Constant root number on integer fibres of elliptic surfaces

joint work with J. Desjardins

Rena Chu
Duke University
June 04, 2021.

Roadmap

1. Background; relevant definitions, theorems, conjectures.

2. Families of elliptic curves, and motivation to study certain cases.

3. Case $\mathcal{F}_{3,r^2}(t)$

4. Results and consequences.

1. Background

- **elliptic curve** E/K : an algebraic curve of genus one, with a specified base point ; it has Weierstrass equation of form
$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \qquad a_i \in K.$$

  - for $\operatorname{char} K \neq 2$, we may write this as
$$y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$$
and define
$$c_4 := b_2^2 - 24 b_4$$
$$c_6 := -b_2^3 + 36 b_2 b_4 - 216 b_6$$
$$\Delta := \frac{1}{1728}(c_4^3 - c_6^2)$$
$$j := \frac{1}{\Delta} c_4^3$$

  - for $\operatorname{char} K \neq 2, 3$, we may further reduce this to
$$y^2 = x^3 - \underbrace{27 c_4}_{A} x - \underbrace{54 c_6}_{B}$$
$$\Delta = -16(4A^3 + 27B^2)$$
$$j = -\frac{1}{\Delta} 1728 (4A)^3$$

(details in Silverman)

- Mordell-Weil theorem:

$$E(\mathbb{Q}) \cong E_{tors} \times \mathbb{Z}^{r}$$ (r: rank)

  - we understand E_{tors} quite well
    for example (Mazur, '77, '78): E_{tors} is isomorphic to one of
    $\mathbb{Z}/N\mathbb{Z}$, $1 \le N \le 10$ or $N = 12$.
    $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, $1 \le N \le 4$.

  - rank remains mysterious.

conjecture (weak Birch and Swinnerton-Dyer):
let $r_{an} := $ order of vanishing of $L(E,s)$ at $s=1$.
Then $r_{an} = r$.

widely believed to be true; proven for $r_{an} = 0, r_{an} = 1$
(Gross-Zagier, '86. Kolyvagin, '89, Rubin '91. Breuil-Conrad-Diamond-Taylor, '01)

how large is the rank on average?

conjecture (Goldfeld):
consider the quadratic twists of E:
$\{E_d : dy^2 = x^3 + Ax + B,$ d squarefree$\}$.
Then ~50% of E_d's have $r = 0$ (resp 1) and the rest have $r \ge 2$.

widely believed to be true

average rank

$$av(r) := \lim_{X \to \infty} \frac{\sum_{H(E(A,B)) \le X} r(E)}{\sum_{H(E(A,B)) \le X} 1}$$

where $H(E(A,B)) := \max\{4|A^3|, 27B^2\}$

$av(r) \le \frac{7}{6}$
(Bhargava-Shankar, '15)

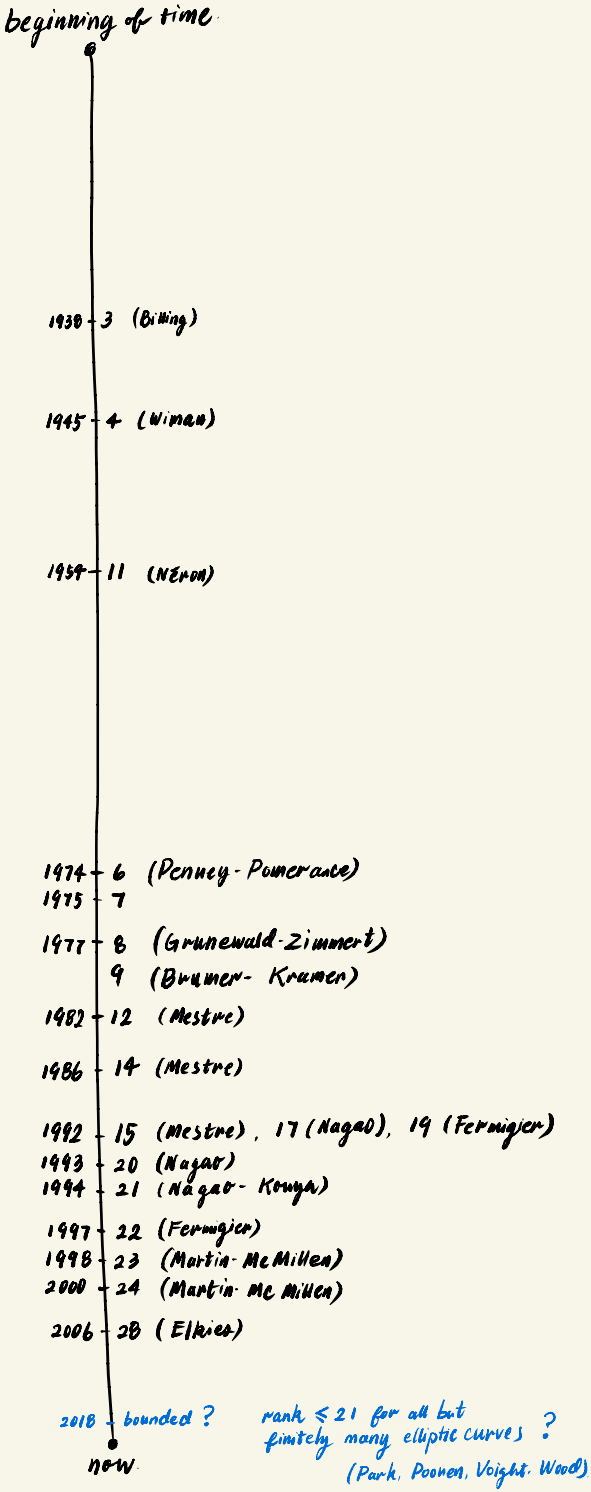
root number
$W(E) := (-1)^{r_{an}}$

parity conjecture
$W(E) = (-1)^{r}$;
$r_{an} \equiv r \pmod 2$

conjecture:
there exists elliptic curves of arbitrarily large rank.

undecided

how large can the rank get?



(timeline taken from Dujella's webpage on the History of elliptic curves rank records)

2. Families of elliptic curves

- **family of elliptic curves** $\mathcal{E}$

(i) $\mathcal{E}: y^2 + a_1(T)xy + a_3(T)y = x^3 + a_2(T)x^2 + a_4(T)x + a_6(T)$, $\quad a_i(T) \in \mathbb{Q}[T]$.

via change of variables

$$\mathcal{E}: y^2 = x^3 + A(T)x + B(T)$$

where $\Delta(T) = -16(4A(T)^3 + 27B(T)^2) \neq 0$

$c_4(T) = -2^4 \cdot 3A(T)$

$c_6(T) = -2^5 \cdot 3^3 B(T)$

$j(T) = -\frac{1}{\Delta(T)} 1728 (4A(T))^3$

(ii) $\{ \mathcal{E}_t : y^2 = x^3 + A(t)x + B(t) \mid t \in \mathbb{Q} \}$ where $\Delta(t) \neq 0$ except for finitely many $t \in \mathbb{Q}$

each $\mathcal{E}_t$ is called a **fibre**.

(iii) elliptic surface $\mathcal{E}$: an algebraic surface $\mathcal{E}$ with

- a surjective morphism $\pi: \mathcal{E} \to C$, C is a smooth proj. curve, where all but finitely many fibres are (nonsingular) elliptic curves.
- a section $\sigma_0: C \to \mathcal{E}$.

- we say a family is **isotrivial** if the j-invariant $j(T) = -\frac{1}{\Delta(T)} 1728 (4A(T))^3$ is constant

else we say it is **non-isotrivial**.

- reduction mod p, $P(T)$
  - E has good reduction mod p iff $v_p(\Delta)=0$.
    multiplicative reduction mod p iff $v_p(\Delta)>0$ and $v_p(c_4)=0$.
    additive reduction mod p iff $v_p(\Delta)>0$ and $v_p(c_4)>0$.

- **Kodaira type**: to classify the type of reduction.

Kodaira type	$v_{P(T)}(\Delta(T))$	$v_{P(T)}(A(T))$	$v_{P(T)}(B(T))$	
I_0	0	0	≥ 0	good
		≥ 0	0	
I_n	$n>0$	0	0	multiplicative
I_{n-6}^*	$n>6$	2	3	additive, potentially multi
II	2	≥ 1	1	additive, potentially good
III	3	1	≥ 2	
IV	4	≥ 2	2	
I_0^*	6	2	≥ 3	
		≥ 2	3	
IV*	8	≥ 3	4	
III*	9	3	≥ 5	
II*	10	≥ 4	5	

- study the rank in a family via the root number

$$W(E) := (-1)^{r_{an}}$$

by BSD conjecture

$$W(E) = (-1)^{r}$$

parity conjecture

note:
$W(E) = -1 \Rightarrow r \neq 0$

easier to compute using an alternate definition

$$W(E) = -\prod_{p<\infty} W_p(E)$$

where each $W_p(E) \in \{+1, -1\}$ is a local root number defined in terms of the epsilon factors of the Weil-Deligne representation of $\mathbb{Q}_p$ and $W_p(E) = 1$ except for finitely many p.

(Deligne, '73
Tate, '75)

Computing the root number

- for $p \geq 5$, let $E: y^2 = x^3 - 27c_4 x - 54c_6$, then (Rohrlich '93):

$$W_p(E) = \begin{cases} 1 & \text{if the reduction of } E \text{ at } p \text{ has type } I_0 \\ \left(\frac{-1}{p}\right) & II,\ II^*,\ I_m^*,\ I_0^* \\ \left(\frac{-2}{p}\right) & III,\ III^* \\ \left(\frac{-3}{p}\right) & IV,\ IV^* \\ -\left(\frac{-6}{p}\right) & I_m \end{cases}$$

- for $p = 2, 3$, we refer to tables in Halberstadt ('95) and Rizzo ('03).

Root number in families

Consider the family $\mathcal{E}(T): y^2 = x^3 + A(T)x + B(T)$

define $W_+(\mathcal{E}(T)) := \{t \in \mathbb{Q} \mid W(\mathcal{E}(t)) = +1\}$

$W_-(\mathcal{E}(T)) := \{t \in \mathbb{Q} \mid W(\mathcal{E}(t)) = -1\}$

- if $\mathcal{E}(T)$ is **isotrivial**, then either
  - both $W_+(\mathcal{E}(T))$ and $W_-(\mathcal{E}(T))$ are infinite.
  - one of $W_+(\mathcal{E}(T))$, $W_-(\mathcal{E}(T))$ is empty.

  e.g. (Cassels-Tschinzel, '82)

  $\mathcal{E}(T): y^2 = x^3 - (T^4+1)^2 x$, $j(\mathcal{E}(T)) = 1728$.

  has $W(\mathcal{E}(t)) = 1$ for all $t \in \mathbb{Q}$.

- if $\mathcal{E}(T)$ is **non-isotrivial**, then
  - under certain conjectures. (here we state the one-variable version which is applied to integer fibres)

let $f(T) \in \mathbb{Z}[T]$ be primitive and squarefree.
let A denote an arithmetic progression
and let $A(X) := \{t \in A : |t| \le X\}$.

Chowla's conjecture:
gives an estimate on the number of values $f(t)$, with $t \in A(X)$, whose number of prime factors has a certain parity.

holds for f s.t. $\deg f = 1$

Squarefree conjecture:
gives an estimate on the number of elements $t \in A(X)$ such that $f(t)$ is squarefree.

apply to $M_{\mathcal{E}} := \prod P$ places of multi. reduction

true when every irred. factor of $\Delta_{\mathcal{E}}$ has deg. at most 3.

apply to $B_{\mathcal{E}} := \prod P$ places of bad reduction.

both $W_+(\mathcal{E}(T))$ and $W_-(\mathcal{E}(T))$ are infinite (Desjardins, '16)
(proves the two-variable version)

- however, the sets

$$W_+(E(T),\mathbb{Z}) := \{t\in\mathbb{Z} \mid W(E(t))=+1\}$$
$$W_-(E(T),\mathbb{Z}) := \{t\in\mathbb{Z} \mid W(E(t))=-1\}$$

are not necessarily both infinite.

- e.g. (Washington's example, Rizzo '03)
  $E(T)$: $y^2=x^3+Tx^2-(T-3)x+1$
  has $W(E(t))=-1$ for all $t\in\mathbb{Z}$.
  and $\operatorname{rank}(E(t))=1$ for $|t|<1000$.

note:
if $W(E(t))=1$ then rank is even but cannot conclude it is nonzero.

- our goal: to find more examples like Washington's

Families with low-degree coefficients

note:
if there is a finite place of multiplicative reduction, then the average root number over $\mathbb{Z}$ is 0.
(Helfgott, '03
Helfgott, '09)

- Consider the family of elliptic curves

$$\mathcal{E}_t : y^2 = x^3 + a_2(t)\,x^2 + a_4(t)\,x + a_6(t),$$

where $\deg a_i \le 2$ for $i = 2, 4, 6$.

- There are 6 different classes of non-isotrivial families with no multiplicative reduction at finite places (Bettin, David, Delaunay, '18)

$\mathcal{F}_s(t)$: $y^2 = x^3 + 3tx^2 + 3sx + st$ $\quad t^2 - s$ (II)

$\mathcal{G}_w(t)$: $wy^2 = x^3 + 3tx^2 + 3tx + t^2$ $\quad t-1$ (II), t (III)

$\mathcal{H}_w(t)$: $wy^2 = x^3 + (6t^2 - 7t + 3)x^2 + 3(2t-1)x + (t+1)$ $\quad t$ (III) $\quad t^2 - \frac{11}{8}t + 1$ (II)

$\mathcal{I}_w(t)$: $wy^2 = x^3 + t(t-7)x^2 - 6t(t-6)x + 2t(5t-27)$ $\quad t$ (II) $\quad t^2 - 10t + 27$ (II)

$\mathcal{J}_{m,w}(t)$: $wy^2 = x^3 + 3t^2x^2 - 3mtx + m^2$ $\quad t^3 + m$ (II)

$\mathcal{L}_{w,s,v}(t)$: $wy^2 = x^3 + 3(t^2+v)x^2 + 3sx + s(t^2+v)$ $\quad t^4 + 2vt^2 + v^2 - s$ (II)

- Claim: only the families $\mathcal{F}_s(t)$ and $\mathcal{L}_{w,s,v}(t)$ with $s = -3r^2$, $r \in \mathbb{Z}$ may have subfamilies with constant root numbers on integer fibres.

We say a finite bad place given by a primitive polynomial $P(T)$ is insipid if it has Kodaira type:

- I_0^*
- II, II*, IV, IV*, and of form $P(T) = f(T)^2 + 3g(T)^2$, $f, g \in \mathbb{Z}[T]$ distinct
- III, III* and of form $P(T) = f(T)^2 + g(T)^2$, $f, g \in \mathbb{Z}[T]$ distinct

Theorem (Desjardins, '18):
Let $\mathcal{E}$ be a family of elliptic curves and sps $\mathcal{E}$ has a bad place that is not insipid. Assuming Chowla and squarefree holds for M_E and B_E, we have $\#\, W_\pm(\mathcal{E}, Z) = \infty$.

- the families $\mathcal{G}_w(t)$, $\mathcal{H}_w(t)$, $\mathcal{I}_w(t)$, $\mathcal{J}_{m,w}(t)$ do not have constant root numbers in integer fibres
- for the families $\mathcal{F}_s(t)$ and $\mathcal{L}_{w,s,v}(t)$, $P(t)$ is insipid iff $s = -3r^2$, $r \in \mathbb{Z}$.

3. The family $\mathcal{F}_{-3r^2}(t)$

$\mathcal{F}_s(t)$: $y^2 = x^3 + 3tx^2 + 3sx + st$, $s = -3r^2$

by a change of variables.

$$\mathcal{F}_s(t): \quad y^2 = x^3 - 3(t^2 - s)x + 2t(t^2 - s)$$

$$\Delta(t) = -2^6 3^3 s (t^2 - s)^2$$

let $P(t) := t^2 - s$ then $P(t)$ is a bad place of Kodaira type II.

Recall that $W(E_t) = \prod_p W_p(E_t)$.

- does the following hold ? ~~NO~~. YES.

  $W(E_t)$ is constant for all t iff $\forall p$. $W_p^*(E_t)$ is constant for all t

- we need to write this differently so that local contributions behave independently.
- need to introduce Jacobi symbol and the Liouville function.

  (Helfgott, '09)

  (Desjardins, '16)

The modified root number

Let $P(t) := t^2 - s$. Then define the modified local root number :

$$W_p^*(E_t) := \begin{cases} \operatorname{sgn}(P(t)) \left(\frac{-1}{P(t)}\right)_{(2)} W_2(E_t), & p = 2 \\ (-1)^{v_3(P(t))} W_3(E_t), & p = 3 \\ \left(\frac{-1}{p}\right)^{v_p(P(t))} W_p(E_t), & p \geq 5 \end{cases}$$

Theorem (Desjardins, '18) : $W(E_t) = -\prod_p W_p^*(E_t)$

we use results from Chinis ('18) and Bettin-David-Delaunay ('18) to compute $W_p^*(E_t)$ depending on $v_p(s)$, $v_p(t)$, $v_p(t^2-s)$, $s_p := \frac{s}{p^{v_p(s)}}$, etc.

goal: find conditions on s so that $F_s(t)$ has constant root number on integer fibres.

example.

$s = -3$ then $W_2^*(E_2) = 1$, $W_2^*(E_6) = -1$

$s = -3 \cdot 4$ then $W_2^*(E_4) = -1$, $W_2^*(E_8) = 1$

$s = -3 \cdot 9$ then $W_2^*(E_2) = -1$, $W_2^*(E_6) = 1$

$s = -3 \cdot 16$ then $W_2^*(E_{-6}) = 1$, $W_2^*(E_{14}) = -1$

$s = -3 \cdot 25$ then $W_2^*(E_2) = -1$, $W_2^*(E_6) = 1$

4. Results and Consequences

Theorem 1 (C. Desjardins)

Recall $W_{\pm}(\mathcal{F}_s(t), \mathbb{Z}) = \{t \in \mathbb{Z} \mid \mathcal{F}_s(t) \text{ nonsingular}, W(\mathcal{F}_s(t)) = \pm 1\}$.

Then $\#W_+(\mathcal{F}_s(t), \mathbb{Z}) = \infty$, and $\#W_-(\mathcal{F}_s(t), \mathbb{Z}) = \infty$.

In other words, there does not exist $s \in \mathbb{Z}$ s.t. $\mathcal{F}_s(t)$ has constant root number for all $t \in \mathbb{Z}$.

goal: find conditions on S so that $\mathcal{F}_s(t)$ has constant root number on integer fibres.

oh no.

but wait...

recall Washington's example $E(T)$: $y^2 = x^3 + Tx^2 - (T-3)x + 1$ has constant root number for $t \in \mathbb{Z}$.

in fact $E(t)$ is isomorphic to $\mathcal{F}_S(au+b)$ with $S = -2^2 \cdot 3^5$, $a = 12$, $b = 18$

$W(E_t)$ not constant for all $t \in \mathbb{Z}$ ✗ $W(E_t)$ not constant in subfamilies $t \in A \subsetneq \mathbb{Z}$.

Consider $t \in a\mathbb{Z} + b$, $a, b \in \mathbb{Z}$.

Theorem 2 (C-Desjardins)

Let $s, a, b \in \mathbb{Z}$ be nonzero and $s = -\delta r^2$, $r \in \mathbb{Z}$.

Then the family $\mathcal{F}_s(au+b)$ has constant root number as u varies through $\mathbb{Z}$ if and only if these 3 conditions hold:

(1) $v_p(b) < v_p(a)$ or $\frac{1}{2} v_p(s) \leq v_p(a) \leq v_p(b)$ for all $p \geq 5$ s.t. $p \mid s$;

(2) $v_3(b) < v_3(a)$ or $\frac{1}{2}(v_3(s)-3) \leq v_3(a) \leq v_3(b)$;

(3) one of the following:

(a) $v_2(b) + 2 < v_2(a)$

(b) $v_2(b) + 2 = v_2(a)$ and $v_2(s) \equiv 0 \pmod 4$ and

(i) $v_2(s) - 2v_2(b) < 0$, or

(ii) $v_2(s) - 2v_2(b) \equiv 2 \pmod 4$, > 0, or

(iii) $v_2(s) - 2v_2(b) \equiv 0 \pmod 4$, > 0 and $b_2 \equiv 1 \pmod 4$

(c) $v_2(b) + 2 = v_2(a)$ and $v_2(s) \equiv 2 \pmod 4$ and

(i) $v_2(s) - 2v_2(b) < 0$, or

(ii) $v_2(s) - 2v_2(b) = 2$ and $b_2 \equiv 3 \pmod 4$, or

(iii) $v_2(s) - 2v_2(b) \equiv 0 \pmod 4$, > 0, or

(iv) $v_2(s) - 2v_2(b) = 6$, or

(v) $v_2(s) - 2v_2(b) \equiv 2 \pmod 4$, > 6 and $b_2 \equiv 1 \pmod 4$

(d) $v_2(b) + 1 = v_2(a)$ and

(i) $v_2(s) - 2v_2(b) < -4$, or

(ii) $v_2(s) - 2v_2(b) = -2$ and $v_2(s) \equiv 2 \pmod 4$

(e) $\frac{1}{2}(v_2(s)+6) \leq v_2(a) \leq v_2(b)$

(f) $\frac{1}{2}(v_2(s)+4) = v_2(a) \leq v_2(b)$ and $v_2(s) \equiv 2 \pmod 4$

To summarize,

given a non-isotrivial family $\mathcal{E}$ of elliptic curves

$$\mathcal{E}_t : \; y^2 = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t), \qquad \deg a_i \leq 2$$

and assuming Chowla's conjecture and the squarefree conjecture hold for $M_{\mathbb{Z}}$ and $B_{\mathbb{Z}}$ respectively.

we show that $W_{\pm}(\mathcal{E}, \mathbb{Z}) = \{t \in \mathbb{Z} : W(\mathcal{E}_t) = \pm 1\}$ are both infinite unless $\mathcal{E}$ is of the form $\mathcal{F}_j(au+b)$ as in Theorem 2 or $\mathcal{L}_{w,s,v}(au+b)$ as in (C-Desjardins).

Rank jumps

Let $\mathcal{E}$ be a family of elliptic curves, and define the generic rank $rk(\mathcal{E})$ to be the rank of $\mathcal{E}$ at an elliptic curve over $\mathbb{Q}(T)$.

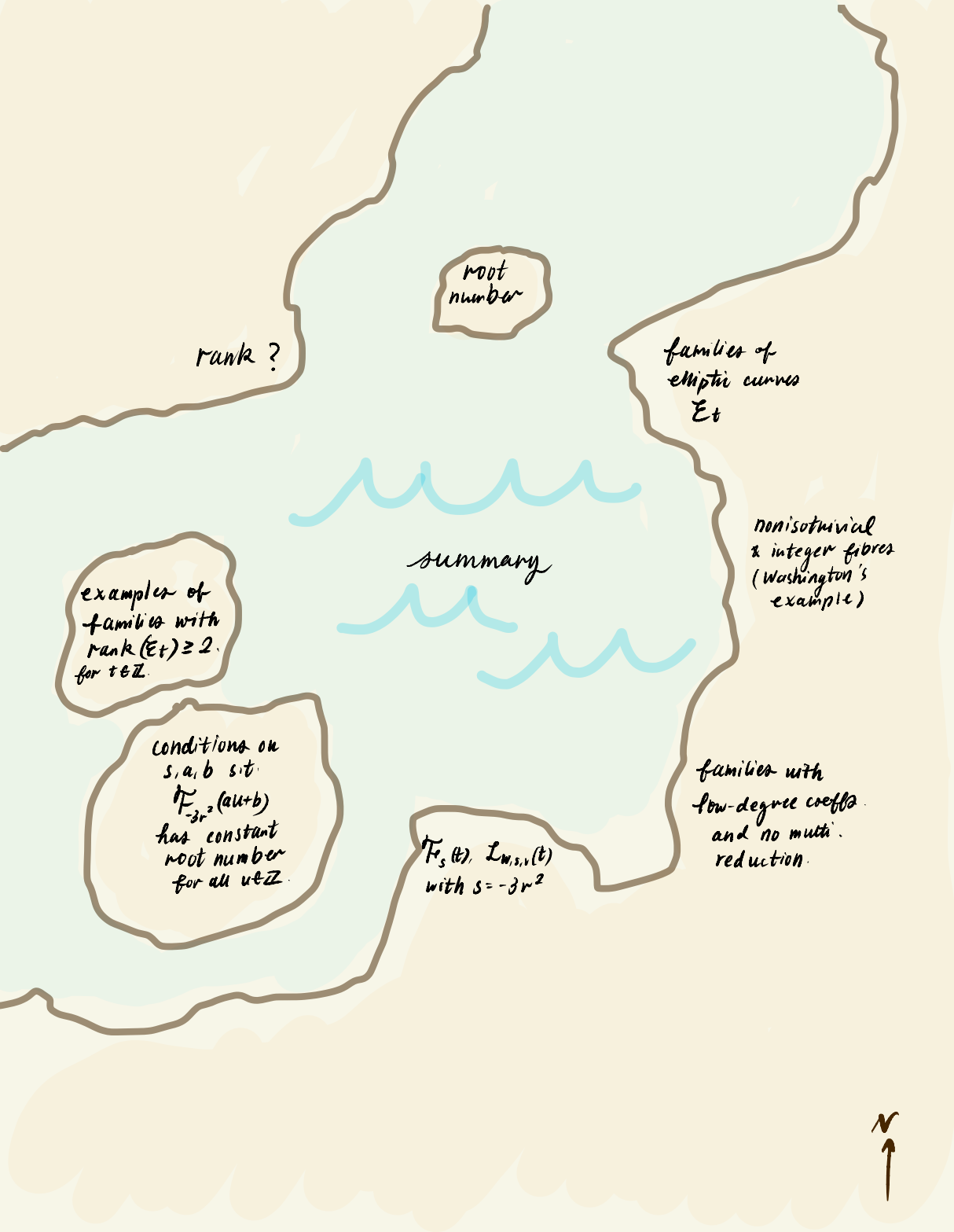
Theorem (Silverman, '83)
$rk(\mathcal{E}) \leq rk(\mathcal{E}_t)$ for all but finitely many $t \in \mathbb{Q}$

Theorem (Bettin-David-Delaunay, '18):
$$rk(\mathcal{F}_s) = \begin{cases} 1, & s = -12k^4,\ k \in \mathbb{N} \\ 0, & \text{otherwise} \end{cases}$$

→ for $s = -12k^4$, $rk(\mathcal{F}_s(t)) \geq 1$

- under the parity conjecture, this means if a subfamily $at+b$ satisfies $W(\mathcal{F}_s(au+b)) = 1$ for all $u \in \mathbb{Z}$, then every non-singular integer fibre $\mathcal{F}_s(au+b)$ has rank 2 or more. (for all but finitely many)
- from Theorem 2 we may compute conditions on a, b under which $W(\mathcal{F}_s(au+b)) = 1$ for all $u \in \mathbb{Z}$.
- example: let $s = -12 \cdot 5^4$, $a = 2^3 \cdot 3 \cdot 5^2 \cdot q$, $b = 2^2 \cdot 3 \cdot 5 \cdot q$ where q is a prime s.t. $q \nmid s$.

  i.e. $\mathcal{E}_u : y^2 = x^3 - 900(1200u^2 + 240u + 37)x + 36000(12000u^3 + 3600u^2 + 610u + 37)$


root number
rank ?
families of elliptic curves E_t
summary
nonisotrivial & integer fibres (Washington's example)
examples of families with rank $(E_t) \geq 2$ for $t \in \mathbb{Z}$
conditions on s, a, b s.t. $T_{-3r^2}(au+b)$ has constant root number for all $u \in \mathbb{Z}$
families with low-degree coeffs and no multi. reduction
$T_s(t)$, $L_{w,s,v}(t)$ with $s = -3r^2$


Thank you