Low-genus curves over finite fields: Problems and variations

Everett W. Howe

Center for Communications Research, La Jolla

IPAM workshop on Number Theory and Cryptography
9–13 October 2006

A basic problem for elliptic curves

The elliptic curve construction problem

Given

- n — *an integer*
- q — *a prime power*

find (*if possible*) *an elliptic curve* $E/\mathbb{F}_q$ *with* $\#E(\mathbb{F}_q) = n$.

Most of this talk:
Generalizations and variants of this problem.

The elliptic curve existence problem

'If possible' part is easy (Deuring, Honda-Tate, Waterhouse).

Set $t = q + 1 - n$, and say q is a power of prime p.

The values of t coming from elliptic curves:

- Every t with $(t, q) = 1$ and $t^2 < 4q$.
- If q is not a square: $\mathbb{Z} \cap \{0, \pm\sqrt{2q}, \pm\sqrt{3q}\}$.
- If q is a square: $\pm 2\sqrt{q}$,

$$\pm\sqrt{q} \quad (\text{if } p \not\equiv 1 \bmod 3),$$

$$0 \quad (\text{if } p \not\equiv 1 \bmod 4).$$

Solutions to the elliptic curve construction problem

The naïve solution

Given q and n,

1. Make sure n is an allowed value.
2. Pick an elliptic curve $E/\mathbb{F}_q$ at random.
3. Check whether $\#E(\mathbb{F}_q) = n$.
4. Repeat steps 2 and 3 until successful.

Run time is $\widetilde{O}(q/\sqrt{4q - t^2})$.

Average run time is $\widetilde{O}(\sqrt{q})$.

Less-naïve solutions

The CM method (for ordinary curves)

Given q and an allowable n,

1. Compute the Hilbert class polynomial $f \in \mathbb{Z}[x]$ of the discriminant $\Delta := t^2 - 4q$.
2. Find a root j of f over $\mathbb{F}_q$.
3. Compute the E's having this root as j-invariant.

Running time is $\widetilde{O}(|\Delta|)$, average running time is $\widetilde{O}(q)$.

Combined solution

If $|\Delta| > q^{2/3}$ use naïve method, otherwise use CM method.

Running time is $\widetilde{O}(q^{2/3})$.

Less-naïve solutions

The CM method (for ordinary curves)

Given q and an allowable n,

1. Compute the Hilbert class polynomial $f \in \mathbb{Z}[x]$ of the discriminant $\Delta := t^2 - 4q$.
2. Find a root j of f over $\mathbb{F}_q$.
3. Compute the E's having this root as j-invariant.

Running time is $\widetilde{O}(|\Delta|)$, average running time is $\widetilde{O}(q)$.

Combined solution

If $|\Delta| > q^{2/3}$ use naïve method, otherwise use CM method.

Running time is $\widetilde{O}(q^{2/3})$.

The Bröker-Stevenhagen approach

Bröker-Stevenhagen: Change question to get better answer.

Problem

Given $n > 0$, find a q and an $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = n$.

Expect to be able to choose q so that

$$\Delta := t^2 - 4q = f^2\Delta_0$$

for a fundamental discriminant Δ_0 of size $O(\log^2 n)$.

Compute Hilbert class polynomial for Δ_0 instead of for Δ.

The Bröker-Stevenhagen approach

Bröker-Stevenhagen: Change question to get better answer.

Problem

Given $n > 0$, find a q and an $E/\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = n$.

Expect to be able to choose q so that

$$\Delta := t^2 - 4q = f^2\Delta_0$$

for a fundamental discriminant Δ_0 of size $O(\log^2 n)$.

Compute Hilbert class polynomial for Δ_0 instead of for Δ.

Generalizations to higher genus

Want to generalize the construction problem to higher genus.
But what was the question, exactly?

Problem

Given n and q, find a genus-1 curve $E/\mathbb{F}_q$ with

$$\#E(\mathbb{F}_q) = n.$$

Generalizations to higher genus

Want to generalize the construction problem to higher genus.
But what was the question, exactly?

Problem

Given n and q, find a genus-1 curve $E/\mathbb{F}_q$ with

$$\#(\operatorname{Jac} E)(\mathbb{F}_q) = n.$$

Generalizations to higher genus

Want to generalize the construction problem to higher genus.
But what was the question, exactly?

Problem

Given n and q, find a genus-1 curve $E/\mathbb{F}_q$ with

$$\textit{Weil polynomial of } E/\mathbb{F}_q = x^2 - tx + q, \quad \textit{where } t = q + 1 - n.$$

Generalizations to higher genus

Want to generalize the construction problem to higher genus.
But what was the question, exactly?

Problem

Given n and q, find a genus-1 curve $E/\mathbb{F}_q$ with

$$\text{Weil polynomial of } E/\mathbb{F}_q = x^2 - tx + q, \quad \text{where } t = q + 1 - n.$$

None of these possibilities gets any easier for higher genus!

The naïve method for higher genus

Average running times for naïve methods

genus	Time to find C with specified value of... $\#C(\mathbb{F}_q)$	$\#(\mathrm{Jac}\,C)(\mathbb{F}_q)$	Weil polynomial
1	$q^{1/2}$	$q^{1/2}$	$q^{1/2}$
2	$q^{1/2}$	$q^{3/2}$	$q^{3/2}$
3	$q^{1/2}$	$q^{5/2}$	q^{3}

The genus-2 CM method

Kristin Lauter spoke about the genus-2 CM method.

To estimate complexity, we need to know how big the Igusa class polynomials will be.

$$\begin{aligned} \text{Degree} &\sim \text{minus class number of reflex field} \\ &\sim \widetilde{O}(q^{3/2}) \qquad \text{in general} \end{aligned}$$

As in EC case, degree is like complexity of naïve method.
Size of coefficients — $\widetilde{O}(q^3)$?? — just makes things worse.

Can we do a Bröker-Stevenhagen trick?

The genus-2 CM method

Kristin Lauter spoke about the genus-2 CM method.

To estimate complexity, we need to know how big the Igusa class polynomials will be.

$$\begin{aligned} \text{Degree} &\sim \text{minus class number of reflex field} \\ &\sim \widetilde{O}(q^{3/2}) \quad \text{in general} \end{aligned}$$

As in EC case, degree is like complexity of naïve method.
Size of coefficients — $\widetilde{O}(q^3)$?? — just makes things worse.

Can we do a Bröker-Stevenhagen trick?

The genus-2 CM method

Kristin Lauter spoke about the genus-2 CM method.

To estimate complexity, we need to know how big the Igusa class polynomials will be.

$$\begin{aligned} \text{Degree} &\sim \text{minus class number of reflex field} \\ &\sim \widetilde{O}(q^{3/2}) \qquad \text{in general} \end{aligned}$$

As in EC case, degree is like complexity of naïve method.
Size of coefficients — $\widetilde{O}(q^3)$?? — just makes things worse.

Can we do a Bröker-Stevenhagen trick?

Genus-2 Bröker-Stevenhagen

Given n, there are $\sim n^{1/4}$ possible q's, each near $\sqrt{n}$.
For each q, at most five $f = x^4 + ax^3 + bx^2 + aqx + q^2$.

$$\begin{array}{ccc} K & \mathcal{O} & R = \mathbb{Z}[\pi, \overline{\pi}] \\ | & | & | \\ K^+ & \mathcal{O}^+ & R^+ = \mathbb{Z}[\pi + \overline{\pi}] \\ | & | & | \\ \mathbb{Q} & \mathbb{Z} & \mathbb{Z} \end{array}$$

$$\Delta_{\mathcal{O}}^- = N_{K^+/\mathbb{Q}}(\mathrm{disc}_{\mathcal{O}/\mathcal{O}^+})$$
$$\Delta_{\mathcal{O}}^+ = \mathrm{disc}_{\mathcal{O}^+/\mathbb{Z}}$$

$$\Delta_R^- = (b + 2q)^2 - 4a^2q$$
$$\Delta_R^+ = a^2 - 4b + 8q$$

Degree of Igusa polynomials grows like $h^-(K) \sim (\sqrt{\Delta_{\mathcal{O}}^- \Delta_{\mathcal{O}}^+})$.
Want large square factor in $\Delta_R^- \Delta_R^+$.

Genus-2 Bröker-Stevenhagen

Given n, there are $\sim n^{1/4}$ possible q's, each near $\sqrt{n}$.
For each q, at most five $f = x^4 + ax^3 + bx^2 + aqx + q^2$.

$$\begin{array}{ccc} K & \mathcal{O} & R = \mathbb{Z}[\pi, \overline{\pi}] \\ | & | & | \\ K^+ & \mathcal{O}^+ & R^+ = \mathbb{Z}[\pi + \overline{\pi}] \\ | & | & | \\ \mathbb{Q} & \mathbb{Z} & \mathbb{Z} \end{array}$$

$$\Delta_{\mathcal{O}}^- = N_{K^+/\mathbb{Q}}(\mathrm{disc}_{\mathcal{O}/\mathcal{O}^+})$$
$$\Delta_{\mathcal{O}}^+ = \mathrm{disc}_{\mathcal{O}^+/\mathbb{Z}}$$

$$\Delta_R^- = (b + 2q)^2 - 4a^2q$$
$$\Delta_R^+ = a^2 - 4b + 8q$$

Degree of Igusa polynomials grows like $h^-(K) \sim (\sqrt{\Delta_{\mathcal{O}}^- \Delta_{\mathcal{O}}^+})$.
Want large square factor in $\Delta_R^- \Delta_R^+$.

Genus-2 Bröker-Stevenhagen

Given n, there are $\sim n^{1/4}$ possible q's, each near $\sqrt{n}$.
For each q, at most five $f = x^4 + ax^3 + bx^2 + aqx + q^2$.

$$\begin{array}{ccc} K & \mathcal{O} & R = \mathbb{Z}[\pi, \overline{\pi}] \\ | & | & | \\ K^+ & \mathcal{O}^+ & R^+ = \mathbb{Z}[\pi + \overline{\pi}] \\ | & | & | \\ \mathbb{Q} & \mathbb{Z} & \mathbb{Z} \end{array}$$

$$\Delta_{\mathcal{O}}^- = N_{K^+/\mathbb{Q}}(\mathrm{disc}_{\mathcal{O}/\mathcal{O}^+})$$
$$\Delta_{\mathcal{O}}^+ = \mathrm{disc}_{\mathcal{O}^+/\mathbb{Z}}$$

$$\Delta_R^- = (b + 2q)^2 - 4a^2q$$
$$\Delta_R^+ = a^2 - 4b + 8q$$

Degree of Igusa polynomials grows like $h^-(K) \sim (\sqrt{\Delta_{\mathcal{O}}^- \Delta_{\mathcal{O}}^+})$.
Want large square factor in $\Delta_R^- \Delta_R^+$.

Heuristics for genus-2 Bröker-Stevenhagen

(From discussions with Lauter and Stevenhagen.)

View $\Delta_R^+\Delta_R^-$ as a random integer $\sim q^3 \approx n^{3/2}$.

What is largest square factor we expect in $n^{1/4}$ such integers?

Answer: f^2, where $f \approx n^{1/4}$.

Expect $\Delta_\mathcal{O}^+\Delta_\mathcal{O}^- \sim n$. Degree of Igusa polynomials $\sim \sqrt{n}$.

If coefficients $> n^{1/4}$ bits long, should use naïve method!

Easier open problems?

The elliptic curve construction problem is hard.

Generalizing to higher genus just made it harder.

What about trying to generalize something easier?

For instance, the elliptic curve existence problem.

Easier open problems?

The elliptic curve construction problem is hard.

Generalizing to higher genus just made it harder.

What about trying to generalize something easier?

For instance, the elliptic curve existence problem.

The genus-2 existence problem

Problem

Suppose $f = x^4 + ax^3 + bx^2 + aqx + q^2$ *is the Weil polynomial of an isogeny class of abelian surfaces. Does there exist a Jacobian with this Weil polynomial?*

To best of my knowledge, first posed in print by Rück (1990).

Note

The Honda-Tate theorem gives a simple criterion for deciding whether a polynomial is a Weil polynomial of an isogeny class.

Key to the genus-2 existence problem

A result of Weil

An abelian surface over $\overline{k}$ is a Jacobian if and only if it has an irreducible principal polarization.

Weil over finite fields

An abelian surface over $\mathbb{F}_q$ is a Jacobian of a curve over $\mathbb{F}_q$ if and only if it has a geometrically irreducible principal polarization.

Solution to the genus-2 existence problem

Recent solution (H.-Nart-Ritzenthaler), using Adleman-Huang, H., Lauter-Serre, Maisner, McGuire-Voloch, Rück, . . .

Suppose we're given a Weil polynomial of an isogeny class of abelian surfaces.

$$f = x^4 + ax^3 + bx^2 + aqx + q^2$$

If the surfaces are not simple, write

$$f = (x^2 - sx + q)(x^2 - tx + q) \qquad \text{with } |s| \geq |t|.$$

Solution to the genus-2 existence problem

Recent solution (H.-Nart-Ritzenthaler), using Adleman-Huang, H., Lauter-Serre, Maisner, McGuire-Voloch, Rück, ...

Suppose we're given a Weil polynomial of an isogeny class of abelian surfaces.

$$f = x^4 + ax^3 + bx^2 + aqx + q^2$$

If the surfaces are not simple, write

$$f = (x^2 - sx + q)(x^2 - tx + q) \qquad \text{with } |s| \geq |t|.$$

Non-existence of genus-2 split Jacobians

p-rank	Condition on p, q	Conditions on s, t
—	—	$\lvert s - t\rvert = 1$
2	—	$s = t$ and $4q - t^2 \in \{3, 4, 7\}$
	$q = 2$	$\lvert s\rvert = \lvert t\rvert = 1$ and $s \neq t$
1	$q = \square$	$s^2 = 4q$ and $s - t$ squarefree
0	$p > 3$	$s^2 \neq t^2$
	$p = 3$ and $q \neq \square$	$s^2 = t^2 = 3q$
	$p = 3$ and $q = \square$	$s - t$ not divisible by $3\sqrt{q}$
	$p = 2$	$s^2 - t^2$ not divisible by $2q$
	$q = 2$ or $q = 3$	$s = t$
	$q = 4$ or $q = 9$	$s^2 = t^2 = 4q$

Conditions that ensure no Jacobians in split isogeny class

Non-existence of genus-2 simple Jacobians

p-rank	Condition on p, q	Conditions on a, b
—	—	$a^2 - b = q$ and $b < 0$ and all prime divisors of b are 1 mod 3
2	—	$a = 0$ and $b = 1 - 2q$
	$p > 2$	$a = 0$ and $b = 2 - 2q$
0	$p \equiv 11 \bmod 12$ and $q = \square$	$a = 0$ and $b = -q$
	$p = 3$ and $q = \square$	$a = 0$ and $b = -q$
	$p = 2$ and $q \neq \square$	$a = 0$ and $b = -q$
	$q = 2$ or $q = 3$	$a = 0$ and $b = -2q$

Conditions that ensure no Jacobians in simple isogeny class

The genus-3 existence problem

Problem

Suppose f is the Weil polynomial of an isogeny class of abelian threefolds. Is there a Jacobian with this Weil polynomial?

A result of Oort and Ueno, after Hoyt

An abelian threefold over $\overline{k}$ is a Jacobian if and only if it has an irreducible principal polarization.

But. . .

The genus-3 existence problem

Problem

Suppose f is the Weil polynomial of an isogeny class of abelian threefolds. Is there a Jacobian with this Weil polynomial?

A result of Oort and Ueno, after Hoyt

An abelian threefold over $\overline{k}$ is a Jacobian if and only if it has an irreducible principal polarization.

But. . .

A complication over finite fields

Jacobians over $\mathbb{F}_q$ have geom. irreducible princ. pols, but. . .
A threefold with such a polarization over $\mathbb{F}_q$ is either a Jacobian or a *quadratic twist* of a Jacobian over $\mathbb{F}_q$.

Why?

If C is a nonhyperelliptic genus-3 curve over k, then

$$\operatorname{Aut}\operatorname{Jac}C \cong \{\pm 1\} \times \operatorname{Aut}C$$

$$H^1(\mathcal{G}_k, \operatorname{Aut}\operatorname{Jac}C) \leftrightarrow H^1(\mathcal{G}_k, \{\pm 1\}) \times H^1(\mathcal{G}_k, \operatorname{Aut}C)$$

$$\{\text{twists of } \operatorname{Jac}C\} \leftrightarrow \{\text{quad. extensions of } k\} \times \{\text{twists of } C\}$$

The upshot: Jacobians have more twists than do curves.

A complication over finite fields

Jacobians over $\mathbb{F}_q$ have geom. irreducible princ. pols, but...
A threefold with such a polarization over $\mathbb{F}_q$ is either a Jacobian or a *quadratic twist* of a Jacobian over $\mathbb{F}_q$.

Why?

If C is a nonhyperelliptic genus-3 curve over k, then

$$\operatorname{Aut}\operatorname{Jac}C \cong \{\pm 1\} \times \operatorname{Aut}C$$

$$H^1(\mathcal{G}_k, \operatorname{Aut}\operatorname{Jac}C) \leftrightarrow H^1(\mathcal{G}_k, \{\pm 1\}) \times H^1(\mathcal{G}_k, \operatorname{Aut}C)$$

$$\{\text{twists of } \operatorname{Jac}C\} \leftrightarrow \{\text{quad. extensions of } k\} \times \{\text{twists of } C\}$$

The upshot: Jacobians have more twists than do curves.

A half-open problem

Problem

Given a principally-polarized abelian threefold over a field k, determine whether or not it is a Jacobian over k.

A related question

How does one 'give' a principally-polarized abelian threefold?

A half-open problem

Problem

Given a principally-polarized abelian threefold over a field k, determine whether or not it is a Jacobian over k.

A related question

How does one ‘give’ a principally-polarized abelian threefold?

Two solutions, in progress

Steve Meagher (Groningen)

Explicit weight-18 modular form χ_{18} on $\mathcal{A}_{3,4}$. Divide by 36^{th} power of 0^{th} theta-null to get a modular function. Quadratic character of its value gives answer.

Christophe Ritzenthaler (Luminy)

Construct quadric in $\mathbb{P}^3$ from geometric data. Quadratic character of its determinant gives answer.

Two solutions, in progress

Steve Meagher (Groningen)

Explicit weight-18 modular form χ_{18} on $\mathcal{A}_{3,4}$. Divide by 36^{th} power of 0^{th} theta-null to get a modular function. Quadratic character of its value gives answer.

Christophe Ritzenthaler (Luminy)

Construct quadric in $\mathbb{P}^3$ from geometric data. Quadratic character of its determinant gives answer.

Can we use these solutions?

Given: Weil polynomial of isogeny class of abelian threefolds.

Say the threefolds are ordinary and absolutely simple.

Can understand the isogeny class, including polarizations, in terms of ‘Deligne modules’.

Problem

Can the Meagher or Ritzenthaler approaches be combined with the Deligne module description to determine whether there are Jacobians in the isogeny class?

Can we use these solutions?

Given: Weil polynomial of isogeny class of abelian threefolds.

Say the threefolds are ordinary and absolutely simple.

Can understand the isogeny class, including polarizations, in terms of ‘Deligne modules’.

Problem

Can the Meagher or Ritzenthaler approaches be combined with the Deligne module description to determine whether there are Jacobians in the isogeny class?

Something completely different. . .

I'll end with a few lattice questions inspired by a completely different topic.

Coding theorists ask:

How many points can a genus-g curve over $\mathbb{F}_q$ have?

Definition

$$N_q(g) = \max\{\#C(\mathbb{F}_q) : C \text{ is a genus-}g\text{ curve over } \mathbb{F}_q\}$$

Problem (silly, but open!)

For fixed q, is $N_q(g)$ an increasing function of g?

Something completely different. . .

I'll end with a few lattice questions inspired by a completely different topic.

Coding theorists ask:

How many points can a genus-g curve over $\mathbb{F}_q$ have?

Definition

$$N_q(g) = \max\{\#C(\mathbb{F}_q) : C \text{ is a genus-}g \text{ curve over } \mathbb{F}_q\}$$

Problem (silly, but open!)

For fixed q, is $N_q(g)$ an increasing function of g?

Tables of van der Geer and van der Vlugt

$g \setminus q$	2	4	8	16	32	64
1	5	9	14	25	44	81
2	6	10	18	33	53	97
3	7	14	24	38	64	113
4	8	15	25	45	71–74	129
5	9	17	29–30	49–53	83–85	132–145
6	10	20	33–35	65	86–96	161
7	10	21–22	34–38	63–69	98–107	177
8	11	21–24	35–42	62–75	97–118	169–193
9	12	26	45	72–81	108–128	209
10	13	27	42–49	81–87	113–139	225

A portion of the van der Geer-van der Vlugt tables of $N_q(g)$.

From curves to Hermitian forms (w/Kristin Lauter)

Can show:

Given a genus-7 curve $C/\mathbb{F}_4$ with 22 points, get matrix M:

- 3×3,
- entries in $\mathcal{O}_{-7} = \mathbb{Z}[(1+\sqrt{-7})/2]$,
- Hermitian,
- positive definite,
- determinant 3.

There's a Hermitian space over $\mathcal{O}_{-7}$ associated to M.

For every vector of squared-length $n > 0$ in this space, get a degree-n map $C \to E$ to an elliptic curve with 8 points.

Observation

If M has a vector of squared-length 2, then C doesn't exist!

From curves to Hermitian forms (w/Kristin Lauter)

Can show:

Given a genus-7 curve $C/\mathbb{F}_4$ with 22 points, get matrix M:

- 3×3,
- entries in $\mathcal{O}_{-7} = \mathbb{Z}[(1+\sqrt{-7})/2]$,
- Hermitian,
- positive definite,
- determinant 3.

There's a Hermitian space over $\mathcal{O}_{-7}$ associated to M.

For every vector of squared-length $n > 0$ in this space, get a degree-n map $C \to E$ to an elliptic curve with 8 points.

Observation

If M has a vector of squared-length 2, then C doesn't exist!

Computing with Hermitian matrices

With a small amount of computation, we can show:

Lemma

Every positive definite Hermitian $M \in M_3(\mathcal{O}_{-7})$ of determinant 3 has a vector of squared length 1 or 2.

Problem

Given an imaginary quadratic PID $\mathcal{O}$ and a determinant $d \in \mathbb{Z}$, find a sharp upper bound on length of short vectors in n-dimensional Hermitian spaces of determinant d over $\mathcal{O}$.

Can deal with small 3×3 cases and very small 4×4 cases.
Can deal with case when determinant is norm from $\mathcal{O}$.

Computing with Hermitian matrices

With a small amount of computation, we can show:

Lemma

Every positive definite Hermitian $M \in M_3(\mathcal{O}_{-7})$ of determinant 3 has a vector of squared length 1 or 2.

Problem

Given an imaginary quadratic PID $\mathcal{O}$ and a determinant $d \in \mathbb{Z}$, find a sharp upper bound on length of short vectors in n-dimensional Hermitian spaces of determinant d over $\mathcal{O}$.

Can deal with small 3×3 cases and very small 4×4 cases.
Can deal with case when determinant is norm from $\mathcal{O}$.

The end

Fin