Points of Fintie Order

[Koblitz]: I.7-9

Tangent–Chord Arithmetic on Cubic Curves

Let K be a field and C a cubic curve defined over K given by a polynomial $f(x, y) = \sum_{i+j=3} a_{ij} x^i y^j$.

Ideas.

- Bézout's Theorem asserts that : new points on C can be construct from known points using tangents and chords.
- The tangent-chord arithmetic gives some sort of composition law on the set $C(K)$.
- Choose a base point on the curve C. The compoistion law gives the curve C a structure of an abelian group.

Tangent–Chord Arithmetic: Conditions

Let K be a field and C a cubic curve defined over K given by a polynomial $f(x, y) = \sum_{i+j=3} a_{ij} x^i y^j$.

Ideas.

- One should work on the projective plane curve:

$$C : F(X, Y, Z) = \sum_{i+j=3} a_{ij} X^i Y^j Z^{3-i-j} = 0.$$

- The curve should be smooth.
- The base point $\mathcal{O}$ should have coordinate in K.

The Composition Law on Elliptic Curves

Let K be a field and E an elliptic curve over K given by a Weierstrass equation with base point $\mathcal{O} = [0, 1, 0]$ (point at infinity).

Composition Law. Let P, $Q \in E$.

- Let $\ell = \overline{PQ}$ be the line through P and Q (if $P = Q$, let ℓ be the tangent line to E at P).
- Let R be the third point of intersection of ℓ with E.
- Let ℓ' be the line through R and $\mathcal{O}$.

Then ℓ' intersects E at R, $\mathcal{O}$, and a third point. We denote that third point by $P + Q$.

Proposition. The composition law makes E into an abelian group with identity element $\mathcal{O}$.

The Addition Law Algorithm

Let K be a field with $\mathrm{Char}(K) \neq 2$ and E an elliptic curve over K given by the equation

$$E:\ y^2 = ax^3 + bx^2 + cx + d.$$

Addition Law Algorithm. Let $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E$, and (x_3, y_3) the coordinates of $P + Q$.

- $-P = (x_1, -y_1)$.
- Let $\ell = \overline{PQ}$ be the line through P and Q (if $P = Q$, let ℓ be the tangent line to E at P). Let m_ℓ be the slope of the line ℓ. Then

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a} \cdot m_\ell^2,$$
$$y_3 = -y_1 + m_\ell(x_1 - x_3).$$

The Addition Formula of $\wp$

Let L be a lattice in $\mathbb{C}$ and E_L the corresponding elliptic curve

$$Y^2Z = 4X^3 - g_2(L)XZ^2 - g_3(L)Z^3.$$

$\mathbb{C}/L$	$\longleftrightarrow$	E_L
0		$\mathcal{O} = [0, 1, 0]$
z		$[\wp(z), \wp'(z), 1]$
$-z$		$[\wp(z), -\wp'(z), 1]$
$z + u$		$[\wp(z+u), \wp'(z+u), 1]$

Propostion. We have the folloing formula:

$$\wp(z+u) = -\wp(z) - \wp(u) + \frac{1}{4}\left(\frac{\wp'(z) - \wp'(u)}{\wp(z) - \wp(u)}\right)^2.$$

Let K be a field with $\mathrm{Char}(K) \neq 2$ and $E: \ y^2 = f(x)$ an elliptic curve over K, for some $f(x) \in K[x]$.

Proposition I.8.13. Let F be any field extension of K and

$$\sigma : \ F \longrightarrow \sigma F$$

be any field isomorphism which leaves fixed all elements of K. Let $P \in \mathbb{P}^2(F)$ be a point of exact order N on E. Then

$$\sigma P := [\sigma X, \sigma Y, \sigma Z] \in \mathbb{P}^2(\sigma F)$$

has exact order N.

Idea.

$$\sigma(P_1 + P_2) = \sigma P_1 + \sigma P_2.$$

Denote $E[N]$ the set of the N-torsion subgroup of E (points of order N), that is,

$$E[N] := \{P \in E(\overline{K}) : \ NP = \mathcal{O}\}.$$

Proposition I.8.14. Let $K \leq \mathbb{C}$. Denote $x(P)$ and $y(P)$ the x- and y-coordinates of P, respectively. The fields

$$\begin{aligned} K_N &:= K\left(x(P), y(P) : \ P \in E[N]\right) \\ K_N^+ &:= K\left(x(P) : \ P \in E[N]\right) \end{aligned}$$

are finite Galois extensions of K. Moreover, the Galois group $\mathrm{Gal}\,(K_N/K)$ is isomorphic to a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Proposition I.8.15. Let N be a positive integer with $N \neq 0$ in K. Then

$$E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}.$$

There are at most N^2 points of order N over any extension F of K.

Suppose $E: \ y^2 = x^3 + ax + b$. The n-th division polynomial is defined as follows: $\psi_1 := 1$, $\psi_2 := 2y$,

$$\begin{aligned} \psi_3 &:= 3x^4 + 6ax^2 + 12bx - a^2, \\ \psi_4 &:= 4y(x^6 + 5ax^4 + 20bx^3 - 5ax^2 - 4abx - 8b^2 - a^3), \\ \psi_{2n+1} &:= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \\ 2y \cdot \psi_{2n} &:= \psi_n \left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right). \end{aligned}$$

Then

$$nP = \left(\frac{x\psi_n^2 - \psi_{n-1}\psi_{n+1}}{\psi_n^2}, \quad \frac{\psi_{2n}}{2\psi_n^4} \right).$$

Note that

$$\begin{aligned} \psi_n^2 &= n^2 x^{n^2-1} + \text{lower terms}, \\ x\psi_n^2 - \psi_{n-1}\psi_{n+1} &= x^{n^2} + \text{lower terms}, \end{aligned}$$

are relatively prime in $K[x]$.

Remark. For the elliptic curve $E_L : y^2 = 4x^3 - g_2 x - g_3$, when $K = \mathbb{Q}(g_2, g_3)$, the field K_N^+ will be a splitting field of certain polynomial which can be determined by the evaluations of $\wp$-function at the points u with $Nu \in L$.

- **N odd.**

$$F_N(x) = N \prod_{0 \neq u \in \mathbb{C}/L, Nu \in L}^{\prime} (x - \wp(u)),$$

  with one u taken from each pair u and $-u$.
  Denote $f_N(z) := F_N(\wp(z))$.

- **N even.**

$$F_N(x) = N \prod_{Nu \in L, 2u \notin L} (x - \wp(u)),$$

  Denote $f_N(z) := -\frac{1}{2}\wp'(z) F_N(\wp(z))$.

We have

$$f_N(z)^2 = N^2 \prod_{0 \neq u \in \mathbb{C}/L, Nu \in L} (\wp(z) - \wp(u)).$$

Let E be any elliptic curve over $\mathbb{Q}$.

Mordell's Theorem. The group $E(\mathbb{Q})$ is a finitely generated abelian group. That is,

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$$

Rank. The non-negative integer r is called the rank of $E(\mathbb{Q})$.

Proposition I.8.17. Let E_n be the elliptic curve $E_n: \ y^2 = x^3 - n^2 x$ for some $n \in \mathbb{Z}$. Then

$$E_n(\mathbb{Q})_{tors} = \{(0, \pm n), (0, 0)\} \cup \{\mathcal{O}\}.$$

Recall. n is congruent if and only if there exist $x, y \in \mathbb{Q}$ with $y \neq 0$ such that $y^2 = x^3 - n^2 x$.

Proposition I.8.18. The positive integer n is a congruent number if and only if $\mathrm{rank} E_n(\mathbb{Q}) \neq 0$.

Recall (Proposition I.2). Let n be a squarefree positive integer. Suppose there exist $x, y \in \mathbb{Q}$ with such that $y^2 = x^3 - n^2 x$ and $x = s^2$ for some rational number s of the form

$$s = \frac{k}{2\ell}, \quad k, \ell \in \mathbb{Z}, \gcd(k, 2\ell) = 1, \quad \gcd(k, n) = 1.$$

Then there exist a right triangle with area n with sides

$$a = \sqrt{x+n} - \sqrt{x-n}, \quad b = \sqrt{x+n} + \sqrt{x-n}, \quad c = 2\sqrt{x}.$$

Proposition I.9.19 . There is a one-to-one correspondence between the following two sets:

$$C_n := \{(a, b, c) : a < b, a^2 + b^2 = c^2, \ ab = 2n\}$$
$$S_n := \{(x, \pm y) : \ (x, \pm y) \in 2E_n(\mathbb{Q}) - \{\mathcal{O}\}\},$$

given by

$$(a, b, c) \mapsto \left(\frac{c^2}{4}, \pm\frac{(b^2 - a^2)c}{8}\right),$$
$$(x, \pm y) \mapsto \left(\sqrt{x+n} - \sqrt{x-n}, \sqrt{x+n} + \sqrt{x-n}, 2\sqrt{x}\right).$$

Proposition I.9.20 . Let E be the elliptic curve

$$E : \; y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3), \quad , \alpha_i \in \mathbb{Q}.$$

Let $P = (x_0, y_0) \in E(\mathbb{Q}) - \{\mathcal{O}\}$. Then

$P = (x_0, y_0) \in 2E(\mathbb{Q}) - \{\mathcal{O}\}$ if and only if all $x_0 - \alpha_i$ are squares of rational numbers.