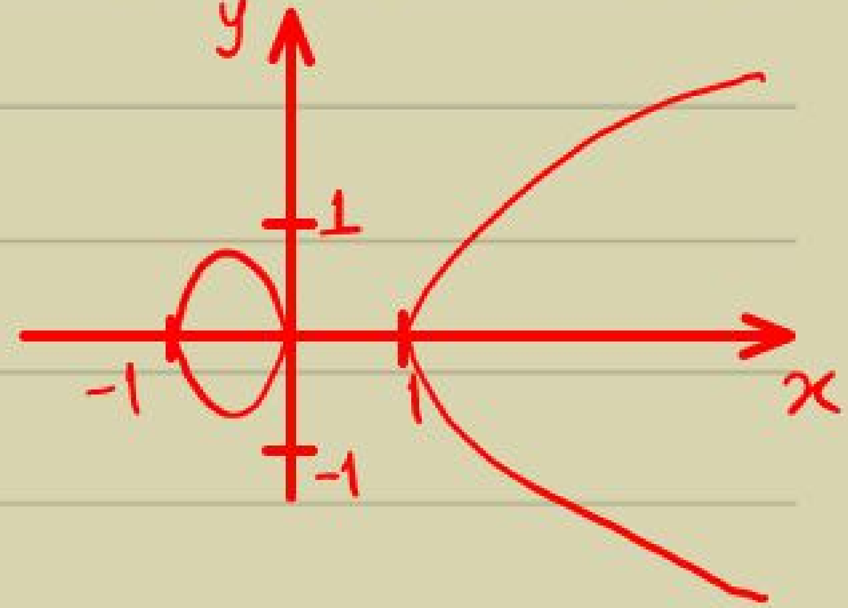
Elliptic Curves

- Elliptic curves are the most basic algebraic-geometric objects (with a rich theory).

- Defn: • Let $\mathbb{F}$ be a field of char $\neq 2,3$ & $x^3+ax+b \in \mathbb{F}[x]$ be square-free.
  • Then, $E = \{(u,v) \in \mathbb{F}^2 \mid v^2 = u^3+au+b\} \cup \{O\}$ is an elliptic curve over $\mathbb{F}$.
  • O is the point at infinity.

- Eg. $E: y^2 = x^3 - x = (x+1)x(x-1)$ over $\mathbb{R}$.



- Its homogenized, or projective, version is
$E_{pr}: y^2 z = x^3 - x z^2$.

▷ $E \longrightarrow E_{pr} \longrightarrow E$

$(u,v) \longmapsto (u:v:1)$

$(u:v:w) \longmapsto \left(\frac{u}{w}, \frac{v}{w}\right)$ for $w \in \mathbb{F}^*$

- This almost gives a bijection between E & E_{pr}, except the "extra" point $(0:1:0)$. This is denoted by O, the point at infinity of E.

- Elliptic curves are interesting because the set E can be seen as a group:

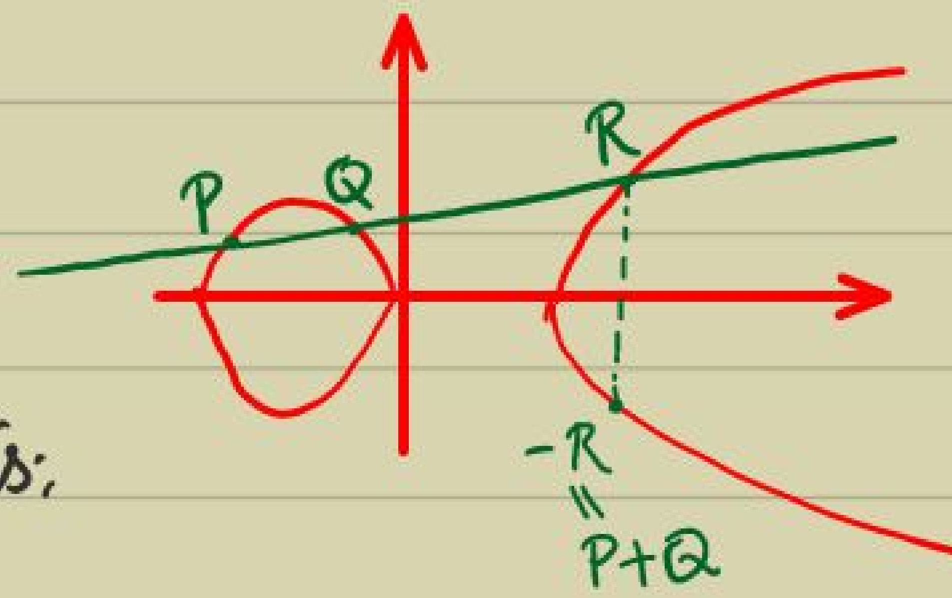
▷ $\forall P, Q \in E$, the line joining them has to intersect E in a third point $R \in E$. Let us denote R by $P \circ Q$.

▷ For a point $(u, v) = P \in E$, define $-P := (u, -v)$. Clearly, $-P \in E$.

▷ The map $\begin{array}{c} E \times E \longrightarrow E \\ (P, Q) \mapsto -(P \circ Q) \end{array}$ makes E into an abelian group, with O as the unity.

Pf: (a nontrivial exercise) $\square$

- Pictorially, the points "addition" is:



- Interesting special cases (with $P \in E$):
  - $P+P =: 2P$ (draw the tangent at P)
  - $P+O = P$ (draw a line parallel to Y-axis)
  - $P-P =: P+(-P) = O$.
  - $k.P =: \begin{cases} P \text{ added } k \text{ times}, & \text{if } k>0, \\ -P \text{ added } -k \text{ times}, & \text{if } k<0, \\ O, & \text{if } k=0. \end{cases}$

- Computing the sum: We can easily deduce explicit formulas to compute it.
  - $E: y^2 = x^3+ax+b$ with points $P_1 = (x_1, y_1)$ & $P_2 = (x_2, y_2)$.
  - If $x_1 = x_2$ then $P_1+P_2 = O$.
  - Else the line-(P_1, P_2) is $Y = mX+c$, where $m := \dfrac{y_2-y_1}{x_2-x_1}$ & $c := y_1 - mx_1$.

$\Rightarrow x(P_1+P_2)$ is given by the "third" root of $(mx+c)^2 = x^3+ax+b$

$\Rightarrow x^3 - m^2x^2 + (a-2mc)x + (b-c^2) = 0$

$\Rightarrow x(P_1+P_2) = m^2 - (x_1+x_2)$ &

$y(P_1+P_2) = -m \cdot x(P_1+P_2) - c$.

- The above facts hold true for any E over a finite field $\mathbb{F}_q$ as well.

- Now we can ask the question: Can we compute, or estimate, $\#E$?

- Heuristic estimate: $\#E(\mathbb{F}_q) = 1 + \sum_{0\leq x<q} 2\cdot[x^3+ax+b \text{ is a square}]$

0 or 1 value

$\approx 1 + 2\cdot\frac{q}{2} = (q+1)$.

- One of the first gems of algebraic geometry is:

Thm (Hasse, 1933): $|\#E - (q+1)| \leq 2\cdot\sqrt{q}$.

- This is called the Hasse bound or the Riemann hypothesis (for zeta functions of elliptic curves).

Lenstra's elliptic curve factoring (ECM)

- In 1987, Lenstra gave an idea for integer factoring using elliptic curves.

- Idea: Pick a random point $P \in (\mathbb{Z}/n\mathbb{Z})^2$ and a random elliptic curve $E \ni P$.

  Let $p|n$ be the smallest prime factor and assume that $\#E(\mathbb{F}_p)$ is B-smooth.

  Try to find k s.t. $k \cdot P = O$ in $E(\mathbb{F}_p)$. Hopefully, $k \cdot P \neq O$ in $E(\mathbb{Z}/\frac{n}{p}\mathbb{Z})$. This factors n.

Input: n coprime to 6 & not a perfect power. Bounds B (for factor base) & C (for smallest $p|n$).

<u>Output</u>: Factoring n.

<u>Algo</u>:

1) Randomly pick $a, u, v \in (\mathbb{Z}/n\mathbb{Z})^*$.

   Let $b = v^2 - u^3 - au$.

2) Consider $E: y^2 = x^3 + ax + b$ over $\mathbb{Z}/n\mathbb{Z}$ with a point $P = (u, v)$.

   Let $\{p_1, \dots, p_B\}$ be the primes in the <u>factor base</u>.

3) For $i = 1, 2, \dots, B$

   $e_i = \lfloor \log_{p_i} (c + 1 + 2\sqrt{c}) \rfloor$

   for $j = 0, 1, \dots, e_i$

   Try computing $\prod_{0 \le r < i} p_r^{e_r} \cdot p_i^j \cdot P$ by repeated squaring. If some step requires division by a <u>zerodivisor</u> then <u>factor n</u>.

4) OUTPUT fail.

Analysis: Let $p | n$ be the smallest prime $< C$.

- Lenstra showed that:
  $\Pr_E [\# E(\mathbb{F}_p) \in S] \geq \#S / 2\sqrt{p}\log p$
  for $S \subset (p+1-\sqrt{p},\ p+1+\sqrt{p})$.

- This, with the smoothness estimate, gives:
  $\Pr_E [\# E(\mathbb{F}_p) \text{ is } (B = p^{1/u})\text{-smooth}] \approx u^{-u}/\log p$.

  $\Rightarrow$ Getting $\# E(\mathbb{F}_p)$ B-smooth would take $(u^u \cdot \log p)$-many trials.

- $\Rightarrow$ the dominant term in the time complexity (of Step 3) is: $u^u \cdot \log p \cdot \sum_{i \in [B]} e_i \cdot \log p_i \cdot \log n$

  $\approx u^u \cdot \log p \cdot B \cdot \log C \cdot \log n$

- $u^u \cdot B = u^u \cdot p^{1/u}$ is minimized when
  $u^{-1} \cdot \log p \approx u \cdot \log u \Rightarrow u = \sqrt{2 \cdot \log p / \log\log p}$.

  $\Rightarrow \log B \approx \frac{1}{\sqrt{2}} \cdot \sqrt{\log p \cdot \log\log p}$.

$\Rightarrow$ time complexity $\approx L_p\left(\frac{1}{2}, \sqrt{2}\right)$.

- Thus, ECM is best when p is relatively <u>small</u>.

<u>Success</u>: Brent (90s) factored the Fermat numbers F_{10} & F_{11}.
(${F_{12}}$ to F_{23} are composite but we do not know the factors!)