Elliptic Curves - Summary

Matteo Durante, s2303760, Leiden University

20th May 2019

Theorem 1 (Mordell)**.** *Given an elliptic curve $E/\mathbb{Q}$,* $\mathrm{rk}(E(\mathbb{Q})) = \mathrm{rk}(E(\mathbb{Q})/2E(\mathbb{Q})) < \infty$.

Theorem 2. *Given a curve C and a rational map $C \xrightarrow{\phi} W \subset \mathbb{P}^n$, if C is smooth, then ϕ is a morphism.*

Corollary 3. *Let $C_1 \xrightarrow{\phi} C_2$ be a morphism of smooth curves. If* $\deg(\phi) = 1$*, then it is an isomorphism.*

Proposition 4. *Given any smooth projective curve C, a morphism $C \to \mathbb{P}^1$ is either constant or surjective.*

Proposition 5. *Let $C_1 \xrightarrow{\phi} C_2$ be a non-constant morphism. Then:*

- *for every $Q \in C_2$,* $\deg(\phi) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)$*;*
- *If $C_2 \xrightarrow{\psi} C_3$ is another morphism, $e_{\psi \circ \phi}(P) = e_\phi(P) \cdot e_\psi(\phi(P))$.*

Proposition 6. *For all but finitely many $Q \in C_2$, $\#\phi^{-1}(Q) = \deg_s(\phi)$. If we are working over $\mathbb{Q}$,* $= \deg(Q)$*.*

—- BEWARE: from now on, $\mathbb{K}$ will always be an algebraically closed field, C a smooth projective curve over $\mathbb{K}$. —-

Proposition 7. *Given a smooth projective curve over $\mathbb{K}$, we have for any $f \in \mathbb{K}(C)$:*

- $\mathrm{div}(f) = 0 \Leftrightarrow f \in \mathbb{K}^\times$*;*
- $\deg(\mathrm{div}(f)) = 0$

Proposition 8. *Ω_C is a 1-dimensional $\mathbb{K}(C)$-vector space and a morphism $C_1 \xrightarrow{\phi} C_2$ induces a map $\Omega_{C_2} \xrightarrow{\phi^*} \Omega_{C_1}$ defined as $\phi^*(f \cdot dx) = \phi^*(f) \cdot d(\phi^*(x))$. Also, ϕ is separable if and only if $\phi^* \neq 0$.*

Theorem 9 (Riemann-Roch)**.** *Given $D \in \mathrm{Div}(C)$, $l(D) - l(K_C - D) = \deg(D) - g + 1$.*

Proposition 10. *Let E be a smooth projective curve of genus 1 and defined over $\mathbb{K}$ not algebraically closed. Also, fixed $O \in E(\mathbb{K})$, there is an isomorphism $C \xrightarrow{\phi} C \subset \mathbb{P}^1_{\mathbb{K}}$ with $\phi(O) = (0 : 1 : 0)$ and C given by $y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$, which is the General Weierstrass equation.*

Proposition 11. *Given C and fixed $O \in E(\mathbb{K})$, there is a map $C(\mathbb{K}) \to \mathrm{Pic}(C)$, $P \mapsto [P - O]$, which gives a bijection $C(\mathbb{K}) \leftrightarrow \mathrm{Pic}^0(C)$.*

Proposition 12. *Let $\Gamma(\mathbb{K}) \neq 2, 3$. If C is given by a Weierstrass equation, then there exists a change of variables which reduces it to $y^2 = x^3 + ax + b$. Also, any isomorphism of elliptic curves is given by $x = u^2 x'$, $y = u^3 y'$ for some $u \in \mathbb{K}^\times$.*

Proposition 13.

- *Given any Weierstrass curve E over a field $\mathbb{K}$ not necessarily algebraically closed:*
  1. *is smooth $\Leftrightarrow \Delta \neq 0$; also, $E(\mathbb{K}) \cong \mathrm{Pic}^0_{\mathbb{K}}(E)$;*
  2. *has a node $\Leftrightarrow \Delta = 0 \neq C_4$; also, $E^{ns}(\overline{K}) \cong \overline{K}^\times$;*
  3. *has a cusp $\Leftrightarrow \Delta = C_4 = 0$; also, $E^{ns}(\mathbb{K}) \cong (\mathbb{K}, +)$.*
- *Two elliptic curves E, E' over $\mathbb{K}$ are isomorphic if and only if $j(E) = j(E')$.*
- *For all $j_0 \in \mathbb{K}$, there exists an elliptic curve E over $\mathbb{K}$ s.t. $j(E) = j_0$.*

Theorem 14. *Let E be a Weierstrass curve over $\mathbb{Q}$ and $n \in \mathbb{Z}_{>0}$ s.t. $p \mid n$. Then, we have an injection $E(\mathbb{Q})[n] \hookrightarrow \tilde{E}(\mathbb{F}_p)$. Also, the order of any point in $E(\mathbb{Q})^{tors}$ divides $p^k \cdot \#\tilde{E}(\mathbb{F}_p)$ for some $k \in \mathbb{N}$.*

Corollary 15. *Given any elliptic curve E over $\mathbb{Q}$, $E(\mathbb{Q})^{tors}$ is a finite subgroup of $E(\mathbb{Q})$.*

Theorem 16 (Nagell-Lutz)**.** *Let $E/\mathbb{Q}$ be an elliptic curve given in short Weierstrass form by $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$. Suppose that $P = (x_P, y_P) \in E(\mathbb{Q})^{tors}$. Then, $x_P, y_P \in \mathbb{Z}$ and either $y_P = 0$, in which case P has order 2, or $y_P^2 | 4a^3 + 27b^2$.*

Theorem 17 (Mazur)**.** *Given an elliptic curve $E/\mathbb{Q}$, we have that $E^{tors}(\mathbb{Q})$ is either isomorphic to $\mathbb{Z}/n\mathbb{Z}$, where $1 \leq n \leq 10$ or $n = 12$, or to $\mathbb{Z}/2n\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, where $1 \leq n \leq 4$.*