Ronyan Sharif: Birch & Swinnerton-Dyer

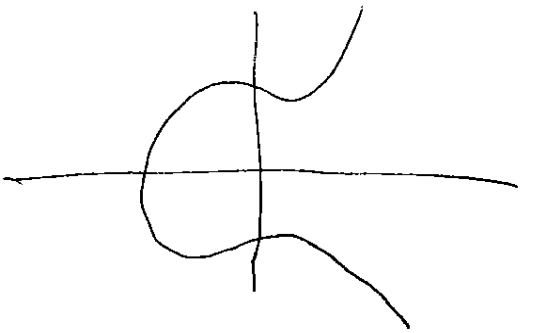
Elliptic curves: eqns of form $y^2 = x^3 + ax + b$ E

$a, b \in \mathbb{Z}$

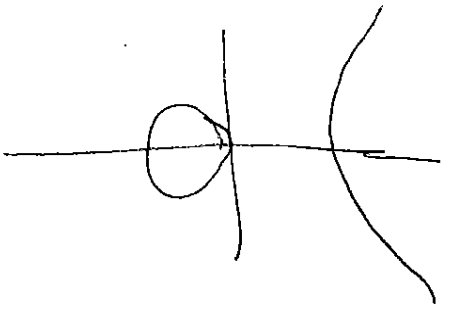
Possibly more general form for elliptic curve:

$$\left(y^2 + a_1 y + a_3 xy = x^3 + a_2 x^2 + a_4 x + a_6 \right)$$

$y^2 = x^3 - x + 1$

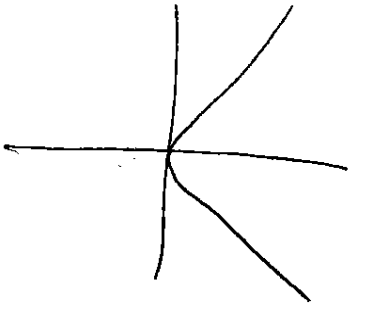


$y^2 = x^3 - x + 0$



$y^2 = x^3 - x - 1$

$y^2 = x^3 + x$



3 possibilities :

Elliptic curve always has nice derivative; does not have a cusp.

~~Does have a self-crossing singularity~~

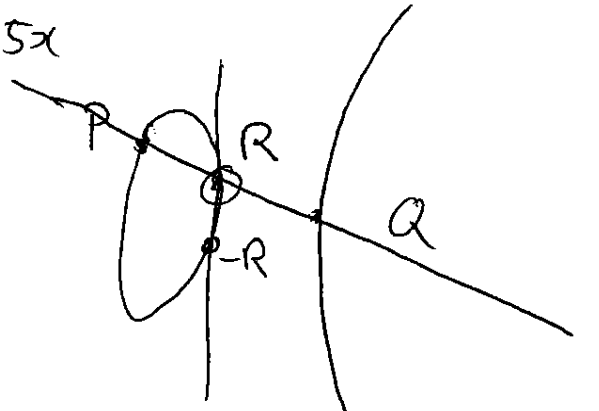
Also, elliptic curve can't have a node – a self-crossing singularity.

Discriminant, Δ of E: $\Delta = -16(4a^3 + 27b^2)$

$\Delta = 0$ iff E has a cusp or a node.

So E is an elliptic curve iff $\Delta \neq 0$.

Addition on elliptic curves $y^2 = x^3 - 25x$



$P(-4,6)$

$Q(5,0)$

R = pt where line PQ meets E

Define $P+Q+R=0$.

$-R$ = pt where vertical line through R intersects the curve.

How to add P to itself?

Take tgt line to E through P, see where it crosses E. If it never crosses E again then

$P+P=O$.

Fact On this curve, for any $n \neq 0$, $nP \neq O$.

There are points Q for which $nQ=O$.

P said to have infinite order.

Q has finite order.

Suppose we consider points on the curve whose coordinates lie in $\mathbb{Q}$.

Question What are the points on E with rational coordinates.

Fact If P, Q have rational coordinates, then so does $P+Q$.

$E(\mathbb{Q}) = \{$ pts of E with rational coordinates $\} \cup \{\infty\}$.

∞ is the "O". Called the Mordell-Weil group of E.

Q. How big is $E(\mathbb{Q})$?

Ex 1) $y^2 = x^3 - x$ $\quad E(\mathbb{Q}) = \{(0,0), (1,0), (-1,0), \infty\}$.

2) $y^2 = x^3 - 5x$ $\quad E(\mathbb{Q})$ contains $n(-4,6)$, $n(-4,6)+(5,0)$ $\forall n$.

Also $n(-4,6)+(0,0)$, $n(-4,6)+(-5,0)$.

Mordell's Theorem Let E be an elliptic curve. Then there is an integer $r \geq 0$ and points $P_1, \dots, P_r \in E(\mathbb{Q})$ s.t. every point in $E(\mathbb{Q})$ is has the form

$$n_1 P_1 + n_2 P_2 + \dots + n_r P_r + Q$$

where $n_1, \dots, n_r \in \mathbb{Z}$ and Q is a point of finite order.

Def The minimal possible r is called the rank of the elliptic curve

Exs 1. rank of $y^2 = x^3 - x$ is 0.

2. rank of $y^2 = x^3 - 5x$ is 1.

The highest known rank is 28 : Elkies, 2006.

Not known if possible ranks are unbounded.

BSD tells what the rank of an elliptic curve can be.

L-function of E: $L(E,s)$ complex-valued function of $s \in \mathbb{C}$.

$L(E,s)$ is defined and ∞'ly differentiable for all real s.

Conjecture $L^{(k)}(E,s)$. k-th derivative.

Def the smallest $k \geq 0$ s.t. $L^{(k)}(E,1) \neq 0$ is called the analytic rank of E.

Conjecture The rank of an elliptic curve E equals its analytic rank.

Def Fix prime p. $y^2 = x^3 + ax + b$ mod p if $y^2 - (x^3 + ax + b)$ is divisible by p; where $x, y \in \mathbb{Z}$.

N_p = # of roots of E mod p.

$a_p = p - N_p$.

Consider $$L(E,s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

Fact $L(E,s)$ is finite if $s \geq \frac{3}{2}$.