Experiments with Canonical Heights on Elliptic Curves

Thank you

Dr Laga

Ms Mok

Dr Rezaee

Prof Ranganathan

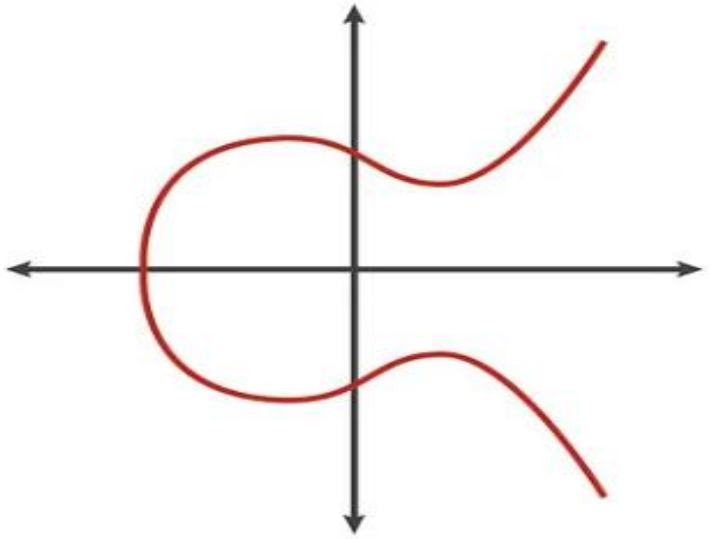
Ms Baume

CCIMI

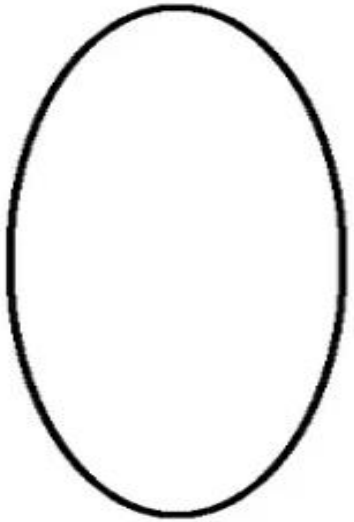
Faculty of Mathematics

G-Research

Elliptic Curve vs Ellipse



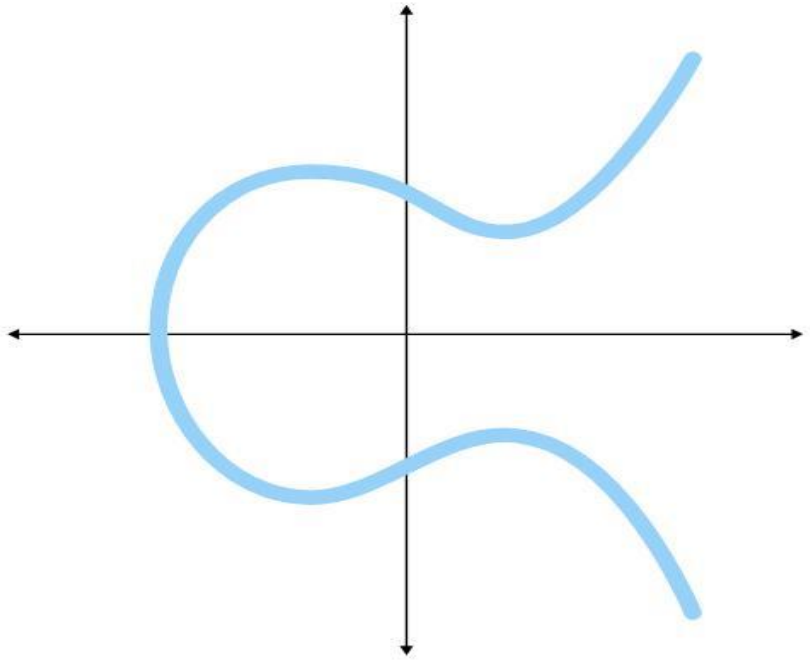
Elliptic Curve



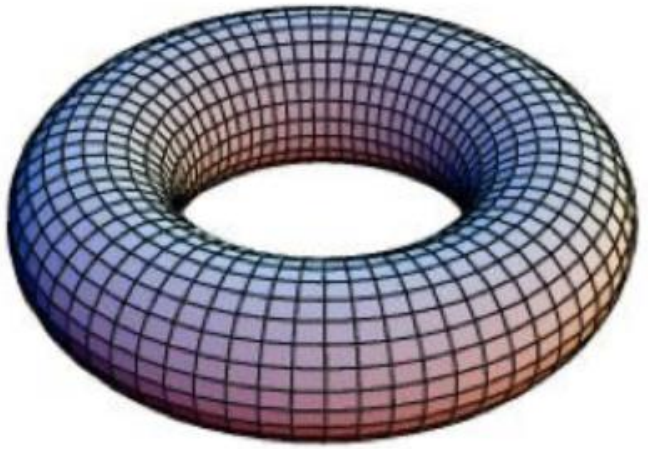
Ellipse

Elliptic Curves Over R and C

Over Real Numbers



Over Complex Numbers

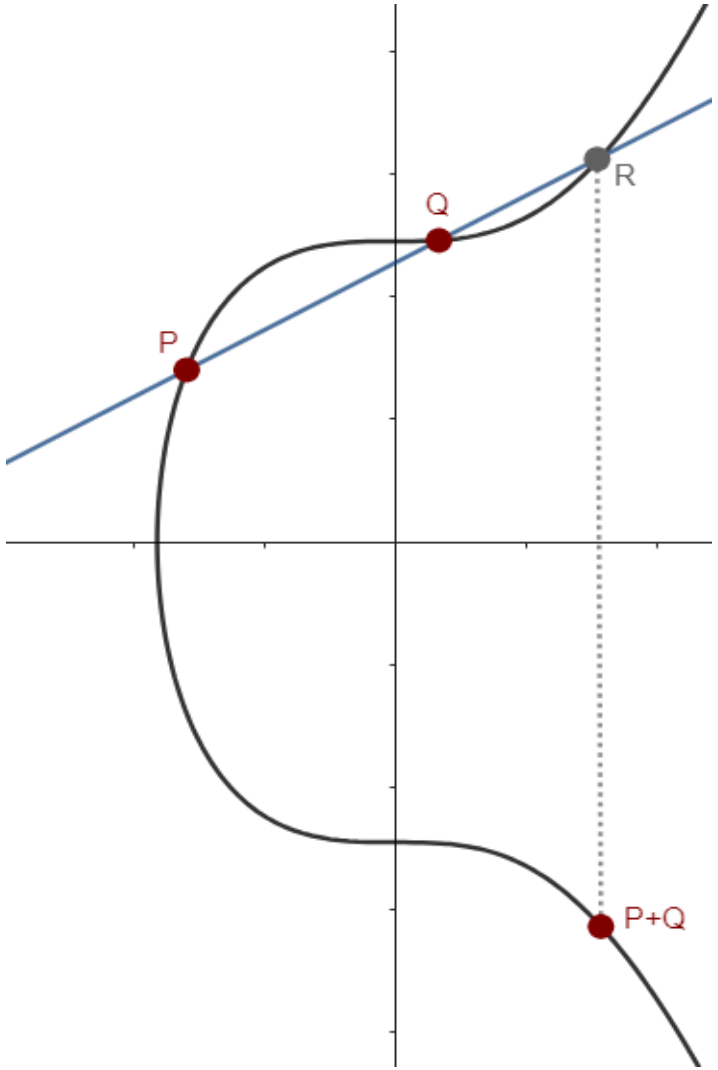


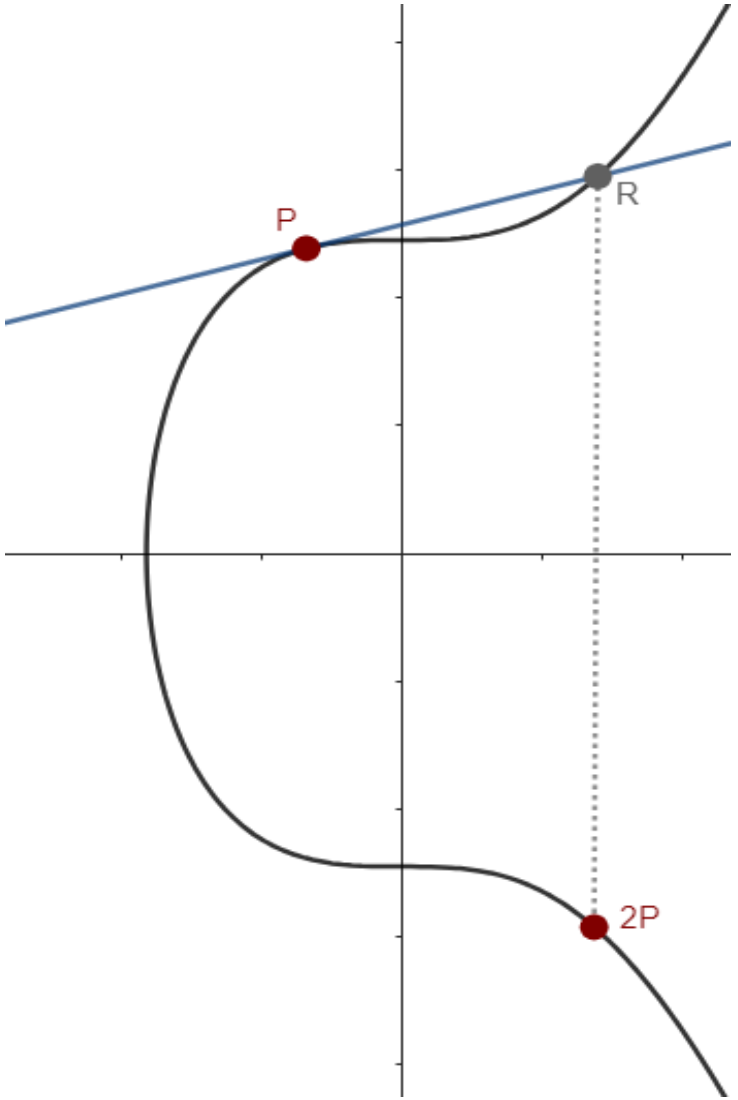
Elliptic Curves Over Q

$$E : y^2 = x^3 + Ax + B$$

$$(A, B \in \mathbb{Q} \implies A, B \in \mathbb{Z})$$

Addition of Points





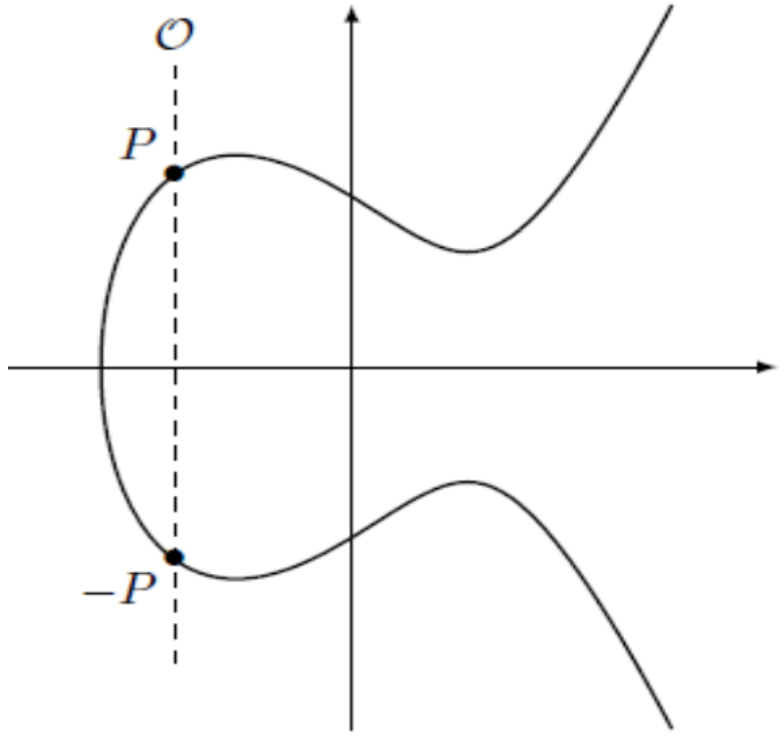
Point at infinity

In projective geometry, parallel lines intersect.

$P + \mathcal{O} = P = \mathcal{O} + P.$

$\mathcal{O}$ is the identity.

Turns out $(E, \oplus)$ is an abelian group.



Mordell-Weil Theorem

$E(\mathbb{Q})$ is a finitely generated abelian group.

Using the structure theorem:

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E_{tors}(\mathbb{Q})$$

$\mathbb{Z}^r$: **free part**
r: **rank**.

Heights

For a point $P = (x, y)$ on $E(\mathbb{Q})$, let $x = \frac{a}{b}$:

$$H(P) = H(x) = max\{|a|, |b|\}$$

$$h(P) = log(H(P))$$

Canonical Height

Measures the *arithmetic complexity* of a rational point P.

$$\hat{h} : E(\overline{\mathbb{Q}}) \to \mathbb{R},$$

$$\hat{h}(P) = \lim_{N \to \infty} 4^{-N} h([2^N]P).$$

Regulator

Height pairing between P and Q:

$$\langle P, Q \rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$$

Let $P_1, ..., P_r$ be the generators of the free part,

the **elliptic regulator** of $E/\mathbb{Q}$ is:

$$R_{E/\mathbb{Q}} = det(\langle P_i, P_j \rangle)_{\substack{1 \le i \le r \\ 1 \le j \le r}} .$$

Our Conjecture

Let p be an odd prime. For two elliptic curves E_{4p} and E_{-p} over $\mathbb{Q}$ with equations:

$$\begin{cases} E_{4p} : y^2 = x^3 + 4px, \\ E_{-p} : y^2 = x^3 - px \end{cases}$$

we have :

(a) rank $= 1$ iff $p \equiv 5, 7, 9, 15 \pmod{16}$

(b)

$$R_{E_{4p}/\mathbb{Q}} = \begin{cases} \frac{1}{2} R_{E_{-p}/\mathbb{Q}}, & \text{iff } p \equiv 5, 9 (mod 16), \\ 2R_{E_{-p}/\mathbb{Q}}, & \text{iff } p \equiv 7 (mod 8). \end{cases} \tag{1}$$

(c)

$$rank = 2 \implies \begin{cases} p \equiv 1 (mod 16), \\ and \\ R_{E_{4p}/\mathbb{Q}} = R_{E_{-p}/\mathbb{Q}}. \end{cases} \tag{2}$$

(d) rank ≤ 2

First Encounter

A	Reg	rank
-11	1	0
-10	1.281529	1
-9	1	0
-8	1	0
-7	1.634282	1
-6	0.844191	1
-5	0.635529	1
-4	1	0
-3	1	0
-2	0.608709	1
-1	1	0
7	1	0
8	1.217418	1
9	1.777252	1
10	1	0
11	1	0
12	1	0
13	2.992409	1
14	2.967457	2
15	1.134764	1
16	1	0
17	1	0
18	0.714741	1
19	2.098759	1
20	1.271057	1
21	3.600933	1
22	1	0
23	1	0
24	1.688382	1
25	1	0
26	1	0
27	1	0
28	0.817141	1
29	3.668299	1

Diving Deeper

p	A = 4p	d	log|d|	Can h	Root number	A = -p	d	log|d|	Can h	mod 16	rank
2	8	-32768	4.51545	1.217418	-1		512	2.70927	0.608709	2	
3	12	-110592	5.043724		1		1728	3.237544		3	
5	20	-512000	5.70927	1.271057	-1		8000	3.90309	0.635529	5	
7	28	-1404928	6.147654	0.817141	-1		21952	4.341474	1.634282	7	
11	44	-5451776	6.736538		1		85184	4.930358		11	
13	52	-8998912	6.95419		1		140608	5.14801		13	
17	68	-2E+07	7.303707		1		314432	5.497527		1	2
19	76	-2.8E+07	7.448621		1		438976	5.642441		3	
23	92	-5E+07	7.697543	2.96538	-1		778688	5.891363	5.93076	7	
29	116	-1E+08	7.999554		1		1560896	6.193374		13	
31	124	-1.2E+08	8.086445	1.457284	-1		1906624	6.280265	2.914568	15	
37	148	-2.1E+08	8.316965	3.059739	-1		3241792	6.510785	1.52987	5	
41	164	-2.8E+08	8.450712	4.186349	-1		4410944	6.644532	2.093175	9	
43	172	-3.3E+08	8.512765		1		5088448	6.706585		11	
47	188	-4.3E+08	8.628654	2.247817	-1		6644672	6.822474	4.495634	15	
53	212	-6.1E+08	8.785188	9.719908	-1		9528128	6.979008	4.859954	5	
59	236	-8.4E+08	8.924916		1		13144256	7.118736		11	
61	244	-9.3E+08	8.968349		1		14526784	7.162169		13	
67	268	-1.2E+09	9.090584		1		19248832	7.284404		3	
71	284	-1.5E+09	9.166135	1.84118	-1		22906304	7.359955	3.68236	7	
73	292	-1.6E+09	9.202329	10.79487	-1		24897088	7.396149	5.397435	9	
79	316	-2E+09	9.305241	6.162387	-1		31554496	7.499061	12.32477	15	

Conjecture - Splitted

Let p be an odd prime. For elliptic curves E_{4p} and E_{-p} over $\mathbb{Q}$ with equations:

$$\begin{cases} E_{4p} : y^2 = x^3 + 4px, \\ \\ E_{-p} : y^2 = x^3 - px \end{cases}$$

Conjecture - Parts (a) & (b)

(a) $\text{rank} = 1$ iff $p \equiv 5, 7, 9, 15 \pmod{16}$

(b)

$$R_{E_{4p}/\mathbb{Q}} = \begin{cases} \frac{1}{2} R_{E_{-p}/\mathbb{Q}}, & \text{iff } p \equiv 5, 9 (mod 16), \\ 2R_{E_{-p}/\mathbb{Q}}, & \text{iff } p \equiv 7 (mod 8). \end{cases}$$

Conjecture - Parts (c)

$$rank = 2 \implies \begin{cases} p \equiv 1 (mod 16), \\ and \\ R_{E_{4p}/\mathbb{Q}} = R_{E_{-p}/\mathbb{Q}}. \end{cases}$$

Conjecture - Parts (d)

$$\text{rank} \leq 2$$

Attempting to Prove

- Isogenies
- Descent Calculations
- Root Numbers

Thank you very much for listening!