Computing of abelian varieties over finite fields

Marseglia Stefano

Stockholm University

06 June 2018

PAPER I : Computing the ideal class monoid of an order

background in number theory

- A **number field** is a finite field extension of $\mathbb{Q}$.
  eg.
  $$\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f) \text{ where } f = x^3 + 10x^2 - 8,$$

- A **number field** is a finite field extension of $\mathbb{Q}$.
  eg.
  $$\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f) \text{ where } f = x^3 + 10x^2 - 8,$$

- An **order** is a subring of a finite product of number fields that has maximal $\mathbb{Z}$-rank.

- A **number field** is a finite field extension of $\mathbb{Q}$.
  eg.
  $$\mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f) \text{ where } f = x^3 + 10x^2 - 8,$$

- An **order** is a subring of a finite product of number fields that has maximal $\mathbb{Z}$-rank.
  eg.
  $$R = \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z},$$
  $$S = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \frac{\alpha^2}{2}\mathbb{Z},$$
  $$\mathcal{O} = \mathbb{Z} \oplus \frac{\alpha}{2}\mathbb{Z} \oplus \frac{\alpha^2}{4}\mathbb{Z}$$

- A **fractional** R**-ideal** I is a finitely generated sub-R-module of K such that $I \otimes \mathbb{Q} = K$

- A **fractional** R**-ideal** I is a finitely generated sub-R-module of K such that $I \otimes \mathbb{Q} = K$
  eg.

$$I = 3\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z} \oplus (\alpha^2 + 2)\mathbb{Z},$$

$$J = 3\mathbb{Z} \oplus (\alpha + 2)\mathbb{Z} \oplus \left(\frac{\alpha^2 + 2\alpha}{8}\right)\mathbb{Z},$$

also R, S and $\mathcal{O}$ are frac. R-ideals.

- A **fractional** R**-ideal** I is a finitely generated sub-R-module of K such that $I \otimes \mathbb{Q} = K$
  eg.

$$I = 3\mathbb{Z} \oplus (\alpha+2)\mathbb{Z} \oplus (\alpha^2+2)\mathbb{Z},$$

$$J = 3\mathbb{Z} \oplus (\alpha+2)\mathbb{Z} \oplus \left(\frac{\alpha^2+2\alpha}{8}\right)\mathbb{Z},$$

also R, S and $\mathcal{O}$ are frac. R-ideals.

- Two fractional R-ideals I and J are **isomorphic**

$$I \simeq_R J \Longleftrightarrow \exists x \in K^\times \text{ s.t. } xI = J$$

eg.

$$(\alpha^2+\alpha)J = I, \qquad I = (-17+18\alpha+2\alpha^2)R.$$

ICM: ideal class monoid

- Define the **ideal class monoid** of R as

$$\mathrm{ICM}(R) := {\{\text{fractional } R\text{-ideals}\}}\big/_{\simeq_R}$$

- Define the **ideal class monoid** of R as

$$\mathrm{ICM}(R) := {\{\text{fractional } R\text{-ideals}\}}\big/_{\simeq_R}$$

eg.

$$\mathrm{ICM}(R) = \{[R],[S],[\mathscr{O}],[S^t]\},$$

where

$$S^t = \mathbb{Z} \oplus \left(\frac{2+F}{4}\right)\mathbb{Z} \oplus \left(\frac{188-312F+F^2}{3784}\right)\mathbb{Z}$$

- A fractional R-ideal I is called **invertible** if there exists an R-ideal J such that

$$IJ = R.$$

ICM: ideal class monoid

- A fractional R-ideal I is called **invertible** if there exists an R-ideal J such that
$$IJ = R.$$

- Put
$$\mathrm{Pic}(R) := \frac{\left\{ \begin{array}{c} \text{invertible} \\ \text{fractional } R\text{-ideals} \end{array} \right\}}{\simeq_R}$$
it can be computed efficiently

- A fractional R-ideal I is called **invertible** if there exists an R-ideal J such that
$$IJ = R.$$

- Put
$$\mathrm{Pic}(R) := \frac{\left\{\begin{array}{c}\text{invertible}\\ \text{fractional } R\text{-ideals}\end{array}\right\}}{\simeq_R}$$
it can be computed efficiently

- We have
$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R)$$
with equality iff $R = \mathcal{O}_K$

ICM: ideal class monoid

- A fractional R-ideal I is called **invertible** if there exists an R-ideal J such that
$$IJ = R.$$

- Put
$$\operatorname{Pic}(R) := \frac{\left\{\begin{array}{c}\text{invertible}\\ \text{fractional } R\text{-ideals}\end{array}\right\}}{\simeq_R}$$
it can be computed efficiently

- We have
$$\operatorname{ICM}(R) \supseteq \operatorname{Pic}(R)$$
with equality iff $R = \mathcal{O}_K$

- ...and actually
$$\operatorname{ICM}(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathcal{O}_K \\ \text{over-orders}}} \operatorname{Pic}(S)$$
with equality iff R is Bass

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)
weak equivalence:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)
weak equivalence:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I)$$ easy to check!

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)
weak equivalence:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I) \quad \text{easy to check!}$$

Let $\mathscr{W}(R)$ be the set of weak eq. classes...

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)
weak equivalence:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I)$$ easy to check!

Let $\mathscr{W}(R)$ be the set of weak eq. classes...
...whose representatives can be found in

$$\left\{\text{sub-}R\text{-modules of } {}^{\mathcal{O}_K}\!/\!_{\mathfrak{f}_R}\right\}$$ finite! and most of the time not-too-big ...

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator rings:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathscr{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathrm{ICM}}(S)$$

Partition w.r.t. the multiplicator rings:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathscr{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathrm{ICM}}(S)$$

the "bar" means "only classes with multiplicator ring S"

Partition w.r.t. the multiplicator rings:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathscr{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathrm{ICM}}(S)$$

the "bar" means "only classes with multiplicator ring S"

Theorem (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\overline{\mathrm{ICM}(S)}$ and

$$\overline{\mathscr{W}}(S) = \overline{\mathrm{ICM}(S)} / \mathrm{Pic}(S)$$

Partition w.r.t. the multiplicator rings:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathscr{W}}(S)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \overline{\mathrm{ICM}}(S)$$

the "bar" means "only classes with multiplicator ring S"

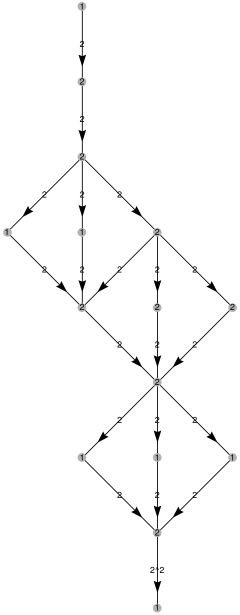
Theorem (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\overline{\mathrm{ICM}(S)}$ and

$$\overline{\mathscr{W}}(S) = \overline{\mathrm{ICM}(S)} / \mathrm{Pic}(S)$$

Repeat for every $R \subseteq S \subseteq \mathscr{O}_K$:

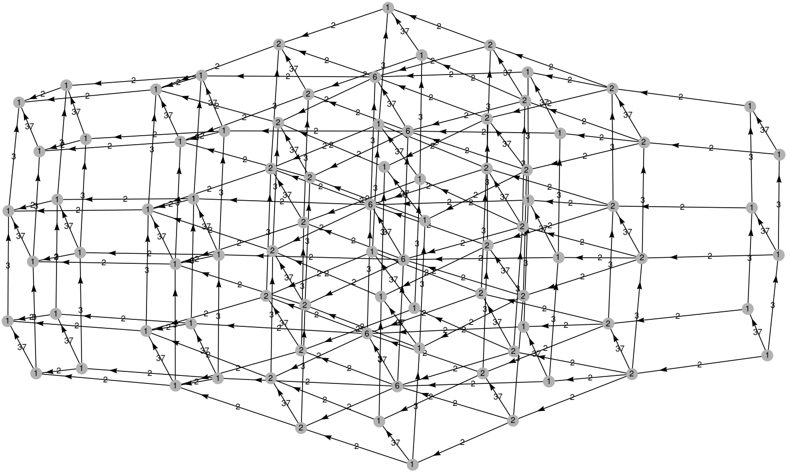
$$\rightsquigarrow \mathrm{ICM}(R).$$



Weak equivalence classes of the monogenic order of $\mathbb{Q}[x]/(f)$ where $f = x^3 + 31x^2 + 43x + 77$.

- vertices are orders, labeled by $\#\overline{\mathcal{W}}$
- edges are inclusions, labeled by the index

Example 2



Weak equivalence classes of the monogenic order of $\mathbb{Q}[x]/(f)$ where

$$f = (x^2 + 4x + 7)(x^3 - 9x^2 - 3x - 1).$$

PAPER II : Computing square-free polarized abelian varieties over finite fields

Fix a **ordinary square-free** characteristic q-Weil polynomial h.

$$\rightsquigarrow \text{an isogeny class } \mathscr{C}_h \text{ (by Honda-Tate).}$$

Put

$$K := \mathbb{Q}[x]/(h) \text{ and } F := x \bmod h.$$

Fix a **ordinary square-free** characteristic q-Weil polynomial h.

$$\rightsquigarrow \text{an isogeny class } \mathscr{C}_h \text{ (by Honda-Tate).}$$

Put

$$K := \mathbb{Q}[x]/(h) \text{ and } F := x \bmod h.$$

Theorem (M.)

$$\left\{\textit{Ordinary abelian varieties over } \mathbb{F}_q \textit{ in } \mathscr{C}_h\right\}_{/\simeq}$$

$$\updownarrow$$

$$\left\{\textit{fractional ideals of } \mathbb{Z}[F,q/F] \subset K\right\}_{/\simeq} \qquad =: \mathrm{ICM}(\mathbb{Z}[F,q/F])$$

ideal class monoid

Fix a **ordinary square-free** characteristic q-Weil polynomial h.

$$\rightsquigarrow \text{an isogeny class } \mathscr{C}_h \text{ (by Honda-Tate).}$$

Put

$$K := \mathbb{Q}[x]/(h) \text{ and } F := x \bmod h.$$

Theorem (M.)

$$\left\{ \textit{Ordinary abelian varieties over } \mathbb{F}_q \textit{ in } \mathscr{C}_h \right\}_{/\simeq}$$

$$\updownarrow$$

$$\left\{ \textit{fractional ideals of } \mathbb{Z}[F,q/F] \subset K \right\}_{/\simeq} \qquad =: \mathrm{ICM}(\mathbb{Z}[F,q/F])$$

ideal class monoid

Also **polarizations** can be described in terms of fractional ideals!

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$;
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4;
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$;
- 8 over-orders of R: two of them are not Gorenstein;
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class;
- 5 are not invertible in their multiplicator ring;
- 8 classes admit principal polarizations;
- 10 isomorphism classes of princ. polarized AV.

Concretely:

$$
\begin{aligned}
I_1 = & 2645633792595191\mathbb{Z} \oplus (F + 836920075614551)\mathbb{Z} \oplus (F^2 + 1474295643839839)\mathbb{Z} \oplus \\
& \oplus (F^3 + 1372829830503387)\mathbb{Z} \oplus (F^4 + 1072904687510)\mathbb{Z} \oplus \\
& \oplus \frac{1}{3}(F^5 + F^4 + F^3 + 2F^2 + 2F + 670480698614361 0)\mathbb{Z} \oplus \\
& \oplus \frac{1}{9}(F^6 + F^5 + F^4 + 8F^3 + 2F^2 + 2991665243621169)\mathbb{Z} \oplus \\
& \oplus \frac{1}{27}(F^7 + F^6 + F^5 + 17F^4 + 20F^3 + 9F^2 + 6801531251872220 1)\mathbb{Z}
\end{aligned}
$$

principal polarizations:

$$
\begin{aligned}
x_{1,1} = \frac{1}{27}(& -121922F^7 + 588604F^6 - 1422437F^5 + \\
& + 1464239F^4 + 1196576F^3 - 7570722F^2 + 15316479F - 12821193) \\
x_{1,2} = \frac{1}{27}(& 3015467F^7 - 17689816F^6 + 35965592F^5 - \\
& - 64660346F^4 + 121230619F^3 - 191117052F^2 + 315021546F - 300025458)
\end{aligned}
$$

$\mathrm{End}(I_1) = R$

$\#\mathrm{Aut}(I_1, x_{1,1}) = \#\mathrm{Aut}(I_1, x_{1,2}) = 2$

Example

$$
\begin{aligned}
I_7 = & 2\mathbb{Z} \oplus (F+1)\mathbb{Z} \oplus (F^2+1)\mathbb{Z} \oplus (F^3+1)\mathbb{Z} \oplus (F^4+1)\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F+3)\mathbb{Z} \oplus \\
& \oplus \frac{1}{36}(F^6+F^5+10F^4+26F^3+2F^2+27F+45)\mathbb{Z} \oplus \\
& \oplus \frac{1}{216}(F^7+4F^6+49F^5+200F^4+116F^3+105F^2+198F+351)\mathbb{Z}
\end{aligned}
$$

principal polarization:

$$x_{7,1} = \frac{1}{54}(20F^7 - 43F^6 + 155F^5 - 308F^4 + 580F^3 - 1116F^2 + 2205F - 1809)$$

$$
\begin{aligned}
\mathrm{End}(I_7) = & \mathbb{Z} \oplus F\mathbb{Z} \oplus F^2\mathbb{Z} \oplus F^3\mathbb{Z} \oplus F^4\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F)\mathbb{Z} \oplus \\
& \oplus \frac{1}{18}(F^6+F^5+10F^4+8F^3+2F^2+9F+9)\mathbb{Z} \oplus \\
& \oplus \frac{1}{108}(F^7+4F^6+13F^5+56F^4+80F^3+33F^2+18F+27)\mathbb{Z}
\end{aligned}
$$

$\#\mathrm{Aut}(I_7, x_{7,1}) = 2$

I_1 is invertible in R, but I_7 is not invertible in $\mathrm{End}(I_7)$.

	isogeny cl.	isom. cl.	isom. cl. non pol.	princ. pol.
$\mathbb{F}_2, g = 2$	14/34	21	7	15
$\mathbb{F}_2, g = 3$	81/210	225	107	141
$\mathbb{F}_3, g = 2$	35/62	75	23	58
$\mathbb{F}_3, g = 3$	315/670 (wip)	2329	1244	1325
$\mathbb{F}_5, g = 2$	94/128	457	207	286
$\mathbb{F}_5, g = 3$	213/2994 (wip)	11733	9336	2721
$\mathbb{F}_7, g = 2$	167/207	1322	638	793
$\mathbb{F}_7, g = 3$	176/7968 (wip)	10379	8026	2702
$\mathbb{F}_{11}, g = 2$	352/400	4925	2675	2797
$\mathbb{F}_{11}, g = 3$	188/30530 (wip)	18513	14291	4830

(wip) = work in progress

other results

PAPER II:

- Period matrices of the canonical lift to $\mathbb{C}$ for square-free ordinary abelian varieties.

PAPER II:

- Period matrices of the canonical lift to $\mathbb{C}$ for square-free ordinary abelian varieties.
- Isomorphism classes of square-free abelian varieties over $\mathbb{F}_p$ (away from $\sqrt{p}$) using Centeleghe/Stix (2015).

PAPER II:

- Period matrices of the canonical lift to $\mathbb{C}$ for square-free ordinary abelian varieties.
- Isomorphism classes of square-free abelian varieties over $\mathbb{F}_p$ (away from $\sqrt{p}$) using Centeleghe/Stix (2015).

PAPER III:

- Isomorphism classes of ab. var. with char. poly of the form h^r (with Bass assumption).

PAPER II:

- Period matrices of the canonical lift to $\mathbb{C}$ for square-free ordinary abelian varieties.
- Isomorphism classes of square-free abelian varieties over $\mathbb{F}_p$ (away from $\sqrt{p}$) using Centeleghe/Stix (2015).

PAPER III:

- Isomorphism classes of ab. var. with char. poly of the form h^r (with Bass assumption).
- Polarizations are work in progress.

PAPER II:

- Period matrices of the canonical lift to $\mathbb{C}$ for square-free ordinary abelian varieties.
- Isomorphism classes of square-free abelian varieties over $\mathbb{F}_p$ (away from $\sqrt{p}$) using Centeleghe/Stix (2015).

PAPER III:

- Isomorphism classes of ab. var. with char. poly of the form h^r (with Bass assumption).
- Polarizations are work in progress.

PAPER IV:

- Use the results from PAPER II and PAPER III to distinguish which isomorphism classes are extension of the base field.

Thank you!