conics and five new triangle cubics, what is very significant result for the classical geometry. In addition, was shown that proceedings of the study could be applied not only in Euclidian space, but in projective as well. Moreover, as was shown in the introduction part, each curve and assigned to it triangle centers may be applied in cryptography as a set of secret keys. However, the main result of the research was developed the method of deriving new triangle curves. This opens an opportunity for creating more triangle curves, while applying the method for various triangles, points, and geometric constructions.

The developed idea significantly simplifies the question of creating curves passing through triangular centers [22]. However, it opens up a number of new questions. Which interesting properties do new curves have? What is the topological nature of these transformations? Is it possible to apply a similar idea to non-Euclidean objects? Could one use the same method over an arbitrary finite field? Can this idea be further generalized?

Table 12. Matching points for the Jerabek hyperbola and Euler triangle.

Jerabek hyperbola for mid-arc triangle	New hyperbola for the base triangle
A, B, C (vertices)	A_1, A_2, A_3 (middles of the arcs of the circumcircle)
O (circumcenter)	O (circumcenter)
H (orthocenter)	I (incenter)
Sy (Lemoine point)	M_{MI} (midpoint of mitterpunkt and incenter)
K (Kosnita point)	S (Schiffler point)
L' (isogonal conjugate of the de Longchamps point)	Be' (isogonal conjugate of the Bevan point)

REFERENCES

- [1] C. Kimberling. Triangle centers and central triangles, Utilitas Mathematica, 1998.
- [2] N. J. Wildberger. Neuberg cubics over finite fields. Algebraic Geometry and its Applications, Vol.5, 488-504, 2008.
- [3] H. M. Cundy, C. F. Parry. Some cubic curves associated with triangle. Journal of Geometry, Vol.53, 41-66, 2000.
- [4] R. J. Walker. Algebraic Curves, Springer-Verlag, New York, 1978.
- [5] G. M. Pinkernell. Cubic Curves in the Triangle Plane, J. Geom, Vol.55, 141-161, 1996.
- [6] Y. A. Drozd, R. V. Skuratovskii. Cubic Rings and Their Ideals, Ukrainskyi Matematychnyi Zhurnal, Vol.62, No.4, 464, 2010.
- [7] W. Fulton. Algebraic curves. An introduction to algebraic geometry. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series. W. A. Benjamin, Inc., New York, 1969.
- [8] R. V. Skuratovskii, A. Williams. Irreducible bases and subgroups of a wreath product in applying to diffeomorphism groups acting on the Mebius band, Rend. Circ. Mat. Palermo, Series 2, 2020.
- [9] R. V. Skuratovskii. On commutator subgroups of Sylow 2-subgroups of the alternating group, and the commutator width in wreath products, European Journal of Mathematics, Vol.7, 353-373, 2021.
- [10] R. V. Skuratovskii. Employment of Minimal Generating Sets and Structure of Sylow 2-Subgroups Alternating Groups in Block Ciphers, Advances in Computer Communication and Computational Sciences, Springer, 351-364, 2019.
- [11] R. V. Skuratovskii, V. Osadchyy. The Order of Edwards and Montgomery Curves, WSEAS Transactions on Mathematics, Vol.19, 253-264, 2020. DOI: 10.37394/23206.2020.19.25
- [12] D. Moody, D. Shumow. Analogues of Velu's formulas for isogenies on alternate models of elliptic curves, Math. Computation, Vol.85, No.300, 1929-1951, 2015.
- [13] S. Pogodayev. Marketing of works as a source of the new hybrid offerings in widened marketing of goods, Journal of Business & Industrial Marketing, Vol. 28, No.8, 2013.
- [14] R. V. Skuratovskii, A. Williams. A solution of the inverse problem to doubling of twisted Edwards curve point over finite field, Processing, transmission and security of information, Vol.2, Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej w Bielsku-Bialej, 2019.
- [15] R. V. Skuratovskii, A. Williams. Irreducible bases and subgroups of a wreath product in applying to diffeomorphism groups acting on the Mobius band, Rendiconti del Circolo Matematico di Palermo Series 2, 1-19, 2020.
- [16] R. V. Skuratovskii. Generating set of wreath product with non faithful action, International Journal of Analysis and Applications, Vol.18, No.1, 104-116, 2020.
- [17] R. V. Skuratovskii, V. Osadchyy. Order of Edwards and Elliptic Curves Over Finite Field, WSEAS Transactions on Mathematics, Vol.19, 253-264, 2020.
- [18] R. Popovych, R. Skuratovskii. Normal high order elements in finite field extensions based on the cyclotomic polynomials, Algebra and Discrete Mathematics, Vol.29, No.2, 241-248, 2020.
- [19] A. V. Akopyan, A. A. Zaslavsky. Geometry of conics, volume 26 of Mathematical World, American Mathematical Society, Providence, RI, 2007.
- [20] F. Lang. Geometry and Group Structures of Some Cubics, Forum Geometricorum ISSN 1534-1178, Vol.2, 135-146, 2002.
- [21] N. Abdigappar, P. Hamid. On the Geometry of Hamiltonian Symmetries, Mathematics and Statistics, Vol.8, No.3, 293-298.
- [22] Z. Burinska, K. Runovski, H. Schmeisser. On the approximation by generalized sampling series in l_p - metrics, Sampling Theory in Signal and Image Processing, Vol.5, No.1, 59-87, 2006.
- [23] R. V. Skuratovskii. The derived subgroups of sylow 2-subgroups of the alternating group, commutator width of wreath product of groups, Mathematics, Vol.8, No.4, 472, 2020.