Explicit formulas for superspecial abelian surfaces over finite fields.

Chia-Fu Yu 21.06.2017

Report on the joint work with Jiangwei Xue and Tse-Chung Yang

We like to know

- the number of isom. classes of superspecial abelian surfaces over a finite field $\mathbb{F}_q$, or in an isogeny class $\mathcal{I}/\mathbb{F}_q$
- the number of isom. classes of endomorphism rings $\mathrm{End}(A)$, for superspecial abelian surfaces A in an isog. class $\mathcal{I}$.

Def. An ab var. $A/k \supset \mathbb{F}_p$ is called superspecial if $A \otimes \bar{k} \simeq E^g$, for a supersingular elliptic curve E.

Typically, the first one = a sum of some class numbers.

the second one = a sum of some type numbers.

- The goal is to determine explicit formulas for them.
- Since any supersingular abel. surface is either superspecial, or the quotient of superspecial one by α_p,

the results obtained can be used to calculate the numbers for supersingular one.

Notations

p: prime number, $q = p^a$, $a \in \mathbb{N}$, $\mathbb{F}_q$: finite field of q elements.

W_q = the set of Weil q-#'s up to conjugate (Galois).

π, A_π : a simple abel. var. / $\mathbb{F}_q$, w. Frob. endomorphism π, unique up to isogeny, by the Honda-Tate Thm.

$$MW_q := \left\{ \pi = \sum_{i=1}^{r} m_i \pi_i \;\middle|\; \begin{matrix} \pi_i \in W_q,\ m_i \in \mathbb{N} \\ \pi_i \neq \pi_j,\ i \neq j \end{matrix} \right\}$$

= the set of multiple Weil q-#'s.

$$A_\pi := \prod_{i=1}^{r} A_{\pi_i}^{m_i} \quad \text{(unique up to isog.)}, \quad d(\pi) := \dim(A_\pi).$$

$$MW_q \simeq \left\{ \begin{matrix} \text{isog. classes of} \\ \text{abel. varieties } / \mathbb{F}_q \end{matrix} \right\}$$

$$\pi \longmapsto A_\pi$$

$\mathrm{Isog}(\pi)$:= the isog class of A_π

also identified w. $\{ A/\mathbb{F}_q \mid A \sim A_\pi \} / \simeq_{\mathbb{F}_q}$.

$H(\pi) := \#\,\mathrm{Isog}(\pi)$.

$$W_q^{ss} := \{ \pi \in W_q \mid A_\pi : \text{supersingular} \}.$$

$$MW_q^{ss} := \{ \pi \in MW_q \mid A_\pi : \text{s.s.} \} = \{ \text{s.s. multiple Weil } q\text{-\#'s} \}$$

parametrizes s.s. isogeny classes / $\mathbb{F}_q$.

$\pi \in MW_q^{ss}$, $Sp(\pi) := \left\{ \begin{array}{l} \text{superspecial abel. var.} \\ \text{in the isog. class } \mathcal{I}sog(\pi) \end{array} \right\} / \simeq_{\mathbb{F}_q}$.

$H_{sp}(\pi) := \# Sp(\pi)$.

For $d \in \mathbb{N}$, $Sp_q(d) := \left\{ \begin{array}{l} \text{superspecial} \\ \text{ab. var. of dim } d \end{array} \right\} / \simeq_{\mathbb{F}_q}$.

Q: $|Sp_q(d)| = ?$

$$|Sp_q(d)| = \sum_{\substack{\pi \in MW_q^{ss} \\ d(\pi) = d}} H_{sp}(\pi).$$

Ex. $d=1$. $q = p^a$

a = odd:	π	p
	$\sqrt{q}\,\zeta_4$	any
	$\pm\sqrt{q}\,\zeta_8$	$p=2$
	$\pm\sqrt{q}\,\zeta_{12}$	$p=3$.

$p=2$. $|Sp_q(1)| = H(\sqrt{q}\,\zeta_4) + 2H(\sqrt{q}\,\zeta_8) = 3$

$p=3$, $|Sp_q(1)| = H(\sqrt{q}\,\zeta_4) + 2H(\sqrt{q}\,\zeta_{12}) = 4$

$p>3$, $|Sp_q(1)| = \begin{cases} h(\sqrt{-p}) & p \equiv 1 \ (4). \\ \left(3 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}), & p \equiv 3 \ (4). \end{cases}$

$h(\sqrt{-p}) = h(\mathbb{Q}(\sqrt{-p}))$, $\left(\frac{\cdot}{p}\right)$ = Legendre symbol.

a: even:	π	p
	$\pm\sqrt{q}$	any
	$\pm\sqrt{q}\,\zeta_6$	$p \not\equiv 1 \ (3)$
	$\sqrt{q}\,\zeta_4$	$p \not\equiv 1 \ (4)$

$$|Sp_q(1)| = \underline{2H(\sqrt{q})} + \underline{2\delta_3(p)H(\sqrt{q}\,\zeta_6)} + \underline{\delta_4(p)H(\sqrt{q}\,\zeta_4)}$$

$\delta_m(p) = \begin{cases} 1, & p \not\equiv 1 \ (m); \\ 0, & \text{o.w.} \end{cases}$ for $m = 3, 4$.

$B_{p,\infty}$ = definite quaternion $\mathbb{Q}$-alg. ramified at $\{p, \infty\}$.

$$h(\sqrt{q}) = h(B_{p,\infty}) = \frac{p-1}{12} + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-4}{p}\right)\right). \quad \left(\begin{array}{c}\text{Deuring,} \\ \text{Eichler}\end{array}\right)$$

$$|Sp_q(1)| = \frac{p-1}{6} + \frac{8}{3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{3}{2}\left(1 - \left(\frac{-4}{p}\right)\right).$$

§ Results for $d=2$ and a: odd.

$q=p^a$, a: odd, $W_q^{ss}(d)=\{\pi\in W_q^{ss} \mid d(\pi)=d\}$.

$$|Sp_q(2)| = \sum_{\pi\in W_q^{ss}(2)} H_{sp}(\pi) + \sum_{\pi_1,\pi_2\in W_q^{ss}(1)} H_{sp}(\pi_1\times\pi_2)$$

simple contribution; non-simple contr. $\begin{cases}\text{elementary}: \pi_1=\pi_2\\ \text{non-elementary}: \pi_1\neq\pi_2\end{cases}$.

$d=1$:

$W_q^{ss}(1)=\{\sqrt{q}\,S_4,\ \pm\sqrt{q}\,S_8\}$ $p=2$

$W_q^{sr}(1)=\{\sqrt{q}\,S_4,\ \pm\sqrt{q}\,S_{12}\}$ $p=3$

$W_q^{ss}(1)=\{\sqrt{q}\,S_4\}$, $p\geq 5$

$d=2$:

$W_q^{ss}(2)=\{\sqrt{q},\sqrt{q}\,S_3,\sqrt{q}\,S_{12},\pm\sqrt{q}\,S_{24}\}$ $p=2$

$W_q^{ss}(2)=\{\sqrt{q},\sqrt{q}\,S_3,\sqrt{q}\,S_8\}$ $p=3$

$W_q^{ss}(2)=\{\sqrt{q},\sqrt{q}\,S_3,\sqrt{q}\,S_8,\sqrt{q}\,S_{12},\pm\sqrt{q}\,S_5\}$, $p=5$

$W_q^{ss}(2)=\{\sqrt{q},\sqrt{q}\,S_3,\sqrt{q}\,S_8,\sqrt{q}\,S_{12}\}$ $p\geq 7$.

	simple	non-simple elementary	non-simple non-elementary	total terms
$p=2$	5	3	3	11
$p=3$	3	3	3	9
$p=5$	6	1	0	7
$p\geq 7$	4	1	0	5
				32

Thm (J. Xue, T.-C. Yang, Y.) $q = p^a$, a: odd.

① $|S_{p_q}(d)|$ depends only on p.

$$|S_{p_q}(2)| = H(p) + \Delta(p).$$

② (formula for $H(p)$)

(a) $H(p) = 1, 2, 3$ for $p = 2, 3, 5$, resp.

(b) For $p > 5$ and $p \equiv 3 \pmod 4$,

$$H(p) = \frac{1}{2} h(F) \zeta_F(-1) + \left(\frac{3}{8} + \frac{5}{8}\left(2 - \left(\frac{2}{p}\right)\right) h(K_{p,1}) + \frac{1}{4} h(K_{p,2}) + \frac{1}{3} h(K_{p,3}) \right.$$

where $F = \mathbb{Q}(\sqrt{p})$, $h(F)$ = class # of F, $\zeta_F(s)$ = Dedekind function of F.

$K_{p,j} = \mathbb{Q}(\sqrt{p}, \sqrt{-j})$, $j = 1, 2, 3$.

(c) For $p > 5$ and $p \equiv 1 \pmod 4$,

$$H(p) = \begin{cases} 8 \zeta_F(-1) h(F) + h(K_{p,1}) + \frac{4}{3} h(K_{p,3}) & \text{for } p \equiv 1 \ (8) \\ \frac{1}{2}(15 w_p + 1) \zeta_F(-1) h(F) + \frac{1}{4}(3 w_p + 1) h(K_{p,1}) & \text{for } p \equiv 5 \ (8) \\ \quad + \frac{4}{3} h(K_{p,3}). \end{cases}$$

where $w_m := 3 \left[O_{\mathbb{Q}(\sqrt{m})}^{\times} : \mathbb{Z}[\sqrt{m}]^{\times} \right]^{-1}$ for $m \equiv 1 \ (4)$. $(w_m \in \{1, 3\})$

③ (formula for $\Delta(p)$)

(a) $\Delta(p) = 15, 20, 9$ for $p = 2, 3, 5$, respectively

(b) For $p > 5$ and $p \equiv 1 \pmod 4$,

$$\Delta(p) = (w_p + 1) h(K_{p,3}) + h(K_{2p,1}) + h(\sqrt{-p}).$$

(c) For $p > 5$ and $p \equiv 3 \pmod 4$,

$$\Delta(p) = h(K_{p,3}) + h(K_{2p,1}) + (w_{3p} + 1) h(K_{3p,3}) + \left(4 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}).$$

④ (Asymptotic behavior) Put

$$\mathrm{Mass}_p := \begin{cases} \frac{1}{2} h(F)\zeta_F(-1) & \text{for } p \equiv 3 \ (4); \\ 8\, h(F)\zeta_F(-1) & \text{for } p \equiv 1 \ (8); \\ \frac{1}{2}(15 w_p + 1) h(F)\zeta_F(-1) & \text{for } p \equiv 5 \ (8). \end{cases}$$

Then $\dfrac{|S_{p_q}(2)|}{\mathrm{Mass}_p} \to 1$ as $p \to \infty$.

§ Galois cohomology

E_0 : s.s. elliptic curve $/\bar{\mathbb{F}}_p$, $\pi_{E_0}^2 + p = 0$.

$\mathcal{O} := \mathrm{End}(E_0 \otimes \bar{\mathbb{F}}_p) \subset \mathrm{End}^0(E_0 \otimes \bar{\mathbb{F}}_p) = B_{p,\infty}$,

max. order w. action by $\Gamma_{\mathbb{F}_p} = \mathrm{Gal}(\bar{\mathbb{F}}_p / \mathbb{F}_p)$.

Thm (Deligne, Shioda, Ogus) If $d > 1$, then any superspecial ab. var of dim d $/\bar{\mathbb{F}}_p$ is isom. to $E_0 \otimes \bar{\mathbb{F}}_p$.

$\Rightarrow \forall\, d > 1, q$, $H^1(\mathbb{F}_q, G) \simeq S_{p_q}(d) = \coprod_{d(\pi)=d} S_p(\pi)$, $G = GL_d(\mathcal{O})$.

If $q = p^a$, $q' = p^{a'}$, suppose $a - a' = 2s \geq 0$.

Identify $\Gamma_{\mathbb{F}_q} \simeq \hat{\mathbb{Z}} \simeq \Gamma_{\mathbb{F}_{q'}}$, and σ_{p^2} acts trivially on G.

$$H^1(\mathbb{F}_q, G) \simeq H^1(\mathbb{F}_{q'}, G) \Rightarrow |S_{p_q}(d)| = |S_{p_{q'}}(d)|$$

under this map

$$S_p(\pi) \xrightarrow{\sim} S_p(\tilde{\pi}) \quad (*)$$

$$\pi = \sum m_i \pi_i \qquad \tilde{\pi} = \sum m_i \tilde{\pi}_i, \quad \tilde{\pi}_i = (-p)^{-s} \cdot \pi_i$$

For $d = 1$, no simple Galois coh. description, but still have $(*)$.

Now $q = p^a$, a: odd.

$$|Sp_q(2)| = |Sp_p(2)| = H(p) + \Delta(p)$$

$H(p) := H_{sp}(\sqrt{p}) = H(\sqrt{p})$

$\Delta(p) :=$ the rest contribution $= \sum_{\pi \neq \sqrt{p}} H_{sp}(\pi)$.

Method for computing $H(\sqrt{p}) = \# Isog(\sqrt{p})$:

$\pi = \sqrt{p}$, $D = End^0(A_\pi)$: definite quat. F-alg, $F = \mathbb{Q}(\sqrt{p})$,
ramified only at two real places of F.

$\mathcal{O}_1 \subset D$ a max. order.

Prop (Waterhouse, Y.)

① Suppose $p \neq 1$ (4). Then $End(X)$ is a max. order for $X \in Isog(\sqrt{p})$.
and $Isog(\sqrt{p}) \simeq Cl(\mathcal{O}_1)$.

② Suppose $p \equiv 1$ (4). Then $End(X)$ has index $1, 8, 16$ for $X \in Isog(\sqrt{p})$.
$\{X \mid End(X)$ has index $r\}$ $(r = 1, 8, 16)$ forms a genus.

and $Isog(X) \simeq Cl(\mathcal{O}_1) \sqcup Cl(\mathcal{O}_8) \sqcup Cl(\mathcal{O}_{16})$,
where $\mathcal{O}_8, \mathcal{O}_{16}$ proper $\mathbb{Z}[\sqrt{p}]$-orders of index $8, 16$.

Then we use Eichler's trace formula to calculate $h(\mathcal{O}_1)$.
(for $\mathcal{O}_F$-order $\Lambda \subset D_{/F}$)

For $h(\mathcal{O}_8), h(\mathcal{O}_{16})$, we use generalized Eichler's trace formula
(for $\mathbb{Z}$-order $\Lambda \subset D_{/F}$, by XYY)

§ Abelian varieties / $\mathbb{F}_p$ (restricted to s.s. case).

X_0 : fixed supersingular ab. var. / $\mathbb{F}_p$

$\pi = \sum m_i \pi_i$ multiple Weil p-# corr. to $\mathcal{I}sog(X_0)$

$\mathcal{E} = End^0(X_0)$, $K = \mathbb{Q}(\pi_0) \subset \mathcal{E}$, $\pi_0 \in End(X_0)$: Frobenius endomorphism

$K = \prod_i K_i$, $K_i = \mathbb{Q}(\pi_i)$.

$V := \bigoplus_i K_i^{m_i}$, $R := \mathbb{Z}[\pi_0, p\pi_0^{-1}] \subset K$ order

$R_{sp} := R[\pi_0^2/p]$.

Prop ① Assume $\pi_i \neq \sqrt{p}$ $\forall i$. Then $\exists$ bijection

$$\mathcal{I}sog(\pi) \simeq \{R\text{-lattices in } V\}/\simeq$$

② Under this bijection

$$Sp(\pi) \simeq \{R_{sp}\text{-lattices in } V\}/\simeq$$

Rmk : • Part ① holds for arbitrary isog classes / $\mathbb{F}_p$.

- Simple isog classes / $\mathbb{F}_p$ was first obtained by Waterhouse (1968).
- Centeleghe - Stix give a categorical description for all ab vars / $\mathbb{F}_p$ having no $\sqrt{p}$-components.
- Poonen's description.

Use Proposition, we compute all terms in $\Delta(p)$.

Rmk: As a by product, we obtain an explicit formula

for $\# H^1(\mathbb{F}_p, G)$, $G = GL_2(\mathbb{O})$.

From our explict formula, we don't see cancellation $H(p)+\Delta(p)$.

§ Results for $q = p^a$, a: even.

For each r-tuple $\underline{n} = (n_1, \cdots, n_r)$, $1 \le n_1 < \cdots < n_r$

Put $A_{\underline{n}} := \mathbb{Z}[t] / \prod_i \Phi_{n_i}(t)$, $\Phi_m(t)$: m^{th} cyclotomic polynomial.

$K_{\underline{n}} := A_{\underline{n}} \otimes \mathbb{Q} = \prod K_i$, $K_i = \mathbb{Q}(\zeta_{n_i})$.

$o(\underline{n}) := \#\, \mathrm{Hom}(A_{\underline{n}}, \mathrm{Mat}_d(\mathcal{O})) / GL_d(\mathcal{O})$.

Prop. $|Sp_q(d)| = \#\, H^1(\mathbb{F}_q, G)$, $G = GL_d(\mathcal{O})$

$= \#\, Cl_0 G$, (set of conj classes of elements of finit order in G)

$= \sum_{\underline{n}} o(\underline{n})$

Now $d = 2$. $\Rightarrow r \le 2$

$r = 1$, $n \in \{1, 2, 3, 4, 6, 5, 8, 10, 12\}$

$r = 2$, $\underline{n} = (n_1, n_2)$, $n_1, n_2 \in \{1, 2, 3, 4, 6\}$.

} There are 19 terms, each term corr. to one isog class.

Simple observation:

$o(1) = o(2) = 1$, $o(3) = o(6)$, $o(5) = o(10)$

$o(1,3) = o(2,6)$, etc.

Thm (XYY) $q = p^a$, a: even. Then

$$|Sp_q(2)| = 2 + 2\,o(3) + o(4) + 2\,o(5) + o(8) + o(12)$$
$$+ o(1,2) + 2\,o(1,3) + 2\,o(1,4) + 2\,o(1,6) + 2\,o(3,4) + o(3,6)$$

Each terms are given as follows :

(1) For $P \neq 3$, $o(3) = 2 - \left(\frac{-3}{P}\right)$.

(2) For $P \neq 2$, $o(4) = 2 - \left(\frac{-4}{P}\right)$.

(3) For $P \neq 5$, $o(5) = \begin{cases} 0 & P \equiv 1 \ (5) \\ 2 & P \equiv 2,3 \ (5) \\ 4 & P \equiv 4 \ (5). \end{cases}$

(4) For $P \neq 2$, $o(8) = \begin{cases} 0 & P \equiv 1 \ (8). \\ 4 & o.w. \end{cases}$

(5) For $P \neq 2,3$, $o(12) = \begin{cases} 0 & P \equiv 1 \ (12) \\ 4 & o.w. \end{cases}$

(6) For $P \neq 2$, $o(1,2) = \frac{(P-1)^2}{9} + \frac{P+15}{18}\left(1 - \left(\frac{-3}{P}\right)\right) + \frac{P+2}{6}\left(1 - \left(\frac{-4}{P}\right)\right)$
$+ \frac{1}{6}\left(1 - \left(\frac{-3}{P}\right)\right)\left(1 - \left(\frac{-4}{P}\right)\right)$.

(7) For $P \neq 3$, $o(1,3) = \frac{5P+11}{12}\left(1 - \left(\frac{-3}{P}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-3}{P}\right)\right)\left(1 - \left(\frac{-4}{P}\right)\right)$.

(8) For $P \neq 2$, $o(1,4) = \frac{P+2}{3}\left(1 - \left(\frac{-4}{P}\right)\right) + \frac{1}{3}\left(1 - \left(\frac{-3}{P}\right)\right)\left(1 - \left(\frac{-4}{P}\right)\right)$.

(9) For $P \neq 3$, $o(1,6) = \frac{P+7}{12}\left(1 - \left(\frac{-3}{P}\right)\right) + \frac{1}{4}\left(1 - \left(\frac{-3}{P}\right)\right)\left(1 - \left(\frac{-4}{P}\right)\right)$.

(10) For $P \neq 2,3$, $o(3,4) = \left(1 - \left(\frac{-3}{P}\right)\right)\left(1 - \left(\frac{-4}{P}\right)\right)$.

(11) For $P \neq 3$, $o(3,6) = 4\left(1 - \left(\frac{-3}{P}\right)\right)$.

Cor (Asymptotic behavior) $q = P^a$, a : even

$$\frac{|S_{P_1}(2)|}{P^2/9} \to 1 \quad \text{as } P \to \infty.$$

$q = p^a$, a : odd

T = # of isom classes of $\mathrm{End}(X)$, for all $X \in Sp(\sqrt{q})$.

T depends only on p, denoted by $T(p)$.

Thm (Xue-Y.)

(1) $T(p) = 1, 2, 3$ for $p = 2, 3, 5$, resp.

(2) $p > 5$ and $p \equiv 3 \ (4)$.

$$T(p) = \frac{\zeta_F(-1)}{2} + \left(13 - 5\left(\frac{2}{p}\right)\right)\frac{h(-p)}{8} + \frac{h(-2p)}{4} + \frac{h(-3p)}{6},$$

where $h(d) = h(\mathbb{Q}(\sqrt{d}))$.

(3) $p > 5$ and $p \equiv 1 \ (4)$,

$$T(p) = 8\,\zeta_F(-1) + \frac{h(-p)}{2} + \frac{2}{3}h(-3p).$$