Notes written by Michał Zając

Theorem 1 *Let $C(x,y,z)$ be a homogeneous cubic polynomial over a field $\mathbb{K}$ and $l_1, l_2, l_3, m_1, m_2, m_3$ be lines in $\mathbb{P}^2(\mathbb{K})$ with P_{ij} as intersection points between l_i and m_j. Furthermore, let $l_i \neq m_j$ for all i, j. We assume that $P_{ij} \in C$ for $(i,j) \neq (3,3)$ and that if there is i such that two or more among P_{i1}, P_{i2}, P_{i3} are equal then $l_i \cap C$ has order $\geqslant 2$ and similarly if there is j such that two or more among P_{1j}, P_{2j}, P_{3j} are equal then $m_j \cap C$ has order $\geqslant 2$. Then $P_{33} \in C$.*

Proof The proof begins with writing l_1 in parametric form, i.e.

$$l_1 = \begin{cases} x = a_0 u + b_0 v \\ y = a_1 u + b_1 v \\ z = a_2 u + b_2 v. \end{cases}$$

and thus $C(x,y,z)$ becomes $\tilde{C}(u,v)$. For $i = 1,2,3$, $\tilde{C}(u_i, v_i) = 0$. Write $m_j = a_j x + b_j y + c_j z$. Before the proof is continued, we will need the following lemma:

Lemma 1 *Let $R(u,v)$ and $S(u,v)$ be homogeneous polynomial of degree 3, with $S(u,v) \neq 0$. For $i = 1,2,3$ let $S(u_i, v_i) = R(u_i, v_i) = 0$. Let for some k $(v_i u - u_i v)^k | R$ and $(v_i u - u_i v)^k | S$. Then there is $\alpha \in \mathbb{K}$ such that $R = \alpha S$.*

Proof Proof skipped.

We describe a line l_1 with a linear equation: $l_1(x,y,z) = ax + by + cz = 0$. Assuming that $a \neq 0$, line l_1 can be parametrised such that:

$$l_1 = \begin{cases} x = \dfrac{-b}{a} u - \dfrac{c}{a} v \\ y = u \\ z = v. \end{cases} \tag{1}$$

$\tilde{C} = \alpha \tilde{m}_1 \tilde{m}_2 \tilde{m}_3$. We define C_1 as

$$C_1(x,y,z) = C(x,y,z) - \alpha(\tilde{m}_1 \tilde{m}_2 \tilde{m}_3)(x,y,z) \tag{2}$$
$$= a_3(y,z)(ax + by + cz)^3 + \ldots + a_0(y,z) \tag{3}$$

Where the last equality comes from the following:

$$x^n = \frac{1}{a^n}(ax + by + cz) - (by + cz)^n = \frac{1}{a^n}(ax + by + cz)^n + \ldots.$$

By composing equations 1 and 2 we get $\tilde{C}_0(u,v) = a_0(u,v)$, hence $a_0(u,v)$ is the zero polynomial. Furthermore from 2 $C_1(x,y,z)$ is multiple of $l_1(x,y,z)$.

Analogously, we show that there exists β such that $\tilde{C} = \beta l_1 l_2 l_3$ and $(C - \beta l_1 l_2 l_3)(x,y,z)$ is a multiple of m_1.

Let $D(x,y,z) = (C - \alpha m_1 m_2 m_3 - \beta l_1 l_2 l_3)(x,y,z)$. We will prove the following lemma:

Lemma 2 *$D(x,y,z)$ is a multiple of $(l_1m_1)(x,y,z)$.*

Proof $D = m_1D_1$ we will show that $l_1|D_1$. Since $D = m_1D_1$, we have $\tilde{D} = \tilde{m}_1\tilde{D}$. We have shown that $l_1|D$, hence $\tilde{D} = 0$. Furthermore, $m_1 \neq l_1$, so $\tilde{m}_1 \neq 0$ and $\tilde{D}_1(u,v)$ is the zero polynomial. Hence, $D_1(x,y,z)$ is a multiple of $l_1(x,y,z)$.

According to the previous lemma, we can write $D(x,y,z) = (l_1m_1l)(x,y,z)$, where l is linear. By assumption $C = 0$ at points P_{22}, P_{23}, P_{32}. Moreover $l_1l_2l_3$ and $m_1m_2m_3$ equal 0 at these points.

Lemma 3 *$l(P_{22}) = l(P_{23}) = l(P_{32})$.*

Proof Proof skipped.

Our goal now is to show that D is the zero polynomial. If l is the zero polynomial, then D is the zero polynomial, hence we assume that $l \neq 0$ and l is a line. If P_{23}, P_{22}, P_{32} are distinct, then $l = l_2$ and $l = m_2$ (since l goes through points P_{23}, P_{22}, P_{32}), thus $m_2 = l_2$. A contradiction.

Now we assume that $P_{22} = P_{32}$, then m_2 is tangent to C, so $\mathrm{ord}_{m_1P_{22}}(l_1m_1l) \geqslant 2$. Hence, $l = m_2$. If $m_1(P_{22}) = 0$ then $P_{22} \in m_1m_2l_2$ and $P_{23} = P_{22}$. So l_2 is tangent and $m_2 = l_2$ — a contradiction. Therefore, $m_1(P_{22}) \neq 0$.

If $l_1(P_{22}) \neq 0$, then $\mathrm{ord}_{m_2,P_{22}} \geqslant 2$ thus $l = m_2$.

If $l_1(P_{22}) = 0$, then $P_{22} = P_{23}$ and it belongs to l_1, l_2, l_3, m_2. Hence, $P_{12} = P_{22} = P_{32}$ and $\mathrm{ord}_{m_2P_{22}}(C) \geqslant 3$, so $\mathrm{ord}_{m_2P_{22}}(l_1m_1l) \geqslant 3$. Since $m_1(P_{22}) \neq 0$, $\mathrm{ord}_{m_2P_{22}}(l) \geqslant 2$, so $l = m_2$.

Putting things together, we have shown that $P_{22} = P_{23}$ (under assumption that $P_{22} = P_{32}$). So, l_2 and m_2 are tangent to C at P_{22}, thus $l_2 = m_2$ – a contradiction. Therefore, $P_{22} \neq P_{32}$.

Similarly we show that $P_{22} \neq P_{23}$. Assuming that $P_{23} = P_{32}$ implies that $P_{23} \in m_2, m_3, l_2, l_3$ thus $P_{22} = P_{32}$, what was shown impossible, so $P_{23} \neq P_{32}$.

We have shown that $l = 0$, hence $D = 0$, so $C = \alpha m_1m_2m_3 + \beta l_1l_2l_3$. Hence $P_{33} \in C$. $\triangle$

Torsion points

Definition 1 (Torsion points) Let E be a elliptic curve over field $\mathbb{K}$, torsion points are points belonging to set $E[m] = \{P : mP = \infty\}$.

Remark 1 Torsion points form a group.

Let $y^2 = x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$, where $e_i \in \overline{K}$. We assume that $\mathrm{char}(K) \neq 2, 3$. Then:

$$E[2] = \{P : 2P = \infty\} = \{(e_1, 0), (e_2, 0), (e_3, 0), \infty\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$E[3] = \{P : 3P = \infty\}$$

Hence, $2P = -P$. $m^2 - 2x = x$, where $m = \frac{3x^2+A}{2y}$. Since, $y^2 = x^3 + Ax + B$, we have $(3x^2 + A)^2 = 12x(x^3 + Ax + B) \Longrightarrow 3x^4 + 6Ax^3 + 12Bx - A^2 = 0$.

$\Delta = -6912(4A^3 + 27B^2)^2 \neq 0$, so there is no multiple roots, hence $E[3]$ consists of 8 points plus ∞. Thus, $E[3] \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

For $\mathrm{char}(K) = 3$, we have $y^2 = x^3 + a_2x^2 + a_4x + a_6$ and

$$\left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 2x + x = 3x = 0$$

Thus, $a_2x^3 + a_2a_6 - a_4^2$. Let us consider following cases:

- $a_2 = a_4 = 0$ is not possible, because there are no multiple roots.
- $a_2 = 0$ and $a_4 \neq 0$, then $E[3] = \{\infty\}$.
- $a_2 \neq 0$ and $a_4 = 0$, then $a_2(x^3 + a_4) = 0$ and $E[3] = \{P_1, P_2, \infty\} \simeq \mathbb{Z}_3$.

Theorem 2 *Let $\mathbb{K}$ be a field and $E(K)$ be a curve, we consider $E[n]$, then*

$$E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n, \text{ for } char(K) = p \nmid n \tag{4}$$

$$E[n] \simeq \begin{cases} \mathbb{Z}_{n'} \oplus \mathbb{Z}_{n'} \\ \mathbb{Z}_n \oplus \mathbb{Z}_{n'} \end{cases} \quad \text{for } \mathrm{char}(K) = p \text{ and } n = p^k n' \tag{5}$$

Corollary 1 *For $p = n$, we have:*

$$E[n] \simeq \begin{cases} \mathbb{Z}_1 \oplus \mathbb{Z}_1 = \{\infty\} & \text{called } \textit{supersingular} \\ \mathbb{Z}_n \oplus \mathbb{Z}_1 = \mathbb{Z}_n & \text{called } \textit{ordinary} \end{cases} \tag{6}$$

Points on Elliptic Curves over finite fields $E(\mathbb{F})$ – finite. For example $\mathbb{F}_{13}$ with a curve E and equation $y^2 = x^3 + 3x + 8$.

$$E[n] \simeq \begin{cases} x = 0 \quad y^2 = 8 \\ x = 1 \quad y^2 = 12 = \begin{cases} 5^2 \bmod 13 \\ 8^2 \bmod 13 \end{cases} \end{cases} \tag{7}$$

Then $E(\mathbb{F}_{13}) = \{\infty, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$ and $|E(F_{13})| = 9$.

Theorem 3 *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. Then $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \oplus \ldots \oplus \mathbb{Z}_{n_k}$, where $n_i \mid n_{i-1}$.*

Counting points on a elliptic curve

Theorem 4 (Hasse-Weil)

$$\underbrace{q + 1 - |E(\mathbb{F}_q)|}_{\textit{Frobenius trace}} \leqslant 2\sqrt{q} \tag{8}$$

The order of point P, denoted by $\mathrm{ord}(P)$, is the smallest k such that $kP = \infty$, $k \mid |E(\mathbb{F}_q)|$ and if $nP = \infty$, then $\mathrm{ord}(P) | n$.

Let $y^2 = x^3 + 7x + 1$ over $\mathbb{F}_{101}$. $P = (0,1) \in E(\mathbb{F}_{101})$ and $\mathrm{ord}(P) = 116$. From theorem 4 we have

$$101 + 1 - 2\sqrt{101} \leqslant |E(\mathbb{F}_{101})| \leqslant 101 + 1 + 2\sqrt{101}$$

$$82 \leqslant |E(\mathbb{F}_{101})| \leqslant 122$$

Then $|E(\mathbb{F}_{101})| = 116$.

Proposition 1 *Let E be an elliptic curve defined over the finite field $\mathbb{F}_q$. If $E(\mathbb{F}_q) \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$ for some n, then either $q = n^2 + 1$ or $q = n^2 \pm n + 1$ or $q = (n \pm 1)^2$.*