ON TORSION POINTS ON AN ELLIPTIC CURVES VIA DIVISION POLYNOMIALS

by Maciej Ulas

Abstract. In this note we propose a new way to prove Nagel’s classical theorem \[3\] about torsion points on an elliptic curve over \(\mathbb{Q}\). In order to prove it, we use basic properties of division polynomials only.

1. Introduction. Let \(a, b \in \mathbb{Z}\) and let us consider the plane curve \(E\) given by

\[ E : y^2 = x^3 + ax + b. \]

Such a curve is called elliptic if \(4a^3 + 27b^2 \neq 0\). This condition states that the polynomial \(x^3 + ax + b\) has simple roots only, or equivalently, that curve \([1]\) is non-singular.

A point \((x, y)\) on \(E\) is called a rational (integral) point if its coordinates \(x\) and \(y\) are in \(\mathbb{Q}\) (in \(\mathbb{Z}\)).

As we know, the set \(E(\mathbb{Q})\) of all rational points on \(E\) plus the so-called point at infinity \(\{O\}\) may be considered as an abelian group with neutral element \(O\). Points of finite order in this group form the subgroup \(\text{Tors } E(\mathbb{Q})\) called the torsion part of the curve \(E\).

The famous Mordell Theorem states that the group \(E(\mathbb{Q})\) is finitely generated. Therefore, there exists an \(r \in \mathbb{N}\) such that

\[ E(\mathbb{Q}) \cong \mathbb{Z}^r \times \text{Tors } E(\mathbb{Q}). \]

Nagell in 1935 and Lutz two years later proved that torsion points on curve \([1]\) have integer coordinates. Nagell’s argument is based on the observation that if the denominator \(p\) of the \(x\)-coordinate of an elliptic curve’s point \(P\) is

2000 Mathematics Subject Classification. Primary 11G05, 14H52.
Key words and phrases. Elliptic curves, torsion points, division polynomials.
greater than 1, then the denominator \( q \) of the \( x \)-coordinate of \( 2P \) is greater then \( p \). Our proof is based on a different idea.

Now let us inductively define the so-called division polynomials \( \psi_m \in \mathbb{Z}[x,y] \), which are used to express coordinates of the point \( mP \) in terms of coordinates of a point \( P \):

\[
\begin{align*}
\psi_1 &= 1, \quad \psi_2 = 2y, \\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2, \\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3), \\
\psi_{2m+1} &= \psi_{m+2}\psi_m - \psi_{m-1}\psi_{m+1}, \quad m \geq 2, \\
2y\psi_{2m} &= \psi_m(\psi_{m+2}\psi_{m-1} - \psi_{m-2}\psi_{m+1}), \quad m \geq 3.
\end{align*}
\]

It is easy to observe that \( \psi_{2m} \) are polynomials indeed. Now we define polynomials \( \phi_m \) and \( \omega_m \) in the following way

\[
\begin{align*}
\phi_m &= x\psi_{2m}^2 - \psi_{m-1}\psi_{m+1}, \\
4y\omega_m &= \psi_{m+2}\psi_{m-1} - \psi_{m-2}\psi_{m+1}.
\end{align*}
\]

Most useful properties of division polynomials are summarized in the following theorem.

**Theorem 1.1.** Let \( m \in \mathbb{N}_+ \). Then

1. \( \psi_m, \phi_m, y^{-1}\omega_m \) for \( m \) odd and \( (2y)^{-1}\psi_m \), \( \phi_m, \omega_m \) for \( m \) even are polynomials in \( \mathbb{Z}[x,y^2] \). Substituting \( y^2 = x^3 + ax + b \), we may consider them as polynomials in \( \mathbb{Z}[x] \).

2. Considering \( \psi_m \) and \( \phi_m \) as polynomials in \( x \) there is

\[
\begin{align*}
\phi_m(x) &= x^{m^2} + \text{lower degree terms}, \\
\psi_{2m}^2(x) &= m^2x^{m^2-1} + \text{lower degree terms}.
\end{align*}
\]

3. If \( P \in E(\mathbb{Q}) \), then

\[
mP = \left( \frac{\phi_m(P)}{\psi_{2m}^2(P)}, \frac{\omega_m(P)}{\psi_{m+1}^3(P)} \right).
\]

We here omit a proof of this theorem. Assertions 1 and 2 are easy to prove by induction, but involve rather long calculations. It is possible to prove assertion 3 in an elementary way; however, it involves extensive computer calculations. Other proofs, using more advanced methods, can be found in [1] and [2].
2. Points of finite order are integral. Before proving that points of finite and positive orders on an elliptic curve are integral, we will prove two useful lemmas. If $p$ is a prime, we write $p^a || s$ if $p^a | s$ and $p^{a+1} \nmid s$.

Lemma 2.1. If $(x_0, y_0)$ is a rational point on an elliptic curve $E: y^2 = x^3 + ax + b$, then $x_0 = u/t^2$ and $y_0 = v/t^3$ for some integers $u$, $v$, $t$ with $\text{GCD}(uv, t) = 1$.

Proof. We write $x_0 = u/s$ and $y_0 = v/r$ with $\text{GCD}(u, s) = 1$ and $\text{GCD}(v, r) = 1$. Inserting this into $y^2 = x^3 + ax + b$ we get
\[ s^3v^2 = r^2(u^3 + aus^2 + bs^3). \]
If $p^e || s$ then $p^{3e} || s^3v^2$. Since $p \nmid u$ and $p | aus^2 + bs^2$, it follows that $p^{3e} || r^2$. No higher power of $p$ can divide $r^2$; otherwise $p | v$, contrary to the assumption that $\text{GCD}(v, r) = 1$. Hence, $p^{3e} || r^2$. If $p^f || r$, then it follows that $3e = 2f$, so $f = 3g$ and $e = 2g$ for some integer $g$. Thus, $p^{3g} || r$ and $p^{2g} || s$. Since this holds for each prime $p$, we conclude that $s = t^2$ and $r = t^3$ for some integer $t$.

Lemma 2.2. Let $E$ be an elliptic curve. If $P = (x, y) \in E(\mathbb{Q})$ and $mP$ is an integral point for some $m \in \mathbb{Z}$ then the point $P$ is integral.

Proof. By Theorem 1.1 there is
\[ mP = (X, Y) = \left( \frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(P)}{\psi_m(P)^3} \right). \]
Hence,
\[ (3) \quad X\psi_m(x)^2 = \phi_m(x). \]
Now let $x = u/t^2$, where $\text{GCD}(u, t) = 1$, and define
\[ \Phi_m(u, t) := u^m + t^{2m-2}\left(\phi_m(x) - x^m\right), \]
\[ (4) \quad \Psi_m(u, t) := t^{2m-2}\psi_m(x)^2. \]
Since
\[ \phi_m(z) = z^m + \text{lower order terms}, \]
\[ \psi_m^2(z) = m^2z^{m-1} + \text{lower order terms}, \]
the functions $\Phi_m(u, t)$, $\Psi_m(u, t)$ are polynomials in $\mathbb{Z}[u, t]$.
Combining (3) and (4), we obtain
\[ (5) \quad t^2(X\Psi_m(u, t) - \Phi_m(u, t) + u^m) = u^m \]
and therefore, \( t^2 \mid u^{m^2} \). But \( \gcd(u, t) = 1 \), hence \( t = \pm 1 \), so the point \( P \) is integral.

Let us remind the formula for doubling a point \( P = (x, y) \) on the curve (1) which says that

\[
2P = \left( \left( \frac{3x^2 + a}{2y} \right)^2 - 2x, -y + \left( \frac{3x^2 + a}{2y} \right) \left( 3x - \left( \frac{3x^2 + a}{2y} \right)^2 \right) \right).
\]

Our aim is to give a proof of the following theorem.

**Theorem 2.3.** Let \( a, b \in \mathbb{Z} \) and \( E : y^2 = x^3 + ax + b \) be an elliptic curve. If \( P = (x, y) \in E(\mathbb{Q}) \) is a non-zero torsion point, then \( P \) is integral.

**Proof.** Note that we may restrict ourselves to torsion points of prime order.

Indeed, let us assume that the theorem is true for such points. Now if \( Q \) is a point of a finite order \( n \) where \( n \) is not prime, then \( n = qr \) where \( q \) is prime and \( r \) is an integer \( > 1 \). Therefore, \( q(rQ) = nQ = O \). From the assumption we conclude that the point \( rQ \) is integral. Thus the point \( Q \) is integral due to Lemma 2.2.

Let us suppose that the point \( P \) is of prime order \( q \).

(i) If \( q = 2 \), then \( 2P = O \), i.e., \( P = -P \). Hence \( x^3 + ax + b = 0 \). We know from Lemma 2.1 that \( x = u/t^2 \) for some \( u, t \in \mathbb{Z} \) and \( \gcd(u, t) = 1 \), so we obtain

\[
u^3 = -t^4(au + bt^2).
\]

Therefore, \( t^4 \mid u^3 \) and \( \gcd(u, t) = 1 \), hence \( t = \pm 1 \) and \( P \) is integral.

(ii) Now let \( q > 2 \). Again, from Lemma 2.1 follows that \( x = u/t^2 \) for some \( u, t \in \mathbb{Z} \) and \( \gcd(u, t) = 1 \). Since \( qP = O \), then \( (q-1)P = -P \). Therefore,

\[
t^2\phi_{q-1}(x) = u\psi_{q-1}(x)^2,
\]

where polynomials \( \phi_{q-1}, \psi_{q-1} \) are as in Theorem 1.1. For a prime \( q > 2 \) let us define polynomials

\[
\Psi_{q-1}(u, t) := t^{2(q-1)^2-4}(\psi_{q-1}(x))^2 - (q-1)^2x(q-1)^2-1),
\]

\[
\Phi_{q-1}(u, t) := t^{2(q-1)^2-2}(\phi_{q-1}(x) - x(q-1)^2).
\]

Note that, due to Theorem 1.1 polynomials 8 have integer coefficients and thus are in \( \mathbb{Z}[u, t] \).
Inserting \( t^2 x = u \) into (8), we obtain:

\[
\begin{align*}
\Phi_{q-1}(x) &= t^2 \Phi_{q-1}(u, t) + u^{(q-1)^2}, \\
(9) &
\end{align*}
\]

Now combining (7) and (9) we get

\[
\begin{align*}
\Phi_{q-1}(u, t) &= \Phi_{q-1}(u, t) + u^{(q-1)^2}, \\
(10) &
\end{align*}
\]

or

\[
\begin{align*}
\Phi_{q-1}(u, t) &= \Phi_{q-1}(u, t) + u^{(q-1)^2}, \\
(11) &
\end{align*}
\]

Since GCD\((u, t) = 1\), we conclude that

\[
\begin{align*}
\Phi_{q-2}(x) &= \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} - 2x, \\
(12) &
\end{align*}
\]

or, equivalently,

\[
\begin{align*}
4\Phi_{q-2}(x)(x^3 + ax + b) &= (x^4 - 2ax^2 - 8bx + a^2)\psi_{q-2}(x)^2. \\
\end{align*}
\]

Inserting \( x = u/t^2 \) and using (8) we get

\[
\begin{align*}
4(u^{(q-2)^2} + t^2 \Phi_{q-2}(u, t))(u^3 + aut^4 + bt^6) &= ((q - 2)^2 u^{(q-2)^2 - 1} + t^2 \Psi_{q-2}(u, t)), \\
(13) &
\end{align*}
\]

where \( H(u, t) \in \mathbb{Z}[u, t] \). Since GCD\((u, t) = 1\), it means that

\[
\begin{align*}
n^2 \mid q(q - 4). \\
(\ast) &
\end{align*}
\]

We have shown that \( n^2 \mid q(q - 2) \) and \( n^2 \mid q(q - 4) \), where \( n \) is an integer and \( q \) is a prime \( > 3 \). Hence, \( n^2 \mid 2 \), so \( n = \pm 1 \). Therefore, the point \( P \) is integral as we claimed. \( \square \)

Acknowledgments. I would like to thank the referee for his valuable comments and Professor K. Rusek for helping me in preparing this paper.
References


Received November 18, 2004

Jagiellonian University
Institute of Mathematics
ul. Reymonta 4
30-059 Kraków
Poland
e-mail: Maciej.Ulas@im.uj.edu.pl