# Abelian varieties and Weil numbers
# University of Pennsylvania, Columbia University, October 2013

Other options:
Abelian varieties over finite fields.
A construction of abelian varieties having a given Weil number as Frobenius.

## Topics to be discussed

In this talk the following topics

- We define the notion of an **abelian variety**,

  give examples, and show properties over the complex numbers.
- **Abelian varieties over finite fields.**
- Definition of **Weil $q$-numbers.**
- A proof for the **Weil conjecture for abelian varieties**.
- **Honda-Tate theory.**
- A proof for the **surjectivity** in the Honda-Tate theory

  (joint work Ching-Li Chai - FO).

Notation; $p$ will be a prime number, $n \in \mathbb{Z}_{>0}$, and $q := p^n$;
write $\kappa = \mathbb{F}_q$, the field with $q$ elements;
$K$ for any field, and $k = \overline{k}$ an algebraically closed field.

Classically abelian varieties have been constructed via analytic parametrizations;

$$0 \to \Lambda \cong \mathbb{Z}^{2g} \to \mathfrak{t}_{A,0} \cong \mathbb{C}^g \to A(\mathbb{C}) \to 0;$$

we will discuss these.

For arithmetic and for many questions in algebraic geometry analytic methods in many cases do not give enough information. Algebraic methods and constructions are necessary, especially for abelian varieties over finite fields.

The Weil conjecture for abelian varieties shows that the Frobenius of an abelian variety has absolute value $\sqrt{q}$,

**Theorem** (Weil, 1948, 1949).

$$\pi_A = \mathrm{Frob}_{A/\mathbb{F}_q}, \quad \psi : \mathbb{Q}(\pi_A) \to \mathbb{C}, \quad \mid \psi(\pi_A) \mid = \sqrt{q}.$$

We sketch a beautiful and rapid proof of this theorem by André Weil. We give an application (bounds on number of rational points).

This theorem assigns to a simple abelian variety $A$ over $\kappa = \mathbb{F}_q$ a Weil $q$-number.
This allows us via the Honda-Tate theory to classify isogeny classes of abelian varieties over a finite field.

Beforehand surjectivity of the map given by $A \mapsto \pi_A$ was done via analytic parametrizations: (the construction of CM abelian varieties over $\mathbb{C}$):

**Theorem** (Honda, Tate, 1968). *For every Weil $q$-number $\pi$ there exists an abelian variety $A$ over $\mathbb{F}_q$ such that*

$$\pi \sim \pi_A := \mathrm{Frob}_{A/\mathbb{F}_q}.$$

In this talk we present a proof (joint work Ching-Li Chai – FO) with methods in algebraic geometry.

# 1 Abelian varieties

An abelian variety over a field $K$ is a connected projective group variety over $K$. This implies (Weil) the group law to be commutative. The name "abelian variety" comes from the fact that Niels Henrik Abel constructed such varieties in order to determine values of *abelian integrals on Riemann surfaces.*

**An example.** A plane cubic curve $E \subset \mathbb{P}^2_K$ which is non-singular, and with a point $0 \in E(K)$ chosen is an abelian variety (of dimension one, and every abelian variety of dimension one can be described this way). These play often a decisive role in geometry and in number theory.

Weierstrass described analytic parametrizations of elliptic curves using $\wp-$functions. This is a particular case of the following. Consider an abelian variety $A$ over $k = \mathbb{C}$. The tangent space $\mathfrak{t}_{A,0}$ of $A$ at the origin is a $\mathbb{C}$-vector space of dimension equal to $\dim(A)$. The theory of commutative Lie-groups constructs an analytic map

$$\exp : \mathfrak{t}_{A,0} \longrightarrow A(\mathbb{C}).$$

Using the fact that $A(\mathbb{C})$ is compact we arrive at an exact sequence

$$0 \to \Lambda \cong \mathbb{Z}^{2g} \to \mathfrak{t}_{A,0} \cong \mathbb{C}^g \to A(\mathbb{C}) \to 0.$$

This gives a useful analytic and topological description of abelian varieties. However for arithmetic applications this is insufficient. Hence abelian varieties over number fields, in mixed characteristic and over finite fields have been studied intensively, where the analytic picture often was used as motivation, but methods were not analytic. The main emphasis: use methods of algebraic geometry and of number theory to study such objects,

## 2 Weil numbers

**Definition.** Fix $q := p^n$. A Weil $q$-number $\pi$ is an *algebraic integer*, such that for every

$$\psi : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}, \quad \mid \psi(\pi_A) \mid = \sqrt{q}.$$

We show:
– these numbers are easy to classify;
– such numbers can easily be constructed.

**Example.**
– Let $\zeta_s$ be a $s$-th root of unity. The number $\zeta_s{\cdot}p$ is a Weil $p^2$-number. (This example was crucial in the theory of CM liftings.)

**Example.**
– Let $f \in \mathbb{Q}[T]$ be an irreducible polynomial such that all zeros are real (e.g. $f = Z^3 - 3Z + 1$). Let $\beta$ be a zero of $f$. Choose $q := p^n$ such that $\psi(\beta)^2 - 4q < 0$ for every real embedding $\psi : \mathbb{Q}(\beta) \hookrightarrow \mathbb{R}$ (observe $\mid \psi(\beta) \mid < 2$ in the example, and choose any $q$). Let $\pi$ be a zero of

$$T^2 - \beta{\cdot}T + q, \quad \psi(\beta)^2 < 4q \text{ for every } \psi.$$

We see that $\pi$ thus defined is a Weil $q$-number. (This example is given in order to convince you that it is easy to construct Weil numbers.)

**Example, start classification.**
It is possible that a Weil $q$-number is real. This happens if and only if:
**even** $\pi \in \mathbb{Q}$, $q := p^n$ with $n$ even and $\pi = \pm p^{n/2}$;
**odd** $\pi \notin \mathbb{Q}$, $q := p^n$ with $n$ odd and $\pi = \pm\sqrt{q}$.

**Remark.** If there exists at least one embedding $\tau : \mathbb{Q}(\pi) \hookrightarrow \mathbb{R}$, then all conjugates of $\pi$ are real.
**Proof.** $\psi(\pi){\cdot}\overline{\psi(\pi)} = q$ and $\overline{\tau(\pi)} = \tau(\pi)$ shows $\pi = \pm\sqrt{q}$.
(Here $\overline{z}$ is the complex conjugate of $z$.)

**Classification.**
Suppose $\pi$ is a Weil $q$-number such that for at least $\tau : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ we have that $\tau(\pi)$ is *not real.* Write $\beta := \pi + (q/\pi) \in \mathbb{Q}(\pi)$ Then:
(1) $\overline{\psi(\pi)} = \psi(q/\pi)$ for every $\psi$;
(2) as $\tau(\pi) \notin \mathbb{R}$ we see $\pi \neq q/\pi$;
(3) $\beta$ is totally real;
(4) $\pi$ is totally complex.
**Proof.** (1) + (2) $\psi(\pi){\cdot}\overline{\psi(\pi)} = q$;
(3) $\overline{\psi(\beta)} = \overline{\psi(\pi)} + \overline{\psi(q/\pi)} = \beta$;

(4) follows from(2).
We see:

$\pi$ is a zero of $T^2 - \beta{\cdot}T + q$, with
$\beta$ totally real, and
$\psi(\beta^2 - 4q) < 0$ for every $\psi$.

**Remark / definition.** A finite extension $L \supset \mathbb{Q}$ is called a CM field if there exists $\mathbb{Q} \subset L_0 \subset L$ such that $L_0$ is totally real (every embedding of $L_0$ into $\mathbb{C}$ lands into $\mathbb{R}$) and $L$ is totally complex ($L$ has no real embeddings).

Equivalently: for every embedding $L \hookrightarrow \mathbb{C}$ complex conjugation induces a nontrivial conjugation on $L$.
We have seen that any non-real Weil number $\pi$ gives a CM field $L_0 = \mathbb{Q}(\beta) \subset L = \mathbb{Q}(\pi)$.

## 3 The Weil conjecture for abelian varieties and for algebraic curves over finite fields

Varieties defined over a finite field have an extra structure.

For a variety $W$ defined over a field $\kappa \supset \mathbb{F}_p$ we define $W^{(p)}$ and

$$F : W \longrightarrow W^{(p)} :$$

if $W$ is given by equations $\sum a_\gamma X^\gamma$ we define $W^{(p)}$ by the equations $\sum a_\gamma^p X^\gamma$. For a point $P \in W$ with coordinates $x_i$ we define $F(P)$ with coordinates $x_i^p$. Note that if $\sum a_\gamma x^\gamma = 0$ then $\sum a_\gamma^p x^{p\gamma} = 0$, and we conclude $F(P) \in W^{(p)}$.

For a variety $W$ defined over the field $\kappa = \mathbb{F}_q$, with $q = p^n$ we define

$$\pi = \mathrm{Frob}_{W/\kappa} : W \longrightarrow W, \quad \text{“} \ \pi = F^n \ \text{''}.$$

Indeed, the definitions imply $W^{(q)} = W$.
Surprising fact: every variety over a finite field has a natural map into itself.
Useful: the set $W(\mathbb{F}_q)$ of $\kappa-$rational points in $W$ is the set of fixed points of this self-map (hence we see that this map is not the identity for positive-dimensional $W$). .
Clear: for a group scheme $G$ the maps $F : G \to G^{(p)}$ and $\mathrm{Frob}_{G/\kappa} : G \to G$ are homomorphisms.

**Reminder.** For a simple abelian variety $A$ the ring $\mathrm{End}(A)$ has no zero divisors, and $\mathrm{End}^0(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division ring.

As is well known, the $\mathbb{Z}-$rank of $\mathrm{End}(A)$ is finite; hence every element of $\mathrm{End}(A)$ is an algebraic integer.

**Conclusion.** For a simple abelian variety $A$ over $\kappa = \mathbb{F}_q$ its Frobenius endomorphism $\pi_a = \pi \in \mathrm{End}(A)$ is an algebraic integer.

**Theorem** (the Weil conjecture for abelian varieties; André Weil, 1948, 1949). *For every $\psi : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$ we have*

$$| \psi(\pi) |= \sqrt{q}.$$

I.e. $\pi_A$ is a Weil $q-$number.

An aside:
**Application** (the Hasse-Weil bound). *Let $C$ be a complete, nonsingular curve over $\mathbb{F}_q$ of genus $g > 0$. The number of $\kappa-$rational points satisfies the following bound:*

$$| \#(C(\mathbb{F}_q)) - (q + 1) |\leq 2g{\cdot}\sqrt{q}.$$

## 4 A proof of the Weil conjecture for abelian varieties.

**Duality for abelian varieties.**
For an abelian variety $A$ over a field $K$ we define its dual abelian variety $A^t$. This is the connected component of its Picard variety: $A^t = \underline{\mathrm{Pic}}^0_{A/K}$. It turns out (no further explanation given here) that $A^t$ is an abelian variety with $\dim(A^t) = \dim(A)$ (and several other properties).

A polarization (no further explanation given here) $\mu : A \to A^t$ together with duality defines a homomorphism

$$\mathrm{End}^0(A) \longrightarrow \mathrm{End}^0(A), \quad \gamma \mapsto \gamma^\dagger.$$

This is defined by:

$$\gamma^\dagger = \mu{\cdot}\gamma^t{\cdot}\mu^{-1}.$$

The following properties hold:

**Lemma I.** *For every $\gamma \in \mathrm{End}^0(A)$ and every $\psi : \mathbb{Q}(\gamma) \hookrightarrow \mathbb{C}$ we have:*

$$\psi(\beta^\dagger) = \overline{\psi(\gamma)}.$$

(This is a general fact for abelian varieties over an arbitrary field. With $K = \mathbb{C}$ this can be proved using complex uniformization.)

In short: “duality induces complex conjugation on endomorphisms”.

**Lemma II.** *For an abelian variety $A$ over $\kappa = \mathbb{F}_q$ we have:*

$$\pi_{A/\kappa}{\cdot}(\pi_{A/\kappa})^\dagger = q.$$

(This is a general fact about duality of commutative group schemes in positive characteristic.)
From

$$\left(A \xrightarrow{F} A^t \xrightarrow{F^t} A^{tt} = A\right) = p$$

and from " $\pi = F^n$ " the result follows. The result of this lemma we already see foreshadowed in a letter by Serre; at that moment (October 1959) the characteristic $p$ theory about the "Verschiebung" plus " $F^t = V$ " was not yet developed.)

**Proof of** $\mid \psi(\pi) \mid = \sqrt{q}$**, for** $\pi = \pi_A$**.**
Choose $\psi : \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$.

$$q = \psi(q) \overset{I}{=} \psi(\pi{\cdot}\pi^{\dagger}) = \psi(\pi)\psi(\pi^{\dagger}) \overset{II}{=} \psi(\pi)\overline{\psi(\pi)}.$$

Hence $\mid \psi(\pi) \mid = \sqrt{q}$.

# 5 Honda-Tate theory

Notation: $A \sim B$ for an isogeny between abelian varieties;
$\gamma \sim \gamma'$ for a conjugation between algebraic numbers,
i.e. existence of an isomorphism $\mathbb{Q}(\gamma) \to \mathbb{Q}(\gamma')$ with $\gamma \mapsto \gamma'$.

Honda-Tate theory classifies (isogeny classes of) abelian varieties with the help of Weil numbers:

**Theorem** (Honda, Tate, 1968). *Let $q = p^n$. The map $A \mapsto \pi_A$, made possible by Weil, induces a* **bijection**

$$\{\text{simpleAV}/\mathbb{F}_q\}/\sim \quad \longrightarrow \quad \{\text{Weil} \;\; q-\text{number}\}/\sim .$$

The fact

$$\pi_A \sim \pi_B \quad \Longleftrightarrow \quad A \sim B$$

is due to Tate. The surjectivity of the map is (mainly) due to Taira Honda.

# 6 Every Weil number is the Frobenius of an abelian variety over a finite field

**Theorem** (Honda, Tate, 1968). *For every Weil $q-$number $\pi$ there is an abelian variety $A$ over $\mathbb{F}_q$ with $\pi \sim \pi_A$.*

We present a new, algebraic proof of this result.

*Notation, property.*
We say $\pi$ is *effective* if there exists an abelian variety $A$ with $\pi \sim \pi_A$.
**Note** that

$$(\pi_A)^m = \pi_{A \otimes \mathbb{F}_{q^m}}.$$

**Lemma** (Tate). Let $m \in \mathbb{Z}_{>0}$

$$\pi \text{ is effective} \quad \Longleftrightarrow \quad \pi^m \text{ is effective.}$$

This shows we need not worry in the proof of the surjectivity about the size of the finite base field.

In the proof we are expected to construct an abelian variety with given Weil number. We first present the proof in *special case* we have to construct an *elliptic curve.* Once we have the proof in that special case, we will see that the general case follows along the same line of thought, provided some minor technical details are solved.

**First observation.** Suppose a Weil number $\pi$ is given such that there exists $m \in \mathbb{Z}_{>0}$ with $\pi^m \in \mathbb{Q}$. In that case we are done: by Tate's Lemma it suffices to prove $\pi^m$ is effective. The Weil number of an abelian variety $E$ over a finite field is in $\mathbb{Q}$ if and only if $E$ is a supersingular curve.

**Easy Fact.** *For every prime number $p$ there exists a supersingular elliptic curve in characteristic $p$.*
**Proof.** For $p = 2$ consider the curve defined by $Y^2 + y = X^3$. For $p > 2$ consider $Y^2 = X(X-1)(X-\lambda)$; for $(p-1)/2$ values of $\lambda$ this defines a supersingular curve.

**Unimportant remarks.** Such a curve can be defined over $\mathbb{F}_{p^2}$. Any two supersingular elliptic curves over $\overline{\mathbb{F}_p}$ are isogenous.

**Conclusion.** *Any Weil number $\pi$ with $\pi^m \in \mathbb{Q}$ is effective.*

**Proof in a special case.**

Suppose $\pi$ is Weil number such that the expected $A$ is a non-supersingular elliptic curve (called an "ordinary elliptic curve"). This is the case if and only if:

- $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2$, an imaginary quadratic field;
- the prime number $p$ is *split* in $\mathbb{Q}(\pi)/\mathbb{Q}$;
- for the two valuations of $\mathbb{Q}(\pi)$ dividing $p$ we have $v_1(\pi) = 1$ and $v_2(\pi) = 0$ (or the other way around).

We suppose these three properties to hold for the Weil $q$-number $\pi$ and we are going to construct $E$, i.e. we show that in this case $\pi$ *is effective.*

**Proof.**
**Step 1.** We have the three properties above, especially $v_1(\pi) = 1$ and $v_2(\pi) = 0$. We write $L = \mathbb{Q}(\pi)$.

**Step 2.** We choose a prime number $r$ such that $r$ is *non-split* in $L/\mathbb{Q}$ (this is possible: roughly half of the prime numbers have this property by Chebotarov). We choose a supersingular elliptic curve $E_1$ over $\kappa_1 = \overline{\mathbb{F}_r}$. We know that $D = \mathrm{End}(E_1)$ is a quaternion division algebra in which $r$ is non-split. Hence we can choose an embedding $L \subset D = \mathrm{End}(E_1)$.

**Step 3.** Choose any $\gamma \in \mathcal{O}_L$ with $\gamma \notin \mathbb{Z}$.
**Lemma** (Deuring, 1942). *The pair $(E_1, \gamma)$ can be lifted to characteristic zero.*
(Time permitting, we will present a nice and clean proof.) The resulting elliptic curve will be called $E_2$, it is defined over a field of characteristic zero, and $L \subset \mathrm{End}^0(E_2)$.

**Step 4.** The curve $E_2$ has CM by (an order in) $L$. General theory implies a CM abelian variety can be defined over a number field. Moreover abelian varieties with (sufficiently many) CM have potentially good reduction (at all primes).
**Conclusion.** *We can choose an elliptic curve $E_3$ defined over a number field $K$, with $L \subset \mathrm{End}^0(E_3)$ such that there exists*

$$K \supset \mathcal{O}_K \to \kappa_4 \supset \mathbb{F}_p$$

*such that $E_4 := E_3 \otimes \kappa_4$ is an elliptic curve with $L \subset \mathrm{End}^0(E_4)$.*

**Step 5.** Note that $p$ is split in $L/\mathbb{Q}$. Write $\rho := \pi_{E_4/\kappa_4}$. We see that $E_4$ is not supersingular, because $L \subset \mathrm{End}^0(E_4)$ (in fact equality holds). We suppose $v_1(\rho) = 1$ and $v_2(\rho) = 0$; if however this is not the case, we choose the embedding $L \hookrightarrow \mathrm{End}^0(E_4)$ after first applying complex conjugation. Choose $q'$ such that $\mathbb{F}_{q'}$ contains $\kappa_4$, with $[\mathbb{F}_{q'} : \kappa_4] = a$ and $\mathbb{F}_{q'}$ contains $\mathbb{F}_q$ with $[\mathbb{F}_{q'} : \mathbb{F}_q] = b$. Let $\rho' := \rho^a$ and $\pi' = \pi^b$.
**Claim.** *The fraction $\rho'/\pi'$ is a root of unity.*
**Proof.** We know that $\pi$ and $\rho$ are units at all places not dividing $p$.

At the two places above $p$ they have the same order.

Conclusion: $\rho'/\pi'$ is a unit at all finite places; in particular $\rho'/\pi' \in \mathcal{O}_L$.

Note that the Weil conjecture implies that for every $\psi : L \to \mathbb{C}$ we have

$$\mid \psi(\rho'/\pi') \mid = 1.$$

Hence in the lattice $(\psi_1, \psi_2)(\mathcal{O}_L)$ the element $\rho'/\pi'$ lands into the intersection of this lattice with the unit circle; as this intersection is finite, this shows $\rho'/\pi'$ is a root of unity.

**Step 6.** Choose $s \in \mathbb{Z}_{>0}$ such that $(\rho'/\pi')^s = 1$. In the field with $(q')^s$ elements we have $(\rho')^s = (\pi')^s$. Hence $(\pi')^s$ is effective. By Tate's lemma this implies $\pi$ is effective, which shows surjectivity in this case.

**Interlude.** We say a simple abelian variety $A$ of dimension $g$ over a field $K$ has *sufficiently many complex multiplications*, or we say that $A$ is a CM abelian variety, if there exists a field of degree $2g$ contained in $\mathrm{End}^0(A)$. In such a case we can choose a CM field $L \subset \mathrm{End}^0(A)$ with $[L : \mathbb{Q}] = 2g$. An abelian variety $B$ up to isogeny can be written as a direct sum of simple abelian varietes $A_i$, and we say $B$ is a CM abelian variety if every $A_i$ is a CM abelian variety. Note that for a simple CM abelian variety $A$ the division algebra $\mathrm{End}^0(A)$ need not be a field.

**A result by Tate.** Suppose $A$ is a simple abelian variety over a finite field $\kappa$. It is easy to see that $\pi = \pi_A$ is in the center of $D := \mathrm{End}^0(A)$. Tate showed:

any abelian variety over a finite field is a CM abelian variety;
we have equality $\mathbb{Q}(\pi) = \mathrm{Center}(D)$;
the structure of the central simple algebra $D$ can be read off from $p$-adic properties of $\pi_A$.

**Example.** Suppose $t > s > 0$ are relatively prime integers write $s + t =: g$. Let $\pi$ be a zero of $T^2 - p^s T + p^g$. It is clear that $\pi$ is an imaginary quadratic algebraic integer in which $p$ is split, and $\pi$ is a Weil $p^g$-number. Any simple abelian variety $A$ over $\mathbb{F}_{p^g}$ having $\pi_A \sim \pi$ is of dimension $g$ where $D = \mathrm{End}^0(A)$ is determined by $[D : \mathbb{Q}] = g^2$ and $D$ has Brauer invariants $s/g$ respectively $t/g$ at the two primes dividing $p$ and all other Brauer invariants of $D/\mathbb{Q}(\pi)$ are zero.

## 7 Proof of the surjectivity in the general case.

**Proof** (details to be explained).
**Step 1.** Suppose $\pi^s \notin \mathbb{Q}$ for every $s \in \mathbb{Z}{>}\, 0$. This defines $D$ (Tate, with the property that if $\pi \sim \pi_A$ then $\mathrm{End}^0(A) \cong D$). Choose a maximal CM field inside $D$. We choose a CM type $\Phi$ determined by the valuations of $\pi \in \mathbb{Q}(\pi) \subset L$.

**Step 2.** We choose a prime number $r$ such that $r$ is totally split in the totally real subfield $L_0$, and such that all valuations above $r$ are *non-split* in $L/L_0$ (this is possible by Chebotarov).

We choose a supersingular elliptic curve $E_1$ over $\kappa_1 = \overline{\mathbb{F}_r}$. We choose $A_1 = E_1^{[L_0:\mathbb{Q}]}$. We choose an appropriate polarization $\mu$ on $A_1$

**Step 3.** We see that $(A_1[p^\infty], \mu)$ with the action by $L$ can be lifted to characteristic zero (use a version of the Deuring result). Arrive at an abelian variety $A_2$ in characteristic zero of CM type $\Phi$.

**Step 4.** The abelian variety has CM by (an order in) $L$. General theory implies $A_2$ can be defined over a number field. Moreover abelian varieties with (sufficiently many) CM have potentially good reduction (at all primes).
**Conclusion.** *We can choose an abelian variety $A_3$ with CM type $\Phi$ defined over a number field $K$, with $L \subset \mathrm{End}^0(A_3)$ such that there exists*

$$K \supset \mathcal{O}_K \to \kappa_4 \supset \mathbb{F}_p$$

*such that $A_4 := A_3 \otimes \kappa_4$ is an abelian variety with $L \subset \mathrm{End}^0(A_4)$.*
**Remark.** In this case it may happen that $L \subsetneq \mathrm{End}^0(A_4)$.

**Step 5.** Choose $q'$ such that $\mathbb{F}_{q'}$ contains $\kappa_4$, with $[\mathbb{F}_{q'} : \kappa_4] = a$ and $\mathbb{F}_{q'}$ contains $\mathbb{F}_q$ with $[\mathbb{F}_{q'} : \mathbb{F}_q] = b$. Let $\rho' := \rho^a$ and $\pi' = \pi^b$. Using properties described above, and obtained along the road of the proof, especially using the CM type, and using the Weil conjecture we conclude:
**Claim.** The fraction $\rho'/\pi'$ is a root of unity.

**Step 6.** Choose $s \in \mathbb{Z}_{>0}$ such that $(\rho'/\pi')^s = 1$. In the field with $(q')^s$ elements we have

$(\rho')^s = (\pi')^s$. Hence $(\pi')^s$ is effective. By Tate's lemma this implies $\pi$ is effective, which shows surjectivity in the general case.

**Postscript / Remark.** We study the problem of existence and construction of a CM abelian variety $A$ over some number field with a given CM field $L$. Choose a prime number $r$ as we did before, i.e.

*$r$ is totally split in the maximal totally real field $L_0$,*
*every prime above $r$ in $L_0$ is non-split in $L/L_0$* (inert or ramified).

In this case the $r$-divisible group $A[r^\infty]$ splits, up to isogeny, as a direct sum of $[L_0 : \mathbb{Q}]$ direct summands of height 2; each of these summands has supersingular reduction mod $r$. We see a particular case where arithmetic properties of $L$ in such a case are reflected in the set of all torsion points of $A$. This observation is rather obvious. It is the core of the construction above.