Solving Cubic Equations in Two Variables

BERND KREUSSLER

Abstract. After recalling a geometric construction of all Pythagorean triples of integers, the same idea is applied to find rational solutions of cubic equations in two variables. This leads to the definition of the Mordell–Weil group. The final section collects some of the basic properties of this group.

1. Pythagoras

The aim of this introductory section is to recall the well-known geometric construction of all Pythagorean triples of integers. Three integers $a, b, c \in \mathbb{Z}$ form a *Pythagorean triple*, if

$$a^2 + b^2 = c^2.$$

Almost everybody knows the Pythagorean triple $(3, 4, 5)$ and many know $(5, 12, 13)$. However, not everybody has come across $(8, 15, 17)$ or $(20, 21, 29)$.

Clearly, if $n \in \mathbb{Z}$ and (a, b, c) is such a triple, (na, nb, nc) will also be one. In this way, starting with the well known triple $(3, 4, 5)$ we obtain $(6, 8, 10)$, $(-3, -4, -5)$, $(12, 16, 20)$ etc.

Note that a prime number which divides two of the three integers in a Pythagorean triple automatically divides the third in the triple. Therefore, it is enough to find all Pythagorean triples in which any two of the three integers are co-prime. We shall call such a Pythagorean triple *reduced*. Because the only Pythagorean triple with $c = 0$ is $(a, b, c) = (0, 0, 0)$, we shall assume in the sequel $c \neq 0$. This allows us to introduce the new variables

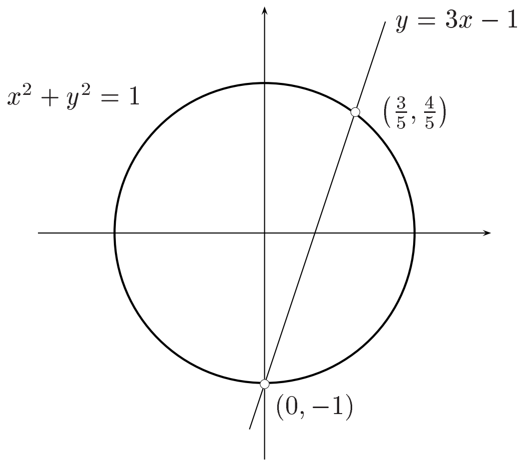
$$x = \frac{a}{c} \quad \text{and} \quad y = \frac{b}{c}.$$

Using these coordinates, the search for reduced Pythagorean triples translates into the problem to find all *rational* solutions of the equation

$$x^2 + y^2 = 1.$$

In other words, we would like to find all points on the unit circle whose coordinates are rational.

The key observation is that a line which connects two points with rational coordinates always has a rational slope. Therefore, we shall look at all lines in the plane which pass through the point $(0, -1)$ and which have rational slope $r \in \mathbb{Q}$.



Such a line is given by the equation $y = rx - 1$. Therefore, the x-coordinates of the two intersection points of this line with the unit circle satisfy the equation $x^2 + (rx - 1)^2 = 1$, which is equivalent to $x\left((r^2 + 1)x - 2r\right) = 0$. The solution $x = 0$ corresponds to the point $(0, -1)$. The second intersection point has coordinates

$$x = \frac{2r}{r^2 + 1} \quad \text{and} \quad y = \frac{r^2 - 1}{r^2 + 1}.$$

The map which sends $r \in \mathbb{Q}$ to the point $\left(\frac{2r}{r^2+1}, \frac{r^2-1}{r^2+1}\right)$ on the unit circle gives a parametrisation of the set of all rational points on this curve. This completely solves our problem.

If we wish to derive a complete description of all Pythagorean triples of integers, we start by writing the slope r as $r = \frac{u}{v}$ with coprime integers u, v. Using symmetry, we may assume $r > 1$. More precisely, switching from r to $-r$ corresponds to a sign change of x, whereas a sign change of y is achieved by switching from r to $\frac{1}{r}$. Thus, we assume $u > v > 0$ and u, v co-prime. Under these assumptions, $r = \frac{u}{v}$ produces the point with coordinates

$$x = \frac{2r}{r^2+1} = \frac{2uv}{u^2+v^2} \quad \text{and} \quad y = \frac{r^2-1}{r^2+1} = \frac{u^2-v^2}{u^2+v^2}.$$

Now it is not hard to see that each reduced Pythagorean triples in which a is odd can be written as

$$(a,b,c) = \left(uv, \frac{u^2-v^2}{2}, \frac{u^2+v^2}{2}\right)$$

with $u > v > 0$, both odd and co-prime. Up to interchanging a and b this gives us all reduced Pythagorean triples, because a and b are co-prime, hence at least one of these to integers is odd. For small values of u, v we obtain the following table

u	v	a	b	c
3	1	3	4	5
5	1	5	12	13
5	3	15	8	17
7	1	7	24	25
7	3	21	20	29

u	v	a	b	c
7	5	35	12	37
9	1	9	40	41
9	3	27	36	45
9	5	45	28	53
9	7	63	16	65

2. A CUBIC EXAMPLE

The aim of this section is to find integer solutions of cubic equations by using the geometric idea used in the previous section. We shall explain this method through the following example

$$b^2c = 4a^3 - 4ac^2 + c^3.$$

As before, we assume $c \neq 0$ and introduce new coordinates $x = \frac{a}{c}$ and $y = \frac{b}{c}$ in which the above equation becomes

$$y^2 = 4x^3 - 4x + 1. \tag{1}$$

This can be rewritten as

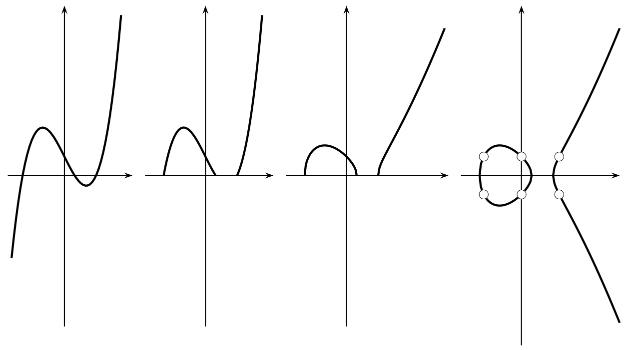
$$(y-1)(y+1) = 4(x+1)x(x-1).$$

In this form it is obvious that we have the following six solutions

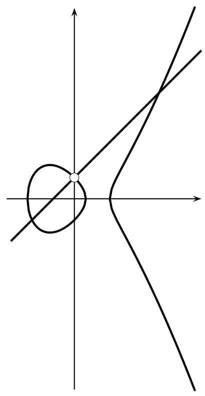
$$(-1, \pm 1),\ (0, \pm 1),\ (1, \pm 1).$$

Question: Are these all the solutions of equation (1)?

It is not hard to produce a sketch of this curve in the real plane. This can be done through the following step-by-step approach. First, we draw the graph of the cubic polynomial $4x^3 - 4x + 1$. The intersection points with the x-axis can be found with Cardano's formula. This polynomial has three real roots because its discriminant is positive. To get the second picture, we remove all points from the graph which have negative y-coordinate. The next picture is produced by applying the square root function. Finally, the cubic curve is obtained by adding in the mirror image along the x-axis, because (x, y) is on this curve if and only if $(x, -y)$ is so.



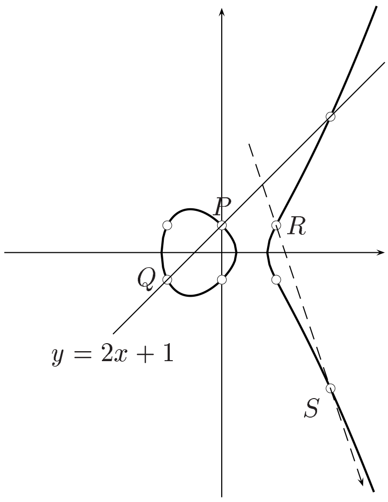
The six marked points in the picture are the points we found before. If we seek to find more rational points on this curve, we may try to use lines with rational slope which pass through one of the known points. This leads to a quadratic equation the solutions of which correspond to two further intersection points of this line with the curve given by equation (1).



For example, the line with slope 1 which passes through the point $(0,1)$ has the equation $y = x+1$. The x-coordinates of its intersection with our curve are the solutions of the equation $(x+1)^2 = 4x^3-4x+1$ or equivalently $4x^3 - x^2 - 6x = 0$. The known solution corresponds to the factor x of this polynomial. The two new intersection points correspond to the solutions of the quadratic equation $4x^2-x-6 = 0$, these are the irrational numbers $\frac{1\pm\sqrt{97}}{8}$.

This example shows that we should allow for one new point only. In other words, we should work with a line connecting two of the known points.

Example 1. Let us see how this works with $P = (0,1)$ and $Q = (-1,-1)$. The line which connects these two points is given by the equation $y = 2x+1$. Substituting this into equation (1) gives $4x^3 - 4x^2 - 8x = 0$. The two points we started with give us two of the roots of this polynomial, namely $x_1 = 0$ and $x_2 = -1$. Now, it is not hard to see that $4x^3 - 4x^2 - 8x = 4x(x+1)(x-2)$. Hence $x_3 = 2$ is the third solution which corresponds to the point $(2,5)$ on our curve. We can even produce another new point, because the given equation does not change when we replace y by $-y$. This gives the point $S = (2,-5)$.



Example 2. We may now continue by using the line through $P = (0,1)$ and $S = (2,-5)$. Its equation is $y = -3x+1$. Therefore, we look at $4x^3 - (-3x+1)^2 - 4x + 1$ which has to be equal to

$4x(x-2)(x-x_3)$. Comparing the coefficients of x^2 of these two polynomials leads to the equation $-9 = -4(2+x_3)$. This gives $x_3 = \frac{1}{4}$. The new points we obtain are $\left(\frac{1}{4}, \pm\frac{1}{4}\right)$.

In general, if we are using a line with slope $r \in \mathbb{Q}$ which passes through two points on our curve whose x-coordinates are x_1 and x_2, we obtain the x-coordinate of the third point by comparing the coefficients of x^2 as above. The result will be $x_3 = \frac{r^2}{4} - x_1 - x_2 \in \mathbb{Q}$.

We may also use other points from the six found originally.

Example 3. The line connecting $S = (2,-5)$ with $R = (1,1)$ has the equation $y = -6x + 7$. This gives a new point with coordinate $x_3 = 9 - 2 - 1 = 6$ and $y_3 = -6x_3 + 7 = -29$. So we have two new points $(6,-29)$ and $(6,29)$ which are not visible in the picture.

Note that we obtained $(6,29)$ as follows. First we connected $P = (0,1)$ and $Q = (-1,-1)$ by a line, whose third point of intersection with the cubic curve had $(2,-5)$ as its mirror image relative to the x-axis. Then we connected $(2,-5)$ and $R = (1,1)$ by a line and obtained $(6,29)$ as the mirror image of the third point of intersection. It is interesting to see what happens if we carry out these steps in another order. Let us first connect $Q = (-1,-1)$ and $R = (1,1)$ by a line, reflect the third point on this line on the x-axis and connect this point in the second step with $P = (0,1)$.

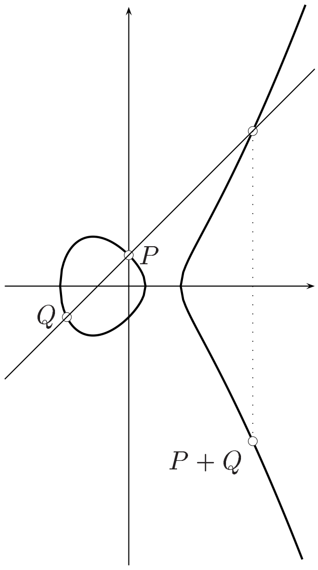
Example 4. The line which connects $Q = (-1,-1)$ and $R = (1,1)$ has the equation $y = x$. This line has $\left(\frac{1}{4}, \frac{1}{4}\right)$ as its third point of intersection with the curve given by equation (1). Therefore, we shall connect its mirror image $\left(\frac{1}{4}, -\frac{1}{4}\right)$ with $P = (0,1)$. The corresponding line has the equation $y = -5x + 1$. The new point produced this way is $(6,-29)$, the same as we obtained in Example 3.

This coincidence is not an accident. It is in fact a special case of a theorem from projective geometry which states that a cubic curve (in projective space) which passes through eight of the nine intersection points of two other cubics, must also contain the ninth of these intersection points.

A closer look at examples 3 and 4 suggest that we are dealing here with a kind of *associativity*. This can indeed be made precise by the following definition.

Definition 5. Let P, Q be points on the cubic curve given by equation (1). We define $P + Q$ to be the mirror image (relative to the

x-axis) of the third point of intersection of the line which connects P and Q and the cubic curve.

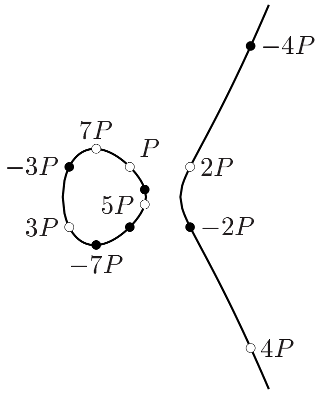


In this language, we have shown above $(P+Q)+R = P+(Q+R)$ where $P = (0,1)$, $Q = (-1,-1)$ and $R = (1,1)$. This definition also extends to give $P + P$, which is obtained by using the *tangent line* to our curve at P.

Example 6. Implicit differentiation reveals that the tangent line to our curve at $P = (0,1)$ has slope equal to -2. Therefore, this line is given by the equation $y = -2x + 1$. In the same way as before, we substitute $y = -2x + 1$ into equation (1) and use the fact that $x = 0$ will be a double root of the cubic equation so obtained. Then, we get that the x-coordinate of the new point of intersection is equal to $x = 1$. This produces the known points $(1, \pm 1)$.

This example shows that we actually need to know only one rational point on our cubic in order to get started. As before, we can then produce many other points. Using the notation suggested by Definition 5, we obtain here:

$$P = (0,1), \qquad 2P = (1,1), \qquad 3P = (-1,-1),$$
$$4P = (2,-5), \qquad 5P = \left(\frac{1}{4}, \frac{1}{4}\right), \qquad 6P = (6,29).$$



We shall see in the next section that this is in fact the structure of an Abelian group in which for each point T, $-T$ is the mirror image of T with respect to the x-axis. The line which connects an arbitrary point T on our cubic with its mirror image $-T$ is a vertical line. Because $T+(-T)=0$, we expect all these lines to go through the neutral element of this group. Therefore, we shall look for the neutral element "at infinity". This can be made more precise with the aid of the projective plane $\mathbb{P}^2$, introduced in the following section.

3. The complete picture

In order to see all points on our cubic curve we have to return to the original equation $b^2c = 4a^3 - 4ac^2 + c^3$. The key observation is here that (a,b,c) is a solution of this equation if and only if $(\lambda a, \lambda b, \lambda c)$ is a solution for all numbers λ. This means that the solution set is a union of lines which pass through the origin. When we switched to coordinates (x,y) in the previous two sections, we agreed that it is sufficient to know one point on each of these lines. But we missed those lines on which $c=0$ due to our division by c. If we would like to keep these lines as well, we arrive at the idea of the projective plane. Set theoretically, the projective plane is defined to be the set of all lines in three-space which pass through the origin. This leads to the following useful description.

Before we proceed we need to fix our notion of "number". So far, we have dealt with rational numbers and integers. But in general it is much easier and more convenient to work with an algebraically closed field like the field $\mathbb{C}$ of complex numbers. Many things which will be said below are true for any field $\mathbb{K}$. Therefore, we shall formulate the next definition for any field $\mathbb{K}$. The reader who is not familiar with the concept of a field may substitute $\mathbb{Q}$ or $\mathbb{C}$ for $\mathbb{K}$.

Definition 7. The projective plane $\mathbb{P}^2(\mathbb{K})$ over the field $\mathbb{K}$ is the set of all equivalence classes $(z_0 : z_1 : z_2)$ of non-zero vectors $(z_0, z_1, z_2) \in \mathbb{K}^3$. Two such vectors (z_0, z_1, z_2) and (w_0, w_1, w_2) are equivalent if and only if there exits a non-zero $\lambda \in \mathbb{K}$ such that $(z_0, z_1, z_2) = \lambda(w_0, w_1, w_2)$. This implies

$$(z_0 : z_1 : z_2) = (\lambda z_0 : \lambda z_1 : \lambda z_2) \quad \text{for all} \quad \lambda \neq 0.$$

The notation $(z_0 : z_1 : z_2)$ for the equivalence class of the vector (z_0, z_1, z_2) is chosen in order to suggest that we are dealing with the ratios between the three numbers z_0, z_1 and z_2 only. A similar construction, of course, can be carried out in any dimension to produce $\mathbb{P}^n(\mathbb{K})$ for all $n \geq 1$. The one-dimensional case is particularly easy. If $\mathbb{K} = \mathbb{C}$ it leads to the Riemannian sphere. Notations used for the Riemannian sphere are $S^2 = \mathbb{C} \cup \infty = \overline{\mathbb{C}}$ and $\mathbb{P}^1(\mathbb{C})$, the notation we are going to use here. Its points are equivalence classes $(z_0 : z_1)$ of non-zero vectors $(z_0, z_1) \in \mathbb{C}^2$. All points in $\mathbb{P}^1(\mathbb{C})$ with $z_0 = 0$ are equivalent to $\infty = (0 : 1)$. Any point with $z_0 \neq 0$ is equivalent to $(1 : z)$ where $z = \frac{z_1}{z_0}$. This gives a bijection between $\mathbb{C}$ and $\mathbb{P}^1(\mathbb{C}) \setminus \{\infty\}$. A neighbourhood of ∞ would be the set of all those points of $\mathbb{P}^1(\mathbb{C})$ which have $z_1 \neq 0$. This is again in bijection with $\mathbb{C}$ by using $w = \frac{z_0}{z_1}$. The relationship between these two patches of $\mathbb{P}^1(\mathbb{C})$ is given by $w = \frac{1}{z}$. This actually makes $\mathbb{P}^1(\mathbb{C})$ into a complex manifold of dimension one, the simplest compact Riemann surface.

The local structure of $\mathbb{P}^2(\mathbb{K})$ can be studied in a similar way. To this end, we define the three basic open sets which cover $\mathbb{P}^2(\mathbb{K})$ completely

$$\begin{aligned}
U_0 &:= \{(z_0 : z_1 : z_2) \mid z_0 \neq 0\} \subset \mathbb{P}^2(\mathbb{K}) \\
U_1 &:= \{(z_0 : z_1 : z_2) \mid z_1 \neq 0\} \subset \mathbb{P}^2(\mathbb{K}) \\
U_2 &:= \{(z_0 : z_1 : z_2) \mid z_2 \neq 0\} \subset \mathbb{P}^2(\mathbb{K}).
\end{aligned}$$

Each of these sets is in bijection with $\mathbb{K}^2$. For example, the map $U_0 \to \mathbb{K}^2$ given by $(z_0 : z_1 : z_2) \mapsto \left(\frac{z_1}{z_0}, \frac{z_2}{z_0}\right)$ has as its inverse the map $\mathbb{K}^2 \to U_0$ which sends (ξ_1, ξ_2) to $(1 : \xi_1 : \xi_2)$.

Similarly, on U_1 we can work with affine coordinates $\eta_j = \frac{z_j}{z_1}$, $j = 0, 2$ and on U_2 we have $\zeta_k = \frac{z_k}{z_2}$, $k = 0, 1$. The gluing maps between these three $\mathbb{K}^2$ are given by

$$\xi_1 = \frac{1}{\eta_0} = \frac{\zeta_1}{\zeta_0} \qquad \xi_2 = \frac{\eta_2}{\eta_0} = \frac{1}{\zeta_0}$$
$$\eta_0 = \frac{1}{\xi_1} = \frac{\zeta_0}{\zeta_1} \qquad \eta_2 = \frac{\xi_2}{\xi_1} = \frac{1}{\zeta_1}$$
$$\zeta_0 = \frac{1}{\xi_2} = \frac{\eta_0}{\eta_2} \qquad \zeta_1 = \frac{\xi_1}{\xi_2} = \frac{1}{\eta_2}.$$

If $\mathbb{K} = \mathbb{C}$ this defines the structure of a two dimensional complex manifold on $\mathbb{P}^2(\mathbb{C})$.

Let us apply this new language to the cubic equation $b^2c = 4a^3 - 4ac^2 + c^3$ studied in the previous section. As we have seen above, if we identify (a, b, c) with $(z_0, z_1, z_2) \in \mathbb{Q}^3$, the set of all solutions of this cubic equation is a well defined subset $E(\mathbb{Q}) \subset \mathbb{P}^2(\mathbb{Q})$. Our assumption $c \neq 0$ means that we restricted our attention to the set U_2. The complement of U_2 is the set of all those points which have $z_2 = 0$. These are the points of the form $(z_0 : z_1 : 0)$, hence the complement of U_2 in $\mathbb{P}^2(\mathbb{K})$ is in bijection with $\mathbb{P}^1(\mathbb{K})$. Therefore, we call

$$L_2 = \{(z_0 : z_1 : 0) \mid (z_0 : z_1) \in \mathbb{P}^1(\mathbb{K})\} \subset \mathbb{P}^2(\mathbb{K})$$

the *line at infinity*. In a similar way we may define lines at infinity L_0 and L_1 which are the complements of U_0 and U_1 respectively.

In order to see what we missed when restricting to U_2 we simply set $c = 0$ in our cubic equation. This leaves us with the equation $0 = 4a^3$. Therefore, the only point missed is the point $O = (0 : 1 : 0) \in L_2 \subset \mathbb{P}^2(\mathbb{Q})$. In order to see how $E(\mathbb{Q})$ looks like around this point, we restrict our attention to the set U_1. Using the coordinates (η_0, η_2) introduced above, $E(\mathbb{Q})$ is described by the equation

$$\eta_2 = 4\eta_0^3 - 4\eta_0\eta_2^2 + \eta_2^3.$$

The line at infinity L_2 intersects U_1 at the η_0-axis, given by the equation $\eta_2 = 0$. This line is a tangent line to the cubic curve with a triple contact at the point $O = (0, 0)$. The point O is an inflection point of our curve.

The main result of the previous section was that we introduced an "addition" of points in $E(\mathbb{Q})$ by the rule that $P + Q + R = O$ if and only if the three points P, Q, R are collinear. Therefore, we need to understand lines in the projective plane. These are given by linear equations. In general, a line in $\mathbb{P}^2(\mathbb{K})$ is the set of all solutions of an equation of the form

$$l_0 z_0 + l_1 z_1 + l_2 z_2 = 0$$

with $l_0, l_1, l_2 \in \mathbb{K}$ but not all three equal to zero. Because $\lambda l_0, \lambda l_1, \lambda l_2$ define the same line in $\mathbb{P}^2(\mathbb{K})$ if $\lambda \neq 0$, the set of all lines in $\mathbb{P}^2(\mathbb{K})$ is another $\mathbb{P}^2(\mathbb{K})$, called the *dual projective plane* and sometimes denoted $\mathbb{P}^2(\mathbb{K})^\vee$.

Each line in $\mathbb{P}^2(\mathbb{K})$ is isomorphic to $\mathbb{P}^1(\mathbb{K})$. The three lines at infinity introduced before are also lines in this sense, because L_j was given by the equation $z_j = 0$. In particular, the line L_2 corresponds to the point $(0:0:1) \in \mathbb{P}^2(\mathbb{K})^\vee$. Any other line, with coefficients $(0:0:1) \neq (l_0:l_1:l_2) \in \mathbb{P}^2(\mathbb{K})^\vee$ intersects U_2 in an ordinary line. The equation of this intersection is

$$l_0 x + l_1 y = -l_2$$

where we used $x = \frac{a}{c}, y = \frac{b}{c}$ instead of $\zeta_0 = \frac{z_0}{z_2}, \zeta_1 = \frac{z_1}{z_2}$ as coordinates on U_2. If $l_1 \neq 0$, this can be rewritten as $y = rx + s$ with $r = -\frac{l_0}{l_1}$ and $s = -\frac{l_2}{l_1}$. If, however, $l_1 = 0$ the equation becomes $l_0 x = -l_2$ and this defines a vertical line which intersects the x-axis at $-\frac{l_2}{l_1}$.

On the other hand, the point $O = (0:1:0)$ is on the line given by $l_0 z_0 + l_1 z_1 + l_2 z_2 = 0$ if and only if $l_1 = 0$. Hence, the vertical lines in U_2 correspond precisely to those lines in $\mathbb{P}^2(\mathbb{K})$ which pass through O and are different from L_2. Therefore, the point at infinity O is the correct choice for the neutral element of the group structure on $E(\mathbb{Q})$ and reflection at the x-axis corresponds to taking the additive inverse of a point.

With some background in projective geometry or by other means it can be shown that the addition of points on $E(\mathbb{Q})$ introduced in the previous section equips $E(\mathbb{Q})$ with the structure of an Abelian group. More about projective geometry and a geometric proof can be found in the article by M. Khalid [11].

Theorem 8. *$E(\mathbb{Q})$ is an Abelian group with neutral element O, its only point at infinity. The group structure is determined by saying that $P+Q+R=O$ if and only if P, Q and R are on a line in $\mathbb{P}^2(\mathbb{Q})$. This implies that $-P$ is obtained from P by changing the sign of the y-coordinate.*

Remark 9. This result is true for any field $\mathbb{K}$ and any cubic equation of the form

$$z_1^2 z_2 = z_0^3 + p z_0 z_2^2 + q z_2^3 \tag{2}$$

with $p, q \in \mathbb{K}$ satisfying $\Delta = -16(4p^3 + 27q^2) \neq 0$. If the characteristic of $\mathbb{K}$ is not equal to two or three (i.e. if $1+1 \neq 0$ and $1+1+1 \neq 0$ in $\mathbb{K}$), every regular cubic with a point over $\mathbb{K}$ can be given by such an equation. When working in characteristic zero (e.g. $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{C}$), we can change coordinates so that (2) becomes

$$z_1^2 z_2 = 4z_0^3 - g_2 z_0 z_2^2 - g_3 z_2^3. \tag{3}$$

The discriminant of such an equation is $\Delta = g_2^3 - 27g_3^2$. A cubic equation of the form (3) is called a *Weierstraß* equation, named after Karl Weierstraß (1815–1897). The coefficient 4 at z_0^3 is used because it appears in the differential equation of the Weierstraß $\wp$-function. (See the article by M. Franz [5].)

The most basic structure result about the group $E(\mathbb{Q})$ was shown in 1922 by Mordell [17].

Theorem 10 (Mordell)**.** *If E is given by (2) with $p, q \in \mathbb{Q}$ and $4p^3 + 27q^2 \neq 0$ then the Abelian group $E(\mathbb{Q})$ is finitely generated.*

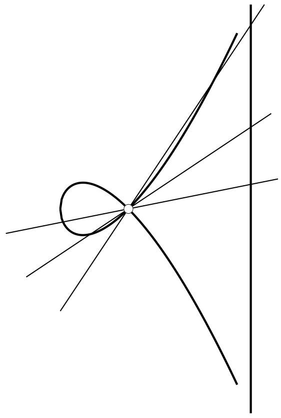
Remark 11. Theorem 10 has been generalised by A. Weil to Abelian varieties of arbitrary dimension over any number field [23]. Therefore Mordell's Theorem is also known as the Mordell–Weil Theorem and the group $E(\mathbb{Q})$ is sometimes called the Mordell–Weil group.

The curve studied in section 2 has $E(\mathbb{Q}) \cong \mathbb{Z}$ with generator $P = (0, 1)$. The discriminant of this curve is $\Delta = 37$.

Remark 12. The assumption $4p^3 + 27q^2 \neq 0$ in Mordell's Theorem is crucial. If $4p^3 + 27q^2 = 0$ the cubic polynomial $x^3 + px + q$ has a multiple root and this gives rise to a singular point on the cubic curve given by (2). This changes the situation completely, because singular cubics are rational. More explicitly, suppose $-4p^3 = 27q^2$ and $p, q \in \mathbb{Q} \setminus \{0\}$. A straightforward calculation shows that, under these assumptions,

$$x^3 + px + q = \left(x - \frac{3q}{p}\right)\left(x + \frac{3q}{2p}\right)^2.$$

This implies that $\left(-\frac{3q}{2p}, 0\right)$ is a singular point of the cubic which means that each line in $\mathbb{P}^2(\mathbb{Q})$ that passes through this point will have at most one other intersection point with the cubic curve (2). Just as in the case of the circle in section 1 this produces a bijection between $\mathbb{Q}$ (the set of slopes) and all rational points on a singular cubic apart from the singular point. This shows that the non-singular rational points on a singular cubic form a group which is not finitely generated.



Example 13. Look at the singular cubic $z_1^2 z_2 = 4z_0^3 - 3z_0 z_2^2 + z_2^3$, which has discriminant $\Delta = 3^3 - 27(-1)^2 = 0$. On U_2, using coordinates x, y as before, its equation is

$$y^2 = 4x^3 - 3x + 1.$$

From $4x^3 - 3x + 1 = (x+1)(2x-1)^2$ we see that the singular point has coordinates $\left(\frac{1}{2}, 0\right)$. Any line with rational slope r through this point will have equation $y = r\left(x - \frac{1}{2}\right)$, hence the new intersection point will be found by solving $\left(\frac{r}{2}\right)^2 (2x-1)^2 = (x+1)(2x-1)^2$. Therefore, the coordinates of this point are given by

$$x = \frac{r^2 - 4}{4} \quad \text{and} \quad y = \frac{r^3 - 6r}{4}.$$

The main difference between this and the non-singular case is that we cannot find such a closed formula for all rational solutions in the non-singular case. This is explained by the involvement of transcendental functions such as theta functions and the Weierstraß $\wp$-function (see the article [5]).

4. Further results

In this section we collect some general results known about the Mordell–Weil group $E(\mathbb{Q})$. We also discuss several normal forms of plane cubic curves.

Let us look at a cubic curve given by an equation of the form

$$y^2 = x^3 + px + q \qquad \text{with} \qquad 4p^3 + 27q^2 \neq 0. \tag{4}$$

Such an equation is also called a Weierstraß equation or Weierstraß canonical form. However, as we shall see below, it is not canonical. To determine this we need to decide whether it is possible that two curves given by a Weierstraß equation with different (p, q) can be transformed into each other by a linear transformation of coordinates. Consider the following.

Given two curves $y^2 = x^3 + px + q$ and $\widetilde{y}^2 = \widetilde{x}^3 + \widetilde{p}\widetilde{x} + \widetilde{q}$ with $p, q, \widetilde{p}, \widetilde{q} \in \mathbb{Q}$, the only possible linear transformations of coordinates with rational coefficients which transform one of these equations into the other are of the form $\widetilde{x} = \lambda^2 x, \widetilde{y} = \lambda^3 y$ with $\lambda \in \mathbb{Q} \setminus \{0\}$. Such a transform is successful if and only if we have $\widetilde{p} = \lambda^4 p$ and $\widetilde{q} = \lambda^6 q$. This can be used, in particular, to obtain *integer* coefficients $p, q \in \mathbb{Z}$. Therefore, the following result is useful in broader generality than it first may seem.

Theorem 14 (Siegel, [20, 16, 18])**.** *The equation $y^2 = x^3 + px + q$ with $p, q \in \mathbb{Z}$ has only finitely many solutions $(x, y) \in \mathbb{Z}^2$, provided that $4p^3 + 27q^2 \neq 0$.*

A point $P \in E(\mathbb{Q})$ is called a *torsion point* if there exists a positive integer $n \in \mathbb{Z}$ such that $nP = O$ in the additive group $E(\mathbb{Q})$. In other words, the torsion points of $E(\mathbb{Q})$ are precisely the points of finite order in the group $E(\mathbb{Q})$. They form the *torsion subgroup* $E(\mathbb{Q})_{\mathrm{tor}} \subset E(\mathbb{Q})$. For example, if the curve is given by a Weierstraß equation, the two-torsion points in $E(\mathbb{Q})$, i.e. the points $P \in E(\mathbb{Q})$ with $2P = O$, are precisely the intersection points of the curve E with the x-axis (and the point O). The example studied in section 2 did not have any two-torsion points apart from O, as the cubic equation $4x^3 - 4x + 1 = 0$ does not have a rational root. The following result sheds some light on the torsion subgroup more generally.

Theorem 15 (Lutz–Nagell, [13, 19])**.** *All torsion points of $y^2 = x^3 + px + q$ with $p, q \in \mathbb{Z}$ have integer coordinates $(x, y) \in \mathbb{Z}^2$, provided*

$4p^3 + 27q^2 \neq 0$. Moreover, if $(x, y) \in E(\mathbb{Q})_{tor}$ then either $y = 0$ or y^2 divides $4p^3 + 27q^2$.

Together with Siegel's Theorem this implies that $E(\mathbb{Q})_{\mathrm{tor}}$ is finite. This, however, is already a consequence of Mordell's Theorem, because every finitely generated Abelian group G is isomorphic to

$$\mathbb{Z}^r \times \underbrace{\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \ldots \times \mathbb{Z}/a_{s-1}\mathbb{Z} \times \mathbb{Z}/a_s\mathbb{Z}}_{G_{\mathrm{tor}}}$$

with positive integers a_i. The number $r \geq 0$ is called the rank of this group. The possibilities for the rank of $E(\mathbb{Q})$ are not yet known, but it is conjectured that there exist cubic curves for which the rank of $E(\mathbb{Q})$ is as large as you want. The largest known rank at the moment seems to be 28, attained by an example found by N. Elkies in 2006.

On the other hand, the torsion subgroup of $E(\mathbb{Q})$ is much better understood. The main result is the following.

Theorem 16 (Mazur, [14, 15])**.** *If $E(\mathbb{Q})$ is given by the equation $y^2 = x^3 + px + q$ with $p, q \in \mathbb{Q}$ and $4p^3 + 27q^2 \neq 0$, then its torsion subgroup $E(\mathbb{Q})_{tor}$ is isomorphic to one of the fifteen groups in the following list:*

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10, \ \textit{or} \ \ n = 12,$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

All these groups in fact occur as torsion subgroups.

Remark 17. This result is in sharp contrast to the situation over an algebraically closed field. If $\mathbb{K}$ is an algebraically closed field whose characteristic does not divide the positive integer m, then the m-torsion subgroup of $E(\mathbb{K})$, which consists of all the elements of $E(\mathbb{K})$ killed by m, is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. In the case $\mathbb{K} = \mathbb{C}$ this will be explained in the article of M. Khalid [11].

Example 18. Because $9 = 8 + 1$, it is not so hard to discover that $P = (2, 3)$ is an element of $E(\mathbb{Q})$, the solution set of the equation $y^2 = x^3 + 1$. The tangent line at P to this cubic curve has equation $y = 2x-1$. If we substitute this into $y^2 = x^3+1$ we obtain $(2x-1)^2 = x^3+1$ or equivalently $0 = x^3-4x^2+4x = x(x-2)^2$. This means that this tangent line intersects the cubic at the new point $(0, -1)$, hence $2P = (0, 1)$. To find $3P$, we use the line which connects $P = (2, 3)$ and $2P = (0, 1)$. It has the equation $y = x+1$ and intersects the cubic at $3P = (-1, 0)$. This point is on the x-axis, so it is a two-torsion point. This implies $6P = O$ and we obtain $4P = -2P = (0, -1)$ and $5P = -P = (2, -3)$. In fact, $E(\mathbb{Q})$ consists of the six points kP, $k = 0, 1, 2, 3, 4, 5$ only, i.e. $E(\mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z}$. In [21] and [7] examples of cubic equations which realise all the other $E(\mathbb{Q})_{\mathrm{tor}}$ can be found.

The Tate canonical form, see (7) below, is very useful in the study of cubics whose Mordell–Weil group has torsion. More precisely, every cubic curve which has at least one point $P \in E(\mathbb{Q})_{\mathrm{tor}}$ of order at least four (i.e. $P \neq O$, $2P \neq O$ and $3P \neq O$) can be brought into Tate canonical form. For example, if $b = 1$ and $c = d$ in (7), it can be shown that the point $(0 : 0 : 1)$ is a point of order four.

A useful method which allows us to gain information about $E(\mathbb{Q})$ is *reduction modulo a prime number p*. This means that one studies solutions of a given cubic equation with coordinates in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. These solutions form the group $E(\mathbb{F}_p)$. An interesting result in this context says that for each prime $p > 2$ which does not divide the discriminant Δ, the map which reduces the coordinates of a torsion point $P \in E(\mathbb{Q})$ modulo p embeds $E(\mathbb{Q})_{\mathrm{tor}}$ as a subgroup into $E(\mathbb{F}_p)$. This can be used to determine the group $E(\mathbb{Q})_{\mathrm{tor}}$. More on the issue of calculating the torsion subgroup of $E(\mathbb{Q})$ can be found for example in [22], [10] and [6].

Example 19. Let us show that $E(\mathbb{Q})_{\mathrm{tor}} = \{O\}$ for the cubic $y^2 = 4x^3 - 4x + 1$ studied in the previous section. The idea is to calculate $E(\mathbb{F}_3)$ and $E(\mathbb{F}_5)$ and show that these groups are of co-prime order. This is sufficient because 3 and 5 do not divide the discriminant $\Delta = 37$ of this cubic. If we reduce the equation $y^2 = 4x^3 - 4x + 1$ modulo 3 we obtain $y^2 = x^3 - x + 1$. Because $x^3 - x = x(x-1)(x+1)$ is equal to zero for all $x \in \mathbb{F}_3$, we see that $(0, \pm 1), (1, \pm 1), (2, \pm 1)$ are the only solutions of this equation with coefficients in the finite field $\mathbb{F}_3$. Therefore, $E(\mathbb{F}_3) = \{O, (0, \pm 1), (1, \pm 1), (2, \pm 1)\}$ is of order 7. Reducing the equation $y^2 = 4x^3 - 4x + 1$ modulo 5 gives $y^2 = -x^3 + x + 1$. Its solutions over $\mathbb{F}_5$ are $(0, \pm 1), (\pm 1, \pm 1)$ and $(2, 0)$. This means that $E(\mathbb{F}_5)$ is a group of order 8. Because $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to a sub-group of $E(\mathbb{F}_3)$ and of $E(\mathbb{F}_5)$, it must be trivial.

More generally, solutions in all finite fields of fixed characteristic p can be studied. If the number of solutions for such finite fields are put together in a kind of generating function, the so-called *zeta-function* is obtained. Lack of space forces us to skip the fascinating theory of zeta-functions of elliptic curves, the Weil conjectures and their proof by Deligne and, last but not least, the Birch and

Swinnerton-Dyer conjecture which is one of the millennium prize problems, a solution of which is worth one million US-Dollars (see http://www.claymath.org/millennium/). A starting point for the interested reader could be [12], [7] or [21]. We confine ourselves to look at Weierstraß equations and other canonical forms over more general fields $\mathbb{K}$ for the rest of this article.

There are several ways to proceed. One possibility would be to introduce the abstract notion of a smooth projective curve of arithmetic genus 1, defined over the field $\mathbb{K}$. If such a curve has a point with coordinates in $\mathbb{K}$, it is possible to show that the curve is isomorphic to a plane cubic curve which has an inflection point at $O = (0 : 1 : 0)$. In particular, if $\mathbb{K}$ is algebraically closed, such a point always exists. However, even in the case $\mathbb{K} = \mathbb{Q}$ an equation like $3z_0^3 + 4z_1^3 + 5z_2^3 = 0$ does not have a single point in $\mathbb{P}^2(\mathbb{K})$. Of course, we shall not proceed along these lines. The interested reader is referred to standard textbooks on algebraic geometry, such as [8].

We shall assume that we have a cubic equation $f(z_0, z_1, z_2) = 0$ which defines a plane cubic curve with at least one point in $\mathbb{P}^2(\mathbb{K})$. Let us first try to see whether any such curve can be described by a Weierstraß equation, whereby we allow linear transformations of coordinates only. The key to making progress is to understand inflection points. It is not hard to show that a point $P \in E(\mathbb{K})$ is an inflection point if and only if it is on the zero set of the *Hessian* of the cubic polynomial f. By definition, the Hessian of f is the determinant of the 3×3–matrix formed by the second partial derivatives of f. This is again a cubic polynomial and Bézout's Theorem implies that there are at most 9 inflection points (with coordinates in the algebraic closure of $\mathbb{K}$). As we have seen earlier, the only point at infinity O of a curve, which is given by a Weierstraß equation, is an inflection point. Therefore, a necessary condition for a cubic to be transformable to a Weierstraß equation is that at least one of the inflection points is defined over $\mathbb{K}$. Let us assume such a point exists on our curve. By a linear transformation of coordinates with coefficients in $\mathbb{K}$ we can arrange that this inflection point has coordinates $(0 : 1 : 0)$ and the tangent line to the curve at this point is the line at infinity with equation $z_2 = 0$. Under these assumptions and using coordinates x, y on $U_2 \subset \mathbb{P}^2(\mathbb{K})$, it is clear that the cubic equation is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

In order to simplify the left hand side to y^2 we have to complete the square, which means that $y + \frac{a_1x+a_3}{2}$ is going to be the new y-coordinate. This obviously requires that we are able to divide by 2 which is possible in full generality only if the characteristic of $\mathbb{K}$ is not equal to 2. On the other hand, in order to absorb the term a_2x^2 on the right hand side we complete the cube. This is possible in general only if the characteristic of $\mathbb{K}$ is not equal to 3. As a result we obtain that any non-singular cubic with an inflection point in $\mathbb{P}^2(\mathbb{K})$ can be given by a Weierstraß equation if the characteristic of $\mathbb{K}$ is not equal to 2 or 3. Moreover, if the characteristic of $\mathbb{K}$ is not equal to 2, we can easily switch between (2) and (3), both are known as the Weierstraß canonical form in the literature.

It seems that the Weierstraß canonical form is the most widely known one. There are other canonical forms for cubic equations, each of which has its own advantages. Usually, it is only possible to achieve such a canonical form under some additional assumptions.

These are the *Legendre canonical form* (Adrien Marie Legendre, 1752–1833)

$$z_1^2z_2 = z_0(z_0 - z_2)(z_0 - \lambda z_2), \tag{5}$$

the *Hesse canonical form* (Ludwig Otto Hesse, 1811–1874)

$$z_0^3 + z_1^3 + z_2^3 + tz_0z_1z_2 = 0 \tag{6}$$

and the *Tate canonical form* (John Tate, 1925–)

$$z_1^2z_2 + bz_0z_1z_2 + cz_1z_2^2 = z_0^3 + dz_0^2z_2. \tag{7}$$

If the cubic is given by (5) or (7), the only point at infinity will again be the inflection point $O = (0 : 1 : 0)$. Therefore, we may also consider

$$y^2 = x(x-1)(x-\lambda)$$

as the Legendre canonical form and

$$y^2 + bxy + cy = x^3 + dx^2$$

as the Tate canonical form.

The Tate canonical form can be achieved for a cubic curve which has at least one point of finite order $n > 3$. So, it is not a general normal form for all cubics but it is very useful in order to find the torsion subgroup of $E(\mathbb{K})$.

The Legendre canonical form exhibits our curve as a double cover of the projective line $\mathbb{P}^1$. This branched double cover is given by the map which forgets the y-coordinate (or z_1 in the projective setting).

The map so defined can be extended to a map which is also defined at the point O at infinity. It has four branch points, namely O and the three points given by the roots of the right hand side, these are $(0:0:1), (1:0:1)$ and $(\lambda:0:1)$. These four points are precisely the 2-torsion points of $E(\mathbb{K})$, i.e. those points P which satisfy $P+P=O$. This shows that only those cubic curves which have four 2-torsion points with coordinates in the field $\mathbb{K}$ can be transformed into a Legendre canonical form. In particular, if $\mathbb{K}=\mathbb{C}$ or any other algebraically closed field of characteristic not equal to two, this is always possible.

On the other hand, an equation in Hesse normal form does not have triple contact with the line at infinity. If the field $\mathbb{K}$ contains three cubic roots of unity (e.g. $\mathbb{K}=\mathbb{C}$), it has three points at infinity, namely the solutions of $z_0^3+z_1^3=0$. These are inflection points of the cubic. If $\mathbb{K}=\mathbb{Q}$, for example, we see only one of them; this is the point $(1:-1:0)$. This point is available over any field $\mathbb{K}$ and can be taken as the origin for the group structure. Then, the set of three-torsion points is precisely the set of inflection points of this cubic. In particular, if $\mathbb{K}$ contains three cubic roots of unity, the cubic contains nine three-torsion points which lie on the three coordinate lines $z_i=0$.

The configuration of these nine points was studied by O. Hesse [9] who found that the nine inflection points lie on 12 lines, each of which contains three of these points. Each of the nine points is contained in four of the 12 lines. This set of nine points and 12 lines is now called the Hesse configuration. A recent survey on the Hesse configuration and an application to the study of examples of K3-surfaces can be found in [1].

Finally, let us mention that it is not hard to give an explicit formula for the group structure on $E(\mathbb{Q})$ if the curve is given in Weierstaß canonical form $y^2=x^3+px+q$. For example, if $P=(x_1,y_1)$ and $Q=(x_2,y_2)\neq -P$, the point $P+Q=(x_3,y_3)$ has coordinates

$$
\begin{aligned}
x_3 &= \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2 \\
y_3 &= -\left(\frac{y_2-y_1}{x_2-x_1}\right) x_3 - \frac{y_1x_2-y_2x_1}{x_2-x_1}.
\end{aligned}
$$

This can be obtained using precisely the same calculations as in our examples in section 2. Remarkably, this formula does not depend on p, q, which is due to the non-presence of x^2 in the Weierstraß canonical form. However, p, q explicitly appear in the formula which describes the coordinates of $2P$. For each normal form such a formula can be obtained.

A formula which is impressive because of its beauty and simplicity is obtained when we start with an equation of the following form

$$x^2 + y^2 = a^2 + a^2x^2y^2.$$

If $P = (x, y)$ and $P' = (x', y')$ are two solutions of this equation, the group structure on the solution set is given by

$$P + P' = \frac{1}{a} \cdot \left(\frac{xy' + yx'}{1 + xyx'y'}, \frac{yy' - xx'}{1 - xyx'y'} \right).$$

The point $O = (0, a)$ is easily seen to be the neutral element of this group. More on this formula can be found in the recent article [3].

Because the given equation is of degree four, it is not clear how this example fits into the theory explained so far. That the solution set of this equation indeed forms a Mordell–Weil group can be explained using projective geometry. The basic idea is to show that, apart from a small number of points, the curve defined by this equation of degree four is isomorphic to a plane cubic curve.

The given curve of degree four has two singular points at infinity, namely $(1 : 0 : 0)$ and $(0 : 1 : 0)$. If $a^5 \neq a$ the curve has no other singular point. We are going to show explicitly that a non-singular version of this curve is the plane cubic given by the equation

$$y^2 = x\left(x + \frac{1 - a^2}{1 + a^2}\right)\left(x + \frac{1 + a^2}{1 - a^2}\right). \tag{8}$$

The outline of the construction is the following. We construct a non-singular version of the degree 4 curve which is embedded in projective three-space in such a way that a certain projection from a centre outside this non-singular curve maps it to the original degree 4 curve. We then find another projection whose centre is on this non-singular curve in three-space and which maps it isomorphically onto the plane cubic given by equation (8).

More specifically, using coordinates $(w : x : y : z)$ in $\mathbb{P}^3$, we define the curve $\widetilde{E}$ in $\mathbb{P}^3$ by the two simultaneous quadratic equations

$$\begin{aligned} xy - wz &= 0 \\ y^2 - a^2w^2 + x^2 - a^2z^2 &= 0. \end{aligned}$$

The projection with centre $(1:0:0:0)$ is the map which sends a point $(w:x:y:z) \in \mathbb{P}^3$ to the point $(x:y:z) \in \mathbb{P}^2$. This projection is not defined at the point $(1:0:0:0)$. All other points on the line in $\mathbb{P}^3$ through $(1:0:0:0)$ and $(0:x:y:z)$ are sent to the same point $(x:y:z) \in \mathbb{P}^2$. Because the line through $(1:0:0:0)$ and $(0:x:y:z)$ meets the curve $\widetilde{E}$ precisely when $z^2(x^2+y^2) = a^2z^4 + a^2x^2y^2$, the image of this projection is the plane curve of degree four given by this equation. Moreover, such a line has more than one intersection point with $\widetilde{E}$ if and only if it passes trough $(0:1:0:0)$ or $(0:0:1:0)$. Therefore, away from the two singular points we obtain an isomorphism between $\widetilde{E}$ and the image curve in $\mathbb{P}^2$.

The point $(0:0:-a:1)$ is on the curve $\widetilde{E}$. The projection with centre $(0:0:-a:1)$ is a map from $\mathbb{P}^3 \setminus \{(0:0:-a:1)\}$ to $\mathbb{P}^2$. It extends to a map which is defined on all of $\widetilde{E}$ and defines an isomorphism between $\widetilde{E}$ and its image curve in $\mathbb{P}^2$, which can be given by the cubic equation (8). The point on the curve $\widetilde{E} \subset \mathbb{P}^3$ which corresponds to the neutral element $O = (0, a)$, is the point $(0:0:a:1)$. The second projection sends this point to our usual neutral element $(0:1:0) \in \mathbb{P}^2$ at infinity. We leave the details of the calculations to the interested reader.

References

[1] M. Artebani, I. Dolgachev, *The Hesse pencil of plane cubic curves*, arXiv:math.AG/0611590

[2] J.W.S. Cassels, *Diophantine equations with special reference to elliptic curves.* J. Lond. Math. Soc. 41, 193–291 (1966); Corrigenda. Ibid. 42, 183 (1967)

[3] H.M. Edwards, *A normal form for elliptic curves.* Bull. Amer. Math. Soc. 44, 393–422 (2007)

[4] T. Ekedahl, *One semester of elliptic curves.* EMS Series of Lectures in Mathematics, European Mathematical Society Publishing House. (2006)

[5] M. Franz, *Theta Functions*, this issue.

[6] I. García-Selfa, M. A. Olalla, J. M. Tornero, *Computing the rational torsion of an elliptic curve using Tate normal form.* J. Number Theory 96, No. 1, 76–88 (2002)

[7] R.V. Gurjar et al., *Elliptic curves.* Praveshika Series. New Delhi: Narosa Publishing House/dist. by the AMS (2006)

[8] R. Hartshorne, *Algebraic geometry.* Graduate Texts in Mathematics 52, Springer (1977)

[9] O. Hesse, *Über die Wendepuncte der Curven dritter Ordnung.* J. Reine Angew. Math. 28, 97–107 (1844)

[10] D.H. Husemoller, *Elliptic curves.* Graduate Texts in Mathematics 111, Springer (1987)
[11] M. Khalid, *Group law on the cubic curve*, this issue.
[12] F. Kirwan, *Comples Algebraic Curves.* London Mathematical Society Study Texts 23, Cambridge University Press (1992)
[13] E. Lutz, *Sur l'équation* $y^2 = x^3 - Ax - B$ *dans les corps* $\mathfrak{p}$*-adiques.* J. reine angew. Math. 177, 238–247 (1937)
[14] B. Mazur, *Modular curves and the Eisenstein ideal.* Publ. Math., Inst. Hautes Étud. Sci. 47, 33–186 (1977)
[15] B. Mazur, *Rational isogenies of prime degree. (With an appendix by D. Goldfeld).* Invent. Math. 44, 129–162 (1978)
[16] L.J. Mordell, *Note on the integer solutions of the equation* $Ey^2 = Ax^3 + Bx^2 + Cx + D$.. Messenger (2) 51, 169–171 (1921)
[17] L.J. Mordell, O*n the rational solutions of the indeterminate equations of the third and fourth degrees.* Cambr. Phil. Soc. Proc. 21, 179–192 (1922)
[18] L.J. Mordell, *On the integer solutions of the equation* $ey^2 = ax^3 + bx^2 + cx + d$. Lond. M. S. Proc. (2) 21, 415–419 (1923)
[19] T. Nagell, *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre.* Wid. Akad. Skrifter Oslo 1935, Nr. 1, 25 p (1935)
[20] C.L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n+1} + \cdots + k$. (Extract from a letter to Prof. L. J. Mordell.) Journal L. M. S. 1, 66–68 (1926)
[21] J.H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics 106, Springer (1986)
[22] J.T. Tate, *The arithmetic of elliptic curves.* Invent. Math. 23, 179–206 (1974)
[23] A. Weil, *Sur un théorème de Mordell.* Bulletin Sc. math. (2) 54, 182–191 (1930)

Bernd Kreussler,
Mary Immaculate College,
South Circular Road,
Limerick, Ireland
bernd.kreussler@mic.ul.ie

Received in final form on 23 August 2007.