

**TWO AND THREE DESCENT FOR ELLIPTIC
CURVES ASSOCIATED WITH PERFECT CUBOIDS.**

JOHN RAMSDEN, RUSLAN SHARIPOV

ABSTRACT. A rational perfect cuboid is a rectangular parallelepiped whose edges and face diagonals are given by rational numbers and whose space diagonal is equal to unity. Recently it was shown that the Diophantine equations describing such a cuboid lead to a couple of parametric families of elliptic curves. Two and three descent methods for calculating their ranks are discussed in the present paper. The elliptic curves in each parametric family are subdivided into two subsets admitting 2-descent and 3-descent methods respectively.

1. INTRODUCTION.

Omitting the historical background of the problem, which can be found in [1], we proceed directly to elliptic curves in question. They are given by the equations

$$2(w^2 - 1) = P_1 \alpha^3, \quad 2(w^2 - 1) = P_2 \alpha^3 \quad (1.1)$$

with respect to the variables w and α . The rational coefficients P_1 and P_2 in the equations (1.1) depend on two rational parameters b and c :

$$\begin{aligned} P_1 = & \frac{1}{2} (7812 b^4 c^4 - 216 b^2 c^4 - 52 b^2 c^3 + 1764 b^3 c^4 - 1200 b^4 c^3 - \\ & - 1848 b^4 c^2 + 720 b^4 c - 36 c^4 b - 1512 b^3 c^3 - 36 c^8 b^3 + 288 b^3 c^2 - \\ & - 108 c^6 b^2 + 380 c^5 b^2 + 378 c^7 b^3 - 231 c^8 b^4 - 300 c^7 b^4 + 3906 c^6 b^4 - \\ & - 13 c^7 b^2 - 8904 c^5 b^4 - 882 c^6 b^3 + 18 c^6 b - 1319 b^6 c^8 + 20952 b^5 c^3 - \\ & - 11952 b^5 c^2 + 2592 b^5 c - 48372 b^6 c^4 + 31620 b^6 c^3 - 10552 b^6 c^2 + \\ & + 816 b^6 c + 1494 b^5 c^8 - 5238 b^5 c^7 - 4 c^5 + 7905 b^6 c^7 - 24186 b^6 c^6 + \\ & + 288 b^6 + 43740 b^6 c^5 + 7686 b^5 c^6 + 576 b^7 + 128 b^8 - 15372 b^5 c^4 - \\ & - 1080 b^7 c^8 - 3546 b^7 c^6 + 51 c^9 b^6 + 400 b^8 c^8 - 162 c^9 b^5 + 8640 b^7 c^2 - \\ & - 3456 b^7 c + 2808 b^7 c^7 - 1560 b^8 c^7 + 3940 b^8 c^6 + 216 c^9 b^7 - 960 b^8 c - \\ & - 6240 b^8 c^3 + 9 c^{10} b^6 + 7880 b^8 c^4 + 4 c^{10} b^8 - 6732 b^8 c^5 + 45 c^9 b^4 + \\ & + 3200 b^8 c^2 - 11232 b^7 c^3 + 7092 b^7 c^4 - 18 c^{10} b^7 - 60 c^9 b^8) \times \\ & \times (b^2 c^4 - 6 b^2 c^3 + 13 b^2 c^2 - 12 b^2 c + 4 b^2 + c^2)^{-1}, \end{aligned} \quad (1.2)$$

2000 *Mathematics Subject Classification.* 11G05, 14H52, 11D25, 11D72.

$$\begin{aligned}
P_2 = \frac{b}{2} & (832b^2c^2 - 1440b^2c^4 - 840b^2c^3 + 4788b^3c^4 + 396bc^3 + \\
& + 720b^3c + 808b^4c^4 + 3032b^4c^3 - 2576b^4c^2 - 96b^4c + 448b^4 - \\
& - 504c^4b - 4176b^3c^3 - 9c^8b^3 + 72b^3c^2 - 720c^6b^2 + 2288c^5b^2 + \\
& + 1044c^7b^3 - 322c^8b^4 + 758c^7b^4 + 404c^6b^4 - 210c^7b^2 - 2464c^5b^4 - \\
& - 2394c^6b^3 + 72c^4 + 252c^6b + 3168b^6c^8 + 441c^9b^5 - 7056b^5c + \\
& + 57960b^6c^4 - 47232b^6c^3 + 25344b^6c^2 - 8064b^6c - 1809b^5c^8 + \\
& + 14472b^5c^2 + 3951b^5c^7 - 72c^5 + 36c^6 - 11808b^6c^7 + 1440b^5 + \\
& + 28980b^6c^6 - 49032b^6c^5 - 4410b^5c^6 + 8820b^5c^4 - 15804b^5c^3 + \\
& + 1152b^6 - 504c^9b^6 - 45c^9b^3 - 6c^9b^4 + 104c^8b^2 + 36c^{10}b^6 + \\
& + 14c^{10}b^4 - 45c^{10}b^5 - 99c^7b)(b^2c^4 - 6b^2c^3 + \\
& + 13b^2c^2 - 12b^2c + 4b^2 + c^2)^{-1}.
\end{aligned} \tag{1.3}$$

Though the equations (1.1) arose within the same problem on perfect cuboids, they define two separate parametric families of elliptic curves.

The coefficients (1.2) and (1.3) are rational functions of two rational parameters b and c . Therefore, for those particular values of b and c where the common denominator of these two rational function is nonzero, i. e. where

$$F = b^2c^4 - 6b^2c^3 + 13b^2c^2 - 12b^2c + 4b^2 + c^2 \neq 0,$$

their values can be represented as two irreducible fractions

$$P_1 = \frac{N_1}{R_1}, \quad P_2 = \frac{N_2}{R_2} \tag{1.4}$$

such that $N_1 \in \mathbb{Z}$, $N_2 \in \mathbb{Z}$, $R_1 \in \mathbb{Z}$, and $R_2 \in \mathbb{Z}$.

Due to (1.4) the formulas (1.1) are transformed to the following ones:

$$2R_1(w^2 - 1) = N_1\alpha^3, \quad 2R_2(w^2 - 1) = N_2\alpha^3. \tag{1.5}$$

Since the equations (1.5) are very similar, we unify them by writing the equation

$$2R(w^2 - 1) = N\alpha^3, \tag{1.6}$$

The main goal of the present paper is to bring together some known results applicable to elliptic curves of the form (1.6) thus preparing a background for further computerized numeric search of their rational points. Some of these points, if one is fortunate, could be responsible for perfect cuboids, which are wanted for centuries.

2. BRINGING TO THE WEIERSTRASS FORM.

Assuming that $R \neq 0$ and $N \neq 0$ in the equation (1.6), we substitute

$$w = \frac{y}{4R^2N}, \quad \alpha = \frac{x}{2RN} \tag{2.1}$$

into this equation. As a result we derive the equation

$$y^2 = x^3 + 16 R^4 N^2. \quad (2.2)$$

The equation (2.2) is a special case of the Weierstrass equation

$$y^2 = x^3 + a x + b \quad (2.3)$$

(see [2]) with $a = 0$ and $b = 16 R^4 N^2$. The transformation (2.1) is used for to bring the cubic equation (1.6) to its Weierstrass form (2.2). For a general cubic equation of two variables such a transformation bringing it to the Weierstrass form (2.3) is obtained using the Nagell's algorithm (see [3], [4]).

3. THE GROUP STRUCTURE.

Points of an elliptic curve constitute an additive Abelian group (see [2]). The infinite point $P_\infty = (\infty; \infty)$ is usually chosen for the neutral element of this group: $P + P_\infty = P$. Let $P_1 = (x_1; y_1)$ and $P_2 = (x_2; y_2)$ be two points of the elliptic curve (2.3) other than P_∞ and let $P_3 = (x_3; y_3)$ be their sum. Then, if $x_1 \neq x_2$, the x -coordinate of the point P_3 is given by the formula

$$x_3 = s^2 - (x_1 + x_2), \quad \text{where } s = \frac{y_1 - y_2}{x_1 - x_2}. \quad (3.1)$$

Similarly, if $x_1 \neq x_2$, the y -coordinate of the point P_3 is given by the formula

$$y_3 = -(y_1 + s(x_3 - x_1)), \quad \text{where } s = \frac{y_1 - y_2}{x_1 - x_2} \quad (3.2)$$

and where x_3 is given by the previous formula (3.1).

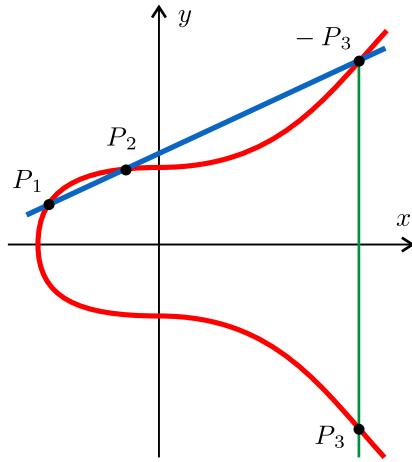


Fig. 3.1

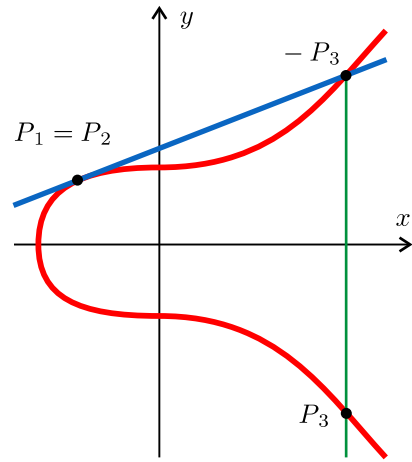


Fig. 3.2

The formulas (3.1) and (3.2) are applicable for $x_1 \neq x_2$. If $x_1 = x_2$, there are two options: $y_1 = y_2$ and $y_1 = -y_2$. If $x_1 = x_2$ and $y_1 = -y_2$, then

$$P_1 + P_2 = P_\infty \quad (3.3)$$

by definition. If $x_1 = x_2$ and $y_1 = y_2$, the x -coordinate of the point P_3 is

$$x_3 = s^2 - 2x_1, \text{ where } s = \frac{3x_1^2 + a}{2y_1}. \quad (3.4)$$

Similarly, if $x_1 = x_2$ and $y_1 = y_2$, the y -coordinate of the point P_3 is

$$y_3 = -(y_1 + s(x_3 - x_1)), \text{ where } s = \frac{3x_1^2 + a}{2y_1} \quad (3.5)$$

and where x_3 is given by the previous formula (3.4).

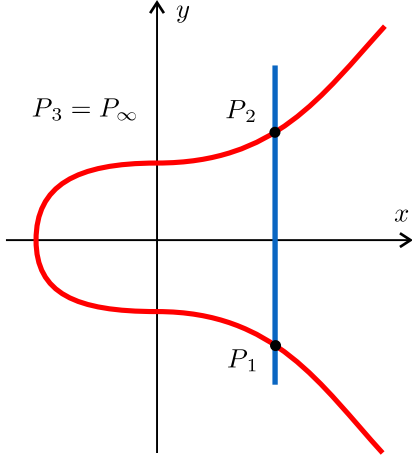


Fig. 3.3

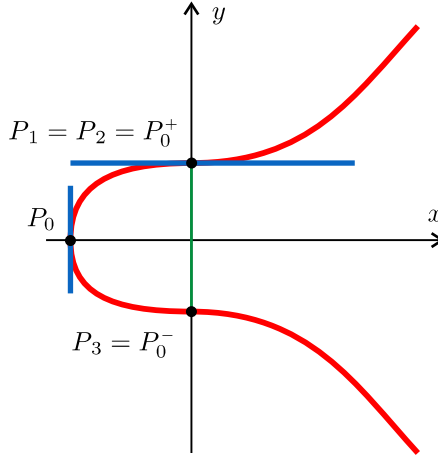


Fig. 3.4

The formulas (3.1) and (3.2) correspond to the case shown in Fig. 3.1. Similarly, the formulas (3.4) and (3.5) correspond to the case shown in Fig. 3.2. The formula (3.3) corresponds to the case shown in Fig. 3.3 above.

The formulas (3.1) and (3.2) corresponding to Fig. 3.1 can be transformed as

$$x_3 = \frac{x_1 x_2^2 + x_2 x_1^2 - 2y_2 y_1 + a x_1 + a x_2 + 2b}{(x_1 - x_2)^2}, \quad (3.6)$$

$$y_3 = \frac{y_2 x_1^3 - y_1 x_2^3 + 4y_2 b - 4y_1 b + y_2 a x_2 - y_1 a x_1}{(x_1 - x_2)^3} + \frac{3y_2 a x_1 - 3y_1 a x_2 + 3y_2 x_2 x_1^2 - 3y_1 x_1 x_2^2}{(x_1 - x_2)^3}. \quad (3.7)$$

The formulas (3.4) and (3.5) corresponding to Fig. 3.2 can be transformed as

$$x_3 = \frac{x_1^4 - 2x_1^2 a - 8x_1 b + a^2}{4(x_1^3 + a x_1 + b)}, \quad (3.8)$$

$$y_3 = \frac{x_1^6 + 5x_1^4 a + 20x_1^3 b - 5x_1^2 a^2 - 4a x_1 b - a^3 - 8b^2}{8(x_1^3 + a x_1 + b)^2} y_1. \quad (3.9)$$

Definition 3.1. Due to the addition law given by Figs. 3.1, 3.2, 3.3 and by the formulas (3.3), (3.6), (3.7), (3.8), (3.9) rational points of an elliptic curve E given by the equation (2.3), where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, constitute an additive Abelian group. This Abelian group is denoted by $E(\mathbb{Q})$.

4. SPECIAL POINTS.

The curve (2.2) is a special form of the general elliptic curve (2.3) with $a = 0$ and $b = 16 R^4 N^2$. Since $b = 16 R^4 N^2$ is a square of the integer number $4 R^2 N$, the curve (2.2) has the following two special points:

$$P_0^+ = (0; 4 R^2 N), \quad P_0^- = (0; -4 R^2 N). \quad (4.1)$$

The special points (4.1) of the elliptic curve (2.2) are shown in Fig. 3.4. Comparing Fig. 3.4 with Figs. 3.2 and 3.3, we derive

$$2 P_0^+ = P_0^+ + P_0^+ = P_0^-, \quad P_0^+ + P_0^- = P_\infty = 0. \quad (4.2)$$

Using (4.2), one easily derives the following formulas:

$$3 P_0^+ = 0, \quad 3 P_0^- = 0. \quad (4.3)$$

The formulas (4.3) constitute a result formulated as the following theorem.

Theorem 4.1. *Let R and N be nonzero integers. Then the rational points (4.1) of the elliptic curve E given by the equation (2.2) generate a finite subgroup of the Abelian group $E(\mathbb{Q})$. This finite subgroup $\{P_\infty, P_0^+, P_0^-\}$ is isomorphic to \mathbb{Z}_3 .*

Now assume that the integer number $4 R^2 N \neq 0$ is an exact cube. In this case we can write $4 R^2 N = 8 M^3$. Applying this equality to (2.2), we derive

$$y^2 = x^3 + 64 M^6. \quad (4.4)$$

The curve (4.4) has one more special point in addition to the points (4.1):

$$P_0 = (-4 M^2; 0). \quad (4.5)$$

The point (4.5) is shown in Fig. 3.4. Comparing Fig. 3.4 and Fig. 3.3, we derive

$$2 P_0 = 0. \quad (4.6)$$

Theorem 4.2. *Let M be a nonzero integer. Then the rational point (4.5) of the elliptic curve E given by the equation (4.4) generates a finite subgroup of the Abelian group $E(\mathbb{Q})$. This finite subgroup $\{P_\infty, P_0\}$ is isomorphic to \mathbb{Z}_2 .*

The formula (4.6) says that P_0 is a second order rational point of the curve (4.4). Similarly, the formulas (4.3) say that P_0^+ and P_0^- are two third order rational points of the curve (2.2). Below in sections 6 and 10 we especially study two classes of elliptic curves — the class of curves with a rational point of the order 2 and the class of curves with two rational points of the order 3.

4. SOME CLASSICAL THEOREMS.

Let E be an elliptic curve given by the equation (2.3), where $a \in \mathbb{Q}$ and $b \in \mathbb{Q}$. The structure of the Abelian group $E(\mathbb{Q})$ for such a curve is described by the following well-known theorem (see [5], [6], or [4]).

Theorem 5.1 (Mordell). *For an elliptic curve (2.3) with $a \in \mathbb{Q}$ and $b \in \mathbb{Q}$ the group of its rational points $E(\mathbb{Q})$ is finitely generated.*

Rational points of finite order constitute a finite subgroup in $E(\mathbb{Q})$. This subgroup $E_{\text{tors}}(\mathbb{Q})$ is called the torsion subgroup. Due to Theorem 5.1 we have

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{\text{tors}}(\mathbb{Q}), \quad \text{where } r < \infty. \quad (5.1)$$

The integer number $0 \leq r < \infty$ in (5.1) is called the *rank* of an elliptic curve. The structure of the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ in the formula (5.1) is described by the following theorem (see [6]).

Theorem 5.2 (Mazur). *For an elliptic curve (2.3) with $a \in \mathbb{Q}$ and $b \in \mathbb{Q}$ if the torsion subgroup of its rational points $E_{\text{tors}}(\mathbb{Q})$ is not trivial, then it is isomorphic to \mathbb{Z}_m , where m is one of the numbers 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, or it is isomorphic to $\mathbb{Z}_m \times \mathbb{Z}_2$, where m is one of the numbers 2, 4, 6, 8.*

Note that the elliptic curves associated with cuboids are not general elliptic curves. They are given by the equation (2.2), which corresponds to $a = 0$ in (2.3). For such curves in [6] we find the following theorem.

Theorem 5.3. *For an elliptic curve $y^2 = x^3 + b$, where b is a sixth-power free integer, if the torsion subgroup of its rational points $E_{\text{tors}}(\mathbb{Q})$ is not trivial, then it is isomorphic to \mathbb{Z}_m , where m is one of the numbers 2, 3, 6. The option $m = 2$ corresponds to the case where b is a cube different from 1. The option $m = 3$ corresponds to the case where b is a square different from 1 or $b = -2^4 3^3$. And finally, the option $m = 6$ corresponds to the case where $b = 1$.*

In general case the parameter $b = 16 R^4 N^2$ in (2.2) is not sixth-power free. However, one can bring it to a sixth-power free form using the transformation

$$x \rightarrow u^2 x, \quad y \rightarrow u^3 y, \quad b \rightarrow u^6 b. \quad (5.2)$$

Theorem 5.3 along with the transformation (5.2) means that the order of a point $P \in E_{\text{tors}}(\mathbb{Q})$ in our case is not greater than 6. The option $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}_2$ is excluded for the curve (2.2) due to Theorem 4.1. Thus we have the following result.

Theorem 5.4. *For an elliptic curve of the form (2.2) associated with cuboids the torsion subgroup of its rational points $E_{\text{tors}}(\mathbb{Q})$ is isomorphic to either \mathbb{Z}_3 or \mathbb{Z}_6 .*

The case $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}_6$ is the most simple. In this case Theorem 5.3 says that the curve (2.2) is isomorphic to the curve

$$y^2 = x^3 + 1. \quad (5.3)$$

Applying the transformation (5.2) backward to the curve (5.3), we derive the equality $16 R^4 N^2 = u^6$. This equality means that the curve (5.3) corresponds to the case where $4 R^2 N \neq 0$ is an exact cube, i.e. $4 R^2 N = 8 M^3$ and $u = 2 M$. This

case was considered above in Theorem 4.2.

Rational points of the curve (5.3) were studied by Euler in 1738. He has proved the following theorem.

Theorem 5.5 (Euler). *If x and y are positive rational numbers satisfying the equation (5.3), then $x = 2$ and $y = 3$.*

Euler's theorem 5.5 is equivalent to the following proposition which is a modern version of Euler's theorem 5.5.

Theorem 5.6. *The rank of the curve (5.3) is equal to zero. Its group of rational points $E(\mathbb{Q})$ is the group of six elements*

$$E(\mathbb{Q}) = \{(\infty; \infty), (2; 3), (0; 1), (-1; 0), (0; -1), (2; -3)\} = E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}_6.$$

Applying the transformation (5.2) backward to the curve (5.3) and using Theorem 5.6, we can strengthen Theorem 4.2 in the following way.

Theorem 5.7. *If the nonzero integer number $4R^2N$ is an exact cube, i. e. if $4R^2N = 8M^3$, then the rank of the curve (2.2), which is written as (4.4) in this case, is equal to zero. The group of rational points $E(\mathbb{Q})$ of the curve (4.4) is finite and is composed by the following six elements:*

$$\begin{aligned} P_\infty &= (\infty; \infty), & P_*^+ &= (8M^2; 24M^3), & P_0^+ &= (0; 8M^3), \\ P_0 &= (-4M^2; 0), & P_0^- &= (0; -8M^3), & P_*^- &= (8M^2; -24M^3). \end{aligned}$$

Theorem 5.7 is immediate from Theorem 5.6. The proof of Theorem 5.6, i. e. a modern proof of Euler's theorem 5.5, can be found in [7]. We reproduce this proof with minor changes below in section 9 for the sake of completeness and as an example of using the 2-descent method.

6. TWO DESCENT. ISOGENIES AND DESCENT MAPPINGS.

The 2-descent method is a method of calculating the rank of an elliptic curve. Here it is applied to curves with at least one rational point of the order 2. Let's consider a general elliptic curve E in Weierstrass form (2.3) possessing a rational point P_0 of the order 2. The equality $2P_0 = 0$ means $P_0 = -P_0$. According to Fig. 3.3, for a point $P = (x; y)$ on the curve (2.3) its opposite point is $-P = (x; -y)$. Then $P_0 = -P_0$ means that the y -coordinate of the point P_0 is equal to zero. Let's denote the x -coordinate of the point P_0 through c . As a result we get $P_0 = (c; 0)$. Substituting $x = c$ and $y = 0$ into (2.3), we find that $b = -c^3 - ac$. Thus, a curve possessing a point of the order 2 is given by the equation

$$y^2 = x^3 + ax - c^3 - ac. \tag{6.1}$$

The curve (5.3) is an example of such a curve (6.1) where $a = 0$ and $c = -1$. The curve (4.4) is another example with $a = 0$ and $c = -4M^2$.

Along with the curve (6.1), we consider the other curve \tilde{E} of the same sort

$$\tilde{y}^2 = \tilde{x}^3 + \tilde{a}\tilde{x} - \tilde{c}^3 - \tilde{a}\tilde{c}, \tag{6.2}$$

where $\tilde{a} = -4a - 15c^2$ and $\tilde{c} = -2c$. The curve \tilde{E} given by the equation (6.2) is called the associated curve for the curve (6.1).

Note that the discriminant of the polynomial in the right hand side of (6.1) is given by the formula $D = -(3c^2 + 4a)(a + 3c^2)^2$, which means that the cases $a = -3c^2$ and $a = -3c^2/4$ in (6.1) correspond to singular curves. Note also that $a = -3c^2$ is equivalent to $\tilde{a} = -3\tilde{c}^2/4$ and $a = -3c^2/4$ is equivalent to $\tilde{a} = -3\tilde{c}^2$. This result is formulated as a lemma.

Lemma 6.1. *Both curves (6.1) and (6.2) are non-singular if and only if $a \neq -3c^2$ and $a \neq -3c^2/4$. Otherwise both of them are singular.*

Now, assuming that $a \neq -3c^2$ and $a \neq -3c^2/4$ and following [7], we define a mapping $\psi: E \rightarrow \tilde{E}$ by means of the formulas

$$\tilde{x} = \frac{x^2 - xc + a + 3c^2}{x - c}, \quad (6.3)$$

$$\tilde{y} = \frac{y(x^2 - 2xc - a - 2c^2)}{(x - c)^2}, \quad (6.4)$$

where $x \neq c$ and $x \neq \infty$. For the special points P_0 and P_∞ we set by definition

$$\psi(P_0) = \tilde{P}_\infty, \quad \psi(P_\infty) = \tilde{P}_0. \quad (6.5)$$

Since the formulas (6.3) and (6.4) are not applicable to the points P_0 and P_∞ , below we shall call these two points the exceptional points of the curve E . The curve \tilde{E} has its own exceptional points \tilde{P}_0 and \tilde{P}_∞ .

Substituting (6.3) and (6.4) into (6.2) and taking into account (6.1), one can prove that the formulas (6.3), (6.4), (6.5) do actually define a mapping from the curve E to its associated curve \tilde{E} .

Lemma 6.2. *The mapping $\psi: E \rightarrow \tilde{E}$ defined by the formulas (6.3), (6.4), (6.5) induces a homomorphism of Abelian groups $\psi: E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{Q})$.*

Lemma 6.2 implicitly assumes that the non-singularity conditions $a \neq -3c^2$ and $a \neq -3c^2/4$ from Lemma 6.1 are fulfilled. The proof of Lemma 6.2 is pure calculations using the formulas (6.3), (6.4), (6.5) along with the formulas (3.3), (3.6), (3.7), (3.8), (3.9).

The curve (6.2) is of the same sort as the curve (6.1). Therefore we can define a mapping $\tilde{\psi}: \tilde{E} \rightarrow E$ by means of the formulas

$$x = \frac{\tilde{x}^2 - \tilde{x}\tilde{c} + \tilde{a} + 3\tilde{c}^2}{4(\tilde{x} - \tilde{c})}, \quad (6.6)$$

$$y = \frac{\tilde{y}(\tilde{x}^2 - 2\tilde{x}\tilde{c} - \tilde{a} - 2\tilde{c}^2)}{8(\tilde{x} - \tilde{c})^2}, \quad (6.7)$$

where $\tilde{x} \neq \tilde{c}$ and $\tilde{x} \neq \infty$. For the exceptional points $\tilde{P}_0 = (\tilde{c}; 0)$ and \tilde{P}_∞ we set

$$\tilde{\psi}(\tilde{P}_0) = P_\infty, \quad \tilde{\psi}(\tilde{P}_\infty) = P_0. \quad (6.8)$$

Substituting (6.6) and (6.7) into (6.1) and taking into account (6.2), one can verify that the formulas (6.6), (6.7), (6.8) define a mapping from \tilde{E} to E .

Lemma 6.3. *The mapping $\tilde{\psi}: \tilde{E} \rightarrow E$ defined by the formulas (6.6), (6.7), (6.8) induces the homomorphism of Abelian groups $\tilde{\psi}: \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$.*

Lemma 6.3 is similar to Lemma 6.2. Its proof is also pure calculations.

Let's consider the composite mapping $\tilde{\psi} \circ \psi: E \rightarrow E$. Due to Lemmas 6.2 and 6.3 it induces an endomorphism of the Abelian group $E(\mathbb{Q})$.

Lemma 6.4. *The endomorphism $\tilde{\psi} \circ \psi: E(\mathbb{Q}) \rightarrow E(\mathbb{Q})$ coincides with the doubling endomorphism, i. e. $\tilde{\psi} \circ \psi(P) = 2P$ for any $P \in E(\mathbb{Q})$.*

The proof of Lemma 6.4 is pure calculations by substituting (6.3) and (6.4) into the formulas (6.6) and (6.7). The formulas (6.5) and (6.8) are also used in the case of exceptional points.

The mappings $\psi: E \rightarrow \tilde{E}$ and $\tilde{\psi}: \tilde{E} \rightarrow E$ defined above are called 2-isogenies (see [8]). Due to Lemma 6.4 the isogeny $\tilde{\psi}$ is dual to the isogeny ψ (see [9]).

Let \mathbb{Q}^* be the set of all nonzero rational numbers. This set possesses the structure of a multiplicative Abelian group. Through \mathbb{Q}^{*2} we denote the set of all nonzero rational numbers which are squares. Then \mathbb{Q}^{*2} is a subgroup of \mathbb{Q}^* and one can define the factor group $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Now we define a mapping $\alpha: E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$. According to [7], this mapping is defined by means of the formula

$$\alpha(P) = x - c \text{ for } x \neq c \text{ and } x \neq \infty. \quad (6.9)$$

The exceptional points P_∞ and P_0 are treated separately. For them we set

$$\alpha(P_\infty) = 1, \quad \alpha(P_0) = a + 3c^2. \quad (6.10)$$

In order to relate (6.10) with (6.9) one should write the equation (6.1) as

$$x - c = \frac{y^2 (x - c)^2}{(x^2 + xc + c^2 + a)^2} \cdot \frac{x^2 + xc + c^2 + a}{x^2 - 2xc + c^2}, \quad (6.11)$$

$$x - c = \frac{y^2}{(x^2 + xc + c^2 + a)^2} \cdot (x^2 + xc + c^2 + a). \quad (6.12)$$

Square factors are neglected modulo \mathbb{Q}^{*2} in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Therefore, due to (6.9) the formulas (6.11) and (6.12) are equivalent to the following relationships:

$$\alpha(P) = \frac{x^2 + xc + c^2 + a}{x^2 - 2xc + c^2}, \quad (6.13)$$

$$\alpha(P) = x^2 + xc + c^2 + a. \quad (6.14)$$

Setting $x \rightarrow \infty$ in (6.13) and $x \rightarrow c$ in (6.14), we obtain the formulas (6.10).

Lemma 6.5. *The mapping $\alpha: E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by the formulas (6.9) and (6.10) induces the homomorphism of Abelian groups $\alpha: E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$.*

In order to prove Lemma 6.5 assume that $P_1 = (x_1; y_1)$ and $P_2 = (x_2; y_2)$ are two non-exceptional rational points of the curve (6.1) and assume that $P_3 = (x_3; y_3)$ is their sum. Then (6.9) yields $\alpha(P_3) = x_3 - c$. Applying the formula (3.6), where $b = -c^3 - ac$ in the case of the curve (6.1), we derive

$$\alpha(P_3) = (x_1 x_2^2 + x_2 x_1^2 + a x_2 - 2c^3 - 2ac - 2y_2 y_1 +$$

$$+ a x_1 - c x_2^2 + 2 c x_2 x_1 - c x_1^2)(x_1 - x_2)^{-2}.$$

The square factor $(x_1 - x_2)^{-2}$ is inessential modulo \mathbb{Q}^{*2} in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Therefore

$$\begin{aligned} \alpha(P_3) &= x_1 x_2^2 + x_2 x_1^2 + a x_2 - 2 c^3 - 2 a c - 2 y_2 y_1 + \\ &\quad + a x_1 - c x_2^2 + 2 c x_2 x_1 - c x_1^2. \end{aligned} \quad (6.15)$$

Now let's calculate the product $\alpha(P_1)\alpha(P_2)$. Applying (6.9), we get

$$\alpha(P_1)\alpha(P_2) = (x_1 - c)(x_2 - c). \quad (6.16)$$

The right hand sides of (6.15) and (6.16) look quite different. However, in $\mathbb{Q}^*/\mathbb{Q}^{*2}$ we can multiply the right hand side of (6.16) by a square factor, which is inessential:

$$\alpha(P_1)\alpha(P_2) = (x_1 - c)(x_2 - c) \left(\frac{y_1}{x_1 - c} - \frac{y_2}{x_2 - c} \right)^2. \quad (6.17)$$

Expanding the right hand side of (6.17) and transforming it with the use of the curve equation (6.1), we derive $\alpha(P_1 + P_2) = \alpha(P_3) = \alpha(P_1)\alpha(P_2)$. Similar tricks are used for proving this equality in the case of exceptional points P_∞ and P_0 .

The curve (6.2) is similar to the curve (6.1). Therefore we can define a mapping $\tilde{\alpha}: E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ using formulas similar to (6.9) and (6.10):

$$\tilde{\alpha}(\tilde{P}) = \tilde{x} - \tilde{c} \text{ for } \tilde{x} \neq \tilde{c} \text{ and } \tilde{x} \neq \infty. \quad (6.18)$$

The exceptional points \tilde{P}_∞ and \tilde{P}_0 are treated separately. For them we set

$$\tilde{\alpha}(\tilde{P}_\infty) = 1, \quad \tilde{\alpha}(\tilde{P}_0) = \tilde{a} + 3\tilde{c}^2. \quad (6.19)$$

Lemma 6.6. *The mapping $\tilde{\alpha}: \tilde{E} \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined by the formulas (6.18) and (6.19) induces a homomorphism of Abelian groups $\tilde{\alpha}: \tilde{E}(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$.*

Lemma 6.6 is absolutely analogous to Lemma 6.5. For this reason we do not provide a proof of this lemma.

The mappings $\alpha: E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ and $\tilde{\alpha}: \tilde{E} \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ defined above are called descent mappings or, more specifically, 2-descent mappings.

Lemma 6.7. *The kernel of the homomorphism $\alpha: E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ coincides with the image of the homomorphism $\tilde{\psi}: \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$.*

Let $P = (x; y)$ be a non-exceptional rational point of the curve (6.1) such that $P \in \text{Ker } \alpha$. Then, according to the formula (6.9), we have

$$\alpha(P) = x - c = \beta^2 \quad (6.20)$$

for some rational number $\beta \neq 0$. From (6.20) we derive $x = \beta^2 + c$. Substituting $x = \beta^2 + c$ into the curve equation (6.1), we get

$$\frac{y^2}{\beta^2} = \beta^4 + 3\beta^2 c + a + 3c^2. \quad (6.21)$$

We need to find a rational point $\tilde{P} = (\tilde{x}; \tilde{y})$ of the curve (6.2) such that $\tilde{\psi}(\tilde{P}) = P$. The formula (6.6) yields the following equation for the coordinate \tilde{x} :

$$\frac{\tilde{x}^2 - \tilde{x}\tilde{c} + \tilde{a} + 3\tilde{c}^2}{4(\tilde{x} - \tilde{c})} = \beta^2 + c. \quad (6.22)$$

Since $\tilde{x} - \tilde{c} \neq 0$ in (6.22), we obtain a quadratic equation for \tilde{x} :

$$\tilde{x}^2 - 2(c - 2\beta^2)\tilde{x} - 11c^2 - 4a - 8\beta^2c = 0. \quad (6.23)$$

It is easy to calculate the discriminant of the quadratic equation (6.23):

$$D = 16(\beta^4 + 3\beta^2c + a + 3c^2). \quad (6.24)$$

Then we apply the standard formula for the roots of a quadratic equation. It yields

$$\tilde{x} = 2\beta^2 + c \pm \frac{\sqrt{D}}{2}. \quad (6.25)$$

Comparing (6.24) with the formula (6.21), we find that the formula (6.25) yields two rational solutions for the quadratic equation (6.23):

$$\tilde{x} = 2\beta^2 + c \pm \frac{2y}{\beta}. \quad (6.26)$$

In order to calculate the second coordinate \tilde{y} of the point \tilde{P} we use the formula (6.7). This formula can be written in the following form:

$$\tilde{y} = \frac{8y(\tilde{x} + 2c)^2}{\tilde{x}^2 + 4\tilde{x}c + 7c^2 + 4a}. \quad (6.27)$$

Substituting (6.26) into (6.27) and applying the curve equation (6.21), we get

$$\tilde{y} = 4y \pm (4\beta^3 + 6c\beta). \quad (6.28)$$

The formulas (6.26) and (6.28) yield explicit expressions for the coordinates of the required rational point \tilde{P} such that $\tilde{\psi}(\tilde{P}) = P$. Thus, for a non-exceptional rational point P of the curve E we have proved that $P \in \text{Ker } \alpha$ implies $P \in \text{Im } \tilde{\psi}$.

Let's proceed to exceptional points P_∞ and P_0 . The case of the point P_∞ is trivial since in this case $P_\infty \in \text{Ker } \alpha$ and $P_\infty = \tilde{\psi}(\tilde{P}_\infty)$.

Assume that $P_0 \in \text{Ker } \alpha$. Then from (6.10) we derive $a + 3c^2 = \beta^2$, where $\beta \neq 0$ is some rational number. Let's resolve the equality $a + 3c^2 = \beta^2$ with respect to a :

$$a = \beta^2 - 3c^2. \quad (6.29)$$

Taking into account the relationships $\tilde{a} = -4a - 15c^2$, $\tilde{c} = -2c$ and applying the formula (6.29) to (6.2), we find that the curve equation (6.2) turns to

$$\tilde{y}^2 = (x + 2c)(x - c - 2\beta)(x - c + 2\beta). \quad (6.30)$$

The formula (6.30) means that under the assumption $P_0 \in \text{Ker } \alpha$ the curve \tilde{E} has

not only the exceptional point $\tilde{P}_0 = (-2c; 0)$ but two other similar points

$$\tilde{P}_{01} = (c + 2\beta; 0), \quad \tilde{P}_{02} = (c - 2\beta; 0). \quad (6.31)$$

The non-exceptional points \tilde{P}_{01} and \tilde{P}_{02} neither can coincide with each other nor with the point \tilde{P}_0 since otherwise the curve \tilde{E} would be singular (see Lemma 6.1). Applying (6.6) and (6.7) to the coordinates of the points (6.31), we derive

$$\tilde{\psi}(\tilde{P}_{01}) = P_0, \quad \tilde{\psi}(\tilde{P}_{02}) = P_0. \quad (6.32)$$

Each of the two formulas (6.32) is sufficient to conclude that if $P_0 \in \text{Ker } \alpha$, then $P_0 \in \text{Im } \tilde{\psi}$. Summarizing the above considerations for exceptional and non-exceptional points, we derive $\text{Ker } \alpha \subseteq \text{Im } \tilde{\psi}$.

Now, conversely, assume that P is a non-exceptional rational point such that $P \in \text{Im } \tilde{\psi}$. Then its coordinates x and y are given by the formulas (6.6) and (6.7), where \tilde{x} and \tilde{y} are the coordinates of some rational point \tilde{P} of the curve (6.2). Note that the formula (6.6) can be written as follows:

$$x - c = \frac{\tilde{x}^2 - 2\tilde{x}c - 11c^2 - 4a}{4(\tilde{x} + 2c)}. \quad (6.33)$$

Multiplying the numerator and the denominator of the fraction (6.33) by $\tilde{x} + 2c$, we derive the following formula for $x - c$:

$$x - c = \frac{\tilde{x}^3 - (15c^2 + 4a)\tilde{x} - 22c^3 - 8ac}{4(\tilde{x} + 2c)^2}. \quad (6.34)$$

Comparing the numerator of (6.34) with the curve equation (6.2), where $\tilde{c} = -2c$ and $\tilde{a} = -4a - 15c^2$, and taking into account (6.9), we transform (6.34) as follows:

$$\alpha(P) = x - c = \frac{\tilde{y}^2}{4(\tilde{x} + 2c)^2}. \quad (6.35)$$

The right hand side of (6.35) is a square of a rational number. For this reason $\alpha(P) \in \text{Ker } \alpha$. Thus, for a non-exceptional rational point P of the curve E we have proved that $P \in \text{Im } \tilde{\psi}$ implies $P \in \text{Ker } \alpha$.

Let's proceed to exceptional points P_∞ and P_0 . The case of the point P_∞ is trivial since in this case $P_\infty = \tilde{\psi}(\tilde{P}_\infty)$ and $P_\infty \in \text{Ker } \alpha$.

Assume that $P_0 \in \text{Im } \tilde{\psi}$. Then the coordinates $x = c$ and $y = 0$ of the point P_0 are given by the formulas (6.6) and (6.7), where \tilde{x} and \tilde{y} are the coordinates of some non-exceptional rational point \tilde{P} of the curve (6.2). Therefore the equality $x = c$ leads to the following equations with respect to \tilde{x} :

$$\frac{\tilde{x}^2 - \tilde{x}\tilde{c} + \tilde{a} + 3\tilde{c}^2}{4(\tilde{x} - \tilde{c})} = c, \quad (6.36)$$

The denominator of the fraction in (6.36) is nonzero. Therefore the equation (6.36) is equivalent to a quadratic equation for \tilde{x} . Due to $\tilde{a} = -4a - 15c^2$ and $\tilde{c} = -2c$

this quadratic equation can be written as

$$\tilde{x}^2 - 2\tilde{x}c - 11c^2 - 4a = 0. \quad (6.37)$$

One can easily calculate the discriminant $D = 16(a + 3c^2)$ of the quadratic equation (6.37) and derive the following explicit formula for its solution \tilde{x} :

$$\tilde{x} = c \pm 2\sqrt{a + 3c^2}. \quad (6.38)$$

The formula (6.38) can be transformed to the following one:

$$a + 3c^2 = \left(\frac{\tilde{x} - c}{2}\right)^2. \quad (6.39)$$

Comparing (6.39) with the formula (6.10) for $\alpha(P_0)$, we derive

$$\alpha(P_0) = \left(\frac{\tilde{x} - c}{2}\right)^2. \quad (6.40)$$

Square factors are neglected modulo \mathbb{Q}^{*2} in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Hence the equality (6.40) is equivalent to $\alpha(P_0) = 1$, which means $P_0 \in \text{Ker } \alpha$. We have proved that $P_0 \in \text{Im } \tilde{\psi}$ implies $P_0 \in \text{Ker } \alpha$. Summarizing the above considerations for exceptional and non-exceptional points, we derive $\text{Im } \tilde{\psi} \subseteq \text{Ker } \alpha$. Then, combining $\text{Im } \tilde{\psi} \subseteq \text{Ker } \alpha$ with the previously derived inclusion $\text{Ker } \alpha \subseteq \text{Im } \tilde{\psi}$, we conclude that $\text{Ker } \alpha = \text{Im } \tilde{\psi}$, which completes the proof of Lemma 6.7.

Lemma 6.8. *The kernel of the homomorphism $\tilde{\alpha}: \tilde{E}(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ coincides with the image of the homomorphism $\psi: E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{Q})$.*

Lemma 6.8 is proved in a way similar to the above proof of Lemma 6.7.

7. FACTOR GROUPS AND THE RANK FORMULA.

Let's proceed to further studying the homomorphisms $\psi: E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{Q})$ and $\tilde{\psi}: \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$. The visual image in Fig. 7.1 will help the reader. In the left

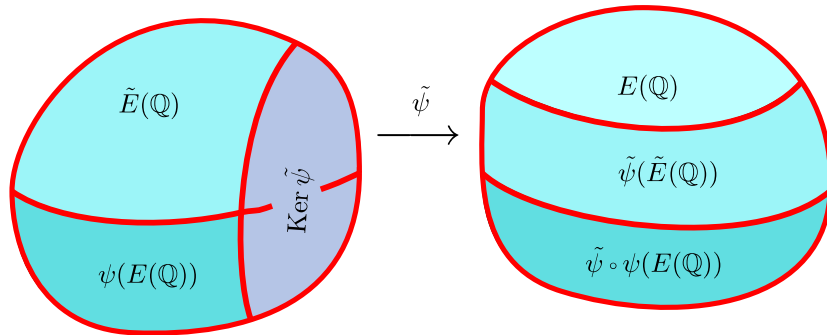


Fig. 7.1

hand side of this image we have two independent inclusions $\psi(E(\mathbb{Q})) \subset \tilde{E}(\mathbb{Q})$ and $\text{Ker } \tilde{\psi} \subset \tilde{E}(\mathbb{Q})$. In the right hand side of the image we have the series of inclusions

$\tilde{\psi} \circ \psi(E(\mathbb{Q})) \subset \tilde{\psi}(\tilde{E}(\mathbb{Q})) \subset E(\mathbb{Q})$. From this series of inclusions we derive

$$E/\tilde{\psi}(\tilde{E}(\mathbb{Q})) \cong (E/\tilde{\psi} \circ \psi(E(\mathbb{Q}))) / (\tilde{\psi}(\tilde{E}(\mathbb{Q}))/\tilde{\psi} \circ \psi(E(\mathbb{Q}))) \quad (7.1)$$

(see basics of the group theory in [10]). The isomorphism (7.1) yields the following relationship for the indices of subgroups in (7.1):

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = [E(\mathbb{Q}) : \tilde{\psi}(\tilde{E}(\mathbb{Q}))] \cdot [\tilde{\psi}(\tilde{E}(\mathbb{Q})) : \tilde{\psi} \circ \psi(E(\mathbb{Q}))]. \quad (7.2)$$

In deriving the above equality (7.2) we used the equality $2E(\mathbb{Q}) = \tilde{\psi} \circ \psi(E(\mathbb{Q}))$ provided by Lemma 6.4.

Note that the mapping $\tilde{\psi}: \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$ in Fig. 7.1 can be treated as the surjective mapping $\tilde{\psi}: \tilde{E}(\mathbb{Q}) \rightarrow \tilde{\psi}(\tilde{E}(\mathbb{Q}))$. This surjective mapping can be combined with the factorization mapping $\tau: \tilde{\psi}(\tilde{E}(\mathbb{Q})) \rightarrow \tilde{\psi}(\tilde{E}(\mathbb{Q}))/\tilde{\psi} \circ \psi(E(\mathbb{Q}))$:

$$\tilde{E}(\mathbb{Q}) \xrightarrow{\tilde{\psi}} \tilde{\psi}(\tilde{E}(\mathbb{Q})) \xrightarrow{\tau} \tilde{\psi}(\tilde{E}(\mathbb{Q}))/\tilde{\psi} \circ \psi(E(\mathbb{Q})). \quad (7.3)$$

Both mappings in (7.3) are surjective. Therefore the composite mapping $\tau \circ \tilde{\psi}$ in (7.3) is also surjective. Its kernel is easily calculated:

$$\text{Ker}(\tau \circ \tilde{\psi}) = \psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi}. \quad (7.4)$$

From (7.3) and (7.4) we derive the isomorphism

$$\tilde{E}(\mathbb{Q})/(\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi}) \cong \tilde{\psi}(\tilde{E}(\mathbb{Q}))/\tilde{\psi} \circ \psi(E(\mathbb{Q})) \quad (7.5)$$

Along with the isomorphism (7.5) we have the following two isomorphisms:

$$\begin{aligned} & \tilde{E}(\mathbb{Q})/(\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi}) \cong \\ & \cong (\tilde{E}(\mathbb{Q})/\psi(E(\mathbb{Q}))) / ((\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi})/\psi(E(\mathbb{Q}))), \end{aligned} \quad (7.6)$$

$$(\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi})/\psi(E(\mathbb{Q})) \cong \text{Ker } \tilde{\psi}/(\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q}))). \quad (7.7)$$

The isomorphisms (7.6) and (7.7) are basic facts from the group theory (see [10]). From (7.5), (7.6), and (7.7) we derive the equalities

$$[\tilde{\psi}(\tilde{E}(\mathbb{Q})) : \tilde{\psi} \circ \psi(E(\mathbb{Q}))] = [\tilde{E}(\mathbb{Q}) : (\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi})], \quad (7.8)$$

$$[\tilde{E}(\mathbb{Q}) : (\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi})] = \frac{[\tilde{E}(\mathbb{Q}) : \psi(E(\mathbb{Q}))]}{[(\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi}) : \psi(E(\mathbb{Q}))]}, \quad (7.9)$$

$$[(\psi(E(\mathbb{Q})) + \text{Ker } \tilde{\psi}) : \psi(E(\mathbb{Q}))] = [\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))]. \quad (7.10)$$

Now, combining (7.2) with (7.8), (7.9), and (7.10), we obtain the equality

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = \frac{[E(\mathbb{Q}) : \tilde{\psi}(\tilde{E}(\mathbb{Q}))] \cdot [\tilde{E}(\mathbb{Q}) : \psi(E(\mathbb{Q}))]}{[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))]}. \quad (7.11)$$

Lemma 7.1. *The index $[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))]$ equals 1 if and only if the curve (6.1) has a rational point $P = (x, 0)$ of the order 2 different from its exceptional point $P_0 = (c; 0)$. Otherwise $[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))] = 2$.*

Looking at (6.8), we see that $\text{Ker } \tilde{\psi}$ consists of two elements \tilde{P}_∞ and \tilde{P}_0 . According to (6.5) the point \tilde{P}_∞ belongs to $\psi(E(\mathbb{Q}))$. The point $\tilde{P}_0 = (\tilde{c}; 0)$ belongs to $\psi(E(\mathbb{Q}))$ if and only if there is a non-exceptional rational point $P = (x, y)$ of the curve (6.1) such that $\psi(P) = \tilde{P}_0$. Applying (6.4) and (6.5), we derive

$$\frac{x^2 - xc + a + 3c^2}{x - c} = \tilde{c}, \quad (7.12)$$

$$\frac{y(x^2 - 2xc - a - 2c^2)}{(x - c)^2} = 0, \quad (7.13)$$

where $x \neq c$. Since $\tilde{c} = -2c$, the equality (7.12) reduces to

$$x^2 + xc + c^2 + a = 0. \quad (7.14)$$

The polynomial $x^2 + xc + c^2 + a$ cannot vanish simultaneously with the polynomial $x^2 - 2xc - a - 2c^2$ in the numerator of the fraction in (7.13). Otherwise we would have the following system of two quadratic equations:

$$\begin{cases} x^2 + xc + c^2 + a = 0, \\ x^2 - 2xc - a - 2c^2 = 0. \end{cases} \quad (7.15)$$

Let's multiply the first equation (7.15) by $9c^2 - 3xc + 2a$ and multiply the second equation (7.15) by $3xc - 2a$. Then, adding the resulting two equations, we derive

$$9c^4 + 15c^2a + 4a^2 = 0. \quad (7.16)$$

The left hand side of the equality (7.16) factors as follows:

$$(a + 3c^2)(4a + 3c^2) = 0. \quad (7.17)$$

Applying Lemma 6.1, we see that the equality (7.17) contradicts the non-singularity condition of the curves (6.1) and (6.2).

The contradiction obtained means that the equation (7.14) should be complemented with the inequality $x^2 - 2xc - a - 2c^2 \neq 0$. Then from (7.13) we derive $y = 0$, which means that $P = (x; y)$ is a rational point of the order 2. Since $x \neq c$ in (7.12) and (7.13), this point does not coincide with P_0 . Lemma 7.1 is proved.

Let's consider the subgroup indices $[E(\mathbb{Q}) : \tilde{\psi}(\tilde{E}(\mathbb{Q}))]$ and $[\tilde{E}(\mathbb{Q}) : \psi(E(\mathbb{Q}))]$ in the numerator of the fraction in the right hand side of (7.11). Applying Lemmas 6.7 and 6.8, for these indices we derive

$$[E(\mathbb{Q}) : \tilde{\psi}(\tilde{E}(\mathbb{Q}))] = |\alpha(E(\mathbb{Q}))|, \quad [\tilde{E}(\mathbb{Q}) : \psi(E(\mathbb{Q}))] = |\tilde{\alpha}(\tilde{E}(\mathbb{Q}))|. \quad (7.18)$$

The number of elements in a group or, more generally, in a set G is often denoted through $\#G$. But we prefer to use the notation $|G|$ in (7.18) instead of $\#G$. Due to

the formulas (7.18) the formula (7.11) is written in the following way:

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = \frac{|\alpha(E(\mathbb{Q}))| \cdot |\tilde{\alpha}(\tilde{E}(\mathbb{Q}))|}{[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))]}. \quad (7.19)$$

Let's recall Mordell's theorem 5.1 and the formula (5.1). From (5.1) we derive

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (Z_2)^r \oplus E_2(\mathbb{Q}), \quad (7.20)$$

where $E_2(\mathbb{Q})$ is the subgroup of $E_{\text{tors}}(\mathbb{Q})$ generated by all elements of the order 2. Applying (7.20) to (7.19), we transform the formula (7.19) as follows:

$$2^r \cdot |E_2(\mathbb{Q})| = \frac{|\alpha(E(\mathbb{Q}))| \cdot |\tilde{\alpha}(\tilde{E}(\mathbb{Q}))|}{[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))]}. \quad (7.21)$$

The formula (7.21) yields a way for calculating the rank r of an elliptic curve.

8. IMAGES OF THE DESCENT MAPPINGS.

The next step is to calculate the groups $\alpha(E(\mathbb{Q}))$ and $\tilde{\alpha}(\tilde{E}(\mathbb{Q}))$. They are images of the descent mappings $\alpha : E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ and $\tilde{\alpha} : \tilde{E}(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$. For calculating them let's present the equation (6.1) in the following form:

$$y^2 = (x - c)((x - c)^2 + 3c(x - c) + B), \quad (8.1)$$

where $B = 3c^2 + a$. The integer number B in (8.1) is nonzero due to Lemma 6.1.

Lemma 8.1. *Let P be a rational point of the curve (6.1). Then $\alpha(P)$ is presented by some integer number being a divisor of $B = 3c^2 + a$.*

For the exceptional points P_∞ and P_0 the proposition of Lemma 8.1 follows from the formulas (6.10). Let $P = (x; y)$ be a non-exceptional rational point of the curve (6.1). Then x and y are rational numbers satisfying the equation (8.1) and such that $x \neq c$. Therefore they are presented by the formulas

$$x = c + \frac{m}{q_1}, \quad y = \frac{n}{q_2}, \quad (8.2)$$

where m , q_1 , and q_2 are nonzero integer numbers such that the fractions (8.2) are irreducible. Assume that $n \neq 0$. Upon substituting (8.2) into (8.1), we obtain

$$\frac{n^2}{q_2^2} = \frac{m}{q_1} \cdot \frac{m^2 + 3cmq_1 + Bq_1^2}{q_1^2}. \quad (8.3)$$

It is easy to see that all of the three fractions in (8.3) are irreducible. This yields

$$q_2^2 = q_1^3. \quad (8.4)$$

Due to (8.4) there is an integer number q such that

$$q_1 = q^2, \quad q_2 = q^3 \quad (8.5)$$

(compare with Lemma 2.1 in [1]). Substituting (8.5) into (8.2), we get

$$x = c + \frac{m}{q^2}, \quad y = \frac{n}{q^3}. \quad (8.6)$$

Similarly, substituting (8.5) into the equation (8.3), we obtain the equation

$$n^2 = m(m^2 + 3cmq^2 + Bq^4). \quad (8.7)$$

The left hand side of (8.7) is positive. Therefore we can write (8.7) as

$$n^2 = |m| \cdot |m^2 + 3cmq^2 + Bq^4|. \quad (8.8)$$

Let's denote $\beta = \gcd(|m|, |m^2 + 3cmq^2 + Bq^4|)$. The fractions in (8.6) are irreducible. Therefore we have $\beta = \gcd(|m|, B)$, i. e. β is a divisor of B . Then

$$m = \pm \beta \mu, \quad m^2 + 3cmq^2 + Bq^4 = \pm \beta \nu, \quad (8.9)$$

where $\mu > 0$, $\nu > 0$, and $\gcd(\mu, \nu) = 1$. Applying (8.9) to (8.8), we get

$$n^2 = \beta^2 \mu \nu. \quad (8.10)$$

The positive integers μ and ν in (8.10) are coprime, while their product is a square. Therefore both of these integer numbers are squares:

$$\mu = M^2, \quad \nu = N^2. \quad (8.11)$$

Applying (8.11) to (8.9) and then applying (8.9) to (8.6), we derive

$$x - c = \frac{m}{q^2} = \pm \frac{\beta \mu}{q^2} = \pm \frac{\beta M^2}{q^2} \equiv \pm \beta \pmod{\mathbb{Q}^{*2}}, \quad (8.12)$$

where β is a divisor of B . The case $n = 0$ in (8.3) is special. In this case

$$x - c = \frac{m}{q_1} = \beta \quad (8.13)$$

and (8.3) yields that β is a rational root of the monic polynomial $\beta^2 - 3c\beta + B = 0$ with integer coefficients. In this case the rational root theorem (see [11]) says that $q_1 = 1$, while $\beta = m$ is a divisor of B . Comparing (8.12) and (8.13) with (6.9), we find that Lemma 8.1 is proved.

Lemma 8.2. *Let \tilde{P} be a point of the curve (6.2). Then $\tilde{\alpha}(\tilde{P})$ is presented by some integer number being a divisor of $\tilde{B} = 3\tilde{c}^2 + \tilde{a}$.*

Lemma 8.2 is similar to the previous lemma 8.1. Its proof is similar to the above proof of Lemma 8.1.

9. PROOF OF EULER'S THEOREM.

Lemma 9.1. *For the curve (5.3) the group $\alpha(E(\mathbb{Q}))$ has two elements presented by the numbers 1 and 3, i. e. $|\alpha(E(\mathbb{Q}))| = 2$.*

The curve (5.3) is a particular case of the curve (6.1) where $a = 0$ and where $c = -1$. Then $B = 3c^2 + a = 3$. The number 3 has two positive divisors 1 and 3. Therefore, according to Lemma 8.1, the group $\alpha(E(\mathbb{Q}))$ has at most four elements presented by the numbers 1, -1 , 3, -3 . The formulas (6.10) yield

$$\alpha(P_\infty) = 1, \quad \alpha(P_0) = 3. \quad (9.1)$$

The relationships (9.1) mean that $\alpha(E(\mathbb{Q}))$ does actually comprise two elements presented by the numbers 1 and 3. Since $-3 = (-1) \cdot 3$, it is sufficient to prove that there is no element presented by the number -1 in $\alpha(E(\mathbb{Q}))$. Assume to the contrary that $\alpha(P) = -1$ for some rational point P . Due to (9.1) we have $P \neq P_\infty$ and $P \neq P_0$, i. e. $P = (x; y)$ is a non-exceptional point. Then we can apply (8.2) to its coordinates and derive (8.3). The curve (5.3) has no rational points with $y = 0$ other than $P_0 = (-1; 0)$. Therefore $n \neq 0$ in (8.2). Then, repeating the logic of the proof of Lemma 8.1, we come from (8.3) to (8.12). But now

$$\alpha(P) = x - c \equiv -1 \pmod{\mathbb{Q}^{*2}}. \quad (9.2)$$

The formula (9.2) means that $\beta = K^2$ for some nonzero integer K and that we should choose the negative sign in (8.12). The sign choices in (8.12) and (8.9) do coincide. Therefore, from (8.9), (8.10), and (8.11) we derive

$$m = -M^2 K^2, \quad n^2 = M^2 N^2 K^4. \quad (9.3)$$

Substituting (9.3) into (8.7), and recalling that now $c = -1$ and $B = 3$, we get

$$N^2 K^2 = -(M^4 K^4 + 3M^2 K^2 q^2 + 3q^4). \quad (9.4)$$

The equality (9.4) means that K^2 divides $3q^4$, i. e. if $K^2 \neq 1$, then K and q would have at least one common prime factor p , which is either $p = 3$ or $p \neq 3$. Due to (9.3) this prime factor p of q would be a prime factor of m and n as well. But the fractions in (8.1) and (8.6) are irreducible. Therefore $K^2 = 1$ and $\beta = 1$. Substituting $K^2 = 1$ into the equality (9.4), we reduce this equality to

$$N^2 = -M^4 - 3M^2 q^2 - 3q^4. \quad (9.5)$$

The equality (9.5) means that $N^2 \equiv -M^4 \pmod{3}$, which implies $N \equiv 0 \pmod{3}$ and $M \equiv 0 \pmod{3}$. But μ and ν given by the formulas (8.11) should be coprime, i. e. $\gcd(\mu, \nu) = 1$, which contradicts $N \equiv 0 \pmod{3}$ and $M \equiv 0 \pmod{3}$. The contradiction obtained proves Lemma 9.1.

The curve (6.1) is associated with the curve (6.2). In the case of the curve (5.3) the associated curve is given by the equation

$$\tilde{y}^2 = \tilde{x}^3 - 15\tilde{x} + 22, \quad (9.6)$$

where $\tilde{c} = -2c = 2$, $\tilde{a} = -4a - 15c^2 = -15$, and $\tilde{B} = 3\tilde{c}^2 + \tilde{a} = -3$.

Lemma 9.2. *For the curve (9.6) the group $\tilde{\alpha}(\tilde{E}(\mathbb{Q}))$ has two elements presented by the numbers 1 and 3, i. e. $|\tilde{\alpha}(\tilde{E}(\mathbb{Q}))| = 2$.*

The number $\tilde{B} = -3$ has two positive divisors 1 and 3. Therefore, according to Lemma 8.2, the group $\tilde{\alpha}(\tilde{E}(\mathbb{Q}))$ has at most four elements presented by the numbers 1, -1 , 3, -3 . The formulas (6.19) in this case yield

$$\tilde{\alpha}(\tilde{P}_\infty) = 1, \quad \tilde{\alpha}(\tilde{P}_0) = -3. \quad (9.7)$$

Since $3 = (-1) \cdot (-3)$, it is sufficient to prove that there is no element presented by the number -1 in $\tilde{\alpha}(\tilde{E}(\mathbb{Q}))$. Assume to the contrary that $\tilde{\alpha}(\tilde{P}) = -1$ for some rational point \tilde{P} . Due to (9.7) we have $\tilde{P} \neq \tilde{P}_\infty$ and $\tilde{P} \neq \tilde{P}_0$, i.e. $\tilde{P} = (\tilde{x}; \tilde{y})$ is a non-exceptional point. The curve (9.6) has no rational points with $\tilde{y} = 0$ other than $\tilde{P}_0 = (2; 0)$. Therefore we can write the formulas analogous to (8.2):

$$\tilde{x} = 2 + \frac{\tilde{m}}{\tilde{q}_1}, \quad \tilde{y} = \frac{\tilde{n}}{\tilde{q}_2}. \quad (9.8)$$

Here \tilde{m} , \tilde{n} , \tilde{q}_1 , and \tilde{q}_2 are nonzero integer numbers such that the fractions (9.8) are irreducible. Substituting (9.8) into (9.6), we derive the equality

$$\frac{\tilde{n}^2}{\tilde{q}_2^2} = \frac{\tilde{m}}{\tilde{q}_1} \cdot \frac{\tilde{m}^2 + 6\tilde{m}\tilde{q}_1 - 3\tilde{q}_1^2}{\tilde{q}_1^2} \quad (9.9)$$

analogous to (8.3). Now, repeating the arguments used in proving Lemma 8.1, we get $\tilde{q}_1 = \tilde{q}^2$ and $\tilde{q}_2 = \tilde{q}^3$. Then we bring (9.9) to the equality

$$\tilde{n}^2 = \tilde{m}(\tilde{m}^2 + 6\tilde{m}\tilde{q}^2 - 3\tilde{q}^4). \quad (9.10)$$

analogous to (8.7). The positive integer $\tilde{\beta}$ defined by the formula

$$\tilde{\beta} = \gcd(|\tilde{m}|, |\tilde{m}^2 + 6\tilde{m}\tilde{q}^2 - 3\tilde{q}^4|) = \gcd(|\tilde{m}|, 3)$$

is a divisor of the number $\tilde{B} = -3$. Since above we assumed $\tilde{\alpha}(\tilde{P}) = -1$, the formula (6.18) complemented with $\tilde{c} = 2$ yields the formula

$$\tilde{\alpha}(\tilde{P}) = \tilde{x} - 2 \equiv -1 \pmod{\mathbb{Q}^{*2}} \quad (9.11)$$

analogous to (9.2). From (9.11) we derive $\tilde{m} < 0$ and write

$$\tilde{m} = -\tilde{\beta}\tilde{\mu}, \quad \tilde{m}^2 + 6\tilde{m}\tilde{q}^2 - 3\tilde{q}^4 = -\tilde{\beta}\tilde{\nu}, \quad (9.12)$$

where $\tilde{\mu} > 0$, $\tilde{\nu} > 0$, and $\gcd(\tilde{\mu}, \tilde{\nu}) = 1$. The formulas (9.12) are analogous to (8.9). Applying these formulas to (9.10), we derive

$$\tilde{n}^2 = \tilde{\beta}^2\tilde{\mu}\tilde{\nu}. \quad (9.13)$$

The positive integers μ and ν in (8.10) are coprime, while their product is a square. Therefore both of these integer numbers are squares:

$$\tilde{\mu} = \tilde{M}^2, \quad \tilde{\nu} = \tilde{N}^2. \quad (9.14)$$

The formulas (9.13) and (9.14) are analogous to (8.10) and (8.11) respectively.

Applying (9.14) to (9.12) and then applying (9.12) to (9.8), we derive

$$\tilde{x} - 2 = \frac{\tilde{m}}{\tilde{q}^2} = -\frac{\tilde{\beta}\tilde{\mu}}{\tilde{q}^2} = -\frac{\tilde{\beta}\tilde{M}^2}{\tilde{q}^2} \equiv -\tilde{\beta} \pmod{\mathbb{Q}^{*2}}, \quad (9.15)$$

Comparing (9.15) with (9.11), we conclude that $\tilde{\beta}$ is a square, i. e. $\tilde{\beta} = \tilde{K}^2$ for some nonzero integer number \tilde{K} . On the other hand, in the present case $\tilde{\beta}$ is a divisor of $\tilde{B} = -3$. Therefore $\tilde{\beta} = \tilde{K}^2 = 1$. As a result from (9.12) and (9.13), we derive

$$\tilde{m} = -\tilde{M}^2, \quad \tilde{n}^2 = \tilde{M}^2 \tilde{N}^2. \quad (9.16)$$

Substituting (9.16) into (9.10), we produce the equality analogous to (9.5):

$$\tilde{N}^2 = -\tilde{M}^4 + 6\tilde{M}^2\tilde{q}^2 + 3\tilde{q}^4. \quad (9.17)$$

The equality (9.17) means that $\tilde{N}^2 \equiv -\tilde{M}^4 \pmod{3}$, which implies $\tilde{N} \equiv 0 \pmod{3}$ and $\tilde{M} \equiv 0 \pmod{3}$. But $\tilde{\mu}$ and $\tilde{\nu}$ given by the formulas (9.14) should be coprime, i. e. $\gcd(\tilde{\mu}, \tilde{\nu}) = 1$, which contradicts $\tilde{N} \equiv 0 \pmod{3}$ and $\tilde{M} \equiv 0 \pmod{3}$. The contradiction obtained proves Lemma 9.2.

Let's apply Lemma 7.1 to the curve (5.3). Substituting $y = 0$ into (5.3), we derive $x^3 + 1 = 0$. The left hand side of this equation factors as follows:

$$(x + 1)(x^2 - x + 1) = 0. \quad (9.18)$$

It is clear that $x = -1$ is the only rational solution of the equation (9.18). If we recall that $c = -1$ for the curve (5.3) and $P_0 = (c; 0)$, then we derive

$$[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))] = 2. \quad (9.19)$$

Let's substitute (9.19) into the formula (7.21). Then, applying Lemma 9.1 and Lemma 9.2 to the formula (7.21), we obtain

$$2^r \cdot |E_2(\mathbb{Q})| = 2. \quad (9.20)$$

The subgroup $E_2(\mathbb{Q}) \subset E_{\text{tors}}(\mathbb{Q})$ in (9.20) and the torsion group $E_{\text{tors}}(\mathbb{Q})$ itself can be calculated with the use of the following Lutz-Nagell theorem.

Theorem 9.1 (Lutz and Nagell). *Let $P = (x; y)$ be a rational point of finite order on an elliptic curve given by the equation (2.3) with integer coefficients a and b . Then its coordinates x and y both are integers and either $y = 0$ or y divides D , where $D = -4a^3 - 27b^2$ is the discriminant of the cubic polynomial in the right hand side of the equation (2.3).*

The discriminant of the cubic polynomial $x^3 + 1$ in the case of the curve (5.3) is calculated explicitly: $D = -27$. Then Theorem 9.1 yields

$$E_{\text{tors}}(\mathbb{Q}) = \{(\infty; \infty), (2; 3), (0; 1), (-1; 0), (0; -1), (2; -3)\} \cong \mathbb{Z}_6.$$

The group \mathbb{Z}_6 has one element $P_0 = (-1; 0)$ of the order 2. Therefore

$$E_2(\mathbb{Q}) = \{(\infty; \infty), (-1; 0)\} \cong \mathbb{Z}_2.$$

and $|E_2(\mathbb{Q})| = 2$. Applying this result to (9.20), we derive $2^r = 1$, which means $r = 0$. The proof of Theorem 5.6 is completed. As we noted above in section 5, this theorem is equivalent to Euler's theorem 5.5.

Theorem 5.6 is very important in the context of cuboid curves (2.2). As we have seen in section 5, it is used for proving Theorem 5.7, which solves the rank problem for the subset of curves (2.2) where $4R^2N$ is an exact cube. The subset of curves where $4R^2N$ is not an exact cube is much more broad and more complicated. Our further efforts below are directed toward solving the rank problem for this subset of curves (2.2), though we do not solve this problem completely.

10. THREE DESCENT. ISOGENIES AND DESCENT MAPPINGS.

From this section on, below we assume that the integer number $4R^2N$ is not an exact cube. Then, applying the transformation (5.2) to the curve equation (2.2), we can bring this curve equation to the form

$$y^2 = x^3 + e^2, \quad (10.1)$$

where $e \neq 1$ is some positive cube free integer number. Like in the case of the curves (6.1) and (6.2), along with each curve E of the form (10.1), we consider its associated curve \tilde{E} . This curve is defined by means of the equation

$$\tilde{y}^2 = \tilde{x}^3 - 27e^2. \quad (10.2)$$

Applying Theorem 5.3 to the curve (10.1), we derive the following lemma.

Lemma 10.1. *If $e \neq 1$ is a positive third power free integer, then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of the curve (10.1) is isomorphic to \mathbb{Z}_3 :*

$$E_{\text{tors}}(\mathbb{Q}) = \{(\infty; \infty), (0; e), (0; -e)\} \cong \mathbb{Z}_3. \quad (10.3)$$

The points $P_0^+ = (0; e)$ and $P_0^- = (0; -e)$ in (10.3) correspond to the exceptional points (4.1) of the initial elliptic curve (2.2).

The associated curve \tilde{E} in (10.2) is different. Applying Theorem 5.3, we derive the following lemma for the associated curve (10.2).

Lemma 10.2. *If $e = 4$, then the torsion subgroup $\tilde{E}_{\text{tors}}(\mathbb{Q})$ of the curve (10.2) is isomorphic to \mathbb{Z}_3 . It is given explicitly by the formula*

$$\tilde{E}_{\text{tors}}(\mathbb{Q}) = \{(\infty; \infty), (12, 36), (12, -36)\},$$

where $P_0^+ = (12; 36)$ and $P_0^- = (12; -36)$ are two third order rational points of the curve \tilde{E} . If $e \neq 1$ and $e \neq 4$ is a positive third power free integer, then the torsion subgroup $\tilde{E}_{\text{tors}}(\mathbb{Q})$ is trivial, i. e. $\tilde{E}_{\text{tors}}(\mathbb{Q}) = \{(\infty; \infty)\}$.

Like in Section 6, we define a mapping $\psi: E \rightarrow \tilde{E}$ by setting

$$\tilde{x} = \frac{x^3 + 4e^2}{x^2}, \quad \tilde{y} = \frac{y(x^3 - 8e^2)}{x^3}, \quad (10.4)$$

where $x \neq 0$. For the exceptional points P_0^+ , P_0^- , and P_∞ we set by definition

$$\psi(P_0^+) = \tilde{P}_\infty, \quad \psi(P_0^-) = \tilde{P}_\infty, \quad \psi(P_\infty) = \tilde{P}_\infty. \quad (10.5)$$

The formulas (10.4) are analogs of the formulas (6.3) and (6.4), while the formulas (10.5) are analogs of the formulas (6.5).

The curve (10.2) is similar to the curve (10.1). Therefore there is a backward mapping $\tilde{\psi}: \tilde{E} \rightarrow E$. This mapping is given by the formulas

$$x = \frac{\tilde{x}^3 - 108e^2}{9\tilde{x}^2}, \quad y = \frac{\tilde{y}(\tilde{x}^3 + 216e^2)}{27\tilde{x}^3}, \quad (10.6)$$

where $\tilde{x} \neq 0$. The formulas (10.6) are analogs of the formulas (6.6) and (6.7). The curve (10.2) has no exceptional rational points with $\tilde{x} = 0$. Therefore the analog of the formulas (6.8) in this case is written as follows:

$$\tilde{\psi}(\tilde{P}_\infty) = P_\infty. \quad (10.7)$$

The transformations (10.4) and (10.6) were discovered by Fueter in [12] (see also [13] and Chapter 26 of [14]).

Lemma 10.3. *The mapping $\psi: E \rightarrow \tilde{E}$ defined by the formulas (10.4) and (10.5) induces a homomorphism of Abelian groups $\psi: E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{Q})$.*

Lemma 10.4. *The mapping $\tilde{\psi}: \tilde{E} \rightarrow E$ defined by the formulas (10.6) and (10.7) induces the homomorphism of Abelian groups $\tilde{\psi}: \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$.*

Lemmas 10.3 and 10.4 are analogs of Lemmas 6.2 and 6.3 respectively. Their proofs are pure calculations using the formulas (3.3), (3.6), (3.7), (3.8), (3.9).

Now let's consider the composite mapping $\tilde{\psi} \circ \psi: E \rightarrow E$. Due to Lemmas 10.3 and 10.4 it induces an endomorphism of the Abelian group $E(\mathbb{Q})$.

Lemma 10.5. *The endomorphism $\tilde{\psi} \circ \psi: E(\mathbb{Q}) \rightarrow E(\mathbb{Q})$ coincides with the tripling endomorphism, i. e. $\tilde{\psi} \circ \psi(P) = 3P$ for any $P \in E(\mathbb{Q})$.*

The proof of Lemma 10.5 is also pure calculations.

Recall that \mathbb{Q}^* is the set of all nonzero rational numbers. This set possesses the structure of a multiplicative Abelian group. Through \mathbb{Q}^{*3} we denote the set of all nonzero rational numbers which are cubes. Then \mathbb{Q}^{*3} is a subgroup of \mathbb{Q}^* and we have the factor group $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Now we define two mappings $\alpha_+: E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$ and $\alpha_-: E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$. The mapping α_- is defined by means of the formula

$$\alpha_-(P) = y - e \text{ for } y \neq e \text{ and } y \neq \infty. \quad (10.8)$$

The exceptional points P_0^+ and P_∞ are treated separately. For them we set

$$\alpha_-(P_\infty) = 1, \quad \alpha_-(P_0^+) = \frac{1}{2e}. \quad (10.9)$$

The mapping α_+ is defined similarly by means of the formula

$$\alpha_+(P) = y + e \text{ for } y \neq -e \text{ and } y \neq \infty. \quad (10.10)$$

The exceptional points in this case are P_0^- and P_∞ . For them we set

$$\alpha_+(P_\infty) = 1, \quad \alpha_+(P_0^-) = -\frac{1}{2e}. \quad (10.11)$$

The formulas (10.8) and (10.9) are taken from [15]. The formulas (10.10) and (10.11) are written by analogy.

In order to relate (10.9) with (10.8) and in order to relate (10.11) with (10.10) we write the equation (10.1) as $(y + e)(y - e) = x^3$. Then (10.8) and (10.10) yield

$$\alpha_-(P) = \frac{x^3}{y + e}, \quad \alpha_+(P) = \frac{x^3}{y - e}, \quad (10.12)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore, the above formulas (10.12) are equivalent to the following four relationships:

$$\alpha_-(P) = \frac{1}{y + e}, \quad \alpha_+(P) = \frac{1}{y - e}, \quad (10.13)$$

$$\alpha_-(P) = \frac{y^3}{x^3(y + e)}, \quad \alpha_+(P) = \frac{y^3}{x^3(y - e)}. \quad (10.14)$$

Passing to the limit as $y \rightarrow e$ and as $y \rightarrow -e$ in (10.13) and passing to the limit as $x \rightarrow \infty$ along with $y \rightarrow \infty$ in (10.14), we derive the formulas (10.9) and (10.11).

Lemma 10.6. *The mapping $\alpha_- : E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$ defined by the formulas (10.8) and (10.9) induces the homomorphism of Abelian groups $\alpha_- : E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$.*

Lemma 10.7. *The mapping $\alpha_+ : E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$ defined by the formulas (10.10) and (10.11) induces the homomorphism of Abelian groups $\alpha_+ : E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$.*

In order to prove Lemma 10.6 assume that $P_1 = (x_1; y_1)$ and $P_2 = (x_2; y_2)$ are two non-exceptional rational points of the curve (10.1) and assume that the point $P_3 = (x_3; y_3)$ is their sum. Then (10.8) yields $\alpha(P_3) = y_3 - e$. Applying the formula (3.7), where $a = 0$ and $b = e^2$ in the case of the curve (10.1), we derive

$$\begin{aligned} \alpha_-(P_3) = & (y_2 x_1^3 - y_1 x_2^3 + 3 y_2 x_2 x_1^2 - 3 y_1 x_1 x_2^2 + 4 y_2 e^2 - 4 y_1 e^2 + \\ & + e x_2^3 - e x_1^3 + 3 e x_2 x_1^2 - 3 e x_1 x_2^2) (x_1 - x_2)^{-3}. \end{aligned} \quad (10.15)$$

Now let's calculate the product $\alpha_-(P_1) \alpha_-(P_2)$. Applying (10.8), we get

$$\alpha_-(P_1) \alpha_-(P_2) = (y_1 - e)(y_2 - e) = \frac{(y_1^2 - e^2)(y_2^2 - e^2)}{(y_1 + e)(y_2 + e)}. \quad (10.16)$$

Then we apply the curve equation to the numerator of the fraction in (10.16):

$$\alpha_-(P_1) \alpha_-(P_2) = \frac{x_1^3 x_2^3}{(y_1 + e)(y_2 + e)}. \quad (10.17)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Keeping in mind this fact, from (10.15) and (10.17) we derive the following relationship:

$$\begin{aligned} \alpha_-(P_3) \alpha_-(P_1)^{-1} \alpha_-(P_2)^{-1} = & (y_2 x_1^3 - y_1 x_2^3 + 3 y_2 x_2 x_1^2 - 3 y_1 x_1 x_2^2 + \\ & + 4 y_2 e^2 - 4 y_1 e^2 + e x_2^3 - e x_1^3 + 3 e x_2 x_1^2 - 3 e x_1 x_2^2) (y_1 + e)(y_2 + e). \end{aligned} \quad (10.18)$$

Taking into account the curve equation (10.1), we can expand and then refactor

the right hand side of the equality (10.18). As a result we get

$$\alpha_-(P_3) \alpha_-(P_1)^{-1} \alpha_-(P_2)^{-1} = (e x_2 - e x_1 + y_1 x_2 - x_1 y_2)^3. \quad (10.19)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore (10.19) yields

$$\alpha_-(P_3) = \alpha_-(P_1) \alpha_-(P_2). \quad (10.20)$$

The equality (10.20) proves Lemma 10.6. Lemma 10.7 is proved similarly.

The homomorphisms $\alpha_+ : E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$ and $\alpha_- : E \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$ are not independent. Indeed, due to (10.8), (10.10), and the curve equation (10.1) we have $\alpha_+(P) \alpha_-(P) = x^3$. But cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Then

$$\alpha_+(P) \alpha_-(P) = 1. \quad (10.21)$$

The formula (10.21) means that Lemma 10.7 is immediate from Lemma 10.6. Moreover, from the formula (10.21) we derive the equality

$$\text{Ker } \alpha_- = \text{Ker } \alpha_+. \quad (10.22)$$

Lemma 10.8. *The kernel of the homomorphism $\alpha_- : E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$ coincides with the image of the homomorphism $\tilde{\psi} : \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$.*

Lemma 10.9. *The kernel of the homomorphism $\alpha_+ : E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$ coincides with the image of the homomorphism $\tilde{\psi} : \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$.*

Due to the formula (10.21) Lemma 10.9 is immediate from Lemma 10.8. Therefore it is sufficient to prove Lemma 10.8.

Let $P = (x; y)$ be a non-exceptional rational point of the curve (10.1) such that $P \in \text{Im } \tilde{\psi}$. Then its coordinates x and y are given by the formulas (10.6). Using the second formula (10.6) and applying (10.8), we derive the following relationship:

$$\alpha_-(P) = y - e = \frac{216 \tilde{y} e^2 + \tilde{y} \tilde{x}^3 - 27 e \tilde{x}^3}{27 \tilde{x}^3}. \quad (10.23)$$

Due to the curve equation (10.2) the numerator of the fraction in the right hand side of (10.23) factors as $216 \tilde{y} e^2 + \tilde{y} \tilde{x}^3 - 27 e \tilde{x}^3 = (\tilde{y} - 9e)^3$. Then

$$\alpha_-(P) = \frac{(\tilde{y} - 9e)^3}{3^3 \tilde{x}^3}. \quad (10.24)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore (10.24) means that $\alpha_-(P) = 1$ and $P \in \text{Ker } \alpha_-$.

For the exceptional point $P = P_0^- = (0; -e)$ the value of $\alpha_-(P)$ is given by the formula (10.8), which serves non-exceptional points as well. Therefore the above reasons remain valid for the exceptional point $P = P_0^-$, i.e. if $P_0^- \in \text{Im } \tilde{\psi}$, then $P_0^- \in \text{Ker } \alpha_-$. The exceptional point $P = P_0^+ = (0; e)$ is more special. Assume that $P_0^+ \in \text{Im } \tilde{\psi}$. Then $P_0^+ = \tilde{\psi}(\tilde{P})$ for some non-exceptional point $\tilde{P} = (\tilde{x}; \tilde{y})$ of the curve (10.2). Applying the formulas (10.6), we derive the following two equations:

$$\frac{\tilde{x}^3 - 108 e^2}{9 \tilde{x}^2} = 0, \quad \frac{\tilde{y} (\tilde{x}^3 + 216 e^2)}{27 \tilde{x}^3} = e. \quad (10.25)$$

Since $\tilde{x} \neq 0$, the equations (10.25) are equivalent to

$$\tilde{x}^3 - 108 e^2 = 0, \quad 216 \tilde{y} e^2 + \tilde{y} \tilde{x}^3 - 27 e \tilde{x}^3 = 0. \quad (10.26)$$

The left hand side of the second equation (10.26) coincides with the numerator of the fraction in (10.23). Therefore, using the curve equation (10.2), we can simplify it to the equation $(\tilde{y} - 9e)^3 = 0$, which yields $\tilde{y} = 9e$. Substituting $\tilde{y} = 9e$ into the curve equation (10.2), we derive the equation $\tilde{x}^3 = 108e^2$, which coincides with the first equation (10.25).

Let's recall that e is a third power free positive integer (see (10.1)) and use the prime factor expansion $108 = 2^2 \cdot 3^3$. Then the equality $\tilde{x}^3 = 108e^2$ can hold in the only case where $e = 4$. For the coordinates of the point \tilde{P} we derive $\tilde{x} = 12$ and $\tilde{y} = 36$. The image of the point $\tilde{P} = (12; 36)$ under the mapping $\tilde{\psi}$ is the exceptional point $P_0^+ = (0; 4)$. The value of $\alpha_-(P_0^+)$ for such a point is given by the formula (10.9). Since $e = 4$, this formula yields $\alpha_-(P_0^+) = 1/8 = (1/2)^3$. Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore $\alpha_-(P_0^+) = 1/8$ is equivalent to $\alpha_-(P_0^+) = 1$, which means $P_0^+ \in \text{Ker } \alpha_-$.

Thus we have proved the inclusion $\text{Im } \tilde{\psi} \subseteq \text{Ker } \alpha_-$.

Now assume that $P = (x; y)$ is some non-exceptional rational point of the curve (10.1) such that $P \in \text{Ker } \alpha_-$. Then $\alpha_-(P) = 1$, which means

$$y - e = z^3, \quad \text{where } z \neq 0 \quad \text{and } z \in \mathbb{Q}. \quad (10.27)$$

The formula (10.27) yields $y = z^3 + e$. Substituting $y = z^3 + e$ into the curve equation (10.1), we derive the following equation for x and z :

$$z^6 + 2z^3e - x^3 = 0. \quad (10.28)$$

Using x and z , we define the point $\tilde{P} = (\tilde{x}; \tilde{y})$ of the associated curve (10.2) whose coordinates \tilde{x} and \tilde{y} are given by the formulas

$$\tilde{x} = \frac{6ez}{x - z^2}, \quad \tilde{y} = \frac{9e(x + z^2)}{x - z^2}. \quad (10.29)$$

The denominator of the fractions (10.29) is nonzero. Indeed, otherwise we would have $x = z^2$. Substituting $x = z^2$ into (10.28), we would derive $2z^3e = 0$. Since $e \neq 0$, this would mean $z = 0$, which contradicts (10.27).

In order to verify that \tilde{x} and \tilde{y} given by the formulas (10.29) do actually form a point of the curve (10.2), we substitute them into the equation (10.2). This yields

$$\frac{108e^2(z^6 + 2z^3e - x^3)}{(x - z^2)^3} = 0. \quad (10.30)$$

It is easy to see that the equation (10.30) is fulfilled due to (10.28).

The homomorphism $\tilde{\psi}: \tilde{E}(\mathbb{Q}) \rightarrow E(\mathbb{Q})$ is defined by means of the formulas (10.6). Substituting (10.29) into (10.6), we derive

$$x = \frac{2z^3e - x^3 + 3x^2z^2 - 3xz^4 + z^6}{3z^2(x - z^2)}, \quad (10.31)$$

$$y = \frac{(z^3 e + x^3 - 3x^2 z^2 + 3x z^4 - z^6)(x + z^2)}{3z^3(x - z^2)}. \quad (10.32)$$

The polynomials in the numerators of the fractions (10.31) and (10.32) are simplified with the use of the equation (10.28). As a result the equality (10.31) turns to the identity $x = x$. The equality (10.32) turns to the equality $y = e + z^3$, which is equivalent to (10.27). Thus we have proved that $P = \tilde{\psi}(\tilde{P})$, where \tilde{P} is the point of the curve (10.2) with the coordinates (10.29), i. e. $P \in \text{Im } \tilde{\psi}$.

The exceptional point $P = P_0^- = (0; -e)$ is similar to non-exceptional points. The value of $\alpha_-(P)$ for it is given by the formula (10.8), which serves non-exceptional points as well. Therefore the above reasons remain valid for the exceptional point $P = P_0^-$, i. e. if $P_0^- \in \text{Ker } \alpha_-$, then $P_0^- \in \text{Im } \tilde{\psi}$. The other exceptional point $P = P_0^+ = (0; e)$ is more special. Assume that $P_0^+ \in \text{Ker } \alpha_-$. Then $\alpha_-(P_0^+) = 1$. Applying the second formula (10.9), we derive the following equation:

$$\frac{1}{2e} = z^3, \text{ where } z \neq 0 \text{ and } z \in \mathbb{Q}. \quad (10.33)$$

Let's recall that e is a third power free positive integer (see (10.1)). Then the equality (10.33) can hold in the only case where $e = 4$. In this case $P_0^+ = (0; 4)$. As we have seen above, if $e = 4$ the point $P_0^+ = (0; 4)$ is the image of the point $\tilde{P} = (12; 36)$ under the mapping $\tilde{\psi}$, i. e. $P_0^+ \in \text{Im } \tilde{\psi}$.

Thus we have proved the inclusion $\text{Ker } \alpha_- \subseteq \text{Im } \tilde{\psi}$. Combining it with the previously proved inclusion $\text{Im } \tilde{\psi} \subseteq \text{Ker } \alpha_-$, we derive the equality $\text{Ker } \alpha_- = \text{Im } \tilde{\psi}$, which proves Lemma 10.8.

The curve (10.2) is different from the curve (10.1). In order to serve this curve we introduce the number field $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. Elements of \mathbb{K} are presented as

$$z = u + v\sqrt{-3}, \text{ where } u \in \mathbb{Q} \text{ and } v \in \mathbb{Q}. \quad (10.34)$$

Nonzero numbers of the form (10.34) constitute a multiplicative Abelian group. We denote it \mathbb{K}^* and consider its factor group $\mathbb{K}^*/\mathbb{K}^{*3}$. Then we define two mappings $\tilde{\alpha}_+ : \tilde{E} \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$ and $\tilde{\alpha}_- : \tilde{E} \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$. The mapping $\tilde{\alpha}_-$ is defined by means of the formula similar to the formula (10.8):

$$\tilde{\alpha}_-(\tilde{P}) = \tilde{y} - 3\sqrt{-3}e \text{ for } y \neq \infty. \quad (10.35)$$

The exceptional point at infinity \tilde{P}_∞ is treated separately. For this point we set

$$\tilde{\alpha}_-(\tilde{P}_\infty) = 1. \quad (10.36)$$

The mapping $\tilde{\alpha}_+$ is defined similarly by means of the formula

$$\tilde{\alpha}_+(\tilde{P}) = \tilde{y} + 3\sqrt{-3}e \text{ for } y \neq \infty. \quad (10.37)$$

For the exceptional point at infinity \tilde{P}_∞ in this case we again set

$$\tilde{\alpha}_+(\tilde{P}_\infty) = 1. \quad (10.38)$$

The formulas (10.35), (10.36), (10.37), (10.38) are written by analogy to the for-

mulas (10.8), (10.9), (10.10), (10.11).

Lemma 10.10. *The mapping $\tilde{\alpha}_- : \tilde{E} \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$ defined by the formulas (10.35) and (10.36) induces the homomorphism of Abelian groups $\tilde{\alpha}_- : \tilde{E}(\mathbb{Q}) \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$.*

Lemma 10.11. *The mapping $\tilde{\alpha}_+ : \tilde{E} \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$ defined by the formulas (10.37) and (10.38) induces the homomorphism of Abelian groups $\tilde{\alpha}_+ : \tilde{E}(\mathbb{Q}) \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$.*

Lemmas 10.10 and 10.11 are similar to Lemmas 10.6 and 10.7. They are proved by analogy to Lemmas 10.6 and 10.7.

Lemma 10.12. *The kernel of the homomorphism $\tilde{\alpha}_- : \tilde{E}(\mathbb{Q}) \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$ coincides with the image of the homomorphism $\psi : E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{Q})$.*

Lemma 10.13. *The kernel of the homomorphism $\tilde{\alpha}_+ : \tilde{E}(\mathbb{Q}) \rightarrow \mathbb{K}^*/\mathbb{K}^{*3}$ coincides with the image of the homomorphism $\psi : E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{Q})$.*

The matter is that the kernels of the homomorphisms $\tilde{\alpha}_-$ and $\tilde{\alpha}_+$ do coincide, i. e. we have a formula similar to the formula (10.22):

$$\text{Ker } \tilde{\alpha}_- = \text{Ker } \tilde{\alpha}_+. \quad (10.39)$$

The formula (10.39) is derived from the equality

$$\tilde{\alpha}_+(\tilde{P})\tilde{\alpha}_-(\tilde{P}) = 1, \quad (10.40)$$

which is similar to (10.21). Indeed, multiplying the formulas (10.35) and (10.37) and applying the curve equation (10.2), we derive

$$\tilde{\alpha}_+(\tilde{P})\tilde{\alpha}_-(\tilde{P}) = \tilde{y}^2 + 27e^2 = \tilde{x}^3. \quad (10.41)$$

The equality (10.41) is equivalent to the equality (10.40) since cubic factors are neglected modulo \mathbb{K}^{*3} in $\mathbb{K}^*/\mathbb{K}^{*3}$.

Let $\tilde{P} = (\tilde{x}; \tilde{y})$ be a non-exceptional rational point of the curve (10.2) such that $\tilde{P} \in \text{Im } \psi$. Then its coordinates \tilde{x} and \tilde{y} are given by the formulas (10.4). Using the second formula (10.4) and applying (10.35), we derive the following relationship:

$$\tilde{\alpha}_-(\tilde{P}) = \tilde{y} - 3\sqrt{-3}e = \frac{yx^3 - 8ye^2 - 3\sqrt{-3}ex^3}{x^3}. \quad (10.42)$$

Due to the curve equation (10.1) the numerator of the fraction in the right hand side of (10.42) factors as $yx^3 - 8ye^2 - 3\sqrt{-3}ex^3 = (\tilde{y} - \sqrt{-3}e)^3$. Then

$$\tilde{\alpha}_-(\tilde{P}) = \frac{(y - \sqrt{-3}e)^3}{\tilde{x}^3}. \quad (10.43)$$

Cubic factors are neglected modulo \mathbb{K}^{*3} in $\mathbb{K}^*/\mathbb{K}^{*3}$. Therefore the formula (10.43) means that $\tilde{\alpha}_-(\tilde{P}) = 1$ and $\tilde{P} \in \text{Ker } \tilde{\alpha}_-$.

Thus we have proved the inclusion $\text{Im } \psi \subseteq \text{Ker } \tilde{\alpha}_-$.

Now assume that $\tilde{P} = (\tilde{x}; \tilde{y})$ is some non-exceptional rational point of the curve (10.2) such that $\tilde{P} \in \text{Ker } \tilde{\alpha}_-$. Then $\tilde{\alpha}_-(\tilde{P}) = 1$, which means

$$\tilde{y} - 3\sqrt{-3}e = z^3, \text{ where } z \neq 0 \text{ and } z \in \mathbb{K}. \quad (10.44)$$

The formula (10.44) yields $\tilde{y} = z^3 + 3\sqrt{-3}e$. Substituting $\tilde{y} = z^3 + 3\sqrt{-3}e$ into the curve equation (10.2), we derive the following equation for \tilde{x} and z :

$$z^6 + 6\sqrt{-3}z^3e - \tilde{x}^3 = 0. \quad (10.45)$$

Using \tilde{x} and z , we define the point $P = (x; y)$ of the curve (10.1) whose coordinates x and y are given by the following formulas:

$$x = \frac{2\sqrt{-3}ez}{\tilde{x} - z^2}, \quad y = \frac{\sqrt{-3}e(\tilde{x} + z^2)}{\tilde{x} - z^2}. \quad (10.46)$$

The denominator of the fractions (10.46) is nonzero. Indeed, otherwise we would have $\tilde{x} = z^2$. Substituting $\tilde{x} = z^2$ into (10.45), we would derive $6\sqrt{-3}z^3e = 0$. Since $e \neq 0$, this would mean $z = 0$, which contradicts (10.44).

In order to verify that x and y given by the formulas (10.46) do actually form a point of the curve (10.1), we substitute them into the equation (10.1). This yields

$$\frac{4e^2(z^6 + 6\sqrt{-3}z^3e - \tilde{x}^3)}{(\tilde{x} - z^2)^3} = 0. \quad (10.47)$$

It is easy to see that the equation (10.47) is fulfilled due to (10.45).

The homomorphism $\psi: E(\mathbb{Q}) \rightarrow \tilde{E}(\mathbb{Q})$ is defined by means of the formulas (10.4). Substituting (10.46) into (10.4), we derive

$$\tilde{x} = \frac{6\sqrt{-3}z^3e - \tilde{x}^3 + 3\tilde{x}^2z^2 - 3\tilde{x}z^4 + z^6}{3z^2(\tilde{x} - z^2)}, \quad (10.48)$$

$$\tilde{y} = \frac{(3\sqrt{-3}z^3e + \tilde{x}^3 - 3\tilde{x}^2z^2 + 3\tilde{x}z^4 - z^6)(\tilde{x} + z^2)}{3z^3(\tilde{x} - z^2)}. \quad (10.49)$$

The polynomials in the numerators of the fractions (10.48) and (10.49) are simplified with the use of the equation (10.45). As a result the equality (10.45) turns to the identity $\tilde{x} = \tilde{x}$. The equality (10.49) turns to the equality $\tilde{y} = z^3 + 3\sqrt{-3}e$, which is equivalent to (10.44).

The formula (10.44) is similar to the formula (10.27). Succeeding formulas (10.45) through (10.49) are similar to the formulas (10.28) through (10.32). However, there is a crucial difference. The number z in (10.44) is not rational, while \tilde{x} and \tilde{y} are rational by assumption. There are also explicit irrationalities of the form $\sqrt{-3}$ in the formulas. For this reason we should take special precautions in order to obtain rational numbers x and y in (10.46). Applying (10.34) to (10.44), we get

$$\tilde{y} = u^3 - 9uv^2 + 3\sqrt{-3}(u^2v - v^3 + e). \quad (10.50)$$

Since \tilde{y} , u , and v are rational numbers, from (10.50) we derive two equations

$$\tilde{y} = u^3 - 9uv^2, \quad u^2v - v^3 + e = 0. \quad (10.51)$$

The first equation (10.51) expresses \tilde{y} through u and v . The second equation (10.51)

can be used in order to express e through u and v :

$$e = v^3 - u^2 v. \quad (10.52)$$

Substituting $\tilde{y} = u^3 - 9uv^2$ and (10.52) into the curve equation (10.2), we derive

$$u^6 + 9u^4v^2 + 27u^2v^4 + 27v^6 - \tilde{x}^3 = 0. \quad (10.53)$$

The equation (10.53) replaces the equation (10.45). It factors as follows:

$$(u^2 + 3v^2 - \tilde{x})(\tilde{x}^2 + \tilde{x}u^2 + 3\tilde{x}v^2 + u^4 + 6u^2v^2 + 9v^4) = 0. \quad (10.54)$$

Due to (10.54) we have two equations which are two options:

$$u^2 + 3v^2 - \tilde{x} = 0, \quad (10.55)$$

$$\tilde{x}^2 + \tilde{x}u^2 + 3\tilde{x}v^2 + u^4 + 6u^2v^2 + 9v^4 = 0. \quad (10.56)$$

The second option (10.56) is a quadratic equation with respect to \tilde{x} . One can easily calculate the discriminant of the quadratic equation (10.56):

$$D = -27v^4 - 3u^4 - 18u^2v^2. \quad (10.57)$$

According to (10.44), the number z is nonzero. Hence its rational components u and v in (10.34) cannot vanish simultaneously. Then (10.57) yields the inequality $D < 0$. But \tilde{x} is a rational number by assumption, which is incompatible with the inequality $D < 0$. Thus we have proved that the equality (10.55) is the only option for u , v , and \tilde{x} derived from (10.53). It yields

$$\tilde{x} = u^2 + 3v^2. \quad (10.58)$$

Now let's proceed to (10.46). Substituting $z = u + v\sqrt{-3}$ from (10.34), $e = v^3 - u^2v$ from (10.52), and $\tilde{x} = u^2 + 3v^2$ from (10.58) into (10.46), we derive

$$x = u^2 - v^2, \quad y = u^3 - uv^2, \quad (10.59)$$

while \tilde{x} and \tilde{y} are given by the formulas taken from (10.58) and (10.51):

$$\tilde{x} = u^2 + 3v^2, \quad \tilde{y} = u^3 - 9uv^2. \quad (10.60)$$

Thus we have proved that if a point $\tilde{P} = (\tilde{x}; \tilde{y})$ belongs to $\text{Ker } \tilde{\alpha}_-$, then there are two rational numbers u and v , which are not zero simultaneously, such that the coordinates of the point \tilde{P} are expressed by means of the formulas (10.60) and there is a point $P = (x; y)$, whose coordinates are given by the formulas (10.59), such that $\tilde{P} = \psi(P)$. The latter fact proves the inclusion $\text{Ker } \tilde{\alpha}_- \subseteq \text{Im } \psi$. Combining it with the previously proved inclusion $\text{Im } \psi \subseteq \text{Ker } \tilde{\alpha}_-$, we derive the equality $\text{Im } \psi = \text{Ker } \tilde{\alpha}_-$ which completes the proof of Lemma 10.12. Lemma 10.13 is immediate from Lemma 10.12 due to the equality (10.39).

11. FACTOR GROUPS AND THE RANK FORMULA.

Further steps are similar to those in Section 7. They are visualized by means of Fig. 7.1. The equality (7.1) goes without changes:

$$E/\tilde{\psi}(\tilde{E}(\mathbb{Q})) \cong (E/\tilde{\psi} \circ \psi(E(\mathbb{Q}))) / (\tilde{\psi}(\tilde{E}(\mathbb{Q}))/\tilde{\psi} \circ \psi(E(\mathbb{Q}))). \quad (11.1)$$

The changes in (7.2) are due to the difference of Lemma 6.4 and Lemma 10.5:

$$[E(\mathbb{Q}) : 3E(\mathbb{Q})] = [E(\mathbb{Q}) : \tilde{\psi}(\tilde{E}(\mathbb{Q}))] \cdot [\tilde{\psi}(\tilde{E}(\mathbb{Q})) : \tilde{\psi} \circ \psi(E(\mathbb{Q}))]. \quad (11.2)$$

The formula (11.2) follows from (11.1) and Lemma 10.5.

Again, we consider the mappings (7.3) and derive the isomorphism (7.5) Then, considering the other two isomorphisms (7.6) and (7.7), we derive the equalities (7.8), (7.9), and (7.10). Combining them with (11.2), we get

$$[E(\mathbb{Q}) : 3E(\mathbb{Q})] = \frac{[E(\mathbb{Q}) : \tilde{\psi}(\tilde{E}(\mathbb{Q}))] \cdot [\tilde{E}(\mathbb{Q}) : \psi(E(\mathbb{Q}))]}{[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))]}. \quad (11.3)$$

Unlike the case of Lemma 7.1, the denominator of the fraction in (11.3) is always equal to 1. Indeed, from (10.7) we derive that $\text{Ker } \tilde{\psi}$ is trivial, i. e. $\text{Ker } \tilde{\psi} = \{\tilde{P}_\infty\}$. The intersection $\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q}))$ is also trivial, i. e. $\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})) = \{\tilde{P}_\infty\}$, which yields $[\text{Ker } \tilde{\psi} : (\text{Ker } \tilde{\psi} \cap \psi(E(\mathbb{Q})))] = 1$. As a result (11.3) is written as

$$[E(\mathbb{Q}) : 3E(\mathbb{Q})] = [E(\mathbb{Q}) : \tilde{\psi}(\tilde{E}(\mathbb{Q}))] \cdot [\tilde{E}(\mathbb{Q}) : \psi(E(\mathbb{Q}))]. \quad (11.4)$$

The next step is to apply Lemmas 10.8 and 10.12 to (11.4). They yield

$$[E(\mathbb{Q}) : 3E(\mathbb{Q})] = |\alpha_-(E(\mathbb{Q}))| \cdot |\tilde{\alpha}_-(\tilde{E}(\mathbb{Q}))|. \quad (11.5)$$

Due to (10.22) and (10.39), we can write (11.5) as

$$[E(\mathbb{Q}) : 3E(\mathbb{Q})] = |\alpha_+(E(\mathbb{Q}))| \cdot |\tilde{\alpha}_+(\tilde{E}(\mathbb{Q}))|. \quad (11.6)$$

The formulas (11.5) and (11.6) are analogs of the formula (7.19).

Let's recall that e in (10.1) is assumed to be a positive third power free integer. Therefore, applying Lemma 10.1, we find $E_{\text{tors}}(\mathbb{Q}) \cong \mathbb{Z}_3$. The third order elements of \mathbb{Z}_3 do vanish under the tripling endomorphism, i. e. $3E_{\text{tors}}(\mathbb{Q}) = \{\tilde{P}_\infty\}$ is trivial. Hence we have the following relationships:

$$[E_{\text{tors}}(\mathbb{Q}) : 3E_{\text{tors}}(\mathbb{Q})] = |E_3(\mathbb{Q})| = |\mathbb{Z}_3| = 3. \quad (11.7)$$

Applying (11.7) to the expression in the left hand sides of (11.5) and (11.6), we get

$$[E(\mathbb{Q}) : 3E(\mathbb{Q})] = 3^r \cdot |E_3(\mathbb{Q})| = 3^{r+1}. \quad (11.8)$$

Combining (11.8) with (11.5) and (11.6), we can write these formulas as

$$\begin{aligned} 3^{r+1} &= |\alpha_-(E(\mathbb{Q}))| \cdot |\tilde{\alpha}_-(\tilde{E}(\mathbb{Q}))|, \\ 3^{r+1} &= |\alpha_+(E(\mathbb{Q}))| \cdot |\tilde{\alpha}_+(\tilde{E}(\mathbb{Q}))|. \end{aligned} \quad (11.9)$$

The formulas (11.9) reduce the problem of calculating ranks to calculating the images of $E(\mathbb{Q})$ and $\tilde{E}(\mathbb{Q})$ under the descent mappings α_- and $\tilde{\alpha}_-$ or, equivalently, under the descent mappings α_+ and $\tilde{\alpha}_+$.

12. IMAGES OF THE DESCENT MAPPINGS.

Lemma 12.1. *Let P be a rational point of the curve (10.1). Then $\alpha_-(P)$ is presented by some integer number $s = A \cdot B^2$, where A and B are two coprime square free positive integer numbers being divisors of the number $2e$.*

The case $P = P_\infty$ is trivial. In this case $\alpha_-(P_\infty) = 1$ and we choose $A = 1$ and $B = 1$. If $P = P_0^+$, then the formula (10.9) yields

$$\alpha_-(P_0^+) = \frac{1}{2e} = \frac{(2e)^2}{(2e)^3}. \quad (12.1)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Hence (12.1) is equivalent to $\alpha_-(P_0^+) = (2e)^2$. Let's consider the prime factor expansion of the number $2e$:

$$2e = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}. \quad (12.2)$$

Using $\alpha_1, \dots, \alpha_r$ in (12.2), we subdivide p_1, \dots, p_r into three disjoint sets:

$$\begin{aligned} p_i &\in \mathcal{A} && \text{if } 2\alpha_i \equiv 1 \pmod{3}, \\ p_i &\in \mathcal{B} && \text{if } 2\alpha_i \equiv 2 \pmod{3}, \\ p_i &\in \mathcal{C} && \text{if } 2\alpha_i \equiv 0 \pmod{3}. \end{aligned} \quad (12.3)$$

Due to (12.3) we have the following two coprime square free positive integers:

$$A = \prod_{p_i \in \mathcal{A}} p_i, \quad B = \prod_{p_i \in \mathcal{B}} p_i. \quad (12.4)$$

Comparing (12.4) with (12.3) and (12.2), we find that the number $(2e)^2$ is presented as the product $(2e)^2 = A \cdot B^2 \cdot C^3$. Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore $\alpha_-(P_0^+) = A \cdot B^2$ as stated in Lemma 12.1.

If the point P is different from P_∞ and P_0^+ , we consider the coordinates of this point: $P = (x; y)$. Since P is a rational point, we have two irreducible fractions

$$x = \frac{m}{q_1}, \quad y = \frac{n}{q_2}. \quad (12.5)$$

Substituting the fractions (12.5) into the curve equation (10.1), we derive

$$\frac{m^3}{q_1^3} = \frac{n^2 - e^2 q_2^2}{q_2^2}. \quad (12.6)$$

Both sides of the equality (12.6) are irreducible fractions. Hence $q_1^3 = q_2^2$. From the equality $q_1^3 = q_2^2$ we derive that the numbers q_1 and q_2 are presented as

$$q_1 = q^2, \quad q_2 = q^3 \quad (12.7)$$

(compare with (8.5)). Applying (12.7) to (12.6), we obtain the equality

$$m^3 = (n - e q^3)(n + e q^3), \quad (12.8)$$

while the formulas (12.5) for the coordinates x and y turn to the following ones:

$$x = \frac{m}{q^2}, \quad y = \frac{n}{q^3}. \quad (12.9)$$

Now let's recall, the formula (10.8). Using (12.9), this formula yields

$$\alpha_-(P) = y - e = \frac{n - e q^3}{q^3}. \quad (12.10)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Hence we can write (12.10) as

$$\alpha_-(P) = s = n - e q^3. \quad (12.11)$$

Comparing (12.11) with (12.8), we obtain the following Diophantine equation

$$m^3 = s(s + 2e q^3). \quad (12.12)$$

The fractions (12.9) are irreducible. Therefore $\gcd(n, q) = 1$. Applying this equality to (12.11), we derive $\gcd(s, q) = 1$. Keeping in mind $\gcd(s, q) = 1$, let's calculate the greatest common divisor of two multiplicands s and $s + 2e q^3$ in the right hand side of the equality (12.12) and denote it through M :

$$M = \gcd(s, s + 2e q^3) = \gcd(s, 2e q^3) = \gcd(s, 2e). \quad (12.13)$$

From (12.13) it is clear that M is a divisor of the number $2e$.

Like in (12.2), let's consider the prime factor expansion of the number m from the left hand side of the equation (12.12):

$$m = \pm p_1^{\gamma_1} \cdot \dots \cdot p_\rho^{\gamma_\rho}. \quad (12.14)$$

If p_i in (12.14) is not a divisor of M in (12.13), then due to (12.12) either $p_i^{3\gamma_i}$ divides s or $p_i^{3\gamma_i}$ divides $s + 2e q^3$. The case where p_i is a divisor of M is more complicated. In this case $3\gamma_i = \alpha_i + \beta_i$, where $\alpha_i \neq 0$, $\beta_i \neq 0$, so that $p_i^{\alpha_i}$ divides s , and $p_i^{\beta_i}$ divides $s + 2e q^3$. Prime factors of this sort are grouped into three subsets:

$$\begin{aligned} p_i \in \mathcal{A} & \text{ if } \alpha_i \equiv 1 \pmod{3} \text{ and } \beta_i \equiv 2 \pmod{3}, \\ p_i \in \mathcal{B} & \text{ if } \alpha_i \equiv 2 \pmod{3} \text{ and } \beta_i \equiv 1 \pmod{3}, \\ p_i \in \mathcal{C} & \text{ if } \alpha_i \equiv 0 \pmod{3} \text{ and } \beta_i \equiv 0 \pmod{3}. \end{aligned} \quad (12.15)$$

Using (12.15), we define two coprime square free positive integer numbers:

$$A = \prod_{p_i \in \mathcal{A}} p_i, \quad B = \prod_{p_i \in \mathcal{B}} p_i. \quad (12.16)$$

From (12.15) and (12.16) we immediately derive $s = A \cdot B^2 \cdot C^3$. Cubic factors are

neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore we can write $\alpha_-(P) = s = A \cdot B^2$. The numbers A and B are divisors of M by construction, while M is a divisor of $2e$. Lemma 12.1 is proved.

Lemma 12.1 yields a very rough description of the set $\alpha_-(E(\mathbb{Q}))$. It can be refined in the following way.

Lemma 12.2. *An integer number $s = A \cdot B^2$, where A and B are two coprime square free positive integers dividing $2e$, represents an element of $\alpha_-(E(\mathbb{Q}))$ if and only if the following Diophantine equation has a non-trivial solution X, Y, Z :*

$$(A \cdot B^2) X^3 + (A^2 \cdot B) Y^3 + (2e) Z^3 = 0. \quad (12.17)$$

Proof. Necessity. If $s = \alpha_-(P_\infty) = 1$, then $A = 1$ and $B = 1$. In this case the equation (12.17) is solvable and $X = 1, Y = -1, Z = 0$ is its explicit solution.

If $s = \alpha_-(P_0^+)$, then, as we have seen in proving Lemma 12.1, $s = A \cdot B^2$, while $A \cdot B^2 \cdot C^3 = (2e)^2$. Multiplying both sides of the equality $A \cdot B^2 \cdot C^3 = (2e)^2$ by $A^2 \cdot B \cdot (2e)$, we derive the following equality:

$$(A^2 \cdot B) (2e)^3 = A^2 \cdot B \cdot (2e) \cdot A \cdot B^2 \cdot C^3 = (2e) (ABC)^3. \quad (12.18)$$

The equality (12.18) yields the solution of the Diophantine equation (12.17) with $X = 0, Y = 2e \neq 0, Z = -ABC$.

Now assume that $s = \alpha_-(P)$ for a rational point P of the curve (10.1) other than P_∞ and P_0^+ . As we have seen above in proving Lemma 12.1, in this case s is a solution of the equation (12.12) given by the formula

$$s = A \cdot B^2 \cdot C^3. \quad (12.19)$$

This formula is derived from (12.15) and (12.16). Similarly, from (12.15) and (12.16) one can derive the following formula for $s + 2eq^3$:

$$s + 2eq^3 = A^2 \cdot B \cdot D^3. \quad (12.20)$$

Subtracting (12.19) from (12.20), we obtain the equality

$$(A^2 \cdot B) D^3 - (A \cdot B^2) C^3 = (2e) q^3. \quad (12.21)$$

It is easy to see that the equality (12.21) yields the solution of the Diophantine equation (12.17) with $X = -C, Y = D, Z = -q \neq 0$.

Sufficiency. Assume that X, Y, Z are three integer numbers composing a non-trivial solution of the equation (12.17). If $Z = 0$, then $X \neq 0$ or $Y \neq 0$. In this case (12.17) reduces to $BX^3 + AY^3 = 0$. It yields the implications

$$\begin{aligned} X \neq 0 &\implies Y^3 = -\frac{B}{A} X^3 \implies Y \neq 0, \\ Y \neq 0 &\implies X^3 = -\frac{A}{B} Y^3 \implies X \neq 0. \end{aligned} \quad (12.22)$$

Using the equation $BX^3 + AY^3 = 0$ and taking into account the implications

(12.22), we can transform the formula $s = A \cdot B^2$ in the following way:

$$s = A \cdot B^2 = -\frac{Y^3}{X^3} B^3 = \left(-\frac{Y B}{X}\right)^3. \quad (12.23)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. The formula (12.23) means that $s = A \cdot B^2$ in this case is equivalent to $s = 1$, which is the value of the mapping α_- at the point $P = P_\infty$.

Now assume that $Z \neq 0$. If under this assumption $Y = 0$, then the equation (12.17) yields $X \neq 0$ and provides the following equalities:

$$s = A \cdot B^2 = -(2e) \frac{Z^3}{X^3}. \quad (12.24)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. The formula (12.24) means that $s = A \cdot B^2$ in this case is equivalent to $s = -2e$, which is the value of the mapping α_- at the point $P = P_0^-$.

The case $Z \neq 0$ and $X = 0$ is another option. In this case the equation (12.17) yields $Y \neq 0$ and provides the following equalities:

$$s = A \cdot B^2 = \frac{(A^2 \cdot B)^2}{A^3} = \frac{1}{A^3} \left(-2e \frac{Z^3}{Y^3}\right)^2 = \frac{1}{2e} \left(\frac{2e Z^2}{A Y^2}\right)^3. \quad (12.25)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. The formula (12.25) means that $s = A \cdot B^2$ in this case is equivalent to $s = 1/(2e)$, which is the value of the mapping α_- at the point $P = P_0^+$.

In the general case we have a solution of the equation (12.17) with $X \neq 0, Y \neq 0, Z \neq 0$. In this case we can write the equation (12.17) as follows:

$$(A^2 \cdot B) Y^3 = (A \cdot B^2) (-X)^3 + (2e) (-Z)^3. \quad (12.26)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore $s = A \cdot B^2$ is equivalent to $s = A \cdot B^2 \cdot (-X)^3$. For the sake of similarity to (12.12) let's denote $q = -Z$. As a result the above equality (12.26) turns to

$$(A^2 \cdot B) Y^3 = s + 2e q^3. \quad (12.27)$$

Multiplying both sides of (12.27) by $s = A \cdot B^2 \cdot (-X)^3$, we find that the product $s(s + 2e q^3)$ is an exact cube. Indeed, we have

$$s(s + 2e q^3) = (-A B X Y)^3. \quad (12.28)$$

Denoting $m = -A B X Y$ in (12.28), we obtain the equality coinciding with (12.12).

$$s(s + 2e q^3) = m^3. \quad (12.29)$$

The rest is to denote $n = s + e q^3$ and compose two fractions:

$$x = \frac{m}{q^2}, \quad y = \frac{n}{q^3}. \quad (12.30)$$

Due to (12.29) the number $n = s + e q^3$ satisfies the equation (12.8), while the values of the fractions (12.30) satisfy the curve equation (10.1). They define a rational point $P = (x; y)$ of this curve different from P_∞ , P_0^+ , and P_0^- . Applying the formula (10.8) to this point, we derive the formula for $\alpha_-(P)$:

$$\alpha_-(P) = y - e = \frac{n - e q^3}{q^3} = \frac{A \cdot B^2 \cdot (-X)^3}{(-Z)^3}. \quad (12.31)$$

Cubic factors are neglected modulo \mathbb{Q}^{*3} in $\mathbb{Q}^*/\mathbb{Q}^{*3}$. Therefore the formula (12.31) means that $s = A \cdot B^2$ is a value of the mapping α_- in the general case too. Lemma 12.2 is proved. \square

The mapping $\tilde{\alpha}_-$ is somewhat different from the mapping α_- . Its domain is the set of rational points of the second curve (10.2). In defining this mapping we replaced the field of rational numbers \mathbb{Q} by its algebraic extension $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. The following definitions are standard.

Definition 12.1. A polynomial of one variable is called monic if its leading coefficient is equal to unity: $f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$.

Definition 12.2. A number x from some extension of the field of rational numbers \mathbb{Q} is called algebraic if it is a root of some polynomial with rational coefficients.

Definition 12.3. An algebraic number x is called an algebraic integer if it is a root of some monic polynomial with integer coefficients.

Definition 12.4. An algebraic integer number x belonging to the number field $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ is called an Eisenstein integer (see [16]).

Eisenstein integers constitute a ring within the field $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$. We denote this ring through $\mathbb{Z}(\sqrt{-3})$. The ring of Eisenstein integers $\mathbb{Z}(\sqrt{-3})$ is an integral domain, i. e. it has no divisors of zero. The field $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$ coincides with the field of fractions for the ring $\mathbb{Z}(\sqrt{-3})$.

Definition 12.5. An algebraic integer number $x \in \mathbb{Z}(\sqrt{-3})$ is called invertible if its inverse element $x^{-1} = 1/x$ is also an algebraic integer, i. e. if $x^{-1} \in \mathbb{Z}(\sqrt{-3})$.

There are exactly six invertible elements in the ring of Eisenstein integers $\mathbb{Z}(\sqrt{-3})$:

$$\begin{aligned} \varepsilon &= \frac{1 + \sqrt{-3}}{2}, & \omega &= \frac{-1 + \sqrt{-3}}{2}, & -1, \\ \bar{\omega} &= \frac{-1 - \sqrt{-3}}{2}, & \bar{\varepsilon} &= \frac{1 - \sqrt{-3}}{2}, & 1. \end{aligned} \quad (12.32)$$

Here ε is an elementary sixth root of unity, while ω is an elementary cubic root of unity. The ring of regular integers \mathbb{Z} has only two invertible elements: 1 and -1 .

Eisenstein integers from the ring $\mathbb{Z}(\sqrt{-3})$ constitute a two-dimensional grid. Indeed, each element $x \in \mathbb{Z}(\sqrt{-3})$ is presented as

$$x = u + v\varepsilon, \quad \text{where } u \in \mathbb{Z}, v \in \mathbb{Z}, \quad (12.33)$$

and where ε is taken from (12.32). The formula (12.33) is similar to (10.34).

Definition 12.6. An algebraic integer number x from the ring of Eisenstein integers $\mathbb{Z}(\sqrt{-3})$ is called prime if it is non-invertible and if it cannot be presented as a product of two other non-invertible algebraic integers from this ring.

It is very important that the ring of Eisenstein integers $\mathbb{Z}(\sqrt{-3})$ is a Euclidean domain (see [16]), where the norm of the number (12.33) is given by the formula

$$|u + v\varepsilon|^2 = u^2 + uv + v^2.$$

Each Euclidean domain is a unique factorization domain. When applied to the ring of Eisenstein integers, this means that each Eisenstein integer $x \in \mathbb{Z}(\sqrt{-3})$ has an expansion into the product of Eisenstein primes:

$$x = p_1 \cdot \dots \cdot p_r \tag{12.34}$$

The expansion (12.34) is unique up to the order of multiplicands and up to multiplying the prime numbers p_1, \dots, p_r by invertible elements (12.32). Due to expansions of the form (12.34) one can formulate two lemmas similar to Lemma 12.1 and Lemma 12.2.

Lemma 12.3. *Let \tilde{P} be a rational point of the curve (10.2). Then $\tilde{\alpha}_-(\tilde{P})$ is presented by some Eisenstein integer $s = \eta \cdot A \cdot B^2$, where A and B are two nonzero coprime square free Eisenstein integers being divisors of the number $6\sqrt{-3}e$ and where η is one of the three invertible Eisenstein integers $1, \varepsilon, \omega$ from (12.32).*

Lemma 12.4. *An Eisenstein integer number $s = \eta \cdot A \cdot B^2$, where A and B are two nonzero coprime square free Eisenstein integers being divisors of $6\sqrt{-3}e$ and where η is one of the three invertible Eisenstein integers $1, \varepsilon, \omega$ from (12.32), represents an element of $\tilde{\alpha}_-(\tilde{E}(\mathbb{Q}))$ if and only if the homogeneous cubic equation*

$$(\eta \cdot A \cdot B^2) X^3 + (\eta^{-1} \cdot A^2 \cdot B) Y^3 + (6\sqrt{-3}e) Z^3 = 0 \tag{12.35}$$

has a non-trivial solution X, Y, Z in $\mathbb{Z}(\sqrt{-3})$ such that if $Z \neq 0$, then the values of the following two fractions are regular rational numbers:

$$x = \frac{-ABXY}{Z^2}, \quad y = \frac{(\eta \cdot A \cdot B^2) X^3 + (3\sqrt{-3}e) Z^3}{Z^3}.$$

Note that the number $6\sqrt{-3}$ used in (12.35) and in the statements of the above lemmas belongs to the ring of Eisenstein integers $\mathbb{Z}(\sqrt{-3})$. Indeed, we have the following presentation of the form (12.33) for this number:

$$6\sqrt{-3} = -6 + 12\varepsilon.$$

As for the proofs of Lemma 12.3 and Lemma 12.4, they use almost the same arguments as the proofs of Lemma 12.1 and Lemma 12.2.

13. CONCLUSIONS.

Elliptic curves (1.1) brought to the form (2.2) are associated with perfect cuboids. Potentially they could be used in finding an example of such a cuboid or in proving their non-existence. Therefore our further efforts will be directed to describing

rational points of these curves by some formula or, which is more likely, to evaluating them numerically. Computing the ranks of the curves is the first step in this direction. For the case where $4R^2N$ in (2.2) is an exact cube the rank problem is already solved by Theorem 5.7 within the 2-descent method.

The case where $4R^2N$ is not an exact cube is more complicated. In this case the formulas (11.9) and Lemmas 12.1, 12.2, 12.3, 12.4 obtained within the 3-descent method could be a background for some numerical algorithm. Building such an algorithm and analyzing its output is a subject for a separate article.

14. ACKNOWLEDGMENTS.

We are grateful to Sonic86 who gave us the reference to [7] on e-science.ru forum.

REFERENCES

1. Sharipov R. A., *A note on rational and elliptic curves associated with the cuboid factor equations*, e-print arXiv:1209.5706 in Electronic Archive <http://arXiv.org>.
2. *Elliptic curve*, Wikipedia, Wikimedia Foundation Inc., San Francisco, USA.
3. Nagell T., *Sur les propriétés arithmétiques des cubiques planes du premier genre*, Acta Math. **52** (1929), no. 1, 93–126; see <http://link.springer.com/article/10.1007/BF02592681>.
4. Connell I., *Elliptic curve handbook*, McGill University, Montreal, 1999; see <http://www.math.mcgill.ca/connell>.
5. *Mordell-Weil theorem*, Wikipedia, Wikimedia Foundation Inc., San Francisco, USA.
6. Husemöller D., *Elliptic curves*, Springer Verlag, 2004.
7. Daems J., *A cyclotomic proof of Catalan's Conjecture*, Master's thesis in mathematics, Leiden University, Netherlands, 2003; see <http://www.math.leidenuniv.nl/~jdaems>.
8. *Isogeny*, Wikipedia, Wikimedia Foundation Inc., San Francisco, USA.
9. *Dual abelian variety*, Wikipedia, Wikimedia Foundation Inc., San Francisco, USA.
10. Van der Waerden B. L., *Algebra*, Vol. 1, Springer Verlag, 1971.
11. *Rational root theorem*, Wikipedia, the Free Encyclopedia, Wikimedia Foundation Inc., San Francisco, USA.
12. Fueter R., *Über kubische diophantische Gleichungen*, Commentarii Math. Helvet. **2** (1930), 69–89; see <http://retro.seals.ch/digbib/view?rid=comahe-001:1930:2::10>.
13. Podsypanin V. D., *On the indeterminate equation $x^3 = y^2 + Az^6$* , Mat. Sbornik **24** (1949), no. 3, 391–403; see http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=sm&paperid=5986&option_lang=eng.
14. Mordell L. J., *Diophantine equations*, Academic Press, London and New York, 1969.
15. Cohen H., Pazuki F., *Elementary 3-descent with a 3-isogeny*, e-print arXiv:0903.4963 in Electronic Archive <http://arXiv.org>.
16. *Eisenstein integer*, Wikipedia, Wikimedia Foundation Inc., San Francisco, USA.

SAMSUNG LTD., ST. JOHN'S HOUSE, CAMBRIDGE, CB4 0ZT, UK
E-mail address: jhnrmsdn@yahoo.co.uk

BASHKIR STATE UNIVERSITY, 32 ZAKI VALIDI STREET, 450074 UFA, RUSSIA
E-mail address: r-sharipov@mail.ru