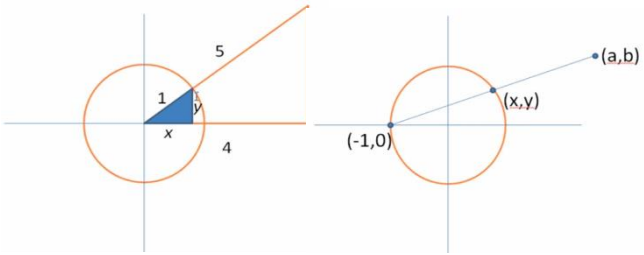
Millenium Problems: Birch und Swinnerton-Dyer Vermutung

Elliptische Kurve gegeben durch eine Gleichung

$$y^3 = x^3 + Ax + B \text{ mit } A, B \in \mathbb{Z} \text{ (und } 4A^3 + 27B^2 \neq 0)$$

Frage: Wie viele rationale Punkte besitzen Kurven der obigen Art? Wie kann man diese Punkte „finden“?



Einfache Betrachtung:

Euklid:

$x^2 + y^2 = z^2 \qquad (x, y, z \in \mathbb{Z})$

minimierbar auf Einheitskreis

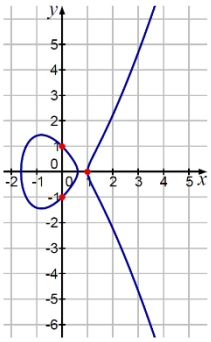
➔ $x = \frac{a^2-b^2}{a^2+b^2}; y = \frac{2ab}{a^2+b^2} \qquad \rightarrow$

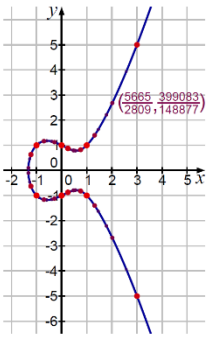
$X = a^2 - b^2; Y = 2ab; Z = a^2 + b^2$

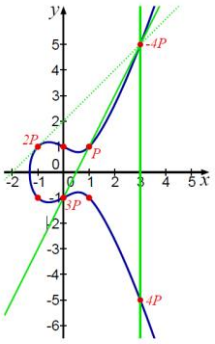
„einfach“ a und b auswählen (Gegensatz dazu: euklidische Tripel finden)

Zurück zu elliptischen Kurven:

Bsp.: $E_0: y^2 = x^3 - 2x + 1$ $\qquad$ $E_1: y^2 = x^3 - x + 1$







$4 \cdot P = (3, -5)$

Findung rationaler Punkte:

Gruppenstruktur (Sekanten-/Tangentenverfahren P. de Fermat):

Satz von Mordell (1922):

Gruppe $E(\mathbb{Q})$ (Menge der rationalen Punkte) ist stets endlich erzeugt.

Nun: Statt rationale Punkte, Rechnung mit ganzen Zahlen modulo p:

Frage: Wieviele Punkte modulo p besitzen die Kurven?

$$N_p = p + A_p$$

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$N_p(E_0)$	2	3	4	11	7	15	15	15	19	31	39	31	47	51	43
$A_p(E_0)$	0	0	−1	4	−4	2	−2	−4	−4	2	8	−6	6	8	−4
$N_p(E_1)$	2	6	7	11	9	18	13	21	22	36	34	35	50	51	38
$A_p(E_1)$	0	3	2	4	−2	5	−4	2	−1	7	3	−2	9	8	−9

Vermutung von Birch und Swinnerton-Dyer:

Eine elliptische Kurve hat genau dann unendlich viele rationale Punkte, falls die Summe über $\frac{A_p}{p}$ für $p < X$ mit X über alle Grenzen wächst.

Präzisere Form, statt Summe ein Produkt: $L(E, s) = \prod_p \frac{1}{1+A_p p^{-s}+p^{1-2s}}$

Vermutung: $L(E, 1) = 0 \Leftrightarrow$ E besitzt unendlich viele rationale Punkte.