Results and Problems on Ranks of Elliptic Curves arising in the work of Tetsuji Shioda

Gary Walsh
gwalsh@uottawa.ca

Tutte Institute and
Dept. Math. University of Ottawa
Ottawa, Ontario, Canada

Number Theory Conference in Honour of Andrej Dujella
June 2025

CONGRATULATIONS ANDREJ!!



Andrej proved many many interesting results on elliptic curves over $\mathbb{Q}$ with fixed torsion and large rank! He inspires us all.

Overview of the Lecture

I. Miscellaneous Results and Strategies for Large Rank Curves.

II. Some New Strategies and Results for Large Rank Curves.

III. Related Open Problems.

Rank Records Over The Years

rank >=	year	Author(s)
3	1938	Billing
4	1945	Wiman
6	1974	Penney - Pomerance
7	1975	Penney - Pomerance
8	1977	Grunewald - Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao - Kouya
22	1997	Fermigier
23	1998	Martin - McMillen
24	2000	Martin - McMillen
28	2006	Elkies
29	2024	Elkies - Klagsbrun

Let E denote an elliptic curve given by

$$E : y^2 = x^3 + ax + b \qquad (a, b \in \mathbb{Z}).$$

The *height* of E is given simply by $\max(|a|, |b|)$.

Let us order elliptic curves by height, and look at the first

$$2.7 \times 10^{10}$$

elliptic curves:

Distribution of rank

Rank	# Curves	% Curves
0	78,039,852	32.685%
1	113,128,980	47.381%
2	40,949,307	17.151%
3	6,259,159	2.615%
4	380,519	0.159%
5	6481	0.003%
6	12	0.0005%
total	238,764,310	

average rank $= 0.901976$

A Strategy for Finding Curves of Large Rank

- Find a generic curve $E(t)$ over $\mathbb{Q}(t)$ with many points.

(the rank can be computed using the Gram matrix consisting of canonical height pairings)

- Find a specialization $t = t_0 \in \mathbb{Q}$ for which the resulting curve $E(t_0)$ over $\mathbb{Q}$ has large rank.

$E(t)$ has a large **jump** at t_0 if $rk(E(t_0)) - rk(E(t))$ is large.

The Record Holding Jump of Elkies and Klagsbrun (2020)

At ANTS XIV, Elkies and Klagsbrun reported on a family of generic curves of rank 9 over $\mathbb{Q}(t)$:

$$E = E_u(t): \ y^2 = x^3 + 2Ax + B,$$

with

$$\begin{aligned} A = {} & (u^8 - 18u^6 + 163u^4 - 1152u^2 + 4096)t^4 + (3u^7 - 35u^5 - 120u^3 + 1536u)t^3 \\ & + (u^8 - 13u^6 + 32u^4 - 152u^2 + 1536)t^2 + (u^7 + 3u^5 - 156u^3 + 672u)t \\ & + (3u^6 - 33u^4 + 112u^2 - 80), \end{aligned}$$

and $B = \prod_{i=1}^{8} B_i(t,u)$ where

$$\begin{aligned} B_1(t,u) &= (u^2 + u - 8)t + (-u + 2), & B_3(t,u) &= (u^2 - u - 8)t + (u^2 + u - 10), \\ B_5(t,u) &= (u^2 - 7u + 8)t + (-u^2 + u + 2), & B_7(t,u) &= (u^2 + 5u + 8)t + (u^2 + 3u + 2), \end{aligned}$$

and u is of the form $u = \frac{2m^2 - 2m - 2}{m^2 + 1}$.

Elkies and Klagsbrun Continued

9 parametric points over $\mathbb{Q}(t)$ can be written down for the curve $E = E_u(t)$.

For the particular choice $m = -3$, the value of u is $u = 11/5$, and for this value of u, the particular value $t = t_0 = -721141/2026305$ yields the following minimal model specialization of **rank 20**.

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

with a_1, a_2, a_3, a_4, a_6 given by

$$(1, -1, 1, -2445376733363196014638034871689617692707575738218598537 07,$$
$$961710182053183034546222979258806817743270682028964434238957830989898438151121499931).$$

The Point: The **jump** of 11 is a record!

Part II: $Y^2 = f(x) + t^2$

Theorem (Bud Brown and Bruce Myers, 2002)

For $m > 1$, let

$$E_m : \ y^2 = x^3 - x + m^2 \ \ \textit{and} \ \ P = (1, m), Q = (-1, m).$$

Then P and Q are independent points on E_m, and hence

$$rank(E_m) \geq 2.$$

$$E_m : \ y^2 = x^3 - x + m^2,$$

$$P = (0, m), Q = (-1, m), P + Q = (1, -m)$$

Proof.

(*i.*) There is no rational 2-torsion on E_m. ($y \neq 0$ on E_m)

(*ii.*) None of P, Q, $P + Q$ are in $2E_m$. (slightly tedious)

(*iii.*) $\{[O], [P], [Q], [P + Q]\}$ is a group of order 4 in $E_m/2E_m$. (*ii.*)

(*iv.*) $k, l \in \mathbb{Z}$ (not both 0) with $kP + lQ = O$ violates (iii.) if k, l are not both even and violate (i.) if k, l are both even.

Subsequent Related Results

- **P. Tadic (2012)- generic rank (function field)**

$E_m = y^2 = x^3 - x + m^2,\ m = m(t)$: $rank_{\mathbb{Q}(t)}\ E_{m(t)} \geq 2$.

- **Fujita and Nara (2017)**

$E_m = y^2 = x^3 - m^2x + n^2$: $rank\ E_m \geq 2$.

- **Rout and Juyal (2021)**

$E_m = y^2 = x^3 - m^2x + m^2$: $rank\ E_m \geq 2$.

- **Hatley and Stack (2021)**

$E_m = y^2 = x^3 - x + m^6$: $rank\ E_m \geq 3$.

Theorem 1. (W. 2022)

Let a, b denote distinct nonzero integers. There is an effectively computable constant $C = C(a, b) > 0$ with the property that if $m > C$ then the rank of the curve given by

$$y^2 = x(x + a)(x + b) + m^2,$$

is at least 2.

Proof: *i.* The curve has no rational 2-torsion. (Baker)
ii. $(-a, m)$ and $(-b, m)$ are points of infinite order. (Lutz-Nagell)
iii. $(-a, m)$, $(-b, m)$ and $(-a, m) + (-b, m) \notin 2E(\mathbb{Q})$. (Runge)

Our strategy to find curves with large rank:

- impose conditions on a, b, m giving a third independent point!

$$E : y^2 = x^3 + (a+b)x^2 + abx + m^2$$

For example, impose the condition $x^3 + m^2 = 0$.

This translates into $m = M^3$, $x = -M^2$ and there is an integer N for which

$$N^2 - (a+b)M^2 = -ab.$$

In this case, $R = (-M^2, NM)$ is a new integral point on the specialization.

```
SetClassGroupBounds("GRH");
R<x>:=PolynomialRing(Integers());
for a in [1..10] do
for b in [a+1..10] do
for M in [50..100] do
if IsSquare((a+b)*M^2-(a*b)) then
[a,b,M];
f:=x*(x+a)*(x+b)+M^6;
E:=EllipticCurve(f);
c1,c2:=RankBounds(E);c2;
end if;
end for;
end for;
end for;
```

Cancel

```
[ 1, 4, 89 ]
4
[ 1, 5, 69 ]
4
[ 1, 6, 79 ]
4
[ 1, 7, 64 ]
4
[ 2, 9, 57 ]
3
[ 3, 4, 62 ]
4
[ 4, 6, 62 ]
4
[ 4, 8, 82 ]
7
[ 4, 9, 53 ]
4
[ 5, 9, 81 ]
5
[ 7, 8, 78 ]
4
```

Theorem 2. (W. 2023)

Let a, b be non-zero distinct integers for which the Pell equation

$$X^2 - (a+b)Y^2 = -ab$$

is solvable in integers $(X, Y) = (n, m)$.

Then, under a certain irreducibility hypothesis, for m sufficiently large, the curve

$$E: \ y^2 = x(x+a)(x+b) + m^6$$

has rank $r \geq 3$.

Proof: $P = (-a, m^3)$, $Q = (-b, m^3)$, $R = (-m^2, nm)$ are independent for m sufficiently large.

Example $X^2 - 3Y^2 = -2, \quad (a, b) = (1, 2)$

$$X + Y\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^k, \quad k \in \mathbb{Z}$$

Example $X^2 - 3Y^2 = -2, \quad (a, b) = (1, 2)$

$$X + Y\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^k, \quad k \in \mathbb{Z}$$

$k = 0, Y = 1$: $E : y^2 = x^3 + 3x^2 + 2x + 1$, $rank(E) = 1$

Example $X^2 - 3Y^2 = -2, \quad (a, b) = (1, 2)$

$$X + Y\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^k, \quad k \in \mathbb{Z}$$

$k = 0, Y = 1$: $E : y^2 = x^3 + 3x^2 + 2x + 1$, $rank(E) = 1$

$k = 1, Y = 3$: $E : y^2 = x^3 + 3x^2 + 2x + 3^6$, $rank(E) = 4$

Example $X^2 - 3Y^2 = -2, \quad (a, b) = (1, 2)$

$$X + Y\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^k, \quad k \in \mathbb{Z}$$

$k = 0, Y = 1$: $E : y^2 = x^3 + 3x^2 + 2x + 1$, $rank(E) = 1$

$k = 1, Y = 3$: $E : y^2 = x^3 + 3x^2 + 2x + 3^6$, $rank(E) = 4$

$k = 2, Y = 11$: $E : y^2 = x^3 + 3x^2 + 2x + 11^6$, $rank(E) = 5$

Example $X^2 - 3Y^2 = -2, \quad (a, b) = (1, 2)$

$$X + Y\sqrt{3} = (1 + \sqrt{3})(2 + \sqrt{3})^k, \quad k \in \mathbb{Z}$$

$k = 0, Y = 1$: $E : y^2 = x^3 + 3x^2 + 2x + 1$, $rank(E) = 1$

$k = 1, Y = 3$: $E : y^2 = x^3 + 3x^2 + 2x + 3^6$, $rank(E) = 4$

$k = 2, Y = 11$: $E : y^2 = x^3 + 3x^2 + 2x + 11^6$, $rank(E) = 5$

$k = 3, Y = 41$: $E : y^2 = x^3 + 3x^2 + 2x + 41^6$, $rank(E) = 7$

Example Let $a = 1, b = t^2 - 2$ so the Pell equation becomes

$$X^2 - (t^2 - 1)Y^2 = -(t^2 - 2).$$

$$(1 + \sqrt{t^2 - 1}) \cdot (t + \sqrt{t^2 - 1})^k \to E_k(t) \qquad (k \in \mathbb{Z})$$

giving families of elliptic curves with moderate rank.

$$E_0(t): \ y^2 = x(x+1)(x+t^2-2) + 1$$

$$E_{\pm 1}(t): \ y^2 = x(x+1)(x+t^2-2) + (t \pm 1)^6$$

$$E_{\pm 2}(t): \ y^2 = x(x+1)(x+t^2-2) + (2t^2 \pm 2t - 1)^6$$

Conjecture (Birch and Swinnerton-Dyer - 1965)

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{\substack{p\leq x \\ p \text{ good}}} \frac{a_p \log p}{p} = -r + \frac{1}{2}.$$

Conjecture (Birch and Swinnerton-Dyer - 1965)

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{\substack{p\leq x \\ p \text{ good}}} \frac{a_p \log p}{p} = -r + \frac{1}{2}.$$

Theorem (Kim and Murty - 2021)

If the limit exists, then BSD-65 holds.

(useful tool, but convergence is very slow)

A Naive Search for Large Rank

- loop over (a, b, m) for $\quad (a+b)m^2 - ab = \square$
- For $x \approx 10^3$, compute

$$\frac{1}{\log x} \sum_{\substack{p \leq x \\ p \text{ good}}} \frac{a_p \log p}{p}$$

- If the above quantity is > 5, then compute the rank of

$$Y^2 = X(X+a)(X+b) + m^6$$

End Result: MANY curves of rank 9 ... and

Current Record Holders

$$y^2 = x(x+2185)(x+929) + 71^6,$$
$$y^2 = x(x+59)(x+1909) + 3737^6$$
$$y^2 = x(x+169)(x+6579) + 2257^6$$
$$y^2 = x(x+471)(x+9217) + 7067^6$$

and

$$E_{-1}(3950) : y^2 = x(x+1)(x+15602498) + 3949^6$$

have rank 10.

Recall $E_{(a,b,m)} : y^2 = x^3 + (a+b)x^2 + abx + m^2$

Type 2: impose $abx + m^2 = 0$
Type 3: impose $(a+b)x^2 + m^2 = 0$

Recall $E_{(a,b,m)} : y^2 = x^3 + (a+b)x^2 + abx + m^2$

Type 2: impose $abx + m^2 = 0$
Type 3: impose $(a+b)x^2 + m^2 = 0$

Type 2: $E_{(a,-b,abm)} : \; y^2 = x(x+a)(x-b) + (abm)^2$

where (n, m) satisfy $n^2 - abm^2 = b - a$.

Naive search gives the curve $E_{(a,-b,abm)}$, with

$(a, b, m) = (2396, 4847, 149)$, having rank 10.

Type 3: $E: \ y^2 = x(x+a)(x-(a+t^2)) + (tm^2)^2$,

where $a(a+t^2) = rs$ and $r+s = 2m^2$.

Almost always (except for a very thin subset)

$P = (-a, tm^2), Q = (a+t^2, tm^2)$,
$R = (m^2, m(r-s)/2), S = (t^2, t(r-s)/2)$

are independent points on E.

Type 3: $E: \ y^2 = x(x+a)(x-(a+t^2)) + (tm^2)^2$,

where $a(a+t^2) = rs$ and $r+s = 2m^2$.

Almost always (except for a very thin subset)

$P = (-a, tm^2), Q = (a+t^2, tm^2),$
$R = (m^2, m(r-s)/2), S = (t^2, t(r-s)/2)$

are independent points on E.

For $(a, t, m) = (1317604, 4, 294627)$

E has rank **13**.

Jump of 11 from $\mathbb{Q}(t)$ to $\mathbb{Q}$ ties the record of Elkies and Klagsbrun!!

$$E: \ y^2 = x(x+a)(x-a-t^2) + (tm^2)^2,$$

with $(a, t, m) = (1317604, 4, 294627)$ contains the independent points

$P1 = (-44417351 : -181680936187 : 1)$
$P2 = (-29884228 : 306472132260 : 1)$
$P3 = (-49377431 : 16092719437 : 1)$
$P4 = (-1317604 : -347220276516 : 1)$
$P5 = (-1767752 : 347216741012 : 1)$
$P6 = (-9593128 : -345970715820 : 1)$
$P7 = (-30390164 : 304216145764 : 1)$
$P8 = (6657228 : -347628252132 : 1)$
$P9 = (100779385 : 1069556473691 : 1)$
$P10 = (-13105292 : -343996879652 : 1)$
$P11 = (81367136 : -811862484636 : 1)$
$P12 = (69338420 : 673652628516 : 1)$
$P13 = (1317620 : -347220276516 : 1)$

(hyperellratpoints in pari and Saturation in Magma)

OPEN PROBLEM 1: Ranks of Jacobians

Let $g \geq 1$ and $A = \{a_1, a_2, \ldots, a_{2g+1}\}$ be distinct integers.

Let $f(x) = \prod_{i=1}^{2g+1}(x - a_i)$, and for $m \in \mathbb{Z}$, let $H_{f,m}$ be the hyperelliptic curve given by

$$H_{f,m}: \; y^2 = f(x) + m^2. \qquad (\textit{assume } f + m^2 \textit{ sq.free})$$

Problem: Prove that there is a constant $C = C(A)$ such that if $m > C$, then

$$rk(J(H)) \geq 2g.$$

OPEN PROBLEM 2: Polynomial Bounds for a Subfamily

$$E_{a,m} : y^2 = x^3 - a^2 x + m^2$$

By the above, there is a constant $C = C(a)$ for which if $m > C$, then $rk(E_{a,m}) \geq 2$.

Our method of proof entails a close relationship between C and an upper bound for the size of integral points on

$$E_{a,0} : y^2 = x^3 - a^2 x.$$

Proposition Under an effective form of the *abc* conjecture, any integral point (x, y) on $E_{a,0}$ satisfies $|x| < 32a^5$.

Problem: Prove an unconditional polynomial bound for $C(a)$.

The work of Shioda

Tetsuji Shioda (1991) proved four theorems on the rank of families of curves, with increasing complexity from one theorem to the next.

Shioda - Theorem 1
Take $(b_1, b_2) \in \mathbb{Q}^2$ such that b_1, b_2 and $b_3 = -b_1 - b_2$ are mutually distinct. Let E be the elliptic curve over $\mathbb{Q}(t)$:

$$E: \ y^2 = (x - b_1)(x - b_2)(x - b_3) + t^2.$$

Then the MW group $E(\mathbb{Q}(t))$ is torsion-free and of rank 2. Any two of the rational points $P_i = (b_i, t)$ $(i = 1, 2, 3)$ generate $E(\mathbb{Q}(t))$, and P_1, P_2, P_3 are collinear.

Observation: Silverman's Specialization Theorem can be applied to obtain rank bounds over $\mathbb{Q}$!

Shioda - Theorem 2

Let $d_1, d_2, d_3, d_4 \in \mathbb{Q}$ such that their squares are mutually distinct. Define

$$q_2 = (1/3)\sum d_i^2$$
$$p_0 = \sum_{i<j} d_i^2 d_j^2 - 3q_2^2$$
$$q_0 = \sum_{i<j<k} d_i^2 d_j^2 d_k^2 - p_0 q_2 - q_2^3$$
$$q_1 = \pm 2 d_1 d_2 d_3 d_4.$$

Then the elliptic curve

$$E: \; y^2 = x^3 + (p_0 - t)x + (q_0 + q_1 t + q_2 t^2)$$

over $\mathbb{Q}(t)$ has MW rank 4.

OPEN PROBLEM 3: Can one produce curves, or subfamilies of curves, with particularly large rank from Shioda's other three constructions?