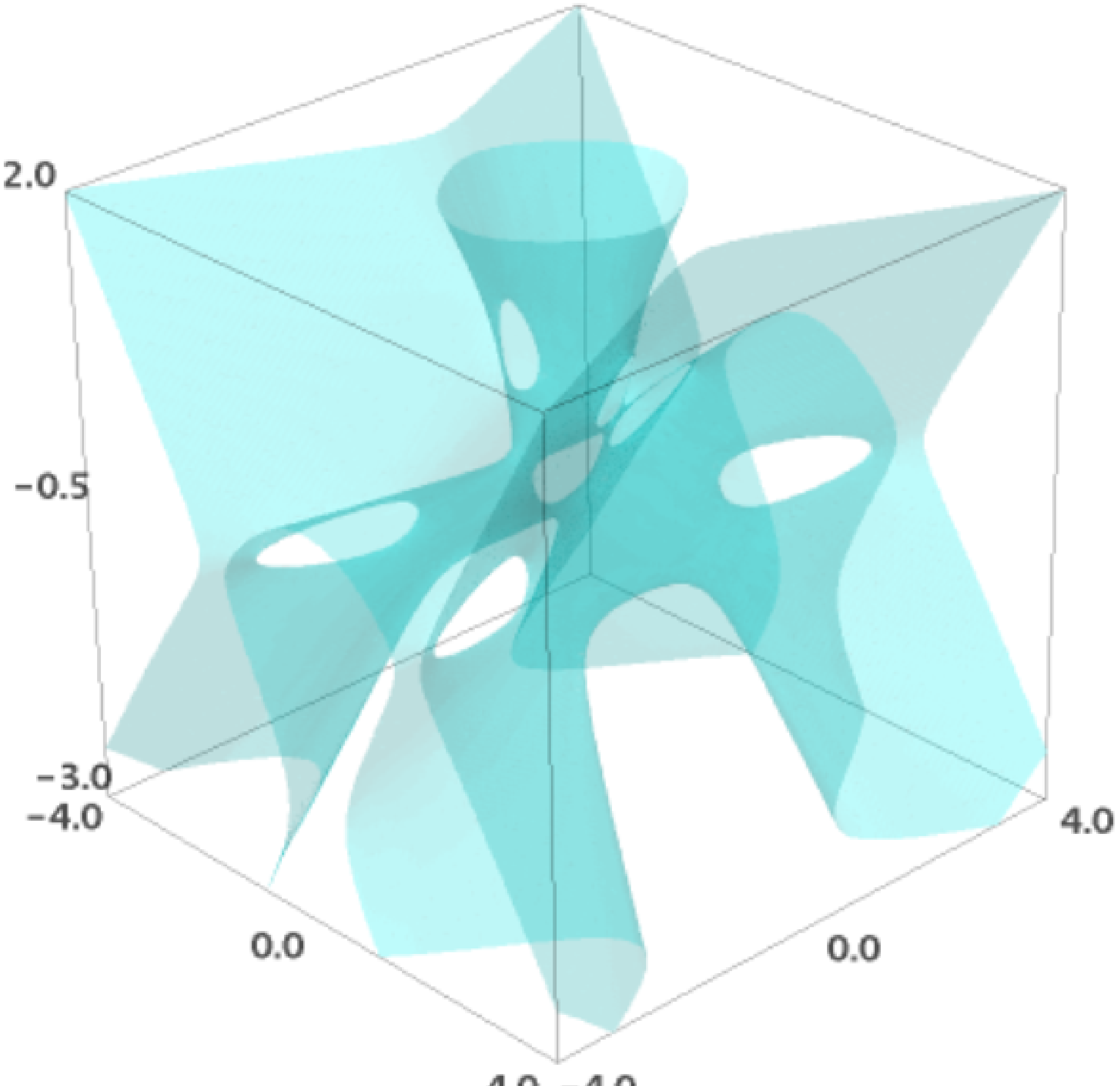

2.0
−0.5
−3.0
−4.0
0.0
4.0
−4.0
0.0
4.0

Curves with many points over number fields
ANTS-XIII Madison WI, 16 July 2018

Noam D. Elkies, Harvard University

Context: Diophantine eqns.; $d = 0$; $d = 1$: $g = 0$ and $g = 1$

Curves of general type: Faltings and Caporaso–Harris–Mazur

Brumer, Mestre, et al.

Connections with algebraic geometry

The K3 (and -163) connection

Fundamental problem(s) of number theory:

- Solve Diophantine equations
- Understand structure of solutions

For us, “Diophantine equation” = simult. polynomial eqns. in (usually too many) rational variables

Equiv.: simult. homogeneous equations in integer variables (e.g. Fermat: $x^n + y^n = z^n \iff (x/z)^n + (y/z)^n = 1$)

[Almost the same as Diophantus (3rd cent.) himself, though he used only positive values, so at most one of (x, y) and $(x, -y)$ in $y^2 = P(x)$.]

More generally: F with $[F : \mathbf{Q}] < \infty$. (Also: $\mathbf{Z}$; more generally: F; O_F and $O_{F,S}$. But not in this talk. Nor exponential Dioph. equations, etc.))

Fundamental problem(s) of number theory:

- Solve Diophantine equations
- Understand structure of solutions

For us, “Diophantine equation” = simult. polynomial eqns. in (usually too many) rational variables

Equiv.: simult. homogeneous equations in integer variables (e.g. Fermat: $x^n + y^n = z^n \iff (x/z)^n + (y/z)^n = 1$)

[Almost the same as Diophantus (3rd cent.) himself, though he used only positive values, so at most one of (x, y) and $(x, -y)$ in $y^2 = P(x)$.]

More generally: F with $[F : \mathbf{Q}] < \infty$. (Also: $\mathbf{Z}$; more generally: F; O_F and $O_{F,S}$. But not in this talk. Nor exponential Dioph. equations, etc.)

Fundamental problem(s) of number theory:

- Solve Diophantine equations
- Understand structure of solutions

For us, “Diophantine equation” = simult. polynomial eqns. in (usually too many) rational variables

Equiv.: simult. homogeneous equations in integer variables (e.g. Fermat: $x^n + y^n = z^n \iff (x/z)^n + (y/z)^n = 1$)

[Almost the same as Diophantus (3rd cent.) himself, though he used only positive values, so at most one of (x, y) and $(x, -y)$ in $y^2 = P(x)$.]

More generally: F with $[F : \mathbf{Q}] < \infty$. (Also: $\mathbf{Z}$; more generally: F; O_F and $O_{F,S}$. But not in this talk. Nor exponential Dioph. equations, etc.)

Fundamental problem(s) of number theory:

- Solve Diophantine equations
- Understand structure of solutions

For us, "Diophantine equation" = simult. polynomial eqns. in (usually too many) rational variables

Equiv.: simult. homogeneous equations in integer variables (e.g. Fermat: $x^n + y^n = z^n \iff (x/z)^n + (y/z)^n = 1$)

[Almost the same as Diophantus (3rd cent.) himself, though he used only positive values, so at most one of (x, y) and $(x, -y)$ in $y^2 = P(x)$.]

More generally: F with $[F : \mathbf{Q}] < \infty$. (Also: $\mathbf{Z}$; more generally: F; O_F and $O_{F,S}$. But not in this talk. Nor exponential Dioph. equations, etc.)

Broadly,

Geometric invariants of V $\iff$ difficulty

of the Diophantine equation.

First invariant: dimension of (components of) V.

Zero, one, (two,) many. . .

Simplest case: Dimension zero, e.g. $x^2 = 2$.

Only finitely many points; are any of them rational?

Easy and well-understood (sort of): elimination, polynomial factorization, Galois theory, etc. (Can still be computationally nontrivial with k equations in k variables once k gets well into "many" territory. . . e.g. computing Belyi functions.)

Broadly,

Geometric invariants of $V \iff$ difficulty

of the Diophantine equation.

First invariant: dimension of (components of) V.

Zero, one, (two,) many. . .

Simplest case: Dimension zero, e.g. $x^2 = 2$.

Only finitely many points; are any of them rational?

Easy and well-understood (sort of): elimination, polynomial factorization, Galois theory, etc. (Can still be computationally nontrivial with k equations in k variables once k gets well into "many" territory. . . e.g. computing Belyi functions.)

Broadly,

Geometric invariants of V $\Longleftrightarrow$ difficulty

of the Diophantine equation.

First invariant: dimension of (components of) V.

Zero, one, (two,) many. . .

Simplest case: Dimension zero, e.g. $x^2 = 2$.

Only finitely many points; are any of them rational?

Easy and well-understood (sort of): elimination, polynomial factorization, Galois theory, etc. (Can still be computationally nontrivial with k equations in k variables once k gets well into “many” territory. . . e.g. computing Belyi functions.)

Broadly,

Geometric invariants of V $\Longleftrightarrow$ difficulty

of the Diophantine equation.

First invariant: dimension of (components of) V.

Zero, one, (two,) many. . .

Simplest case: Dimension zero, e.g. $x^2 = 2$.

Only finitely many points; are any of them rational?

Easy and well-understood (sort of): elimination, polynomial factorization, Galois theory, etc. (Can still be computationally nontrivial with k equations in k variables once k gets well into "many" territory. . . e.g. computing Belyi functions.)

Broadly,

Geometric invariants of $V \iff$ **difficulty**

of the Diophantine equation.

First invariant: dimension of (components of) V.

Zero, one, (two,) many. . .

Simplest case: Dimension zero, e.g. $x^2 = 2$.

Only finitely many points; are any of them rational?

Easy and well-understood (sort of): elimination, polynomial factorization, Galois theory, etc. (Can still be computationally nontrivial with $\geq k$ equations in k variables once k gets well into “many” territory. . . e.g. computing Belyi functions.)

Dimension 1: an algebraic curve C. Complexity measured by "genus" $g = 0, 1, 2, 3, \ldots$

Again "zero, one, (two,) many"; here conic, elliptic curve, curve of general type.

$\underline{g = 0}$: Always a conic (sections of $-K$). Fully understood, at least in theory: $C \longleftrightarrow$ Br[2] obstruction, say $\beta(C)$, which is trivial $\Longleftrightarrow \exists$ rational point $\Longleftrightarrow C \cong_F \mathbf{P}^1$. [Minkowski; Hasse principle]

In practice, identifying C with conic can still be hard [e.g. $P_{71}(j, j')/(j \leftrightarrow j')$]; testing if $\beta(C) = 0 \longleftrightarrow$ factoring Δ, but then identifying with $\mathbf{P}^1$ is "easy" (in RP).

Dimension 1: an algebraic curve C. Complexity measured by "genus" $g = 0, 1, 2, 3, \ldots$

Again "zero, one, (two,) many"; here conic, elliptic curve, curve of general type.

$\underline{g = 0}$: Always a conic (sections of $-K$). Fully understood, at least in theory: $C \longleftrightarrow$ Br[2] obstruction, say $\beta(C)$, which is trivial $\Longleftrightarrow \exists$ rational point $\Longleftrightarrow C \cong_F \mathbf{P}^1$. [Minkowski; Hasse principle]

In practice, identifying C with conic can still be hard [e.g. $P_{71}(j, j')/(j \leftrightarrow j')$]; testing if $\beta(C) = 0 \longleftrightarrow$ factoring Δ, but then identifying with $\mathbf{P}^1$ is "easy" (in RP).

$g = 1$: The set $C(F)$ of "F-rational points" (points with coords. in F) can be empty, nonempty but finite, or infinite but sparse. It has "affine commutative group structure": a commutative group once any $P_0 \in C(F)$ is chosen as the origin. Also, always finitely generated [Mordell ($F = \mathbf{Q}$), Weil ($[F : \mathbf{Q}] < \infty$)].

Still a rich source of results and open questions for both theory and computation:

• Is $C(F) = \emptyset$? (Beyond Hasse, $C \longleftrightarrow$ obstruction in the still mysterious Tate-Šafarevič group Ш.)

• Torsion subgroup of $J_C(F)$? (Not hard)

• Rank and generators of $J_C(F)$? (Can be hard, even in theory [Ш again, also BSD, modularity, ...])

$g = 1$: The set $C(F)$ of "F-rational points" (points with coords. in F) can be empty, nonempty but finite, or infinite but sparse. It has "affine commutative group structure": a commutative group once any $P_0 \in C(F)$ is chosen as the origin. Also, always finitely generated [Mordell ($F = \mathbf{Q}$), Weil ($[F : \mathbf{Q}] < \infty$)].

Still a rich source of results and open questions for both theory and computation:

- Is $C(F) = \emptyset$? (Beyond Hasse, $C \longleftrightarrow$ obstruction in the still mysterious Tate-Šafarevič group Ш.)

- Torsion subgroup of $J_C(F)$? (Not hard)

- Rank and generators of $J_C(F)$? (Can be hard, even in theory [Ш again, also BSD, modularity, ...])

$g = 1$: The set $C(F)$ of "F-rational points" (points with coords. in F) can be empty, nonempty but finite, or infinite but sparse. It has "affine commutative group structure": a commutative group once any $P_0 \in C(F)$ is chosen as the origin. Also, always finitely generated [Mordell ($F = \mathbf{Q}$), Weil ($[F : \mathbf{Q}] < \infty$)].

Still a rich source of results and open questions for both theory and computation:

• Is $C(F) = \emptyset$? (Beyond Hasse, $C \longleftrightarrow$ obstruction in the still mysterious Tate-Šafarevič group Ш.)

• Torsion subgroup of $J_C(F)$? (Not hard)

• Rank and generators of $J_C(F)$? (Can be hard, even in theory [Ш again, also BSD, modularity, . . .])

$g = 1$: The set $C(F)$ of "F-rational points" (points with coords. in F) can be empty, nonempty but finite, or infinite but sparse. It has "affine commutative group structure": a commutative group once any $P_0 \in C(F)$ is chosen as the origin. Also, always finitely generated [Mordell ($F = \mathbf{Q}$), Weil ($[F : \mathbf{Q}] < \infty$)].

Still a rich source of results and open questions for both theory and computation:

- Is $C(F) = \emptyset$? (Beyond Hasse, $C \longleftrightarrow$ obstruction in the still mysterious Tate-Šafarevič group Ш.)

- Torsion subgroup of $J_C(F)$? (Not hard)

- Rank and generators of $J_C(F)$? (Can be hard, even in theory [Ш again, also BSD, modularity, . . .])

$g = 1$: The set $C(F)$ of "F-rational points" (points with coords. in F) can be empty, nonempty but finite, or infinite but sparse. It has "affine commutative group structure": a commutative group once any $P_0 \in C(F)$ is chosen as the origin. Also, always finitely generated [Mordell ($F = \mathbf{Q}$), Weil ($[F : \mathbf{Q}] < \infty$)].

Still a rich source of results and open questions for both theory and computation:

- Is $C(F) = \emptyset$? (Beyond Hasse, $C \longleftrightarrow$ obstruction in the still mysterious Tate-Šafarevič group Ш.)

- Torsion subgroup of $J_C(F)$? (Not hard)

- Rank and generators of $J_C(F)$? (Can be hard, even in theory [Ш again, also BSD, modularity, ...])

How do rank and torsion vary with C and F?

Easy to make either or both arbitrarily large, even for fixed C, if we may vary F (though there are still big questions about just how large either can get as a function of F).

For fixed F and varying C, the torsion is bounded [Mazur for $F = \mathbf{Q}$, with a known list: $\mathbf{Z}/N\mathbf{Z}$ for $N \leq 10$ or $N = 12$, or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ or $N \leq 4$); Merel in general, even if only $d = [F : \mathbf{Q}]$ is given, though the exact list is known only for d up to about 5.]

It remains a mystery whether the rank is bounded for varying C over any fixed F. If yes then $\limsup_C(\text{rank}(C/F))$ is unbounded as F varies, e.g. $\limsup \geq 2^{s-1}$ for $F = \mathbf{Q}(d_1^{1/2}, \ldots, d_s^{1/2})$.

How do rank and torsion vary with C and F?

Easy to make either or both arbitrarily large, even for fixed C, if we may vary F (though there are still big questions about just how large either can get as a function of F).

For fixed F and varying C, the torsion is bounded [Mazur for $F = \mathbf{Q}$, with a known list: $\mathbf{Z}/N\mathbf{Z}$ for $N \leq 10$ or $N = 12$, or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ or $N \leq 4$); Merel in general, even if only $d = [F : \mathbf{Q}]$ is given, though the exact list is known only for d up to about 5.]

It remains a mystery whether the rank is bounded for varying C over any fixed F. If yes then $\limsup_C(\mathrm{rank}(C/F))$ is unbounded as F varies, e.g. $\limsup \geq 2^{s-1}$ for $F = \mathbf{Q}(d_1^{1/2}, \ldots, d_s^{1/2})$.

How do rank and torsion vary with C and F?

Easy to make either or both arbitrarily large, even for fixed C, if we may vary F (though there are still big questions about just how large either can get as a function of F).

For fixed F and varying C, the torsion is bounded [Mazur for $F = \mathbf{Q}$, with a known list: $\mathbf{Z}/N\mathbf{Z}$ for $N \leq 10$ or $N = 12$, or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ or $N \leq 4$); Merel in general, even if only $d = [F : \mathbf{Q}]$ is given, though the exact list is known only for d up to about 5.]

It remains a mystery whether the rank is bounded for varying C over any fixed F. If yes then $\limsup_C(\mathrm{rank}(C/F))$ is unbounded as F varies, e.g. $\limsup \geq 2^{s-1}$ for $F = \mathbf{Q}(d_1^{1/2}, \ldots, d_s^{1/2})$.

How do rank and torsion vary with C and F?

Easy to make either or both arbitrarily large, even for fixed C, if we may vary F (though there are still big questions about just how large either can get as a function of F).

For fixed F and varying C, the torsion is bounded [Mazur for $F = \mathbf{Q}$, with a known list: $\mathbf{Z}/N\mathbf{Z}$ for $N \leq 10$ or $N = 12$, or $(\mathbf{Z}/2\mathbf{Z}) \oplus (\mathbf{Z}/2N\mathbf{Z})$ or $N \leq 4$); Merel in general, even if only $d = [F : \mathbf{Q}]$ is given, though the exact list is known only for d up to about 5.]

It remains a mystery whether the rank is bounded for varying C over any fixed F. If yes then $\limsup_C(\mathrm{rank}(C/F))$ is unbounded as F varies, e.g. $\limsup \geq 2^{s-1}$ for $F = \mathbf{Q}(d_1^{1/2}, \ldots, d_s^{1/2})$.

$g > 1$: Faltings (1983) proved $\#C(F) < \infty$, all C and F. (Mordell conjecture c.1920)

Every known proof is *ineffective*: given C, F, can get upper bound on $\#C(F)$, but typically no way to prove that a given list of solutions is complete, not even in principle. (Worse than Mordell–Weil theorem, which becomes effective once we know that Ш, or even one Ш$[p^\infty]$, is finite.) That's still a major open question for both theory and computation.

As with Mordell–Weil for rank and torsion of $g = 1$ curves: the upper bound on $\#C(F)$ can depend on C, F, and the actual $\#C(F)$ is easily unbounded if we let F vary, even with C fixed.

$g > 1$: Faltings (1983) proved $\#C(F) < \infty$, all C and F. (Mordell conjecture c.1920)

Every known proof is *ineffective*: given C, F, can get upper bound on $\#C(F)$, but typically no way to prove that a given list of solutions is complete, not even in principle. (Worse than Mordell–Weil theorem, which becomes effective once we know that Ш, or even one Ш$[p^\infty]$, is finite.) That's still a major open question for both theory and computation.

As with Mordell–Weil for rank and torsion of $g = 1$ curves: the upper bound on $\#C(F)$ can depend on C, F, and the actual $\#C(F)$ is easily unbounded if we let F vary, even with C fixed.

Fix F, then — say $F = \mathbf{Q}$. Remaining questions:

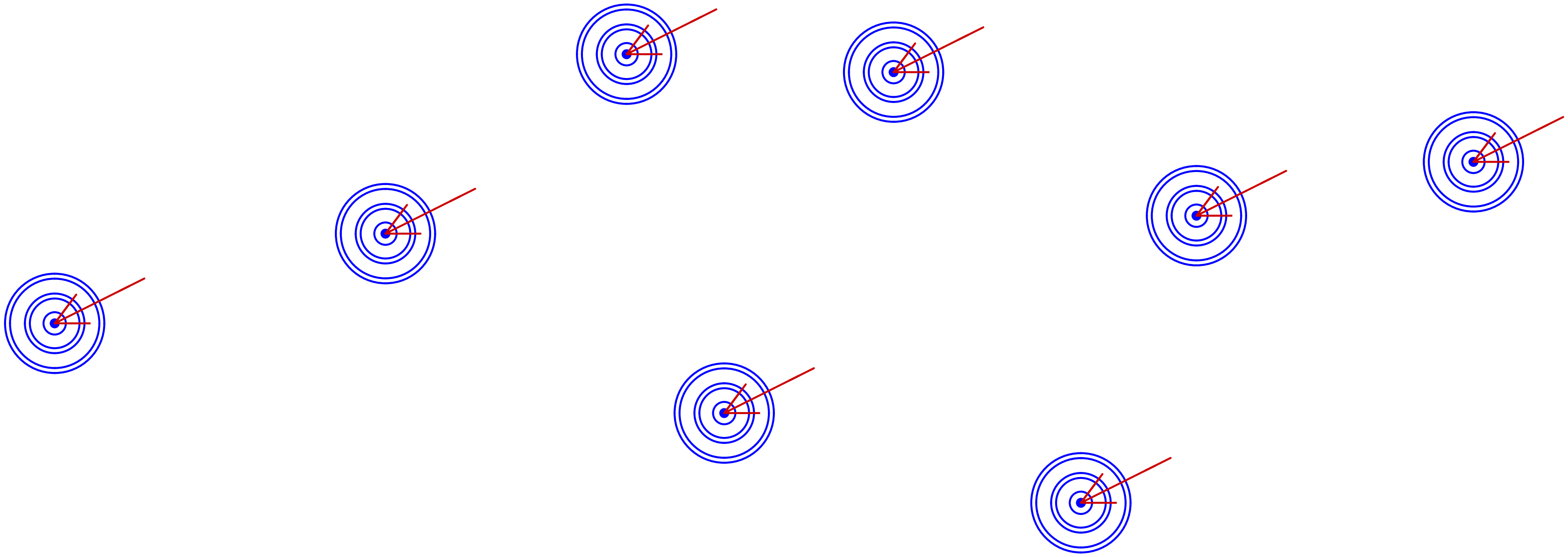
- How many points can C have? In particular, is the number unbounded as C varies over curves with $g > 1$?

Yes, easily. . . "Texas sharpshooter":

Fix F, then — say $F = \mathbf{Q}$. Remaining questions:

- How many points can C have? In particular, is the number unbounded as C varies over curves with $g > 1$?

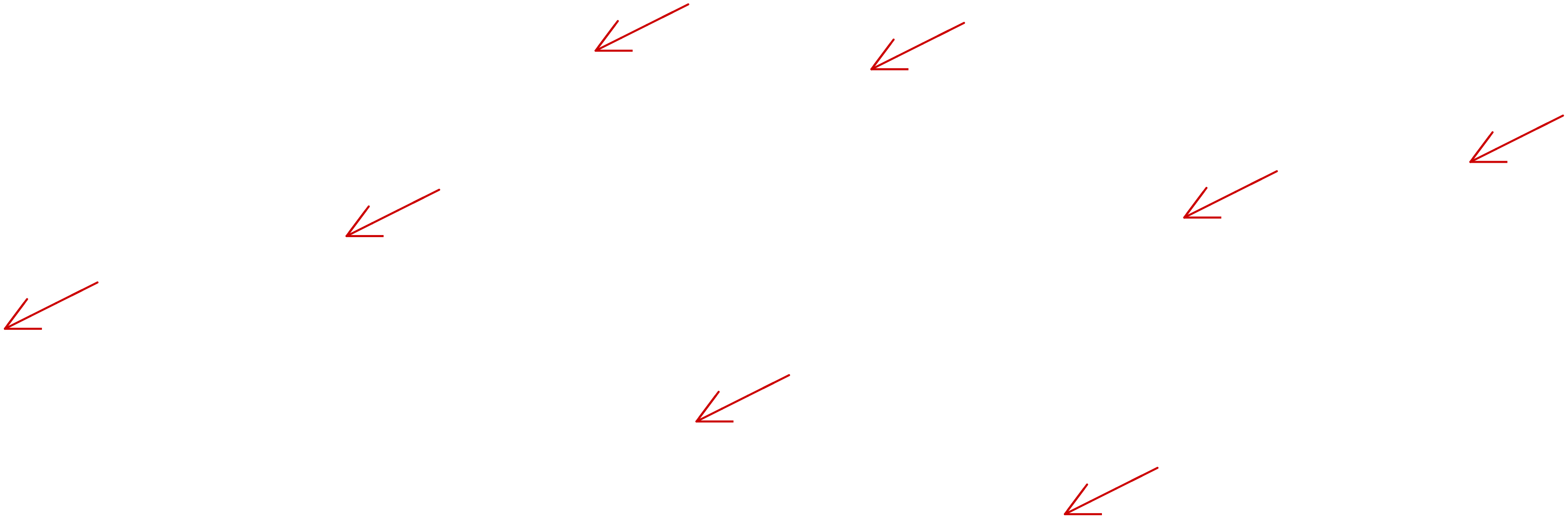
Yes, easily. . . “Texas sharpshooter”:



Fix F, then — say $F = \mathbf{Q}$. Remaining questions:

- How many points can V have? In particular, is the number unbounded as V varies over curves with $g > 1$?

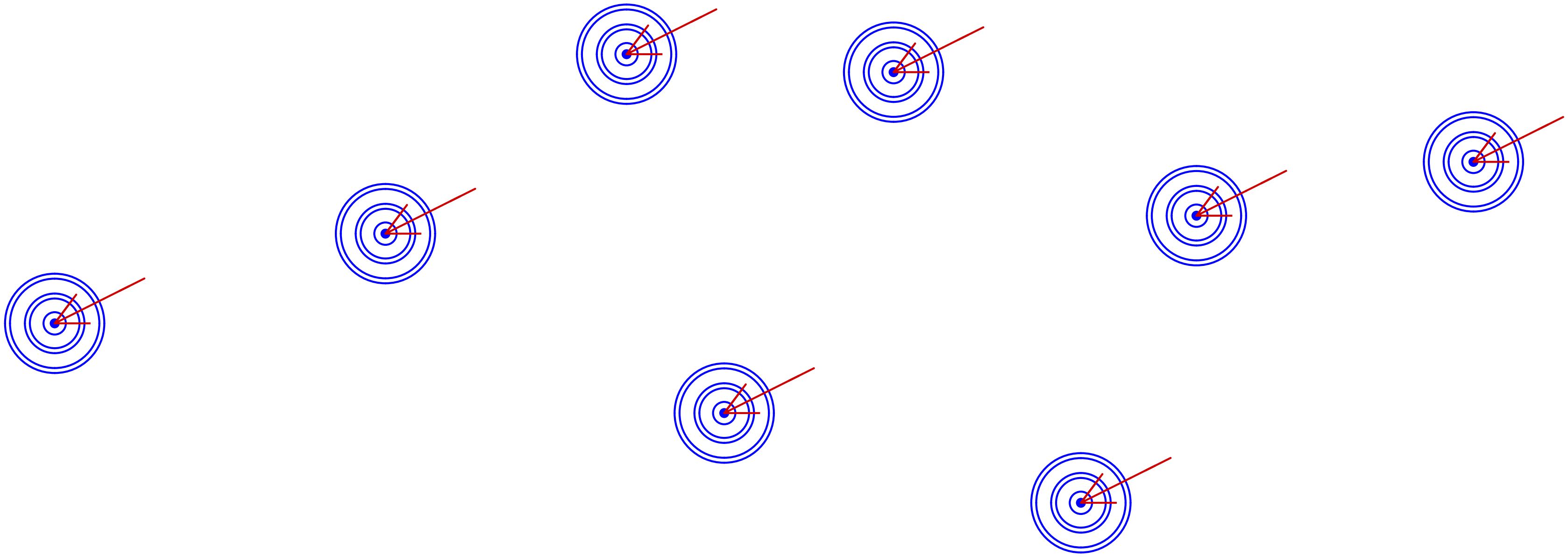
Yes, easily. . . “Texas sharpshooter”:



Fix F, then — say $F = \mathbf{Q}$. Remaining questions:

- How many points can V have? In particular, is the number unbounded as V varies over curves with $g > 1$?

Yes, easily. . . "Texas sharpshooter":



For example: given (x_i, y_i), solve for the coefficients of P to make each $y_i^2 = P(x_i)$ — simultaneous linear equations, so rational (and usually no repeated factors).

So the number of points can get arbitrarily large if g may vary. The right question is:

- Fix $g > 1$. How many points can a genus-g curve C have? In particular, is the number unbounded as C varies over all such C?

In other words: let $B(g, F)$ be $\sup_C(\#C(F))$ over all genus-g curves C/F. Is $B(g, F) = \infty$ for some/any $g > 1$ and F with $[F : \mathbf{Q}] < \infty$?

For example: given (x_i, y_i), solve for the coefficients of P to make each $y_i^2 = P(x_i)$ — simultaneous linear equations, so rational (and usually no repeated factors).

So the number of points can get arbitrarily large if g may vary. The right question is:

- Fix $g > 1$. How many points can a genus-g curve C have? In particular, is the number unbounded as C varies over all such C?

In other words: let $B(g, F)$ be $\sup_C(\#C(F))$ over all genus-g curves C/F. Is $B(g, F) = \infty$ for some/any $g > 1$ and F with $[F : \mathbf{Q}] < \infty$?

For example: given (x_i, y_i), solve for the coefficients of P to make each $y_i^2 = P(x_i)$ — simultaneous linear equations, so rational (and usually no repeated factors).

So the number of points can get arbitrarily large if g may vary. The right question is:

- Fix $g > 1$. How many points can a genus-g curve C have? In particular, is the number unbounded as C varies over all such C?

In other words: let $B(g, F)$ be $\sup_C(\#C(F))$ over all genus-g curves C/F. Is $B(g, F) = \infty$ for some/any $g > 1$ and F with $[F : \mathbf{Q}] < \infty$?

This may feel like the $g = 1$ question of whether an elliptic curve can have arbitrarily large rank; indeed similar techniques are used (often by the same people) to search for records on both questions. But there's a difference:

Theorem (Caporaso-Harris-Mazur 1997): *Assume Bombieri-Lang conjecture. Then $B(g) < \infty$ for all $g > 1$.*

“Bombieri-Lang conjecture” = analogue of Mordell-Faltings for algebraic varieties of arbitrary dimension:

Conjecture (Bombieri-Lang 1986): *Suppose V is an algebraic variety of general type, and $[F : \mathbf{Q}] < \infty$. Then all of $V(F)$ is in a finite union of subvarieties V_i' each of dimension $< \dim(V)$.*

[NB A curve is of “general type” iff its genus is > 1.]

This may feel like the $g = 1$ question of whether an elliptic curve can have arbitrarily large rank; indeed similar techniques are used (often by the same people) to search for records on both questions. But there's a difference:

Theorem (Caporaso-Harris-Mazur 1997): *Assume Bombieri-Lang conjecture. Then $B(g) < \infty$ for all $g > 1$.*

"Bombieri-Lang conjecture" is an analogue of Mordell-Faltings for algebraic varieties of arbitrary dimension:

Conjecture (Bombieri-Lang 1986): *Suppose V is an algebraic variety of general type, and $[F : \mathbf{Q}] < \infty$. Then all of $V(F)$ is in a finite union of subvarieties V_i' each of dimension $< \dim(V)$.*

[NB A curve is of "general type" iff its genus is > 1.]

This may feel like the $g = 1$ question of whether an elliptic curve can have arbitrarily large rank; indeed similar techniques are used (often by the same people) to search for records on both questions. But there's a difference:

Theorem (Caporaso-Harris-Mazur 1997): *Assume Bombieri-Lang conjecture. Then $B(g) < \infty$ for all $g > 1$.*

"Bombieri-Lang conjecture" is an analogue of Mordell-Faltings for algebraic varieties of arbitrary dimension:

Conjecture (Bombieri-Lang 1986): *Suppose V is an algebraic variety of general type, and $[F : \mathbf{Q}] < \infty$. Then all of $V(F)$ is in a finite union of subvarieties V_i' each of dimension $< \dim(V)$.*

[NB A curve is of "general type" iff its genus is > 1.]

There is even a corresponding result that is uniform in F, once we allow a finite number of exceptions (that may depend on F). That is, instead of

$$B(g, F) := \sup_C (\#C(F))$$

consider

$$N(g, F) := \limsup_C (\#C(F)) \leq B(g, F)$$

again with C varying over all genus-g curves C/F. Now it is not so easy to refute an upper bound uniform in F, i.e. the possibility that

$$N(g) := \sup_{[F:\mathbf{Q}]<\infty} N(g, F)$$

might be finite. Indeed, Caporaso-Harris-Mazur also proved:

$$\text{[repeat]}\qquad \begin{aligned} B(g,F) &:= \sup_C(\#C(F));\\ N(g,F) &:= \limsup_C(\#C(F)) \leq B(g,F);\\ N(g) &:= \sup_{[F:\mathbf{Q}]<\infty} N(g,F). \end{aligned}$$

Theorem: *Assume uniform Bombieri-Lang conjecture. Then $N(g) < \infty$ for all $g > 1$.*

Uniform Bombieri-Lang conjecture:

Suppose V is an algebraic variety of general type. Then $\exists$ finitely many subvarieties V_i' with each $\dim V_i' < \dim V$, s.t. $[F : \mathbf{Q}] < \infty \Rightarrow V(F) - \bigcup_i V_i'(F)$ is finite.

So what are $B(g,F)$, $N(g,F)$ and $B(g)$? Again ineffective . . . would need effective Bombieri-Lang.

[repeat]

$$\begin{aligned} B(g,F) &:= \sup_C(\#C(F)); \\ N(g,F) &:= \limsup_C(\#C(F)) \leq B(g,F); \\ N(g) &:= \sup_{[F:\mathbf{Q}]<\infty} N(g,F). \end{aligned}$$

Theorem: *Assume <u>uniform</u> Bombieri-Lang conjecture. Then* $N(g) < \infty$ *for all* $g > 1$.

Uniform Bombieri-Lang conjecture:

Suppose V *is an algebraic variety of general type. Then* $\exists$ *finitely many subvarieties* V_i' *with each* $\dim V_i' < \dim V$, *s.t.* $[F:\mathbf{Q}] < \infty \Rightarrow V(F) - \bigcup_i V_i'(F)$ *is finite.*

So what are $B(g,F)$, $N(g,F)$ and $B(g)$? Again ineffective . . . would need effective Bombieri-Lang.

Idea of Caporaso-Harris-Mazur: given g, put any C in one of finitely many parametrized families of curves. E.g.

$$g = 2 : \quad y^2 = \sum_{i=0}^{6} t_i x^i = P_6(x);$$

$g = 3$: either $y^2 = P_8(x)$ or $P_4(x, y) = 0$. Then if each of $P_1, \ldots, P_n$ is on C then $(C, P_1, P_2, \ldots, P_n)$ is a point on some variety V, which is of general type for n large enough. So Bombieri-Lang ⇒ they satisfy some relation. Now carefully repeat until $(C, P_1, P_2, \ldots, P_{N+1})$ must have some $P_i = P_j$ with finitely many exceptions.

As noted, the resulting upper bounds on $N(g, F)$ and $N(g)$, and thus on $B(g, F)$, are ineffective; they seem likely to remain so for some time. So for now we play the record-hunting game of seeking genus-g curves, or families of such curves, with many F-rational points.

Idea of Caporaso-Harris-Mazur: given g, put any C in one of finitely many parametrized families of curves. E.g.

$$g = 2 : \quad y^2 = \sum_{i=0}^{6} t_i x^i = P_6(x);$$

$g = 3$: either $y^2 = P_8(x)$ or $P_4(x, y) = 0$. Then if each of $P_1, \ldots, P_n$ is on C then $(C, P_1, P_2, \ldots, P_n)$ is a point on some variety V, which is of general type for n large enough. So Bombieri-Lang $\Rightarrow$ they satisfy some relation. Now carefully repeat until $(C, P_1, P_2, \ldots, P_{N+1})$ must have some $P_i = P_j$ with finitely many exceptions.

As noted, the resulting upper bounds on $N(g, F)$ and $N(g)$, and thus on $B(g, F)$, are ineffective; they seem likely to remain so for some time. So for now we play the record-hunting game of seeking genus-g curves, or families of such curves, with many F-rational points.

While ineffective, this suggests a geometric interpretation for $N(g)$: the largest N such that $\exists$ parametrized family $\mathcal{C} \xrightarrow{\pi} B$ of genus-g curves $C = \pi^{-1}(\mathrm{pt})$ with N sections (one-sided inverses $s_i : B \to \mathcal{C}$ and $B(F) = \infty$. Because $\dim \mathcal{C} = \dim B + 1$, we usually want $\dim B = 1$ (recall "zero, one, (two,) many"); then, for $\#B(F) = \infty$ for some F, need B of genus 0 or 1.

More explicitly: seek algebraic identities for parametrized family of genus-g curves, e.g. $C(t_1, \ldots, t_d)$ if B is rational of dim. d, together with points $P_1, \ldots, P_N$ (images of $(t_1, \ldots, t_d)$ under $s_1, \ldots, s_N$).

We can then try to push lower bound on $B(g, F)$ (max. known number of points on genus-g curve over F) by searching $B(F)$ (e.g. $(t_1, \ldots, t_d) \in F^d$) for which C has numerous points other than the s_i images (minus collisions among those images ...).

While ineffective, this suggests a geometric interpretation for $N(g)$: the largest N such that $\exists$ parametrized family $\mathcal{C} \xrightarrow{\pi} B$ of genus-g curves $C = \pi^{-1}(\mathrm{pt})$ with N sections (one-sided inverses $s_i : B \to \mathcal{C}$ and $B(F) = \infty$. Because $\dim \mathcal{C} = \dim B + 1$, we usually want $\dim B = 1$ (recall "zero, one, (two,) many"); then, for $\#B(F) = \infty$ for some F, need B of genus 0 or 1.

More explicitly: seek algebraic identities for parametrized family of genus-g curves, e.g. $C(t_1, \ldots, t_d)$ if B is rational of dim. d, together with points $P_1, \ldots, P_N$ (images of $(t_1, \ldots, t_d)$ under $s_1, \ldots, s_N$).

We can then try to push lower bound on $B(g, F)$ (max. known number of points on genus-g curve over F) by searching $B(F)$ (e.g. $(t_1, \ldots, t_d) \in F^d$) for which C has numerous points other than the s_i images (minus collisions among those images ...).

While ineffective, this suggests a geometric interpretation for $N(g)$: the largest N such that $\exists$ parametrized family $\mathcal{C} \overset{\pi}{\to} B$ of genus-g curves $C = \pi^{-1}(\mathrm{pt})$ with N sections (one-sided inverses $s_i : B \to \mathcal{C}$ and $B(F) = \infty$. Because $\dim \mathcal{C} = \dim B + 1$, we usually want $\dim B = 1$ (recall "zero, one, (two,) many"); then, for $\#B(F) = \infty$ for some F, need B of genus 0 or 1.

More explicitly: seek algebraic identities for parametrized family of genus-g curves, e.g. $C(t_1, \ldots, t_d)$ if B is rational of dim. d, together with points $P_1, \ldots, P_N$ (images of $(t_1, \ldots, t_d)$ under $s_1, \ldots, s_N$).

We can then try to push lower bound on $B(g, F)$ (max. known number of points on genus-g curve over F) by searching $B(F)$ (e.g. $(t_1, \ldots, t_d) \in F^d$) for which C has numerous points other than the s_i images (minus collisions among those images . . .).

Indeed "arrows, then bullseyes" is an example: the parameters are x_i, y_i; for genus g, we need $y^2 = P(x)$ with $\deg P = 2g + 2$, so we can force $2g + 3$ points. Thanks to the symmetry $(x, y) \longleftrightarrow (x, -y)$ we double the count of points for free.

This illustrates two further themes:

- $N(g, \mathbf{Q}) \gg g$ as $g \to \infty$. Thus *a fortiori* $B(g, \mathbf{Q}) \gg g$ and $N(g) \gg g$. Open question: can we do better? That is: are $\limsup_g B(g, \mathbf{Q})/g$ and $\limsup_g N(g)/g$ finite?

- Aut(C) can help. Already for $g = 3$ all the records are for hyperelliptic curves $y^2 = P_8(x)$, even though that's a special case (5 parameters, not 6). Maybe more natural to aim for many Aut(C) orbits in $C(F)$.

Indeed “arrows, then bullseyes” is an example: the parameters are x_i, y_i; for genus g, we need $y^2 = P(x)$ with $\deg P = 2g + 2$, so we can force $2g + 3$ points. Thanks to the symmetry $(x, y) \longleftrightarrow (x, -y)$ we double the count of points for free.

This illustrates two further themes:

• $N(g, \mathbf{Q}) \gg g$ as $g \to \infty$. Thus *a fortiori* $B(g, \mathbf{Q}) \gg g$ and $N(g) \gg g$. Open question: can we do better? That is: are $\limsup_g B(g, \mathbf{Q})/g$ and $\limsup_g N(g)/g$ finite?

• $\mathrm{Aut}(C)$ can help. Already for $g = 3$ all the records are for hyperelliptic curves $y^2 = P_8(x)$, even though that's a special case (5 parameters, not 6). Maybe more natural to aim for many $\mathrm{Aut}(C)$ orbits in $C(F)$.

The $4g + O(1)$ construction can still be improved to hyperelliptic curves attaining $N(g, \mathbf{Q}) \geq 8g + C$ and $N(g) \geq 16g + C'$ (Brumer and Mestre independently).

For $N(g, \mathbf{Q}) > 8g + C$: for rational x_i write

$$\prod_{i=1}^{2n} (X - x_i) = Q(X)^2 - R(X)$$

with $\deg Q = n$ and $\deg R < n$ (usually $n - 1$). Then each $Q(x_i)^2 = R(x_i)$ so we have $2n$ pairs $(x_i, \pm Q(x_i))$ of rational points on the curve $Y^2 = R(X)$ of $g < n/2$.

Likewise

$$\prod_{i=1}^{4} (X^n - x_i^n) = Q(X^n)^2 - (R_1 X^n + R_0),$$

so if $n = 2g+2$ and $F \supset \boldsymbol{\mu}_n$ then $Y^2 = R_1 X^n + R_0$ has $16(g+1)$ points $(\zeta x_i, \pm Q(x_i^n))$ with $1 \leq i \leq 4$ and $\zeta^n = 1$ (though in only four $\mathrm{Aut}(C)$ orbits).

The $4g + O(1)$ construction can still be improved to hyperelliptic curves attaining $N(g, \mathbf{Q}) \geq 8g + C$ and $N(g) \geq 16g + C'$ (Brumer and Mestre independently).

For $N(g, \mathbf{Q}) > 8g + C$: for rational x_i write

$$\prod_{i=1}^{2n} (X - x_i) = Q(X)^2 - R(X)$$

with $\deg Q = n$ and $\deg R < n$ (usually $n - 1$). Then each $Q(x_i)^2 = R(x_i)$ so we have $2n$ pairs $(x_i, \pm Q(x_i))$ of rational points on the curve $Y^2 = R(X)$ of $g < n/2$.

Likewise

$$\prod_{i=1}^{4} (X^n - x_i^n) = Q(X^n)^2 - (R_1 X^n + R_0),$$

so if $n = 2g+2$ and $F \supset \boldsymbol{\mu}_n$ then $Y^2 = R_1 X^n + R_0$ has $16(g+1)$ points $(\zeta x_i, \pm Q(x_i^n))$ with $1 \leq i \leq 4$ and $\zeta^n = 1$ (though in only four $\mathrm{Aut}(C)$ orbits).

For all but finitely many g, these constructions and variations [to be detailed in the paper] are still the best lower bounds known on $B(g, \mathbf{Q})$ and $N(g)$.

For example, here is a table of current lower bounds on $N(g)$. "Method" line: "BM" for the Brumer-Mestre $16(g+1)$ bound; "T", other Twists of a fixed curve with many symmetries; "F", other (non-isotrivial) Families of highly symmetric curves; "L", curves obtained by slicing surfaces with many Lines.

g	2	3	4	5	6	7	8	9	10	45	other
$N(g) \geq$	150	100	126	132	146	128	144	180	192	781	$16(g+1)$
Method	L	T	F	T	L	BM	BM	L	T	L	BM

For the sake of time, and to give context for new $g = 2, 3$ results, the rest of this talk concerns the Line method, relegating the others (which often attain large $\#C(F)$ but few $\mathrm{Aut}(C)$ orbits) to the eventual conference paper.

For all but finitely many g, these constructions and variations [to be detailed in the paper] are still the best lower bounds known on $B(g, \mathbf{Q})$ and $N(g)$.

For example, here is a table of current lower bounds on $N(g)$. "Method" line: "BM" for the Brumer-Mestre $16(g+1)$ bound; "T", other Twists of a fixed curve with many symmetries; "F", other (non-isotrivial) Families of highly symmetric curves; "L", curves obtained by slicing surfaces with many Lines.

g	2	3	4	5	6	7	8	9	10	45	other
$N(g) \geq$	150	100	126	132	146	128	144	180	192	781	$16(g+1)$
Method	L	T	F	T	L	BM	BM	L	T	L	BM

For the sake of time, and to give context for new $g = 2, 3$ results, the rest of this talk concerns the Line method, relegating the others (which often attain large $\#C(F)$ but few $\mathrm{Aut}(C)$ orbits) to the eventual conference paper.

Idea: use geometry of the surface $\mathcal{C}$.

Harris suggested many years ago: construct infinitely many curves with many points by using geometry of surfaces directly.

Paradigmatic example: if smooth degree-d surface $S \in \mathbf{P}^3$ has n lines over F, generic plane section is a smooth curve of degree d (so $g = (d-1)(d-2)/2$) with n rational points. Hence $N(g) \geq n$.

The idea has many variations, e.g. use rational points off the n lines to increment $N(g)$, or to decrement g (intersection of S with a tangent plane has a node).

This connects our questions on $N(g)$ etc. with a classical problem in algebraic geometry: given $d > 3$, how big can n be? Also arithmetic geometry: find big n for F fixed, notably $F = \mathbf{Q}$.

Natural guess: Fermat surface $X^d + Y^d + Z^d + T^d = 0$. It has $3d^2$ lines over $\mathbf{C}$, and thus over some finite extension F_d of $\mathbf{Q}$: d^2 factorizations of each of

$$X^d + Y^d = Z^d + T^d = 0,$$
$$X^d + Z^d = T^d + Y^d = 0,$$
$$X^d + T^d = Y^d + Z^d = 0.$$

This gives "only" $6g + O(g^{1/2})$ points, and not for all g (only $3, 6, 10, \ldots$); but $\mathrm{Aut}(C)$ is usually trivial.

This $3d^2$ is the best known for all but a few d; but the true maximum is not yet known except for $d = 4$, when it is not $48 (= 3 \cdot 4^2)$ but 64, for $X^4 + XY^3 = Z^4 + ZT^3$ (Schur 1882: each side has the same tetrahedral rather than dihedral symmetry). This is maximal (~~Segre 1943~~ Rams–Schütt 2012).

Natural guess: Fermat surface $X^d + Y^d + Z^d + T^d = 0$. It has $3d^2$ lines over $\mathbf{C}$, and thus over some finite extension F_d of $\mathbf{Q}$: d^2 factorizations of each of

$$X^d + Y^d = Z^d + T^d = 0,$$
$$X^d + Z^d = T^d + Y^d = 0,$$
$$X^d + T^d = Y^d + Z^d = 0.$$

This gives "only" $6g + O(g^{1/2})$ points, and not for all g (only $3, 6, 10, \ldots$); but $\mathrm{Aut}(C)$ is usually trivial.

This $3d^2$ is the best known for all but a few d; but the true maximum is not yet known except for $d = 4$, when it is not $48 (= 3 \cdot 4^2)$ but 64, for $X^4 + XY^3 = Z^4 + ZT^3$ (Schur 1882: each side has the same tetrahedral rather than dihedral symmetry). This is maximal (~~Segre 1943~~ Rams–Schütt 2012).

Likewise $P_6(X,Y)+P_6(Z,T)=0$ and $P_8(X,Y)+P_8(Z,T)=0$ with octahedral symmetry, $P_{12}(X,Y) + P_{12}(Z,T) = 0$ and $P_{20}(X,Y) + P_{20}(Z,T) = 0$ with icosahedral symmetry. (The record is $3d^2$ for all $d > 2$ other than $4, 6, 8, 12, 20$.) For $d = 12$, each line meets 781 others so $N(45) \geq 781$.

But each of these records is over some F_d that is never just $\mathbf{Q}$. How well can we do over $\mathbf{Q}$?

Here even the case $d = 4$ is open; current record: a tie at 46.

The K3 (and -163) connection

A smooth quartic is a K3 surface — an analogue for surfaces of $g = 1$ for curves (“between” rational and general type), and just tractable enough for this kind of application (and also for elliptic curves of high rank, “etc.”).

Recall that the points of a $g = 1$ curve have a kind of group structure. The *curves* on a surface $\mathcal{X}$ have one too, the Néron-Severi group $\mathrm{NS}(\mathcal{X})$. Intersection theory gives $\mathrm{NS}(\mathcal{X})$ the structure of a lattice in some hyperbolic space with signature $(1, \rho - 1)$. For a K3 surface, the lattice is even with $\rho \leq 20$. If $\rho = 20$ and $\mathrm{NS}(\mathcal{X}) = \mathrm{NS}_{\mathbf{Q}}(\mathcal{X})$ then the lattice discriminant is one of the 13 discriminants of quadratic orders with $h = 1$:

$$-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

For each of those 13 choices

$$\Delta = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163$$

there is a unique $\mathcal{X}$ with $(\rho, \text{disc}) = (20, \Delta)$ over $\mathbf{Q}$.

Quartic model $\longleftrightarrow$ choice of $H \in \text{NS}$ with $(H, H) = 4$, up to equivalence $\longleftrightarrow$ even lattice L of rank 19, disc. $4|\Delta|$ (with one further condition on L^*/L if Δ not squarefree). Smooth: no vector of norm 2. Then lines $\longleftrightarrow$ $\pm$ pairs of dual vectors of norm 9/4. There are literally thousands of choices; the first picture shows the unique one with $n = 46$.

The $g = 2$ setup: Let $P(X,Y,Z)$ be a homogeneous sextic such that the curve $S : P = 0$ is not too singular, and consider

$$\mathcal{X} : T^2 = P(X,Y,Z),$$

the double cover of the plane branched on S.

Pairs of “lines” $\Longleftrightarrow$ lines l_i in the plane on which P restricts to a perfect square; geometrically, l_i is tritangent to S (with allowances made for double points, etc.). Each yields a pair of points on the genus-2 curve obtained by restricting to a random line l in the plane. In NS: line $\Longleftrightarrow$ L^* vector of norm 5/2 modulo $R(L)$, with disc$(L) = 2|\Delta|$ and $R(L) =$ span of norm-2 vectors $\longleftrightarrow$ singularities of S.

So, how many tritangents can such a curve have?

Again an open question. For $\mathbb{C}$, probably 72 (for S invariant under Jordan’s “Hessian” group = Weil rep’n on $\mathbb{C}^3$). But for ANTS let me concentrate on $\mathbb{Q}$ . . .

The $g = 2$ setup: Let $P(X, Y, Z)$ be a homogeneous sextic such that the curve $S : P = 0$ is not too singular, and consider

$$\mathcal{X} : T^2 = P(X, Y, Z),$$

the double cover of the plane branched on S.

Pairs of "lines" $\Longleftrightarrow$ lines l_i in the plane on which P restricts to a perfect square; geometrically, l_i is tritangent to S (with allowances made for double points, etc.). Each yields a pair of points on the genus-2 curve obtained by restricting to a random line l in the plane. In NS: line $\Longleftrightarrow$ L^* vector of norm 5/2 modulo $R(L)$, with disc$(L) = 2|\Delta|$ and $R(L) =$ span of norm-2 vectors $\longleftrightarrow$ singularities of S.

So, how many tritangents can such a curve have?

Again an open question. For $\mathbf{C}$, probably 72 (for S invariant under Jordan's "Hessian" group = Weil rep'n on $\mathbf{C}^3$). But for ANTS let me concentrate on $\mathbf{Q}$ . . .

The $g = 2$ setup: Let $P(X, Y, Z)$ be a homogeneous sextic such that the curve $S : P = 0$ is not too singular, and consider

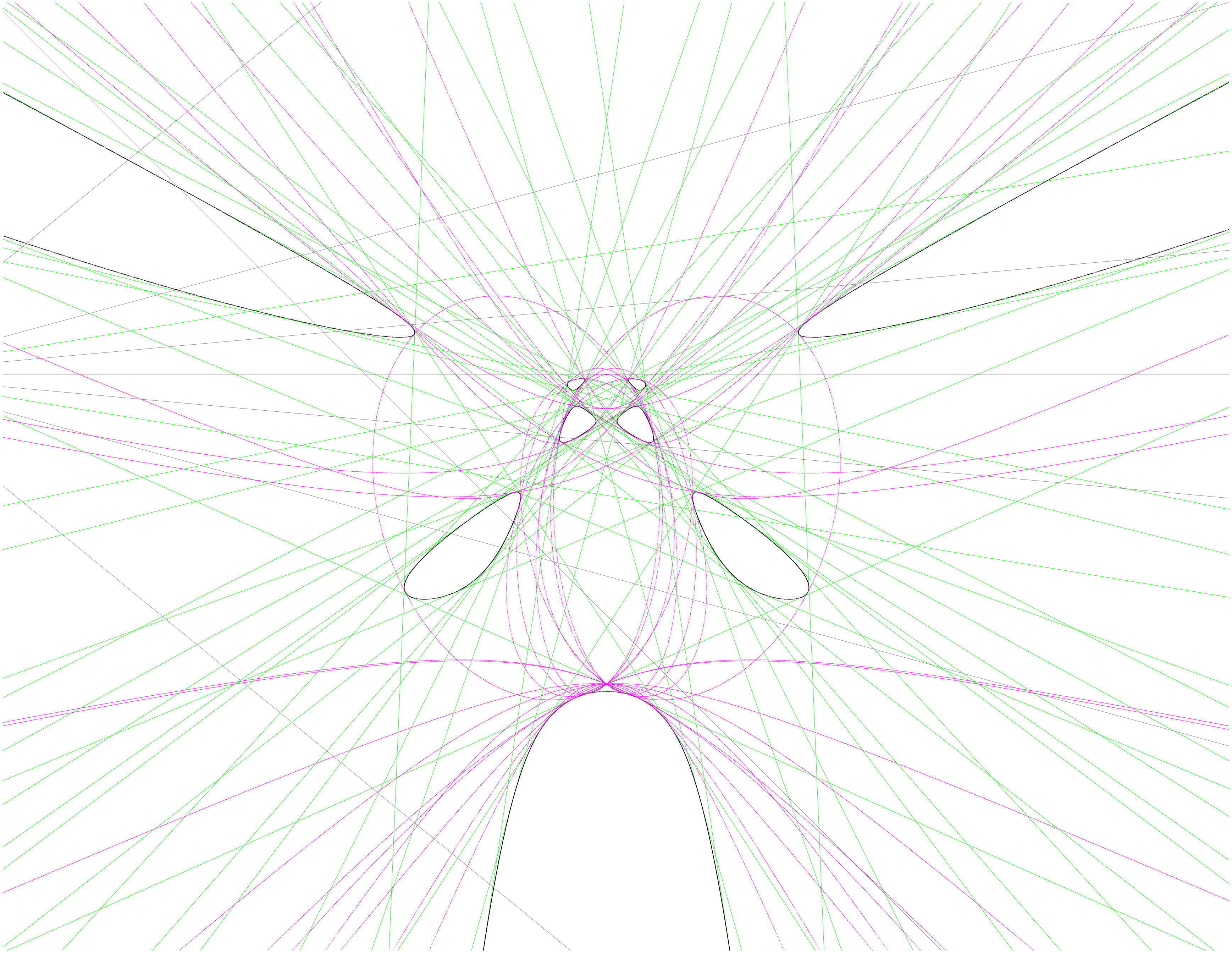
$$\mathcal{X} : T^2 = P(X, Y, Z),$$

the double cover of the plane branched on S.

Pairs of "lines" $\Longleftrightarrow$ lines l_i in the plane on which P restricts to a perfect square; geometrically, l_i is tritangent to S (with allowances made for double points, etc.). Each yields a pair of points on the genus-2 curve obtained by restricting to a random line l in the plane. In NS: line $\Longleftrightarrow$ L^* vector of norm 5/2 modulo $R(L)$, with disc$(L) = 2|\Delta|$ and $R(L) =$ span of norm-2 vectors $\longleftrightarrow$ singularities of S.

So, how many tritangents can such a curve have?

Again an open question. For $\mathbf{C}$, probably 72 (for S invariant under Jordan's "Hessian" group = Weil rep'n on $\mathbf{C}^3$). But for ANTS let me concentrate on $\mathbf{Q}$ . . .



The "Rorschach test" shows one of five examples with minimal $R(L)$ (just one node) and $n \in [52, 54]$ such tritangents (allowing intersection with the double point as "tangency"), and the only one with bilateral symmetry. The restriction to a generic line l yields a curve of genus 2 with at least n pairs of rational points and no symmetry beyond the automatic $(x, y) \leftrightarrow (x, -y)$. That was a new record for $N(2, \mathbf{Q})$ by a large margin.

You might have noticed that our construction doesn't quite fit in the $\mathcal{C} \xrightarrow{\pi} \mathbf{P}^1$ picture: we started with a K3 surface (dimension 2), but somehow got a 2-parameter family of curves, one for each line l.

But it works exactly if we require l to go through a point P_0 on the plane, and then every other point is on a unique l.

Some choices of P_0 raise our $N(2)$ bound well beyond $2 \cdot 54$, thanks to the purple conics. . .

The “Rorschach test” shows one of five examples with minimal $R(L)$ (just one node) and $n \in [52, 54]$ such tritangents (allowing intersection with the double point as “tangency”), and the only one with bilateral symmetry. The restriction to a generic line l yields a curve of genus 2 with at least n pairs of rational points and no symmetry beyond the automatic $(x, y) \leftrightarrow (x, -y)$. That was a new record for $N(2, \mathbf{Q})$ by a large margin.

You might have noticed that our construction doesn’t quite fit in the $\mathcal{C} \overset{\pi}{\to} \mathbf{P}^1$ picture: we started with a K3 surface (dimension 2), but somehow got a 2-parameter family of curves, one for each line l.

But it works exactly if we require l to go through a point P_0 on the plane, and then every other point is on a unique l.

Some choices of P_0 raise our $N(2)$ bound well beyond $2 \cdot 54$, thanks to the purple conics. . .

The K3 theory promises 1000+ conics c on which the sextic $P(X,Y,Z)$ is a perfect square (geometrically, the 12 intersections of c with S pair up into six tangency points). It happens that 18 of those go through a point that lies on only two of the l_i. Using that point as our P_0, we sacrifice one point-pair but gain at least 18 others.

With some further fiddling we find two more, and can force another four using two other conics. At the end we find $N(2) \geq 2 \cdot 75 = 150$, the current record.

Some of these curves have many more points; I found one with at least $2 \cdot 268 = 536$. This already beat Stahlke's record for a genus-2 curve with minimal automorphism group. Later Stoll searched more extensively, finding a number of examples with even more points, some even beyond the $12 \cdot 49 = 588$ of Keller and Kulesz; his current record curve (2008–9) has at least $642 = 2 \cdot 321$ points. (Can the list be proved complete!?)

The K3 theory promises 1000+ conics c on which the sextic $P(X,Y,Z)$ is a perfect square (geometrically, the 12 intersections of c with S pair up into six tangency points). It happens that 18 of those go through a point that lies on only two of the l_i. Using that point as our P_0, we sacrifice one point-pair but gain at least 18 others.

With some further fiddling we find two more, and can force another four using two other conics. At the end we find $N(2) \geq 2 \cdot 75 = 150$, the current record.

Some of these curves have many more points; I found one with at least $2 \cdot 268 = 536$. This already beat Stahlke's record for a genus-2 curve with minimal automorphism group. Later Stoll searched more extensively, finding a number of examples with even more points, some even beyond the $12 \cdot 49 = 588$ of Keller and Kulesz; his current record curve (2008–9) has at least $642 = 2 \cdot 321$ points. (Can the list be proved complete!?)

The K3 theory promises 1000+ conics c on which the sextic $P(X,Y,Z)$ is a perfect square (geometrically, the 12 intersections of c with S pair up into six tangency points). It happens that 18 of those go through a point that lies on only two of the l_i. Using that point as our P_0, we sacrifice one point-pair but gain at least 18 others.

With some further fiddling we find two more, and can force another four using two other conics. At the end we find $N(2) \geq 2 \cdot 75 = 150$, the current record.

Some of these curves have many more points; I found one with at least $2 \cdot 268 = 536$. This already beat Stahlke's record for a genus-2 curve with minimal automorphism group. Later Stoll searched more extensively, finding a number of examples with even more points, some even beyond the $12 \cdot 49 = 588$ of Keller and Kulesz; his current record curve (2008–9) has at least $642 = 2 \cdot 321$ points. (Can the list be proved complete!?)

In case you haven't seen this curve yet . . .

$$y^2 = P(x) := 82342800\,x^6 - 470135160\,x^5 + 52485681\,x^4 + 2396040466\,x^3 + 567207969\,x^2 - 985905640\,x + 15740^2,$$

with P having no repeated roots, has (at least) $2 \cdot 321 = 642$ rational solutions, in pairs $(x, \pm y)$ with x equal

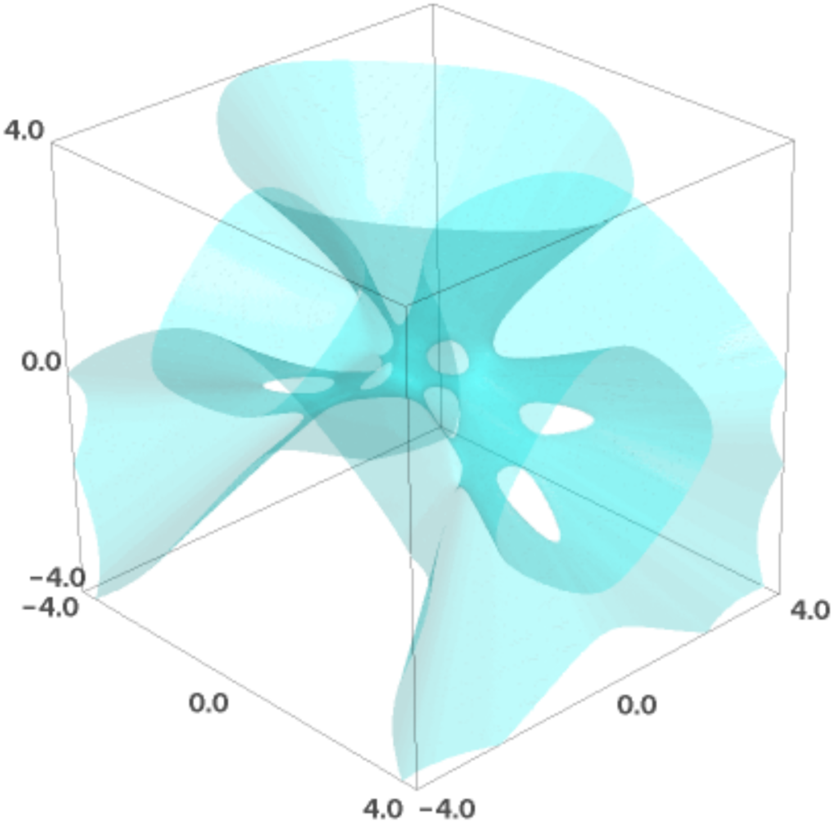
0, −1, −4, 4, 5, 6, 1/3, −5/3, −3/5, 7/4, . . . , 12027943/13799424,
−71658936/86391295, 148596731/35675865,
58018579/158830656, 208346440/37486601,
−1455780835/761431834, −3898675687/2462651894

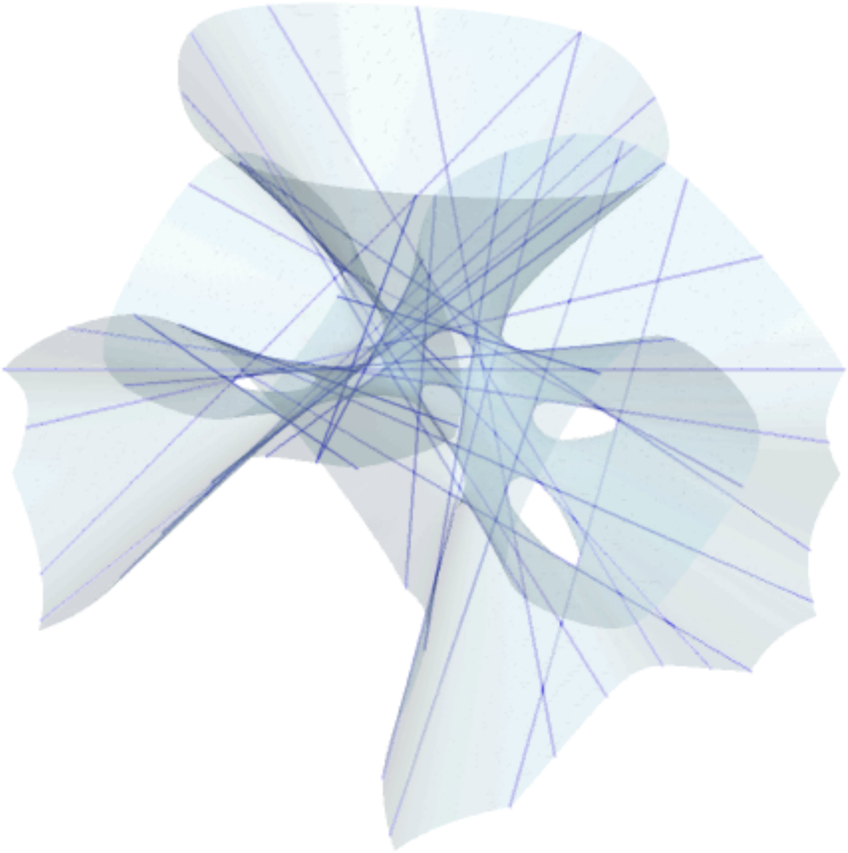
. . . now you have.

Similar tricks starting with the 46-line quartic yield infinitely many $g = 3$ curves C with $\#(C/\mathbf{Q}) \geq 64$.

Again can search for special planes that intersect $\mathcal{X}$ in a smooth quartic with even more points. Current strategy: find all $\mathcal{X}(\mathbf{Q})$ points of height at most H (i.e. $(x : y : z : t)$ with $x, y, z, t \in \mathbf{Z}$ all in $[-H, H]$) that are not on any of the n lines on $\mathcal{X}$; find all coplanar quadruples of height at most H_0; for each one that has a few more point in the list up to height H, search further (using p-adic version of technique introduced at ANTS-IV).

Repeat with $\mathcal{X}$ replaced by runners-up such as this quartic with 42 lines (30 "in the frame"):


4.0
0.0
−4.0
−4.0
0.0
4.0
−4.0
0.0
4.0



Current records for $g = 3$:

Quartic curve with $\operatorname{Aut}(C) = 1$: at least 108 points on

$$(-8140y + 5970z)x^3 + (-8022y^2 - 4983zy + 16372z^2)x^2 \\ + (-930y^3 - 19287zy^2 + 40107z^2y + 1922z^3)x \\ + 572y^4 - 8712zy^3 + 17885z^2y^2 + 10838z^3y - 23712z^4 = 0.$$

Quartic with involution from $\mathcal{X}$: at least $144 = 2 \cdot 72$ pts. on

$$4x^2 - (37y^2 + 67zy + 13586z^2)x + 9y^4 \\ + 4383zy^3 + 75814z^2y^2 - 1819700z^3y - 12562100z^4 = 0.$$

Hyperelliptic curve with $\#\operatorname{Aut} = 2$, from double $\mathbf{P}^1 \times \mathbf{P}^1$: at least $176 = 2 \cdot 88$ points, tying Keller-Kulesz record of $11 \cdot 16$ for $B(3, \mathbf{Q})$, on

$$Y^2 = 76X^8 + 671X^7 - 8539X^6 - 89512X^5 + 147851X^4 \\ + 3076727X^3 + 6159667X^2 - 3720486X - 3527271.$$

P.S. How to find equations such as

$$-76c^4 + 52c^3d - 68c^2d^2 - 52cd^3 + (167c^2 + 2cd + 75d^2)a^2 \\ + (77c^2 + 98cd - 3d^2)b^2 - 100a^4 + 29a^2b^2 - b^4 = 0$$

for the 46-line quartic surface?

Well, it's determined uniquely by more equations than variables (-163 and all that), and rational points on a zero-dimensional variety are easy.

In theory. . .

[But that's another talk.]

P.S. How to find equations such as

$$-76c^4 + 52c^3d - 68c^2d^2 - 52cd^3 + (167c^2 + 2cd + 75d^2)a^2 \\ + (77c^2 + 98cd - 3d^2)b^2 - 100a^4 + 29a^2b^2 - b^4 = 0$$

for the 46-line quartic surface?

Well, it's determined uniquely by more equations than variables (-163 and all that), and rational points on a zero-dimensional variety are easy.

In theory. . .

[But that's another talk.]

Further questions etc.:

Better search strategy? Having found a family of genus-g curves C with N rational points, still a nontrivial computational problem to efficiently find good candidates for curves in the family with $\#C(\mathbf{Q})$ much above N.

Jacobian ranks? These families with $\mathrm{Aut}(C) = \{1\}$ or $\{1, \iota\}$ are also good candidates for record ranks of simple Jacobians $J_C(\mathbf{Q})$; e.g. $r \geq 29$ for

$$\begin{aligned} Y^2 = {} & 3115323179136X^6 + 13377846720672X^5 \\ & + 2083591459177X^4 - 31185870903704X^3 \\ & + 3365838909904X^2 + 11170486506240X + 1337760^2, \end{aligned}$$

and $r \geq 31$ for

$$\begin{aligned} Y^2 = {} & 3690^2X^8 + 136193480460X^7 + 855554427369X^6 \\ & - 97341477968X^5 + 8046400145942X^4 + 7241370511844X^3 \\ & + 2187498173777X^2 + 273643583472X + 110152^2, \end{aligned}$$

in each case generated by points of height $< 10^3$.

Further questions etc.:

Better search strategy? Having found a family of genus-g curves C with N rational points, still a nontrivial computational problem to efficiently find good candidates for curves in the family with $\#C(\mathbf{Q})$ much above N.

Jacobian ranks? These families with $\mathrm{Aut}(C) = \{1\}$ or $\{1, \iota\}$ are also good candidates for record ranks of simple Jacobians $J_C(\mathbf{Q})$; e.g. $r \geq 29$ for

$$\begin{aligned} Y^2 = {} & 3115323179136X^6 + 13377846720672X^5 \\ & + 2083591459177X^4 - 31185870903704X^3 \\ & + 3365838909904X^2 + 11170486506240X + 1337760^2, \end{aligned}$$

and $r \geq 31$ for

$$\begin{aligned} Y^2 = {} & 3690^2X^8 + 136193480460X^7 + 855554427369X^6 \\ & - 973414777968X^5 + 8046400145942X^4 + 7241370511844X^3 \\ & + 2187498173777X^2 + 273643583472X + 110152^2, \end{aligned}$$

in each case generated by points of height $< 10^3$.

(Why "simple"? Reducible Jacobians may be unfair competition, e.g. $r = 38$ for $g = 2$ from $E(\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z}) \oplus \mathbf{Z}^{19}$.)

Genus 4 and beyond? As g grows, so do the lower bounds on $B(g, \mathbf{Q})$ and $N(g)$, with either the elementary Brumer-Mestre approach or via K3's; but B-M et al. are faster. Already for $g = 4$, I don't know better than 126 (for any of $N(4)$, $N(4, \mathbf{Q})$, $B(4, \mathbf{Q})$!). But that's with big Aut(C), so probably still some small-Aut(C) records to be found.

If you have any constructions, curves, references, suggestions, etc. to add, please tell me!

THANK YOU

(Why "simple"? Reducible Jacobians may be unfair competition, e.g. $r = 38$ for $g = 2$ from $E(\mathbf{Q}) \cong (\mathbf{Z}/2\mathbf{Z}) \oplus \mathbf{Z}^{19}$.)

Genus 4 and beyond? As g grows, so do the lower bounds on $B(g, \mathbf{Q})$ and $N(g)$, with either the elementary Brumer-Mestre approach or via K3's; but B-M et al. are faster. Already for $g = 4$, I don't know better than 126 (for any of $N(4)$, $N(4, \mathbf{Q})$, $B(4, \mathbf{Q})$!). But that's with big Aut(C), so probably still some small-Aut(C) records to be found.

If you have any constructions, curves, references, suggestions, etc. to add, please tell me!

THANK YOU