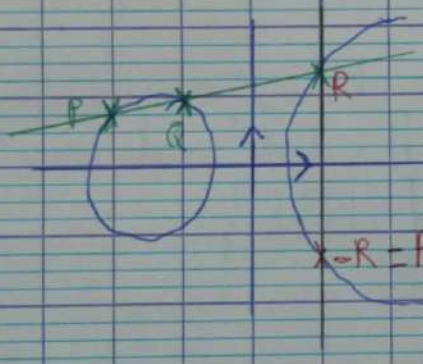
Elliptic curve 3

I) Addition law on elliptic curve:

1) Geometric interpretation:

$E/k : y^2 = x^3 + ax + b$

- $O_E = (0:1:0)$ in projective coordinates is the neutral point.
- $P, Q \in E$ so $l_{P,Q}$ the line going through P and Q.



Lemma: $l_{P,Q} \cap E \subset \mathbb{P}^2$ has exactly 3 points in k (with multiplicity)

Proof: by Bezout's theorem, if $\mathcal{C}_1$ and $\mathcal{C}_2 \subset \mathbb{P}^2_k$ are curve of degree d_1 and d_2, $\mathcal{C}_1 \neq \mathcal{C}_2$, then $\mathcal{C}_1 \cap \mathcal{C}_2$ has $d_1 \times d_2$ points in $\mathbb{P}^2(\bar{k})$.

Definition: let R be the third point of intersection then $\boxed{P+Q+R = O_E}$ so $\boxed{P+Q = -R}$.

* Finding $-R$: $O_E + R + (-R) = O_E$

$l_{Q,R}$ the line going through Q and R intersect E at $(-R)$.

$l_{Q,R} = v_R$ the vertical line going through R.

2) Algebraic formula:

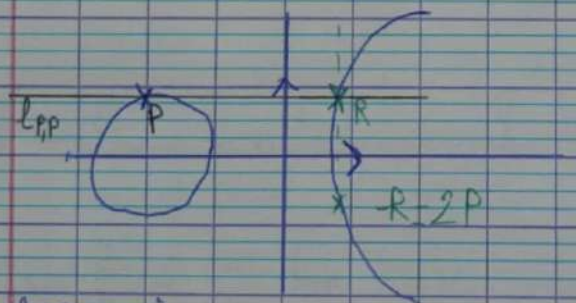
$R = (x_R, y_R)$ so $\boxed{-R = (x_R, -y_R)}$ only y get the minus

$P = (x_P, y_P)$
$Q = (x_Q, y_Q)$
$\boxed{P, Q \neq O \\ P \neq -Q}$ $\Rightarrow P + Q = (-R) = (x_R, -y_R)$

$l_{P,Q}$: $y - y_P = \alpha (x - x_P)$ where α is the slope of $l_{P,Q}$

$\boxed{\alpha = \frac{y_Q - y_P}{x_Q - x_P}}$ if $P \neq Q$

Question: What is $l_{P,Q}$ when $P = Q$?
$l_{P,P}$ is the tangent to E at P which exists since by definition E is smooth at P. $l_{P,P} \cap E = \{(P, P, R)\}$



$f(x, y) = y^2 - x^3 - ax + b$

$l_{P,P} = \frac{\delta f(P)}{\delta y}(y - y_P) + \frac{\delta f(P)}{\delta x}(x - x_P)$

$l_{P,P} = 2y_P(y - y_P) = (-3x_P^2 - a)(x - x_P)$

The slope $\boxed{\alpha = \frac{3x_P^2 + a}{2y_P}}$

$l_{P,Q}: y = \alpha x + \beta$ $\quad (\beta = y_P - \alpha x_P)$

$l_{P,Q} \cap E = \{P, Q, R\}$ $\quad \begin{cases} y_R = \alpha x_R + \beta \\ y_R^2 = x_R^3 + a x_R + b \end{cases} \Rightarrow x_R^3 - (\alpha x_R + \beta)^2 + a x_R + b = 0$

Since x_P, x_Q are also roots

$x_P + x_Q + x_R = +\alpha^2 = \alpha^2$

So $x_R = \alpha^2 - x_P - x_Q$

$y_R = \alpha x_R + \beta = y_P + \alpha(x_R - x_P)$

$P + Q = -R = x_R, -y_R$

Summary: 1) $\alpha = \dfrac{y_Q - y_P}{x_Q - x_P}$

Special case $x_P = x_Q$: a) $P = -Q$, $y_P = -y_Q \Rightarrow P + Q = O_E$

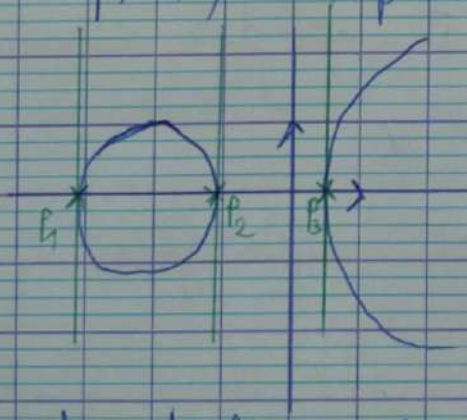
b) $P = Q$, $\alpha = \dfrac{3x_P^2 + a}{2y_P}$

c) Last special case: $P = Q$ and $y_P = 0$

$P = (x_P, 0)$, $0^2 = x_P^3 + a x_P + b$

P is called a Weierstrass point

x_P is one of the three roots of $x^3 + ax + b = 0$



The tangent $l_{P,P}$ is the vertical line v_P.

So $P + P = O_E$ ie $P = -P$.

II) Structure of $E(\overline{\mathbb{F}_q})$ as a group:

1) Complex elliptic curves:

Theorem: Every elliptic curve $E/\mathbb{C}$ is analytically isomorphic to a torus $E: \mathbb{C}/(\mathbb{Z} \oplus \tau\mathbb{Z})$ where $\mathrm{Im}\,\tau > 0$. (and conversely)

τ

$\uparrow$

$\cdots$ $E[3]$

$\xrightarrow[E]{}$

Definition: $E[n]$ is the points of n-torsion. i.e. $\{P \mid nP = O_E\}$

Corollary: Over $\mathbb{C}$, $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$

2) Over $\overline{\mathbb{F}_q}$:

Prop: If $E/\overline{\mathbb{F}_q}$ is an elliptic curve, $q = p^d$ then if $p \nmid m$, $E[n](\overline{\mathbb{F}_q}) \simeq (\mathbb{Z}/n\mathbb{Z})^2$

1) $E[p](\overline{\mathbb{F}_q}) = \mathbb{Z}/p\mathbb{Z}$ $\rightarrow E$ is said to be ordinary

$\Rightarrow E[p^m](\overline{\mathbb{F}_q}) \simeq \mathbb{Z}/p^m\mathbb{Z}$

2) $E[p](\overline{\mathbb{F}_q}) = \{O_E\}$ $\rightarrow E$ is supersingular

$\Rightarrow E[p^m](\overline{\mathbb{F}_q}) = \{O_E\}$

Corollary: $\boxed{E(\overline{\mathbb{F}_q}) \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \quad \text{with } d_1 \mid d_2 \text{ (possibly } d_1 = 1)}$

Remark: We will see that also $\boxed{d_1 \mid q-1}$

III) Number of points in $E(\mathbb{F}_q)$

- $O_E \longrightarrow$ 1 point $\qquad h(x) = x^3 + ax + b$
- For each x in $\mathbb{F}_q$:
  a) if $h(x) = 0 \Rightarrow (x, 0)$ a weierstrass point : 1 point
  b) if $h(x)$ is a square y^2, $y \in \mathbb{F}_q$
  $\Rightarrow (x, y), (x, -y)$: 2 points
  c) if $h(x)$ ~~if $h(x)$~~ is not a square $\longrightarrow$ 0 point

Summary: (if $q = p$):
$$\#E(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{h(x)}{p}\right)\right) \quad \text{with } \left(\frac{h(x)}{p}\right) \text{ the jacobi symbol}$$

Heuristic: If x is "random" in $\mathbb{F}_p$, $h(x)$ is "random" in $\mathbb{F}_p$.
So $h(x)$ has proba $\simeq 1/2$ to be a square, and $\simeq 1/2$ not to be
We expect the average of $\left(\frac{h(x)}{p}\right)$ to be 0.

So we expect $\#E(\mathbb{F}_p) \simeq p + 1$.
Where the deviation $t = p + 1 - \#E(\mathbb{F}_p)$ would be $O(\sqrt{p})$ by the central limit theorem.

2) Weierstrass theorem:

Th. $E/\mathbb{F}_q$, $\#E(\mathbb{F}_q) = 1 + q - t$, $|t| \leq 2\sqrt{q}$

"Sorry, I don't have time to write the proof."

Definition: An endomorphism ϕ of E is a rational application $\phi : E \longrightarrow E$ such that
(i) $\phi(O_E) = O_E$
(ii) $\phi(P+Q) = \phi(P) + \phi(Q)$

En fait: For elliptic curves (i) $\Rightarrow$ (ii)

The degree $\deg \phi$ is the number of points (counted with multiplicities) of $\operatorname{Ker} \phi(\overline{\mathbb{F}}_q)$.

Example: $\deg \pi_q = q$, $\operatorname{Ker} \pi_q = \{P \in E(\overline{\mathbb{F}}_q) / \pi(P) = O_E\} = O_E$ ← multiplicity q

$X^q = 0$
$Y^q = 1$
$Z^q = 0$

Theorem: deg is a positive quadratic form on $\operatorname{End}(E)$. In fact if $\phi \in \operatorname{End}(E)$, there is a dual endomorphism $\hat{\phi}$, and
$\deg \phi = \phi\hat{\phi} = \hat{\phi}\phi \in \mathbb{Z}$

Definition: $(\phi|\psi) = \dfrac{\phi\hat{\psi} + \hat{\phi}\psi}{2}$ $\quad \deg \phi = (\phi|\phi)$

I want to compute the degree of $\pi_q - 1$.

$$\begin{aligned}\deg(\pi_q - 1) &= (\pi_q - 1 | \pi_q - 1) \\ &= (\pi_q | \pi_q) + (1|1) - 2(\pi_q | 1) \\ &= \deg \pi_q + \deg 1 - 2(\pi_q|1) \\ &= q + 1 - 2(\pi_q|1)\end{aligned}$$

Let $t = 2(\pi_q|1) = \pi_q + \hat{\pi}_q$, we have $2(\pi_q|1) \leq 2\sqrt{(\pi_q|\pi_q)(1|1)}$ by CS
$\leq 2\sqrt{q}$

Summary: $\#E(\mathbb{F}_q) = q + 1 - t$ where $t = \pi_q + \hat{\pi}_q$ and $|t| \leq 2\sqrt{q}$

Definition: If $\phi \in \operatorname{End} E$, λ ϕ the characteristic polynomial as
$X_\phi = (X - \phi)(X - \hat{\phi}) = X^2 - (\phi + \hat{\phi})X + \phi\hat{\phi} = X^2 - (\operatorname{tr} \phi)X + \deg \phi$

Example: $X_\pi = X^2 - \operatorname{tr}(\pi)X + \deg \pi = X^2 - (\operatorname{tr} \pi)X + q = X^2 - tX + q$
$\#E(\mathbb{F}_q) = \deg(1 - \pi_q) = X_\pi(1) = 1 - t + q$

Property: Let $t = \pi_q + \bar{\pi}_q \in \mathbb{Z}$ be the trace of Frobenius.
Then E is supersingular $\Leftrightarrow p \mid t$

Property: * If E is ordinary, $\mathrm{End}(E|_{\bar{\mathbb{F}}_q}) = \mathbb{Q}(\pi)$
$= \mathbb{Q}[x] / \chi_{\pi}(x)$
$= (\mathbb{Q}[x]/(x^2 - t_x + q))$
is a quadratic number field of discriminant $\Delta = t^2 - 4q \leq 0$
→ so $\mathrm{End}(E) \otimes \mathbb{Q}$ is an imaginary quadratic field and $\bar{\cdot}$ is the complex conjugation.

* If E is supersingular, then $\mathrm{End}(E_{\bar{\mathbb{F}}_q}) \otimes \mathbb{Q}$ is a quaternion algebra (non commutative of dim 4 over $\mathbb{Q}$).