Elliptic curve $E : Y^2 = X^3 + aX + bZ^2, a, b \in \mathbb{Q}, \Delta = 4a^3 + 27b^2 \neq 0$

There are variables $X \rightarrow \mathbb{C}$, $Y \rightarrow \mathbb{C}$, $Z \rightarrow \mathbb{C}$ (assumed $a, b \in \mathbb{C}$)

Look at them mod $p$, curve $E$ over $\mathbb{F}_p$

1) Algebraic groups of dim 1. Assume $K$ is a separable field (every finite extension is separable)

Elliptic curves: only irreducible projective curves having group structure defined by polynomials

- Additive group $\mathbb{G}_a$
  
  $\mathbb{A}^1(K) = K, (x, y) \mapsto x + y : K \times K \rightarrow K$

- Multiplicative group $\mathbb{G}_m$

  $\mathbb{A}^1(K) \setminus \{0\} = K^\times, (x, y) \mapsto xy : K \times K \rightarrow K$

  $(x + y, x - y) \mapsto \mathbb{G}_m \subset \mathbb{A}^1$ affine $X_Y = 1$

- Twisted multiplicative groups, a nonsquare in $K^\times, q = \sqrt{-1}$

  Let $\mathbb{G}_m^q(a)$ (this is definition) over $K$ s.t.

  $\mathbb{G}_m^q(a)(K) = \{(x \in K^\times | N_{K/L}(x) = 1) \}$

  Define $\mathbb{G}_m^q(a)$ to be $X^2 - aY^2 = 1$ with group structure

  $(x, y), (x', y') \mapsto (xx' + ayy', x'y' + x'y)$

  Involutory change of variables by transform $\mathbb{G}_m^q(a) \rightarrow \mathbb{G}_m^q(a')$

  $\overline{\mathbb{E}}(a)$ only depends on $K(\sqrt{a})$

  When $a$ is square in $K^\times : X^2 - aY^2 = (x + y)(x - y) = x^2 - y^2$

  1) $\mathbb{G}_m^q(a) \cong \mathbb{G}_m$ over $K(\sqrt{a}) = k$, hence $x^2 - y^2$ is a twist $\mathbb{G}_m^q(a)$
C, D projective plane curves, hom-ns. Comps. in common
m n

\[ X^2 - \alpha Y^2 = 0 \]

\[ \sum_{a, b \in \mathbb{C}(k)} \mathbb{C}(k)^{a+b} \]

**Ex.**

\[ k = \mathbb{F}_q \implies [G_n(k)] = q \quad \left\{ \begin{array}{ll} G_m(k) & = q - 1 \quad \text{for any non-square } \alpha_m \\ G_m(\alpha_m) & = q - 1 \end{array} \right. \]

From field theory, \( \mathbb{F}_q(\sqrt{\alpha}) = \mathbb{F}_{q^2} \)

| Sequence | \( \mathbb{F}_q \longrightarrow G_m(\alpha_m) \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q} \rightarrow 0 \) |

In any characteristic, by 1st isomorphism thm, \( [G_m(\alpha_m)] = q - 1 \)

Q. In general, talk if nonsingular projective curve has genus 1, then it has a group structure, Converse is true. Uses Lefschetz fixed pt theorem.

Sing. cubic curves E singular plane projective curve over \( \mathbb{F}_q \).

\[ k, \text{ char}(k) \neq 2 \]

\[ k \text{ prime field } \mathbb{F}_q \implies \text{ only } 1 \text{ sing. pt. } \]

Assume \( E(k) \) has pt O \( \neq S \); then \( E_S = E(k) \setminus \{S\} \) is a group with zero 0.

\[ \text{Conubber line through two singular points } P, Q \text{ by Bezout, it will only intersect at one additional pt. } PQ \text{ which isn't sing.} \]

\( PQ = 3rd \) pt of intersection of two line through sing. points.

(1) Cubic curves \( \mathbb{F}_q \) cubic:

\[ (12) \]

\[ E: Y^2 = X^3 + a, b/c Y^2 = X^3 \text{ has } q \]

\[ \text{cusp at } \left( 0, 0 \right) \]

Only pt on curve \( Y \)-coord. 0, so \( E(k) \setminus \{S\} = E_1 \{Y \neq 0\} \)

\[ = E_1 : Z = X^2 \]

\[ Z = \alpha X + \beta \quad \text{int. of } X \quad \text{at } P_i = (X_i, Z_i), 1 \leq i \leq 3 \]

\[ X^3 = X - \beta \]

\[ X + X_2 + X_3 = 0 \quad \text{by Vieta} \]

\[ \text{When } P_1 + P_2 + P_3 = 0 \quad (i.e., \text{all lie on same line}) \]

\[ X(P_1) + X(P_2) + X(P_3) = 0 \]
\[ y^2 = x^3 + ax^2 \]

Tangent at \( y = \pm \sqrt{ax^2} \)
define \( y = \pm \sqrt{ax^2} \)
define \( x = \pm \sqrt{y^2} \)

\[ \{ a = 0 \} \rightarrow \text{node} \]
\[ a < 0 \rightarrow \text{cusp} \]

Singularity at \( (0,0) \)

\[ \Theta = (0,0) \rightarrow P \rightarrow \text{P is} (x, z) \rightarrow (x^2 - z^2) \]

So \( P \rightarrow X(P) \) satisfies

\[ x(-P) = -x(P) \]

\[ \theta(P) \rightarrow \text{E}(k) \rightarrow \text{a homomorphism} \]

\[ E \rightarrow \mathbb{G}_a \]

\[ p \rightarrow \theta(p) \]

\( E \rightarrow \mathbb{G}_a \) is an isomorphism of algebraic groups.

\[ \text{Cubic Curve over } \mathbb{Q} \text{ with a node:} \]

\[ (a, b, c) \rightarrow y^2 = x^3 + ax^2 + bx + c \]

has a node at \( (0,0) \)

Tangent lines at \( (0,0) \) given by \( y^2 = c = 0 \)

\[ (y - \sqrt{c})(y + \sqrt{c}) = x \text{ when } c \text{ is square} \]

\[ E^{ns} = \text{E-singular } p + 3 \]

\[ E \cong \mathbb{G}_a \]

- No square \( \Rightarrow \) tangent lines not rational over \( K \)

\( \text{Criterion } E: y^2 z = x^3 + axz^2 + bx^2 \quad a, b \in K, \Delta = 4a^3 + 27b^2 = 0 \)

Which of the above cases does \( E \) fall into? Assume \( char(k) \neq 2 \)

\( (0,1,0) \) always nonsingular \( \Rightarrow \) only need to study.

\[ y^2 = x^3 + ax + b \]

We wish to find \( a \) s.t.

\[ y^2 = (x^2 + 2t)^2 - (x^3 + 2t)^2 = x^2 - 3 + 2x + 2t \]

\( \Rightarrow \) need to choose \( t \) s.t.

\[ t^2 = -\frac{a}{3}, \quad t^3 = \frac{b}{2} \Rightarrow \frac{b}{a^2} = -\frac{3}{2} \]

Rewrite as

\[ y^2 = (x^2 + t^2)^2 \]

Has singularity at \( (t, 0) \)

\( \{ a = 0 \} \rightarrow \text{cusp if } \exists t = 0 \)

\( \{ a < 0 \} \rightarrow \text{node if } \exists t \text{ is square in } K \)

\( \{ a > 0 \} \rightarrow \text{node if } \exists t \text{ is an irrational tangent if } \Delta \) is square in \( K \)

\[ \text{For } a, b = -2(-t^2)(2t^3) = (2t^2)^3 + 3t \]

\( \Rightarrow 3t \) is non-zero \( \Leftrightarrow \Delta \text{ is square or nonsquare, according to } -2ab \)
Reduction of an elliptic curve

\[ E : y^2 = x^3 + ax + b \]

\[ \Delta = 4a^3 + 27b^2 \neq 0 \]

Change \( x \to x/c^2, y \to y/c^3 \) \( \forall c \) chosen s.t. \( a, b \) are minimal.

Equation is minimal.

\[ \bar{E} : y^2 = x^3 + ax^2 + bx \]

\( a, b \equiv a, b \mod p \) is reduction \( \mod p \)

3 cases:

(a) Good reduction: \( p \neq 2 \) and \( p \nmid \Delta \) then \( \bar{E} \) is an e.c. over \( \mathbb{F}_p \)

(b) \( p = 4g^2 + 27b^2 \) \( \Rightarrow \) choose rep. \((x, y, z)\) \( \forall \) \( x, y, z \in \mathbb{F}_p \)

- and having \( g \cdot d(x, y, z) = 1 \) \( \Rightarrow \) \( p = (x : y : z) \) well-defined

As \((0, 1, 0) \equiv (0, 1, 0) \) and lines relate to lines.

\( E(\mathbb{Q}) \rightarrow E(\mathbb{F}_p) \) hom

(b) Weil reduction: \( E \) has \( \nu \leq p \), i.e. \( p \neq 2, \alpha \nmid 2

(c) \( E \) has node, i.e. \( p \neq 2, \alpha \nmid 2

- Split reduction: Tangency at nodes are rational over \( \mathbb{F}_p \)

- \( -2ab \) is square in \( \mathbb{F}_p \)

- \( \frac{(a)}{p} \cdot \frac{(b)}{p} = \frac{(p^2 + 4p - 5)}{q} \cdot \frac{(p+1)(p+3)}{q} = (-1) \)

- \( E^{ns} \cong \mathbb{G}_m \)

- Nonsplit reduction: \( \neq -2ab \) not \( q \) square in \( \mathbb{F}_p \)

- \( E^{ns} \cong \mathbb{G}_m \cdot (-2ab) \)

- \( E^{ns} \cong \mathbb{G}_m \cdot (-2ab) \)

- \( E^{ns} \cong \mathbb{G}_m \cdot (-2ab) \)
<table>
<thead>
<tr>
<th>Type</th>
<th>Tangents</th>
<th>$\Delta \text{mod } p$</th>
<th>$-2ab \text{mod } p$</th>
<th>$E_n^\infty$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>good</td>
<td>$\neq 0$</td>
<td>0</td>
<td>0</td>
<td>$G_a$</td>
<td>$p$</td>
</tr>
<tr>
<td>$\mathcal{C} \mathcal{P}$</td>
<td>0</td>
<td>0</td>
<td>$G_m$</td>
<td>$p-1$</td>
<td></td>
</tr>
<tr>
<td>node</td>
<td>rational</td>
<td>0</td>
<td>0</td>
<td>$G_a(-2\beta)$</td>
<td>$p+1$</td>
</tr>
<tr>
<td>node</td>
<td>not rational</td>
<td>0</td>
<td>$\neq 0$</td>
<td>$G_a(-2\beta)$</td>
<td></td>
</tr>
</tbody>
</table>

The key equation is: $$(w')^2 = 4w^2 - k_1w - k_2$$

Suppose a solution of the form $\frac{4\theta}{2} + \frac{4\theta^2}{2} = 0$.

We may integrate this equation.

$$w' = \frac{3}{2}w^{\frac{3}{2}} + \frac{1}{4}w$$

Multiply by $w' \Rightarrow c'w = \frac{3}{4}w^{\frac{5}{2}} + \frac{1}{4}w'' + \gamma, w'$

$$\Rightarrow \frac{c}{2} - \frac{1}{4}w^{\frac{3}{2}} + \frac{1}{2}w'' + \gamma, w''$$

$$\Rightarrow (w')^2 = -2w^3 + 4c'w^2 - 8\gamma w - 8\gamma$$

The general solution to this equation can be written in terms of a Weierstrass $\wp$-function, specifically:

$$\wp(z) = -2c(z + c_1k_2k_3) + \frac{2c}{3} + \text{constant } \wp$$

with:

$$k_1 = \frac{4\gamma}{3} - \frac{4}{3}, k_2 = \frac{8\gamma}{3}, k_3 = \frac{4\gamma}{3}$$

$$\Rightarrow \wp(z) = -2c(x + ct + c_1k_2k_3) + \frac{2c}{3} \text{ soln. } \wp \in \mathbb{C}$$