Rank speculation

VaNTAGe*, 15 September 2020

Noam D. Elkies
Harvard University

***V**irtu**a**l **N**umber **T**heory & **A**rithmetic **Ge**ometry

Overview

- Mordell(–Weil) & Mazur; Questions about rank

- Heuristics for and against boundedness of rank

- Uniform Mordell–Weil vs. uniform Mordell–Faltings

- The quest for high rank:

algebraic identities and algebraic geometry

- Another route to 21 (and 13 with 2-torsion, etc.)

Mordell(–Weil) & Mazur

Theorem (Mordell c.1920): *For any elliptic curve $E/\mathbf{Q}$, the group $E(\mathbf{Q})$ is finitely generated.*

[Weil 1928: Ditto $A(K)$ for any ab. var. A and number field K. Thus "Mordell–Weil theorem", and "Mordell–Weil group" for $E(\mathbf{Q})$ or $A(K)$.]

Therefore $E(\mathbf{Q}) \cong E(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^r$, for some finite abelian group $E(\mathbf{Q})_{\text{tors}}$ and integer $r \geq 0$, the **rank** of E (over $\mathbf{Q}$).

Question: Which finitely generated groups arise? Equivalently: **Which pairs** $(E(\mathbf{Q})_{\text{tors}}, r)$ **are possible?**

Theorem (Mazur 1977): *The torsion group of any $E/\mathbf{Q}$ is either $\mathbf{Z}/N\mathbf{Z}$ (some $N \leq 12$ with $N \neq 11$) or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ (some $N \in \{1, 2, 3, 4\}$).*

It was already known that each of these 15 groups arises for infinitely many curves $E/\mathbf{Q}$.

Mordell(–Weil) & Mazur

Theorem (Mordell c.1920): *For any elliptic curve $E/\mathbf{Q}$, the group $E(\mathbf{Q})$ is finitely generated.*

[Weil 1928: Ditto $A(K)$ for any ab. var. A and number field K. Thus "Mordell–Weil theorem", and "Mordell–Weil group" for $E(\mathbf{Q})$ or $A(K)$.]

Therefore $E(\mathbf{Q}) \cong E(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^r$, for some finite abelian group $E(\mathbf{Q})_{\text{tors}}$ and integer $r \geq 0$, the **rank** of E (over $\mathbf{Q}$).

Question: Which finitely generated groups arise?
Equivalently: **Which pairs** $(E(\mathbf{Q})_{\text{tors}}, r)$ **are possible?**

Theorem (Mazur 1977): *The torsion group of any $E/\mathbf{Q}$ is either $\mathbf{Z}/N\mathbf{Z}$ (some $N \leq 12$ with $N \neq 11$) or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ (some $N \in \{1, 2, 3, 4\}$).*

It was already known that each of these 15 groups arises for infinitely many curves $E/\mathbf{Q}$.

Mordell(–Weil) & Mazur

Theorem (Mordell c.1920): *For any elliptic curve $E/\mathbf{Q}$, the group $E(\mathbf{Q})$ is finitely generated.*

[Weil 1928: Ditto $A(K)$ for any ab. var. A and number field K. Thus "Mordell–Weil theorem", and "Mordell–Weil group" for $E(\mathbf{Q})$ or $A(K)$.]

Therefore $E(\mathbf{Q}) \cong E(\mathbf{Q})_{\text{tors}} \oplus \mathbf{Z}^r$, for some finite abelian group $E(\mathbf{Q})_{\text{tors}}$ and integer $r \geq 0$, the **rank** of E (over $\mathbf{Q}$).

Question: Which finitely generated groups arise?
Equivalently: **Which pairs** $(E(\mathbf{Q})_{\text{tors}}, r)$ **are possible?**

Theorem (Mazur 1977): *The torsion group of any $E/\mathbf{Q}$ is either $\mathbf{Z}/N\mathbf{Z}$ (some $N \leq 12$ with $N \neq 11$) or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ (some $N \in \{1, 2, 3, 4\}$).*

It was already known that each of these 15 groups arises for infinitely many curves $E/\mathbf{Q}$.

Questions about rank

So: Given each of the 15 possible torsion groups G, which ranks r are possible?

In particular, is r bounded?

If unbounded, how far must we look to find a rank r curve?

If bounded, what's the maximal r, and the limsup (i.e., the largest r that arises infinitely often)?

Similar questions for other families of curves, e.g. $Dy^2 = x^3 - x$ ("congruent number" curves = quad. twists of $y^2 = x^3 - x$)? Quadratic twists of other $E_0/\mathbf{Q}$? "Taxicab curves" = twisted Fermat cubics $x^3 + y^3 = T$? Quartic twists $y^2 = x^3 + a_4x$ (the general $j = 1728$ curve; special case of torsion $\mathbf{Z}/2\mathbf{Z}$)? "Mordell curves" $y^2 = x^3 + a_6$ (sextic twists, general $j = 0$)?

Questions about rank

So: Given each of the 15 possible torsion groups G, which ranks r are possible?

In particular, is r bounded?

If unbounded, how far must we look to find a rank r curve?

If bounded, what's the maximal r, and the limsup (i.e., the largest r that arises infinitely often)?

Similar questions for other families of curves, e.g. $Dy^2 = x^3 - x$ ("congruent number" curves = quad. twists of $y^2 = x^3 - x$)? Quadratic twists of other $E_0/\mathbf{Q}$? "Taxicab curves" = twisted Fermat cubics $x^3 + y^3 = T$? Quartic twists $y^2 = x^3 + a_4 x$ (the general $j = 1728$ curve; special case of torsion $\mathbf{Z}/2\mathbf{Z}$)? "Mordell curves" $y^2 = x^3 + a_6$ (sextic twists, general $j = 0$)?

Questions about rank

So: Given each of the 15 possible torsion groups G, which ranks r are possible?

In particular, is r bounded?

If unbounded, how far must we look to find a rank r curve?

If bounded, what's the maximal r, and the limsup (i.e., the largest r that arises infinitely often)?

Similar questions for other families of curves, e.g. $Dy^2 = x^3 - x$ ("congruent number" curves = quad. twists of $y^2 = x^3 - x$)? Quadratic twists of other $E_0/\mathbf{Q}$? "Taxicab curves" = twisted Fermat cubics $x^3 + y^3 = T$? Quartic twists $y^2 = x^3 + a_4 x$ (the general $j = 1728$ curve; special case of torsion $\mathbf{Z}/2\mathbf{Z}$)? "Mordell curves" $y^2 = x^3 + a_6$ (sextic twists, general $j = 0$)?

Questions about rank

So: Given each of the 15 possible torsion groups G, which ranks r are possible?

In particular, is r bounded?

If unbounded, how far must we look to find a rank r curve?

If bounded, what's the maximal r, and the limsup (i.e., the largest r that arises infinitely often)?

Similar questions for other families of curves, e.g. $Dy^2 = x^3 - x$ ("congruent number" curves = quad. twists of $y^2 = x^3 - x$)? Quadratic twists of other $E_0/\mathbf{Q}$? "Taxicab curves" = twisted Fermat cubics $x^3 + y^3 = T$? Quartic twists $y^2 = x^3 + a_4 x$ (the general $j = 1728$ curve; special case of torsion $\mathbf{Z}/2\mathbf{Z}$)? "Mordell curves" $y^2 = x^3 + a_6$ (sextic twists, general $j = 0$)?

Heuristics for and against boundedness of rank

Those questions are all still wide open.

There has been considerable discussion about these questions, including purely intuitive/speculative guesses as well as heuristics based on analogy or data. Unfortunately even the more principled guesses don't all point in the same direction!

Thanks to B. Poonen for recounting some of these approaches (such as the function-field analogue, where r is unbounded [Šafarevič-Tate, Ulmer], and the observations of rank records as a function of time) in his Sep. 1 VaNTAGe talk.

I'll briefly add three more to this list: the ranks of tabulated curves (Antwerp/Tingley, Cremona, LMFDB); arithmetic and analytic bounds on N_E; an unpublished(?) counting heuristic.

Tabulations suggest large rank is rare . . .

The first table of (modular) elliptic curves (MFIV, Antwerp 1976, computed by Tingley et al.) listed all curves with conductor $N_E \leq 200$. There are 749 such E, in 281 isogeny classes [per LMFDB]. All have rank 0 or 1 (in 206+75 classes)!

The searches have now reached all $N_E \leq 500,000$, and ranks as large as 4 do arise, but slowly; e.g. LMFDB reports 3,064,705 curves but only 8899 of rank 3 and just one has rank 4 (conductor 234446, which also features two of the rank-3 curves).

Tabulations suggest large rank is rare . . .

The first table of (modular) elliptic curves (MFIV, Antwerp 1976, computed by Tingley et al.) listed all curves with conductor $N_E \leq 200$. There are 749 such E, in 281 isogeny classes [per LMFDB]. All have rank 0 or 1 (in 206+75 classes)!

The searches have now reached all $N_E \leq 500,000$, and ranks as large as 4 do arise, but slowly; e.g. LMFDB reports 3,064,705 curves but only 8899 of rank 3 and just one has rank 4 (conductor 234446, which also features two of the rank-3 curves).

. . . but this is to be expected.

Mestre (1986) obtained lower bounds on the conductor of an elliptic curve $E/\mathbf{Q}$ of rank r, assuming BSD + GRH for $L(E,s)$, by regarding the functional equation

$$\Lambda(E,s) := (2\pi)^{-s}\Gamma(s)L(E,s) = \pm N_E^{1-s}\Lambda(E,2-s)$$

as a formula for the conductor N_E. (This adapted a technique introduced by Odlyzko (1975) to bound the discriminant of a number field of degree $r_1 + 2r_2$.) For example, $r \geq 0 \Rightarrow N_E > 10$, and $r \geq 1 \Rightarrow N_E > 36$. That's sharp, since $N_E = 11$ and $N_E = 37$ actually happen! For $r \geq 2$ the bound is not as sharp but still exceeds 200 (rank 2 first happens for a curve of conductor 389).

In general Mestre shows $r \ll \log N_E$, so the smallest conductor of a rank-r curve must grow at least exponentially in r.

Nontrivial torsion even forces $r = o(\log N_E)$.

Once E_{tors} is nontrivial, N_E must grow at least as $\exp(Cr \log r)$.

For example, 2-torsion says $E : y^2 = x^3 + a_2 x^2 + a_4 x$. Assume $a_2, a_4 \in \mathbf{Z}$. Then x is square × S-unit where $S = \{p|a_4\}$. But x mod squares gives image of (x, y) in $E(\mathbf{Q})/\hat{\phi}(E'(\mathbf{Q}))$ where $E' : Y^2 = X^3 - 2a_2 X^2 + (a_2^2 - 4a_4)X$ is the 2-isogenous curve. Repeating the argument for E' bounds the size of $E(\mathbf{Q})/\hat{\phi}\phi E(\mathbf{Q}) = E(\mathbf{Q})/2E(\mathbf{Q})$, which is 2^{r+1}. So, N must be a product of at least r primes, etc.

Similarly for other torsion orders, using descent via the relevant isogeny. (NB there's no such bound for curves without torsion; e.g. the smallest known conductor of a curve of rank 11 is the prime 18031737725935636520843 [NDE-Watkins 2004]. For $y^2 = x^3 + a_6$ high rank may signal large 2- and 3-torsion in the class groups of $\mathbf{Q}(a_6^{1/3})$ and $\mathbf{Q}(a_6^{1/2})$ respectively.)

Point counting suggests lots of rank-2 curves!?

The rank of E also controls the growth of rational points of height $\leq H$, i.e. with $x = m/n$ with $|m|, |n| \leq H$: the number of such points is asymptotically proportional to (log $H)^{r/2}$ (the constant is $V_r|E_{\text{tors}}|/R^{1/2}$, where R = regulator; NB there's a factor $R/|E_{\text{tors}}|^2$ in BSD).

But if $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ then $x = m/n$ works iff $m^3n + a_2m^2n^2 + a_4mn^3 + a_6n^4$ is square, which should happen "with probability" $\sim C \max(|m|, |n|)^{-2}$, because a random large N is square with probability about $\frac{1}{4}|N|^{-1/2}$. Summing this over coprime (m, n) in $|m|, |n| \leq H$ gives a multiple of $\log H$. [Yes, n must be a square, but it's still $\log H$ growth.]

So, do we expect that $r = 2$ on average? Or mostly 0's and 1's but enough curves of rank ≥ 3 to make up the shortfall? Or is $m^3n + a_2m^2n^2 + a_4mn^3 + a_6n^4$ somehow a bit less likely to be a square than a random number of that size? . . .

Point counting suggests lots of rank-2 curves!?

The rank of E also controls the growth of rational points of height $\leq H$, i.e. with $x = m/n$ with $|m|, |n| \leq H$: the number of such points is asymptotically proportional to $(\log H)^{r/2}$ (the constant is $V_r|E_{\text{tors}}|/R^{1/2}$, where $R =$ regulator; NB there's a factor $R/|E_{\text{tors}}|^2$ in BSD).

But if $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ then $x = m/n$ works iff $m^3n + a_2m^2n^2 + a_4mn^3 + a_6n^4$ is square, which should happen "with probability" $\sim C \max(|m|, |n|)^{-2}$, because a random large N is square with probability about $\frac{1}{4}|N|^{-1/2}$. Summing this over coprime (m, n) in $|m|, |n| \leq H$ gives a multiple of $\log H$. [Yes, n must be a square, but it's still $\log H$ growth.]

So, do we expect that $r = 2$ on average? Or mostly 0's and 1's but enough curves of rank ≥ 3 to make up the shortfall? Or is $m^3n + a_2m^2n^2 + a_4mn^3 + a_6n^4$ somehow a bit less likely to be a square than a random number of that size? . . .

Point counting suggests lots of rank-2 curves!?

The rank of E also controls the growth of rational points of height $\leq H$, i.e. with $x = m/n$ with $|m|, |n| \leq H$: the number of such points is asymptotically proportional to $(\log H)^{r/2}$ (the constant is $V_r|E_{\text{tors}}|/R^{1/2}$, where $R =$ regulator; NB there's a factor $R/|E_{\text{tors}}|^2$ in BSD).

But if $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ then $x = m/n$ works iff $m^3n + a_2m^2n^2 + a_4mn^3 + a_6n^4$ is square, which should happen "with probability" $\sim C \max(|m|, |n|)^{-2}$, because a random large N is square with probability about $\frac{1}{4}|N|^{-1/2}$. Summing this over coprime (m, n) in $|m|, |n| \leq H$ gives a multiple of $\log H$. [Yes, n must be a square, but it's still $\log H$ growth.]

So, do we expect that $r = 2$ on average? Or mostly 0's and 1's but enough curves of rank ≥ 3 to make up the shortfall? Or is $m^3n + a_2m^2n^2 + a_4mn^3 + a_6n^4$ somehow a bit less likely to be a square than a random number of that size? . . .

Uniform Mordell–Weil vs. uniform Mordell–Faltings

⚠ A *misleading* analogy:

$E/\mathbf{Q}$ of genus 1:

Mordell(–Weil): $\forall E\ \exists r < \infty$: rank at most r
Uniform Mordell–Weil conjecture: $\exists r < \infty : \forall E$, rank at most r

$C/\mathbf{Q}$ of genus $g > 1$:

(Mordell–)Faltings: $\forall C\ \exists B < \infty : |C(\mathbf{Q})| \leq B$
Uniform Mordell–Faltings conj.: $\exists B_g < \infty : \forall C, |C(\mathbf{Q})| \leq B$

It's true that there's a lot of overlap between the two questions when it comes to record-hunting techniques (and record hunters), for both the "max" and "limsup" questions. But . . .

While both conjectures are open, for Mordell–Faltings all the evidence points in one direction, that uniform boundedness is true. There's even a theorem (Caporaso–Harris–Mazur 1997) that the existence of B_g is a consequence of the Bombieri–Lang conjectures on rational points on varieties of general type.

CHM start by proving that for each $g > 1$ there is B'_g and finitely many varieties of general type that together parametrize all genus-g curves C together with a B'_g-tuple of points on C. Then B–L supplies an algebraic dependence, "etc." by induction on dimension. That B'_g can even be made effective, though alas B_g and even the upper bound on $\limsup_C |C(\mathbf{Q})|$ is ineffective.

There can be no such path to uniform MW, because E^r is never of general type; indeed once E has positive rank there can be no algebraic condition on r-tuples of rational points.

While both conjectures are open, for Mordell–Faltings all the evidence points in one direction, that uniform boundedness is true. There's even a theorem (Caporaso–Harris–Mazur 1997) that the existence of B_g is a consequence of the Bombieri–Lang conjectures on rational points on varieties of general type.

CHM start by proving that for each $g > 1$ there is B'_g and finitely many varieties of general type that together parametrize all genus-g curves C together with a B'_g-tuple of points on C. Then B–L supplies an algebraic dependence, "etc." by induction on dimension. That B'_g can even be made effective, though alas B_g and even the upper bound on $\limsup_C |C(\mathbf{Q})|$ is ineffective.

There can be no such path to uniform MW, because E^r is never of general type; indeed once E has positive rank there can be no algebraic condition on r-tuples of rational points.

While both conjectures are open, for Mordell–Faltings all the evidence points in one direction, that uniform boundedness is true. There's even a theorem (Caporaso–Harris–Mazur 1997) that the existence of B_g is a consequence of the Bombieri–Lang conjectures on rational points on varieties of general type.

CHM start by proving that for each $g > 1$ there is B'_g and finitely many varieties of general type that together parametrize all genus-g curves C together with a B'_g-tuple of points on C. Then B–L supplies an algebraic dependence, "etc." by induction on dimension. That B'_g can even be made effective, though alas B_g and even the upper bound on $\limsup_C |C(\mathbf{Q})|$ is ineffective.

There can be no such path to uniform MW, because E^r is never of general type; indeed once E has positive rank there can be no algebraic condition on r-tuples of rational points.

The quest for high rank

It's easy to get E with a (usually) non-torsion point P_1: just fix $P_1 = (x_1, y_1)$ and A, and solve $y^2 = x^3 + Ax + B$ for B.

Two points: fix $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, and solve simult.lin.eqs. $y_i^2 = x_i^3 + Ax_i + B$ $(i = 1, 2)$ for A, B.

Three points: $y^2 = x^3 + a_2x^2 + a_4x + a_6$.

Five points: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Six: $a_0y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

The quest for high rank

It's easy to get E with a (usually) non-torsion point P_1: just fix $P_1 = (x_1, y_1)$ and A, and solve $y^2 = x^3 + Ax + B$ for B.

Two points: fix $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, and solve simult.lin.eqs. $y_i^2 = x_i^3 + Ax_i + B$ $(i = 1, 2)$ for A, B.

Three points: $y^2 = x^3 + a_2x^2 + a_4x + a_6$.

Five points: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Six: $a_0y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

The quest for high rank

It's easy to get E with a (usually) non-torsion point P_1: just fix $P_1 = (x_1, y_1)$ and A, and solve $y^2 = x^3 + Ax + B$ for B.

Two points: fix $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, and solve simult.lin.eqs. $y_i^2 = x_i^3 + Ax_i + B$ $(i = 1, 2)$ for A, B.

Three points: $y^2 = x^3 + a_2x^2 + a_4x + a_6$.

Five points: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Six: $a_0y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

The quest for high rank

It's easy to get E with a (usually) non-torsion point P_1: just fix $P_1 = (x_1, y_1)$ and A, and solve $y^2 = x^3 + Ax + B$ for B.

Two points: fix $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, and solve simult.lin.eqs. $y_i^2 = x_i^3 + Ax_i + B$ $(i = 1, 2)$ for A, B.

Three points: $y^2 = x^3 + a_2x^2 + a_4x + a_6$.

Five points: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Six: $a_0y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

The quest for high rank

It's easy to get E with a (usually) non-torsion point P_1: just fix $P_1 = (x_1, y_1)$ and A, and solve $y^2 = x^3 + Ax + B$ for B.

Two points: fix $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, and solve simult.lin.eqs. $y_i^2 = x_i^3 + Ax_i + B$ $(i = 1, 2)$ for A, B.

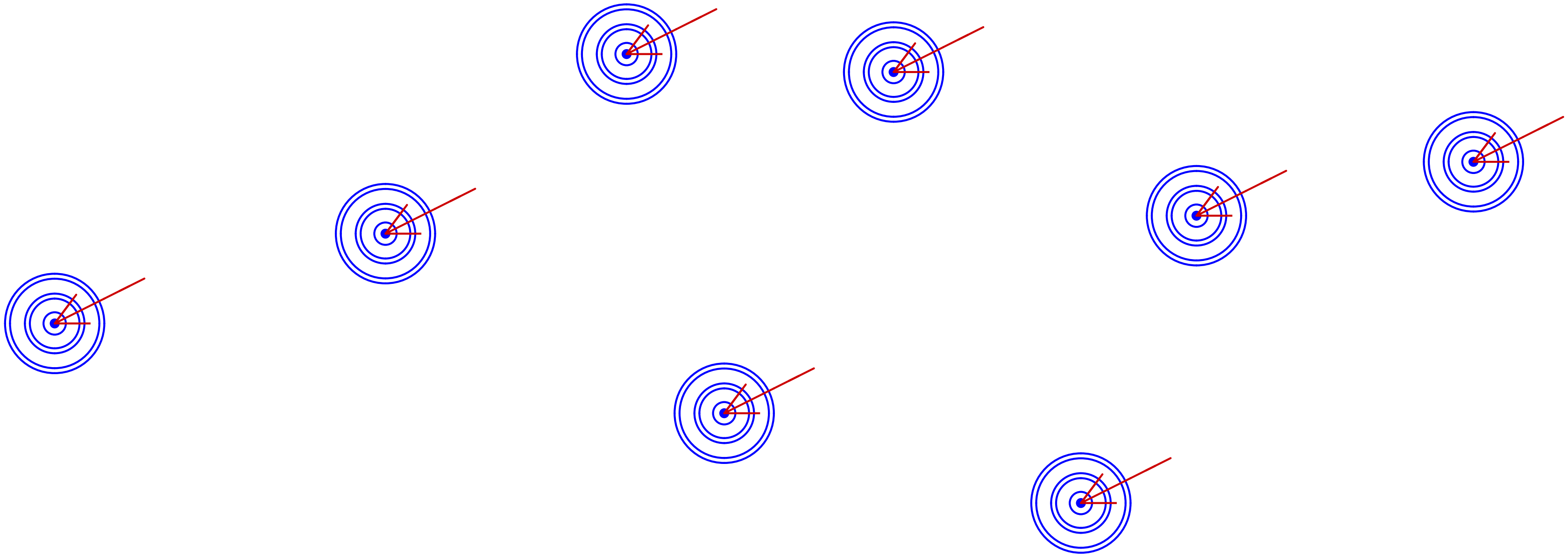
Three points: $y^2 = x^3 + a_2x^2 + a_4x + a_6$.

Five points: $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

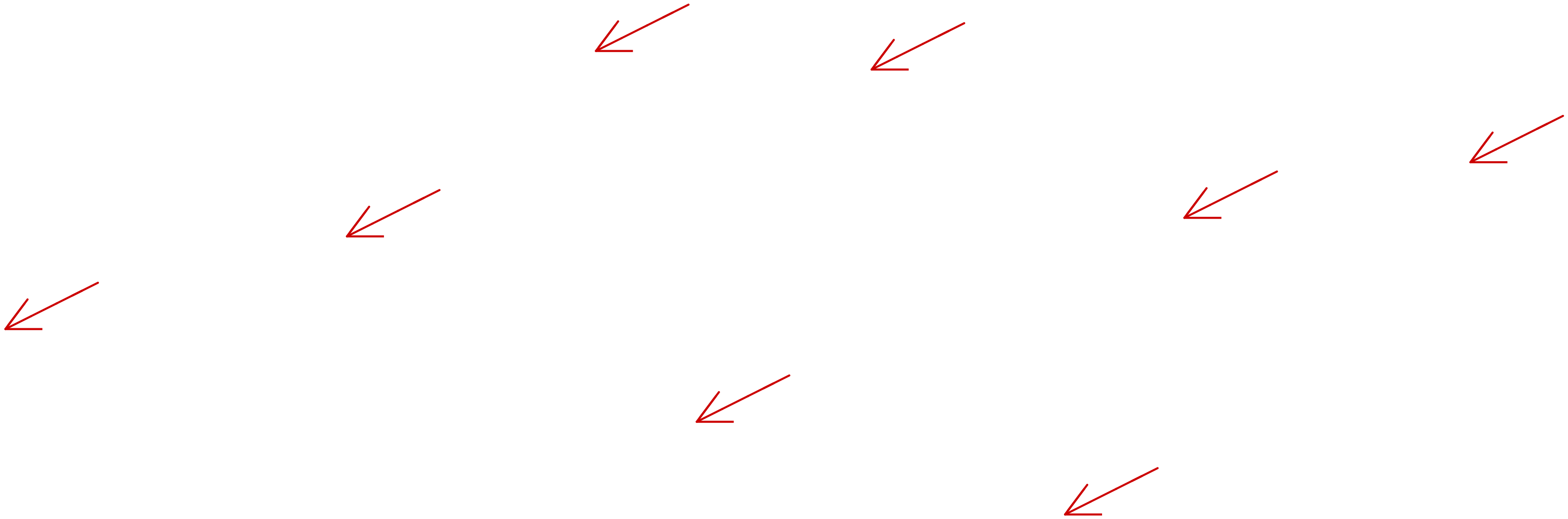
Six: $a_0y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

“Texas sharpshooter” :

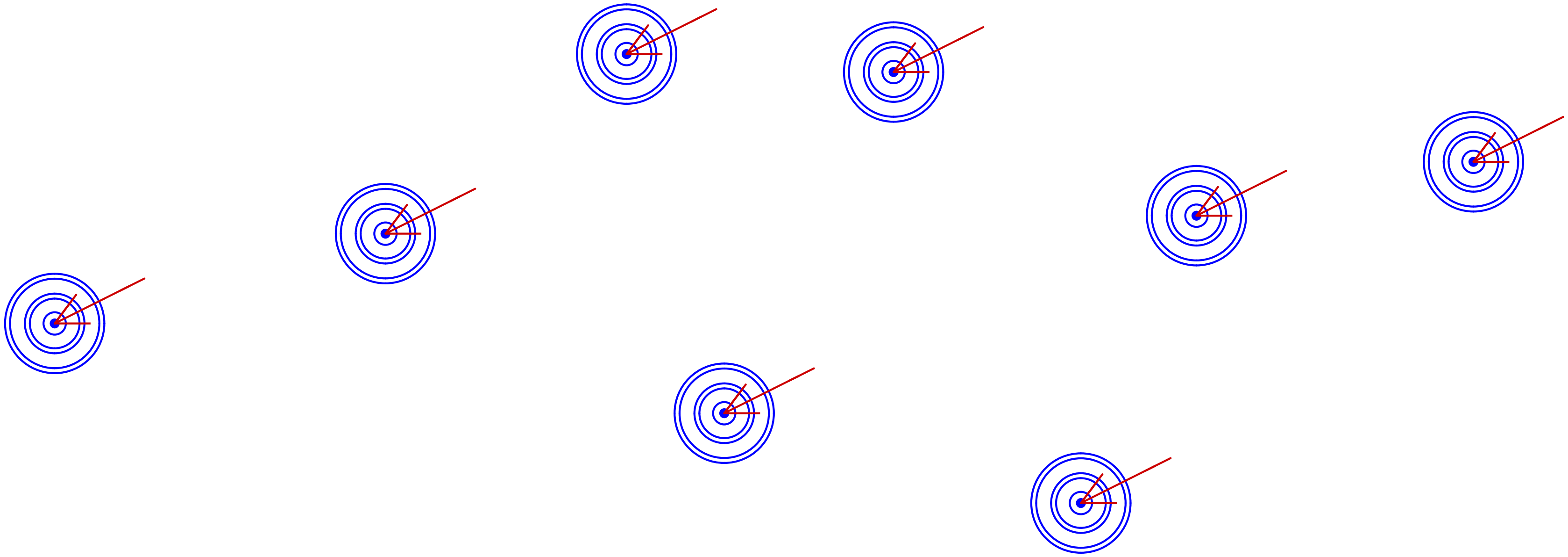
“Texas sharpshooter” :



“Texas sharpshooter” :



“Texas sharpshooter”:



Quest for high rank, cont'd

Nine points: Plane cubic through nine "random" points in $\mathbf{P}^2(\mathbf{Q})$

But that's the last case where we can fully describe all $(r+1)$-tuples $(E; P_1, \ldots, P_r)$: this variety is rational iff $r \leq 9$. [For $r = 10$ the point counts mod p include $-\tau(p)$, where $\tau(p) =$ Ramanujan function $= q^p$ coefficient of $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$!]

But our quiver is not empty yet: it is enough to find some infinite family of $(E; P_1, \ldots, P_r)$.

For example, Néron (1954) found a way to locate $P_1, \ldots, P_9$ that yields independent P_{10}, P_{11}.

Quest for high rank, cont'd

Nine points: Plane cubic through nine "random" points in $\mathbf{P}^2(\mathbf{Q})$

But that's the last case where we can fully describe <u>all</u> $(r+1)$-tuples $(E; P_1, \ldots, P_r)$: this variety is rational <u>iff</u> $r \leq 9$. [For $r = 10$ the point counts mod p include $-\tau(p)$, where $\tau(p) =$ Ramanujan function $= q^p$ coefficient of $\Delta = q \prod_{n=1}^{\infty}(1-q^n)^{24}$!]

But our quiver is not empty yet: it is enough to find <u>some</u> infinite family of $(E; P_1, \ldots, P_r)$.

For example, Néron (1954) found a way to locate $P_1, \ldots, P_9$ that yields independent P_{10}, P_{11}.

Quest for high rank, cont'd

Nine points: Plane cubic through nine "random" points in $\mathbf{P}^2(\mathbf{Q})$

But that's the last case where we can fully describe all $(r+1)$-tuples $(E; P_1, \ldots, P_r)$: this variety is rational iff $r \leq 9$. [For $r = 10$ the point counts mod p include $-\tau(p)$, where $\tau(p) =$ Ramanujan function $= q^p$ coefficient of $\Delta = q \prod_{n=1}^{\infty}(1-q^n)^{24}$!]

But our quiver is not empty yet: it is enough to find some infinite family of $(E; P_1, \ldots, P_r)$.

For example, Néron (1954) found a way to locate $P_1, \ldots, P_9$ that yields independent P_{10}, P_{11}.

Specialization theorems

How do we know that the P_i are independent?

Well, they might not be. But they're *generically* independent: there's no nontrivial relation $\sum_i a_i P_i = 0$ that holds identically. (Can be checked in various ways, including the canonical height pairing.)

Over a number field F, it follows by a specialization theorem that "most" choices yield E/F with independent rational points P_i (and that we get infinitely many different E this way).

Néron: exceptional set is "thin"; Silverman (1983), using heights: in one-dimensional family, exceptional set is finite.

For example, if we find a *nonconstant* $E/\mathbf{Q}(t)$ with torsion group G and independent points $P_1, \ldots, P_r$, we have infinitely many $E_t/\mathbf{Q}$ with torsion group (at least) G and r independent points $P_i(t)$. So, the rank limsup is at least r.

Moreover, we can search for t such that E_t has even more rational points; and search for base changes $t \in \mathbf{Q}(u)$ such that E_t has even more rational points over $\mathbf{Q}(u)$, increasing our lower bound on the rank limsup.

That's now the standard overall strategy for finding rank records.

NB: Likewise for Mordell-Faltings, and the specialization thm. is much easier. But by CHM the Bombieri-Lang conj. implies $\exists B_g$: any nonconstant $C/\mathbf{Q}(t)$ of genus g has $|C(\mathbf{Q}(t))| \leq B_g$. For elliptic curves this, too, is an open question even under standard conjectures.

For example, if we find a *nonconstant* $E/\mathbf{Q}(t)$ with torsion group G and independent points $P_1, \ldots, P_r$, we have infinitely many $E_t/\mathbf{Q}$ with torsion group (at least) G and r independent points $P_i(t)$. So, the rank limsup is at least r.

Moreover, we can search for t such that E_t has even more rational points; and search for base changes $t \in \mathbf{Q}(u)$ such that E_t has even more rational points over $\mathbf{Q}(u)$, increasing our lower bound on the rank limsup.

That's now the standard overall strategy for finding rank records.

NB: Likewise for Mordell-Faltings, and the specialization thm. is much easier. But by CHM the Bombieri-Lang conj. implies $\exists B_g$: any nonconstant $C/\mathbf{Q}(t)$ of genus g has $|C(\mathbf{Q}(t))| \leq B_g$. For elliptic curves this, too, is an open question even under standard conjectures.

Algebraic identities and algebraic geometry

Now a nonconstant curve $E/\mathbf{Q}(t)$ with independent points $P_1, \ldots, P_r$ can be viewed as both:

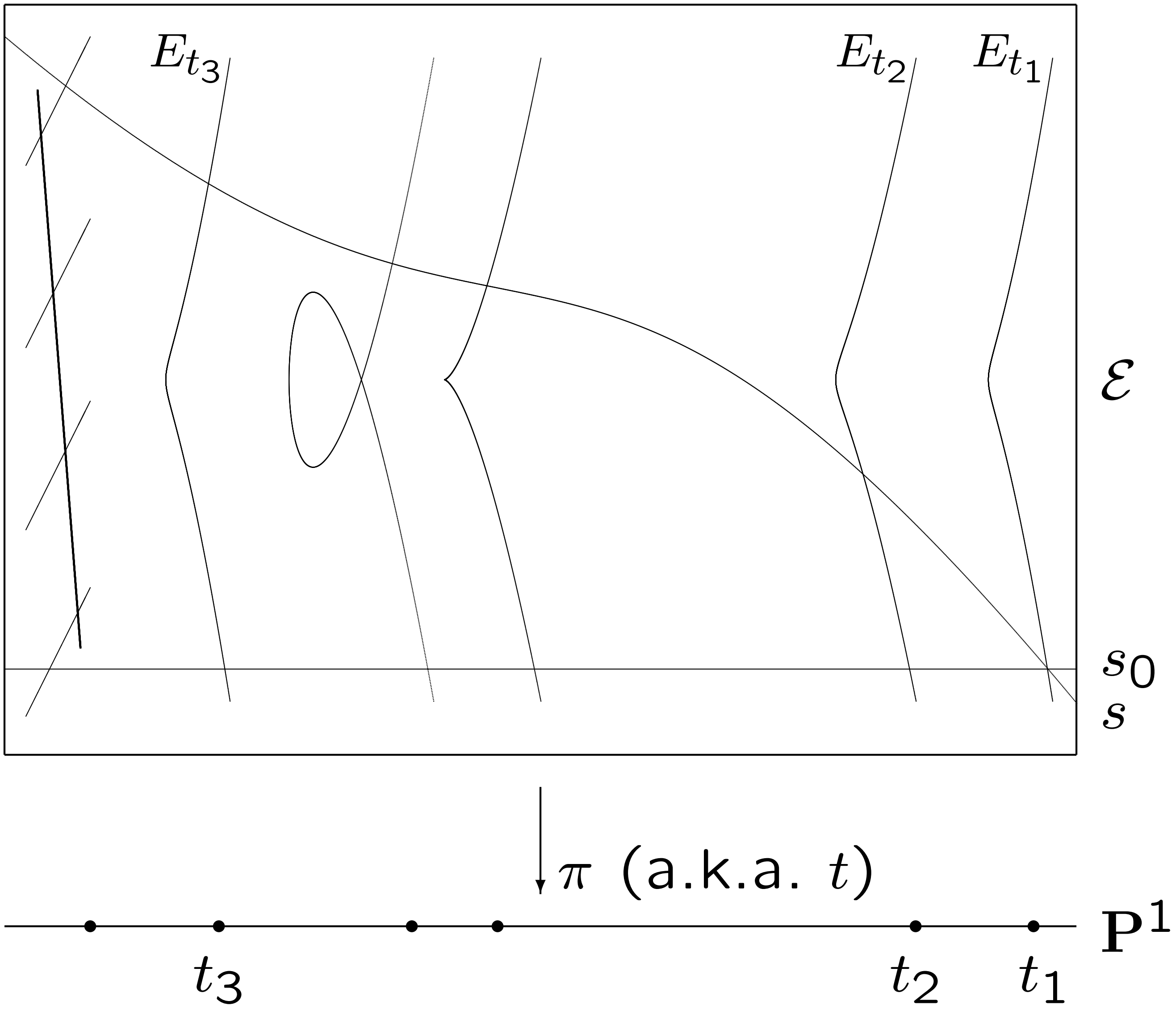
- A collection of r identities in rational functions $x_i(t), y_i(t)$ $(i = 1, \ldots, r)$ and $A(t), B(t)$: $y_i(t)^2 = x_i(t)^3 + A(t)x_i(t) + B(t)$,

and

- (The generic fiber of) an elliptic fibration $\mathcal{E} \to \mathbf{P}^1_t$ with r independent sections $s_i : \mathbf{P}^1_t \to \mathcal{E}$.

Likewise for E with nontrivial torsion group G (changing $y^2 = x^3 + Ax + B$ to $y^2 = x^3 + Ax^2 + Bx$, $y^2 + Axy + By = x^3$, "etc." for $G = \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$ etc.), or curves over other fields such as $Q(t_1, \ldots, t_n)$.

Standard picture/cartoon of an elliptic surface:



The geometric approach also lets us use the algebraic geometry of surfaces (intersection theory, moduli, etc.).

Néron's approach is geometric, closely related to geometry of rational elliptic surfaces $y^2 = x^3 + A(t)x + B(t)$ with $\deg A = 4$, $\deg B = 6$ (via $\mathbf{P}^2$ blown up at 8 of the 9 points).

Later constructions, with r as large as 14 (Mestre), emphasized the algebraic approach (often with clever exploitation of symmetry).

Recent records for small G (namely $|G| \leq 4$) use the geometry of elliptic K3 surfaces, with with $\deg A = 8$, $\deg B = 12$.

E.g. for trivial G we get $r = 17$ on a K3 surface, $r = 18$ on a quadratic base change, and $r = 19$ for an infinite family parametrized by an elliptic curve of positive rank (compositum of two quadratic base changes).

The geometric approach also lets us use the algebraic geometry of surfaces (intersection theory, moduli, etc.).

Néron's approach is geometric, closely related to geometry of rational elliptic surfaces $y^2 = x^3 + A(t)x + B(t)$ with $\deg A = 4$, $\deg B = 6$ (via $\mathbf{P}^2$ blown up at 8 of the 9 points).

Later constructions, with r as large as 14 (Mestre), emphasized the algebraic approach (often with clever exploitation of symmetry).

Recent records for small G (namely $|G| \leq 4$) use the geometry of elliptic K3 surfaces, with with $\deg A = 8$, $\deg B = 12$.

E.g. for trivial G we get $r = 17$ on a K3 surface, $r = 18$ on a quadratic base change, and $r = 19$ for an infinite family parametrized by an elliptic curve of positive rank (compositum of two quadratic base changes).

The geometric approach also lets us use the algebraic geometry of surfaces (intersection theory, moduli, etc.).

Néron's approach is geometric, closely related to geometry of rational elliptic surfaces $y^2 = x^3 + A(t)x + B(t)$ with $\deg A = 4$, $\deg B = 6$ (via $\mathbf{P}^2$ blown up at 8 of the 9 points).

Later constructions, with r as large as 14 (Mestre), emphasized the algebraic approach (often with clever exploitation of symmetry).

Recent records for small G (namely $|G| \leq 4$) use the geometry of elliptic K3 surfaces, with with $\deg A = 8$, $\deg B = 12$.

E.g. for trivial G we get $r = 17$ on a K3 surface, $r = 18$ on a quadratic base change, and $r = 19$ for an infinite family parametrized by an elliptic curve of positive rank (compositum of two quadratic base changes).

The geometric approach also lets us use the algebraic geometry of surfaces (intersection theory, moduli, etc.).

Néron's approach is geometric, closely related to geometry of rational elliptic surfaces $y^2 = x^3 + A(t)x + B(t)$ with $\deg A = 4$, $\deg B = 6$ (via $\mathbf{P}^2$ blown up at 8 of the 9 points).

Later constructions, with r as large as 14 (Mestre), emphasized the algebraic approach (often with clever exploitation of symmetry).

Recent records for small G (namely $|G| \leq 4$) use the geometry of elliptic K3 surfaces, with with $\deg A = 8$, $\deg B = 12$.

E.g. for trivial G we get $r = 17$ on a K3 surface, $r = 18$ on a quadratic base change, and $r = 19$ for an infinite family parametrized by an elliptic curve of positive rank (compositum of two quadratic base changes).

Another route to rank 21

(and 13,9,9 with $G = \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$, $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2\mathbf{Z})$, etc.)

Curiously the K3 route almost reproduces the heuristic of Park–Poonen–Voight–Wood for each of Mazur's fifteen G's except those that don't fit on an elliptic K3, namely $\mathbf{Z}/N\mathbf{Z}$ for $N = 9, 10, 12$ and $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/8\mathbf{Z})$.

Rather than try to develop the K3 picture towards the end of the lecture, let's just count parameters in identities; remarkably for K3 surfaces over $\mathbf{C}$ these dimension heuristics become theorems ("K3 Torelli")!

Start from $y^2 = x^3 + A(t)x + B(t)$ with A, B of degree $8, 12$. That's 9+13 coefficients for A and B, but scaling A, B by λ^4, λ^6 yields an equivalent surface, as do projective linear transformations of t (since A, B are really homogeneous polynomials in the projective coords. $(t_0 : t_1)$ on $\mathbf{P}^1$). So, $22 - 3 - 1 = 18$ parameters.

Suppose P_i has $x(t), y(t) =$ polynomials of degree $4, 6$. (More general rational functions make the analysis more complicated but the final count is the same). That's 5+7 more coefficients, and $y^2 = x^3 + Ax + B$ is 13 conditions, so we expect each P_i to impose $13 - (5 + 7) = 1$ condition on our 18 parameters.

Thus we expect to be able to do this 18 times, so there should be elliptic K3's of rank as large as 18, but no more. (True over $\mathbf{C}$; over $\mathbf{Q}$, not quite, but it does work over some other number fields.)

Start from $y^2 = x^3 + A(t)x + B(t)$ with A, B of degree $8, 12$. That's 9+13 coefficients for A and B, but scaling A, B by λ^4, λ^6 yields an equivalent surface, as do projective linear transformations of t (since A, B are really homogeneous polynomials in the projective coords. $(t_0 : t_1)$ on $\mathbf{P}^1$). So, $22 - 3 - 1 = 18$ parameters.

Suppose P_i has $x(t), y(t) =$ polynomials of degree $4, 6$. (More general rational functions make the analysis more complicated but the final count is the same). That's 5+7 more coefficients, and $y^2 = x^3 + Ax + B$ is 13 conditions, so we expect each P_i to impose $13 - (5 + 7) = 1$ condition on our 18 parameters.

Thus we expect to be able to do this 18 times, so there should be elliptic K3's of rank as large as 18, but no more. (True over $\mathbf{C}$; over $\mathbf{Q}$, not quite, but it does work over some other number fields.)

Start from $y^2 = x^3 + A(t)x + B(t)$ with A, B of degree $8, 12$. That's 9+13 coefficients for A and B, but scaling A, B by λ^4, λ^6 yields an equivalent surface, as do projective linear transformations of t (since A, B are really homogeneous polynomials in the projective coords. $(t_0 : t_1)$ on $\mathbf{P}^1$). So, $22 - 3 - 1 = 18$ parameters.

Suppose P_i has $x(t), y(t) =$ polynomials of degree $4, 6$. (More general rational functions make the analysis more complicated but the final count is the same). That's 5+7 more coefficients, and $y^2 = x^3 + Ax + B$ is 13 conditions, so we expect each P_i to impose $13 - (5 + 7) = 1$ condition on our 18 parameters.

Thus we expect to be able to do this 18 times, so there should be elliptic K3's of rank as large as 18, but no more. (True over $\mathbf{C}$; over $\mathbf{Q}$, not quite, but it does work over some other number fields.)

So, H^2 choices of t of height $\leq H$, each giving $r \geq 18$ with discriminant H^{24}. About half of these should have sign -1, so $r \geq 19$ which matches PPVW.

To reach $r = 20$, find $x(t)$ of degree 4 s.t. $x^3 + Ax + B$ is *almost* square, i.e. $Q_2 Q_5^2$. This does not cost a parameter. Then make $Q_2(t) = s^2$; that's a quadratic base change to a genus-0 curve, and we still have H such t of height $\leq H$.

Do this a second time to reach $r = 21$, parametrized by an elliptic curve so $\log^{\rho/2} H$ examples up to height H.

Likewise for the 10 nontrivial torsion groups that fit on a K3; e.g. $y^2 = x^3 + Ax^2 + Bx$ (with 2-torsion) has $4+8$ coefficients instead of $8+12$ so we end up with $r = 10$ on the K3 surface and $r = 13$ using the sign and biquadratic base change. In a few cases (such as $\mathbf{Z}/4\mathbf{Z}$, with $r = 7$) this works over $\mathbf{Q}$!

So, H^2 choices of t of height $\leq H$, each giving $r \geq 18$ with discriminant H^{24}. About half of these should have sign -1, so $r \geq 19$ which matches PPVW.

To reach $r = 20$, find $x(t)$ of degree 4 s.t. $x^3 + Ax + B$ is *almost* square, i.e. $Q_2 Q_5^2$. This does not cost a parameter. Then make $Q_2(t) = s^2$; that's a quadratic base change to a genus-0 curve, and we still have H such t of height $\leq H$.

Do this a second time to reach $r = 21$, parametrized by an elliptic curve so $\log^{\rho/2} H$ examples up to height H.

Likewise for the 10 nontrivial torsion groups that fit on a K3; e.g. $y^2 = x^3 + Ax^2 + Bx$ (with 2-torsion) has $4+8$ coefficients instead of $8+12$ so we end up with $r = 10$ on the K3 surface and $r = 13$ using the sign and biquadratic base change. In a few cases (such as $\mathbf{Z}/4\mathbf{Z}$, with $r = 7$) this works over $\mathbf{Q}$!

So, H^2 choices of t of height $\leq H$, each giving $r \geq 18$ with discriminant H^{24}. About half of these should have sign -1, so $r \geq 19$ which matches PPVW.

To reach $r = 20$, find $x(t)$ of degree 4 s.t. $x^3 + Ax + B$ is *almost* square, i.e. $Q_2 Q_5^2$. This does not cost a parameter. Then make $Q_2(t) = s^2$; that's a quadratic base change to a genus-0 curve, and we still have H such t of height $\leq H$.

Do this a second time to reach $r = 21$, parametrized by an elliptic curve so $\log^{\rho/2} H$ examples up to height H.

Likewise for the 10 nontrivial torsion groups that fit on a K3; e.g. $y^2 = x^3 + Ax^2 + Bx$ (with 2-torsion) has $4+8$ coefficients instead of $8+12$ so we end up with $r = 10$ on the K3 surface and $r = 13$ using the sign and biquadratic base change. In a few cases (such as $\mathbf{Z}/4\mathbf{Z}$, with $r = 7$) this works over $\mathbf{Q}$!

Caveats

- These curves don't actually look like what PPVW predicts: instead of r generators of height $\sim H^{2/r}$ it's $r-1$ of height $\sim \log H$ and a huge final generator of height $H^{2\pm o(1)}$.

- Over $\mathbb{Q}$ we end up just under the PPVW heuristic except for torsion groups 2×2, 4, 7, 8, 2×6. (E.g. $|\Delta| = 163$ is too small for $|G| \le 3$.)

- Going beyond K3 doesn't help directly, but the parameter-count heuristics might fail, allowing higher r. (Recall Shioda's rank-68 surface; even over $\mathbb{Q}$ there are examples for torsion 8 and 2×6 (Dujella–Peral 2012) with rank 1 more than the PPVW prediction.

Caveats

• These curves don't actually look like what PPVW predicts: instead of r generators of height $\sim H^{2/r}$ it's $r-1$ of height $\sim \log H$ and a huge final generator of height $H^{2\pm o(1)}$.

• Over $\mathbf{Q}$ we end up just under the PPVW heuristic except for torsion groups 2×2, 4, 7, 8, 2×6. (E.g. $|\Delta| = 163$ is too small for $|G| \leq 3$.)

• Going beyond K3 doesn't help directly, but the parameter-count heuristics might fail, allowing higher r. (Recall Shioda's rank-68 surface; even over $\mathbf{Q}$ there are examples for torsion 8 and 2×6 (Dujella–Peral 2012) with rank 1 more than the PPVW prediction.

Caveats

• These curves don't actually look like what PPVW predicts: instead of r generators of height $\sim H^{2/r}$ it's $r-1$ of height $\sim \log H$ and a huge final generator of height $H^{2\pm o(1)}$.

• Over $\mathbf{Q}$ we end up just under the PPVW heuristic except for torsion groups 2×2, 4, 7, 8, 2×6. (E.g. $|\Delta| = 163$ is too small for $|G| \leq 3$.)

• Going beyond K3 doesn't help directly, but the parameter-count heuristics might fail, allowing higher r. (Recall Shioda's rank-68 surface; even over $\mathbf{Q}$ there are examples for torsion 8 and 2×6 (Dujella–Peral 2012) with rank 1 more than the PPVW prediction.

Caveats

- These curves don't actually look like what PPVW predicts: instead of r generators of height $\sim H^{2/r}$ it's $r-1$ of height $\sim \log H$ and a huge final generator of height $H^{2\pm o(1)}$.

- Over $\mathbf{Q}$ we end up just under the PPVW heuristic except for torsion groups 2×2, 4, 7, 8, 2×6. (E.g. $|\Delta| = 163$ is too small for $|G| \leq 3$.)

- Going beyond K3 doesn't help directly, but the parameter-count heuristics might fail, allowing higher r. (Recall Shioda's rank-68 surface; even over $\mathbf{Q}$ there are examples for torsion 8 and 2×6 (Dujella–Peral 2012) with rank 1 more than the PPVW prediction.