Brief Overview of Elliptic Curves

Marcel Eichberg

11. April 2022

While the question of finding the solutions of general curves is of great interest and importance in both algebraic geometry and algebraic number theory, cubic (elliptic) curves are of particular interest to us as their sets of points admit abelian group structures. We aim here to give a brief overview of some elementary results in the theory of Elliptic curves. Unless otherwise stated, we assume that the characteristic of all fields in question is not 2 or 3.

Definition 1. An **Elliptic Curve** E over a field $\mathbb{F}$ is a Cubic curve given by the equation $y^2 = x^3 + ax + b,\ a, b \in \mathbb{F}$. Often times one replaces the variable x with $x + c$ for some constant $c \in \mathbb{F}$, giving the curve the form $y^2 = x^3 + Cx^2 + Ax + B,\ A, B, C \in \mathbb{F}$

We consider from now on points on curves of the form above, together with a 'point at infinity', conventially called O and denote them with (E, O) if we want to specify which field E is over, we use the notation $E/\mathbb{F}$. The Theorem of Bézout tells us that the points intersecting a line L with an Elliptic curve of the above form is three counting multiplicities (i.e a tangent line through a point $P \in E$ counts twice).

Definition 2. The **Composition Law** works as follows, let $P, Q \in E$ and define L to be the line through P and Q (the tangent if they coincide). Then there exists a third (and final) point $R \in L \cap E$. Define L' to be the line parallel to the y-axis, the second point of intersection is O, the third point we define as $P \oplus Q$.

Theorem 3. *The Triple $(E, O, \oplus)$ defines an abelian group on E with neutral element O*

For any integer m we denote $[m]P = P + ... + P$ and $[m]P = -P - ... - P$ if m is positive or negative respectively. We also denote the composition law with a standard $+$ instead of $\oplus$.
Every element of a group admits an inverse element, thus the natural question that arises would be how do we construct the inverse $-P$ of an element $P \in E$. The next would be, given two points P_0, P_1, how do we obtain $P_0 + P_1$

Lemma 4. *For a point $P_0 = (x_0, y_0)$ the inverse is given by $-P_0 = -(x_0, y_0) = (x_0, -y_0)$. The sum $P_0 + P_1 = P_2$ is given by the formula $P_2 = (x_2, y_2)$ with $x_2 = m^2 - C - x_1 - x_2$ and $y_3 = m(x_3 - x_1) + y_1$ with* $m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \text{ if } x_2 \neq x_1 \\ \frac{3x_1^2 + 2Cx_1 + A}{2y_1} \text{ if } x_2 = x_1 \end{cases}$.

Before looking at an example, we note that in some literature, Elliptic curves are defined in a slightly more complicated manner, e.g $F(x,y) = y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6 = 0$. This yields slightly different, albeit as easily derivable, formulas for the inverse and the composition laws.

Example 5. *Consider $E : y^2 = x^3 + 17$ over $\mathbb{Q}$. Given the points $P_1 = (-2, 3), P_2 = (-1, 4)$ and $P_3 = (2, 5)$, using the laws above we can calculate $[-2]P_1 = (8, 23), P_1 - P_3(4, 9)$ and $[2]P_2 = (\frac{127}{64}, \frac{-2651}{512})$.*

Definition 6. Let E be an Elliptic curve, and $m \in \mathbb{Z}$, we define $E[m] = \{P \in E : [m]P = O\}$ the **m-torsion subgroup** of E.

Theorem 7. *let $\mathbb{F}$ be a finite Field. For an Elliptic curve $E/\mathbb{F}$ one of the following is true:*

i) $E[p^e] = O$ *for all* $e = 1, 2, 3...$

ii $E[p^e] = \mathbb{Z}/p^e\mathbb{Z}$ *for all* $e = 1, 2, 3...$

Definition 8. If i) holds, we call the Elliptic curve E **supersingular**, otherwise we say E is **ordinary**.

Theorem 9. *(Hasse) let F_{p^k} be the finite field of order p^k, then an Elliptic curve E/F_{p^k} satisfies*

$$|\#E - (p^k + 1)| \leq 2\sqrt{p^k}.$$

Theorem 10. *(Deuring) For any integer $m \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$, there exists a pair (a, b) in $\{(a, b) : a, b \in \mathbb{F}_p : 4a^3 + 27b^2 \neq 0\}$ such that*

$$\#E = m.$$

Theorem 11. *(Lenstra) There is a positive number c such that if $p > 0$ and S a set of integers in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$ with atleast three members, then*

$$N_1(S) > c(\#S)p^{3/2}/\ln p, \quad N_2(S) > c(\#S)p^{5/2}/\ln p.$$

where $N_1(S)$ is the number of pairs (a, b) such that $4a^3 + 27b^2 \neq 0$ and $N_2(S)$ is the number of triples (a, x_0, y_0) such that for $b = y_0^2 - x_0^3 - ax_0$ we have $4a^3 + 27b^2 \neq 0$