AN EFFECTIVE VERSION OF A THEOREM OF SHIODA ON RANKS OF ELLIPTIC CURVES

Gary Walsh
gwalsh@uottawa.ca

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

Maine-Quebec Number Theory Conference 2022
HAPPY BIRTHDAY ANDREW

Theorem (Bud Brown and Bruce Myers, 2002)

For a non-zero integer m, let

$$E_m: \ y^2 = x^3 - x + m^2 \ \ and \ \ P = (0, m), Q = (-1, m).$$

Then P and Q are independent points (of infinite order) 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.

- **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)**

$E_{m,n}: \ y^2 = x^3 - m^2x + n^2: \ rank \ E_{m,n} \geq 2.$

- **Rout and Juyal (2021)**

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

- **Hatley and Stack (2021)**

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

Other Polynomials

What about

$$f(x) = (x - a)(x - b)(x - c)$$

with distinct integers a, b, c?

$$E_{(a,b,c),m} : \ y^2 = f(x) + m^2$$

Other Polynomials

What about

$$f(x) = (x - a)(x - b)(x - c)$$

with distinct integers a, b, c?

$$E_{(a,b,c),m} : \; y^2 = f(x) + m^2$$

Example: $(a, b, c) = (5, 7, 11)$, m=42.

$$E : y^2 = x^3 - 23x^2 + 167x + 1379$$

$rank(E) = 2$ and

$E(\mathbb{Q}) =< P, Q >$ with $P = (5, -42), Q = (7, -42)$.

Beware: Rank 1 Examples Do Exist

```
R<x>:=PolynomialRing(Integers());
f:=(x-Random(10^2))*(x-Random(10^2))*(x-Random(10^2));f;
for i in [1..32] do
f1:=f+i^2;
if IsSquarefree(f1) then
E:=EllipticCurve(f1);
SetClassGroupBounds("GRH");
[i,Rank(E)];
end if;
end for;
```

Clear Submit

```
x^3 - 242*x^2 + 19281*x - 504252
[ 1, 3 ]
[ 2, 3 ]
[ 3, 3 ]
[ 4, 4 ]
[ 5, 2 ]
[ 6, 2 ]
[ 7, 3 ]
[ 8, 2 ]
[ 9, 2 ]
[ 10, 2 ]
[ 11, 4 ]
[ 12, 1 ]
[ 13, 2 ]
```

$$E: y^2 = (x-92)(x-87)(x-63) + 12^2$$

$$E(\mathbb{Q}) = < P >, \; P = (87, -12)$$

$$E : y^2 = (x - 92)(x - 87)(x - 63) + 12^2$$

$$E(\mathbb{Q}) =< P >, \; P = (87, -12)$$

$2P = (93, -18)$

$3P = (63, -12)$

$4P = (92, -12)$

$5P = (93, -18)$

$6P = (2151/5^2, 2076/5^3)$

$7P = (957, 25938)$

Lemma

Let a, b, c be distinct integers and m a non-zero integer for which

$$f(x) = (x-a)(x-b)(x-c) + m^2$$

is squarefree. Let $P = (a, m), Q = (b, m)$ on

$$E : y^2 = f(x).$$

Lemma

Let a, b, c be distinct integers and m a non-zero integer for which

$$f(x) = (x - a)(x - b)(x - c) + m^2$$

is squarefree. Let $P = (a, m), Q = (b, m)$ on

$$E : y^2 = f(x).$$

If

i. $E(\mathbb{Q})$ is 2-torsion free,

ii. P, Q are points of infinite order, and

iii. P, Q and $P + Q$ are not in $2E(\mathbb{Q})$,

then P and Q are independent.

Theorem (W. 2022)

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

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

is at least 2.

Strategy of the proof:

i. The curve has no rational 2-torsion.

ii. (a, m) and (b, m) are points of infinite order.

iii. (a, m), (b, m) and $(a, m) + (b, m)$ are not in $2E(\mathbb{Q})$.

Simplifications

1. The translation $x \to x + c$ allows us to assume that $c = 0$.

2. Put

$$A = -27(a^2 - ab + b^2)$$
$$B = 3^6 m^2 + 27(a+b)^3 + 3A(a+b),$$
$$X = 9x - 3(a+b), \quad Y = 27y,$$

then

$$Y^2 = X^3 + AX + B.$$

Step One: 2-torsion

Assume that (r, s) is a rational point of order two on $Y^2 = X^3 + AX + B$. Then $s = 0$ and r is a root, so that

$$X^3 + AX + B = (X - r)(X^2 + rX + t)$$

for some integer t.

$(*)\ \ (27m)^2 = (-r)^3 + (-r) - 3A(a + b) - 27(a + b)^3.$

Thus, $m < C_1 = C_1(a, b)$ by **Baker's Theorem.**

(the cubic above never has multiple roots)

Lutz-Nagell

Let E be an elliptic curve given by

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

If P is a non-zero torsion point, then

i. $x(P), y(P) \in \mathbb{Z}$.

ii. Either $2P = 0$ or $y(P)^2$ divides $4A^3 + 27B^2$.

$P = \phi((a, m))$ (mapped to the short model) is torsion, and $2P$ is also. So $2P \in E(\mathbb{Z})$ by Lutz-Nagell, and $\lambda \in \mathbb{Z}$.

The quantity λ arising in the doubling formula is precisely

$$\lambda = \frac{a(a-b)}{54m},$$

and is not integral for $m > C_2(a, b)$ (and note that $\lambda \neq 0$).

It remains to show that $P = (a, m)$, $Q = (b, m)$, $P + Q = (0, -m)$ are all **not** in $2E(\mathbb{Q})$ for m large.

Assume that $2(x, y) = (0, -m)$, need to show that m is bounded.

$$\lambda = \frac{3x^2 - 2(a+b)x + ab}{2y},\ \nu = \frac{-x^3 + abx + 2m^2}{2y}.$$

The coordinates (r, s) of $2(x, y)$ are given by

$$(\lambda^2 + a_1\lambda - a_2 - 2x, -(\lambda + a_1)r - \nu - a_3).$$

Since $(r, s) = (0, -m)$, and $a_3 = 0$, it follows that $\nu = m$.

Step Three: Completion of the Proof

Combining the two expressions for ν and simplifying gives

$$x^4 - 2abx^2 - 8m^2x + (a^2b^2 + 4m^2(a+b)) = 0.$$

The above polynomial in x, m satisfies the hypotheses of **Runge's Theorem** on Diophantine equations, from which it follows that $m < C_3 = C_3(a, b)$.

Combining the two expressions for ν and simplifying gives

$$x^4 - 2abx^2 - 8m^2x + (a^2b^2 + 4m^2(a+b)) = 0.$$

The above polynomial in x, m satisfies the hypotheses of **Runge's Theorem** on Diophantine equations, from which it follows that $m < C_3 = C_3(a, b)$.

i. The weighted sum of highest order terms is reducible.
ii. The polynomial is irreducible in $\mathbb{Q}[x]$ for $m > C_4(a, b)$.

Combining the two expressions for ν and simplifying gives

$$x^4 - 2abx^2 - 8m^2x + (a^2b^2 + 4m^2(a+b)) = 0.$$

The above polynomial in x, m satisfies the hypotheses of **Runge's Theorem** on Diophantine equations, from which it follows that $m < C_3 = C_3(a,b)$.

i. The weighted sum of highest order terms is reducible.
ii. The polynomial is irreducible in $\mathbb{Q}[x]$ for $m > C_4(a,b)$.

Open Problem:
Compare the *explicit* constants arising from both the Diophantine method and the Shioda/Silverman method.

Theorem (W. 2023 - work in progress)

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, for $m > C = C(a, b)$, the curve

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

has rank at least 3.

Proof: $P = (-a, m^3)$, $Q = (-b, m^3)$, $R = (-m^2, Xm)$ are independent for $m > C$.

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

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

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

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

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

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

USING PELL EQUATIONS TO GET RANK ≥ 3

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

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

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

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

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

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

Example Let $a = 1$ so the Pell equation becomes

$$X^2 - (b+1)Y^2 = -b$$

(which is always solvable with $X = Y = 1$), and restrict to $b = t^2 - 2$ so that small units of positive norm exist.

$$(1 + \sqrt{t^2-1}) \cdot (t + \sqrt{t^2-1}) = t^2 + t - 1 + (t+1)\sqrt{t^2-1},$$

so $(X, Y) = (t^2 + t - 1, t + 1)$ is also solution to the Pell equation.

$$E_1(t):\ y^2 = x(x+1)(x+t^2-2) + 1$$

$$E_2(t):\ y^2 = x(x+1)(x+t^2-2) + (t+1)^6$$

should have (somewhat) large rank.

Current Record Holder

$$E_2(346) : y^2 = x(x+1)(x+346^2-2)+347^6$$

has rank 8.

$$E: \ y^2 = x^3 + (a+b)x^2 + abx + m^6,$$

$$P = (-a, m^3), Q = (-b, m^3), R(-m^2, mn),$$

Need to show $R, P+R, Q+R, P+Q+R \notin 2E(\mathbb{Q})$.

$$E: \; y^2 = x^3 + (a+b)x^2 + abx + m^6,$$

$$P = (-a, m^3), Q = (-b, m^3), R(-m^2, mn),$$

Need to show $R, P + R, Q + R, P + Q + R \notin 2E(\mathbb{Q})$.

$X(R) = -m^2 \neq X(2(x, y))$ for m large means showing that

$$x^4 + 4m^2x^3 + (4(a+b)m^2 - 2ab)x^2 + (4abm^2 - 8m^6)x$$
$$+(a^2b^2 + 4m^8 - 4(a+b)m^6) = 0$$

has no solutions x for m large.

Runge's Method: weighted sum of highest order terms

Is $x^4 + 4m^2x^3 - 8m^6x + 4m^8$ reducible?

Runge's Method: weighted sum of highest order terms

Is $x^4 + 4m^2x^3 - 8m^6x + 4m^8$ reducible?

$$x^4 + 4m^2x^3 - 8m^6x + 4m^8 = (x^2 + 2xm^2 - 2m^4)^2.$$

$$P+R, Q+R, P+Q+R \notin 2E(\mathbb{Z})$$

$$F_{a,b}(x,m) =$$

```
x^8*m^2 - x^8*a - 4*x^7*m^6 - 4*x^7*m^4*a - 4*x^7*m^4*b - 8*x^7*m^4 + 4*x^7*m^2*a*b
+ 8*x^7*m^2*a + 8*x^7*m^2*b - 8*x^7*a*b + 4*x^6*m^10 - 4*x^6*m^8*a
- 8*x^6*m^8*b + 16*x^6*m^8 + 8*x^6*m^6*a*b + 12*x^6*m^6*a + 4*x^6*m^6*b^2
- 4*x^6*m^6*b + 16*x^6*m^6 - 4*x^6*m^4*a^2 - 4*x^6*m^4*a*b^2 - 40*x^6*m^4*a*b
- 24*x^6*m^4*a - 20*x^6*m^4*b^2 - 40*x^6*m^4*b + 4*x^6*m^2*a^2*b + 8*x^6*m^2*a^2
+ 20*x^6*m^2*a*b^2 + 44*x^6*m^2*a*b + 24*x^6*m^2*b^2 - 4*x^6*a^2*b - 24*x^6*a*b^2
+ 8*x^5*m^10*a + 8*x^5*m^10*b - 8*x^5*m^8*a^2 - 24*x^5*m^8*a*b
+ 32*x^5*m^8*a - 16*x^5*m^8*b^2 + 32*x^5*m^8*b - 16*x^5*m^8 + 16*x^5*m^6*a^2*b
+ 32*x^5*m^6*a^2 + 24*x^5*m^6*a*b^2 + 36*x^5*m^6*a*b + 48*x^5*m^6*a + 8*x^5*m^6*b^3
+ 32*x^5*m^6*b - 8*x^5*m^4*a^2*b^2 - 60*x^5*m^4*a^2*b - 32*x^5*m^4*a^2 - 8*x^5*m^4*a*b^3
- 92*x^5*m^4*a*b^2 - 88*x^5*m^4*a*b - 32*x^5*m^4*b^3 - 64*x^5*m^4*b^2 + 28*x^5*m^2*a^2*b^2
+ 56*x^5*m^2*a^2*b + 32*x^5*m^2*a*b^3 + 88*x^5*m^2*a*b^2 + 32*x^5*m^2*b^3
- 24*x^5*a^2*b^2 - 32*x^5*a*b^3 + 28*x^4*m^12 + 4*x^4*m^10*a^2
+ 16*x^4*m^10*a*b + 28*x^4*m^10*a + 4*x^4*m^10*b^2 + 28*x^4*m^10*b + 56*x^4*m^10
- 4*x^4*m^8*a^3 - 24*x^4*m^8*a^2*b + 16*x^4*m^8*a^2 - 36*x^4*m^8*a*b^2 + 36*x^4*m^8*a*b
- 64*x^4*m^8*a - 8*x^4*m^8*b^3 + 16*x^4*m^8*b^2 - 64*x^4*m^8*b + 8*x^4*m^6*a^3*b + 16*x^4*m^6*a^3
+ 36*x^4*m^6*a^2*b^2 + 72*x^4*m^6*a^2*b + 24*x^4*m^6*a^2
+ 24*x^4*m^6*a*b^3 + 24*x^4*m^6*a*b^2 + 128*x^4*m^6*a*b + 4*x^4*m^6*b^4
+ 16*x^4*m^6*b^2 - 4*x^4*m^4*a^3*b^2 - 24*x^4*m^4*a^3*b - 16*x^4*m^4*a^3 - 16*x^4*m^4*a^2*b^3
- 128*x^4*m^4*a^2*b^2 - 80*x^4*m^4*a^2*b - 4*x^4*m^4*a*b^4 - 88*x^4*m^4*a*b^3 - 128*x^4*m^4*a*b^2
- 16*x^4*m^4*b^4 - 32*x^4*m^4*b^3 + 8*x^4*m^2*a^3*b^2 + 16*x^4*m^2*a^3*b + 56*x^4*m^2*a^2*b^3
+ 118*x^4*m^2*a^2*b^2 + 16*x^4*m^2*a*b^4 + 80*x^4*m^2*a*b^3 + 16*x^4*m^2*b^4 - 6*x^4*a^3*b^2
- 48*x^4*a^2*b^3 - 16*x^4*a*b^4 + 8*x^3*m^16 - 8*x^3*m^14*a - 16*x^3*m^14*b + 32*x^3*m^14
+ 16*x^3*m^12*a*b + 80*x^3*m^12*a + 8*x^3*m^12*b^2 + 48*x^3*m^12*b + 32*x^3*m^12 + 8*x^3*m^10*a^2*b
+ 48*x^3*m^10*a^2 + 32*x^3*m^10*a*b + 64*x^3*m^10*a + 16*x^3*m^10*b^2 + 32*x^3*m^10*b - 8*x^3*m^8*a^3*b
- 24*x^3*m^8*a^2*b^2 - 16*x^3*m^8*a^2*b - 96*x^3*m^8*a^2 - 16*x^3*m^8*a*b^3 + 16*x^3*m^8*a*b^2 - 96*x^3*m^8*a*b
- 64*x^3*m^8*b^2 + 16*x^3*m^6*a^3*b^2 + 32*x^3*m^6*a^3*b + 24*x^3*m^6*a^2*b^3 + 36*x^3*m^6*a^2*b^2
+ 96*x^3*m^6*a^2*b + 8*x^3*m^6*a*b^4 + 96*x^3*m^6*a*b^2 - 8*x^3*m^4*a^3*b^3 - 60*x^3*m^4*a^3*b^2
- 32*x^3*m^4*a^3*b - 8*x^3*m^4*a^2*b^4 - 92*x^3*m^4*a^2*b^3 - 88*x^3*m^4*a^2*b^2 - 32*x^3*m^4*a*b^4
- 64*x^3*m^4*a*b^3 + 28*x^3*m^2*a^3*b^3 + 56*x^3*m^2*a^3*b^2 + 32*x^3*m^2*a^2*b^4 + 88*x^3*m^2*a^2*b^3
+ 32*x^3*m^2*a*b^4 - 24*x^3*a^3*b^3 - 32*x^3*a^2*b^4 + 8*x^2*m^16*a + 8*x^2*m^16*b - 8*x^2*m^14*a^2
- 24*x^2*m^14*a*b + 32*x^2*m^14*a - 16*x^2*m^14*b^2 + 32*x^2*m^14*b + 64*x^2*m^14 + 16*x^2*m^12*a^2*b
+ 48*x^2*m^12*a^2 + 24*x^2*m^12*a*b^2 + 104*x^2*m^12*a*b - 32*x^2*m^12*a + 8*x^2*m^12*b^3 + 16*x^2*m^12*b^2
+ 32*x^2*m^12*b + 16*x^2*m^10*a^3 - 4*x^2*m^10*a^2*b^2 + 24*x^2*m^10*a^2*b - 8*x^2*m^10*a*b^3 - 8*x^2*m^10*a*b^2
+ 48*x^2*m^10*a*b - 16*x^2*m^10*b^3 - 32*x^2*m^10*b^2 - 4*x^2*m^8*a^3*b^2 - 16*x^2*m^8*a^3*b
- 32*x^2*m^8*a^3 - 8*x^2*m^8*a^2*b^3 - 24*x^2*m^8*a^2*b^2 - 96*x^2*m^8*a^2*b + 16*x^2*m^8*a*b^3 - 64*x^2*m^8*a*b^2
+ 8*x^2*m^6*a^3*b^3 + 12*x^2*m^6*a^3*b^2 + 16*x^2*m^6*a^3*b + 4*x^2*m^6*a^2*b^4 - 4*x^2*m^6*a^2*b^3 + 112*x^2*m^6*a^2*b^2
- 4*x^2*m^4*a^4*b^2 - 4*x^2*m^4*a^3*b^4 - 40*x^2*m^4*a^3*b^3 - 24*x^2*m^4*a^3*b^2 - 20*x^2*m^4*a^2*b^4 - 40*x^2*m^4*a^2*b^3
+ 4*x^2*m^2*a^4*b^3 + 8*x^2*m^2*a^4*b^2 + 20*x^2*m^2*a^3*b^4 + 44*x^2*m^2*a^3*b^3 + 24*x^2*m^2*a^2*b^4 - 4*x^2*a^4*b^3 - 24*x^2*a^3*b^4
+ 32*x*m^18 + 8*x*m^16*a*b + 32*x*m^16*a + 32*x*m^16*b + 64*x*m^16 - 8*x*m^14*a^2*b - 16*x*m^14*a*b^2 + 16*x*m^12*a^2*b^2
+ 48*x*m^12*a^2*b - 64*x*m^12*a^2 + 8*x*m^12*a*b^3 + 16*x*m^12*a*b^2 + 32*x*m^12*a*b
+ 16*x*m^10*a^3*b - 8*x*m^10*a^2*b^3 - 32*x*m^10*a^2*b^2 - 16*x*m^10*a*b^3 - 32*x*m^10*a*b^2 - 16*x*m^8*a^3*b^2 - 32*x*m^8*a^3*b
+ 16*x*m^8*a^2*b^3 - 16*x*m^8*a^2*b^2 - 4*x*m^6*a^3*b^3 + 48*x*m^6*a^3*b^2 - 4*x*m^4*a^4*b^3 - 4*x*m^4*a^3*b^4 - 8*x*m^4*a^3*b^3
+ 4*x*m^2*a^4*b^4 + 8*x*m^2*a^4*b^3 + 8*x*m^2*a^3*b^4 - 8*x*a^4*b^4 + 4*m^22 - 4*m^20*a - 8*m^20*b + 16*m^20 + 8*m^18*a*b
+ 32*m^18*a + 4*m^18*b^2 + 16*m^18*b + 16*m^18 + 16*m^16*a^2 - 4*m^16*a*b^2 + 16*m^16*a - 16*m^14*a^2*b - 16*m^14*a^2 - 16*m^12*a^3
- 4*m^12*a^2*b^2 - 4*m^10*a^3*b^2 - 4*m^10*a^2*b^3 - 8*m^10*a^2*b^2 + 4*m^8*a^3*b^3 + 8*m^6*a^4*b^2 + m^2*a^4*b^4 - a^5*b^4
```

satisfies Runge's condition for all a, b.