

On Jacobians with complex multiplication by $\mathbb{Q}\left(\sqrt{-5 + \sqrt{5}}\right)$

Tomasz Jędrzejak

University of Szczecin

NuTMiC 2026

Introduction

The arithmetic of abelian varieties with complex multiplication (CM) plays a central role in several areas of modern public-key cryptography. In particular, Elliptic Curve Cryptography (ECC) and its higher-dimensional generalizations, such as Hyperelliptic Curve Cryptography (HCC), rely on the group structure of Jacobians of algebraic curves over finite fields. The security of these systems is typically based on the hardness of the discrete logarithm problem in the associated groups, which in turn depends strongly on the arithmetic properties of the underlying curves and their Jacobians. A fundamental aspect influencing both efficiency and security is the type of reduction of an abelian variety at a prime: ordinary, supersingular, or superspecial. These notions are closely tied to the structure of the endomorphism ring and the action of the Frobenius morphism.

Introduction

Definition

An abelian variety A (over $\mathbb{Q}$) of dimension g has *complex multiplication* by a number field L if there is an injective homomorphism $\iota : L \rightarrow \text{End}(A) \otimes \mathbb{Q}$ where $[L : \mathbb{Q}] = 2g$ (then L is necessarily a *CM field*, i.e., a totally imaginary quadratic extension of a totally real field).

Definition

An elliptic curve E defined over a field K of characteristic $p > 0$ is called *ordinary* if $E(\overline{K})[p] \simeq \mathbb{Z}/p\mathbb{Z}$, and *supersingular* if $E(\overline{K})[p] \simeq \{0\}$. An abelian variety A/K where $\dim A = g$ is called *supersingular* (resp. *superspecial*), if A is geometrically isogenous (resp. isomorphic) to a product of supersingular elliptic curves, and *ordinary* if $A(\overline{K})[p] \simeq (\mathbb{Z}/p\mathbb{Z})^g$.

Introduction

By 'Weil conjectures', proven by Dwork, Grothendieck, and Deligne, for a nonsingular algebraic curve C of genus g defined over a finite field $\mathbb{F}_q$, we have

$$Z(C/\mathbb{F}_q, T) = \frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) = \prod_{i=1}^{2g} (1 - \alpha_i T)$ and α_i are algebraic integers of an absolute value $\sqrt{q}$. Moreover,

$$|C(\mathbb{F}_{q^k})| = 1 + q^k - (\alpha_1^k + \alpha_2^k + \dots + \alpha_{2g}^k)$$

and $P(T) = q^g T^{2g} P(1/qT)$. It can be shown that values $|C(\mathbb{F}_{q^k})|$ for $k = 1, \dots, g$ fully express $|C(\mathbb{F}_{q^k})|$ for all $k \geq 1$ and

$$|J(\mathbb{F}_q)| = P(1) = \prod_{i=1}^{2g} (1 - \alpha_i).$$

Introduction

There are 13 families of elliptic curves over $\mathbb{Q}$ with CM; the most famous families $y^2 = x^3 + ax$ and $y^2 = x^3 + a$ having CM by $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ respectively. Note that if $p > 3$ then $E/\mathbb{Q}$ has supersingular reduction at p if and only if $|E(\mathbb{F}_p)| = 1 + p$.

The case of ordinary reduction is more subtle, and the formulae for the number of points (and consequently for zeta functions) are not that simple. Hyperelliptic curves $y^2 = x^5 + a$ (over $\mathbb{Q}$) of genus 2 have CM by the cyclotomic field $\mathbb{Q}(\zeta_5)$. More generally, hyperelliptic curves

$$C^{p,a} : y^2 = x^p + a$$

and superelliptic curves

$$C^{q,p,a} : y^q = x^p + a,$$

where $2 \neq p \neq q$ are primes, have complex multiplication by $\mathbb{Q}(\zeta_p)$ and $\mathbb{Q}(\zeta_{qp})$ respectively.

Introduction

Many researchers have investigated the curves $C^{p,a}$, $C^{q,p,a}$ and their Jacobians $J^{p,a}$ and $J^{q,p,a}$.

Van Wamelen (1997) found the zeta functions of $C^{p,-1}$.

Stoll (1998, 2002) gave a formula of the dimension of the $(1 - \zeta_p)$ -Selmer group of $J^{p,a}$ and determined the L -series and the root numbers.

J. (2013, 2025) received an almost complete characterization of torsion subgroups of $J^{p,a}(\mathbb{Q})$, and obtained upper bounds for the ranks $J^{p,a}(\mathbb{Q})$ respectively. In 2014 I studied torsion parts of $J^{q,p,a}(\mathbb{Q})$, and, to this end, found exact formulae for zeta functions of $C^{q,p,a}$.

Dąbrowski (2014) used these formulae to obtain pairing-friendly families of superelliptic curves of genus 4.

Van Wamelen (1999) obtained 19 families of genus 2 curves defined over $\mathbb{Q}$ such that their Jacobians are simple and have complex multiplication by a quartic CM field.

In 2024 I considered the first 'non-cyclotomic' example (i.e., a CM field is not a cyclotomic field $\mathbb{Q}(\zeta_p)$) from van Wamelen's list, namely, a one-parameter family of hyperelliptic curves of genus 2 (over $\mathbb{Q}$)

$$y^2 = x^5 + 3ax^4 - 2a^2x^3 - 6a^3x^2 + 3a^4x + a^5$$

which has complex multiplication by $\mathbb{Q}(\sqrt{-2 + \sqrt{2}})$, and obtained types of reduction at p in terms of congruences modulo 16 and the exact formulae for the zeta function over $\mathbb{F}_p$ for $p \equiv 3, 5, 9, 11, 13, 15 \pmod{16}$.

Introduction

Now, let consider complex multiplication by $\mathbb{Q}(\sqrt{-5 + \sqrt{5}})$. There are two families of hyperelliptic curves in the van Wamelen list with CM by this field, namely

$$C_a^{(1)} : ay^2 = -4x^5 + 30x^3 - 45x + 22,$$

$$C_a^{(2)} : ay^2 = -8x^6 + 52x^5 - 250x^3 + 321x + 131,$$

where a is a nonzero rational. Note that these curves are the first examples from his list where the class number of a CM field is greater than one (in fact, $\text{cl } \mathbb{Q}(\sqrt{-5 + \sqrt{5}}) = 2$). Let J_a^1 and J_a^2 denote their Jacobian varieties, respectively. Since C_a^1 and C_a^2 is the quadratic twist (by a) of C_1^1 and C_1^2 , respectively, we will assume (without loss of generality) that a is a non-zero squarefree integer

Introduction

We can rewrite (by appropriate replacement of variables) the above equations in the form $C_a^{(1)} : y^2 = f_a^{(1)}(x)$ and $C_a^{(2)} : y^2 = f_a^{(2)}(x)$, where

$$f_a^{(1)}(x) = x^5 - 120a^2x^3 + 2880a^4x + 5632a^5,$$

$$f_a^{(2)}(x) = x^5 + 110ax^4 - 52030a^2x^3 - 5563580a^3x^2 \\ - 177156100a^4x - 1714871048a^5.$$

Since the discriminant of $f_a^{(1)}$ is equal to $2^{34}5^5a^{20}$, the curves $C_a^{(1)}$ and their Jacobians $J_a^{(1)}$ have a good reduction at odd primes not dividing $5a$. Similarly, $C_a^{(2)}$ and $J_a^{(2)}$ have a good reduction at odd primes not dividing $55a$.

Results

Let C_a be any of the curves $C_a^{(1)}$, $C_a^{(2)}$, and $J_a = \text{Jac } C_a$.

Theorem (J. 2026)

Let p be an odd prime not dividing $55a$, and $Z(C_a/\mathbb{F}_p, T)$ denote the zeta function of C_a over $\mathbb{F}_p$.

1) If $p \equiv 3, 7 \pmod{10}$ then J_a has a supersingular (but not a superspecial) reduction at p and

$$Z(C_a/\mathbb{F}_p, T) = \frac{p^2 T^4 + 1}{(1 - T)(1 - pT)}.$$

In particular,

$$|C_a(\mathbb{F}_p)| = 1 + p, \quad |C_a(\mathbb{F}_{p^2})| = 1 + p^2, \quad |J_a(\mathbb{F}_p)| = 1 + p^2.$$

Theorem (cont. J. 2026)

2) If $p \equiv 9, 11, 21, 39 \pmod{40}$ then J_a has a superspecial reduction at p and

$$Z(C_a/\mathbb{F}_p, T) = \frac{(pT^2 + 1)^2}{(1 - T)(1 - pT)}.$$

In particular,

$$|C_a(\mathbb{F}_p)| = 1 + p, \quad |C_a(\mathbb{F}_{p^2})| = 1 + 4p + p^2, \quad |J_a(\mathbb{F}_p)| = (1 + p)^2.$$

3) If $p \equiv 1, 19, 29, 31 \pmod{40}$ then J_a has an ordinary reduction at p .

Remark

In the last case, one can show that

$$Z(C_a/\mathbb{F}_p, T) = \frac{p^2 T^4 + a_1 p T^3 + a_2 T^2 + a_1 T + 1}{(1 - T)(1 - pT)},$$

where a_1, a_2 are integers such that $p \nmid a_1 a_2$, $2 \mid a_2$. Moreover, they both depend only on p and $\left(\frac{a}{p}\right)$.

Remark

For $p \equiv 9, 11, 21, 39 \pmod{40}$ the number of points on the curve C_a over $\mathbb{F}_{p^2}$ reaches the Hasse upper bound. Moreover, in this case the reduction $\overline{J}_a$ at p is already isomorphic to a product of two supersingular elliptic curves over $\mathbb{F}_p$ which is stronger that $\overline{J}_a$ is superspecial.

Results

We can deduce the following information about the group structure of Jacobians: in particular, the torsion subgroup and the rank of $J_a(\mathbb{Q})$. Note that $G[m] := \{g \in G : mg = 0\}$ denotes the m -torsion subgroup of an abelian group G where $m \in \mathbb{Z}$.

Proposition

Let $a \neq 0$. If prime $p \equiv 3, 7 \pmod{10}$ and $p \nmid a$ then $J_a(\mathbb{F}_p)[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z}$, and consequently, $J_a(\mathbb{Q})[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z}$.

Corollary

For any $a \neq 0$, we have $J_a(\mathbb{Q})_{\text{tors}} = J_a(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. More precisely,

$$J_a^{(1)}(\mathbb{Q})_{\text{tors}} = \{0, [(8a, 0) - \infty]\},$$

$$J_a^{(2)}(\mathbb{Q})_{\text{tors}} = \{0, [(-242a, 0) - \infty]\}.$$

Corollary

If there is a point $(x, y) \in C_a(\mathbb{Q})$ with $y \neq 0$ then $\text{rank } J_a(\mathbb{Q}) \geq 1$. In other words, if $\text{rank } J_a(\mathbb{Q}) = 0$ then $|C_a(\mathbb{Q})| = 2$, or more precisely,

$$C_a^{(1)}(\mathbb{Q}) = \{\infty, (8a, 0)\},$$

$$C_a^{(2)}(\mathbb{Q}) = \{\infty, (-242a, 0)\}.$$

We start with well-known properties of Jacobians. For a hyperelliptic curve $C : y^2 = f(x)$ defined over a field K , let J denote the Jacobian variety of C , and let us recall that $J(K)[m]$ is the kernel of the multiplication by m endomorphism of the Mordell-Weil group $J(K)$. The following lemma allows us to compute the group $J(K)[2]$.

Lemma

Let K be a finite field of odd characteristic or an extension of $\mathbb{Q}$. Let $f(x) = f_1(x) \dots f_s(x)$, where $f_i \in K[x]$ are mutually distinct monic polynomials irreducible in $K[x]$. Then

$$J(K)[2] \cong (\mathbb{Z}/2\mathbb{Z})^{s-1}.$$

The next lemma concerns the embedding of the torsion subgroup of the Mordel-Weil group.

Lemma

Let $C : y^2 = f(x)$ (where $f \in \mathbb{Z}[x]$) be a hyperelliptic curve over $\mathbb{Q}$ and let p be a prime such that $p \nmid 2 \operatorname{disc}(f)$. Then the reduction modulo p homomorphism induces the embedding

$$J(\mathbb{Q})_{\text{tors}} \hookrightarrow J(\mathbb{F}_p).$$

In particular,

$$|J(\mathbb{Q})_{\text{tors}}| \text{ divides } |J(\mathbb{F}_p)|.$$

Proof of Proposition

It suffices to prove the non-existence of a point of order 4. Let us recall that $p \equiv 3, 7 \pmod{10}$. We consider separately the curves $C_a^{(1)}$ and $C_a^{(2)}$. First, we get, $f_a^{(1)}(x) = (x - 8a) h_a(x)$ where $h_a(x) := x^4 + 8ax^3 - 56a^2x^2 - 448a^3x - 704a^4 \in \mathbb{F}_p[x]$. The polynomial h_a has the following roots (in $\overline{\mathbb{F}}_p$): $2 \left(-a - a\sqrt{5} - a\sqrt{5 - \sqrt{5}} \right)$, $2 \left(-a - a\sqrt{5} + a\sqrt{5 - \sqrt{5}} \right)$, $2 \left(-a + a\sqrt{5} - a\sqrt{5 + \sqrt{5}} \right)$, and $2 \left(-a + a\sqrt{5} + a\sqrt{5 + \sqrt{5}} \right)$. Since $\left(\frac{5}{p}\right) = -1$, that is $\sqrt{5} \notin \mathbb{F}_p$, we obtain that it is irreducible in $\mathbb{F}_p[x]$. Therefore, by Lemma 7, $J_a^{(1)}(\mathbb{F}_p)[2] = \langle [(8a, 0) - \infty] \rangle$. Let $D_1 = (8a, 0) - \infty$, so $[D_1]$ is the unique element of order 2 in $J_a^{(1)}(\mathbb{F}_p)$. Then the group $J_a^{(1)}(\mathbb{F}_p)$ has an element of order four if and only if $[D_1] \in 2J_a^{(1)}(\mathbb{F}_p)$.

Proof of Proposition cont.

Now we use the Cassels map. This map has been exploited in the 2-descent method for Jacobians of hyperelliptic curves in the computation of 2-Selmer groups. We define $\mathbb{F}_p$ -algebra

$$\begin{aligned}\mathbb{F}_p[\Theta] &:= \mathbb{F}_p[x] / \left(f_a^{(1)}(x)\right) \simeq \mathbb{F}_p[x] / (x - 8a) \times \mathbb{F}_p[x] / (h_a(x)) \\ &\simeq \mathbb{F}_p \times \mathbb{F}_p(\beta),\end{aligned}$$

where β is a root of h_a . Note that we can put $\Theta = (8a, \beta)$. For a degree zero divisor $d = \sum n_Q Q$ of $C_a^{(1)}$ over $\mathbb{F}_p$ whose support does not include any Weierstrass points, i.e., the point at infinity ∞ and points with zero y -coordinate, we set

$$\delta_p(d) := \prod_Q (x_Q - \Theta)^{n_Q} \in \mathbb{F}_p[\Theta],$$

where $Q = (x_Q, y_Q)$. This map induces the well-defined map from $J_a^{(1)}(\mathbb{F}_p)$ which is an injection from $J_a^{(1)}(\mathbb{F}_p) / 2J_a^{(1)}(\mathbb{F}_p)$ to $\mathbb{F}_p[\Theta]^\times / \mathbb{F}_p[\Theta]^{\times 2}$.

Proof of Proposition cont.

We get that

$$\begin{aligned}\delta_p([D_1]) &= (-1)(\Theta - 8a) + (-1)^4 h_a(\Theta) \\ &= (h_a(8a) - 8a + 8a, h_a(\beta) - \beta + 8a) \\ &= (320a^4, 8a - \beta) = (5, 8a - \beta) \pmod{\mathbb{F}_p^{\times 2} \times \mathbb{F}_p(\beta)^{\times 2}}.\end{aligned}$$

Since 5 is not a square in $\mathbb{F}_p^\times$, we obtain, $\delta_p([D_1]) \notin \mathbb{F}_p[\Theta]^{\times 2}$, and consequently, $[D_1] \notin 2J_a^{(1)}(\mathbb{F}_p)$, which proves that $J_a^{(1)}(\mathbb{F}_p)[2^\infty] \simeq \mathbb{Z}/2\mathbb{Z}$. The polynomial h_a is also irreducible over $\mathbb{Q}$. Hence, by Lemma 1, $J_a^{(1)}(\mathbb{Q})[2] = \langle [(8a, 0) - \infty] \rangle$. Moreover, by Lemma 2, $J_a^{(1)}(\mathbb{Q})[2^\infty] \hookrightarrow J_a^{(1)}(\mathbb{F}_p)[2^\infty]$, and the assertion for $J_a^{(1)}$ follows. The case $C_a^{(2)}$ is proceed similarly.

The following proposition, which is also of independent interest, plays a key role in the proof of the main result.

Proposition

Let $p \neq 5$ be an odd prime and let $L = \mathbb{Q}(\sqrt{-5 + \sqrt{5}})$. We have

- 1) 2 and 5 are the only ramified primes in L ,*
- 2) p is inert in L if and only if $p \equiv 3, 7 \pmod{10}$,*
- 3) p splits in two prime ideals in L if and only if $p \equiv 9, 11, 21, 39 \pmod{40}$,*
- 4) p splits completely in L if and only if $p \equiv 1, 19, 29, 31 \pmod{40}$.*

Proof of Proposition

First, we claim that L is contained in the cyclotomic field $\mathbb{Q}(\zeta_{40})$ and it is the fixed field of the subgroup

$\langle 19, 29 \rangle = \{1, 19, 29, 31\} \subset (\mathbb{Z}/40\mathbb{Z})^\times \simeq \text{Gal}(\mathbb{Q}(\zeta_{40})/\mathbb{Q})$. Indeed, one can compute that

$$\cos \frac{\pi}{20} = \frac{1 + \sqrt{5}}{4\sqrt{2}} + \frac{\sqrt{5 - \sqrt{5}}}{4}, \quad \sin \frac{\pi}{20} = \frac{1 + \sqrt{5}}{4\sqrt{2}} - \frac{\sqrt{5 - \sqrt{5}}}{4},$$

and consequently, we obtain,

$$\begin{aligned} \sqrt{-5 + \sqrt{5}} &= 2i \left(\cos \frac{\pi}{20} - \sin \frac{\pi}{20} \right) = 2i \operatorname{Im}(i\zeta_{40} - \zeta_{40}) \\ &= i\zeta_{40} - \zeta_{40} - \overline{i\zeta_{40}} + \overline{\zeta_{40}} = -(\zeta_{40} + \zeta_{40}^{19} + \zeta_{40}^{29} + \zeta_{40}^{31}). \end{aligned}$$

Proof of Proposition cont.

The decomposition of primes follows from the description of Frobenius automorphisms in cyclotomic extensions, together with the fact that for subfields the Frobenius is given by the image of p in the quotient of the Galois group. This implies that the splitting of p in L depends only on the group structure of $\langle p, 19, 29 \rangle / \langle 19, 29 \rangle$, and consequently on $p \bmod 40$. In particular, the primes dividing 40 are the only ramified primes in L , hence 2 and 5 are the only ramified primes. Next, let $p \neq 2, 5$, and $H = \langle 19, 29 \rangle$. Then, p is inert in L if and only if $p^2 \bmod 40 \notin H$ (so $p \equiv 3, 7 \pmod{10}$), p splits in two prime ideals in L if and only if $p \bmod 40 \notin H$ but $p^2 \bmod 40 \in H$ (i.e., $p \equiv 9, 11, 21, 39 \pmod{40}$), and finally p splits completely in L if and only if $p \bmod 40 \in H$, which completes the proof.

Proof of Theorem

We consider both curves $C_a^{(1)}$, $C_a^{(2)}$ simultaneously, and denote them by C_a . Let $P_a(T)$ denote the polynomial in the numerator of the zeta function of C_a . Our proof starts with the case $p \equiv 3, 7 \pmod{10}$. By Proposition, p is inert in $L = \mathbb{Q}(\sqrt{-5 + \sqrt{5}})$. Recall that the Jacobian $J_a = \text{Jac } C_a$ has CM by L . Hence, by the Goren theorem, J_a has a supersingular reduction at p . It suffices to calculate the polynomial $P_a(T)$. By 'Weil conjectures', we know that

$$P_a(T) = p^2 T^4 + pa_1 T^3 + a_2 T^2 + a_1 T + 1$$

where

$$\begin{aligned} a_1 &= |C_a(\mathbb{F}_p)| - p - 1, \\ 2a_2 &= a_1^2 + |C_a(\mathbb{F}_{p^2})| - p^2 - 1. \end{aligned}$$

Proof of Theorem cont.

Since the reduction is supersingular, due to Oort, all slopes of the Newton polygon of P_a are equal to $1/2$. Therefore, $p \mid a_1$ and $p \mid a_2$.

Consequently, since by the Hasse theorem, $||C_a(\mathbb{F}_q)| - q - 1| \leq 4\sqrt{q}$ for $q = p^k$, we obtain that $|a_1| \leq 4\sqrt{p}$, and so $a_1 = 0$ for $p > 16$ (and for remaining primes it follows from the direct calculation). Then,

$2a_2 = |C_a(\mathbb{F}_{p^2})| - p^2 - 1$, and so $|a_2| \leq 2p$, i.e., $a \in \{0, \pm p, \pm 2p\}$. If $a_2 = \pm p$ then $|J_a(\mathbb{F}_p)| = P_a(1) = 1 \pm p + p^2 \equiv 1 \pmod{2}$ but $J_a(\mathbb{F}_p)$ has an element of order two. We thus get $a_2 \neq \pm p$. Similarly, if $a_2 = \pm 2p$ then $|J_a(\mathbb{F}_p)| = P_a(1) = (1 \pm p)^2 \equiv 0 \pmod{4}$ but by Proposition, $J_a(\mathbb{F}_p)$ has no element of order four and only one element of order 2. Hence $a_2 = 0$, and $P_a(T) = p^2 T^4 + 1$.

Proof of Theorem cont.

Now, assume that $p \equiv 9, 11, 21, 39 \pmod{40}$. Then, p splits into two prime ideals in L . Moreover, since $\left(\frac{5}{p}\right) = 1$, p splits completely in $K = \mathbb{Q}(\sqrt{5})$ (the maximal totally real subfield of L), say $p\mathcal{O}_K = \mathfrak{p}\mathfrak{q}$. Then, clearly each prime ideal $\mathfrak{p}, \mathfrak{q}$ remains prime in L and the action of $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ is defined over $\mathbb{F}_p$. Consequently, by the Sugiyama theorem, J_a has a superspecial reduction at p , more precisely, its reduction $\overline{J}_a$ is isomorphic (over $\mathbb{F}_p$) to a product of two supersingular elliptic curves. Furthermore, $P_a(T) = (pT^2 + 1)^2$. Finally, let $p \equiv 1, 19, 29, 31 \pmod{40}$. Then, p splits completely in L . Hence, due to Gorem or Sugiyama, J_a has an ordinary reduction at p , and the assertion follows.

Proof of Corollaries

We prove Corollary 1 as follows. Let $q \neq 5$ be any odd prime. By the Dirichlet theorem on arithmetic progressions and the Chinese remainder theorem, there exists a prime p (in fact, infinitely many) such that $p \equiv 5 \pmod{8}$, $p \equiv 1 \pmod{5}$, $p \equiv 1 \pmod{q}$, and $p > |a|$. Then $p \equiv 21 \pmod{40}$ and $p \nmid 55a$. Hence, by Theorem, $|J_a(\mathbb{F}_p)| = (1 + p)^2$. Since $(1 + p)^2 \equiv 4 \pmod{40q}$ and, by Lemma 2, $|J_a(\mathbb{Q})_{\text{tors}}|$ divides $|J_a(\mathbb{F}_p)|$, we get that $8 \nmid |J_a(\mathbb{Q})_{\text{tors}}|$, $5 \nmid |J_a(\mathbb{Q})_{\text{tors}}|$, and $q \nmid |J_a(\mathbb{Q})_{\text{tors}}|$. Moreover, by Proposition, $J_a(\mathbb{Q})$ has no element of order four and only one element of order 2, and we are done.

Now we prove Corollary 2. By Corollary 1, the divisor $(x, y) - \infty$ gives the element of infinite order in $J_a(\mathbb{Q})$, which is our claim.

- J. W. S. Cassels, E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge University Press, 1996.
- A. Dąbrowski, *A family of pairing-friendly superelliptic curves of genus 4*, *Studia Bezpieczeństwa Narodowego* **6**, No. 2 (2014), 133-137.
- E. Z. Goren, *On certain reduction problems concerning abelian surfaces*, *Manuscripta Math.* **94** (1997), 33-43.
- T. Jędrzejak, *On hyperelliptic Jacobians with complex multiplication by $\mathbb{Q}(\sqrt{-2 + \sqrt{2}})$* , *Finite Fields Appl.* **100** (2024), Paper No. 102512, 9 pp.
- T. Jędrzejak, *Ranks of quadratic twists of Jacobians of generalized Mordell curves*, *J. Algebra* **663** (2025), 565-588.

- F. Oort, *Subvarieties of moduli spaces*, Invent. Math. **24** (1974), 95–119.
- M. Stoll, *On the Arithmetic of the Curves $y^2 = x^l + A$ and their Jacobians*, J.reine angew. Math. **501** (1998), 171-189.
- M. Stoll, *On the Arithmetic of the Curves $y^2 = x^l + A$, II*, J. Number Theory **93** (2002), 183-206.
- K. Sugiyama, *On a generalization of Deuring's results*, Finite Fields Appl. **26** (2014), 69-85.
- P. van Wamelen, *Examples of genus two CM curves defined over the rationals*, Math. Comp. **68** (1999), no. 225, 307-320.

Thanks

Thank you for your attention!