Notes written by Agnieszka Zgorzelska

Let $E_{ns}(\mathbb{K})$ denote an elliptic curve $E(\mathbb{K})$ without singular points.

1. Additive reduction. The curve $E(\mathbb{K}) : y^2 = x^3$ has one singular point $(0, 0)$ - triple root. Note that the curve $y^2 = x(x + 35)(x - 55)$ in $\mathbb{F}_5$ is $y^2 = x^3$.

Theorem 1 *There exists an isomorphism $\varphi : E_{ns}(\mathbb{K}) \to (\mathbb{K}, +)$ given by $\varphi(x, y) = \frac{x}{y}$, $\varphi(\infty) = 0$.*

Proof (Sketch) Let $t = \frac{x}{y}$ then: $x = \frac{y^2}{x^2} = \frac{1}{t^2}$ and $y = \frac{x}{t} = \frac{1}{t^3}$. We'll show for $t_1 = \varphi(x_1, y_1)$, $t_2 = \varphi(x_2, y_2)$ and $t_3 = \varphi(x_3, y_3)$, where $(x_1, y_1) \neq (x_2, y_2)$, that: $(x_1, y_1) + (x_2, y_2) = (x_3, y_3) \iff t_1 + t_2 = t_3$.

$$x_3 = m^2 - x_1 - x_2 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$t_3^{-2} = \left(\frac{t_2^{-3} - t_1^{-3}}{t_2^{-2} - t_1^{-2}}\right)^2 - t_1^{-2} - t_2^{-2} = (\star)$$

Take $a = t_2^{-1}$ and $b = t_1^{-1}$.

$$(\star) = \left(\frac{a^3 - b^3}{a^2 - b^2}\right)^2 - a^2 - b^2 = \left(\frac{a^2 + ab + b^2}{a + b}\right)^2 - (a^2 + b^2) = \frac{(a^2 + b^2 + ab)^2}{a^2 + b^2 + 2ab} - (a^2 + b^2) =$$

$$= \frac{(A + C)^2}{A + 2C} - A = \frac{A^2 + 2AC + C^2 - A^2 - 2AC}{A + 2C} = \frac{C^2}{A + 2C} = \frac{a^2b^2}{a^2 + b^2 + 2ab} = \frac{1}{a^{-2}b^{-2}(a^2 + b^2 + 2ab)}$$

$$= \frac{1}{t_2^2 t_1^2 (t_2^{-2} + t_1^{-2} + 2t_1^{-1}t_2^{-1})} = \frac{1}{t_1^2 + t_2^2 + 2t_1t_2} = (t_1 + t_2)^{-2}$$

Similarly, from $y_3 = m(x_1 - x_3) - y_1$ we get $t_3^{-3} = (t_1 + t_2)^{-3}$. Therefore $\frac{t_3^{-3}}{t_3^{-2}} = \frac{(t_1+t_2)^{-3}}{(t_1+t_2)^{-2}}$ and $t_3 = t_1 + t_2$.

2. Multiplicative reduction. Consider a curve $E_{ns}(\mathbb{K}) : y^2 = x^2(x + a)$ where $a \in \mathbb{K} - \{0\}$.

Case 1. *Split multiplicative reduction* when $\alpha^2 = a$ and $\alpha \in K$. Note that the curve $y^2 = x(x + 35)(x - 55)$ in $\mathbb{F}_7$ is $y^2 = x^2(x + 1)$ and $\alpha = 1 \in \mathbb{F}_7$.

Theorem 2 *There exists an isomorphism $\varphi : E_{ns}(\mathbb{K}) \to (\mathbb{K}, \cdot)$ given by: $\varphi(x, y) = \frac{x+\alpha y}{x-\alpha y}$ and $\varphi(\infty) = 1$.*

Proof (Sketch) Let $t = \frac{y+\alpha x}{y-\alpha x}$, then $t + 1 = \frac{2y}{y-\alpha x}$, $t - 1 = \frac{2\alpha x}{y-\alpha x}$, $\frac{t+1}{t-1} = \frac{y}{\alpha x}$, $\frac{y}{x} = \alpha\frac{t+1}{t-1}$. Now, from the equation of the curve we get $x + a = \frac{y^2}{x^2}$, so $x = \frac{4\alpha^2 t}{(t-1)^2}$ and $y = x \cdot \frac{y}{x} = \frac{4\alpha^2 t(t+1)}{(t-1)^2}$. One can show that $t_3 = t_1 \cdot t_2$

Case 2. *Non-split multiplicative reduction* when $\alpha^2 = a$ and $\alpha \notin K$. Note that the curve $y^2 = x(x + 35)(x - 55)$ in $\mathbb{F}_{11}$ is $y^2 = x^2(x + 2)$ where $\alpha = \sqrt{2} \notin \mathbb{F}_{11}$

Theorem 3 *There exists an isomorphism* $\varphi : E_{ns}(\mathbb{K}) \to \{u + \alpha v : u, v \in K \wedge u^2 - av^2 = 1\}$.

Proof $\frac{y+\alpha x}{y-\alpha x} \cdot \frac{y+\alpha x}{y+\alpha x} = \frac{(y+\alpha x)^2}{y^2-ax^2} = u + \alpha v$, $\frac{y-\alpha x}{y+\alpha x} \cdot \frac{y-\alpha x}{y-\alpha x} = \frac{(y-\alpha x)^2}{y^2+ax^2} = u - \alpha v$
$u^2 - av^2 = (u - \alpha v)(u + \alpha v) = \frac{y+\alpha x}{y-\alpha x} \cdot \frac{y-\alpha x}{y+\alpha x} = 1$
$x = (\frac{u+1}{v})^2 - a$ and $y = (\frac{u+1}{v})x$
$\varphi(x, y) = \frac{\frac{y}{x}+\alpha}{\frac{y}{x}-\alpha} = \frac{u+1+\alpha v}{u+1-\alpha v} = u + \alpha v$
Taking $x_i = \frac{4\alpha^2 t_i}{(t_i-1)^2}$ one can show that $\frac{4t_3}{(t_3-1)^2} = \frac{4t_1t_2}{(t_1t_2-1)^2}$. Again $y_3 = m(x_1 - x_3) - y_1$, which gives us $\frac{4\alpha^3 t_3(t_3+1)}{(t_3-1)^3} = \frac{4\alpha^3 t_1t_2(t_1t_2+1)}{(t_1t_2-1)^3}$. Finally we get $\frac{t_3-1}{t_3+1} = \frac{t_1t_2-1}{t_1t_2+1}$ and $t_3 = t_1t_2$.

For $p \geq 13$ we get *good reduction* of the curve $y^2 = x(x + 35)(x - 55)$ in $\mathbb{F}_p$.

Projective space. $\mathbb{P}^2(\mathbb{K}) = \{(x, y, z) : x, y, z \in K\}$. Lines in $\mathbb{P}^2(\mathbb{K})$ are given by an equation: $ax + by + cz = 0$ or parametric representation: $(x, y, z) = (a_1u + b_1v, a_2u + b_2v, a_3u + b_3v)$ where u, v are parameters.
The matrix $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}$ of a rank 2 gives a line. Notice: if $(u', v') = \lambda(u, v)$ then both pairs give the same point so consider $(u : v) \in \mathbb{P}^1(\mathbb{K})$

Intersection of a line and a curve in the affine space.
$L = \begin{cases} x = a_1t + b_1 \\ y = a_2t + b_2 \end{cases} \quad C : f(x, y) = 0$
$\tilde{f}(t) = f(a_1t + b_1, a_2t + b_2)$. Let $P_0(x_0, y_0) \to t = t_0$
A line and a curve intersect at $P_0 \iff \tilde{f}(t_0) = 0 \iff (t - t_0)|\tilde{f}(t)$
If $(t - t_0)^2|\tilde{f}(t)$ then L is tangent. If $(t - t_0)^n|\tilde{f}(t)$ and $(t - t_0)^{n+1} \nmid \tilde{f}(t)$ then n is the *order of intersection* in P_0.

Intersection of a line and a curve in projective space.
$L = \begin{cases} x = a_1u + b_1v \\ y = a_2u + b_2v \\ z = a_3u + b_3v \end{cases} \quad C : f(x, y, z) = 0$
f- homogeneous
$\tilde{f}(u, v) = f(a_1u + b_1v, a_2u + b_2v, a_3u + b_3v)$
$P_0(u_0, v_0) = (x_0, y_0, z_0)$ - point of intersection.
$\tilde{f}(u_0, v_0) = 0 \iff (v_0u - u_0v)|\tilde{f}(u, v)$
n is an order of intersection $\iff (v_0u - u_0v)^n|\tilde{f}(u, v) \wedge (v_0u - u_0v)^{n+1} \nmid \tilde{f}(u, v)$. If $\tilde{f} = 0$ then order$= \infty$.

Lemma 1 *Given homogeneous polynomial* $G(u, v)$ *and* $(u_0, v_0) \in \mathbb{P}^2(\mathbb{K})$. *There exists* $k \geq 0$ *and polynomial* $H(u, v)$ *such that* $H(u_0, v_0) \neq 0$ *and* $G(u, v) = (v_0u - u_0v)^k H(u, v)$.

Proof Assume $v_0 \neq 0$ and $\deg(G) = m$. Define $g(u) = G(u, v_0)$, then $\exists_k (u - u_0)^k h(u) = g(u)$ where $h(u) \neq 0$ and $\deg(h) = m - k$. Now define: $H(u, v) = \frac{v^{m-k}}{v_0^m} \cdot h(u \cdot \frac{v_0}{v})$. $H(u, v)$ is homogeneous of degree $m - k$.
$G(u, v) = (\frac{v}{v_0})^m g(\frac{uv_0}{v}) = \frac{v^m}{v_0^m}(\frac{uv_0}{v} - u_0)^k h(\frac{uv_0}{v}) = \frac{v^{m-k}}{v_0^m}(uv_0 - u_0v)^k h(\frac{uv_0}{v}) = (uv_0 - u_0v)^k H(u, v)$

Example

$$L = \begin{cases} x = au \\ y = bu \\ z = v \end{cases} \qquad f(x,y,z) = y^2z - x^3 = 0 \implies \tilde{f}(u,v) = b^2u^2v - a^3u^3 = u^2(b^2v - a^3u) = 0$$

For $b = 0$ we have singular point $(0:1)$ of order 3.

Point P is nonsingular $\iff f_x(P) \neq 0 \vee f_y(P) \neq 0 \vee f_z(P) \neq 0$.
A line is tangent in $P \iff f_x(P)x + f_y(P)y + f_z(P)z = 0$.

Theorem 4 *Let $C : f(x,y,z) = 0$ and P be a nonsingular point. Then $\exists!$ line L in $\mathbb{P}^2(\mathbb{K})$ such that the order of intersection in P is ≥ 2 ($ord_C(P) \geq 2$). This line is the tangent.*

Proof L and C intersect at point $P(x_0, y_0)$. Order of intersection is $k \geq 1$

$$L = \begin{cases} x = a_1u + b_1v \\ y = a_2u + b_2v \\ z = a_3u + b_3v \end{cases} \qquad C : f(x,y,z) = 0$$

From lemma we know that $\exists H(u,v)$ such that $H(u_0,v_0) \neq 0$ and $(v_0u - u_0v)^k H(u,v) = \tilde{f}(u,v)$.
$\tilde{f}_u = kv_0(v_0u - u_0v)^{k-1}H(u,v) + (v_0u - u_0v)^k H_u(u,v)$
$\tilde{f}_v = ku_0(v_0u - u_0v)^{k-1}H(u,v) + (v_0u - u_0v)^k H_v(u,v)$
$k \geq 2 \iff \tilde{f}_u(u_0,v_0) = \tilde{f}_v(u_0,v_0) = 0$. Assume that we have a line L intersecting C at order ≥ 2. Then:
$\tilde{f}_u = a_1f_x + a_2f_y + a_3f_z = 0$
$\tilde{f}_v = b_1f_x + b_2f_y + b_3f_z = 0$
The rank of the matrix $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}$ in ≥ 2. Let $a = (a_1, a_2, a_3)$ and $b = (b_1, b_2, b_3)$. Assume that there is another such line L' with $a' = (a'_1, a'_2, a'_3)$ and $b' = (b'_1, b'_2, b'_3)$.

Case 1.
Vectors a' and b' are linear combinations of a and b. These two pairs span the same affine plane.
$a' = \alpha a + \beta b$
$b' = \gamma a + \delta b$
Then $ua' + vb' = (u\alpha + v\gamma)a + (u\beta + v\delta)b = u_1a + v_1b$ and we get the same projective line.

Case 2.
a, b, a', b' span $\mathbb{K}^3$. If $(f_x, f_y, f_z) \cdot c = 0$ for every $c \in \{a, b, a', b'\}$ then $(f_x, f_y, f_z) = (0,0,0) \implies P$ is singular (contradiction). Thus, if the line L exists, it is unique.
Assume $f_x \neq 0$ and take $L = \begin{cases} x = -\frac{f_y}{f_x}u - \frac{f_z}{f_x}v \\ y = u \\ z = v \end{cases}$
$\tilde{f}_u = -\frac{f_y}{f_x}f_x + 1 \cdot f_y + 0 \cdot f_z = 0$
$\tilde{f}_v = -\frac{f_z}{f_x}f_x + 0 \cdot f_y + 1 \cdot f_z = 0$

L intersects C at order ≥ 2.