

Point counting on reductions of CM abelian surfaces

Nick Alexander

University of California, Irvine
ncalexander@gmail.com

Workshop on Counting Points: Theory, Algorithms and Practice
April 19-23, 2010

This work is part of my PhD dissertation at University of California, Irvine under the supervision of Alice Silverberg.

Thanks to David Grant, Colorado at Boulder, for unpublished work on genus 2 curves.

Thanks to Points10 organizers for invitation to speak.

Gauss:

$$E : y^2 = x^3 + B$$

p - odd prime of good reduction, $p \equiv 2 \pmod{3} \implies$

$$\#E(\mathbf{F}_p) = p + 1.$$

p - odd prime of good reduction, $p \equiv 1 \pmod{3} \implies$

$$\#E(\mathbf{F}_p) = p + 1 - (\pi + \bar{\pi})$$

where $\pi \in \mathbf{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] = \mathcal{O}_{\mathbf{Q}(\zeta_3)}$ and $p = \pi\bar{\pi}$, and π satisfies the congruence condition

$$\pi \equiv 1 \pmod{3}$$

Gauss-Herglotz:

$$E : y^2 = x^3 + 4x$$

p - odd prime of good reduction, $p \equiv 1 \pmod{4} \implies$

$$\#E(\mathbf{F}_p) = p + 1 - (\pi + \bar{\pi})$$

where $\pi \in \mathbf{Z}[\sqrt{-1}] = \mathcal{O}_{\mathbf{Q}(i)}$ and $p = \pi\bar{\pi}$, and π satisfies the congruence condition

$$\pi \equiv 1 \pmod{2 + 2i}$$

Rajwade:

$$E : y^2 = x(x^2 - 4ax + 2a^2)$$

p - odd prime of good reduction, $p \equiv 1, 3 \pmod{8} \implies$

$$\#E(\mathbf{F}_p) = p + 1 - \left(\frac{a}{p}\right) (\pi + \bar{\pi})$$

where $\pi \in \mathbf{Z}[\sqrt{-2}] = \mathcal{O}_{\mathbf{Q}(\sqrt{-2})}$ and $p = \pi\bar{\pi}$, and π satisfies the congruence condition

$$\pi \pmod{4\sqrt{-2}}$$

$$\in \left\{ 1, 3, 1 \pm \sqrt{-2}, 3 \pm \sqrt{-2}, 5 + 2\sqrt{-2}, 7 + 2\sqrt{-2} \right\}.$$

Suppose:

- d - square-free positive integer, $d \equiv 7, 11 \pmod{12}$
- (π) - prime ideal of $\mathbf{Q}(\sqrt{-d})$ of norm p with $(p, 6d) = 1$
- $\pi = u + v\sqrt{-d}$ with $u, v \in \frac{1}{2}\mathbf{Z}$
- H - Hilbert class field of $\mathbf{Q}(\sqrt{-d})$, \mathfrak{P} - prime of H above π

Then:

$$E : y^2 = x^3 + \frac{a^2 d \gamma_2(\tau)}{48} x - \frac{a^3 d \sqrt{-d} \gamma_3(\tau)}{864}$$

is defined over H and has CM by $\mathbf{Q}(\sqrt{-d})$, and

$$\#E(\mathcal{O}_H/\mathfrak{P}) = N_{H/\mathbf{Q}}(\mathfrak{P}) + 1 - \left(\frac{(-1)^{\frac{d+1}{4}} a}{\mathfrak{P}} \right)_{2,H} \left(\frac{4u}{d} \right) 2u,$$

where $\tau = \frac{-3 + \sqrt{-d}}{2}$, and γ_2, γ_3 are the Weber modular functions, and $(\cdot/\mathfrak{P})_{2,H}$ is the quadratic residue symbol in H .

Suppose:

- K - CM-field, $[K : \mathbf{Q}] = 4$, some restrictions, K' - reflex field
- $\tau \in \mathfrak{h}_2$ and $\text{Jac}(C(\tau))$ - as below
- k - field of definition as below
- $\mathfrak{P} \nmid 2$ - prime of k where $\text{Jac}(C(\tau))$ has good reduction
- $\eta(\mathbf{N}_{k/K'}(\mathfrak{P})) = \lambda \mathcal{O}_K$ with $|\lambda|_v = \sqrt{\mathbf{N}_{k/\mathbf{Q}}(\mathfrak{P})}$ for all $v | \infty$
- $\lambda = a\nu + b\nu w + c w + d$ with $a, b, c, d \in \mathbf{Z}$, fixed $\nu \in K$, and

$$\epsilon(\lambda) = \begin{cases} +1 & \text{if } d \equiv 1 \pmod{4}, \\ -1 & \text{if } d \equiv 3 \pmod{4}. \end{cases}$$

Then: $\text{Jac}(C(\tau))$ is defined over k and has CM by \mathcal{O}_K , and

$$\# \text{Jac}(C(\tau))(\mathcal{O}_k/\mathfrak{P}) = \mathbf{N}_{K/\mathbf{Q}}(1 - \epsilon(\lambda)\lambda).$$

We view all number fields as embedded in \mathbf{C} .

A *CM-field* is a totally imaginary quadratic extension K of a totally real number field K_0 . Unique complex conjugation \bar{x} in K .

A *CM-type* is a pair $\Phi = (\{\varphi_1, \dots, \varphi_n\}, K)$ with K a CM-field and with distinct $\varphi_i : K \hookrightarrow \mathbf{C}$ and no $\varphi_i = \overline{\varphi_j}$.

Abuse of notation: $\Phi : K \hookrightarrow \mathbf{C}^n$ defined by $\Phi(x) = {}^t(x^{\varphi_1}, \dots, x^{\varphi_n})$.

These data determine a *reflex CM-type* $(K', \{\psi_1, \dots, \psi_n\})$ and a multiplicative homomorphism

$$\eta : (K')^\times \rightarrow K^\times$$

$$\eta(x) = \prod_i x^{\psi_i}.$$

The map η extends to a map of ideals.

$$C(\tau) : y^2 = x(x-1) \left(x - \frac{\vartheta_{21}^2 \vartheta_{30}^2}{\vartheta_{01}^2 \vartheta_{10}^2} \right) \left(x - \frac{\vartheta_{20}^2 \vartheta_{30}^2}{\vartheta_{00}^2 \vartheta_{10}^2} \right) \left(x - \frac{\vartheta_{20}^2 \vartheta_{21}^2}{\vartheta_{00}^2 \vartheta_{01}^2} \right)$$

where $\vartheta_{AB} : \mathfrak{h}_2 \rightarrow \mathbf{C}$ are Siegel modular functions

$$\vartheta_{AB} = \theta[\delta](0, \tau), \quad (A, B \in \{0, 1, 2, 3\})$$

where the binary expansions of A, B are $2a, 2b$ ($a, b \in \frac{1}{2}\mathbf{Z}^2$)

$$\theta : \mathbf{C}^2 \times \mathfrak{h}_2 \rightarrow \mathbf{C}$$

$$\theta[\delta](z, \tau) = \sum_{g-a \in \mathbf{Z}^2} \mathbf{e}(2^{-1} \cdot {}^t g \tau g + {}^t g(z+b)).$$

Compare Stark:

$$E : y^2 = x^3 + \frac{a^2 d \gamma_2(\tau)}{48} x - \frac{a^3 d \sqrt{-d} \gamma_3(\tau)}{864}$$

Let Θ_i denote the i -th symmetric function of $\frac{\vartheta_{21}^2 \vartheta_{30}^2}{\vartheta_{01}^2 \vartheta_{10}^2}, \frac{\vartheta_{20}^2 \vartheta_{30}^2}{\vartheta_{00}^2 \vartheta_{10}^2}, \frac{\vartheta_{20}^2 \vartheta_{21}^2}{\vartheta_{00}^2 \vartheta_{01}^2}$.

Each Θ_i is in $\overline{\mathbf{Q}}$.

$\text{Jac}(C(\tau))$ is defined over

$$k_0 := \mathbf{Q}(\Theta_1, \dots, \Theta_3).$$

My results need certain class field k over K' with $k \supseteq K' \cdot k_0$.

Conjecturally

$$k = K' \cdot k_0.$$

Compare Stark: $k = H_K$ - Hilbert class field

A - principally polarized abelian variety with CM by K .

Take $F : \mathbf{C}^n \rightarrow \mathbf{A}$ and ideal \mathfrak{a} of K such that:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathfrak{a} & \longrightarrow & K \otimes \mathbf{R} & \longrightarrow & (K \otimes \mathbf{R})/\mathfrak{a} \longrightarrow 0 \\ & & \downarrow & & \downarrow \Phi & & \downarrow \\ 0 & \longrightarrow & \Phi(\mathfrak{a}) & \longrightarrow & \mathbf{C}^n & \xrightarrow{F} & \mathbf{A} \longrightarrow 0. \end{array}$$

A determines an alternating Riemann form $E : \mathbf{C}^n \times \mathbf{C}^n \rightarrow \mathbf{R}$.

Choose $\Omega \in M_{n \times 2n}(\mathbf{C})$ whose columns are basis for $\Phi(\mathfrak{a})$ such that

$$E(\Omega x, \Omega y) = {}^t x J y, \quad (x, y \in \mathbf{R}^{2n}).$$

Write $\Omega = (\omega_1 \ \omega_2)$ with $n \times n$ matrices ω_i . Define

$$\tau = \omega_2^{-1} \omega_1.$$

Then τ is in Siegel upper half space \mathfrak{h}_n and is the moduli point for the principally polarized abelian variety (A, E) .

Complex representation $\phi : K \rightarrow M_2(\mathbf{C})$:

$$\Phi(\alpha x) = \phi(\alpha)\Phi(x)$$

Rational representation $\xi : K \rightarrow M_4(\mathbf{Q})$ given by

$$\phi(\alpha)\Omega = \Omega^t\xi(\alpha).$$

Suppose:

- k - number field, A - abelian variety over k
- A has CM by K , $[K : \mathbf{Q}] = 2 \dim A$, $\mu_\infty \cap \mathcal{O}_K^\times = \{\pm 1\}$
- K' - reflex field, $K' \subseteq k$
- \mathfrak{P} - prime of k such that A has good reduction modulo \mathfrak{P}
- $\eta(N_{k/K}(\mathfrak{P})) = \lambda \mathcal{O}_K$ with $|\lambda|_v = \sqrt{N_{k/\mathbf{Q}}(\mathfrak{P})}$ for all $v | \infty$

Then:

$$\begin{aligned} \#A(\mathcal{O}_k/\mathfrak{P}) &= N_{K/\mathbf{Q}}(1 - \epsilon(\lambda)\lambda) \quad \text{with } \epsilon(\lambda) \in \{\pm 1\} \\ &= \chi(1), \end{aligned}$$

where $\chi(x) \in \mathbf{Z}[x]$ is the characteristic polynomial of $\epsilon(\lambda)\lambda$.

Complex multiplication for genus 1

Suppose:

- k - number field, E - elliptic curve over k
- E has CM by $K \subseteq k$ with $K \neq \mathbf{Q}(i), \mathbf{Q}(\zeta_3)$
- \mathfrak{P} - prime of k such that E has good reduction modulo \mathfrak{P}
- $N_{k/K}(\mathfrak{P}) = \pi \mathcal{O}_K$

Then:

$$\begin{aligned} \#E(\mathcal{O}_k/\mathfrak{P}) &= N_{k/\mathbf{Q}}(\mathfrak{P}) + 1 - \epsilon(\pi)(\pi + \bar{\pi}) \quad \text{with } \epsilon(\pi) \in \{\pm 1\} \\ &= N_{K/\mathbf{Q}}(1 - \epsilon(\pi)\pi) \end{aligned}$$

Compare Stark:

$$\epsilon(\pi) = \epsilon(u + v\sqrt{-d}) = \left(\frac{(-1)^{\frac{d+1}{4}} a}{\mathfrak{P}} \right)_{2,H} \left(\frac{4u}{d} \right), \quad \pi + \bar{\pi} = 2u$$

Complex multiplication for genus 1

$$\begin{array}{c}
 K \\
 \swarrow \quad \searrow \\
 \mathbb{Q}
 \end{array}
 \xleftarrow{\text{id}}
 \begin{array}{c}
 k \\
 | \\
 K
 \end{array}
 \begin{array}{c}
 \mathfrak{P} \\
 | \\
 N_{k/K'}(\mathfrak{P}) \\
 | \\
 N_{k/\mathbb{Q}}(\mathfrak{P})
 \end{array}
 \quad \Bigg| \quad
 \lambda \mathcal{O}_K
 \begin{array}{c}
 K \\
 \swarrow \quad \searrow \\
 \mathbb{Q}
 \end{array}
 \xleftarrow{\eta}
 \begin{array}{c}
 k \\
 | \\
 K'
 \end{array}
 \begin{array}{c}
 \mathfrak{P} \\
 | \\
 N_{k/K'}(\mathfrak{P}) \\
 | \\
 N_{k/\mathbb{Q}}(\mathfrak{P})
 \end{array}$$

Suppose:

- K - CM-field, $[K : \mathbf{Q}] = 4$
- discriminant of $K_0 = \mathbf{Q}(d_{K_0})$ is d_{K_0} , assume $d_{K_0} \equiv 3 \pmod{4}$ so that $\mathcal{O}_{K_0} = \mathbf{Z} + w\mathbf{Z}$ with $w = \sqrt{d_{K_0}}$
- *Simplify* by choosing lattice \mathcal{O}_{K_0} in K
- K_0 - class number one so that $\mathcal{O}_K = \mathcal{O}_{K_0} + \nu\mathcal{O}_{K_0}$

Then: $\{\nu, -\nu w, w, 1\}$ is a symplectic basis for

$$E_\zeta : K \times K \rightarrow \mathbf{Q}$$

$$E_\zeta(x, y) = \text{Tr}_{K/\mathbf{Q}}(\zeta x \bar{y})$$

with $\zeta = (-2w(\nu - \bar{\nu}))^{-1}$

Suppose:

- $\text{Im } \zeta^{\varphi_i} > 0$ for $i = 1, 2$
- $\Omega = \begin{pmatrix} \nu^{\varphi_1} & -(\nu w)^{\varphi_1} & w^{\varphi_1} & 1 \\ \nu^{\varphi_2} & -(\nu w)^{\varphi_2} & w^{\varphi_2} & 1 \end{pmatrix} \in M_{2 \times 4}(\mathbf{C})$

Then: CM-point $\tau \in \mathfrak{h}_2$ corresponding to $(\mathbf{C}^2/\Omega\mathbf{Z}^4, E_\zeta)$ is

$$\tau := \begin{pmatrix} w^{\varphi_1} & 1 \\ w^{\varphi_2} & 1 \end{pmatrix}^{-1} \begin{pmatrix} \nu^{\varphi_1} & \nu^{\varphi_2} \\ -(\nu w)^{\varphi_1} & -(\nu w)^{\varphi_2} \end{pmatrix} \in \mathfrak{h}_2.$$

Compare Stark:

$$\tau = \frac{-3 + \sqrt{-d}}{2} \in \mathfrak{h}$$

$\alpha = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GSp}^+(2n, \mathbf{Q})$ acts on $\mathbf{C}^n \times \mathfrak{h}_n$ by

$$\alpha(z, \tau) = ({}^t(C\tau + D)^{-1}z, (A\tau + B)(C\tau + D)^{-1}).$$

For $f : \mathbf{C}^n \times \mathfrak{h}_n \longrightarrow \mathbf{C}$ and $\gamma \in \mathrm{GSp}^+(2n, \mathbf{Q})$

$$(f|_k\gamma)(z, \tau) = \det(C\tau + D)^{-k} f(\alpha(z, \tau)).$$

(Restricted class of) Theta functions are holomorphic f such that

$$f|_k\gamma = f \quad \text{for all } \gamma \in \Gamma,$$

$$f(z + \tau p + q, \tau) = f(z, \tau) \quad \text{for all } ({}^t(p, q) \text{ in a lattice } \Lambda \subset \mathbf{Q}^n).$$

Theta functions have Fourier expansions. A theta function is called *arithmetic* if its Fourier coefficients are in \mathbf{Q}^{ab} .

Examples:

- classical theta $\theta[\delta](z, \tau)$ (Fourier coefficients in \mathbf{Q} or $\mathbf{Q}(i)$)
- Weierstrass \wp, \wp' (arithmetic up to $2\pi i$ factors)

Really: use *half-integral weight* and *vector-valued* theta functions.

Shimura: $\text{GSp}^+(2n, \mathbf{A}_{\mathbf{Q}})$ acts on arithmetic theta functions.

Suppose $F : \mathbf{C}^n \times \mathfrak{h}_n \rightarrow \mathbf{P}^m$ is a projective embedding,
 $F = (f_0, \dots, f_m)$, each f_i an arithmetic theta function.

Define *projective group*

$$P = \{x \in \mathrm{GSp}^+(2n, \mathbf{R}) \times \prod_p \mathrm{GSp}(2n, \mathbf{Z}_p) : f_i^x = f_i \text{ for all } 0 \leq i \leq m\}.$$

Rumely: in terms of P , gives

- field of definition for $F(\tau)$ as class field over K'
- formula for grössencharacter of $F(\tau)$

Extension: suppose f_i even or odd, then $P \cap (-P) = \emptyset$.

Correct Frobenius element $\lambda \in K$ should have rational representation

$$\xi(\lambda) \in P.$$

Genus 2 theorem reduces to computation of P for particular projective embedding. Result:

$$P = \{x \in \mathrm{GSp}^+(2n, \mathbf{R}) \times \prod_p \mathrm{GSp}(2n, \mathbf{Z}_p) :$$

$$x_2 \equiv \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & 0 & * \\ 0 & 0 & 1 & 0 \\ 0 & * & 0 & * \end{pmatrix} \pmod{2}, x_2 \equiv \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & 1 & * \\ * & * & * & * \end{pmatrix} \pmod{4}\}.$$

Congruence condition on Frobenius element $\lambda \in K$ is this congruence modulo 4.

Why distinguished moduli point?

Recall $\xi : K \rightarrow M_4(\mathbf{Q})$ given by

$$\phi(\alpha)\Omega = \Omega^t\xi(\alpha).$$

Suppose $w^2 + aw + b = 0$, $a, b \in \mathbf{Z}$.

Distinguished moduli point controls rational representation:

$${}^t\xi(\nu) = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & 0 & 0 \\ * & * & 0 & 0 \end{pmatrix}, {}^t\xi(-\nu w) = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & 0 & 0 \\ * & * & 0 & 0 \end{pmatrix},$$

$${}^t\xi(w) = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & -a & -b \\ * & * & 1 & 0 \end{pmatrix}, {}^t\xi(1) = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & 1 & 0 \\ * & * & 0 & 1 \end{pmatrix}.$$

Thanks to David Grant, Colorado at Boulder.

Define Siegel modular forms $D, \Delta : \mathfrak{h}_2 \rightarrow \mathbf{C}$ by

$$D(\tau) = \prod_{\eta \text{ even}} \theta[\eta](0, \tau)$$

$$\Delta(\tau) = D(\tau)^2.$$

D defined only up to sign.

Fix $\tau \in \mathfrak{h}_2$ such that $\Delta(\tau) \neq 0$.

Fix odd theta characteristic δ .

Grant's generalization of Jacobi derivative formula

$X^{\text{num}}[\delta]_z : \mathbf{C}^2 \times \mathfrak{h}_2 \rightarrow \mathbf{C}$ defined by

$$X^{\text{num}}[\delta]_z(z, \tau) = \theta[\delta](z, \tau)^3 \det_{1 \leq i, j \leq 2} \left(\frac{\partial^2}{\partial z_i \partial z_j} \log \theta[\delta](z, \tau) \right).$$

Define $U[\delta](\tau) := \begin{pmatrix} \theta[\delta]_{z,1}(0, \tau) & \theta[\delta]_{z,2}(0, \tau) \\ X^{\text{num}}[\delta]_{z,1}(0, \tau) & X^{\text{num}}[\delta]_{z,2}(0, \tau) \end{pmatrix}$.

Then (Grant, unpublished):

$$\det U[\delta](\tau) = \pm 2\pi^6 D(\tau).$$

Compare Jacobi:

$$\theta'_{11}(0, \tau) = \pi \theta_{00}(0, \tau) \theta_{01}(0, \tau) \theta_{11}(0, \tau).$$

Compare Rosenhain:

$$\det \begin{pmatrix} \theta[\delta_1]_{z,1}(0, \tau) & \theta[\delta_1]_{z,2}(0, \tau) \\ \theta[\delta_2]_{z,1}(0, \tau) & \theta[\delta_2]_{z,2}(0, \tau) \end{pmatrix} = \pm \vartheta_1 \vartheta_2 \vartheta_3 \vartheta_4.$$

Modify $U[\delta](\tau)$ to $W[\delta](\tau)$ such that

$$w = W[\delta](\tau)z \in \mathbf{C}^2$$

are parameters for \mathbf{C}^2 (when $\Delta(\tau) \neq 0$).

Grant:

$$\theta[\delta]_w(w, \tau) = \frac{1}{2}w_1 - \frac{1}{(2\pi^6 D(\tau))^2} \frac{w_2^3}{3!} + w_1(e_{11}w_1^2 + 2e_{12}w_1w_2 + e_{22}w_2^2).$$

Let $\sigma[\delta]_w(w, \tau) : \mathbf{C}^2 \times \mathfrak{h}_2 \rightarrow \mathbf{C}$ be

$$\sigma[\delta]_w(w, \tau) := \frac{2}{2\pi^6 D(\tau)} \mathbf{e} \left(-{}^t w \begin{pmatrix} e_{11} & e_{12} \\ e_{12} & e_{22} \end{pmatrix} w \right) \theta[\delta]_w(w, \tau).$$

Define $\wp_* : \mathbf{C}^2 \times \mathfrak{h}_2 \longrightarrow \mathbf{C}$ for $i, j, k \in \{1, 2\}$:

$$\wp_{ij}[\delta](w, \tau) := \frac{-1}{(2\pi i)^2} \frac{\partial^2}{\partial w_i \partial w_j} \log \sigma[\delta](w, \tau),$$

$$\wp_{ijk}[\delta](w, \tau) := \frac{-1}{(2\pi i)^3} \frac{\partial^3}{\partial w_i \partial w_j \partial w_k} \log \sigma[\delta](w, \tau),$$

$$\wp[\delta](w, \tau) := \wp_{11}\wp_{22} - \wp_{12}^2.$$

Map $F(z, \tau) : \mathbf{C}^2 \rightarrow \mathbf{P}^8$ given by

$$z \mapsto (\sigma^3, \sigma^3 \wp_{11}, \sigma^3 \wp_{12}, \sigma^3 \wp_{22}, \sigma^3 \wp_{111}, \sigma^3 \wp_{112}, \sigma^3 \wp_{122}, \sigma^3 \wp_{222}, \sigma^3 \wp)$$

defines a projective embedding $\mathbf{C}^2/(\tau - 1)\mathbf{Z}^4 \hookrightarrow \mathbf{P}^8$.

That is, $\{\wp_*\}$ are a basis for $\mathcal{L}(3\Theta)$.

Modifications of these \wp_* are weight 0 arithmetic theta functions we can apply Rumely and extensions to resulting embedding.

Can recover model of genus 2 hyperelliptic curve,

$$C[\delta](\tau) : y^2 = x^5 + b_2x^3 + b_3x^2 + b_4x + b_5.$$

Each $b_i = b_i[\delta](\tau)$ modular of weight $3i$, with character.

\wp -like functions given in terms of curve coordinates:

$$\wp_{22}[\delta](w, \tau) = X_1 + X_2,$$

$$\wp_{12}[\delta](w, \tau) = -X_1X_2,$$

$$\wp_{222}[\delta](w, \tau) = -2 \frac{Y_1 - Y_2}{X_1 - X_2},$$

$$\wp_{122}[\delta](w, \tau) = 2 \frac{Y_1X_2 - Y_2X_1}{X_1 - X_2}.$$

Have isomorphism:

$$\text{Jac}(C[\delta](\tau)) \xrightarrow{\sim} F(\tau)$$

Thanks!

Thanks!