Abelian varieties and cryptography

T. Shaska

Department of Mathematical Sciences
Oakland University
Rochester, MI. 48386

(joint work with G. Frey)

Outline

Definitions and basic properties

Let I_h (resp. I) be a homogeneous ideal in $k[Y_0, \cdots, Y_n]$ different from $\langle Y_0, \ldots Y_n \rangle$ (resp. an ideal in $k[X_1, \ldots, X_n]$). Let $R_h := k[Y_0, \ldots, Y_n]/I_h$ (resp. $R := k[X_1, \ldots, X_n]/I$) be the quotients. R_h is a graded ring, and so localizations $R_{h,\mathfrak{A}}$ with respect to hom. ideals $\mathfrak{A}$ are graded, too. Let $R_{h,\mathfrak{A},0}$ be the ring of elements of grade 0.

The **projective scheme** $\mathcal{S}_h$ (resp. **affine scheme** $\mathcal{S}$) defined by I_h (resp. I) consists of

- the topological space $V_h := \mathrm{Proj}(R_h)$ ($V := \mathrm{Spec(R)}$) of homogeneous prime ideals in R_h with preimage in $k[Y_0, \ldots, Y_n]$ different from $\langle Y_0, \ldots Y_n \rangle$ (prime ideals in R) endowed with the Zariski topology and
- the sheaf of **rings of holomorphic functions** given on Zariski-open sets $U \subset V_h$ (resp. $U \subset V$) as elements of grade 0 in localization of $R_{h,0}$ (resp. R) with respect to elements that become invertible when restricted to U.

Examples:

- The projective space $\mathbb{P}^n$ over k of dimension n is given by the ideal $\langle 0 \rangle \subset k[Y_0, \ldots, Y_n]$. The ring of holomorphic functions on $\mathbb{P}^n$ (take $U = \mathbb{P}^n$) is k. Take $U = \emptyset$ to get the ring of *meromorphic* functions on $\mathbb{P}^n$: consists of quotients

  $$f/g \text{ with } f, g \text{ homogeneous of degree d with } g \neq 0.$$

- The affine space $\mathbb{A}^n$ of dimension n over k is the topological space

  $$\mathrm{Spec}(k[X_1, \ldots X_n]).$$

  The ring of holomorphic functions on A^n is $k[X_1, \ldots, X_n]$, where polynomials are interpreted as polynomial functions. The ring of meromorphic functions on $\mathbb{A}^n$ (take $U = \emptyset$) is the field of rational functions $k(X_1, \ldots, X_n)$.
- The easiest but important example for an affine scheme: Take $n = 1$, $I = \langle X_1 \rangle$, $V = \mathrm{Spec}(k) = \{(0)\}$ and $O_{(0)} = k^*$.

Morphisms

Morphisms of affine or projective schemes are continuous maps between the underlying topological spaces induced (locally) by (in the projective case, quotients of the same degree) of polynomial maps of the sheaves.

Rational maps f between affine or projective schemes $\mathcal{S}$ and $\mathcal{T}$ are equivalence classes of morphisms defined on open subschemes U_i of $\mathcal{S}$ with image in $\mathcal{T}$ and compatible with restrictions to $U_i \cap U_j$. If f is invertible (as rational maps from $\mathcal{T}$ to $\mathcal{S}$), then f is **birational**, and $\mathcal{S}$ and $\mathcal{T}$ are **birationally equivalent**.

The k**-rational points** $\mathcal{S}(k)$ of a scheme $\mathcal{S}$ is the set of morphisms from $\mathrm{Spec}(k)$ to $\mathcal{S}$. For projective schemes defined by the ideal I_h the set $\mathcal{S}(k)$ is identified with points $(y_0 : y_1 \cdots : y_n)$ with k-rational homogeneous coordinates in $\mathbb{P}^n$ which are common zeros of the polynomials in I_h (similarly for affine schemes).

Constant field extensions: Let $k \overset{\iota}{\hookrightarrow} L$ be an embedding of k into a field L. Let $\mathcal{S}$ be a projective (affine) scheme defined over k with ring R. ι induces a morphism f_ι from R in $R \otimes_k L =: R_\iota$ given by the interpretation via ι of polynomials with coefficients in k as polynomials with coefficients in L. The prime ideal $I_\mathcal{S}$ extends to a prime ideal in R_ι and hence we get in a natural way a projective variety $\mathcal{S}_\iota$ with a morphism

$$\mathcal{S}_\iota \to \mathcal{S}$$

as $\mathrm{Spec}(k)$ schemes. $\mathcal{S}_\iota$ is a scheme now defined over L, denoted $\mathcal{S}_\iota$ by $\mathcal{S}_L$.

A scheme $\mathcal{S}$ is **irreducible** if the ideal I_h (respectively I) is a prime ideal. $\mathcal{S}$ is absolutely irreducible if $\mathcal{S}_{\bar{k}}$ is irreducible. This is the case if and only if k is algebraically closed in R. Classically, irreducible schemes are called **irreducible varieties**.

Group schemes:

A projective (affine) group scheme G defined over k is a projective (affine) scheme over k endowed with

i) addition, i.e., a morphism

$$m : \ G \times G \to G$$

ii) inverse, i.e., a morphism

$$i : \ G \to G$$

iii) the identity, i. e., a k-rational point $0 \in G(k)$,

such that it satisfies group laws. The group law is uniquely determined by the choice of the identity element.
A morphism of group schemes that preserves addition is a **homomorphism**.
Let L/k be a field extension. $G(L)$ is the set of L-rational points of G and it is also a group. A homomorphism between groups schemes induces a homomorphism between the group of rational points. If G is a projective variety, then the group law m is commutative.

An **Abelian variety** defined over k is an absolutely irreducible projective variety (over k) which is a group scheme.

The addition $m(P, Q)$ will be denoted by $P \oplus Q$ or simply $P + Q$ and the inversion $i(P)$ by $\ominus P$ or simply by $-P$.

Fact: *A morphism from the Abelian varieties, say $\mathcal{A}_1 \to \mathcal{A}_2$ is a homomorphism if and only if it maps the identity element of $\mathcal{A}_1$ to the identity element of $\mathcal{A}_2$.*

An abelian variety over k is called **simple** if it has no proper non-zero Abelian subvariety over k, it is called **absolutely simple** (or **geometrically simple**) if it is simple over the algebraic closure of k.

Complex tori and abelian varieties

Abelian varieties are connected, projective algebraic group schemes. Their analytic counterparts are the connected compact Lie groups.
Let $d \in \mathbb{Z}^{>0}$ and $\mathbb{C}^d$ the complex Lie group (i.e., with vector addition as group composition). $\mathbb{C}^d$ is not compact, but we can find quotients which are compact. Choose a lattice $\Lambda \subset \mathbb{C}^d$ which is a $\mathbb{Z}$-submodule of rank $2d$. The quotient $\mathbb{C}^d/\Lambda$ is a complex, connected Lie group which is called a **complex d-dimensional torus**.

Every connected, compact Lie group of dimension d is isomorphic to a torus $\mathbb{C}^d/\Lambda$.

A hermitian form H on $\mathbb{C}^d \times \mathbb{C}^d$ is a form that can be decomposed as

$$H(x, y) = E(ix, y) + i\,E(x, y),$$

where E is a skew symmetric real form on $\mathbb{C}^d$ satisfying $E(ix, iy) = E(x, y)$. E is called the imaginary part $\mathrm{Img}(H)$ of H. The torus C^d/Λ can be embedded into a projective space if and only if there exists a positive Hermitian form H on $\mathbb{C}^d$ with $E = \mathrm{Img}(H)$ such that restricted to $\Lambda \times \Lambda$ has values in $\mathbb{Z}$.

Let $\mathbb{H}_g$ be the Siegel upper half plane

$$\mathbb{H}_d = \{\tau \in \mathrm{Mat}_d(\mathbb{C}) \mid \tau^T = \tau,\ \mathrm{Img}(\tau) > 0\}.$$

Lemma
Let $\mathbb{C}^d/\Lambda$ be a complex torus attached to an abelian variety $\mathcal{A}$. Then Λ is isomorphic to $\mathbb{Z}^d \oplus \Omega \cdot \mathbb{Z}^d$, where $\Omega \in \mathbb{H}_d$.

The matrix Ω is called the **period matrix** of $\mathcal{A}$. The lattice $\hat{\mathcal{A}}$ given by

$$\hat{\mathcal{A}} := \{x \in \mathbb{C}^d \mid E(x, y) \in \mathbb{Z}, \text{ for all } y \in \lambda\}$$

is called the **dual lattice** of Λ. If $\hat{\mathcal{A}} = \mathcal{A}$ then $\mathcal{A}$ is called a **principally polarized** abelian variety.
For a principally polarized abelian variety $\mathcal{A}$ there exists a basis $\{\mu_1, \ldots, \mu_{2d}\}$ of Λ such that

$$J := \left[E(\mu_i, \mu_j)\right]_{1 \le i,j \le 2d} = \begin{bmatrix} 0 & I_d \\ -I_d & 0 \end{bmatrix}.$$

The symplectic group

$$Sp(2d, \mathbb{Z}) = \{M \in GL(2d, \mathbb{Z}) \mid MJM^T = J\}$$

acts on $\mathbb{H}_d$, via

$$\begin{aligned} Sp(2d, \mathbb{Z}) \times \mathcal{H}_d &\to \mathcal{H}_d \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \tau &\to (a\tau + b)(c\tau + d)^{-}1 \end{aligned}$$

where a, b, c, d, τ are $d \times d$ matrices. The moduli space of d-dimensional abelian varieties is

$$\mathbf{A}_g := \mathbb{H}_d / Sp(2d, \mathbb{Z}).$$

The Jacobian of a projective irreducible nonsingular curve is a principally polarized abelian variety.

Endomorphisms and isogenies

Let $\mathcal{A}$, $\mathcal{B}$ be abelian varieties over a field k. We denote the $\mathbb{Z}$-module of homomorphisms $\mathcal{A} \mapsto \mathcal{B}$ by $\mathrm{Hom}(\mathcal{A}, \mathcal{B})$ and the ring of endomorphisms $\mathcal{A} \mapsto \mathcal{A}$ by $\mathrm{End}\,\mathcal{A}$. In the context of Linear Algebra it can be more convenient to work with the vector spaces $\mathrm{Hom}^0(A, B) := \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$, and $\mathrm{End}^0 A := \mathrm{End}\, A \otimes_{\mathbb{Z}} \mathbb{Q}$. Determining $\mathrm{End}\,\mathcal{A}$ or $\mathrm{End}^0 A$ is an interesting problem on its own; see (Oort, 1988).

For any abelian variety $\mathcal{A}$ defined over a a number field K, computing $\mathrm{End}_K(\mathcal{A})$ is a harder problem than computation of $\mathrm{End}_{\bar{K}}(\mathcal{A})$; see (Lombardo, 2016, lemma 5.1) for details.

Lemma

If there exists an algorithm to compute $\mathrm{End}_K(\mathcal{A})$ *for any abelian variety of dimension* $g \geq 1$ *defined over a number field* K*, then there is an algorithm to compute* $\mathrm{End}_{\bar{K}}(\mathcal{A})$.

A homomorphism $f : \mathcal{A} \to \mathcal{B}$ is called an **isogeny** if $\mathrm{Img}\, f = \mathcal{B}$ and $\ker f$ is a finite group scheme. If an isogeny $\mathcal{A} \to \mathcal{B}$ exists we say that $\mathcal{A}$ and $\mathcal{B}$ are isogenous. We remark that this relation is symmetric, see Lemma 6.
The degree of an isogeny $f : \mathcal{A} \to \mathcal{B}$ is the degree of the function field extension

$$\deg f := [K(\mathcal{A}) : f^\star K(\mathcal{B})].$$

It is equal to the order of the group scheme $\ker(f)$.
The group of $\bar{k}$-rational points has order $\#(\ker f)(\bar{k}) = [K(A) : f^\star K(B)]^{sep}$, where $[K(A) : f^\star K(B)]^{sep}$ is the degree of the maximally separable extension in $K(\mathcal{A})/f^\star K(\mathcal{B})$.

f is a **separable isogeny** iff

$$\#\ker f(\bar{k}) = \deg f.$$

Equivalently: The group scheme $\ker f$ is étale.

Lemma

For any Abelian variety $\mathcal{A}/k$ there is a one to one correspondence between the finite subgroup schemes $\mathcal{K} \leq \mathcal{A}$ and isogenies $f : \mathcal{A} \to \mathcal{B}$, where $\mathcal{B}$ is determined up to isomorphism. Moreover, $\mathcal{K} = \ker f$ and $\mathcal{B} = \mathcal{A}/\mathcal{K}$.
f is separable if and only if $\mathcal{K}$ is étale, and then $\deg f = \#\mathcal{K}(\bar{k})$.

Lemma

If $\mathcal{A}$ and $\mathcal{B}$ are isogenous then $\mathrm{End}^0(\mathcal{A}) \cong \mathrm{End}^0(\mathcal{B})$.

Theorem (Poincare-Weil)

Let $\mathcal{A}$ be an Abelian variety. Then $\mathcal{A}$ is isogenous to

$$\mathcal{A}_2^{n_1} \times \mathcal{A}_2^{n_2} \times \cdots \times \mathcal{A}_r^{n_r},$$

where (up to permutation of the factors) $\mathcal{A}_i$, for $i = 1, \ldots, r$ are simple, non-isogenous, Abelian varieties. Moreover, up to permutations, the factors $\mathcal{A}_i^{n_i}$ are uniquely determined up to isogenies.

Lemma

If $\mathcal{A}$ is a absolutely simple Abelian variety then every endomorphism not equal 0 is an isogeny.

Computing isogenies between Abelian varieties

Fix a field k and let $\mathcal{A}$ be an Abelian variety over k. Let H denote a finite subgroup of $\mathcal{A}$. From the computational point of view we have the following problems:

- Compute all Abelian varieties $\mathcal{B}$ over k such that there exists an isogeny $\mathcal{A} \to \mathcal{B}$ whose kernel is isomorphic to H.
- Given $\mathcal{A}$ and H, determine the quotient $\mathcal{B} := \mathcal{A}/H$ and the isogeny $\mathcal{A} \to \mathcal{B}$.
- Given two Abelian varieties $\mathcal{A}$ and $\mathcal{B}$, determine if they are isogenous and compute a rational expression for an isogeny $\mathcal{A} \to \mathcal{B}$.

Torsion points and Tate modules

The most classical example of a separable isogeny is the scalar multiplication by n:

$$[n] : \mathcal{A} \to \mathcal{A}$$

The kernel of $[n]$ is a group scheme of order $n^{2\dim \mathcal{A}}$. Let $\mathcal{A}[n]$ be the group $\ker[n](\bar{k})$ (called n-torsion group).

Lemma

Let $f : \mathcal{A} \to \mathcal{B}$ be a degree n isogeny. Then there exists an isogeny $\hat{f} : \mathcal{B} \to \mathcal{A}$ such that

$$f \circ \hat{f} = \hat{f} \circ f = [n].$$

Theorem

Let $\mathcal{A}/k$ be an Abelian variety, $p = \operatorname{char} k$, and $\dim \mathcal{A} = g$.
i) If $p \nmid n$, then $[n]$ is separable, $\#\mathcal{A}[n] = n^{2g}$ and $\mathcal{A}[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.
ii) If $p \mid n$, then $[n]$ is inseparable. Moreover, there is an integer $0 \leq i \leq g$ such that

$$\mathcal{A}[p^m] \cong (\mathbb{Z}/p^m\mathbb{Z})^i, \text{ for all } m \geq 1.$$

If $i = g$ then $\mathcal{A}$ is called **ordinary**. If $\mathcal{A}[p^s](\bar{K}) = \mathbb{Z}/p^{ts}\mathbb{Z}$ then the abelian variety has p**-rank** t. If $\dim \mathcal{A} = 1$ (elliptic curve) then it is called **supersingular** if it has p-rank 0. An abelian variety $\mathcal{A}$ is called **supersingular** if it is isogenous to a product of supersingular elliptic curves.

Remark

If $\dim \mathcal{A} \leq 2$ and $\mathcal{A}$ has p-rank 0 then $\mathcal{A}$ is supersingular. This is not true for $\dim \mathcal{A} \geq 3$.

Let l be a prime different from $p = \text{char } K$ and $k \in \mathbb{N}$. Then,

$$[l]\mathcal{A}\left[l^{k+1}\right] = \mathcal{A}[l^k].$$

Hence, the collection of groups

$$\ldots \mathcal{A}[l^{k+1}], \ldots, \mathcal{A}[l^k], \ldots$$

forms a projective system. The l-adic Tate module of $\mathcal{A}$ is

$$T_l(\mathcal{A}) := \varprojlim \mathcal{A}[l^k].$$

Lemma

The Tate module $T_l(\mathcal{A})$ is a $\mathbb{Z}_l$-module isomorphic to $\mathbb{Z}_l^{2\dim \mathcal{A}}$.

Torsion points on abelian varieties are used to construct very important representations of the Galois group of k. Let n be relatively prime to p. Then G_k acts on $\mathcal{A}[n]$ which gives rise to a representation

$$\rho_{\mathcal{A},n} : G_k \to \text{Aut}\left((\mathbb{Z}/n\mathbb{Z})^{2g}\right)$$

and after a choice of basis in $\mathcal{A}[n]$ yields a representation

$$\rho_{\mathcal{A},n} : G_k \to GL_{2g}(\mathbb{Z}/n\mathbb{Z})$$

This action extends in a natural way to $T_l(\mathcal{A}) \otimes \mathbb{Q}_\ell$ and therefore to a ℓ-adic representation $\tilde{\rho}_{\mathcal{A},l}$ which is called the **l-adic Galois representation attached to** $\mathcal{A}$.

Representations of endomorphisms

Let ϕ be an endomorphism of the g-dimensional Abelian variety $\mathcal{A}$. By restriction ϕ induces a $\mathbb{Z}$-linear map ϕ_n on $\mathcal{A}[n]$. Since the collection (ϕ_{ℓ^k}) is compatible with the system defining $T_\ell(\mathcal{A})$ it yields a $\mathbb{Z}_\ell$-linear map $\tilde{phi}_\ell$ on $T_\ell(\mathcal{A})$.
Applying this construction to all elements in $\mathrm{End}(\mathcal{A})$ we get an injection (since $\mathcal{A}[\lambda^\infty]$) is Zariski-dense in $\mathcal{A}$) from $\mathrm{End}(\mathcal{A})$ into $Gl(2g, \mathbb{Z}_\ell)$. By tensorizing with $\mathbb{Q}_\ell$ we get the ℓ-adic representation

$$\tilde{\eta}_\ell : \mathrm{End}(\mathcal{A}) \otimes \mathbb{Q}_\ell \to Gl_{2g}(\mathbb{Q}_\ell).$$

Theorem
$\tilde{\eta}_\ell$ is injective.

This result has important consequences for the structure of $\mathrm{End}^0(\mathcal{A})$, more precisely $\mathrm{End}^0(\mathcal{A})$ is a $\mathbb{Q}$-algebra of dimension $\leq 4\dim(\mathcal{A})^2$.
$\mathrm{End}^0(\mathcal{A})$ is a semi-simple algebra, and by duality (keyword Rosati-involution) one can apply a complete classification due to Albert of *possible* algebra structures on $\mathrm{End}^0(\mathcal{A})$.

Question
Which algebras occur as endomorphism algebras?

The situation is well understood if k has characteristic 0 (due to Albert) but wide open in characteristic $p > 0$.

Characteristic Polynomial:

For $\phi \in \mathrm{End}^0(\mathcal{A})$ let $\tilde{\phi}_\ell$ its ℓ-adic representation. Denote its characteristic polynomial by $\chi_{\ell,\phi}(T) \in \mathbb{Z}_\ell[T]$.

Theorem (Weil)

$\chi_{\ell,\phi}(T)$ is a monic polynomial $\chi_\phi(T) \in \mathbb{Z}[T]$ which is independent of ℓ. We have

$$\chi_\phi(\phi) \equiv 0 \text{ on } \mathcal{A},$$

*and so it is justified to call $\chi_\phi(T)$ the **characteristic polynomial** of ϕ.*

The degree of $\chi_\phi(T)$ is $2\dim(\mathcal{A})$, the second-highest coefficient is the negative of the trace of ϕ, and the constant coefficient is equal to the determinant of ϕ.
Frobenius representations Let $\mathcal{A}$ be a g-dimensional Abelian variety defined over $\mathbb{F}_q$, where $q = p^d$ for a prime p and $\bar{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$. Let $\pi \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ be the Frobenius automorphism of $\mathbb{F}_q$, given by

$$\pi \,:\, x \to x^p.$$

Since $\mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by π and because of continuity of $\rho_{\mathcal{A},n}$ it is determined by $\rho_{\mathcal{A},n}(\pi)$.

$$\chi_{\mathcal{A},q}(T) := \chi(T)\left(\tilde{\rho}_{\mathcal{A},l}(\pi)\right) \in \mathbb{Z}_\ell[T] \tag{1}$$

is the characteristic polynomial of the image of π under $\tilde{\rho}_{\mathcal{A},l}$.

Lemma (Weil)

$\chi_{\mathcal{A},q}(T)$ is a monic polynomial of degree $2g$ in $\mathbb{Z}[T]$, independent of ℓ, and for all $n \in \mathbb{N}$ we get

$$\chi_{\mathcal{A},q}(T) \equiv \chi(\rho_{\mathcal{A},n}(\pi) \mod n.$$

Lemma (Tate)

We continue to take $k = \mathbb{F}_q$. The ℓ-adic representation $\tilde{\rho}_{\mathcal{A},l}$ is semi-simple and so is determined by their characteristic polynomials of the Frobenius, $\chi(T)\left(\tilde{\rho}_{\mathcal{A},l}(\pi)\right)$.[1]

Theorem (Tate)

Let $\mathcal{A}$ and $\mathcal{B}$ be Abelian varieties over a finite field $\mathbb{F}_q$ and $\chi_{\mathcal{A}}$ and $\chi_{\mathcal{B}}$ the characteristic polynomials of their Frobenius endomorphism and $l \neq p$ a prime. The following are equivalent.

- *$\mathcal{A}$ and $\mathcal{B}$ are isogenous.*
- $\chi_{\mathcal{A},q}(T) \equiv \chi_{\mathcal{B},q}(T)$
- *The zeta-functions for $\mathcal{A}$ and $\mathcal{B}$ are the same. Moreover, $\#\mathcal{A}(\mathbb{F}_{q^n}) = \#\mathcal{B}(\mathbb{F}_{q^n})$ for any positive integer n.*
- $T_l(\mathcal{A}) \otimes \mathbb{Q} \cong T_l(\mathcal{B}) \otimes \mathbb{Q}$

[1] An analogous result for $k = K$ a number field is the main result of Faltings on his way to prove Mordell's conjecture.

Geometric Interpretation

We continue to assume that $\mathcal{A}$ is an Abelian variety defined over $\mathbb{F}_q$ Hence π acts on the algebraic points of $\mathcal{A}$ by exponentiation on coordinates with q. This action induces an action on the function field $\mathbb{F}_q(\mathcal{A})$ given again by exponentiation by q.
This action is polynomial, and so it induces a morphism on $\mathcal{A}$. Without loss of generality we can assume that this morphism fixes $0_{\mathcal{A}}$ and so is an endomorphism ϕ_q called the **Frobenius endomorphism**.
So for given $\mathcal{A}$, the Frobenius automorphism plays a double role as Galois element and as endomorphism, and this is of great importance for the arithmetic of Abelian varieties over finite fields.
The explicit knowledge of ϕ_q yields immediately that it is purely inseparable and

$$\deg \phi_q = [K(\mathcal{A}) : \pi^\star K(\mathcal{A})] = q^g.$$

As endomorphism ϕ_q has an ℓ-adic representation. By construction its characteristic polynomial is equal to $\chi_{\mathcal{A},q}(T)$. It follows that $\chi_{\mathcal{A},q}(\phi_q) \equiv 0$ as endomorphism. This motivates the following definition.

Definition

$\chi_{\mathcal{A},q}(T)$ is the characteristic polynomial of the Frobenius endomorphism ϕ_q of $\mathcal{A}$.

This polynomial can be used for **counting points** on $\mathcal{A}(\mathbb{F}_q)$: Since ϕ_q is purely inseparable the endomorphism $\phi_q - id_{\mathcal{A}}$ is separable, and hence $\deg \ker(\phi_q - id_{\mathcal{A}})$ is equal to the number of elements in its kernel. Since π fixes exactly the elements of $\mathbb{F}_q$ the endomorphism ϕ_q fixes exactly $\mathcal{A}(\mathbb{F}_q)$ and so $\ker(\phi_q - id_{\mathcal{A}})(\bar{\mathbb{F}}_q) = \mathcal{A}(\mathbb{F}_q)$. By linear algebra it follows

Theorem

$$\#(\mathcal{A}(\mathbb{F}_q) = \chi_{\mathcal{A},q}(1).$$

Curves

By a **curve** $\mathcal{C}_k$ we mean a smooth, irreducible, projective variety of dimension 1. Sometimes it is convenient to have that $\mathcal{C}(k) \neq \emptyset$, and without loss of generality we then can assume that there is a point P_∞ "at infinity", i.e. in $\mathcal{C}(k) \setminus U_0$.

Let $\mathcal{C}$ be a curve defined over k. Hence there is a homogeneous *prime* ideal $\langle X_0, X_1, \ldots, x_n \rangle \neq I_\mathcal{C} \subset k[X_0, \ldots, X_n]$ and $R = k[X_0, \ldots, X_n]/I_\mathcal{C}$ such that:

- $\mathcal{C}$ is the scheme consisting of the topological space $\mathrm{Proj}(R)$ and the sheaf of holomorphic functions given on open subsets U of $\mathrm{Proj}(R)$ by the localization with respect to the functions in R not vanishing on U.
- The dimension of $\mathcal{C}$ is one, i.e. for every non-empty affine open subset $U \subset \mathrm{Proj}(R)$ the ring of holomorphic functions R_U on U is a ring with Krull dimension 1.
- $\mathcal{C}$ is regular, i.e. the localization of R with respect to every maximal ideal M in R is a discrete valuation ring R_M of rank 1. The equivalence class of the valuations attached to R_M is the *place* $\mathfrak{p}$ of $\mathcal{C}$, A place $\mathfrak{p}$ of $\mathcal{C}$ is also called **prime divisor** of $\mathcal{C}$.
- (Absolute irreducibility) $I_\mathcal{C} \cdot \bar{k}[X_0, \ldots, X_n]$ is a prime ideal in $\bar{k}[X_0, \ldots, X_n]$. This is equivalent with: k is algebraically closed in $\mathrm{Quot}(R)$.

As important consequence we note that for all open $\emptyset \neq U \neq \mathcal{C}$ the ring R_U is a *Dedekind domain*.

Prime Divisors and Points

Denote the set of all places $\mathfrak{p}$ of $\mathcal{C}$ by $\Sigma_{\mathcal{C}}(k)$.

Proposition

There is a one-to-one correspondence between $\Sigma_{\mathcal{C}}(k)$ and the equivalence classes of valuations of $k(\mathcal{C})$, which are trivial on k.

Let $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ be a prime divisor with maximal ideal $M_{\mathfrak{p}}$ and valuation ring $R_{\mathfrak{p}}$. We have

$$r_{\mathfrak{p}} : R_{\mathfrak{p}} \to R_p/M_{\mathfrak{p}} =: L$$

where L is a finite algebraic extension of k. The **degree** of $\mathfrak{p}$ is $\deg(\mathfrak{p}) := [L : k]$.
If $\deg(\mathfrak{p}) = 1$ then $L = k$ and $r_{\mathfrak{p}}$ induces a morphism from $\mathrm{Spec}(k)$ into $\mathcal{C}$ and so corresponds to a point $P \in \mathcal{C}(k)$, uniquely determined by $\mathfrak{p}$. More explicitly: The point P has the homogeneous coordinates $(y_0 : y_1 : \ldots, : y_n)$ with $y_i = r_{\mathfrak{p}}(Y_i)$.

Lemma

The set $\Sigma^1_{\mathcal{C}}(k)$ of prime divisors of $\mathcal{C}$ of degree 1 is in bijective correspondence with the set of k-rational points $\mathcal{C}(k)$ of the curve $\mathcal{C}$.

Now look at $\mathcal{C}_{\bar{k}}$. Obviously, every prime divisor of $\mathcal{C}_{\bar{k}}$ has degree 1, and so

Lemma

The set of prime divisors of $\mathcal{C}_{\bar{k}}$ corresponds one-to-one to the points in $\mathcal{C}_{\bar{k}}(\bar{k})$.

Since $\bar{k}/k$ is separable we get that every equivalence classes $\mathfrak{p}$ of valuations of $k(\mathcal{C})$, which are trivial on k has $\deg(\mathfrak{p}) = d$ extensions to $\bar{k}$, and these extensions are conjugate under the operation of G_k (Hilbert theory of valuations). Denote these extension by $\tilde{\mathfrak{p}}_1, \ldots, \tilde{\mathfrak{p}}_d$ and the corresponding points in $\mathcal{C}_{\bar{k}}(\bar{k}$ by $(P_1, \ldots, P_d)$. Then $\{P_1, \ldots, P_d\}$ is an orbit under the action of G_k and

Corollary

$\Sigma_{\mathcal{C}}(k)$ corresponds one-to-one to the G_k-orbits of $\mathcal{C}_{\bar{k}}(\bar{k})$.

Divisors and Picard groups

Let $\mathcal{C}$ be curve over k. A group of k-rational divisors $\mathrm{Div}_{\mathcal{C}}(k)$ of $\mathcal{C}$ is defined by

Definition

$\mathrm{Div}_{\mathcal{C}}(k) = \bigoplus_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} \mathbb{Z}\cdot\mathfrak{p}$, i.e. $\mathrm{Div}_{\mathcal{C}}(k)$ is the free abelian group with base $\Sigma_{\mathcal{C}}(k)$.

Hence a **divisor** D of $\mathcal{C}$ is a formal sum

$$D = \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}\, P$$

where $z_{\mathfrak{p}} \in \mathbb{Z}$ and $z_{\mathfrak{p}} = 0$ for all but finitely many prime divisors $\mathfrak{p}$. So it makes sense to define

$$\deg(D) = \sum_{\mathfrak{p}\in\Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}.$$

From Corollary 1 we can interpret divisors as formal sum of G_k-orbits in $\mathcal{C}_{\bar{k}}(\bar{(}k)$. But we remark that taking points in $\mathcal{C}(k)$ is in general not enough to get all k-rational divisors of $\mathcal{C}$.

The map

$$D \mapsto \deg(D)$$

is a homomorphism from $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathbb{Z}$. Its kernel is the subgroup $\mathrm{Div}_{\mathcal{C}}(k)^0$ of divisors of degree 0.

Example

Let $f \in k(\mathcal{C})^*$ be a meromorphic function on $\mathcal{C}$. For $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we have defined the normalized valuation $w_{\mathfrak{p}}$. The divisor of f is defined as

$$(f) = \sum_{\Sigma_{\mathcal{C}}(k)} w_{\mathfrak{p}} \cdot \mathfrak{p}.$$

The Picard Functor:

Let L/k be a finite extension and $\mathcal{C}_L$ the curve obtained from $\mathcal{C}$. Then places of $k(\mathcal{C})$ can be extended to places of $L(\mathcal{C}_L)$ and by the conorm map we get an injection of $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathrm{Div}_{\mathcal{C}_L}(L)$. Then, $conorm_{L/k}(\mathrm{Div}^0_{\mathcal{C}}(k)) \subset \mathrm{Div}^0_{\mathcal{C}_L}(L)$ and that principal divisors are mapped to principal divisors. Hence we get a homomorphism

$$conorm_{L/k} : \mathrm{Pic}^0_{\mathcal{C}}(k) \to \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

and so we get a functor

$$\mathrm{Pic}^0 : L \mapsto \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

from the category of **algebraic extension fields of** k to the category of **abelian groups**. Coming "from above" we have a Galois theoretical description of this functor:

$$\mathrm{Div}_{\mathcal{C}_L}(L) = \mathrm{Div}_{\mathcal{C}_{\{\bar{k}}}(\bar{k})^{G_L}$$

and the same is true for functions. The analogue is true for $\mathrm{PDiv}_{\mathcal{C}_L}(L)$ and for $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$:

Theorem

Under the assumption made for curves $\mathcal{C}$ we have that for finite extension fields L with $k \subset L \subset \bar{k}$ the functor $L \mapsto \mathrm{Pic}^0_{\mathcal{C}_L}(L)$ is the same as the functor

$$L \mapsto \mathrm{Pic}^0_{\mathcal{C}_{\bar{k}}}(\bar{k})^{G_L}.$$

In particular, we have

$$\mathrm{Pic}^0_{\mathcal{C}_{\bar{k}}}(\bar{k}) = \bigcup_{k \subset L \subset \bar{k}} \mathrm{Pic}^0_{\mathcal{C}_L}(L)$$

where inclusions are obtained via conorm maps.

Remark

For L/k finite algebraic we have also the norm map of places of $\mathcal{C}_L$ to places of $\mathcal{C}_k$, which induces a homomorphism from $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$ *to* $\mathrm{Pic}^0_{\mathcal{C}}(k)$*. In general, this map will be neither injective nor surjective.*

It is one of the most important facts for the theory of curves that the functor Pic^0 can be represented: There is a variety $\mathcal{J}_{\mathcal{C}}$ defined over k such that for all extension fields L of K we have a functorial equality

$$\mathcal{J}_{\mathcal{C}}(L) = \mathrm{Pic}^0_{\mathcal{C}_L}(L).$$

$J_{\mathcal{C}}$ is the **Jacobian variety** of $\mathcal{C}$. This variety will be discussed soon.

Riemann-Roch Spaces

We define a partial ordering of elements in $\mathrm{Div}_{\mathcal{C}}(k)$ as follows; $D = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}$ is *effective* ($D \geq 0$) if $z_{\mathfrak{p}} \geq 0$ for every $\mathfrak{p}$, and $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.
Let $D = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}} \in \mathrm{Div}_{\mathcal{C}}(k)$. The **Riemann-Roch space** associated to D is

$$\mathcal{L}(D) = \{f \in k(\mathcal{C})^* \text{ with } (f) \geq -D\} \cup \{0\}.$$

So $x \in \mathcal{L}(D)$ are defined by the property that $w_{\mathfrak{p}}(x) \geq -z_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$.
Then $\mathcal{L}(D)$ is a vector space over k. $\mathcal{L}(D)$ has positive dimension if and only if there is a function $f \in k(\mathcal{C})^*$ with $D + (f) \geq 0$, or equivalently, $D \sim D_1$ with $D_1 \geq 0$. Moreover; $\mathcal{L}(0) = k$ and if $\deg(D) < 0$ we get $\mathcal{L}(D) = \{0\}$. If $\deg(D) = 0$ then either D is a principal divisor or $\mathcal{L}(D) = \{0\}$.

Proposition

Let $D = D_1 - D_2$ with $D_i \geq 0$. Then

$$\dim(\mathcal{L}(D)) \leq \deg(D_1) + 1.$$

If $D \sim D'$ we have $\ell(D) \sim \ell(D')$. In particular $\mathcal{L}(D)$ is a finite-dimensional k-vector space. Define $\ell(D) := \dim_k(\mathcal{L}(D))$.
To compute $\ell(D)$ is a fundamental problem in the theory of curves. It is solved by the Theorem of Riemann-Roch. A first estimate is a generalization of the proposition above: For all divisors D we have the inequality

$$\ell(D) \leq \deg(D) + 1.$$

For a proof one can assume that $\ell(D) > 0$ and so $D \sim D' > 0$. The important fact is that one can estimate the interval given by the inequality.

Theorem (Riemann)

For given curve $\mathcal{C}$ there is a minimal number $g_{\mathcal{C}} \in \mathbb{N} \cup \{0\}$ such that for all $D \in Div_{\mathcal{C}}$ we have

$$\ell(D) \geq \deg(D) + 1 - g_{\mathcal{C}}.$$

For a proof see (Stichtenoth, 2009, Proposition 1.4.14). So

$$g_{\mathcal{C}} = \max\{\deg D - \ell(D) + 1;\ D \in \mathrm{Div}_{\mathcal{C}}(k)\}$$

exists and is a non-negative integer independent of D. $g_{\mathcal{C}}$ is the **genus** of $\mathcal{C}$.
The genus does not change under constant field extensions because we have assumed that k is perfect. This can be wrong in general if the constant field of $\mathcal{C}$ has inseparable algebraic extensions.

Corollary

There is a number $n_{\mathcal{C}}$ such that for $\deg(D) > n_{\mathcal{C}}$ *we get equality*

$$\ell(D) = \deg(D) + 1 - g_{\mathcal{C}}.$$

Theorem 11 together with its corollary is the ”Riemann part” of the Theorem of Riemann-Roch for curves. To determine $n_{\mathcal{C}}$ and to get more information about the inequality for small degrees one needs canonical divisors.

Canonical Divisors

Let $k(\mathcal{C})$ be the function field of a curve C defined over k. To every $f \in k(\mathcal{C})$ we attach a symbol df, the *differential* of f lying in a $k(\mathcal{C})$-vector space $\Omega(k(\mathcal{C}))$ generated by the symbols df modulo the following relations: For $f, g \in k(\mathcal{C})$ and $\lambda \in k$ we have
i)$d(\lambda f + g) = \lambda df + dg$
ii)$d(f \cdot g) = fdg + gdf$.
The relation between derivations and differentials is given by the

Definition (Chain rule)

Let x be as above and $f \in k(\mathcal{C})$. Then $df = (\partial f/\partial x)dx$.

As in calculus one shows that the $k(\mathcal{C})$-vector space of differentials $\Omega(k(\mathcal{C}))$ has dimension 1 and it is generated by dx for any $x \in k(\mathcal{C})$ for which $k(\mathcal{C})/k(x)$ is finite separable.
We use a well known fact from the theory of function fields F in one variable i.e finitely generated fields of transcendence degree 1 over a perfect field k:
Let $\mathfrak{p}$ be a place of F, i.e. an equivalence class of discrete rank one valuations of F trivial on k). Then there exist a function $t_{\mathfrak{p}} \in F$ with $w_{\mathfrak{p}}(t_{\mathbb{P}}) = 1$ and $[F : k(t_{\mathfrak{p}})$ separable. We apply this to $F = k(\mathcal{C})$. For all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we choose a function $t_{\mathfrak{p}}$ as above. For a differential $0 \neq \omega \in \Omega(k(\mathcal{C})$ we get $\omega = f_{\mathfrak{p}} \cdot dt_{\mathfrak{p}}$.

Definition
The divisor (ω) is given by

$$(\omega) := \sum_{\mathfrak{p} \in \Sigma_{\mathfrak{p}}} w_{\mathfrak{p}}(f_{\mathfrak{p}}) \cdot \mathfrak{p}.$$

ω is a called a **canonical divisor** of $\mathcal{C}$.

The chain rule implies that this definition is independent of the choices, and the relation to differentials yields that (ω) is a divisor.
Since $\Omega(k(\mathcal{C})$ is one-dimensional over $k(\mathcal{C})$ it follows that the set of canonical divisors of $\mathcal{C}$ form a divisor class $\mathcal{K}_{\mathcal{C}} \in \mathrm{Pic}_{\mathcal{C}}(k)$ called the **canonical class** of $\mathcal{C}$.
We are now ready to formulate the **Theorem of Riemann-Roch**

Theorem
Let (W) be a canonical divisor of $\mathcal{C}$. For all $D \in Div_{\mathcal{C}}(k)$ we have

$$\ell(D) = \deg(D) + 1 - g_{\mathcal{C}} + \ell(W - D).$$

For a proof see Section 1.5 in the book (Stichtenoth, 2009).
A differential ω is *holomorphic* if (ω) is an effective divisor. The set of holomorphic differentials is a k-vector space denoted by $\Omega^0_{\mathcal{C}}$ which is equal to $\mathcal{L}(W)$.

Take $D = 0$ respectively $D = W$ in the theorem of Riemann-Roch to get

Lemma
$\Omega^0_{\mathcal{C}}$ is a $g_{\mathcal{C}}$- dimensional k- vector space and $\deg(W) = 2g_{\mathcal{C}} - 2$.

For the applications we have in mind there are two further consequences of the Riemann-Roch theorem important.

Lemma
The following are true:

1. *If* $\deg(D) > 2g_{\mathcal{C}} - 2$ *then* $\ell(D) = \deg(D) + 1 - g_{\mathcal{C}}$.
2. *In every divisor class of degree g there is a positive divisor.*

Take D with $\deg(D) \geq 2g_{\mathcal{C}} - 1$. So $\deg(W - D) \leq -1$ and so $\ell(W - D) = 0$. Take D with $\deg(D) = g_{\mathcal{C}}$. Then $\ell(D) = 1 + \ell(W - D) \geq 1$ and so there is a positive divisor in the class of D.

Cantor's Algorithm

Inspired by the group law on elliptic curves and its geometric interpretation we give an explicit algorithm for the group operations on Jacobian varieties of hyperelliptic curves.

Take a genus $g \geq 2$ hyperelliptic curve $\mathcal{C}$ with a least one rational Weierstrass point given by the affine Weierstrass equation

$$W_{\mathcal{C}} : \; y^2 + h(x)\, y = x^{2g+1} + a_{2g} x^{2g} + \cdots + a_1 x + a_0, \tag{2}$$

over k. We denote the prime divisor corresponding to $P_\infty = (0 : 1 : 0)$ by $\mathfrak{p}_\infty$.
We note that the affine coordinate ring of $W_{\mathcal{C}}$ is

$$\mathcal{O} = k[X, Y]/\langle (Y^2 + h(X)\, Y - (X^{2g+1} + a_{2g} X^{2g} + \cdots + a_1 X + a_0) \rangle$$

So degree d prime divisors $\mathfrak{p}$ of $\mathcal{C}$ correspond to prime ideals $P \neq 0$, $[\mathcal{O}/P : k] = d$.

Let ω be the hyperelliptic involution of $\mathcal{C}$. It operates on $\mathcal{O}$ and on $\mathrm{Spec}(\mathcal{O})$ and fixes exactly the prime ideals which "belong" to Weierstrass points, i.e. split up in such points over $\bar{k}$.

Following (Mumford, 2008) we introduce polynomial coordinates for points in $J_{\mathcal{C}}(k)$. The first step is to normalize representations of divisor classes. In each divisor class $c \in \mathrm{Pic}^0(k)$ we find a unique *reduced* divisor

$$D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\mathfrak{p}\infty$$

with $\sum_{i=1}^{r} n_i \deg(\mathfrak{p}_i) = d \leq g$, $\mathfrak{p}_i \neq \omega(\mathfrak{p}_j$ for $i \neq j$ and $\mathfrak{p}_i \neq \mathfrak{p}_i nfty$. (We use Riemann-Roch and the fact that ω induces $-id_{J_{\mathcal{C}}}$.)

Using the relation between divisors and ideal in coordinate rings we get that $n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r$ corresponds to an ideal $I \subset \mathcal{O}$ of degree d and the property that if the prime ideal P_i is such that both P and $\omega(P)$ divide I then it belongs to a Weierstrass point.
By algebra we get that the ideal I is a free $\mathcal{O}$-module of rank 2 and so

$$I = k[X]u(X) + k[x](v(X) - Y).$$

Fact: $u(X), v(X) \in k[X]$, u monic of degree d, $\deg(v) < d$ and u divides $v^2 + h(X)v - f(X)$.

Moreover, c is uniquely determined by I, I is uniquely determined by (u, v) and so we can *take* (u, v) *as coordinates for c.*

Theorem (Mumford representation)

Let $\mathcal{C}$ be a hyperelliptic curve of genus $g \geq 2$ with affine equation

$$y^2 + h(x)\, y \;=\; f(x),$$

where $h, f \in K[x]$, $\deg f = 2g+1$, $\deg h \leq g$. Every non-trivial group element $c \in \mathrm{Pic}^0_{\mathcal{C}}(k)$ can be represented in a unique way by a pair of polynomials $u, v \in K[x]$, such that

- **i)** *u is a monic*
- **ii)** $\deg v < \deg u \leq g$
- **iii)** $u \mid v^2 + vh - f$

How to find the polynomials u, v?
We can assume without loss of generality that $k = \bar{k}$ and identify prime divisors $\mathfrak{p}_i$ with points $P_i = (x_i, y_i) \in k \times k$. Take the reduced divisor $D = n_1\mathfrak{p}_1 + \cdots + n_r\mathfrak{p}_r - d\mathfrak{p}_\infty$ now with $r = d \leq g$. Then

$$u(X) = \prod_{i=1}^{r} (X - x_i)^{n_i}.$$

Since $(X - x_i)$ occurs with multiplicity n_i in $u(X)$ we must have for $v(X)$:

$$\left(\frac{d}{dx}\right)^j \Big[v(x)^2 + v(x)\, h(x) - f(x)\Big]_{x=x_i} = 0,$$

and one determines $v(X)$ by solving this system of equations.

Isogenies of Jacobians via Correspondences

Let K be a perfect field and L/K a finite extension. Let $\mathcal{D}_1$ be a regular projective curve over L and $\mathcal{D}_2$ a regular projective curve defined over K. Let $\mathcal{H}$ be a curve over L and

$$\varphi_1 : \mathcal{H} \to \mathcal{D}_1, \text{ respectively } \varphi_2 : \mathcal{H} \to \mathcal{D}_2 \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L) =: \mathcal{D}_{2,L},$$

be L-rational morphisms. The morphism φ_1 induces the L-rational **conorm morphism**

$$\varphi_1^* : \mathcal{J}_{\mathcal{D}_1} \to \mathcal{J}_{\mathcal{H}}$$

and the morphism φ_2 induces the **norm morphism**

$$\varphi_{2,*} : \mathcal{J}_{\mathcal{H}} \to \mathcal{J}_{\mathcal{D}_{2,L}}.$$

By composition we get a homomorphism (defined over L)

$$\eta_L : \mathcal{J}_{\mathcal{D}_1} \to \mathcal{J}_{\mathcal{D}_{2,L}}$$

Let $\mathcal{W}_{L/K}$ be the Weil restriction of the Jacobian of $\mathcal{D}_1$ to K. It is an abelian variety over K with $\mathcal{W}_{L/K}(K) = \mathrm{Pic}^0_{\mathcal{D}_1}$. Applying the norm map from L to K we get a homomorphism

$$\eta : \mathcal{W}_{L/K} \to \mathcal{J}_{\mathcal{D}_2}.$$

In general, neither the kernel nor the cokernel of η will be finite. But under mild conditions one can assure that that η has a finite kernel, and so it induces an isogeny of $\mathcal{W}_{L/K}$ to an abelian subvariety of $\mathcal{J}_{\mathcal{D}_2}$.

So we get a transfer of the DLP from $\mathrm{Pic}^0_{\mathcal{D}_1}$ (defined over L) to the DLP in a subvariety of $\mathcal{J}_{\mathcal{D}_2}$ (defined over K). The efficiency of this depends on the complexity of the algorithms computing the norm- and conorm maps (φ_i and $[L : K]$ must have small degrees), and it makes sense only if the DLP after the transfer is easier than before.

Weil Descent

Take $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^d}$ with $d > 1$ and $\mathcal{H} = \mathcal{D}_{2,L}$, i.e. a given curve $\mathcal{X}$ (over $\mathbb{F}_{q^d}$) is covered by a curve $\mathcal{D}_{\mathbb{F}_{q^d}}$, which is the scalar extension of a curve $\mathcal{D}$ defined over K.

This yields a K-rational homomorphism from the Weil restriction $\mathcal{W}_{L/K}$ of $\mathcal{J}_\mathcal{X}$ to $\mathcal{J}_\mathcal{D}$. $\mathcal{D}$ will (in all non-trivial cases) be a curve of a genus larger than the genus of $\mathcal{X}$ but since it is defined over the smaller field $\mathbb{F}_q$ one can hope that one can apply fast algorithms to compute the discrete logarithm in $\mathcal{J}_\mathcal{D}(\mathbb{F}_q)$, e.g. by methods of index-calculus.

Indeed, if $\mathcal{X}$ is not defined of a proper subfield of $\mathbb{F}_{q^d}$ this is the principle of the so-called GHS-attack in (see (Gaudry et al., 2002) which is successful in remarkably many cases.

If $\mathcal{X}$ is already defined over $\mathbb{F}_q$ one is lead to the so-called trace-zero varieties in $\mathcal{J}_\mathcal{X}(\mathbb{F}_{q^d})$ and again correspondences induced by covers of curves can be used for attacks on crypto systems based on DL on these varieties by work of Diem.

These results already indicate that the use of Picard groups of curves (e.g. elliptic curves) over non-prime fields $\mathbb{F}_{qd}$ with $d \geq 4$ is not advisable for cryptographic use. By more recent work of C. Diem this ”feeling” is reinforced for instance for families of elliptic curves in towers of finite fields.

Correspondences via Monodromy Groups

We assume that we have a degree n cover morphism defined over K

$$f : \mathcal{X} \to \mathbb{P}^1$$

and fixed monodromy group $G_f := \text{Mon}(f)$. We have morphisms

$$\tilde{f} : \tilde{\mathcal{H}} \xrightarrow{h} \mathcal{X} \xrightarrow{f} \mathbb{P}^1$$

with $\tilde{f}$ a Galois cover of f with Galois group G_f. For simplicity, we assume that the field of constants of $\tilde{\mathcal{H}}$ is K. Choose subgroups $H_1 \subset G_f$ fixing $\mathcal{X}$ and H_2 containing H_1. Let $\mathcal{H}$ be the curve fixed by H_1 and $\mathcal{D}$ the fixed curve under H_2. So $\mathcal{H}$ covers both $\mathcal{X}$ and $\mathcal{D}$. Let

$$h : \mathcal{H} \to \mathcal{X} \quad \textit{and} \quad g : \mathcal{H} \to \mathcal{D}$$

with morphisms induced by the Galois action. Hence, $\deg(h) = \frac{|G_f|}{|H_1| \cdot n}$ and $\deg(g) = \frac{|H_2|}{|H_1|}$. We get a correspondence

$$\eta : \mathcal{J}_{\mathcal{X}} \to \mathcal{J}_{\mathcal{D}}$$

by applying $g_* \circ h^*$ to the Picard groups. In general, η will be neither injective nor surjective.

Assume that $\mathcal{J}_{\mathcal{D}}$ is simple with $\dim \mathcal{J}_{\mathcal{D}} = g(\mathcal{X})$ and there is a prime divisor $\mathfrak{p}_\infty$ of $\mathcal{X}$ totally ramified under h (there is exactly one prime divisor $\mathfrak{P}_\infty$ of $\mathcal{H}$ with norm $\mathfrak{p}$, and that there is no non-constant morphism of degree $\leq \deg(h)$ from $\mathcal{D}$ to $\mathbb{P}^1$).

Lemma

Then η is an isogeny.

It is an open and challenging problem to find other interesting correspondences of low degree between Jacobian varieties induced by correspondences between curves and (possibly) attached to Hurwitz spaces.

Elliptic curve cryptography

The definitions from the Abelian varieties apply here. In the case of elliptic curves we have the following:

Definition
If char $(K) = 0$, then we say that an elliptic curve E/K has complex multiplication or (historically) that E is singular, if $\mathrm{End}(E) \neq \mathbb{Z}$. If char $(K) > 0$, we say that E/K is **supersingular** if $\mathrm{End}(E)$ is an order in a rational quaternion algebra, otherwise we say that E is **ordinary**.

Let E be an elliptic curve over $\mathbb{F}_q$, where $q = p^n$ for some prime p and an integer n. Its characteristic polynomial of the Frobenius π is

$$\chi_{E,q}(T) = T^2 - \mathrm{tr}(\pi)\, T + q = (T - \lambda_1)(T - \lambda_1).$$

where the eigenvalues λ_1, λ_2 are in some quadratic extension of $\mathbb{Q}$. Let $K_E = \mathbb{Q}(\lambda_1)$ and $\mathcal{O}_{K_E}$ its ring of integers. An elliptic curve E defined over $\mathbb{F}_q$ is called **ordinary** if the separable degree of $[p]$ is p.
The following results are mostly due to M. Deuring and mainly contained in the beautiful paper (Deuring, 1941).

Deuring's theorem

Theorem

Let E be an elliptic curve defined over a field K. The following hold:
i) If $\mathrm{char}(K) = 0$, *then E is ordinary and*

- $\mathrm{End}_{\overline{K}}(\mathcal{E}) = \mathbb{Z}$ *(generic case) or* $\mathrm{End}_{\overline{K}}(\mathcal{E})$ *is an order* $O_{\mathcal{E}} \subset \mathbb{Q}(\sqrt{-d_{\mathcal{E}}})$, $d_{\mathcal{E}} > 0$ *(CM-case).*
- *Take $\mathcal{E}$ with CM with order $O_{\mathcal{E}}$. Let $\mathcal{S}_{\mathcal{E}}$ be the set of $\mathbb{C}$-isomorphy classes of elliptic curves with endomorphism ring $O_{\mathcal{E}}$. Then* $\mathrm{Pic}(O_{\mathcal{E}})$ *acts in a natural and simply transitive way on $\mathcal{S}_{\mathcal{E}}$, hence $\mathcal{S}_{\mathcal{E}}$ is a principally homogeneous space with translation group* $\mathrm{Pic}(O_{\mathcal{E}})$*: For* $c \in \mathrm{Pic}(O_{\mathcal{E}})$, $\mathfrak{A} \in c$ *and* $\mathbb{C}/O_{\mathcal{E}} = \mathcal{E}_0$ *we get* $c \cdot [\mathcal{E}_0]$ *is the class of* $\mathbb{C}/\mathfrak{A}$.

*ii) (**Deuring's Lifting Theorem**) Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$ which is ordinary over $\overline{\mathbb{F}_q}$. Then there is, up to $\mathbb{C}$-isomorphisms, exactly one elliptic curve $\mathcal{E}$ with CM over a number field K such that*

- *there is a prime $\mathfrak{p}$ of K with $\mathcal{E}_{\mathfrak{p}} \cong \mathcal{E}$, and*
- $\mathrm{End}(\mathcal{E}) = \mathrm{End}(\mathcal{E})_{\mathfrak{p}} = O_{\mathcal{E}}$, *with $O_{\mathcal{E}}$ an order in an imaginary quadratic field.*

iii) If $\mathcal{E}$ is supersingular, then

- *Up to twists, all supersingular elliptic curves in characteristic p are defined over $\mathbb{F}_{p^2}$, i.e. their j-invariant lies in $\mathbb{F}_{p^2}$.*
- $|\mathcal{E}(\mathbb{F}_{p^2}| = (p \pm 1)^2$, *and the sign depends on the twist class of $\mathcal{E}$.*
- $\mathrm{End}_{\overline{\mathbb{F}_p}}(\mathcal{E})$ *is a maximal order in the quaternion algebra $\mathbb{Q}_p$, which is unramified outside of ∞ and p.*

Hasse's Bound

Endomorphism rings of elliptic curves over finite fields $\mathbb{F}_q$ are never equal to $\mathbb{Z}$ since there is the Frobenius endomorphism $\phi_{\mathbb{F}_q,\mathcal{E}}$ induced by the Frobenius automorphism of $\mathbb{F}_q$ which has degree q. We give a first application of the lifting theorem.

Corollary (Hasse)

Let $\mathcal{E}$ be an ordinary elliptic curve over $\mathbb{F}_q$. Then the Frobenius endomorphism $\phi_{\mathbb{F}_q,\mathcal{E}}$ is an integer in an imaginary quadratic fields with norm q, and hence has a minimal polynomial

$$\chi_{\mathcal{E},q}(T) = T^2 - \mathrm{tr}(\phi_{\mathbb{F}_q,\mathcal{E}}) \cdot T + q$$

with

$$|(\mathrm{tr}(\phi_{\mathbb{F}_q,\mathcal{E}})^2 - 4q| < 0.$$

Recall that the number of $\mathbb{F}_q$-rational points of $\mathcal{E}$ is

$$|\mathcal{E}(\mathbb{F}_q)| =: n_{\mathbb{F}_q,\mathcal{E}} = \chi_{\mathcal{E},q}(1).$$

Corollary

$|n_{\mathbb{F}_q,\mathcal{E}} - q - 1| < 2\sqrt{q}$.

Using the result iii) in Theorem 17 and the observation that the eigenvalues of $\phi_{\mathbb{F}q^d,\mathcal{E}}$ are the d-th power of the eigenvalues of $\phi_{\mathbb{F}_q,\mathcal{E}}$ we get that

$$|n_{\mathbb{F}_q,\mathcal{E}} - q - 1| \leq 2\sqrt{q}$$

for all elliptic curves of $\mathbb{F}_q$. This is the *Hasse bound* for elliptic curves, a special case of the Weil bound for points on curves over finite fields.

Point Counting

Corollary 4 is the key fact for a polynomial time algorithm for computing the order of $\mathcal{E}(\mathbb{F}_q)$, which is called **Schoof's Algorithm**.
The idea is to compute $\chi_{\mathcal{E},q}(T) \mod n$ for small numbers n by computing the action of $\phi_{\mathbb{F}_q,\mathcal{E}}$ on $\mathcal{E}[n]$ (take for instance $n = \ell$ as small prime number or $n = 2^k$ with k small) and then to use CRT and the Hasse bound for trace of $\phi_{\mathbb{F}_q,\mathcal{E}}$ to determine $\chi_{\mathcal{E},q}(T)$. To do this use the classical n-division polynomials Ψ_n and then use *CRT*. The disadvantage is that $\deg(\Psi_n) \sim n^2/2$ and therefore the Schoof algorithm is too slow.

The way out of this problem is to use étale isogenies with cyclic kernel of order n and the fact that we can interpret these isogenies with the help of points on an explicitly known curve, namely the modular curve $X_0(n)$. It allows an effective computation of isogenies at least if n is of moderate size).

Theorem (Vélu, Couveignes, Lercier, Elkies, Kohel, and many other contributors:)
The cost for the computation of an isogeny of degree ℓ of an elliptic curve $\mathcal{E}$ over $\mathbb{F}_q$ is

$$\mathcal{O}(\ell^2 + \ell \log(\ell) \log(q)).$$

Idea of Atkin-Elkies: Use *isogenies* of small degree of E instead of points and ϕ_n.
The resulting *Schoof-Atkin-Elkies algorithm* is very fast, in particular if one assumes as "standard conjecture" the Generalized Riemann Hypothesis (GRH).

Corollary
$|E(\mathbb{F}_q)|$ can be computed (probabilistically, with GRH) with complexity $\mathcal{O}((\log q)^4)$. Therefore we can construct, for primes p sufficiently large, (many) elliptic curves with $|\mathcal{E}(\mathbb{F})| = k \cdot \ell$ with k small (e.g. $k = 1$ if we want) and ℓ a prime so large that (using classical computers and according to our best knowledge) the security level of the discrete logarithm in $\mathcal{E}(\mathbb{F}_p)$ is matching AES 128 (or larger).

Looking for Post-Quantum Security

From above we can construct elliptic curves over prime fields such that the resulting DL-systems are secure under the known attacks. But the situation changes totally if we allow algorithms based on quantum computers.

The System of Couveignes-Stolbunov: For an ordinary elliptic curve $\mathcal{E}_0$ over $\mathbb{F}_q$ with $\mathrm{End}(\mathcal{E}_0) = O$, which is an order in a quadratic imaginary field we let $\mathcal{S}_{E_0}$ be the set of isomorphism classes of elliptic curves over $\overline{\mathbb{F}_q}$ with ring of endomorphisms O. Then $\mathcal{S}_{E_0}$ is a $\mathrm{Pic}(O)$-set and we can use it for *Key Exchange protocols:*

The partner P choses $c \in \mathrm{Pic}(O)$ and publishes the j-invariant of $c \cdot E_0$.

The exchange is not as fast as DL-systems since we cannot use a *double-and add* algorithm but it is feasible. The **security** depends on the hardness of the following:

Problem

Find an isogeny between two given isogenous elliptic curves.

Proposition (Kohel, Galbraith, Hess, Smart et al.)

*The expected number of **bit**-operations for the computation of an isogeny between ordinary elliptic curves over $\mathbb{F}_q$ with endomorphism ring O_{K_E} is*

$$\mathcal{O}(q^{1/4+o(1)} \log^2(q) \log\log(q)).$$

Recall: We have an abelian group is acting on a set, and so there is a subexponential algorithm to solve the hidden-shift problem. This means that we can only expect *subexponential* security for the key exchange scheme; see (Childs et al., 2014). Comparing this with the situation we have nowadays with respect to the widely tolerated RSA-system this may be not so disastrous.

The Key Exchange System of De Feo

The suggestion is now to use supersingular elliptic curves over $\mathbb{F}_{p^2}$ and their properties also stated in Theorem 17. Take

$$p = r^a \cdot s^b \cdot f - 1$$

with $p \equiv 1 \mod 4$. Then

$$E_0 : Y^Z = X^3 + XZ^2$$

is a supersingular elliptic curve over $\mathbb{F}_{p^2}$. We describe the key exchange scheme invented and implemented by De Feo, Jao and Plût (De Feo et al., 2014).
As categories $\mathcal{C}_i$; $(i = 1, 2)$ are given by the **objects** are isomorphism classes of supersingular curves E over $\mathbb{F}_{p^2}$ isogenous to $\mathcal{E}_0$ and hence with

$$|E(\mathbb{F}_{p^2})| = (r^a \cdot s^b \cdot f)^2.$$

Recall that:
i) The **morphisms in** $\mathcal{C}_1$ are isogenies φ with $|\ker(\varphi)|$ dividing r^a.
ii) The **morphisms in** $\mathcal{C}_2$ are isogenies ψ with $|\ker(\psi)|$ dividing s^b.
For these categories pushouts exist. For additional information choose P_1, P_2 of order r^a and Q_1, Q_2 of order s^b in $\mathcal{E}_0(\mathbb{F}_{p^2})$.

Key Exchange:

- The Partner P_1 chooses $n_1, n_2 \in \mathbb{Z}/r^a$ and the isogeny

$$\eta : E_0 \to E_0/\langle n_1 P_1 + n_2 P_2 \rangle =: E_1.$$

- P_2 chooses $m_1, m_2 \in \mathbb{Z}/s^b$ and computes the isogeny

$$\psi : E_0/\langle m_1 Q_1 + m_2 Q_2 \rangle =: E_2.$$

- P_2 sends $(\mathcal{E}_2, \psi(P_1), \psi(P_2))$.
- P_1 can compute the common secret, the pushout of η and ψ as

$$\mathcal{E}_3 := E_2/\langle n_1 \psi(P_1) + n_2 \psi(P_2) \rangle.$$

Again **security** depends on the hardness to compute an isogeny of two elliptic curves, but now the two elliptic curves are supersingular.
State of the art: The best known algorithms have exponential complexity $p^{1/4}$ (bit-computer) resp. $p^{1/6}$ (quantum computer), and so one can hope that a prime p with 768 bit yields AES128 security level. So we have, compared with other post-quantum suggestions for key exchange schemes, a very small key size.
In contrast to the ordinary case the groups around like the class groups of left ideals in maximal orders **are not abelian**, and so the hidden shift problem is not solved till now in subexponential time.

Genus 2 curves and cryptography

Let $\mathcal{X}$ be a genus 2 curve defined over a field k (char $k \neq 2$) with Weierstrass equation

$$y^2 = f(x) = a_6 x^6 + \ldots a_1 x + a_0, \tag{3}$$

The moduli space $\mathcal{M}_2$, via the Torelli morphism, can be identified with the moduli space of the principally polarized abelian surfaces A_2 which are not products of elliptic curves. Its compactification $A_2^\star$ is the weighted projective space $\mathbb{P}^3_{(2,4,6,10)}(\bar{\mathbb{Q}})$ via the Igusa invariants J_2, J_4, J_6, J_{10}. Hence, $A_2 \cong \mathbb{P}^3_{(2,4,6,10)}(\bar{\mathbb{Q}}) \setminus \{J_{10} = 0\}$.

Jacobians with nontrivial endomorphisms are parametrized by proper subvarieties of $A_2^\star$ as follows:

- Points on the Humbert space $\mathcal{H}_{n^2}$, where $\mathcal{H}_1$ denotes the locus of abelian surfaces which are the product of two elliptic curves.
- For each quaternion ring R there are $S_{R,1}, \ldots, S_{R,k}$ Shimura curves contained in $A_2^\star$ that parametrize genus 2 curves whose Jacobians admit an optimal action of R.
- Curves whose jacobians admit complex multiplication correspond to isolated points in the moduli space.

Proposition

Jac($\mathcal{X}$) *is a geometrically simple Abelian variety if and only if it is not* (n, n) *decomposable for some* n.

Proposition

The endomorphism ring $\mathrm{End}^0_{\bar{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{X})$ *of an abelian surface is either* $\mathbb{Q}$*, a real quadratic field, a CM field of degree 4, a non-split quaternion algebra over* $\mathbb{Q}$*,* $F_1 \oplus F_2$ *where each* F_i *is either* $\mathbb{Q}$ *or an imaginary quadratic field, the Mumford-Tate group where* F *is either* $\mathbb{Q}$ *or an imaginary quadratic field.*

A word on the characteristic Frobenius polynomial

Let us recall a few facts on characteristic polynomials of Frobenius for abelian surfaces. The Weil q-polynomial arising in genus 2 have the form

$$f(T) = T^4 - aT^3 + (b + 2q)T^2 - aqT + q^2, \tag{4}$$

for $a, b \in \mathbb{Z}$ satisfying the inequalities

$$2|a|\sqrt{q} - 4q \leq b \leq \frac{1}{4}a^2 \leq 4q.$$

Let $\mathcal{X}$ be a curve of genus 2 over $\mathbb{F}_q$ and $J = \operatorname{Jac}\mathcal{X}$. Let f be the Weil polynomial of J as in 4. We have that $\#\mathcal{X}(\mathbb{F}_q) = q + 1 - a$, $\#J(\mathbb{F}_q) = f(1)$ and it lies in the genus-2 Hasse interval

$$\mathcal{H}_q^{(2)} = \left[(\sqrt{q} - 1)^4, (\sqrt{q} + 1)^4\right]$$

One can construct decomposable $(3, 3)$-jacobians with a given number of rational points by glueing two elliptic curves together.

Let K be a number field and M_K the set of norms of K. Let $\mathcal{A}$ be an abelian surface defined over K and f_v the characteristic Frobenius for every norm $v \in M_K$.

Lemma

Let v be a place of characteristic p such that $\mathcal{A}$ has good reduction. Then $\mathcal{A}_v$ is ordinary if and only if the characteristic polynomial of the Frobenius

$$f_v(x) = x^4 + ax^3 + bx^2 + apx + p^2,$$

satisfies $b \not\equiv 0 \mod p$.

Lemma ((Lombardo, 2016))

Let $\mathcal{A}$ be an absolutely simple abelian surface. The endomorphism algebra $\mathrm{End}^0_{\bar{K}}(\mathcal{A})$ is non-commutative (thus a division quaternion algebra) if and only if for every $v \in M_K$, the polynomial $f_v(x^{12})$ is a square in $\mathbb{Z}[x]$.

The following gives a condition for geometrically reducible abelian surfaces.

Proposition

If $\mathcal{A}/K$ is geometrically reducible then for all $v \in M_k$ for which $\mathcal{A}$ has good reduction the polynomial $f_v(x^{12})$ is reducible in $\mathbb{Z}[x]$.

Proposition

If $\mathcal{X}$ is a smooth, irreducible genus 2 curve with affine equation $y^2 = f(x)$ such that $f(x) \in K[x]$ is an irreducible polynomial of degree 5 then $\mathrm{Jac}\,\mathcal{X}$ is absolutely irreducible.

In (Lombardo, 2016) is given a detailed account of all the cases and an algorithm how to compute $\mathrm{End}_K\,\mathcal{A}$.

Isogenies

Let $\mathcal{X}$ be a curves of genus 2 defined over a perfect field k such that char $k \neq 2$ and $\mathcal{J} = \mathrm{Jac}(\mathcal{X})$ its Jacobian. Fix a prime $\ell \geq 3$ and let S be a maximal ℓ-Weil isotropic subgroup of $\mathcal{J}[n]$. From Theorem 17 we have $S \cong (\mathbb{Z}/\ell\mathbb{Z})^2$. Let $\mathcal{J}' := \mathcal{J}/S$ be the quotient variety and $\mathcal{Y}$ a genus 2 curve such that $\mathrm{Jac}(\mathcal{Y}) = \mathcal{J}'$. Hence, the classical isogeny problem becomes to compute $\mathcal{Y}$ when given $\mathcal{X}$ and S.

If $\ell = 2$ this problem is done with the Richelot construction. Over finite fields this is done in (Lubicz and Robert, 2012) using theta-functions.

For $\mathcal{X}$ given as in Eq. (3), we have the divisor at infinity

$$D_\infty := (1 : \sqrt{f(x)} : 0) + (1 : -\sqrt{f(x)} : 0)$$

The Weierstrass points of $\mathcal{X}$ are the projective roots of $f(x)$, namely $w_i := (x_i, z_i)$, for $i = 1, \ldots, 6$ and the Weierstrass divisor $W_\mathcal{X}$ is

$$W_\mathcal{X} := \sum_{i=1}^{6} (x_i, 0, z_i).$$

A canonical divisor on $\mathcal{X}$ is

$$\mathcal{K}_\mathcal{X} = W_\mathcal{X} - 2D_\infty.$$

Let $D \in \mathrm{Jac}\,\mathcal{X}$, be a divisor expressed as $D = P + Q - D_\infty$. The effective divisor $P + Q$ is determined by an ideal of the form $(a(x), b(x)$ such that $a(x) = y - b(x))$, where $b(x)$ is a cubic and $a(x)$ a monic polynomial of degree $d \leq 2$.

We can define the ℓ-tuple embedding $\rho_{2\ell} : \mathbb{P}^2 \to \mathbb{P}^{2\ell}$ by

$$(x, y, z) \to (z^{2\ell}, \ldots, x^i z^{2\ell - i}, x^{2\ell})$$

and denote the image of this map by $\mathcal{R}_{2\ell}$. It is a rational normal curve of degree 2ℓ in $\mathbb{P}^{2\ell}$. Hence, any $2\ell + 1$ distinct points on $\mathcal{R}_{2\ell}$ are linearly independent. Therefore, the images under $\rho_{2\ell}$ of the Weierstrass points of $\mathcal{X}$ are linearly independent for $\ell \geq 3$. Thus, the subspace

$$W := \langle \rho_{2\ell}(W_{\mathcal{X}}) \rangle \subset \mathbb{P}^{2\ell}$$

is 5-dimensional. For any pair of points P, Q in $\mathcal{X}$, the secant line $\mathcal{L}_{P,Q}$ is defined to be the line in $\mathbb{P}^{2\ell}$ intersecting $\mathcal{R}_{2\ell}$ in $\rho_{2\ell}(P) + \rho_{2\ell}(Q)$. In other words,

$$\mathcal{L}_{P,Q} = \begin{cases} \langle \rho_{2\ell}(P), \rho_{2\ell}(Q) \rangle & \text{if } P \notin \{Q, \tau(Q)\} \\ T_{\rho_{2\ell}(P)}(\mathcal{R}_{2\ell}) & \text{otherwise .} \end{cases}$$

Theorem ((Dolgachev and Lehavi, 2008))

There exists a hyperplane $H \subset \mathbb{P}^{2\ell}$ such that:

- *H contains W and*
- *the intersection of H with the secants $\mathcal{L}_e$ for each nonzero $e \in S$ are contained in a subspace N of codimension 3 in H.*

The image of the Weierstrass divisor under the map $\mathbb{P}^{2\ell} \to \mathbb{P}^3$ with centre N lies on a conic $\mathcal{C}$, and the double cover of $\mathcal{C}$ ramified over this divisor is a stable curve $\mathcal{Y}$ of genus 2 such that $\operatorname{Jac} \mathcal{Y} \cong \operatorname{Jac} \mathcal{X}/S$.

This was used by Smith (Smith, 2012) to devise an algorithm for determining $\mathcal{Y}$ and ϕ. The algorithm works well for $\ell = 3$.

Genus 3 curves and cryptography

For $g = 3$ a generic cover has degree three and 9 branch points. The signature is $\sigma = (\sigma_1, \ldots, \sigma_9)$ where $\sigma_i \in S_3$ is an transposition for $i = 1, \ldots, 8$ and σ_9 is the 3-cycle.

Lemma ((Shaska and Thompson, 2005))

Let $\mathcal{X}$ be a generic curve of genus 3 defined over a field k, char $k \neq 2, 3$. Then, there is a degree 3 covering $\psi : \mathcal{X} \to \mathbb{P}^1$ of full moduli dimension. Moreover, $\mathcal{X}$ is isomorphic to a curve with affine equation

$$Y^3(X + a) + Y^2(bX + c) + Y(dX^2 + eX) + X^3 + fX^2 + X = 0$$

for $a, b, c, d, e, f \in \bar{k}$ such that $\Delta \neq 0$, where Δ is the discriminant of the quartic.

Such curves are non-hyperelliptic. Their isomorphism classes are determined invariants of ternary quartics, (Dixmier, 1987). The discriminant of curve with respect to Y is given by

$$\Delta(X) = -X(27X^7 + A_6X^6 + A_5X^5 + A_4X^4 + A_3X^3 + A_2X^2 + A_1X + 4c^3)$$

where $A_1, \ldots A_6 \in k[a, b, c, d, e, f]$. The branch points of the cover $\psi : \mathcal{X} \to \mathbb{P}^1$ coalesce when $\Delta(X)$ has multiple roots. Thus, its discriminant Δ in X is $\Delta = 0$. There are four factors of the discriminant

$$\Delta = \Delta_1 \cdot \Delta_2 \cdot \Delta_3 \cdot \Delta_4 = 0,$$

each corresponding to one of the degenerate cases, which are obtained when the branch points of ψ coalesce. The information for the corresponding Hurwitz spaces is given in (Shaska and Thompson, 2005, Table 1).

Hyperelliptic Curves

Let $\mathcal{X}$ be a hyperelliptic curve of genus 3 over the field k, such that $\mathrm{char(k)} \neq 2$. Then there is a degree 2 cover map $\pi : \mathcal{X} \to \mathbb{P}^1$, which is uniquely determined up to automorphisms of $\mathbb{P}^1$. This cover is Galois, and the non-trivial automorphism on $\mathcal{X}$ fixing $\mathbb{P}^1$ is the the hyperbolic involution ω. Hence, we can give $\mathcal{X}$ by a plane projective Weierstrass equation, which has an affine part

$$\mathcal{X}_a : y^2 = f(x)$$

invariant under ω and

$$\mathbb{P}^1 \setminus \pi(\mathcal{X}_a) =: \{P_\infty\} \subset \mathbb{P}^1(k).$$

Moreover, $\deg(f) = 7$ if the fiber $\pi^{-1}(P_\infty) = \mathcal{X}(k) \setminus \mathcal{X}_a(k)$ has a unique point (i.e. P_∞ is a k- rational Weierstraß point of $\mathcal{X}$) and $\deg(f) = 8$ otherwise.
Since $\mathcal{X}$ is determined up to automorphisms of $\mathbb{P}^1$ we get that the hyperelliptic locus of curves of genus 3 is a 5-dimensional subspace of the moduli space $\mathcal{M}_3$. In fact, there is a system of invariants that describes this locus, namely the Shioda invariants $J_2, \ldots, J_8$ as described in (Shioda, 1967), (Shaska, 2014).

Remark

This explains why it is very hard to use constructions of curves of genus 3*, for instance as modular curves (*(Weng, 2001)*) or by CM-methods (*(Weng, 2001)*) to find hyperelliptic curves. A rough and heuristic argument is that (for large q) the probability to find a point in* $\mathcal{M}_3(\mathbb{F}_q)$ *that corresponds to a hyperelliptic curve is* $1/q$.

Picard Groups of Curves of Genus 3 in Cryptography

The following is the natural question when considering genus $g = 3$ cryptography.

Question
Can one use Picard groups of curves of genus 3 *for DL-systems?*

Addition As pointed out above, there are relatively fast algorithms which allow addition in Picard groups of curves of any genus (at least if one knows a relatively simple plane model found after a pre-computation).
We recall the general procedure: We assume that there is a point $P_\infty \in \mathcal{X}(k)$ with corresponding prime divisor $\mathfrak{p}_\infty$. In the divisor classes $c_1, c_2 \in \mathrm{Pic}_k^0 \mathcal{X}$ we choose convenient divisors D_i, e.g.

$$D_i = E_i - d \cdot \mathfrak{p}_\infty,$$

with E_i an effective divisor of degree $d \leq g$. Then $c_1 + c_2$ is the divisor class of

$$E_1 + E_2 - (d_1 + d_2)\mathfrak{p}_\infty,$$

and the "reduction algorithm" has to compute a divisor

$$E_3 - d_3\mathfrak{p}_0 \sim E_1 + E_2 - (d_1 + d_2)\mathfrak{p}_\infty$$

with $d_3 \leq g$. This is an interpolation problem solved by Hess by the computation of Riemann-Roch spaces; see (Hess, 2002) for details.

Theorem (Diem, Hess)

Let $\mathcal{X}$ be a genus $g \geq 2$ curve defined over $\mathbb{F}_q$. The arithmetic in the degree 0 class group of $\mathcal{X}$ can be performed in the expected time, which is polynomially bounded in g and $\log q$.

For curves of genus 3 it is convenient to distinguish between non-hyperelliptic and hyperelliptic curves. In the first case one can give $\mathcal{X}$ easily as smooth quartic. Using its geometry one finds, concretely given, fast addition algorithms, which can be found in work of Oyono et al; see (Flon et al., 2008). As we shall see below the hardness of the DL is insufficient for cryptographical applications, and so the fast addition is only relevant for attacking systems. So it is enough for us to keep the existence of the addition algorithm in mind.
Next assume that $\mathcal{X}$ is hyperelliptic. We can find rather easily a Weierstrass equation, and the most convenient case is that one of its Weierstrass points is k-rational. We shall restrict to this case (often called "imaginary" because of its analogy to imaginary quadratic fields (E. Artin)) and hence we can give $\mathcal{X}$ by an affine Weierstrass equation

$$\mathcal{X}_a : y^2 = f(x),$$

where $f(x) \in k[x]$ is a monic polynomial of degree 7 without multiple roots. By homogenization we get a plane projective curve with exactly one additional point P_∞, which corresponds to a Weierstraß point of $\mathcal{X}$ and so exactly to one prime divisor $\mathfrak{p}_\infty$ of degree 1 of $\mathcal{X}$. Hence divisors on $\mathcal{X}$ are of the form $D = D_a + z \cdot \mathfrak{p}_\infty$ with D_a a divisor with support on $\mathcal{X}$.

Hence we can represent divisor classes in $\mathrm{Pic}_k^0(\mathcal{X})$ by divisors

$$D = E_a - d\,\mathfrak{p}_\infty,$$

with E_a an effective divisor of degree $d \leq 3$ and support in $\mathcal{X}_a$.

Using the special form of $\mathcal{X}_a$ we can give E_i in the so-called "Mumford presentation" as in Theorem 15 and for the reduction step of divisors we can use the very effective Cantor algorithm.

Behind these results is the analogy (developed by E. Artin) between the arithmetic of hyperelliptic function fields and imaginary quadratic fields respectively the arithmetic of quadratic forms due to C.F. Gauß.

This algorithmic approach can be translated into **formulas** (involving, alas, many special cases) that are sometimes more convenient for implementations near to specialized hardware. The generic cases for addition and doubling are explicitly given by Algorithms 14.52 and 14.53 in (Cohen et al., 2006). These additions are rather fast and not too far away from the timings of additions on elliptic curves.

Hence one may well consider to use Picard groups of curves of genus 3 for DL-based cryptographic applications. This will need fast algorithms for point counting, and before that, a security discussion.

Isogenies via S_4-Covers

As observed in (Smith, 2012) ”many” hyperelliptic curves are isogenic to non-hyperelliptic curves via an isogeny with degree dividing 8. This is interpreted in terms of Hurwitz spaces and connected modular spaces in (Frey and Kani, 2015).

Assume K is algebraically closed. For applications in cryptography one has to study rationality problems; see (Smith, 2012). The construction relies on the so-called **trigonal construction** in (Donagi and Livné, 1999).

Begin with a hyperelliptic curve $\mathcal{X}$ of genus 3 and its uniquely determined hyperelliptic projection $f_1 : \mathcal{X} \to \mathbb{P}^1$ with 8 ramification points $P_1, \cdots, P_8$. There is a map

$$f_2 : \mathbb{P}^1 \to \mathbb{P}^1$$

of degree 3 with the following properties:

- f_2 is unramified in $P_1, \cdots P_8$, its ramification points are denoted by $Q_1, \cdots Q_4$ on the base line $\mathbb{P}^1$. The ramification order in Q_i is 2, and so each Q_i has exactly one unramified extension under f_2 denoted by Q_i'.
- $f_2(\{P_1, \cdots P_8\} = \{S_1, \cdots S_4\}$ such that, after a suitable numeration, $f_2(P_i) = f_2(P_{4+i})$ for $1 \leq i \leq 4$.

Now use Galois theory.

The monodromy group of f_2

Obviously, the Galois closure $\tilde{f}_2 = f_2 \circ h_2$ of f_2 has as Galois group the symmetric group S_3 (since f_2 is not Galois because of the ramification type), and h_2 is degree 2 cover $\mathcal{E}' \stackrel{h_2}{\to} \mathcal{X}$. From Galois theory we get that $\tilde{f}_2 = \pi \circ \eta$, where

$$\eta : \mathcal{E}' \to \mathcal{E}$$

is a cyclic cover of degree 3 with Galois group equal to the alternating subgroup A_3. Then, $\mathcal{E}$ is a quadratic cover of $\mathbb{P}^1$ ramified exactly at the discriminant

$$\Delta_1 = Q_1 + \cdots + Q_4$$

of f_2. Therefore $\mathcal{E}$ is an elliptic curve with cover map π to $\mathbb{P}^1$. From construction and Abhyankar's lemma it follows that η is unramified. Hence $\mathcal{E}'$ is an elliptic curve, too, and η is an isogeny of degree 3 (after applying a suitable translation).

The monodromy group of $f = f_2 \circ f_1$

f is a cover of degree 6 and so its Galois group can be embedded into S_6.

Lemma ((Frey and Kani, 2011))

The monodromy group of f is isomorphic to S_4.

Let $\tilde{f} : \tilde{\mathcal{X}} \to \mathbb{P}^1$ be the Galois cover of curves factoring over f with Galois group S_4. Let $\mathcal{X}'$ be the subcover of $\tilde{\mathcal{X}}$ with function field equal to the composite of the function fields of $\mathcal{X}$ and $\mathcal{E}'$, i.e. the normalization of the fiber product of $\mathcal{X}$ with $\mathcal{E}'$. Let

$$\pi_{\mathcal{X}} : \mathcal{X}' \to \mathcal{X}$$

the projection to $\mathcal{X}$, which is a cover of degree 2. The Galois group of $\tilde{\mathcal{X}}/\mathcal{X}$ contains 2 transpositions. Let σ be one of them chosen such that with $G_2 = \langle \sigma \rangle$ we get $\mathcal{X}' := \tilde{\mathcal{X}}/G_2$. Hence, σ is contained in precisely two of the stabilizers $T_1, \ldots, T_4$ of the elements $\{1, 2, 3, 4\}$ on which S_4 acts. Let

$$\pi_T : \tilde{\mathcal{X}} \to \mathcal{D} := \tilde{\mathcal{X}}/T$$

be the quotient map. Then $\tilde{f}$ factors over π_T as $\tilde{f} = g \circ \pi_T$, where $g : \mathcal{D} \to \mathbb{P}^1$ has $\deg(g) = 4$. Note that g is primitive (does not factor over a quadratic subcover). We can use the Hurwitz genus formula to compute the genus of $\mathcal{D}$. For this we have to determine the ramification of $\mathcal{D}/\mathbb{P}^1$ under g.

Lemma

The genus of $\mathcal{D}$ is equal to 3*, and so is equal to the genus of $\mathcal{X}$.*

We are interested in the case that $\mathcal{J}(\mathcal{X})$ is simple. Then we get from 4 that:

Proposition

Let $\mathcal{J}_{\mathcal{X}}$ be a simple abelian variety and $\mathcal{D}$ be non-hyperelliptic. The pair of cover maps $(\pi_{\mathcal{X}}, \pi_T)$ from $\mathcal{X}'$ to $(\mathcal{X}, \mathcal{D})$ induces an isogeny

$$\eta : \mathcal{J}_{\mathcal{X}} \to \mathcal{J}_{\mathcal{D}},$$

whose kernel is elementary-abelian and has degree ≤ 8.

A more detailed analysis due to E. Kani shows that the proposition is true without the assumption that $\mathcal{D}$ is non-hyperelliptic. Then we have the following:

Corollary

Let K be equal to $\mathbb{F}_q$ and assume that $\mathcal{D}$ is non-hyperelliptic. Then the computation of the Discrete Logarithm in $\mathrm{Pic}^0_{\mathcal{X}}$ *has complexity $\mathcal{O}(q)$.*

This result motivates the question whether the assumptions of the Corollary are often satisfied. Empirically, B. Smith has given a positive answer. A rigorous answer is given in (Frey and Kani, 2015).

We have already explained that by the construction of a $(2,3)$-cover as above we have found a generically finite and dominant morphism from a Hurwitz space $\mathcal{H}_\infty$ to the hyperbolic locus in the moduli space $\mathcal{M}_3$ of curves of genus 3. Hence $\mathcal{H}_\infty$ is a scheme of dimension 5.

Via the trigonal construction we have, to each hyperelliptic curve $\mathcal{X}$, found a curve $\mathcal{D}$ of genus 3 with a cover map

$$g : \mathcal{D} \to \mathbb{P}^1$$

with $\deg(g) = 4$ and the monodromy group of g equal to S_4. Moreover, a detailed study of the construction allows to determine the ramification type of g in the generic case:

There are 8 ramification points of g, exactly 4 points $P_1, \ldots, P_4$ amongst them are of type $(2,2)$ (i.e. $g^*(P_i) = 2(Q_{i,1} + Q_{i,2})$, and the other 4 ramification points are of type $(2,1,1)$. Hence $(\mathcal{D}, g)$ yields a point in a Hurwitz space $\mathcal{H}_2$ of dimension 5.

In (Frey and Kani, 2015) one discusses the hyperelliptic locus $\mathcal{H}_{hyp}$ in $\mathcal{H}_2$. The computational part of this discussion determines conditions for the coefficients of Weierstraß equations for curves $\mathcal{D}$ lying in $\mathcal{H}_{hyp}$. This is rather complicated, but one sees that generically these coefficients are parametrized by a 4-dimensional space. Rather deep and involved geometric methods have to be used to transfer these computations into scheme-theoretical results and to get

Theorem

The Hurwitz space $\mathcal{H}_{hyp}$ is a unirational, irreducible variety of dimension 4, provided that char$(K) > 5$. Moreover, the natural forget map

$$\mu : \mathcal{H}_{hyp} \to \mathcal{M}_3$$

to the moduli space $\mathcal{M}_3$ of genus 3 curves has finite fibers and so its image is also irreducible of dimension 4.

Corollary

We take the notation from above. We assume that K is algebraically closed. There is a one-codimensional subscheme U of $\mathcal{M}_{3,hyp}$ such that for $\mathcal{X} \notin U$ the isogeny η maps $\mathcal{J}_{\mathcal{X}}$ to the Jacobian of a non-hyperelliptic curve $\mathcal{D}$.

Replacing the algebraically closed field K by a finite field $\mathbb{F}_q$ one has to study rationality conditions for η. This is done in (Smith, 2012) and (Frey and Kani, 2015). Then,

Corollary

There are $\mathcal{O}(q^5)$ isomorphism classes of hyperelliptic curves of genus 3 defined over $\mathbb{F}_q$ for which the discrete logarithm in the divisor class group of degree 0 has complexity $\mathcal{O}(q)$, up to log-factors. Since $|\mathrm{Pic}^0(C)| \sim q^3$, the DL system of these hyperelliptic curves of genus 3 is weak.

Resistance against the Trigonal Attack

Let $\mathcal{X}$ be a hyperelliptic curve with an automorphism φ of order 4. We apply the trigonal construction.

First we see that φ induces an automorphism $\varphi_{\mathbb{P}^1}$ of order 2 on $\mathbb{P}^1$, taken as subcover of $\mathcal{X}$ under f_1. Since cross ratios are not changed by automorphisms we see that there is an extension of $\varphi_{\mathbb{P}^1}$ to the elliptic curve $\mathcal{E}'$ having order 4 and so to an automorphism φ' of the curve $\mathcal{X}'$ of order 4.

Now we have exactly two choices for the construction of $\mathcal{D}$ as subcover of $\mathcal{X}'$, and this yields that at least two of the curves $\mathcal{D}^{(\varphi')^j}$, $j = 0, 1, 2, 3$, have to be equal, and so $\mathcal{D}$ has an automorphism of order 2 and is, because of the simplicity of $\mathcal{J}$, hyperelliptic.

Conclusion: Hyperelliptic curves with automorphisms of order 4 are resistant against the trigonal attack.

Lemma ((Frey and Shaska, 2018))

Let $\mathcal{X}$ be a hyperelliptic curve with an automorphism of order 4 and with simple Jacobian variety $\mathcal{J}$ and

$$\eta : \mathcal{J} \to \mathcal{J}'$$

an isogeny with $\mathcal{J}'$ principally polarized. Then $\mathcal{J}'$ is the Jacobian variety of a hyperelliptic curve.

Hence, it follows that a ”minimal bad” isogeny has to have a two-power and rather large degree.

References

Oort, Frans. 1988. *Endomorphism algebras of abelian varieties*, Algebraic geometry and commutative algebra, Vol. II, pp. 469–502. MR977774

Lombardo, Davide. 2016. *Computing the geometric endomorphism ring of a genus 2 jacobian*, arxiv.

Stichtenoth, Henning. 2009. *Algebraic function fields and codes*, Second, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin. MR2464941

Mumford, David. 2008. *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Published for the Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition. MR2514037

Gaudry, P., F. Hess, and N. P. Smart. 2002. *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15**, no. 1, 19–46. MR1880933

Deuring, Max. 1941. *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14**, 197–272. MR0005125

Childs, Andrew, David Jao, and Vladimir Soukharev. 2014. *Constructing elliptic curve isogenies in quantum subexponential time*, J. Math. Cryptol. **8**, no. 1, 1–29. MR3163097

De Feo, Luca, David Jao, and Jérôme Plût. 2014. *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol. **8**, no. 3, 209–247. MR3259113

Lubicz, David and Damien Robert. 2012. *Computing isogenies between abelian varieties*, Compos. Math. **148**, no. 5, 1483–1515. MR2982438

Dolgachev, I. and D. Lehavi. 2008. *On isogenous principally polarized abelian surfaces*, Curves and abelian varieties, pp. 51–69. MR2457735

Smith, Benjamin. 2012. *Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method*, Arithmetic, geometry, cryptography and coding theory, pp. 159–170. MR2961408

Shaska, T. and J. L. Thompson. 2005. *On the generic curve of genus 3*, Affine algebraic geometry, pp. 233–243. MR2126664

Dixmier, J. 1987. *On the projective invariants of quartic plane curves*, Adv. in Math. **64**, no. 3, 279–304. MR888630

Shioda, Tetsuji. 1967. *On the graded ring of invariants of binary octavics*, Amer. J. Math. **89**, 1022–1046. MR0220738

Shaska, T. 2014. *Some remarks on the hyperelliptic moduli of genus 3*, Comm. Algebra **42**, no. 9, 4110–4130. MR3200084

Weng, Annegret. 2001. *A class of hyperelliptic CM-curves of genus three*, J. Ramanujan Math. Soc. **16**, no. 4, 339–372. MR1877806

Hess, F. 2002. *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic