Contemporary Mathematics
Volume **724**, 2019
https://doi.org/10.1090/conm/724/14596

Curves, Jacobians, and cryptography

Gerhard Frey and Tony Shaska

Abstract. The main purpose of this paper is to give an overview over the theory of abelian varieties, with main focus on Jacobian varieties of curves reaching from well-known results till to latest developments and their usage in cryptography. In the first part we provide the necessary mathematical background on abelian varieties, their torsion points, Honda-Tate theory, Galois representations, with emphasis on Jacobian varieties and hyperelliptic Jacobians. In the second part we focus on applications of abelian varieties on cryptography and treating separately, elliptic curve cryptography, genus 2 and 3 cryptography, including Diffie-Hellman Key Exchange, index calculus in Picard groups, isogenies of Jacobians via correspondences and applications to discrete logarithms. Several open problems and new directions are suggested.

Preface

There has been a continued interest on Abelian varieties in mathematics during the last century. Such interest is renewed in the last few years, mostly due to applications of abelian varieties in cryptography. In these notes we give a brief introduction to the mathematical background on abelian varieties and their applications on cryptography with the twofold aim of introducing abelian varieties to the experts in cryptography and introducing methods of cryptography to the mathematicians working in algebraic geometry and related areas.

A word about cryptography. Information security will continue to be one of the greatest challenges of the modern world with implications in technology, politics, economy, and every aspect of everyday life. Developments and drawbacks of the last decade in the area will continue to put emphasis on searching for safer and more efficient crypto-systems. The idea and lure of the quantum computer makes things more exciting, but at the same time frightening.

There are two main methods to achieve secure transmission of information: *secret-key cryptography* (*symmetric-key*) and *public-key cryptography* (*asymmetric-key*). The main disadvantage of symmetric-key cryptography is that a shared key must be exchanged beforehand in a secure way. In addition, managing keys in a large public network becomes a very complex matter. Public-key cryptography is used as a complement to secret-key cryptography for signatures , authentication and key-exchange. There are two main methods used in public-key cryptography, namely RSA and the discrete logarithm problem (DLP) in cyclic groups of prime

2010 *Mathematics Subject Classification.* Primary 14H10, 14H45.

order which are embedded in rational points of Abelian varieties, in particular of Jacobian varieties of curves. The last method is usually referred to as *curve-based cryptography*.

In addition, there is always the concern about the post-quantum world. What will be the crypto-systems which can resist the quantum algorithms? Should we develop such systems now? There is enthusiasm in the last decade that some aspects of curve-based cryptography can be adapted successfully to the post-quantum world. Supersingular Isogeny Diffie-Hellman (SIDH), for example, is based on isogenies of supersingular elliptic curves and is one of the promising schemes for post-quantum cryptography. Isogenies of hyperelliptic Jacobians of dimension 2 or 3 have also been studied extensively in the last decade and a lot of progress has been made. In this paper we give an overview of recent developments in these topics.

Audience. Computer security and cryptography courses for mathematics and computer science majors are being introduced in all major universities. Curve-based cryptography has become a big part of such courses and a popular area even among professional mathematicians who want to get involved in cryptography. The main difficulty that these newcomers is the advanced mathematical background needed to be introduced to curve-based cryptography.

Our target audience is advanced graduate students and researchers from mathematics or computer science departments who work with curve-based cryptography. Many researchers from other areas of mathematics who want to learn about abelian varieties and their use in cryptography will find these notes useful.

Notations and bibliography. The symbols $\mathbb{N}$ and $\mathbb{Z}$ will denote the natural numbers and the ring of integers while $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ the fields of rationals, reals, and complex numbers. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ will denote the field of p elements, for a prime number p and $\mathbb{F}_q$ a field of q elements, where $q = p^n$ is a power of p.

In general a field will be denoted by k. We shall always assume that k is a perfect field, i.e., every algebraic extension of k is separable. Denote its characteristic by $\operatorname{char} k$, and its algebraic closure by $\bar{k}$. The Galois group $\operatorname{Gal}(\bar{k}/k)$ will be denoted by G_k. A number field will be denoted by K and its ring of integers by $\mathcal{O}_K$.

By a "curve" we mean an irreducible, smooth, projective algebraic curve. A genus $g \geq 2$ curve defined over k will be denoted by $\mathcal{C}/k$ or sometimes by $\mathcal{C}_g$ and its Jacobian by $\operatorname{Jac}_{\mathcal{C}}$. The automorphism group of $\mathcal{C}$ GF is denoted by $\operatorname{Aut}\mathcal{C}$ and it means the full group of automorphisms of $\mathcal{C}$ over the algebraic closure $\bar{k}$.

We will use $\mathcal{A}$, $\mathcal{B}$ to denoted Abelian varieties defined over a field k and $k(\mathcal{A})$, $k(\mathcal{B})$ their function fields. The set of n-torsion points of $\mathcal{A}$ will be denoted by $\mathcal{A}[n]$. For a subscheme G of $\mathcal{A}$, the quotient variety is denoted by $\mathcal{A}/G$.

Background and preliminaries. We assume the reader is familiar with the basic tools from algebra and algebraic geometry. Familiarity with algebraic curves is expected and the ability to read some of the classical works on the subject [**56**].

Organization of these notes. In Part 1 we give the mathematical background on Abelian varieties, their torsion points, endomorphisms and isogenies. We focus mostly on Abelian varieties defined over fields of positive characteristic. The main references here are [**56**], and [**21**].

We give a brief introduction of abelian varieties as complex tori with period matrices in Section 1. Of course, of special interest for us are Jacobian varieties,

hence we define in detail algebraic curves, constant field extensions, group schemes, and principally polarized varieties.

In Section 2 we focus on endomorphism rings of abelian varieties and isogenies, the characteristic polynomial of the Frobenius, l-adic Tate module, and Tate's result on determining necessary and sufficient conditions for two Abelian varieties to be isogenous.

Algebraic curves and Jacobian varieties are treated in detail in Section 3, including Picard groups on curves, the group of divisors, canonical divisors, Riemann-Roch theorem, and the definition of Jacobians of curves.

In Section 4 we focus on applications of the Riemann-Roch theorem, including the Hurwitz genus formula, gonality of curves and Hurwitz spaces, Cantor's algorithm on Jacobians of hyperelliptic curves, and automorphism groups of curves and their Jacobians. As illustration and for later applications curves of small genus are discussed in more detail.

In Section 5 we give a brief description of the theory of modular curves over $\mathbb{C}$, modular polynomials, and the arithmetic theory of modular curves.

In Part 2 we focus on applications of abelian varieties on cryptography. Our main reference is [**7**] and the material provided in Part 1.

In Section 6 we go over the preliminaries of the Diffie-Hellman Key Exchange and the mathematical challenges including Q-bit security, Key Exchange with G-sets, and the abstract setting of Key Exchange.

In Section 7 we describe the methods of index calculus in Picard groups and their use in cryptography. Such methods have been quite successful due to work of Diem, Gaudry, et al. As consequence one sees that only elliptic and hyperelliptic curves of genus ≤ 3 provide candidates for secure crypto systems based on discrete logarithms. Hence we shall discuss these curves in detail. In Section 8 we focus on isogenies of Jacobians via correspondences. We discuss the Weil descent, modular correspondences, and correspondences via monodromy groups. It is an open and difficult problem to find interesting correspondences of low degree between Jacobian varieties induced by correspondences between curves.

In Section 9 we study hyperelliptic Jacobians of dimension 3. We give a short introduction of non-hyperelliptic and hyperelliptic genus 3 curves and their plane equations. Then we define Picard groups of genus 3 curves and their use in cryptography and results of Diem and Hess. In the following part we describe the index-calculus attacks applied to genus 3 and results of Diem, Gaudry, Thomé, Thériault. We also discuss isogenies via S_4-covers and work of Frey and Kani [**22**], [**23**] and Smith [**66**].

In Section 4.2.7 we focus on dimension 2 Jacobians and their use in cryptography. Methods based on [**47**] of how to compute the endomorphism ring of a dimension 2 Jacobian are described and in particular isogenies of Abelian surfaces via Donagi-Livné approach and some recent results of Smith [**66**]. Further we give details of point counting algorithms on genus 2 Jacobians and explicit formulas for $[n]D$, when D is a reduced divisor. Work of Gaudry, Harley, Schost and others is briefly described. In Section 11 we focus on the elliptic curves and elliptic curve cryptography. We give an explicit description of the methods used in supersingular isogeny-based cryptography. We describe the necessary background including Velu's formula, ordinary and supersingular elliptic curves and the more recent results [**11**], [**10**], [**12**] among others.

Part 1. Abelian varieties

In the first part of these notes we give the basic theory of abelian varieties, their endomorphisms, torsion points, characteristic polynomial of the Frobenius, Tate models, and then focus on Jacobian varieties and hyperelliptic Jacobians. While there are many good references on the topic, we mostly use [**56**], [**69**].

1. Definitions and basic properties

We shall use projective respectively affine *schemes* defined over k. Let $n \in \mathbb{N}$ and I_h (respectively I) be a homogeneous ideal in $k[Y_0, \cdots, Y_n]$ different from $\langle Y_0, \dots Y_n \rangle$ (respectively an arbitrary ideal in $k[X_1, \dots, X_n]$).

Let $R_h := k[Y_0, \dots, Y_n]/I_h$ (respectively $R := k[X_1, \dots, X_n]/I$) be the quotients. By assumption, R_h is a graded ring, and so localizations $R_{h,\mathfrak{A}}$ with respect to homogeneous ideals $\mathfrak{A}$ are graded, too. Let $R_{h,\mathfrak{A}\ 0}$ be the ring of elements of grade 0.

The projective scheme $\mathcal{S}_h$ (respectively the affine scheme $\mathcal{S}$) defined by I_h (I) consists of

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

Examples:

(1) The projective space $\mathbb{P}^n$ over k of dimension n is given by the ideal $\langle 0 \rangle \subset k[Y_0, \dots, Y_n]$. The ring of holomorphic functions on $\mathbb{P}^n$ (take $U = \mathbb{P}^n$) is k.

    Next take $U = \emptyset$ to get the ring of *meromorphic* functions on $\mathbb{P}^n$: It consists of the quotients

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

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

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

    The ring of holomorphic functions on A^n is $k[X_1, \dots, X_n]$, 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 $k(X_1, \dots, X_n)$.
(3) 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 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 $\mathcal{S}$. The reader should verify that for projective schemes defined by the ideal I_h the

set $\mathcal{S}(k)$ is, in a natural way, identified with points $(y_0 : y_1 \cdots : y_n)$ with k-rational homogeneous coordinates in the projective space of dimension n which are common zeros of the polynomials in I_h, and an analogous statement holds for affine schemes.

Constant field extensions: Let $k \overset{\iota}{\hookrightarrow} L$ be an embedding of k into a field L (or $k \subset L$ if the embedding is clear) of k. Let $\mathcal{S}$ be a projective (affine) scheme defined over k with ring R. ι induces a morphism $\mathfrak{f}_\iota$ 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 ideal $I_{\mathcal{S}}$ extends to a ideal in R_ι and hence we get in a natural way a projective scheme $\mathcal{S}_\iota$ with a morphism

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

as Spec(k) schemes. $\mathcal{S}_\iota$ is again a projective (affine) scheme now defined over L, which is denoted as *scalar extension* by ι. If there is no confusion possible (for instance if $k \subset L \subset \bar{k}$ and ι is the inclusion) we denote $\mathcal{S}_\iota$ 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*.

Affine covers There are many possibilities to embed $\mathbb{A}^n$ into $\mathbb{P}^n$, and there is no "canonical" way to do this. But after having chosen coordinates there is a standard way to construct a covering of $\mathbb{P}^n$ by $n+1$ copies of $\mathbb{A}^n$. Every homogeneous polynomial $P(Y_0, ..., Y_n)$ can be transformed into $n+1$ polynomials $p_j(X)$ $(j = 0, ..., n)$ in n variables by the transformation

$$t_j : Y_i \mapsto X_i := Y_i / Y_j.$$

Define U_j as open subscheme of $\mathbb{P}^n$ which is the complement of the projective scheme attached to the ideal $\langle Y_j \rangle$. Then $t_j \,_{|U_j}$ is holomorphic and bijective and its image is isomorphic to $\mathbb{A}^n$.

By the inverse transform ι_j we embed $\mathbb{A}^n$ into $\mathbb{P}^n$ and so U_j is isomorphic to $\mathbb{A}^n$ as affine variety. Taking the collection $(\iota_0, \ldots \iota_n)$ we get a finite open covering of $\mathbb{P}^n$ by $n+1$ affine subspaces.

Having an affine cover U_j of $\mathbb{P}^n$ one can intersect it with projective varieties V and get

$$V = \bigcup_j V_{j,a} \quad \text{with} \quad V_{j,a} := V \cap U_j$$

as union of affine varieties.

Converse process: Given a polynomial $p(X_1, ..., X_n)$ of degree d we get a homogeneous polynomial $p^h(Y_0, ..., Y_n)$ of degree d by the transformation

$$X_i \mapsto Y_i / Y_0 \text{ for } i = 1, \ldots, n$$

and then clearing denominators. Assume that V_a is an affine variety with ideal $I_a \subset k[X_1, \ldots, X_n]$. By applying the homogenization explained above to all polynomials in I_a we get a homogeneous ideal $I_a^h \subset k[Y_0, ..., Y_n]$ and a projective variety V with ideal I_a^h containing V_a in a natural way. V is called a projective closure of V_a. By abuse of language one calls $V \cap U_0 = V \setminus V_a$ "infinite points" of V_a.

Function fields: Let $\mathcal{S} \subset \mathbb{A}^n$ be an affine irreducible variety with ring R. In particular, R is an integral domain. The function field $k(\mathcal{S})$ is the quotient field of R. It consists of the meromorphic functions of $\mathbb{A}^n$ restricted to $\mathcal{S}$. $\mathcal{T}$ is birational equivalent to $\mathcal{S}$ if and only if $k(\mathcal{S}) = k(\mathcal{T})$.

If $U \neq \emptyset$ is affine and open in a projective variety $\mathcal{S}$ then the field of meromorphic functions $k(\mathcal{S}) = k(U)$. In particular, it is independent of U.

DEFINITION 1. Let $\mathcal{S}$ be an irreducible variety. The dimension of $\mathcal{S}$ is the transcendental degree of $k(\mathcal{S})$ over k.

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 is compatible with the addition law is a homomorphism.

Let L be a field extension of k. $G(L)$ denotes 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 an absolutely irreducible projective variety, then the group law m is commutative.

DEFINITION 2. An Abelian variety defined over k is an absolutely irreducible projective variety defined over k which is a group scheme.

We will denote an Abelian variety defined over a field k by $\mathcal{A}_k$ or simply $\mathcal{A}$ when there is no confusion. From now on the addition $m(P, Q)$ in an abelian variety 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 $\mathcal{A}_1$ to the Abelian variety $\mathcal{A}_2$ 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 a field 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.

1.1. Complex tori and abelian varieties. Though we are interested in Abelian varieties over arbitrary fields k or in particular, over finite fields, it is helpful to look at the origin of the whole theory, namely the theory of Abelian varieties over the complex numbers. Abelian varieties are connected, projective algebraic group schemes. Their analytic counterparts are the connected compact Lie groups.

Let d be a positive integer and $\mathbb{C}^d$ the complex Lie group (i.e., with vector addition as group composition). The group $\mathbb{C}^d$ 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 $\mathbb{C}^d/\Lambda$ 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

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

Then, we have the following.

LEMMA 1. *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 $\hat{\Lambda}$ given by

$$\hat{\Lambda} := \{x \in \mathbb{C}^d \,|\, E(x,y) \in \mathbb{Z},\ \text{ for all }\ y \in \Lambda\}$$

is called the **dual lattice** of Λ. If $\hat{\Lambda} = \Lambda$ then E is called a *principal polarization* on $\mathcal{A}$ and the pair $(\mathcal{A}, E)$ is called a **principally polarized** abelian variety; we may also say that $\mathcal{A}$ admits a principal polarization.

For a principally polarized abelian variety $(\mathcal{A}, E)$ there exists a basis $\{\mu_1, \ldots, \mu_{2d}\}$ of Λ such that

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

The symplectic group

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

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

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

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

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

Jacobian varieties of projective irreducible nonsingular curves admit canonical principal polarizations. These Abelian varieties are in the center of our interest and will be discussed in detail in Section 3.

1.1.1. *Elliptic curves over* $\mathbb{C}$. Take $d = 1$ and a lattice $\Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$ with τ in the upper half plane $\mathbb{H}_1 = \mathbb{H}$. The torus $\mathbb{C}/\Lambda_\tau$ is a compact Riemann surface and so an algebraic projective curve $\mathcal{E}_\tau$ over $\mathbb{C}$.

The function field $\mathbb{C}(\mathcal{E}_\tau)$ is generated by the Weierstrass function $\wp_\tau$ and its derivative $\wp'_\tau$, which are meromorphic functions on $\mathbb{C}$ with periods $1, \tau$ and poles of order 2 respectively 3 in Λ_τ. $\wp_\tau$ satisfies a differential equation

$$W_\tau : \wp'^2_\tau = \wp^3_\tau - g_2(\tau)\wp^2_\tau - g_3(\tau).$$

This is an affine equation for $\mathcal{E}_\tau$, by introducing homogeneous coordinates $(X : Y : Z)$ by $\wp_\tau = X/Z, \wp'_\tau = Y/Z$, we get the projective plane curve $\mathcal{E}_\tau$ with equation

$$Y^2Z = X^3 - g_2(\tau)XZ^2 - g_3(\tau)Z^3$$

with coefficients $g_2(\tau), g_3(\tau)$ depending on Λ_τ in a very specific way: g_2 and g_3 are Eisenstein series in τ. It follows that $\Delta_\tau = 4g_2(\tau)^3 - 27g_3(\tau)^2 \neq 0$ and so $\mathcal{E}$ is without singularities. We get a parametrization

$$\phi : \mathbb{C} \to \mathcal{E}_\tau(\mathbb{C})$$

by

$$z \mapsto (\wp_\tau(z) : \wp'_\tau(z) : 1) \text{ if and only if } z \notin \Lambda_\tau$$

and $\phi(\Lambda_\tau) = (0 : 1 : 0)$, the point at infinity. This parametrization yields on $\mathcal{E}_\tau$ an addition and makes $\mathcal{E}_\tau$ to an Abelian variety of dimension 1 over $\mathbb{C}$.

Definition 3. An Abelian variety of dimension 1 is called an **elliptic curve**.

We have seen that we can attach to every elliptic curve $\mathcal{E}$ an element $\tau \in \mathbb{H}$ such that $\mathcal{E}$ is isomorphic to $\mathcal{E}_\tau$. Let $\mathcal{E}_{\tau'}$ be another elliptic curve. Then $\mathcal{E}_\tau$ is isomorphic to $\mathcal{E}_{\tau'}$ if and only if τ is equivalent to τ' under the action of $Sp(2d, \mathbb{Z}) = Sl(2, \mathbb{Z})$ on $\mathbb{H}$.

Since $\mathbb{H}/Sl(2, \mathbb{Z})$ is as Riemann surface isomorphic to $\mathbb{A}^1$ we get a one-to-one correspondence between isomorphism classes of elliptic curves over $\mathbb{C}$ and points on the affine line. This correspondence is given by a modular function (i.e. a holomorphic function on $\mathbb{H}$ invariant under $Sl(2, \mathbb{Z})$): the j-function.

Definition 4. The absolute invariant of $\mathcal{E}_\tau$ is given by $j(\tau) := 12^3 \frac{4g_2^3(\tau)}{\Delta_\tau}$.

Theorem 5. *$\mathcal{E}_\tau$ is isomorphic to $\mathcal{E}_{\tau'}$ if and only it $j(\tau) = j(\tau')$. Hence the j-function is an analytic map from $\mathbb{A}^1$ to $\mathbb{A}^1$.*

We remark that we shall define elliptic curves $\mathcal{E}$ in a purely algebraic setting over arbitrary fields k (cf. Section 4.2.3) and that we shall define an absolute invariant j for such curves, which coincides with $j(\tau)$ if $k = \mathbb{C}$, and which also has the property: If $\mathcal{E}$ is isomorphic to $\mathcal{E}'$ then $j_\mathcal{E} = j'_\mathcal{E}$, and the converse holds if k is algebraically closed.

2. 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 $\mathbb{Q}$-vector spaces $\mathrm{Hom}^0(\mathcal{A}, \mathcal{B}) := \mathrm{Hom}(\mathcal{A}, \mathcal{B}) \otimes_\mathbb{Z} \mathbb{Q}$, and $\mathrm{End}^0\,\mathcal{A} := \mathrm{End}\,\mathcal{A} \otimes_\mathbb{Z} \mathbb{Q}$. Determining $\mathrm{End}\,\mathcal{A}$ or $\mathrm{End}^0\,\mathcal{A}$ is an interesting problem on its own; see [**58**].

For any abelian variety $\mathcal{A}$ defined over a number field K, computing $\mathrm{End}_K(\mathcal{A})$ is a harder problem than computation of $\mathrm{End}_{\bar{K}}(\mathcal{A})$; see [**47**, lemma 5.1] for details.

2.1. Isogenies. 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 Lem. 5.

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 $\ker(f)$, which is, by definition, the scheme theoretical inverse image $f^{-1}(\{0_{\mathcal{A}}\})$.

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** if and only if

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

Equivalently: The group scheme $\ker f$ is étale. The following result should be compared with the well known result of quotient groups of abelian groups.

LEMMA 2. *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 $\deg f = \#\mathcal{K}(\bar{k})$.

Isogenous Abelian varieties have commensurable endomorphism rings.

LEMMA 3. *If $\mathcal{A}$ and $\mathcal{B}$ are isogenous then* $\mathrm{End}^0(\mathcal{A}) \cong \mathrm{End}^0(\mathcal{B})$.

LEMMA 4. *If $\mathcal{A}$ is a absolutely simple Abelian variety then every endomorphism not equal* 0 *is an isogeny.*

We can assume that $k = \bar{k}$. Let f be a nonzero isogeny of $\mathcal{A}$. Its kernel $\ker f$ is a subgroup scheme of $\mathcal{A}$ (since it is closed in the Zariski topology because of continuity and under $\oplus$ because of homomorphy). It contains $0_{\mathcal{A}}$ and so its connected component, which is, by definition, an Abelian variety.

Since $\mathcal{A}$ is simple and $f \neq 0$ this component is equal to $\{0_{\mathcal{A}}\}$. But it has finite index in $\ker f$ (Noether property) and so $\ker f$ is a finite group scheme.

2.1.1. *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 scheme of $\mathcal{A}$. From the computational point of view we have the following problems:

- Given $\mathcal{A}$ and H, determine $\mathcal{B} := \mathcal{A}/H$ 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 $\mathcal{A} \to \mathcal{B}$.

There is a flurry of research activity in the last decade to solve these problems explicitly for low dimensional Abelian varieties; see [**48**], [**49**] among many others. For a survey and some famous conjectures on isogenies see [**21**].

REMARK 1. *For elliptic curves (Abelian varieties of dimension* 1*) and for Jacobians of curves of genus* 2 *we shall come back to these questions in more detail.*

2.2. Torsion points and Tate modules. The most classical example of an isogeny is the scalar multiplication by n map $[n] : \mathcal{A} \to \mathcal{A}$. The kernel of $[n]$ is a group scheme of order $n^{2\dim \mathcal{A}}$ (see [**56**]). We denote by $\mathcal{A}[n]$ the group $\ker[n](\bar{k})$. The elements in $\mathcal{A}[n]$ are called n-**torsion points** of $\mathcal{A}$.

LEMMA 5. *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*

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

COROLLARY 1. *Let $\mathcal{A}$ be an absolutely simple Abelian variety. Then* $\mathrm{End}(\mathcal{A})^0$ *is a skew field.*

PROOF. Every endomorphism $\neq 0$ of $\mathcal{A}$ is an isogeny, hence invertible in $\mathrm{End}(\mathcal{A})^0$. □

THEOREM 6. *Let $\mathcal{A}/k$ be an Abelian variety, $p = \mathrm{char}\ k$, 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.[1] An abelian variety $\mathcal{A}$ is called **supersingular** if it is isogenous to a product of supersingular elliptic curves.

REMARK 2. *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 that is (here and in the following) different from $p = \mathrm{char}\ k$ 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 6. *The Tate module $T_l(\mathcal{A})$ is a $\mathbb{Z}_l$-module isomorphic to $\mathbb{Z}_l^{2\dim \mathcal{A}}$.*

2.3. l-adic representations and characteristic polynomials.

2.3.1. *Galois representations.* 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 and $g = \dim \mathcal{A}$. Then G_k acts on $\mathcal{A}[n]$ which gives rise to a representation

$$\rho_{\mathcal{A},n} : G_k \to \mathrm{Aut}\,(\mathcal{A}[n])$$

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** $\mathcal{A}$.

2.3.2. *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 $\mathcal{A}[\lambda^\infty] := \cup_{k\in\mathbb{N}}\mathcal{A}[\ell^k]$) 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 7. *$\tilde{\eta}_\ell$ is injective.*

[1]For an alternative definition see Thm. 43.

For a proof see [**56**, Theorem 3, p.176]. 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 $\leq 4\dim(\mathcal{A})^2$.

Adding more information (see Corollary 2 in [**56**]) one gets that $\mathrm{End}^0(\mathcal{A})$ is a semi-simple algebra, and by duality (key word Rosati-involution) one can apply a complete classification due to Albert of *possible* algebra structures on $\mathrm{End}^0(\mathcal{A})$, which can be found on [**56**, pg. 202].

The question is: Which algebras occur as endomorphism algebras? The situation is well understood if k has characteristic 0 (due to Albert) but wide open in characteristic $p > 0$. For $g = 1$ (elliptic curves) everything is explicitly known due to M. Deuring. We describe the results in Thm. 43. For curves of genus 2 we give an overview on results in Section 4.2.7

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

THEOREM 8 (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.

2.3.3. *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

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

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

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

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

LEMMA 7 (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 8 (Tate). *Let $k = \mathbb{F}_q$. The ℓ-adic representation $\tilde{\rho}_{\mathcal{A},l}$ is semi-simple and so is determined by $\chi(T)\left(\tilde{\rho}_{\mathcal{A},l}(\pi)\right)$.*[2]

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**.

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

By definition it follows that the characteristic polynomial of the ℓ-adic representation of ϕ_q is equal to the characteristic polynomial $\chi_{\mathcal{A},q}(T)$ of the $\ell - adic$ Galois representation of π.

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

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

DEFINITION 9. $\chi_{\mathcal{A},q}(T)$ is the characteristic polynomial of the Frobenius endomorphism ϕ_q of $\mathcal{A}$.

Its importance for the arithmetic of Abelian varieties over finite fields becomes evident by the following theorem.

THEOREM 10 (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.*

i) *$\mathcal{A}$ and $\mathcal{B}$ are isogenous.*
ii) $\chi_{\mathcal{A},q}(T) \equiv \chi_{\mathcal{B},q}(T)$
iii) *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.*
iv) $T_l(\mathcal{A}) \otimes \mathbb{Q} \cong T_l(\mathcal{B}) \otimes \mathbb{Q}$

$\chi_{\mathcal{A},q}(T)$ is the most important tool 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 $\ker(\phi_q - id_{\mathcal{A}})(\overline{\mathbb{F}}_q) = \mathcal{A}(\mathbb{F}_q)$. By linear algebra it follows that:

THEOREM 11. *The number of points over $\mathbb{F}_q$ is given by*

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

The importance of this observation for *algorithms* for the computation of $\#(\mathcal{A}(\mathbb{F}_q)$ is due to one of the deepest results (**Hasse** for $g = 1$ and **Weil** for general g) in the arithmetic of Abelian varieties over finite fields, which is the analogue of the Riemann Hypothesis in number theory.

THEOREM 12. *Let $\mathcal{A}$ be an Abelian variety of dimension g over $\mathbb{F}_q$. The zeroes $\lambda_1, \ldots, \lambda_2 g$ of the characteristic polynomial of the Frobenius endomorphism $\chi_{\mathcal{A},q}(T)$ have the following properties:*

- *Each λ_i is an algebraic integer.*
- *After a suitable numeration one gets for $1 \leq i \leq g$*

$$\lambda_i \cdot \lambda_{i+g} = q.$$

- *The complex absolute value $|\lambda_i|$ is equal to $\sqrt{q}$.*

For the proof we refer to [**56**].

It is evident that this theorem yields bounds for the size of the coefficients of $\chi_{\mathcal{A},q}(T)$ deepening only on g and q and so estimates for the size of $\#(\mathcal{A}(\mathbb{F}_q))$. We state the following Corollary.

COROLLARY 2.
$$|\#(\mathcal{A}(\mathbb{F}_q)) - q^g| = \mathcal{O}(q^{g-1/2}).$$

REMARK 3. *If $\mathcal{A}$ is the Jacobian of a curve $\mathcal{C}$ of genus g one can use this result to prove the Riemann Hypothesis for curves over finite fields:*
$$||\mathcal{C}(\mathbb{F}_q)| - q - 1| \leq 2g\sqrt{q}.$$

For a proof and refinements see [**67**].

In the next few sections we will focus on some special cases of Abelian varieties, namely Jacobian varieties and more specifically Jacobians of hyperelliptic curves.

3. Projective curves and Jacobian varieties

3.1. Curves. First let us establish some notation and basic facts about algebraic curves. In this paper the notion *curve* is an absolutely irreducible projective variety of dimension 1 without singularities.

At some rare points of the following discussion 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 $\mathcal{C}(k) \setminus U_0$. If we have to study curves with different properties (like being affine or having singularities) we shall state this explicitly.

Let $\mathcal{C}$ be a curve defined over k. Hence there is $n \in \mathbb{N}$ and a homogeneous *prime* ideal $I_\mathcal{C} \subset k[X_0, \ldots, X_n]$ such that, with $R = k[X_0, \ldots, X_n]/I_\mathbb{C}$, we have

(1) $\mathcal{C}$ 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.
(2) 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.
(3) $\mathcal{C}$ 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 $\mathcal{C}$, in this class the valuation with value group $\mathbb{Z}$ is denoted by w_M. Alternatively we use the notation $R_\mathfrak{p}$ and $w_\mathfrak{p}$. A place $\mathfrak{p}$ of $\mathcal{C}$ is also called *prime divisor* of $\mathcal{C}$.
(4) (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*.

3.1.1. *Prime divisors and points.* The set of all places $\mathfrak{p}$ of the curve $\mathcal{C}$ is denoted by $\Sigma_\mathcal{C}(k)$. The *completeness* of projective varieties yields:

PROPOSITION 1. *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 corresponding maximal ideal $M_\mathfrak{p}$ and valuation ring $R_\mathfrak{p}$. We have a homomorphism
$$r_\mathfrak{p} : R_\mathfrak{p} \to R_p/M_\mathfrak{p} =: L$$
where L is a finite algebraic extension of k.

DEFINITION 13. The **degree** of the prime divisor $\mathfrak{p}$ 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 9. *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 $\mathcal{C}_{\bar{k}}$, the curve obtained from $\mathcal{C}$ by constant field extension to the algebraic closure of k. Obviously, every prime divisor of $\mathcal{C}_{\bar{k}}$ has degree 1.

COROLLARY 3. *The set of prime divisors of $\mathcal{C}_{\bar{k}}$ corresponds one-to-one to the points in $\mathcal{C}_{\bar{k}}(\bar{k})$.*

Let's go back to k. Since $\bar{k}/k$ is separable, every equivalence class $\mathfrak{p}$ of valuations of $k(\mathcal{C})$ 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 we have:

COROLLARY 4. *$\Sigma_{\mathcal{C}}(k)$ corresponds one-to-one to the G_k-orbits of $\mathcal{C}_{\bar{k}}(\bar{k})$.*

3.2. Divisors and Picard groups. Given a curve $\mathcal{C}/k$, the group of k-rational divisors $\mathrm{Div}_{\mathcal{C}}(k)$ is defined as follows.

DEFINITION 14. $\mathrm{Div}_{\mathcal{C}}(k) = \bigoplus_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} \mathbb{Z} \cdot \mathfrak{p}$, 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 $\mathfrak{p}$. The degree of a divisor is defined as

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

As we have seen in Cor. 4 we can interpret divisors as formal sums 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 1. *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*

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

It is not difficult to verify that (f) is a divisor, and that its degree is 0, see [**67**]. *Moreover $(f \cdot g) = (f) + (g)$ for functions f, g, and $(f^{-1}) = -(f)$. The completeness of $\mathcal{C}$ implies that $(f) = 0$ if and only if $f \in k^*$, and so (f) determines f up to scalars $\neq 0$.*

Thus, the set of principal divisors $\mathrm{PDiv}_{\mathcal{C}}(k)$ consisting of all divisors (f) with $f \in k(\mathcal{C})^*$ is a subgroup of $\mathrm{Div}^0_{\mathcal{C}}(k)$.

DEFINITION 15. The group of divisor classes of $\mathcal{C}$ is defined by

$$\mathrm{Pic}_{\mathcal{C}}(k) := \mathrm{Div}_{\mathcal{C}}(k)/\,\mathrm{PDiv}_{\mathcal{C}}(k)$$

and is called the **divisor class group** of $\mathcal{C}$. The group of divisor classes of degree 0 of $\mathcal{C}$ is defined by

$$\mathrm{Pic}^0_{\mathcal{C}}(k) := \mathrm{Div}^0_{\mathcal{C}}(k)/\,\mathrm{PDiv}_{\mathcal{C}}(k)$$

and is called the **Picard group** (of degree 0) of $\mathcal{C}$.

The Picard functor: Let L be a finite algebraic extension of k and $\mathcal{C}_L$ the curve obtained from $\mathcal{C}$ by constant field extension. Then places of $k(\mathcal{C})$ can be extended to places of $L(\mathcal{C}_L)$. By the conorm map we get an injection of $\mathrm{Div}_{\mathcal{C}}(k)$ to $\mathrm{Div}_{\mathcal{C}_L}(L)$. The well known formulas for the extensions of places yield that

$$\mathrm{conorm}_{L/k}(\mathrm{Div}^0_{\mathcal{C}}(k)) \subset \mathrm{Div}^0_{\mathcal{C}_L}(L)$$

and that principal divisors are mapped to principal divisors. Hence we get a homomorphism

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

and therefore 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. Clearly,

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

and the same is true for functions. With a little bit of more work one sees that an analogue result is true for $\mathrm{PDiv}_{\mathcal{C}_L}(L)$ and for $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$.

THEOREM 16. *For any curve $\mathcal{C}_k$ and any extension L/k 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 4. *For a finite extension L/k we also have the norm map of places of $\mathcal{C}_L$ to places of $\mathcal{C}_k$ 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.

3.3. Riemann-Roch theorem. Here we take as guideline the book [**67**] of H. Stichtenoth.

3.3.1. *Riemann-Roch spaces.* We define a partial ordering of elements in $\mathrm{Div}_{\mathcal{C}}(k)$ as follows;

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

is *effective* ($D \geq 0$) if $z_{\mathfrak{p}} \geq 0$ for every $\mathfrak{p}$, and $D_1 \geq D_2$ if $D_1 - D_2 \geq 0$.

Definition 17. The **Riemann-Roch space** associated to D is

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

So the elements $x \in \mathcal{L}(D)$ are defined by the property that $w_{\mathfrak{p}}(x) \geq -z_{\mathfrak{p}}$ for all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$. Basic properties of valuations imply immediately that $\mathcal{L}(D)$ is a vector space over k. This vector space 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 $D_1 \geq 0$.

Here are some immediately obtained facts: $\mathcal{L}(0) = k$ and if $\deg(D) < 0$ then $\mathcal{L}(D) = \{0\}$. If $\deg(D) = 0$ then either D is a principal divisor or $\mathcal{L}(D) = \{0\}$. The following result is easy to prove but fundamental.

Proposition 2. *Let $D = D_1 - D_2$ with $D_i \geq 0$. Then*

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

We remark that for $D \sim D'$ we have $\mathcal{L}(D) \sim \mathcal{L}(D')$. In particular $\mathcal{L}(D)$ is a finite-dimensional k-vector space.

Definition 18. $\ell(D) := \dim_k(\mathcal{L}(D))$.

To compute $\ell(D)$ is a fundamental problem in the theory of curves. It is solved by the Theorem of Riemann-Roch. 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 19 (**Riemann**). *For given curve $\mathcal{C}$ there is a minimal number $g_C \in \mathbb{N} \cup \{0\}$ such that for all $D \in \mathrm{Div}_{\mathcal{C}}$ we have*

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

For a proof see [**67**, Proposition 1.4.14]. Therefore,

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

exists and is a non-negative integer independent of D.

Definition 20. The integer $g_{\mathcal{C}}$ is called the **genus** of $\mathcal{C}$.

We remark that 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 5. *There is a number $n_{\mathcal{C}}$ such that for $\deg(D) > n_{\mathcal{C}}$ we get equality*

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

Thm. 19 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.

3.3.2. *Canonical divisors.* Let $k(\mathcal{C})$ be the function field of a curve $\mathcal{C}$ 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) $d(f \cdot g) = f dg + g df$.

The relation between derivations and differentials is given by the

DEFINITION 21 (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 and separable. We use a well known fact from the theory of function fields F in one variable.

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 $w_{\mathfrak{p}}(t_{\mathfrak{p}}) = 1$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 $\omega = f_{\mathfrak{p}} \cdot dt_{\mathfrak{p}}$. The divisor (ω) is given by

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

and 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 $k_{\mathcal{C}} \in \mathrm{Pic}_{\mathcal{C}}(k)$ called the **canonical class** of $\mathcal{C}$. We are now ready to formulate the Riemann-Roch Theorem.

THEOREM 22 (**Riemann-Roch theorem**). *Let W be a canonical divisor of $\mathcal{C}$. For all $D \in \mathrm{Div}_{\mathcal{C}}(k)$ we have*

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

For a proof see [**67**, Section 1.5].

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 $\mathcal{L}(W)$. If we take $D = 0$ respectively $D = W$ in the theorem of Riemann-Roch we get the following:

COROLLARY 6. *$\Omega^0_{\mathcal{C}}$ is a $g_{\mathcal{C}}$-dimensional k-vector space and* $\deg(W) = 2g_{\mathcal{C}} - 2$.

For our applications there are two further important consequences of the Riemann-Roch theorem.

COROLLARY 7. *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.*

PROOF. Take D with $\deg(D) \geq 2g_{\mathcal{C}} - 1$. Then $\deg(W - D) \leq -1$ and therefore $\ell(W - D) = 0$. 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. □

4. Applications of the Riemann-Roch theorem

4.1. The Hurwitz genus formula. In the theory of curves the notion of a cover is important.

DEFINITION 23. Let $\mathcal{C}$, $\mathcal{D}$ be curves defined over k, with $\mathcal{D}$ not necessarily absolutely irreducible. A finite surjective morphism

$$\eta : \mathcal{D} \to \mathcal{C}$$

from $\mathcal{D}$ to $\mathcal{C}$ is a *cover morphism*, and if such a morphism exists we call $\mathcal{D}$ a **cover** of $\mathcal{C}$.

As usual, we denote by

$$\eta^* : k(\mathcal{C}) \hookrightarrow k(\mathcal{D})$$

the induced monomorphism of the function fields and identify $k(\mathcal{C})$ with its image. η is separable if and only if $k(\mathcal{D})$ is a separable extension of $k(\mathcal{C})$, and η is Galois with Galois group G if $k(\mathcal{D})/k(\mathcal{C})$ is Galois with group G. The cover η is geometric if k is algebraically closed in $k(\mathcal{D})$.

Assume in the following that η is separable. We shall use the well known relations between prime divisors of $k(\mathcal{C})$ and those of $k(\mathcal{D})$ such as extensions, ramifications and sum formulas for the degrees. In particular we get:

Let $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ be a prime divisor and $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ the primes divisors in $\Sigma_{\mathcal{D}}(k)$ which extend $\mathfrak{p}$, written as $\mathfrak{P}/\mathfrak{p}$. Let $t_{\mathfrak{p}}$ be an element in $k(\mathcal{C})$ with $w_{\mathfrak{p}}(t_{\mathfrak{p}}) = 1$. The ramification index $e(\mathfrak{P}_i/\mathfrak{p}) =: e_i$ is defined as $e_i = w_{\mathfrak{P}_i}(t_{\mathfrak{p}})$, hence there is a function $t_{\mathfrak{P}_i}$ on $\mathcal{D}$ such that $t_{\mathfrak{P}_i}^{e_i} = t_{\mathfrak{p}} \cdot u$ with $w_{\mathfrak{P}_i}(u) = 0$. The *conorm* of $\mathfrak{p}$ is the divisor

$$\operatorname{conorm}(\mathfrak{p}) = \sum_i \mathfrak{P}_i^{e_i}$$

and its degree is $[k(\mathcal{D}) : k(\mathcal{C})]$, the *norm* of $\mathfrak{P}_i$ is $\mathfrak{p}$. The cover η is *tamely ramified* if for all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ the ramification numbers of all extensions are prime to char(k).

We want to relate the genus of $\mathcal{D}$ to the genus of $\mathcal{C}$. Let $x \in k(\mathcal{C})$ be such that $k(\mathcal{C})/k(x)$ is finite separable, and let $dx_{\mathcal{C}}$ respectively $dx_{\mathcal{D}}$ be corresponding differentials with divisors $(dx)_{\mathcal{C}}$ and dx_D. We know that

$$2g_{\mathbb{C}} - 2 = \deg(dx)_{\mathcal{C}} \text{ and } 2g_{\mathcal{D}} - 2 = \deg(dx)_{\mathcal{D}}.$$

We compute the value $z_{\mathfrak{p}}$ respectively $z_{\mathfrak{P}_i}$ of these divisors at $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ and in the extensions $\mathfrak{P}_1, \ldots \mathfrak{P}_r$ with ramification numbers e_i. To ease notation we take $\mathfrak{P} := \mathfrak{P}_i$, $e_i = e_{\mathfrak{P}}$ and $t_{\mathfrak{P}} \in k(\mathcal{D})$ with $w_{\mathfrak{P}} = 1$. Then we can choose

$$t_{\mathfrak{p}} = u \cdot t_{\mathfrak{P}}^{e_{\mathfrak{P}}} \in k(\mathcal{C}),$$

with $w_{\mathfrak{p}}(u) = 0$. By the rules for differentials we get $dt_p = (e_{\mathfrak{P}} \cdot u \cdot t_{\mathfrak{P}}^{e_{\mathfrak{P}}-1} + u' \cdot t_{\mathfrak{P}}^{e_{\mathfrak{P}}}) dt_{\mathfrak{P}}$ and so

$$w_{\mathfrak{P}}(dx) = e_{\mathfrak{P}} \cdot w_{\mathfrak{p}}(dx) + e_{\mathfrak{P}} - 1.$$

Summing up over $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ we get that

$$\deg\left(\sum_{\mathfrak{P}|\mathfrak{p}} z_{\mathfrak{P}}\right) = \deg\left(\sum_{i=1}^{r} z_{\mathfrak{p}} \mathfrak{P}_i^e\right) + \sum_{i=1}^{r} (e_i - 1).$$

Summing up over all $\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)$ we get the Hurwitz theorem.

THEOREM 24 (Hurwitz). *Any separable, tamely ramified degree n cover $\eta : \mathcal{D} \to \mathcal{C}$ with $e_{\mathfrak{P}}$ the ramification index of $\mathfrak{P} \in \Sigma_{\mathcal{D}}(k)$ satisfies*

$$2g_{\mathcal{D}} - 2 = n \cdot (2g_{\mathcal{C}} - 2) + \sum_{\mathfrak{P} \in \Sigma_{\mathcal{D}}} (e_{\mathfrak{P}} - 1).$$

Let us illustrate the theorem with a classical example.

EXAMPLE 2. *Assume that $\mathcal{C} = \mathbb{P}^1$, the genus $g_{\mathbb{P}^1} = 0$ curve. Let $\mathcal{D}$ be tamely ramified cover of degree n of $\mathbb{P}^1$. Then*

$$g_{\mathcal{D}} = 1 - n + \frac{1}{2} \sum_{\mathfrak{P} \in \Sigma_{\mathcal{D}}(k)} (e_{\mathfrak{P}} - 1).$$

In particular $\mathbb{P}^1$ has no unramified extensions.

The special case $n = 2$ will be important for us. Assume that char(k) $\neq 2$. Then we can apply the Hurwitz formula and get

$$g_{\mathcal{D}} = \frac{1}{2} r - 1,$$

where r is the number of prime divisors of $\mathbb{P}^1$ (or of $\mathcal{D}$) which are ramified (i.e. ramification order is larger than 1) under η.

4.2. Gonality of curves and Hurwitz spaces. Let $\mathcal{C}$ be a curve defined over k and $\eta : \mathcal{C} \to \mathbb{P}^1$ a degree n cover. We assume that $\mathcal{C}$ has a k-rational point P_∞ and hence a prime divisor $\mathfrak{p}_\infty$ of degree 1.

DEFINITION 25. The gonality $\gamma_{\mathcal{C}}$ of $\mathcal{C}$ is defined by

$$\gamma_{\mathcal{C}} = \min \left\{ \deg(\eta) : \mathcal{C} \to \mathbb{P}^1 \right\} = \min \left\{ [k(\mathcal{C}) : k(x)] \mid x \in k(\mathcal{C}) \right\}.$$

For $x \in k(\mathcal{C})^*$, define the pole divisor $(x)_\infty$ by

$$(x)_\infty = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} \max(0, -w_{\mathfrak{p}}(x)) \cdot \mathfrak{p}.$$

By the property of conorms of divisors we get $\deg((x)_\infty) = [k(\mathcal{C}) : k(x)]$ if $x \notin k$ and so

$$\gamma_{\mathcal{C}} = \min \left\{ \deg (x)_\infty, \mid x \in k(\mathcal{C}) \setminus k. \right\}$$

PROPOSITION 3. *For $\gamma_{\mathcal{C}} \geq 2$ we have $\gamma_{\mathcal{C}} \leq g$.*

PROOF. By Riemann-Roch theorem

$$\ell(g_{\mathcal{C}} \cdot P_\infty) = 1 + \ell(W - g_{\mathcal{C}} \cdot P_\infty)$$

and since $g_{\mathcal{C}} \geq 2$ the divisor $(W - g_{\mathcal{C}} \cdot P_\infty)$ has degree ≥ 0 and so $\ell(W - g_{\mathcal{C}} \cdot P_\infty) \geq 1$. But then $\ell(g_{\mathcal{C}} \cdot P_\infty) \geq 2$ and there is a non-constant function x whose pole divisor is a multiple of $\mathfrak{p}_\infty$ of order $\leq g_{\mathcal{C}}$.

□

This proves more than the proposition.

COROLLARY 1. *For curves $\mathcal{C}$ of genus ≥ 2 with prime divisor $\mathfrak{p}_\infty$ of degree 1 there exists a cover*

$$\eta : \mathcal{C} \to \mathbb{P}^1$$

with $\deg(\eta) = n \leq g_{\mathcal{C}}$ such that $\mathfrak{p}_\infty$ is ramified of order n and so the point $P_\infty \in \mathcal{C}(k)$ attached to $\mathfrak{p}_\infty$ is the only point on $\mathcal{C}$ lying over the infinite point $(0 : 1)$ of $\mathbb{P}^1$.

In general, the inequality in the proposition is not sharp but of size $g/2$ as we shall see below. Curves with smaller gonality are special and so per se interesting.

4.2.1. *Gonality of the generic curve.* Let us assume that k is algebraically closed. We are interested in the classification of isomorphism classes of projective irreducible regular curves of genus $g \geq 2$.

The moduli scheme $\mathcal{M}_g$ is a scheme defined over k with the property that it parametrizes these classes (i.e., to every point P there is a unique class of a curve $\mathcal{C}$ of genus g). The coordinates of $\mathcal{C}$ (chosen in an appropriate affine open neighborhood) are the invariants of $\mathcal{C}$. It is a classical task to determine such systems of invariants and then to find the curve $\mathcal{C}$ with these invariants. We shall come back to this in the case of curves of small genus.

REMARK 5. *The scheme $\mathcal{M}_g$ is defined over non-algebraically closed fields k but then it is only a coarse moduli scheme.*

The construction of $\mathcal{M}_g$ is done over $\mathbb{C}$ either by Teichmüller theory or, more classically, by Hurwitz spaces (see below), and so over algebraically closed fields of characteristic 0 by the so-called Lefschetz principle. Its existence in the abstract setting of algebraic geometry uses deep methods of geometric invariant theory as developed and studied by Deligne and Mumford in [**13**].

One knows that $\mathcal{M}_g$ is irreducible and so there exists a generic curve of genus g. Moreover the dimension of $\mathcal{M}_g$ is equal to $3g-3$. Curves with special properties (i.e. non-trivial automorphisms or small gonality) define interesting subschemes of $\mathcal{M}_g$. Here is one example.

DEFINITION 26. A curve $\mathcal{C}$ with genus ≥ 2 is hyperelliptic if and only if it has gonality 2.

The subspace of hyperelliptic curves in $\mathcal{M}_g$ is the *hyperelliptic locus* $\mathcal{M}_{g,h}$. We shall see below that this locus has dimension $2g-1$.

Hurwitz spaces: We continue to assume that k is algebraically closed and consider separable covers $\eta : \mathcal{C} \to \mathbb{P}^1$ of degree n. Then η^* allows to identify $k(\mathbb{P}^1) =: k(x)$ with a subfield of $k(\mathcal{C})$. First, we introduce the equivalence: $\eta \sim \eta'$ if there are isomorphisms $\alpha : \mathcal{C} \to \mathcal{C}'$ and $\beta \in \mathrm{Aut}(\mathbb{P}^1)$ with

$$\beta \circ \eta = \eta' \circ \alpha.$$

The *monodromy group* of η is the Galois group of the Galois closure L of $k(\mathcal{C})/k(x)$. We embed G into S_n, the symmetric group with n letters, and fix the ramification type of the covers η. We assume that exactly $r \geq 3$ points in $\mathbb{P}^1(k)$ are ramified (i.e. the corresponding prime divisors have at least one extension to $k(\mathcal{C})$ with ramification order > 1) and that all ramification orders are prime to char(k). It follows that the ramification groups are cyclic.

By the classical theory of covers of Riemann surfaces, which can be transferred to the algebraic setting by the results of Grothendieck (here one needs tameness of ramification) it follows that there is a tuple $(\sigma_1, \ldots, \sigma_r)$ in S_n such that $\sigma_1 \cdots \sigma_r = 1$, $\mathrm{ord}(\sigma_i) = e_i$ is the ramification order of the i-th ramification point P_i in L and $G := \langle \sigma_1, \ldots, \sigma_r \rangle$ is a transitive group in S_n. We call such a tuple the **signature** σ of the covering η and remark that such tuples are determined up to conjugation in S_n, and that the genus of $\mathcal{C}$ is determined by the signature because of the Hurwitz genus formula.

Let $\mathcal{H}_\sigma$ be the set of pairs $([\eta], (p_1, \ldots, p_r)$, where $[\eta]$ is an equivalence class of covers of type σ, and $p_1, \ldots, p_r$ is an ordering of the branch points of ϕ modulo automorphisms of $\mathbb{P}^1$. This set carries the structure of a algebraic scheme, in fact it is a quasi-projective variety, the *Hurwitz space* $\mathcal{H}_\sigma$. We have the forgetful morphism

$$\Phi_\sigma : \mathcal{H}_\sigma \to \mathcal{M}_g$$

mapping $([\eta], (p_1, \ldots, p_r)$ to the isomorphic class $[\mathcal{C}]$ in the moduli space $\mathcal{M}_g$. Each component of $\mathcal{H}_\sigma$ has the same image in $\mathcal{M}_g$.

Define the **moduli dimension of** σ (denoted by $\dim(\sigma)$) as the dimension of $\Phi_\sigma(\mathcal{H}_\sigma)$; i.e., the dimension of the locus of genus g curves admitting a cover to $\mathbb{P}^1$ of type σ. We say σ has **full moduli dimension** if $\dim(\sigma) = \dim \mathcal{M}_g$; see [**50**] for details.

EXAMPLE 3. *Take $n = 2$, so $G = S_2$, $r \geq 6$ and $\mathrm{char(k)} \neq 2$ and the notations from above. A signature σ is completely determined by the r ramification points $P_1, \cdots, P_r$. Hence $\mathcal{H}_\sigma$ consists of classes of hyperelliptic curves of genus $g_r = r/2 - 1$ (so r is even). Since we can apply automorphisms of $\mathbb{P}^1$ we can assume that $P_1 = (1:0), P_2 = (1,1), P_3 = (0:1)$ and so we have $r-3$ free parameters modulo a finite permutation group.*

So the moduli dimension is $r-3 = 2g+2$, and the hyperelliptic locus $\mathcal{M}_{g,h}$ has dimension $2g-1$ and codimension $g-2$. Hence all curves of genus 2 are hyperelliptic, and for $g \geq 3$ the locus of the hyperelliptic curves has positive codimension.

For a fixed $g \geq 3$, we want to find σ of full moduli dimension and of minimal degree. This would give a generic covering of minimal degree for a generic curves of genus g and so its gonality.

A first condition is that $r = 3g$. Because of the Hurwitz genus formula this yields conditions for the ramification cycles, which have to have minimal order. This is worked out in [**61**].

LEMMA 10. *For any $g \geq 3$ there is a minimal degree $d = \lfloor \frac{g+3}{2} \rfloor$ generic cover*

$$\psi_g : \mathcal{C}_g \to \mathbb{P}^1$$

of full moduli dimension from a genus g curve $\mathcal{C}_g$ such that it has $r = 3g$ branch points and signature:

i) If g is odd, then $\sigma = (\sigma_1, \ldots, \sigma_r)$ such that $\sigma_1, \ldots, \sigma_{r-1} \in S_d$ are transpositions and $\sigma_r \in S_d$ is a 3-cycle.

ii) If g is even, then $\sigma = (\sigma_1, \ldots, \sigma_r)$ such that $\sigma_1, \ldots, \sigma_r \in S_d$ are transpositions.

4.2.2. *Equations for curves.* There is a one-to-one correspondence between function fields F of transcendence degree 1 over the field of constants k with k algebraically closed in F and isomorphism classes of projective regular absolutely irreducible curves $\mathcal{C}$ with $k(\mathcal{C}) = F$. The natural question is: Given F, how can one find $\mathcal{C}$ as embedded projective curve in an appropriate $\mathbb{P}^n$?

The main tool to solve this question are Riemann-Roch systems. Let D with $\ell(D) = d + 1 > 0$ and $(f_0, f_1, \ldots, f_d)$ a base of $\mathcal{L}(D)$. Then

$$\begin{aligned} \Phi_D : \mathcal{C}(\bar{k}) &\to \mathbb{P}^d(\bar{k}) \\ P &\mapsto (f_0(P) : f_1(p) : \cdots : f_d(P)) \end{aligned}$$

is a rational map defined in all points for which $f_0, \ldots, f_d$ do not vanish simultaneously. $\mathcal{L}(D)$ is without base points if this set is empty, and then Φ_D is a morphism from $\mathcal{C}$ in $\mathbb{P}^d$.

LEMMA 11. *For $g \geq 3$ and $D = W_{\mathcal{C}}$ the space $\mathcal{L}(W) = \Omega^0_{\mathcal{C}}$ is without base points, and so Φ_W is a morphism from $\mathcal{C}$ to $\mathbb{P}^{g_{\mathcal{C}}-1}$.*

Φ_W may not be an embedding but the only exception is that $\mathcal{C}$ is hyperelliptic, and than the image of Φ_W is the projective line.

THEOREM 27. *Let $\mathcal{C}$ be a curve of genus $g_{\mathcal{C}} > 2$ and assume that $\mathcal{C}$ is not hyperelliptic. Then Φ_W is an embedding of $\mathcal{C}$ into $\mathbb{P}^{g_{\mathcal{C}}-1}$ and the image is a projective regular curve of degree $2g_{\mathcal{C}} - 2$ (i.e. the intersection with a generic hyperplane has $2g_{\mathcal{C}} - 2$ points).*

So having determined a base of the canonical class of $\mathcal{C}$ one gets a parameter representation of $\mathcal{C}$ and then one can determine the prime ideal in $k[Y_0, \ldots, Y_{g_{\mathcal{C}}}]$vanishing on $\Phi_W(\mathcal{C})$. Φ_W is the **canonical embedding** of $\mathcal{C}$.

EXAMPLE 4. *Take $g_{\mathcal{C}} = 3$ and assume that $\mathcal{C}$ is not hyperelliptic. Then the canonical embedding maps $\mathcal{C}$ to a regular projective plane curve of degree 4. In other words: All non-hyperelliptic curves of genus 3 are isomorphic to non-singular quartics in $\mathbb{P}^2$.*

Plane curves: Only very special values of the genus of $\mathcal{C}$ allow to find plane regular projective curves isomorphic to $\mathcal{C}$. We have just seen that $g = 3$ is such a value. The reason behind is the Plücker formula, which relates degree, genus and singularities of plane curves. But of course, there are many projective plane curves which are birationally equivalent to $\mathcal{C}$.

Take $x \in k(\mathcal{C}) \setminus k$ with $k(\mathcal{C})/k(x)$ separable. Then there is an element $y \in k(\mathcal{C})$ with $k(x, y) = k(\mathcal{C})$, and by clearing denominators we find a polynomial $G(x, y) \in k[X, Y]$ with $G(x, y) = 0$. Then the curve $\mathcal{C}'$ given by the homogenized polynomial

$$G_h(X, Y, Z) = 0$$

is a plane projective curve birationally equivalent to $\mathcal{C}$ but, in general, with singularities. Using the gonality results we can chose $G(X, Y)$ such that the degree in Y is $\lfloor \frac{g+3}{2} \rfloor$. Using the canonical embedding for non hyperelliptic curves and general projections we can chose $G_h(X, Y, Z)$ as homogeneous polynomial of degree $2g_{\mathcal{C}} - 2$.

In the next subsection we shall describe a systematic way to find plane equations for hyperelliptic curves.

4.2.3. *Plane equations for elliptic and hyperelliptic curves, Weierstrass normal forms.* We first focus on elliptic curves.

Elliptic curves: We assume that $\mathcal{E}$ is a curve of genus 1 with a k-rational point P_∞ and corresponding prime divisor $\mathfrak{p}_\infty$. By definition, $\mathcal{E}$ is an *elliptic curve defined over k*. We look at the Riemann-Roch spaces $\mathcal{L}_i := \mathcal{L}(i \cdot \mathfrak{p}_\infty)$ and denote their dimension by ℓ_i. Since $2g_{\mathcal{E}} - 2 = 0$ we can use the theorem of Riemann-Roch to get that $\ell_i = i$. Hence $\mathcal{L}_1 = \langle 1 \rangle$, $\mathcal{L}_2 = \langle 1, x \rangle$ with a function $x \in k(\mathcal{E})$ with $(x)_\infty = 2\mathfrak{p}_\infty$, $\mathcal{L}_3 = \langle 1, x, y \rangle$ with $(y)_\infty = 3\mathfrak{p}_\infty$ and $\mathcal{L}_5 = \langle 1, x, x^2, y, xy \rangle$ with 5 linearly independent functions.

Now look at $\mathcal{L}_6$. This is a vector space of dimension 6 over k. It contains the seven elements $\{1, x, x^2, x^3, y, xy, y^2\}$ and hence there is a non-trivial linear relation

$$\sum_{0\le i\le 3;\, 0\le j\le 2} a_{i,j} x^i y^2.$$

Because of the linear independence of $(1, x, x^2, y, xy)$ we get that either $a_{3,0}$ or $a_{0,2}$ are not equal 0, and since x^3 and y^2 have a pole of order 6 in $\mathfrak{p}_\infty$ it follows that $a_{0,2} \cdot a_{3,0} \neq 0$. By normalizing we get x and y satisfy the equation

$$Y^2 + a_1 X \cdot Y + a_3 Y = a_0 X^3 + a_2 X^2 + a_4 X + a_6.$$

By multiplying with a_0^2 and substituting (X, Y) by $(a_0 X, a_0 Y)$ we get an **affine Weierstrass equation** for $\mathcal{E}$:

$$W_{\mathcal{E}aff} :\ Y^2 + a_1 X \cdot Y + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.$$

The homogenization give the cubic equation

$$W_{\mathcal{E}} :\ Y^2 \cdot Z + a_1 X \cdot Y \cdot Z + a_3 Y \cdot Z^2 = a_0 X^3 + a_2 X^2 \cdot Z + a_4 X \cdot Z^2 + a_6 \cdot Z^3,$$

which defines a plane projective curve.

The infinite points of this curve have $Z = 0$, and so the only infinite point is $P_\infty = (0, 1, 0)$ corresponding to the chosen $\mathfrak{p}_\infty$. Looking at the partial derivatives one verifies that $\mathcal{E}$ has no singularities if and only if the discriminant of the affine equation $W_{\mathcal{E}aff}$ as polynomial in X is different from 0, and that this is equivalent with the condition that $k(\mathcal{E})$ is not a rational function field.

THEOREM 28. *Elliptic curves defined over k correspond one-to-one the isomorphism classes of plane projective curves without singularities given by Weierstrass equations*

$$W_{\mathcal{E}} : Y^2 \cdot Z + a_1 X \cdot Y \cdot Z + a_3 Y \cdot Z^2 = X^3 + a_2 X^2 \cdot Z + a_4 X \cdot Z^2 + a_6 \cdot Z^3$$

with non-vanishing X-discriminant.

Since we are dealing with isomorphism classes of such curves we can further normalize the equations and finally find invariants for the isomorphism class of a given $\mathcal{E}$. This is a bit tedious if char(k) | 6. In this case we refer to [**65**].

Assume that char(k) $\neq 2, 3$. Then we can use Tschirnhausen transformations to get an equation

$$W_{\mathcal{E}} : Y^2 \cdot Z = X^3 - g_2 X \cdot Z^2 - g_3 \cdot Z^3$$

and the reader should compare this equation with the differential equation satisfied by the Weierstrass $\wp$-function.

We use this analogy and define $\Delta(\mathcal{E}) = 4g_2^3 - 27g_3^2$ and this is, because of the regularity of $\mathcal{E}$, an element $\neq 0$, and

$$j_E = 12^3 \frac{4g_2^3}{\Delta_{\mathcal{E}}}.$$

If k is algebraically closed then $j_{\mathcal{E}}$ determines the isomorphic class of $\mathcal{E}$. For an arbitrary k the curve E is determined up to a *twist*, which is quadratic if char(k) is prime to 6 (see [**65**]).

Weierstrass equations for hyperelliptic curves: Let $\mathcal{C}$ be a curve over k of genus $g \geq 2$ with a degree 2 cover

$$\eta : \mathcal{C} \to \mathbb{P}^1.$$

We assume that there is a point $P_\infty \in \mathcal{C}(k)$ corresponding to a prime divisor $\mathfrak{p}_\infty$ of $\mathcal{C}$ of degree 1. Take $Q_\infty = \eta(P_\infty) \in \mathbb{P}^1(k)$ and $x \in k(\mathbb{P}^1)$ with $(x)_\infty = \mathfrak{p}_{0,\infty}$ with $\mathfrak{p}_{0,\infty}$ a prime divisor of degree 1 of $\mathbb{P}^1$. Thus, $\text{conorm}(\mathfrak{p}_{0,\infty}) = 2 \cdot \mathfrak{p}_\infty$ and so η is ramified in Q_0, or $\text{conorm}(\mathfrak{p}_{0,\infty}) = \mathfrak{p}_\infty \cdot \mathfrak{p}'_\infty$. In any case $\text{conorm}(\mathfrak{p}_{0,\infty}) =: D$ is a positive divisor of degree 2. We define the Riemann-Roch spaces $\mathcal{L}_i = \mathcal{L}(i \cdot D)$ and $\ell_i = \dim_k(\mathcal{L}_i)$.

By assumption $\mathcal{L}_1$ has as base $(1, x)$ and so $\ell_1 = 2$. Since $\deg(g+1) \cdot D > 2g-2$ the theorem of Riemann- Roch implies that $\ell_{g+1} = 2(g+1) - g + 1 = g + 3$. Hence there is a function $y \in \mathcal{L}_{g+1}$ linearly independent from powers of x. So $y \notin k[x]$. The space $\mathcal{L}_{2(g+1)}$ has dimension $3g + 3$ and contains the $3g + 4$ functions

$$\{1, x, x^{g+1}, y, x^{g+2}, xy, \ldots, x^{2(g+1)}, x^{g+1}y, y^2\}.$$

So there is a nontrivial k-linear relation between these functions, in which y^2 has to have a non-trivial coefficient. We can normalize and get the equation

$$y^2 + h(x)y = f(x) \quad \textit{with} \quad h(x), f(x) \in k[x]$$

and $\deg(h(x)) \leq g + 1$, $\deg(f) \leq 2g + 2$. So

$$W_{\mathcal{C}aff} : Y^2 + h(X)Y = f(X)$$

is the equation for an affine part $\mathcal{C}_{aff}$ of a curve birationally equivalent to $\mathcal{C}$. It is called an *affine Weierstrass equation* for $\mathcal{C}$, and its homogenization is the equation of a projective plane curve $\mathcal{C}'$ birationally equivalent to $\mathcal{C}$.

The prime divisors of $\mathcal{C}$ are extensions of prime divisors of $k(x)$ and hence correspond (over $\bar{k}$) to points (x, y) in $\mathbb{A}^2$ or the points lying over $\mathfrak{p}_{0,\infty}$. To get more information we use the Hurwitz genus formula and assume for simplicity that char(k) $\neq 2$ and so η is tamely ramified and separable; for the general case see [**7**, Section 14.5.1].

Then we can apply the Tschirnhausen transformation and can assume that $h(x) = 0$. We know that η has to have $2g + 2$ ramification points. Ramification points of η are fixed points under the hyperelliptic involution ω which generates $\text{Gal}(k(\mathcal{C})/k(x)$. Since ω acts on points (x, y) by sending it to $(x, -y)$ the affine ramification points correspond to the zeros of $f(X)$. If $\mathfrak{p}_{0,\infty}$ is unramified then it follows that $f(X)$ has to have $2g+2$ zeros, and so $\deg(f(X)) = 2g+2$ and all zeros are simple.

Assume that $\mathfrak{p}_{0,\infty}$ is ramified. Then there have to be $2g - 1$ places with norm $\neq \mathfrak{p}_{0,\infty}$ and so $\deg(f(X)) = 2g + 1$ and again all zeros are different. Hence in both cases we have that $\mathcal{C}_{aff}$ is without singularities. This is not true for the point $(0, 1, 0)$, the only point at infinity of $\mathcal{C}'$. It is a singular point, and it corresponds to two points (over $\bar{k}$) on $\mathcal{C}$ if $\mathfrak{p}_{0,\infty}$ is unramified, and to one point on $\mathcal{C}(k)$ if $\mathfrak{p}_{0,\infty}$ is ramified. For computational purposes the latter case is more accessible. The arithmetic in $k(\mathcal{C})$ is analogue to the arithmetic in imaginary quadratic fields.

The automorphism group of $\mathcal{C}$: We assume that k is algebraically closed. We identify the places of $k(x)$ with the points of $\mathbb{P}^1 = k \cup \{\infty\}$ by their X-coordinate. As seen $k(\mathcal{C})$ is a quadratic extension field of $k(x)$ ramified exactly at $2g + 2$ places

$\alpha_1, \ldots, \alpha_{2g+2}$ of $k(x)$. The corresponding places of $k(\mathcal{C})$ are called the *Weierstrass points* $Q_1, \ldots, Q_{2g+2}$ of $k(\mathcal{C})$, the set formed by these points is denoted by $\mathcal{P}$.

Weierstrass points play a very important role in the arithmetic of curves. For a detailed discussion see [**67**]. In particular, Weierstrass points of $\mathcal{C}$ are uniquely determined up to permutations. So, every automorphism of $\mathcal{C}$ and equivalently, of $k(\mathcal{C})/k$, fixes $\mathcal{P}$ and so fixes $k(x)$, and therefore $k(x)$ is the unique subfield of index 2 in $k(\mathcal{C})$.

It follows that $\langle\omega\rangle$ is central in $\mathrm{Aut}(k(\mathcal{C})/k)$, and $\bar{G} := G/\langle\tau\rangle$ is naturally isomorphic to the subgroup of $\mathrm{Aut}(k(x)/k)$ induced by G. We have a natural isomorphism $\Gamma := PGL_2(k) \xrightarrow{\cong} \mathrm{Aut}(k(x)/k)$. The action of Γ on the places of $k(x)$ corresponds under the above identification to the usual action on $\mathbb{P}^1$ by fractional linear transformations $t \mapsto \frac{at+b}{ct+d}$. Since G permutes the Weierstrass points and $2g+2 \geq 6$ its action determines G and so we get an embedding $\bar{G} \to S_n$.

Since $k(\mathcal{C})$ is the unique degree 2 extension of $k(x)$ ramified exactly at $a_1, \ldots, a_{2g+2}$, each automorphism of $k(x)$ permuting these $2g+2$ places extends to an automorphism of $k(\mathcal{C})$. Hence under the isomorphism $\Gamma \mapsto \mathrm{Aut}(k(x)/k)$, $\bar{G}$ corresponds to the stabilizer $\Gamma_{\mathcal{P}}$ in Γ of the $2g+2$-set $\mathcal{P}$. By a theorem of Klein, $\bar{G}$ is isomorphic to a cyclic group, a dihedral group, or A_4, S_4 or A_5. Hence, we can determine $\mathrm{Aut}(\mathcal{C})$ as a degree 2 central extension of $\bar{G}$ for any fixed genus $g \geq 2$.

Minimal degrees: We have seen above that non-hyperelliptic curves of genus ≥ 3 are birational equivalent to plane projective curves of degree $\leq 2g+2$. But in general, this is not the minimal degree one can achieve. On the other side one has an estimate from below for the degree of plane curves birational equivalent to a hyperelliptic curve of genus $g \geq 3$; see [**8**] for details.

PROPOSITION 4. *Let $\mathcal{C}$ be a hyperelliptic curve of genus g and let $\mathcal{C}'$ be a plane projective curve birationally equivalent to $\mathcal{C}$. Then the degree of the equation of $\mathcal{C}'$ is $\geq g+2$.*

4.2.4. *Addition in Picard groups over $\mathbb{F}_q$.* We take $k = \mathbb{F}_q$ and $\mathcal{C}$ a curve of genus g defined over $\mathbb{F}_q$. By a result of F. K. Schmidt (proved by using Zeta-functions) curves over finite fields have a rational divisor D_0 of degree 1 (Caution: Only for curves of genus ≤ 1 this implies that they have a rational point.) It is not difficult to show that this divisor can be computed effectively. We use this to present divisor classes c of degree 0 of $\mathcal{C}$.

Let $\mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0}$ denote the positive divisors of degree g of $\mathcal{C}$. A consequence of the theorem of Riemann-Roch is that the map

$$\begin{aligned} \varphi : \mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0} &\to \mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q) \\ D &\mapsto \varphi(D) = D - g \cdot D_1 \end{aligned}$$

is surjective. A first consequence is that $\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$ is a finite abelian group since there are only finitely many positive divisors of degree D rational over $\mathbb{F}_q$. Our aim is to find an algorithm, which computes the addition in $\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$ fast. The main task is the following *reduction*:

Given $D, D' \in \mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0}$ find a divisor $S \in \mathcal{D}_{\mathcal{C}}(\mathbb{F}_q)^g_{>0}$ with

$$D + D' - 2gD_1 \sim S - gD_1.$$

Then $S - \mathcal{D}_1$ lies in the divisor class that is the sum of the divisor class of $D - D_1$ with the class of $D' - D_1$. An analogue reduction is well-known from computational number theory and ideal classes of orders. There one uses Minkowski's theorem instead of the Riemann-Roch theorem.

The idea of F. Heß in [**34**] and worked out with many additional details in [**16**] is to use the fact the holomorphic functions in affine open parts of $\mathcal{C}$ are Dedekind domains and that divisors with support on these parts can be identified with ideals of these rings. As first step compute (e.g. from the function field $k(\mathcal{C})$) a plane curve $\mathcal{C}'$ birationally equivalent to $\mathcal{C}$ of a degree d of size $\mathcal{O}(g)$ (see our arguments above).

The next step is to go to an affine part of $\mathcal{C}'$ which is without singularities and for which divisors can be identified with ideals in its coordinate ring (approximation properties of functions in function fields can be used since we are only interested in divisor classes). Now the algorithms known from number theory are applicable. The result is given by the following theorem.

THEOREM 29. *[Heß, Diem] Let $\mathcal{C}$ be a curve of genus g over $\mathbb{F}_q$. The addition in the degree 0 class group of C can then be performed in an expected time which is polynomially bounded in g and* $\log(q)$.

This result is a highlight in algorithmic arithmetic geometry and it opens the access to the Picard groups as abelian groups for arbitrary curves. Of course, it will be a challenge to implement it. In our context, namely to construct crypto systems, its importance is the *existence* of the algorithm which make certain attacks thinkable!

In the next sections we shall see how we can find explicit algorithms and even formulas to perform group operations in Picard groups of hyperelliptic curve very rapidly.

4.2.5. *The Jacobian variety of a curve.* In Section 3.2 we defined the *Picard functor* $\mathrm{Pic}^0_{\mathcal{C}}$ from the category of extension fields L/k into the category of abelian groups given by

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

In addition we stated that $\mathrm{Pic}^0_{\mathcal{C}}$ is a Galois functor, i.e. that if $k \subset L \subset \bar{k}$ then $\mathrm{Pic}^0_{\mathcal{C}\,L}(L) = \mathrm{Pic}^0_{\mathcal{C}\,\bar{k}}(\bar{k})^{G_L}$. We also announced that this functor is *representable* in terms of algebraic geometry.

More precisely: Let $\mathcal{C}$ be a curve of positive genus and assume that there exists a k-rational point $P_0 \in \mathcal{C}(k)$ with attached prime divisor $\mathfrak{p}_0$. There exists an abelian variety $\mathcal{J}_{\mathcal{C}}$ defined over k and a uniquely determined embedding

$$\phi_{P_0} : \mathcal{C} \to \mathcal{J}_{\mathcal{C}} \quad \text{with} \quad \phi_{P_0}(P_0) = 0_{\mathcal{J}_{\mathcal{C}}}$$

such that

(1) for all extension fields L of k we get $J_{\mathcal{C}}(L) = \mathrm{Pic}^0_{\mathcal{C}_L}(L)$ where this equality is given in a functorial way and
(2) if $\mathcal{A}$ is an Abelian variety and $\eta : \mathcal{C} \to \mathcal{A}$ is a morphism sending P_0 to $0_{\mathcal{A}}$ then there exists a uniquely determined homomorphism $\psi : \mathcal{J}_{\mathcal{C}} \to \mathcal{A}$ with $\psi \circ \phi_{P_0} = \eta$.

$\mathcal{J}_\mathcal{C}$ is uniquely determined by these conditions and is called the **Jacobian variety** of $\mathcal{C}$. The map ϕ_{P_0} is given by sending a prime divisor $\mathfrak{p}$ of degree 1 of $\mathcal{C}_\mathcal{L}$ to the class of $\mathfrak{p} - \mathfrak{p}_0$ in $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$.

Properties of Jacobian varieties: From functoriality and universality of the Jacobian it follows that we can introduce coordinates for divisor classes of degree 0 such that the group law in $\mathrm{Pic}^0_{\mathcal{C}_L}(L)$ is given by rational functions defined over k and depending only on $\mathcal{C}$ (and not on L). Moreover, we can interpret the norm and conorm maps on divisor classes geometrically.

Let L/k be a finite algebraic extension. Then the Jacobian variety $\mathcal{J}_{\mathcal{C}_L}$ of $\mathcal{C}_L$ is the scalar extension of $\mathcal{J}_\mathcal{C}$ with L, hence a fiber product with projection p to $\mathcal{J}_\mathcal{C}$. The norm map is p_*, and the conorm map is p^*.

PROPOSITION 5. *If $f : \mathcal{C} \to \mathcal{D}$ is a surjective morphism of curves sending P_0 to Q_0, then there is a uniquely determined surjective homomorphism*

$$f_* : \mathcal{J}_\mathcal{C} \to J_\mathcal{D}$$

such that $f_* \circ \phi_{P_0} = \phi_{Q_0}$.

PROOF. Apply the universal property to the morphism $\phi_{Q_0} \circ f$ to get f_*. The surjectivity follows from the fact that for $k = \bar{k}$ the sums of divisor classes of the form $\mathfrak{p} - \mathfrak{p}_0$ with $\mathfrak{p} \in \Sigma_\mathcal{C}(k)$ generate $\mathrm{Pic}^0_\mathcal{C}(\bar{k})$. □

A useful observation is

COROLLARY 2. *Assume that $\mathcal{C}$ is a curve of genus ≥ 2 such that FG $\mathcal{J}_\mathcal{C}$ is a simple abelian variety, and that $\eta : \mathcal{C} \to \mathcal{D}$ is a separable cover of degree > 1. Then $\mathcal{D}$ is the projective line.*

For the proof use the Hurwitz genus formula and the universal properties of Jacobians.

What about the **existence** of Jacobian varieties? Over the complex numbers the classical theory of curves (key words: Riemann surfaces and the Theorem of Abel-Jacobi) is used to prove the existence of Jacobian varieties already in the 19-th century. In fact, this notion is historically earlier than the notion "Abelian variety" introduced by A. Weil as most important tool for his proof of the geometric Riemann hypothesis. By the Lefschetz principle the existence of Jacobian varieties follows for algebraically closed fields of characteristic 0.

For a proof in the framework of Algebraic Geometry (and so over arbitrary ground fields k) see Lang [**45**]. The important fact is that we "know" a birational affine model of $J_\mathcal{C}$.

By the Theorem of Riemann-Roch we have a surjective map from $\Sigma^g_\mathcal{C}(L)$ to $\mathrm{Pic}^0_\mathcal{C}(L)$ by sending any positive divisor D of degree g to $D - g \cdot \mathfrak{p}_0$. We can interpret such positive divisors geometrically. Take the g-fold cartesian product $\mathcal{C}^g$ of the curve $\mathcal{C}$ of genus g and embed it (via Segre's map) into a projective space. On this variety we can permute the factors and so have an action of S_g, the symmetric group with g letters. Define the g-fold symmetric product $\mathcal{C}^{(g)}$ by $\mathcal{C}^g/S_g$. Then we can identify $\mathcal{C}^{(g)}(L)$ with $\Sigma^g_\mathcal{C}(L)$ and so define a birational map from $\mathcal{C}^{(g)}$ to $\mathcal{J}_\mathcal{C}$. Taking an affine part of $\mathcal{C}$ (e.g. found as a regular part of a plane model of $\mathcal{C}$) we get an affine variety which is birational equivalent to $\mathcal{J}_\mathcal{C}$.

The Jacobian varieties connect the arithmetic in divisor classes of curves (which is very accessible to algorithms) with the very rich geometric structure of abelian varieties (e.g. isogenies, endomorphisms and ℓ-adic representations).

4.2.6. *Construction of curves by period matrices.* It is convenient to assume in the following that k is algebraically closed. We look at the following task: Assume that a point P in the moduli scheme $\mathcal{M}_g(k)$ is given by coordinates in a certain coordinate system. How can we find an equation for a curve $\mathcal{C}$ corresponding to P?

It is useful to look at the case that $k = \mathbb{C}$ and at the parametrization of isomorphism classes principally polarized abelian varieties by period matrices. We reformulate the question and ask whether we can find a curve such that the Jacobian has a given period matrix. Of course, the first problem is that not every principally polarized abelian variety is the Jacobian of a curve, and the decision for this is the well-known *Schottky Problem* which is unsolved till now.

There are two cases where the situation is better: If the dimension of the Abelian variety is ≤ 3 then such a curve exists, and if we are looking for hyperelliptic curves we can solve the Schottky Problem and determine a Weierstrass equation if we know the period matrix.

This latter result is based on *invariant theory.* Details are worked out in the thesis of H.J. Weber [**72**] (explicitly for curves up to genus 5). Important cases for our applications are curves of genus 1 (use the j-invariant), genus 2 and genus 3. We remark that this method works very well over number fields and by reduction, over finite fields, too.

We shall give more details in the interesting case that the genus of $\mathcal{C}$ is equal to 2.

4.2.7. *Example: Curves of genus 2.* Let $\mathcal{C}$ be a genus 2 curve defined over a field k. By Prop. 3 we have that its gonality is $\gamma_{\mathcal{C}} = 2$. Hence, genus 2 curves are hyperelliptic and we denote the hyperelliptic projection by $\pi : \mathcal{C} \to \mathbb{P}^1$. By the Hurwitz's formula this covering has $r = 6$ branch points which are images of the Weierstrass points of $\mathcal{C}$. The moduli space has dimension $r - 3 = 3$; see Example 3.

The arithmetic of the moduli space of genus two curves was studied by Igusa in his seminal paper [**35**] expanding on the work of Clebsch, Bolza, and others. Arithmetic invariants by $J_2, J_4, J_6, J_8, J_{10}$ determine uniquely the isomorphism class of a genus two curve. Two genus two curves $\mathcal{C}$ and $\mathcal{C}'$ are isomorphic over $\bar{k}$ if and only if there exists $\lambda \in \bar{k}^\star$ such that $J_{2i}(\mathcal{C}) = \lambda^{2i} J_{2i}(\mathcal{C}')$, for $i = 1, \ldots, 5$. If char $k \neq 2$ then the invariant J_8 is not needed.

From now on we assume char $k \neq 2$. Then $\mathcal{C}$ has an affine Weierstrass equation

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

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

$$A_2 \cong \mathbb{WP}^3_{(2,4,6,10)}(k) \setminus \{J_{10} = 0\}.$$

A point $\mathfrak{p} \in \mathbb{WP}^3_{(2,4,6,10)}$ for $J_2 \neq 0$ can be written as

$$\left[1 : \frac{1}{2^4 3^2}\mathbf{x}_1 : \frac{1}{2^6 3^4}\mathbf{x}_2 + \frac{1}{2^4 3^3}\mathbf{x}_1 : \frac{1}{2 \cdot 3^5}\mathbf{x}_3\right]$$

where $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are given as ratios of Siegel modular forms and are called *absolute invariants* and denoted by i_1, i_2, i_3 by other authors; see [**36**]. Two genus 2 curves are isomorphic over $\bar{k}$ if and only if they have the same absolute invariants. Notice that the absolute invariants are not defined for $J_2 = 0$. There are different sets of absolute invariants used by many authors, but all of them are not defined over $J_2 = 0$.

Recovering the curve from invariants. Given a moduli point $\mathfrak{p} \in \mathcal{M}_2$, with automorphism group of order 2, we can recover the equation of the corresponding curve over a minimal field of definition following Mestre's approach [**55**], where the point is given in terms of the absolute invariants. The case of automorphism group of order > 2 was done in [**5**] and [**62**]. In all these papers the case when the absolute invariants are not defined had to be treated differently, introducing a new set of invariants. In [**51**] it is given an equation of the curve in terms of J_2, J_4, J_6, J_{10} without using any absolute invariants.

In [**52**], for any number field K, a *height* on the moduli space $\mathbb{WP}^3_{(2,4,6,10)}(K)$ is introduced. This makes it possible to store the *smallest* tuple of invariants in a unique way. This is used in [**2**] to create a database of all genus 2 curves with small height and defined over K including all the twists of minimal moduli height.

4.2.8. *Example: Elliptic curves.* Let $\mathcal{E}$ be an elliptic curve over k, i.e. a curve of genus 1 with a k-rational point. Its isomorphy class over $\bar{k}$ is uniquely determined by the j-invariant. As seen above, $\mathcal{E}$ is isomorphic to a plane curve $\mathcal{E}'$ given by a Weierstrass equation.

We choose one k-rational point P_∞ with prime divisor $\mathfrak{p}_\infty$ and projective coordinates such that $P_\infty = (0 : 1 : 0)$ is the infinite point of the curve $\mathcal{E}'$ with equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and identify $\mathcal{E}$ with $\mathcal{E}'$.

Let $\mathcal{J}_\mathcal{E}$ be the Jacobian variety of $\mathcal{E}$. We look at $\phi_{P_\infty} : \mathcal{E} \to \mathcal{J}_\mathcal{E}$ given by

$$P \mapsto [\mathfrak{p} - \mathfrak{p}_\infty]$$

where $[.]$ means divisor class. Since $2g_\mathcal{E} - 2 = 0$ the Riemann-Roch theorem implies that for all extension fields L of k in each L-rational divisor class of degree 1 there is exactly one prime divisor $\mathfrak{p}$ of degree 1 corresponding to a point $P \in \mathcal{E}(L)$, and to each divisor class c of degree 0 there is exactly one prime divisor $\mathfrak{p}$ of degree 1 with $c = [\mathfrak{p} - \mathfrak{p}_\infty]$. So ϕ_{P_∞} is injective and surjective and hence an isomorphism of projective varieties. By transport of structure we endow $\mathcal{E}$ with a group structure:

For extension fields L of k and $P_1, P_2 \in \mathcal{E}(L)$ define $P_1 \oplus P_2$ as the point belonging to the prime divisor in the class $\mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{p}_\infty$.

It is obvious that this makes $\mathcal{E}(L)$ to an abelian group with neutral element P_∞. We conclude: Three points P_1, P_2, P_3 sum up to 0 if $\mathfrak{p}_1 + \mathfrak{p}_2 + \mathfrak{p}_3 - 3\mathfrak{p}_\infty = (f)$ with $f \in L(\mathcal{E})$.

Now recall that $\mathcal{E}$ has degree 3 and so lines intersect with $\mathcal{E}$ in 3 points (counted with multiplicities) and so f defines a line in $\mathbb{P}^2$. Hence $P_1 + P_2 + P_3 = 0$ if and only if the three points are collinear, and then $P_1 \oplus P_2 = \ominus P_3$. Using coordinates we get an algebraic recipe for addition:

For given $P \neq P\infty$ take the line through P and P_∞ to get: $\ominus(P)$ is the third intersection point of the line with $\mathcal{E}$ (if this point is equal to P the line is a tangent

and $P = \ominus P$ is an element of order 2). Given two points $P_1 \neq P_2$ compute the line through these two points, take its third intersection point P_3 with $\mathcal{E}$ to get $P_1 \oplus P_2 = \ominus P_3$.

By elementary algebra one can perform this recipe by writing down formulas in rational functions in (X, Y, Z) and so we get

THEOREM 30. *After the choice of a base point P_∞ the elliptic curve $\mathcal{E}$ is an Abelian variety of dimension 1 with neutral element P_∞ which is equal to $\mathcal{J}_\mathcal{E}$.*

Division polynomials for elliptic curves: To simplify we assume that char $k \neq 2, 3$ and so we can take the affine Weierstrass equation of E as

$$E: \quad Y^2 = X^3 + aX + b,$$

for $a, b \in k$. Recall that for $m \in \mathbb{N}$ the endomorphism $[m]$ of $\mathcal{E}$ is induced by the scalar multiplication by m. We want to give formulas for this endomorphism.

LEMMA 12. *For any integer m and point $P(x, y) \neq \mathcal{O}$ in E, the point $[m]P$ has coordinates*

$$[m]P = \left(\frac{\phi_m(x,y)}{\psi_m(x,y)^2}, \frac{\omega_m(x,y)}{\psi_m(x,y)^3} \right)$$

where the polynomials ϕ_m, ψ_m, ω_m are given by the recurrences

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = 2Y^2,\\
&\psi_3 = 3X^4 + 6aX^2 + 12bX - a^2,\\
&\psi_4 = (2X^6 + 10aX^4 + 40bX^3 - 10a^2X^2 - 8abX - 2a^3 - 16b^2)2Y^2, \qquad (3)\\
&\quad \cdots\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \textit{for } m \geq 2,\\
&\psi_2\psi_{2m} = (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m \quad \textit{for } m \geq 3.
\end{aligned}$$

and

$$\begin{aligned}
\phi_m &= x\psi_m^2 - \psi_{m+1}\psi_{m-1},\\
\omega_m &= \psi_{m-1}^2\psi_{m+2} + \psi_{m-2}\psi_{m+1}^2. \qquad (4)
\end{aligned}$$

The proof follows from classical identities of the Weierstrass function $\wp$ if $k = \mathbb{C}$ and is then transferred to arbitrary perfect fields (see [**65**]). The polynomial ψ_m is called the **m-th division polynomial** and it vanishes in $E[m]$

COROLLARY 8. *All m-torsion points $P(x, y)$ of E have coordinates satisfying $\psi_m(x, y) = 0$*

This provides a computational approach on how to determine the m-torsion points for any given $m \geq 2$.

4.3. 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 at least one rational Weierstrass point given by the affine Weierstrass equation

$$W_\mathcal{C}: \; y^2 + h(x)\, y = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_1x + a_0 \qquad (5)$$

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

$$\mathcal{O} = k[X,Y]/(Y^2 + h(X)\,\langle Y - (X^{2g+1} + a_{2g}X^{2g} + \cdots + a_1X + a_0)\rangle)$$

and so prime divisors $\mathfrak{p}$ of degree d of $\mathcal{C}$ correspond to prime ideals $P \neq 0$ with $[\mathcal{O}/P : k] = d$. 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 [**56**] 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 $\mathfrak{p}_i \neq \mathfrak{p}_\infty$ (we use Riemann-Roch and the fact that ω induces $-id_{J_\mathcal{C}}$).

Using the relation between divisors and ideals 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. 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 $v^2 + h(X)v - f(X)$; see [**7**, Theorem 4.143].

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 31 (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 $v(X)$ that

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

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

Addition: Take the divisor classes represented by $[(u_1, v_1)]$ and $[(u_2, v_2)]$ and in "general position". Then the product is represented by the ideal $I \in \mathcal{O}$ given by

$$\langle u_1 u_2, u_1(y - v_2), u_2(y - v_1), (y - v_1)(y - v_2)\rangle.$$

We have to determine a base, and this is done by Hermite reduction. The resulting ideal is of the form $\langle u_3'(X), v_3'(X) + w_3'(X)Y\rangle$ but not necessarily reduced. To reduce it one uses recursively the fact that $u \mid (v^2 - hv - f)$.

The formalization of this procedure and the treatment of special cases is called **Cantor's algorithm**. For readers acquainted with algorithmic number theory it may be enlightening to compare this algorithm with the well known method to add in class groups of imaginary quadratic number fields, going back to Gauss and based on the theory of definite quadratic forms with fixed discriminant. The very explicit and efficient "generic" algorithm can be found in [**7**, Algorithm 14.7]. For curves of genus 2 a detailed analysis including all special cases is done in [**7**, Section 14.3.2], including a determination of complexity (see Table 14.2 and Table 14.13). For curves of genus 3 we refer to Section 14.6 in[**7**].

Addition by interpolation Another approach to describe addition in the Jacobians of hyperelliptic curves is to use approximation by rational functions; see [**46**]. This is analogous to the geometric method used for elliptic curves.

For simplicity we assume that $k = \bar{k}$. Let D_1 and D_2 be reduced divisors on $\mathrm{Jac}_k \mathcal{C}$ given by

$$\begin{aligned} D_1 &= \mathfrak{p}_1 + \mathfrak{p}_2 + \cdots + \mathfrak{p}_{h_1} - h_1 \mathfrak{p}_\infty, \\ D_2 &= \mathfrak{q}_1 + \mathfrak{q}_2 + \cdots + \mathfrak{q}_{h_2} - h_2 \mathfrak{p}_\infty, \end{aligned} \tag{6}$$

where $\mathfrak{p}_i$ and $\mathfrak{q}_j$ can occur with multiplicities, and $0 \le h_i \le g$, $i = 1, 2$. As usual we denote by P_i respectively Q_j the points on $\mathcal{C}$ corresponding to $\mathfrak{p}_i$ and $\mathfrak{q}_j$.

Let $g(X) = \frac{b(X)}{c(X)}$ be the unique rational function going through the points P_i, Q_j. In other words we are determining $b(X)$ and $c(X)$ such that $h_1 + h_2 - 2r$ points P_i, Q_j lie on the curve

$$Y\, c(X) - b(X) \,=\, 0.$$

This rational function is uniquely determined and has the form

$$Y = \frac{b(X)}{c(X)} = \frac{b_0 X^p + \ldots b_{p-1} X + b_p}{c_0 X^q + c_1 X^{q-1} + \cdots + c_q} \tag{7}$$

where

$$p = \frac{h_1 + h_2 + g - 2r - \epsilon}{2}, \;\; q = \frac{h_1 + h_2 - g - 2r - 2 + \epsilon}{2},$$

ϵ is the parity of $h_1 + h_2 + g$. By replacing Y from Eq. (7) in Eq. (5) we get a polynomial of degree $\max\{2p,\, 2q(2g-1)\}$, which gives $h_3 \le g$ new roots apart from the X-coordinates of P_i, Q_j. Denote the corresponding points on $\mathcal{C}$ by $R_1, \ldots, R_{h_3}$ and $\bar{R}_1, \ldots, \bar{R}_{h_3}$ are the corresponding symmetric points with respect to the $y = 0$ line. Then, we define

$$D_1 + D_2 = \bar{R}_1 + \ldots \bar{R}_{h_3} - h_3 \mathcal{O}.$$

For details we refer the reader to [**46**].

REMARK 6. *For $g = 1, 2$ we can take $g(X)$ to be a cubic polynomial.*

EXAMPLE 5 (Curves of genus 2.). *Let $\mathcal{C}$ be a genus 2 curve defined over a field k with a rational Weierstrass point. If char $k \neq 2, 3$ the $\mathcal{C}$ is birationally isomorphic to an affine plane curve with equation*

$$Y^2 = a_5X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0. \tag{8}$$

Let $\mathfrak{p}_\infty$ be the prime divisor corresponding to the point at infinity. Reduced divisors in generic position

are given by

$$D = \mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{p}_\infty$$

where $P_1(x_1, y_1)$, $P_2(x_2, y_2)$ are points in $\mathcal{C}(k)$ (since k is algebraically closed) and $x_1 \neq x_2$. For any two divisors $D_1 = \mathfrak{p}_1 + \mathfrak{p}_2 - 2\mathfrak{p}_\infty$ and $D_2 = \mathfrak{q}_1 + \mathfrak{q}_2 - 2\mathfrak{p}_\infty$ in reduced form, we determine the cubic polynomial

$$Y = g(X) = b_0X^3 + b_1X^2 + b_2X + b_3, \tag{9}$$

going through the points $P_1(x_1, y_1)$, $P_2(x_2, y_2)$, $Q_1(x_3, y_3)$, and $Q_2(x_4, y_4)$. This cubic will intersect the curve $\mathcal{C}$ at exactly two other points R_1 and R_2 with coordinates

$$R_1 = (x_5, g(x_5)) \quad \text{and} \quad R_2 = (x_6, g(x_6)), \tag{10}$$

where x_5, x_6 are roots of the quadratic equation

$$x^2 + \left(\sum_{i=1}^{4} x_i\right) x + \frac{b_3^2 - a_5}{b_0^2 \prod_{i=1}^{4} x_i} = 0. \tag{11}$$

Let us denote by $\overline{R}_1 = (x_5, -g(x_5))$ and $\overline{R}_2 = (x_6, -g(x_6))$. Then,

$$[D_1] \oplus [D_2] = [\overline{R}_1 + \overline{R}_2 - 2\mathfrak{p}_\infty]. \tag{12}$$

After having defined explicitly the addition in $\mathrm{Jac}_\mathcal{C}$ it is a natural problem that given a reduced divisor $D \in \mathrm{Jac}_\mathcal{C}$, determine explicitly the formulas for $[n]D$, at least in generic cases similarly as in the case of elliptic curves. Hence, one wants to determine explicitly division polynomials (i.e polynomials that have torsion points of order n as zeroes) or more generally, ideals which define zero-dimensional schemes containing $J_\mathcal{C}[n]$). There has been a lot of activity on this area lately; see [**57**], [**38**], [**39**].

4.4. Automorphisms of curves and their Jacobians. Let $\mathcal{C}$ be an algebraic curve defined over k and $\mathrm{Jac}_k(\mathcal{C})$ its Jacobian. What are the automorphism groups of $\mathcal{C}$ and $\mathrm{Jac}_k(\mathcal{C})$?

4.4.1. *Automorphisms of curves.* Let $\mathrm{Aut}(\mathcal{C})$ be the automorphism of the curve $\mathcal{C}$. If $\mathcal{C} = \mathbb{P}^1$ the automorphism group over an infinite field k is infinite, as seen in Section 4.2.3. The same is true for elliptic curves $\mathcal{E}$, if $E(k)$ is infinite, i.e. $k = \bar{k}$, for then there are infinitely many translations. But caution: If we look only at automorphisms with a fixed point (which are automatically homomorphisms with respect to the group structure with the fixed point as origin) then the group is finite, well understood, and for generic elliptic curves $\mathcal{E}$ equal to $\{id_\mathcal{E}, -id_\mathcal{E}\}$.

For curves of genus ≥ 2 the picture changes completely. The automorphism group $\mathrm{Aut}(\mathcal{C})$ is a finite group. The reason is the existence of $2g + 2$ Weierstrass points and the faithful action of $\mathrm{Aut}(\mathcal{C})$ on these points, which gives an injection

of $\mathrm{Aut}(\mathcal{C})$ into S_{2g+2}. In fact, one can describe all occurring groups. If $\mathrm{char}(\mathrm{k}) = 0$ one has the *Hurwitz bound*

$$\#\,\mathrm{Aut}(\mathcal{C}) \leq 84(g-1).$$

One gets a stratification of $\mathcal{M}_g$ by strata of curves with the same automorphism group, and the generic curve of genus $G > 2$ has trivial automorphism group.

It is very interesting to study curves with large automorphism group; for instance a curve of genus 3 with group $PSl(2,7)$ (168 automorphisms) is the famous Klein Quartic, which also occurs as modular curve (see below). For more details and a full account of automorphisms of curves see [**50**].

4.4.2. *Automorphisms of Jacobian varieties.* By functoriality it follows that automorphism of $\mathcal{C}$ induce automorphisms of $\mathcal{J}_{\mathcal{C}}$, or, to be more precise, of $(\mathrm{Jac}_{\mathcal{C}}, \iota)$ where ι is the principal polarization of $\mathcal{J}_{\mathcal{C}}$ attached to $\mathcal{C}$.

THEOREM 32. *Let $\mathcal{C}$ be an algebraic curve and $\mathcal{A} := \mathrm{Jac}(\mathcal{C})$ with canonical principal polarization ι. Then,*

$$\mathrm{Aut}\,\mathcal{C} \cong \begin{cases} \mathrm{Aut}(\mathcal{A},\iota), & \text{if } \mathcal{C} \text{ is hyperelliptic} \\ \mathrm{Aut}(\mathcal{A},\iota)/\{\pm 1\}, & \text{if } \mathcal{C} \text{ is non-hyperelliptic} \end{cases}$$

The above result can be used to find Jacobians of genus 3 hyperelliptic curves; see [**73**] and Section 9.

4.4.3. *Endomorphism of Abelian varieties.* The ring of endomorphisms of generic Abelian varieties is "as small as possible". For instance, if $\mathrm{char}(\mathrm{k}) = 0$ $\mathrm{End}(\mathcal{A}) = \mathbb{Z}$ in general. If k is a finite field, the Frobenius endomorphism will generate a larger ring, but again, this will be all in the generic case. A concrete result is the following [**75**]:

THEOREM 33 (Zarhin). *Let $\mathcal{C}$ be a hyperelliptic curves with affine equation $y^2 = f(x)$, $n = \deg f$, and $f \in \mathbb{Q}[x]$. If $\mathrm{Gal}(f)$ is isomorphic to A_n or S_n then $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{C}) \cong \mathbb{Z}$.*

The theorem is actually true over any number field K. See [**76**] for detailed results on endomorphisms of Jacobians of hyperelliptic and superelliptic curves.

From this point of view it will be interesting to find Abelian varieties with larger endomorphism rings. This leads to the theory of real and complex multiplication. For instance, the endomorphism ring of the Jacobian of the Klein quartic contains an order in a totally real field of degree 3 over $\mathbb{Q}$. We shall see in Section 8 that the Jacobians of modular curves have real multiplication.

4.5. Endomorphism ring of an abelian surface. For $\mathrm{char}\ k \neq 2$, a point $\mathfrak{p}$ in the moduli space $\mathcal{M}_2$ is determined by the tuple (J_2, J_4, J_6, J_{10}), for discriminant $D := J_{10} \neq 0$. In the case of $\mathrm{char}\ k = 2$ another invariant J_8 is needed; see [**35**].

Humbert surfaces: For every $D := J_{10} > 0$ there is a Humbert hypersurface H_D in $\mathcal{M}_2$ which parametrizes curves $\mathcal{C}$ whose Jacobians admit an optimal action on $\mathcal{O}_D$; see [**33**]. Points on H_{n^2} parametrize curves whose Jacobian admits an (n,n)-isogeny to a product of two elliptic curves.

Shimura curves: For every quaternion ring R there are irreducible curves $S_{R,1}, \ldots, S_{R,s}$ in $\mathcal{M}_2$ that parametrize curves whose Jacobians admit an optimal action of R. Those $S_{R,1}, \ldots, S_{R,s}$ are called *Shimura curves*.

Curves with complex multiplication: Curves whose Jacobians admit complex multiplication correspond to isolated points in $\mathcal{M}_2$. We have the following:

PROPOSITION 6. *$\mathrm{Jac}(\mathcal{C})$ is a geometrically simple Abelian variety if and only if it is not (n,n)-decomposable for some $n>1$.*

A more detailed discussion is given in [**47**, Section 2.5]. The endomorphism rings of Abelian surfaces can be determined by the Albert's classification and results in [**58**]. We summarize in the following:

PROPOSITION 7. *The endomorphism ring $\mathrm{End}^0_{\overline{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{C})$ 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 F, where F is either $\mathbb{Q}$ or an imaginary quadratic field.*

REMARK 7. *Genus 2 curves with extra involutions have endomorphism ring larger than $\mathbb{Z}$. Let $\mathcal{C}$ be a genus 2 curve defined over $\mathbb{Q}$. If $\mathrm{Aut}(\mathcal{C})$ is isomorphic to the Klein 4-group V_4,then $\mathcal{C}$ is isomorphic to a curve $\mathcal{C}'$ with equation*

$$y^2 = f(x) = x^6 - ax^4 + bx^2 - 1.$$

We denote $u = a^3+b^3$ and $v = ab$. The discriminant $\Delta_f = -2^6\cdot\left(27-18v+4u-u^2\right)^2$, is not a complete square in $\mathbb{Q}$ for any values of $a,b\in\mathbb{Q}$. In this case $\mathrm{Gal}_{\mathbb{Q}}(f)$ has order 24. There is a twist of this curve, namely $y^2 = f(x) = x^6+a'x^4+b'x^2+1$, in which case Δ_f is a complete square in $\mathbb{Q}$ and $\mathrm{Gal}_{\mathbb{Q}}(f)$ has order 48. In both cases, from Thm. 33 we have that $\mathrm{End}_{\overline{\mathbb{Q}}}(\mathrm{Jac}\,\mathcal{C}') \neq \mathbb{Z}$.

Next we turn our attention to determining the endomorphism ring of abelian surfaces. Let us first recall a few facts on characteristic polynomials of Frobenius for abelian surfaces. The Weil q-polynomial arising in genus 2 have the form

$$f(T) = T^4 - aT^3 + (b+2q)T^2 - aqT + q^2, \tag{13}$$

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

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

We follow the terminology from [**3**]. Let $\mathcal{C}$ be a curve of genus 2 over $\mathbb{F}_q$ and $\mathcal{J} = \mathrm{Jac}_{\mathcal{C}}$. Let f be the Weil polynomial of J as in Eq. (13). We have that $\#\mathcal{C}(\mathbb{F}_q) = q+1-a$, $\#J(\mathbb{F}_q) = f(1)$ and it lies in the genus-2 Hasse interval

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

In [**3**] are constructed decomposable $(3,3)$-jacobians with a given number of rational points by glueing two elliptic curves together.

Next we describe some of the results obtained in [**47**] for $\mathrm{End}_K(\mathcal{A})$ in terms of the characteristic polynomial of the Frobenius. We 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 13. *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 $b \not\equiv 0 \mod p$.

Then from [**47**, Lemma 4.3] we have the following.

LEMMA 14. *Let $\mathcal{A}$ be an absolutely simple abelian surface. The endomorphism algebra $\mathrm{End}_K^0(\mathcal{A})$ 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 8 ([**47**]). *i) 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 $\mathbb{Z}[x]$.*

ii) If $\mathcal{C}$ 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 $\mathrm{Jac}\,\mathcal{C}$ is absolutely irreducible.

In [**47**] is given a detailed account of all the cases and an algorithm how to compute $\mathrm{End}_K \mathcal{A}$.

5. Modular curves

As stated in Section 2 we are interested in isogenies between Abelian varieties. Of special interest is the case of elliptic curves, and it turns out that their isogenies are fairly well accessible both from the theoretical and algorithmic point of view. The reason for this is is the very rich and well understood structure of *modular curves*, which parametrize isogenies of elliptic curves.

5.1. Modular curves over $\mathbb{C}$. As we have seen in Section 1 the isomorphism classes of elliptic curves $\mathcal{E}$ over $\mathbb{C}$ correspond one-to-one to isomorphism classes of lattices Λ_τ with τ in $\mathbb{H} = \{z = x + iy \in \mathbb{C} \mid \ y > 0\} \subset \mathbb{C}$. Moreover, $\Lambda_\tau \cong \Lambda_{\tau'}$ if and only if $\tau' = \frac{a\tau+b}{c\tau+d}$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL_2(\mathbb{Z})$.

So the moduli space of isomorphism classes of elliptic curves over $\mathbb{C}$ is in a natural way equal to $\mathbb{H}/\,\mathrm{SL}_2(\mathbb{Z})$, which is, via the j-function, identified with $\mathbb{A}^1$. It is more convenient to work with compact Riemann surfaces and so, with projective curves. Hence we compactify by adjoining *cusps*.

Define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{i \cdot \infty\}$ and extend the action of $\mathrm{SL}_2(\mathbb{Z})$ in an obvious way (e.g.: $1/z$ interchanges the cusp 0 with $i \cdot \infty$). Then $\mathbb{H}^*/\,\mathrm{SL}_2(\mathbb{Z}) = \mathbb{P}^1$, the j-function extends to a meromorphic function on $\mathbb{H}^*$ with a simple pole at the cusps (which are all equivalent) and all points $P \in \mathbb{P}^1 \setminus \{j(i \cdot \infty)\}$ have a *modular interpretation*: to $P = j(\tau)$ there corresponds the isomorphism class of the elliptic curve $\mathcal{E}_\tau$ with lattice $\mathbb{Z} + \tau\mathbb{Z}$. In this interpretation we call $\mathbb{P}^1 = X(1)$ and $\mathbb{A}^1 = Y(1)$ modular curves of level 1.

We introduce now a special family of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, which are linked to isogenies. For $N \in \mathbb{N}$ define

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid c \equiv 0 \mod N \right\}$$

This is a subgroup of $SL_2(\mathbb{Z})$ of finite index, and so $\mathbb{H}^*/\Gamma_0(N)$ is a compact Riemann surface $X_0(N)$ with a natural cover morphism

$$\eta_N : X_0(N) \to X(1)$$

of degree $\varphi(N)$, the value of the Euler function of N. As affine part in $X_0(N)$ we find $Y_0(N) = X_0(N) \setminus \eta^{-1}(j(i \cdot \infty))$ and points P in $Y_0(N)$ have the following modular interpretation.

Let $P \in Y(1)$ corresponding to an isomorphism class of the lattice $\Lambda_\tau = \mathbb{Z}+\tau\mathbb{Z}$. The inverse image $\eta^{-1}(P)$ consists of the equivalence classes of lattices isomorphic to Λ_τ *with the additional information* consisting of a lattice $\Lambda_\tau(N) \supset \Lambda_\tau$ with $\Lambda_\tau(N)/\Lambda_\tau \cong \mathbb{Z}/N$. Hence a point $P_N \in Y_0(N)$ is the $\mathbb{C}$-isomorphism class of a *pair* $(\mathcal{E}_\tau, C_N)$ where C_N is a cyclic group of order N in $\mathcal{E}[N]$.

In other words, $Y_0(N)$ parametrizes *isomorphism classes of elliptic curves together with cyclic isogenies η_N of order N* and so they are moduli spaces for the pairs $(\mathcal{E}, \eta_N)$ over $\mathbb{C}$. Using Hurwitz genus formula and the well known fixed points of $\Gamma_0(N)$ one can compute the genus g_N of $X_0(N)$. We have that $g_N \sim N$. For $N = p$ a prime we get

$$g_N = \begin{cases} 0 \quad if \quad p = 2, 3 \\ \dfrac{(p-13)}{12} \quad if \quad p \equiv 1 \mod 12 \\ \dfrac{(p-5)}{12} \quad if \quad p \equiv 5 \mod 12 \\ \dfrac{(p-7)}{12} \quad if \quad p \equiv 7 \mod 12 \\ \dfrac{(p-11)}{12} \quad if \quad p \equiv 11 \mod 12 \end{cases}$$

5.1.1. *Modular functions and forms.* Because of the construction as quotient of $\mathbb{H}^*$ we can identify algebraic-geometric objects on X_0 with analytic objects attached to $\mathbb{H}^*$ with specific symmetry properties. For instance, rational functions on $X_0(N)$ come from those meromorphic functions on $\mathbb{H}^*$ that are invariant under the action of $\Gamma_0(N)$, ie.

$$f\left(\frac{az+b}{cz+d}\right) = f(z) \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

and are called *modular functions* of level N. A basic example is $j(z)$, which is modular of level 1 and hence of all levels. Since for all τ the elliptic curve the lattice $\mathbb{Z} + \frac{\tau}{N}\mathbb{Z}$ gives rise to an isogeny of $\mathcal{E}_\tau$ with cyclic kernel of order N the function $j\left(\frac{z}{N}\right) =: j_n(z)$ is a modular function of level N, and one checks that $\mathbb{C}(X_0(N))$ is isomorphic to $\mathbb{C}(j(z), j(\frac{z}{N}))$.

Differentials ω on $X_0(N)$ are of the form $f(z)dz$ with $f(z)$ meromorphic on $\mathbb{H}^*$ and, because of their invariance under $\Gamma_0(N)$, they satisfy a functional equation

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z) \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Such functions f are called *modular forms of weight* 2. If ω is holomorphic then $f(z)$ is holomorphic on $\mathbb{H}$ and vanishes on the cusps: $f(z)$ is a cusp form of weight 2 and level N. We know from the Riemann-Roch theorem that the cusp forms $\mathcal{S}_0(N)(\mathbb{C})$ are a $\mathbb{C}$-vector space of dimension g_N. This space plays a very important role in the arithmetic of modular forms.

5.1.2. *q-expansion.* Modular forms and functions are invariant under the transformation $z \mapsto z + 1$. Define as new variable $q = e^{2\pi i z}$ (hence transform neighborhoods of $i \cdot \infty$ to neighborhoods of 0). Then we can form the Fourier series of modular forms and functions $f(q)$ and get the **q-expansion**

$$f(q) = \sum_{j=k}^{\infty} a_j q^j$$

with $k \in \mathbb{Z}$. If f is a cusp form then $k \geq 1$. Modular forms and functions are uniquely determined by their Fourier expansion.

5.2. Modular polynomials. The important fact is that in many cases one can compute the coefficients of the q-expansion effectively. This is so for $j(q)$ (and hence for j_N in the variable $q^{1/N}$). In particular, $j(q)$ has a pole of order 1 at 0 and has coefficients in $\mathbb{Z}$, and for the exact expression see [**7**, Proposition 5.41].

We know that j_N satisfies a polynomial over $\mathbb{C}(j)$ of degree $\varphi(N)$. To find this polynomial (and so an equation for $X_0(N)$) one compares sufficiently many coefficients of the Fourier expansion and finds the *modular polynomials* $\phi(j, j_N)$ which are monic and symmetric in (j, j_N) and have degree $\varphi(N)$ in j and j_N.

So two elliptic curves with j-invariants j_1 and j_2 are isogenous under a cyclic isogeny of degree N if and only if $\phi_N(j_1, j_2) = 0$. The equation $\phi_N(X, Y) = 0$ is the canonical equation of the affine modular curve $Y_0(N)$, and $X_0(N)$ is given by the closure in $\mathbb{P}^2$. We display $\phi_N(x, y)$ for $N = 2, 3$.

$$\begin{aligned}
\phi_2 &= x^3 - x^2y^2 + y^3 + 1488xy(x+y) + 40773375xy - 162000(x^2+y^2) \\
&\quad + 8748000000(x+y) - 157464000000000 \\
\phi_3 &= -x^3y^3 + 2232x^3y^2 + 2232y^3x^2 + x^4 - 1069956x^3y + 2587918086x^2y^2 \\
&\quad - 1069956y^3x + y^4 + 36864000x^3 + 8900222976000x^2y + 8900222976000y^2x \\
&\quad + 36864000y^3 + 452984832000000x^2 - 770845966336000000xy + 452984832000000y^2 \\
&\quad + 18554258718720000000x + 18554258718720000000y
\end{aligned}$$

There are tables of modular polynomials for large N.

REMARK 8. *There have been some attempts in the last decade to generalize modular polynomials for higher dimensional varieties. The interested reader should consult* [**4**] *for abelian surfaces.*

5.3. The arithmetical theory of modular curves. A general reference for the following discussions is [**53**]. One observes that the modular polynomials have coefficients in $\mathbb{Z}$. This is no accident.

Looking at the modular interpretation one sees that the curves $X_0(N)$ represent over $\mathbb{C}$ a moduli problem: "Parametrize the isomorphism classes of pairs $(\mathcal{E}, \eta_N)$ of elliptic curves with cyclic isogeny of degree N".

This problem makes sense over any ring R with invertible element N and so over $\mathbb{Z}[1/N]$. Because of the existence of twists χ and the fact that the pair $(\chi(\mathcal{E}), \chi(\eta_N))$ is isomorphic to $(\mathcal{E}, \eta_N)$ over $\bar{k}$ but in general not over k we cannot expect to find a fine moduli scheme for our problem. But a coarse moduli scheme exists and so $\mathbb{H}^*/\Gamma_0(N)$ is the constant field extension of a curve $X_0(N)$ (i.e a scheme of relative dimension 1) over $\mathbb{Z}[1/N]$ with affine part given by the equation $\phi_N(X, Y)$.

A deep analysis of reductions of modulo prime numbers dividing N due to Deligne-Rapoport ([**14**]) and Katz-Mazur ([**40**]) shows that one can define $X_0(N)$ over $\mathbb{Z}$. Hence all geometric objects like holomorphic differentials (and so cusp forms) have a $\mathbb{Z}$-structure and so it makes sense to speak of $\mathcal{S}_0(N)(R)$, the R-module of cusp forms over the commutative ring R (to avoid complications assume that N is invertible in R).

How to find these cusp forms? Following a ground breaking idea of **J. Tate** one replaces the theory of elliptic curves over $\mathbb{C}$ by the theory of elliptic curves in the realm of rigid p-adic spaces and finds the elliptic Tate curve in $\mathbb{Z}((q))$, the

ring of formal Laurent series in one variable in q. Using this curve and exploiting functions and differentials on this curve one finds the q-expansion over all rings R and gets for instance:

THEOREM 34 (**q-expansion principle**). *Let R be a commutative ring with $N \in R^*$. Then the q-expansion determines uniquely holomorphic differentials on $X_0(N)$, and in particular we have:*

(1) *$f \in \mathcal{S}_0(N)(R)$ if and only if the Fourier expansion of f has coefficients in R, and*
(2) *there exists a $\mathbb{Z}$-base $f_1, \ldots, f_{g_N}$ of $\mathcal{S}_0(N)(\mathbb{Z})$ such that*

$$\mathcal{S}_0(N)(R) = \langle f_1, \ldots, f_{g_N} \rangle \otimes R.$$

We can apply these results to the Jacobian variety and its minimal model over $\mathbb{Z}$, denoted by $\mathcal{J}_0(N)_{\mathbb{Z}}$. Endomorphism of this variety are uniquely determined by their action on $\mathcal{S}_0(N)(\mathbb{C})$ and so accessible to computation after we have computed a base of the cusp forms over $\mathbb{Z}$. This computation is done in an effective way by using *modular symbols* (see [**54**]). It turns out that $\mathrm{End}_{\mathbb{Z}}(\mathcal{J}_0(N)_{\mathbb{Z}})$ is large, it contains the Hecke algebra $\mathcal{T}_N$ generated by Hecke operators constructed in Section 8. In particular, it follows that simple factors of $\mathcal{J}_0(N)$ have real multiplication.

Galois representations of $G_{\mathbb{Q}}$ attached to the Tate modules of these factors split up in a sum of 2-dimensional representations. One of the greatest results in Arithmetic Geometry is the theorem of Khare-Kisin-Wintenberger (see [**41**], [**42**]) which confirms the conjecture of Serre and states that all odd two-dimensional Galois representations are obtained (up to twists by characters) by the operations on appropriate factors of $\mathcal{J}_0(N)$ with an explicit recipe how to find N and the twist character. From this, the Fermat conjecture FLT is an easy consequence (a "five line proof").

Part 2. Cryptography

For communication in the modern world it is crucial that one can use open communication channels to

- exchange keys,
- sign messages
- authenticate entities, and
- encrypt and decrypt (not too large) messages

with simple protocols, clear and easy to follow implementation rules based on *cryptographic primitives*, which rely on (hopefully) hard mathematical tasks. The part of cryptology, which is devoted to solve these challenges is *public key cryptography* and relies on the ground breaking ideas of Diffie and Hellman [**17**]. In this paper we shall concentrate to the first item in its simplest form (and not using a secure protocol). The reader is encouraged to look at the other aspects, too, e.g. in [**7**].

6. Diffie-Hellman key exchange

6.1. The classical case. The task to solve is: find a protocol such that two partners P_1 and P_2 can agree on a common secret by using public channels and algorithms.

A groundbreaking solution was found by W. Diffie and H. E. Hellman in [**17**] with the idea to use (computational) one-way functions. They suggest to use the

multiplicative group of finite fields $\mathbb{F}_q$ and, for a prime number $\ell | q-1$ choose a primitive root ζ_ℓ, private keys $k_i \in \mathbb{Z}$ and public keys $p_i = \zeta_\ell^{k_i}$. The common secret is

$$s_{1,2} = \zeta_\ell^{k_1 \cdot k_2}.$$

All computations are very fast (polynomial in $\log(q)$). The security is measured by the hardness of the **Diffie-Hellman** computational problem (CDH):

For random elements $a, b \in \{0, \ldots, \ell - 1\}$ and given $\zeta_\ell^a,\ \zeta_\ell^b$ compute $\zeta_\ell^{a \cdot b}$.

Let ζ be a primitive root of unity in $\mathbb{F}_q^*$. Define the (classical) discrete logarithm (DL) of an element $x \in \mathbb{F}_q^*$ with respect to the base ζ by

$$\log_\zeta(x) = \min \{n \in \mathbb{N} \text{ such that } \zeta^n = x.\}$$

It is obvious that an algorithm that computes discrete logarithms (e.g. in ζ_ℓ) solves (CDH). This problem is rather old (going back at least to the 19-th century). C.F. Gauss introduced the term "index" in the Disquisitiones Arithmeticae (1801) for the discrete logarithm modulo p, and there are tables for primes up to 1000 by C. G. Jacobi (1839).

A systematic algorithm is given in the book of Kraichik (1922) [**43**]; in fact this is the index-calculus algorithm reinvented and refined in cryptography from 1980 till today [**37**]. As result one gets algorithms of subexponential complexity (with relatively small constants, see [**37**]), which are even dramatically faster if q is not a prime. The reason for these fast algorithms is the fact that it is easy to lift elements in $\mathbb{F}_q$ to elements in rings of integers of number fields.

6.2. A first abstraction. Obviously we can use the Diffie-Hellman key exchange scheme if we have

- a finite cyclic group $(C, \circ)$ with a generator g_0,
- a numeration, i.e. an injective map

$$f : C \to \mathbb{N},$$

- an addition law $\oplus$ on $f(C)$ with

$$f(f^{-1}(a) \circ f^{-1}(b)) = a \oplus b \text{ for all } a, b \in f(C).$$

$f(C)$ becomes a $\mathbb{Z}$-module with the usual scalar multiplication: $0 \cdot a = f(0_C)$, $n \cdot a = (n-1)$-fold addition of a to itself, $(-n) \cdot a = n \cdot (\ominus a)$ for $a \in f(C)$, $n \in \mathbb{N}$.

The private keys are again $k_i \in \mathbb{Z}$, the public keys are $k_i \cdot f(g_0)$, and the common secret is $k_1 \cdot (k_2 \cdot f(g_0))$. The CDH problem is: for random $a_1,\ a_2 \in f(C)$ with publicly unknown k_1, k_2 such that $k_i \cdot f(g_0) = a_i$ compute $c = (k_1 \cdot k_2) \cdot f(g_0)$.

Define the discrete logarithm (DL) by

$$\log_{g_0}(a) := \min \{n \in \mathbb{N} \mid \text{ such that } n \cdot f(g_0) = a.\}$$

Again, the computation of the (DL) solves CDH. By elementary number theory (CRT and p-adic expansion) one sees immediately that the computation of (DL) is reduced to the computation of the discrete logarithms in all $f(C_\ell)$ with C_ℓ the subgroup of C of elements of order dividing ℓ and ℓ dividing $|C|$. Hence we can and will assume from now on that C is cyclic of prime order ℓ. For shortness, we denote the task to compute the discrete logarithm by (DLP).

6.2.1. *Black box groups.* A "generic" object of the situation above is given by a black box group C of prime order ℓ.

(1) There are algorithms that compute (DL) (probabilistically) with $\mathcal{O}(\sqrt{\ell})$ group operations in C (e.g. Shank's bay-step giant step algorithm, Pollard's ρ algorithm et.al.), these algorithms are applicable for all finite cyclic groups, and one cannot do better.
(2) Up to algorithms with subexponential complexity, the computation of (DL) in C is equivalent with (CDH)(Maurer-Wolf).

6.3. Mathematical task. In order that we can use (a family of) groups C for crypto systems based on discrete logarithms they have to satisfy four crucial conditions:

(1) C has a known large prime order ℓ and a numeration $f : C \to \mathbb{N}$.
(2) Condition for the numeration: The elements in C can be stored in a computer in a compact way (e.g. $\mathcal{O}(\log \ell)$ bits needed).
(3) The group composition $\oplus$ induced by f is given by an algorithm that is easily and efficiently implemented and very fast.
(4) The computation of the DL in $f(C)$ (for random elements) is very hard and so infeasible in practice (ideally the bit-complexity should be exponential in $\log \ell$).

It is surprisingly hard to construct such groups. All known examples today are related with subgroups of Picard groups of hyperelliptic curves of genus ≤ 3 over prime fields $\mathbb{F}_p$. It will be one of the main aims of the paper to explain this statement.

6.4. Q-bit security. As said, we shall describe below DL-systems for which we have good reasons to believe that the bit-complexity is exponential and so the task in Section 6.3 is solved. But the possibility that *quantum computing* may be realizable in foreseeable time yields new aspects for the discussion of security of crypto systems. By Shor's algorithm it follows that the q-bit complexity of discrete logarithms in **all** finite groups is polynomial!.

So it is challenging to find key exchange systems that are not based on discrete logarithms in groups but still are near to the original idea of Diffie and Hellman. In the quantum world new relations between crypto primitives arise, and it seems that hidden subgroup problem and connected to it, the hidden shift problem related to groups G are central ([**60**] and [**44**]). Here the state of the art is that for abelian groups G the problems can be solved in subexponential time and space, for dihedral groups there is "hope".

6.5. Key exchange with G-sets. The DL-system in Section 6.3 can be seen in the following way: By scalar multiplication $f(C)$ becomes a $\mathbb{Z}$-set, and so elements of $\mathbb{Z}$ induce commuting endomorphisms on $f(C)$.

Denote by $\mathbb{Z}'$ the semigroup of elements in $\mathbb{Z}$ prime to $|f(C)|$. Then the set A of generators of $f(C)$ becomes a $\mathbb{Z}'$-set, and elements in $\mathbb{Z}'$ induce commuting endomorphisms of A. A next step to generalize the Diffie-Hellman key exchange is to replace $\mathbb{Z}'$ by a (semi-) group G and the set of generators of $f(C)$ by a G-set $A \subset \mathbb{N}$ on which G operates transitively. For $g \in G$, define $t_g \in \mathrm{End}_{set}(A)$ by

$$a \mapsto t_g(a) := g \cdot a.$$

Let G_1 be a semi-subgroup of G and $G_2 = Z(G_1)$ the centralizer of G_1 in G (if G is abelian then $G = G_1 = G_2$). Because of

$$g_1 \cdot (g_2 \cdot a_0) = (t_{g_1} \circ t_{g_2}) \cdot a_0 = (t_{g_2} \circ t_{g_1}) \cdot a_0$$

for $g_1 \in G_1$ and $g_2 \in G_2$ we can use (A, a_0, G_1, G_2) for key exchange by defining an obvious analogue of the scheme in Section 6.3.

The security of this exchange depends on the difficulty to find the translations t_{g_i}. We remark that though the security of such systems is, in general, not related to discrete logarithms, it may happen that the generic algorithms from Section 6.3 can still be applied.

What about quantum security? One breaks the system if one can determine t_{g_1}. This is a typical problem for the hidden shift. Take the maps

$$f_0 : G_1 \to A, \text{ such that } f_0(g) = t_g \cdot a_0$$
$$f_1 : G_1 \to A, \text{ such that } f_1(g) = t_g \cdot (t_{g_1} \cdot a_0)$$

and find the shift. For G_1 abelian and finite there is an algorithm of Kuperberg [**44**], which solves this task in subexponential time. In particular we see that every Diffie-Hellman key exchange based on $\mathbb{Z}$-sets has at best subexponential security.

6.6. Abstract setting of key exchange. On our way to generalization we get rid of the algebraic structures. Assume $A \subset \mathbb{N}$ and let $B_1, B_2 \subset \mathrm{End}_{set}(A)$. Choose $a_0 \in A$. We need the **centralizing condition**. The elements of B_1 commute with the elements of B_2 on $B_i\{a_0\}$. Then

$$b_1(b_2(a_0)) = b_2(b_1(a_0))$$

and this is all we need for key exchange.

The effectiveness of this exchange is given if for $b_i \in B_i, b_j \in B_j$ the value $b_i(b_j(a_0))$ can be quickly evaluated (i.e., calculated and represented). The analogue of the Computational Diffie-Hellman problem is

CDH: For randomly given $a_1, a_2 \in A$, compute (if exists) a_3 with
$$a_3 = b_{a_1} \cdot (b_{a_2} \cdot a_0),$$

where $b_{a_i} \in B_i$ such that $b_{a_i} \cdot a_0 = a_i$. It is clear that CDH can be solved if one can calculate for random $a \in B_i \cdot \{a_0\}$ an endomorphism $b_a \in B_i$ with $b_a(a_0) = a$. We remark that b_a may not be uniquely determined by a.

Problem:

(1) Find a "genuine" usable instance for the abstract setting!
(2) What can one say about quantum computing security?

6.7. Key exchange in categories. We make a final step of abstraction. As always we assume that we have two partners P_1 and P_2 who want to have a common secret key.

Let $\mathcal{C}_i$, $i = 1, 2$ be two categories whose objects are the same sets A_j and with morphisms $B^i_{j,k} = \mathrm{Mor}^i(A_j, A_k)$. We fix a "base" object A_0 and assume that $\mathcal{C}_1, \mathcal{C}_2, A_0$ satisfies the following conditions:

(1) For every $\varphi \in B^1(A_0, A_j)$ and every $\psi \in B^2(A_0, A_k)$ the pushout exists, i.e. there is a uniquely (up to isomorphisms) determined triple
$$(A_l,\ \gamma_1 \in B^1(A_k, A_l),\ \gamma_2 \in B^2(A_j, A_l))$$

with

$$\gamma_2 \circ \varphi = \gamma_1 \circ \psi$$

such that this triple is minimal (universality condition).

(2) P_1 can determine A_l if he knows φ, A_k and an additional (publicly known) information $P(\psi)$ (which is often a subset of A_k), and an analogue fact holds for P_2.

Key exchange. Given such categories $\mathcal{C}_1, \mathcal{C}_2$ the partners can chose φ, ψ, send A_j, A_k and $P(\psi)$ respectively $P(\varphi)$ and compute the ***common secret*** A_l.

Effectiveness. We assume that all the objects concerning $\mathcal{C}_i$ can be handled by computers in a fast and compact way, in particular, for chosen φ, ψ the objects A_j, A_k as well as the additional information can be computed rapidly. Moreover, using the given information, P^i can compute of A_l quickly.

Security. The scheme is broken if (CDH) is weak: For randomly given A_j, A_k determine A_l, which is the pushout of

$$A_0 \stackrel{\varphi}{\to} A_j$$

and

$$A_0 \stackrel{\psi}{\to} A_k.$$

For this, it is allowed to use the additional information. We shall see an example for this categorial key exchange in Section 11.3.3, and till now all algorithms for breaking this system have exponential complexity.

7. Index calculus in Picard groups

We want to use systems based on discrete logarithms in groups G and so find groups which satisfy the conditions formulated in Section 6.3. Motivated by ideas of V. Miller and N. Koblitz we want to use subgroups of Picard groups of curves over finite fields. Thm. 29 of Hess-Diem implies that at least in principle for such groups the conditions 2 and 3 are satisfied. For finding subgroups of large prime order one has to be able to determine the order of Picard groups rapidly. Here the key word is point counting, and again there is, in principle, a solution by a polynomial time algorithm due to Pila generalizing the Schoof algorithm for elliptic curves. But these algorithms are much too slow, and an acceleration is only known for elliptic curves (AES-algorithm), for curves of genus 2 (Gaudry, Schost) and for curves with special endomorphism rings (complex multiplication or real multiplication).

But before investing a lot of work in point counting it is useful to look at the security aspect. We want to compare the hardness of the computation of the DL in the specific groups with the generic hardness, i.e. $\sim |G|^{1/2}$. We recall that a main reason against the classical DL was the index-calculus algorithm, which is based on the (easy) lifting of finite fields to integers in number fields or function fields over finite fields. This kind of attack is not possible in Picard groups of curves of positive genus as pointed out by Miller and Koblitz: The "golden shield" of the Néron-Tate quadratic form prevents a (easy) lifting of elements in Abelian varieties over finite fields to global fields. But unfortunately there are very effective variants of the index- calculus attack to Picard groups.

7.1. Introduction to index calculus. Let $(G, \oplus)$ be a cyclic group of order N with generator g_0.

First step: Find a "*factor base*" consisting of relatively few elements and compute G as $\mathbb{Z}-$module given by the free abelian group generated by the base elements modulo relations.

So choose a subset $\mathcal{B} = \{g_1, \ldots, g_r\}$ of G generating G and look for relations

$$R_j : \oplus_{i=1}^{r} [n_i] g_i = 0_G. \tag{14}$$

Obviously R_j yields the relation

$$\sum_{i=1}^{r} n_i \log_{g_0}(g_i) \equiv 0 \mod N \tag{15}$$

for discrete logarithm.

We assume that we can find sufficiently many independent relations as in Eq. (14) for solving the system in Eq. (15) via linear algebra for $\log_g g_i$, $i = 1, \ldots, r$. Then we have an explicit presentation of G as $\mathbb{Z}$-module by

$$G \cong \mathbb{Z}^r / \langle \ldots, R_j, \ldots \rangle.$$

Second step: Take $g \in G$ randomly and chose a "random walk" with steps $g^0 = g, \ldots, g^j = [k_j] g^{j-1}$ and assume that after a few steps j we find a tuple $e_1, \ldots, e_r$ with e_i small and

$$g^j = [e_1] g_1 + \cdots [e_r] g_r.$$

"To find" means: There is a fast algorithm to decide whether such e_i exist, and then the computation of these e_i is also fast. This boils down to a smoothness condition. (Recall: A number $n \in \mathbb{N}$ is B-smooth if all prime divisors of n are $\leq B$, and results from analytic number theory by Canfield, Erdös, Pomerance determine the probability for n being smooth.) The second step is usually done by an appropriate sieving method.

The important task in this method is to balance the number of elements in the factor base to make the linear algebra over $\mathbb{Z}$ manageable and to guarantee "smoothness" of arbitrary elements with respect to this base. Usually one finds a kind of *size* in G (size of lifted elements in $\mathbb{Z}$ or degree in polynomial rings, degree of reduced divisors , ...) to define factor bases. Typically , successful index-calculus approaches give rise to algorithms for the computation of the DL in G which have *subexponential* complexity and so, for large enough order of G, the DL-system has a poor security.

For an axiomatic approach of index-calculus algorithms we refer to [**19**]. This principle is refined in concrete situations with enormous effect as we shall see below.

7.2. Index calculus for hyperelliptic Jacobians. Index calculus can be applied to a DL in Jacobians of hyperelliptic curves. Let $\mathcal{C}$ be a hyperelliptic curve of genus $g \geq 2$ over a finite field $\mathbb{F}_q$ of characteristic p and G a cyclic subgroup in $\mathrm{Pic}^0_{\mathcal{C}}$.

We can represent every element in G in a unique way by the Mumford representation $[u(x), v(x)]$, where $u(x)$ is a polynomial in $\mathbb{F}_q[X]$ of degree $\leq g$.

As factor base we choose points in $\mathrm{Pic}^0_{\mathcal{C}}$ with $u(X)$ irreducible of degree at most B, a chosen smoothness bound. A divisor is said to be B-*smooth* if all the prime divisors in its decomposition have degree at most B. This leads to the historically

first algorithm to compute discrete logarithms in Picard groups of hyperelliptic curves. It is due to Adleman, Demarrais, and Huang. For an explicit description of the algorithm see [**7**, pg. 525]. For $N \in \mathbb{Z}^{>0}$, $s, c \in \mathbb{R}$, with $0 \leq s \leq 1$ denote

$$L_N(s,c) = \exp\left((c+o(1))\left(\log N\right)^s \left(\log\log N\right)^{1-s}\right),$$

as $N \to \infty$. Then we have:

THEOREM 35. *For* $\log q \leq (2g+1)^{1-\epsilon}$, *there exists a constant* $c \leq 2.18$ *such that the discrete logarithms in* $\mathrm{Jac}_{\mathcal{C}}(\mathbb{F}_q)$ *can be computed in expected time* $L_{q^{2g+1}}(1/2, c)$.

This remarkable result gives an subexponential algorithm for "large" genus. But much more important for practical applications are *exponential* algorithms, which weaken the DLP for small but realistic genus. The first groundbreaking result is

THEOREM 36 (Gaudry). *Let* $\mathcal{C}$ *be a a hyperelliptic curve of genus* $g \geq 2$ *defined over a finite field* $\mathbb{F}_q$. *If* $q > g!$ *then discrete logarithms in* $\mathrm{Jac}_{\mathbb{F}_q}(\mathcal{C})$ *can be computed in expected time* $O(g^3 q^{2+\epsilon})$.

Since the expected size of $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)$ is q^g (see Weil's result, Thm. 12) we are, for $g > 4$, far away from the generic security bound, and so we have to exclude hyperelliptic curves of genus ≥ 5 if we want a DL-system in Picard groups. But Gaudry's result can be sharpened. N. Thériault suggested to use "large primes" as well as the original elements of the factor base consisting of points on the curve of small degree. With many more refinements [**28**] one gets

THEOREM 37. *There exists a (probabilistic) algorithm which computes the DL, up to* log*-factors, in the divisor class group of hyperelliptic curves of genus* g *in expected time of* $\mathcal{O}(q^{(2-2/g)})$.

This rules out $g = 4$ for hyperelliptic curves since the ratio of the expected group order to time complexity, $\mathcal{O}(q^g)/\mathcal{O}(q^{2-2/g})$, gets too big.

7.3. Index-calculus in Picard groups in curves with plane models of small degree. The following is mainly work of C. Diem. He gives an algorithm for computing discrete logarithms in $J_{\mathcal{C}}(\mathbb{F}_q)$ assuming that one has a plane curve $\mathcal{C}'$ of degree d. We recall that for non-hyperelliptic curves $d = 2g_{\mathcal{C}} - 2$ is possible but that for hyperelliptic curves $d \geq g_{\mathcal{C}} + 1$.

So the minimal degree of plane models of hyperelliptic curves of genus ≥ 3 is larger than the degree of such models for non-hyperelliptic curves. Using factor bases constructed with the help of Semaev polynomials and using a large amount of ingredients from abstract algebraic geometry (e.g. membership tests for zero-dimensional schemes) Diem succeeds to prove:

THEOREM 38. *Fix* $d \geq 4$. *Then the DLP in* $\mathrm{Pic}^0_{\mathcal{C}}$ *of curves birationally equivalent to plane curves of degree* d *can be solved, up to* log*-factors, in expected time* $\mathcal{O}(q^{2-\frac{2}{d-2}})$.

For genus 4 and non-hyperelliptic curve $\mathcal{C}$ we get $d = 6$ and so the hardness of D is bounded, up to log-factors, by $\mathcal{O}(q^{3/2})$. Since the expected group size is q^4 this is too far away from the generic complexity, and it is not advisable to use (hyperelliptic or not hyperelliptic) curves of genus 4 for DL-systems.

For non-hyperelliptic curves of genus 3 we get $d = 4$ and so the complexity of the DL is $\mathcal{O}(g)$ and again such curves can not be used for DL-systems. Hence our discussion for fulfilling conditions 3 and 4 in Section 6.3 can be restricted to hyperelliptic and elliptic curves of genus $1, 2, 3$. Before doing this in detail we have one more general section, interesting both from theoretical and practical point of view.

8. Isogenies of Jacobians via correspondences and applications to discrete logarithms

We describe a general construction of isogenies between abelian varieties closely attached to Jacobians of curves. The crypto-graphical relevance of these constructions is that every computable isogeny yields a transfer of the (DLP), and it may be easier to solve the problem after the application of the isogeny.

As always, k is assumed to be a perfect field. Let L be a finite algebraic extension field of k. Let $\mathcal{D}_1$ be a regular projective curve over L and $\mathcal{D}_2$ a regular projective curve defined over k. We recall some properties of cover morphisms of curves and attached norm and conorm homomorphisms of Jacobians. Let $\mathcal{H}$ be a curve over L and

$$\varphi_1 : \mathcal{H} \to \mathcal{D}_1,$$

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_1 induces the **norm morphism**

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

By composition we get a homomorphism

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

defined over L.

Let $\mathcal{W}_{L/k}$ be the Weil restriction of the Jacobian of $\mathcal{D}_1$ to k. This is an abelian variety defined over k with $\mathcal{W}_{L/k}(k) = \mathrm{Pic}^0_{\mathcal{D}_1}$. Applying the norm map from L to k and using the functorial properties of the Weil restriction 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, usually 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 $\mathcal{J}_{\mathcal{D}_2}$.

As application we get a transfer of the discrete logarithm problem from $\mathrm{Pic}^0_{\mathcal{D}_1}$ (defined over L) to the DL-problem in a subvariety of $\mathcal{J}_{\mathcal{D}_2}$ (defined over k). Of course, the efficiency of this transfer depends on the complexity of the algorithms computing the norm and conorm maps (hence φ_i and $[L : k]$ must have reasonably small degrees), and an attack makes sense only if the DL-problem after the transfer is easier than before.

8.1. 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 $\mathcal{C}$ defined 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 $\mathcal{J}_\mathcal{C}$ to $\mathcal{J}_\mathcal{D}$. Then $\mathcal{D}$ will (in all non-trivial cases) be a curve of a genus larger than the genus of $\mathcal{C}$ 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 in Section 7. Indeed, if $\mathcal{C}$ is not defined over a proper subfield of $\mathbb{F}_{q^d}$ this is the principle of the so-called GHS-attack in (see [**25**] and [**7**, Section 22.3.2]), which is successful in remarkably many cases.

If $\mathcal{C}$ is already defined over $\mathbb{F}_q$ one is lead to the so-called trace-zero varieties in $\mathrm{Jac}_\mathcal{C}(\mathbb{F}_{q^d})$ (see [**7**, Section 7.4.2]) and again correspondences induced by covers of curves can be used for attacks on crypto systems based on discrete logarithms on these varieties by work of Diem [**7**, 22.3.4]. These results already indicate that the use of Picard groups of curves (e.g. elliptic curves) over non-prime fields $\mathbb{F}_{q^d}$ 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. The methods used in these papers use the Weil restriction method explained above only as a "guideline" and sometimes as tools for proof. The real heart of the methods of Diem is the use of Semaev's summation polynomials. In this context and in particularly because of suggestions of pairing based cryptography using (supersingular) elliptic curves it is important to mention the enormous progress made in the computation of discrete logarithm in the multiplicative group of finite non-prime fields [**37**].

8.2. Modular correspondences. We recall from Section 5 that for N prime to char (k) the modular curve $X_0(N)$ is a regular projective curve, defined over $\mathbb{Z}[1/N]$ and so in particular over $\mathbb{Q}$ and over $\mathbb{F}_p$ with p prime to N. As explained in Section 5 there is an affine part $Y_0(N)$, which is a (coarse) moduli scheme for the isomorphism classes of pairs (E, η_N) of elliptic curves with cyclic isogeny of degree N. This means that for every point $P = (j_E, j_\eta)$ in $Y_0(N)(k)$ there is an elliptic curve E defined over k and an isogeny $\eta_N : E \to E'$ with $\ker(\eta_N)$ invariant under the action of G_k and as abelian group isomorphic to $\mathbb{Z}/N$ such that the invariants of E and E' are (j_E, j_η).

The points in $X_0(N) \setminus Y_0(N)$ are the cusps, and it is important that these points have a modular interpretation, too. For example, if N is squarefree, then there is one cusp point at ∞ (in the upper half plane) which corresponds to the pair (Néron polygon with N vertices, $\langle\zeta_N\rangle$) where ζ_N is a primitive N-th root of unity.

Let ℓ be a prime not dividing $\mathrm{char(k)} \cdot \mathrm{N}$. By the splitting $\mathbb{Z}/\ell \cdot N \cong \mathbb{Z}/\ell \times \mathbb{Z}/N$ and an analogous splitting of the kernel of a cyclic isogeny of degree $\ell \cdot N$ in $C_\ell \times C_N$ we get a natural k-morphism

$$\varphi_\ell : X_0(\ell \cdot N) \to X_0(N).$$

Let ω_ℓ be the involution of $X_0(\ell \cdot N)$ induced by the map that sends the pair (E, η) with $\ker(\eta) = C_\ell \times C_N$ to the pair (E, η') where the kernel of η' is $E[\ell]/C_\ell \times C_N$. Define

$$\psi_\ell := \varphi_\ell \circ \omega_\ell : X_0(\ell \cdot N) \to X_0(N).$$

We are in the situation described above (with $k = L$) and can define the Hecke correspondence

$$T_\ell : \mathcal{J}_0(N) \to \mathcal{J}_0(N),$$

by $T_\ell := \varphi_{\ell *} \circ \psi_\ell^*$.

The Hecke ring of $X_0(N)$ is $\mathcal{T}_N = \langle T_\ell \text{ with } \ell \text{ prime to } N \rangle$, the ring generated by the endomorphisms T_ℓ. It is a commutative ring, which is very near to $\mathrm{End}(\mathcal{J}_0(N))$ (see [**53**]). It acts on the vector space of holomorphic differentials of $X_0(N)$ which can be identified with the k-vector space of k-rational cusp forms $\mathcal{S}_0(k)$ of level N (and trivial nebentype). By classical theory one knows that $\mathcal{T}_N$ is endowed with an Hermitian structure due to the Peterson scalar product, and so the eigenvalues of the operators T_ℓ are totally real numbers.

REMARK 9. *Assume that $\mathcal{A}$ is a simple factor of $\mathcal{J}_0(N)$. Then* $\mathrm{End}^0(\mathcal{A})$ *contains a totally real field of degree* $\dim(\mathcal{A})$.

This means that factors of $\mathcal{J}_0(N)$ have very special and large endomorphism rings. As consequence there is a splitting of Galois representations of $G_{\mathbb{Q}}$ constructed by the action on Tate modules of $\mathcal{J}_0(N)$ into a sum of two-dimensional representations with real eigenvalues, and these "modular representations" play a most important role in number theory, e.g. for the proof of Fermat's Last Theorem. The narrow relation to arithmetic is reflected by the **Eichler-Shimura** congruence

$$T_\ell = \mathrm{Frob}_\ell + \ell/\mathrm{Frob}_\ell,$$

where Frob is the Frobenius endomorphism on $\mathcal{J}_0(N) \bigotimes \mathbb{F}_\ell$. In particular, Frob_ℓ satisfies the **Eichler-Shimura** equation

$$X^2 - T_\ell \cdot X + \ell = 0.$$

A curve $\mathcal{C}$ whose Jacobian is a factor of $\mathcal{J}_0(N)$ is called **modular of level** N.

Using cusps forms it is possible to determine its period matrix, decide whether it is hyperelliptic, and then compute its Weierstrass equation (see [**73**], [**72**]). The *importance for cryptography* is the fact that Frob satisfies the quadratic Eichler-Shimura equation over a totally real number field, and this can be used for point counting for curves of genus ≥ 2 as in [**26**]. Hence *modular curves of genus* 2 *are potentially usable for DL-systems.*

8.3. Correspondences via monodromy groups. We assume that we have a cover morphism

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

defined over k of degree n, satisfying some fixed ramification conditions and having a fixed monodromy group $G_f := \mathrm{Mon}\ (f)$. We have morphisms

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

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. This setting is motivated by the theory of *Hurwitz spaces* and it is hoped that one can exploit their rich and, over $\mathbb{C}$, well understood theory ([**22**] and [**23**]).

Next we choose subgroups $H_1 \subset G_f$ fixing $\mathcal{C}$ 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 $\mathcal{C}$ and $\mathcal{D}$. Let

$$h : \mathcal{H} \to \mathcal{C} \quad \text{and} \quad g : \mathcal{H} \to \mathcal{D}$$

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

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

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

LEMMA 15. *Assume that $\mathcal{J}_\mathcal{D}$ is a simple abelian variety,* $\dim \mathcal{J}_\mathcal{D} = g_\mathcal{C}$, *and that there is a prime divisor $\mathfrak{p}_\infty$ of $\mathcal{C}$ which is totally ramified under h, i.e. 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 the projective line. Then η is an isogeny.*

PROOF. Since $J_\mathcal{D}$ is simple, it is enough to show that η is not the zero map. Let $\mathfrak{p}'_\infty$ be the norm of $\mathfrak{P}_\infty$ under g. Without loss of generality we can assume that k is algebraically closed. So we find a prime divisor $\mathfrak{P}$ of $\mathcal{H}$ which is different from all prime divisors in $g^{-1}(\mathfrak{p}'_\infty)$.

Let c be the class of $\mathfrak{p} - \mathfrak{p}_\infty$, where $\mathfrak{p} = h_*(\mathfrak{P})$. Then $\eta(c)$ is the class of the divisor

$$D_\mathfrak{p} := \sum_{\mathfrak{P}\in h^{-1}(\mathfrak{p})} g_*(\mathfrak{P}) - \deg(h)\cdot g_*(\mathfrak{P}_\infty).$$

Note that $D_\mathfrak{p} \neq 0$ (as divisor). If the class of $D_\mathfrak{p}$ would be trivial, then there would be a non-constant function on $\mathcal{D}$ with pole order $\leq \deg(h)$ and hence a non-constant map of $\mathcal{D}$ to the projective line of degree $\leq \deg(h)$, which is a contradiction. □

We shall see in Section 9 that we can realize the situation (over $\bar{k}$) of the lemma for hyperelliptic curves of genus 3 with non-decomposable Jacobian, f a polynomial of degree 6, $G_f = S_4$, H_1 a subgroup of order 2 and H_2 a subgroup of order 6. This leads to isogenies of degree 8 discussed by B. Smith, and generically maps hyperelliptic curves to non-hyperelliptic curves. The *importance for cryptography* is that generic hyperelliptic curves of genus 3 are not usable for DL-systems.

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.

9. Genus 3 curves and cryptography

QUESTION 1. *Can one use curves $\mathcal{C}$ of genus* 3 *for DL-systems?*

To find equations for random curves of genus 3 is easy: Either take a regular plane quartic (non-hyperelliptic curve) or a curve with equation $Y^2 = f(X)$ with $\deg(f) = 7$. In both cases the addition law is easily implemented and fast. If $\mathcal{C}$ is hyperelliptic, the Cantor algorithm is well-studied and fast, moreover one can transform it into formulas (involving, alas, many special cases), which 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 [**7**]. The timings are not too far away from additions in groups in elliptic curves (with comparable size order)(see [**7**, Table 14.13]). For non-hyperelliptic curves see [**20**]. But we have already discussed the security problem: One can only use hyperelliptic curves of genus 3 for which the Jacobians do not possess an easily computed isogeny to another principally polarized abelian variety which has

a non-hyperelliptic polarization. As we shall see next this will endanger the DL in "generic" hyperelliptic curves of genus 3.

9.1. Isogenies via S_4-covers. As observed by B. Smith [**66**] "many" hyperelliptic curves are isogenous to non-hyperelliptic curves via an isogeny with degree dividing 8. This fact is interpreted in terms of Hurwitz spaces and connected modular spaces in [**22**, **23**]. We refer for details and refinements to these papers.

For our purposes it will be enough to look at the case that the base field k is algebraically closed, which we shall assume from now on. For applications in cryptography one has to study rationality problems; see [**66**] and [**23**]. The construction relies on the so-called trigonal construction of Donagi-Livné [**18**]. We begin with a hyperelliptic curve $\mathcal{C}$ of genus 3 and its uniquely determined hyperelliptic projection $f_1 : \mathcal{C} \to \mathbb{P}^1$ with 8 ramification points $P_1, \cdots, P_8$, which extend to the Weierstrass points of $\mathcal{C}$. By linear algebra we show that 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 we can use Galois theory.

9.1.1. *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 a degree 2 cover $\mathcal{E}' \stackrel{h_2}{\to} \mathcal{C}$. 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).

9.1.2. *The monodromy group of $f = f_2 \circ f_1$.* Since f is a cover of degree 6, its Galois group can be embedded into S_6. But a closer analysis using the specific ramification situation shows; see [**22**, Thm. 3].

LEMMA 16. *The monodromy group of f is isomorphic to S_4.*

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

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

the projection to $\mathcal{C}$, which is a cover of degree 2. The Galois group of $\tilde{\mathcal{C}}/\mathcal{C}$ contains two transpositions. Let σ be one of them, chosen such that with $G_2 = \langle \sigma \rangle$ we get

$\mathcal{C}' := \tilde{\mathcal{C}}/G_2$. 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

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

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

We are interested in the case that $\mathcal{J}(\mathcal{C})$ is simple. Then we get from Section 8 that:

PROPOSITION 9. *Let $\mathcal{J}_\mathcal{C}$ be a simple abelian variety and $\mathcal{D}$ be non-hyperelliptic. The pair of cover maps $(\pi_\mathcal{C}, \pi_T)$ from $\mathcal{C}'$ to $(\mathcal{C}, \mathcal{D})$ induces an isogeny*

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

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. Thus we have the following:

COROLLARY 9. *The notations are as above. Let k be equal to $\mathbb{F}_q$ and assume that $\mathcal{D}$ is non-hyperelliptic. Then the computation of the Discrete Logarithm in $\mathrm{Pic}^0_\mathcal{C}$ 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 [**23**]. 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 hyperelliptic 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 $\mathcal{C}$, 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 [**23**] 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 39. *The Hurwitz space $\mathcal{H}_{hyp}$ is a unirational, irreducible variety of dimension* 4*, provided that char $k > 5$. Moreover, the natural forgetful 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 10. *Assume that k is algebraically closed. There is a 1-codimensional subscheme U of $\mathcal{M}_{3,hyp}$ such that for $\mathcal{C} \notin U$ the isogeny η maps $\mathcal{J}_\mathcal{C}$ 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 [**66**] and [**23**]. As result we get the following:

COROLLARY 11. *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 $|\operatorname{Pic}^0(C)| \sim q^3$, the DL system of these hyperelliptic curves of genus 3 is weak.*

9.2. Point counting. In general, not much is known about fast point counting algorithms on curves of genus 3 (aside of the general fact that for all abelian varieties there is a polynomial time algorithm due to Pila). But as we have seen above, for applications in cryptography we have to restrict ourselves to special hyperelliptic curves (where it is not at all clear what "special" means for a concrete curve), and so we do not lose much by restricting to hyperelliptic curves $\mathcal{C}$ whose Jacobian $\mathcal{J}_\mathcal{C} =: \mathcal{J}$ has a special endomorphism ring $\mathcal{O}_\mathcal{J}$.

9.2.1. *Real multiplication.* A first possibility is to assume that $\mathcal{J}$ has real multiplication. This means that $\mathcal{O}_\mathcal{J}$ contains an order $\mathcal{R}$ of a totally real field of degree 3. An immediate consequence is that there are many isogenies at hand, and in the case of genus 2 this situation has accelerated the point counting dramatically [**30**]. So there is hope that the same could happen for Jacobians of dimension 3. Hence it is interesting to construct hyperelliptic curves $\mathcal{C}$ such that $\mathcal{J}_\mathcal{C}$ has real multiplication. In view of the results about Jacobians of the modular curves $X_0(N)$ in Section 8.2 it is natural to look for curves whose Jacobian is a quotient of $J_0(N)$ for some N. This was successfully done by H. J. Weber ([**72**]). The procedure is as follows:

First, one computes eigenspaces of dimension 3 of the space of cusp forms of level N under the Hecke operators. Using the attached differentials one can compute (over $\mathbb{C}$) the period matrix of the corresponding factor $\mathcal{J}$ of $J_0(N)$ and decides whether it is principally polarized and hence is the Jacobian of a curve $\mathcal{C}$. Using theta-null values one decides whether $\mathcal{C}$ is hyperelliptic.

If so, one can compute invariants of the curve, and (e.g by using Rosenhain models compute a Weierstrass equation (at the end over $\mathbb{Z}[1/N]$) of $\mathcal{C}$ whose Jacobian is a simple factor of $\mathcal{J}_0(N)$. Reduction modulo p gives hyperelliptic curves over $\mathbb{Z}/p$ of genus 3 with (known) real multiplication.

The method works quite well but has one disadvantage: Since there are many non-hyperelliptic curves of genus 3 with real multiplication we are not sure whether the constructed curve is isogenous to a non-hyperelliptic curve under the trigonal construction described above.

9.2.2. *Complex multiplication.* We strengthen the condition on $\operatorname{End}(\mathcal{J})$ and assume that $\mathcal{J}$ has complex multiplication and so is the reduction of a curve defined over a number field. Recall that this means that there is an embedding of $\operatorname{End}(\mathcal{J})$ as order $\mathcal{O}$ into a CM-field K, i.e. K is a totally imaginary quadratic extension of a totally real field K_0 of degree 3 over $\mathbb{Q}$.

The arithmetic of $\mathcal{C}$ and $\mathcal{J}$ is reflected by the arithmetic of orders in K. In particular, one finds the Frobenius endomorphism of reductions of $\mathcal{C}$ modulo prime ideals $\mathfrak{p}$ of K as element in $\mathcal{O}$. This solves the problem of point counting on $\mathcal{C}$ modulo $\mathfrak{p}$ immediately. Moreover, class field theory of K gives both a classification of isomorphism classes of curves $\mathcal{C}$ with CM-field K and methods to find period matrices of $\mathcal{J}$ and so equations of $\mathcal{C}$. Details and more references can be found in [**7**] sections 5.1 and 18.3.

But trying to find examples for hyperelliptic curves attached to CM fields of degree 6 one runs into trouble since these examples seem to be very rare. (Recall that the hyperelliptic locus in $\mathcal{M}_3$ has codimension 1.) This was one of the results of the thesis of A. Weng (Essen 2001). So one has to use some force: If $\mathcal{J}$ has an automorphism of order 4 the curve $\mathcal{C}$ has an automorphism of order at least 2 and if $\mathcal{J}$ is simple the quotient of $\mathcal{C}$ by this automorphism has to be $\mathbb{P}^1$, and so $\mathcal{C}$ is hyperelliptic and has an automorphism of order 4. The existence of J with automorphism φ of order 4 is obtained by a special choice of the CM-field K:

Let K_0 be a totally real field of degree 3 with class number 1 (there are many fields with these properties) and take $K = K_0(\sqrt{-1})$, and for $\mathcal{O}$ take the maximal order of K. In [**73**] one finds in detail how these choices lead to many examples of hyperelliptic curves over finite fields suitable for cryptography.

There is a bit of hope that the following question may have an affirmative answer.

QUESTION 2. *We assume now that $\mathcal{C}$ is a hyperelliptic curve with an automorphism of order 4. Is $\mathcal{C}$ resistant against the trigonal attack?*

If the answer would be yes and since automorphisms of degree 4 survive under isogenies of degree prime to 2 one could hope to have a positive answer to the following.

QUESTION 3. *Let $\mathcal{C}$ be a hyperelliptic curve with an automorphism of order 4 and with simple Jacobian variety $\mathcal{J}$. Let*

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

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

In the case of a positive answer to the question the CM-curves with CM-field K of degree 4 containing $\sqrt{-1}$ would deliver nice and easy to handle candidates for cryptographically usable DL-systems

10. Genus 2 curves and cryptography

Curves $\mathcal{C}$ of genus 2 with at least one rational Weierstrass point P_∞ are very interesting objects for creating DL-systems and in most aspects they can very well compete with elliptic curves (see Section 11). The research area around these curves is attractive since there is a lot of activity but also a lot of unsolved problems till now.

Security. The hardness of the DL in the Picard groups of randomly chosen curves over prime fields of order q is comparable with the hardness on elliptic curves over prime fields of order q^2, in particular, all known versions of index-calculus attacks have a complexity equal to $\mathcal{O}(q)$ and hence are not more efficient than generic algorithms. (Recall that because of Thm. 12 we can expect that $|\operatorname{Pic}^0_{\mathcal{C}}| \sim q^2$.)

Addition: By our assumption we can assume that $\mathcal{C}$ is given by a Weierstrass equation

$$Y^2Z^3 = f(X, Z)$$

with $f(X, Z)$ homogenous and of degree 5 in X.

Hence we can use Mumford representations of reduced divisors and the Cantor algorithm (see Section 4.3). A detailed analysis including all special cases is done in [**7**, Section 14.3.2], including a determination of complexity (see Table 14.2 and Table 14.13).

Alternatively we use the interpolation formulas given explicitly in Example 5, and we have the choice to chose coordinates taylor-made to soft- and hardware environments. As result we can state that the efficiency of group operations in $\mathrm{Pic}^0_{\mathcal{C}}$ is on the same level as it is for elliptic curves.

If we are only interested in scalar multiplication (e.g. for key exchange) we can use, as in the case of elliptic curves, a "Montgomery ladder" to compute this multiplication. The role of x-coordinates of points on elliptic curves is played by coordinates on the Kummer surface related to the Abelian surface $\mathcal{J}_{\mathcal{C}}$.

Kummer surfaces The following is due to P. Gaudry [**24**] and Gaudry/Lubicz [**31**]. We embed $\mathcal{C}$ into $J_{\mathcal{C}}$ by using P_∞ as base point, and continue the hyperelliptic involution ω of $\mathcal{C}$ to $J_{\mathcal{J}_{\mathcal{C}}}$. Then $J_{\mathcal{C}}/w =: K$ is the Kummer variety of $\mathcal{C}$, and we have an embedding of $\mathbb{P}^1 \cong \mathcal{C}/w$ into K.

On K the action of $\mathbb{Z}$ is induced by the group structure on the Jacobian. One checks that one has a scalar multiplication but no group structure (compare the case of elliptic curves). Hence the usual add-and double algorithm to get a fast scalar multiplication does not work. To repair this one uses the **Montgomery ladder** (see [**7**]) which is well known for elliptic curves.

To make the ladder very fast one uses a remarkable tool: classical modular forms in an abstract setting!

More concretely, P. Gaudry uses in [**24**] classical theory of theta functions, their p-adic interpretation and reduction, exploits "classical" doubling formulas and gets **extremely simple doubling formulas**.

One drawback is that the model used for $\mathcal{C}$ based on Theta functions has bad reduction modulo 2. So in [**24**] Gaudry had to exclude the important case that the ground field has even characteristic. More arithmetic geometry, namely the theory of minimal models enabled him together with D. Lubicz to remove this restriction [**31**].

The third necessary aspect important for the construction of DL-systems is point counting, which has to be so effective that in reasonable time one finds by a random search curves $\mathcal{C}$ and fields $\mathbb{F}_p$ with the property that a large prime number ℓ with size $\sim q^2$ divides $|\mathcal{J}_{\mathcal{C}}(\mathbb{F}_p)|$.

10.1. Point counting on curves of genus 2.

10.1.1. *Point counting on random curves.* A generic method to determine the order of a finite group is given by a variant of Shank's baby-step giant-step method, whose efficiency depends on the size of the interval in which on can place $|\mathcal{J}_{\mathcal{C}}(\mathbb{F}_p)|$. This is used if one knows $|\mathcal{J}_{\mathcal{C}}(\mathbb{F}_p)|$ modulo a rather big number N together with the information given by the Hasse estimate.

To get such a congruence one tries to determine the characteristic polynomial of the Frobenius endomorphism ϕ_p modulo "enough" small numbers by its action on

torsion points. So a first step for counting algorithms is to determine polynomial or ideals which vanish on torsion points of a given order. This procedure was already the key part of Schoof's algorithm for elliptic curves (Section 11.2).

But for really fast algorithms for elliptic curves one needs one more ingredient: isogenies and corresponding modular polynomials respectively ideals.

For curves of genus 2 division polynomials and modular polynomials are not so well understood as for elliptic curves but as we have announced already in Example 5 this is an active area of research.

The starting point is the Mumford representation of points on $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_p)$. We assume that $\mathcal{C}$ is given by $y^2 = f(x)$ as before and $D = \langle u, v\rangle$ is a reduced divisor. Most reduced divisors have weight 2, i.e the degree of u is 2. The set of those divisors with strictly lower weight is called Θ. A divisor of weight 1 i.e., with a single point $P = (x_P, y_P)$, is represented by

$$\langle u(x), v(x)\rangle = \langle x - x_P, y_P\rangle. \tag{16}$$

The unique divisor of weight 0, is the identity $\mathcal{O}$ given as $\mathcal{O} = \langle u(x), v(x)\rangle = \langle 1, 0\rangle$. Any divisor of weight 2 is given as

$$\langle u(x), v(x)\rangle = \langle x^2 + u_1 x + u_2, v_0 x + v_1\rangle.$$

The following algorithm using **division polynomials** is due to Gaudry and Harley.

For a divisor of weight 1, i.e. given by an ideal $P = \langle x - x_P, y_P\rangle$ in general position we have

$$[l]P = \left\langle x^2 + \frac{d_1^{(l)}(x_p)}{d_0^{(l)}(x_p)}x + \frac{d_2^{(l)}(x_p)}{d_0^{(l)}(x_p)}, y_P\left(\frac{e_1^{(l)}(x_p)}{e_0^{(l)}(x_p)}x + \frac{e_2^{(l)}(x_p)}{e_0^{(l)}(x_p)}\right)\right\rangle$$

where $e_i^{(l)}, d_i^{(l)}$ are polynomials with degrees $\deg d_i^{(l)} = 2l^2 - (i+1)$ and $\deg e_i^{(l)} = 3l^2 - (i+1)$, for $i = 0, 1, 2$; see [**29**] for details.

For a divisor of weight two, we consider it as a sum of two divisors of weight 1, say $D = P_1 + P_2$ where $P_1 = \langle x - x_1, y_1\rangle$ and $P_2 = \langle x - y_2, y_2\rangle$, where x_1 and x_2 are roots of $u(x)$ and $y_i = v(x_i)$ and u, v come from the Mumford presentation. Then,

$$[l]D = [l]P_1 + [l]P_2.$$

With these formulas one computes the order of $\mathrm{Jac}_{\mathcal{C}}\,\mathbb{F}_p$ modulo l; see [**29**, Section 5.4]. The cost of the algorithm is

$$O(l^2)M(l^2) + O(d\log q)M(l^4) + O(l^2 + \log q)M(d),$$

where $M(n)$ is the number of field operations required to multiply two polynomials of degree n, and d is the smallest degree of resultants of $u(x)$ and $v(x)$; see [**29**].

Next one tries to determine "modular equations" for finite subschemes of $\mathcal{J}_{\mathcal{C}}$. Here a paper of P. Gaudry and E. Schost is a remarkable beginning (see [**27**]. Mixing the results and methods and using many tricks Gaudry and Schost succeed in [**32**] to count points on the Jacobian of some hundreds of random curves of genus 2 and finally found one having the security level of AES 128. The development still goes further. The interested reader should have a look at the paper [**1**].

10.2. Modular curves of genus two. In Section 10.1.1 we have seen that in principle one can find cryptographically relevant curves of genus 2 by a search on random curves using an analogue of Schoof's algorithm. But the necessary input of computing capacity (and implementation art) is rather heavy.

So it may be useful to look for classes of special curves for which point counting is easier. Again work of Gaudry, together with David Kohel and Benjamin Smith shows that one can accelerate the algorithm dramatically if the Jacobian of $\mathcal{C}$ has real multiplication (see [**30**].

The new algorithm has, for large p, complexity $\widetilde{\mathcal{O}}(\log^5 q)$. This is used to compute a 256-bit prime-order Jacobian, suitable for cryptographic applications, and also the order of a 1024-bit Jacobian.

Hence it is interesting to construct curves of genus 2 with real multiplication. We describe how this can be done by using factors of Jacobians of modular curves. The basic reference is Wang [**71**].

Let N be a positive integer and $X_0(N)$ the modular curve as described in Section 5.1. Let $S_2(N)$ be the space of cusp forms of weight 2 for $\Gamma_0(N)$ and $f = \sum_{n=1}^{\infty} a_n q^n \in S_2(N)$ be a newform. This newform determines a simple abelian variety $\mathcal{A}_f$ which is a factor of $J_0(N) := \operatorname{Jac} X_0(N)$. The knowledge of the newform is equivalent with the knowledge of holomorphic differentials on the factor and this is used by Wang to compute the period matrix of $\mathcal{A}_f$ by computing the complex integrals of a symplectic basis. Moreover, he determined conditions when this period matrix Ω_f corresponds to a principally polarized abelian variety. He did this for factors of dimension ≥ 2 but we focus on the case when this variety has dimension two.

Having found the period matrix one has to construct the curve. We have mentioned this task already in before and cited [**72**].

10.2.1. *Thetanulls.* Once the period matrix Ω_f is determined, one can compute the theta functions. For any genus 2 curve we have six odd theta characteristics and ten even theta characteristics. The following are the sixteen theta characteristics, where the first ten are even and the last six are odd. For simplicity, we denote them by $\theta_i = \begin{bmatrix} a \\ b \end{bmatrix}$ instead of $\theta_i = \begin{bmatrix} a \\ b \end{bmatrix}(z, \tau)$ where $i = 1, \ldots, 10$ for the even theta functions.

$$\theta_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \theta_2 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \theta_3 = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \theta_4 = \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \theta_5 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix},$$
$$\theta_6 = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \theta_7 = \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \theta_8 = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \theta_9 = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \theta_{10} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix},$$

and the odd theta functions correspond to the following characteristics

$$\begin{bmatrix} 0 & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix}, \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} \end{bmatrix}$$

We call fundamental theta constants θ_1, θ_2, θ_3, θ_4. All the other theta constants can be expressed in terms of these four; see [**59**] for details. The classical result of Picard determines the relation between theta characteristics and branch points of a genus two curve.

LEMMA 18 (Picard). *Let a genus 2 curve be given by*

$$Y^2 = X(X-1)(X-\lambda)(X-\mu)(X-\nu). \tag{17}$$

Then, λ, μ, ν can be written as follows:

$$\lambda = \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}, \quad \mu = \frac{\theta_3^2\theta_8^2}{\theta_4^2\theta_{10}^2}, \quad \nu = \frac{\theta_1^2\theta_8^2}{\theta_2^2\theta_{10}^2}. \tag{18}$$

Such branch points were expressed in terms of the fundamental theta constants.

LEMMA 19 ([**59**]). *Every genus 2 curve $\mathcal{X}$ can be written in the form:*

$$y^2 = x\,(x-1)\left(x - \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\right)\left(x^2 - \frac{\theta_2^2\,\theta_3^2 + \theta_1^2\,\theta_4^2}{\theta_2^2\,\theta_4^2}\cdot\alpha\,x + \frac{\theta_1^2\theta_3^2}{\theta_2^2\theta_4^2}\,\alpha^2\right),$$

where $\alpha = \frac{\theta_8^2}{\theta_{10}^2}$ and in terms of $\theta_1, \ldots, \theta_4$ is given by

$$\alpha^2 + \frac{\theta_1^4 + \theta_2^4 - \theta_3^4 - \theta_4^4}{\theta_1^2\theta_2^2 - \theta_3^2\theta_4^2}\,\alpha + 1 = 0$$

Furthermore, if $\alpha = \pm 1$ then $V_4 \hookrightarrow \mathrm{Aut}(\mathcal{X})$.

From the above we have that $\theta_8^4 = \theta_{10}^4$ implies that $V_4 \hookrightarrow \mathrm{Aut}(\mathcal{X})$. in [**59**, Lemma 15] determines a necessary and equivalent statement when $V_4 \hookrightarrow \mathrm{Aut}(\mathcal{X})$ in terms of thetanulls.

The last part of the lemma above shows that if $\theta_8^4 = \theta_{10}^4$ then all coefficients of the genus 2 curve are given as rational functions of powers of these 4 fundamental theta functions. Such fundamental theta functions determine the field of moduli of the given curve. Hence, the curve is defined over its field of moduli.

Once the fundamental thetanulls are computed, the arithmetic invariants J_2, J_4, J_6, J_{10} can be computed via formulas given in [**36**].

Till now the computations were made over $\mathbb{R}$ with large enough precision. Now we use the $\mathbb{Z}$-structure of $X_0(N)$ to identify the invariants with integers. Reducing modulo primes one finds invariants of curves defined over finite fields. Then by [**51**] we compute an equation of the genus 2 curves over a minimal field of definition for these invariants and so over a finite field.

REMARK 10. *In* [**71**] *there are used absolute invariants instead of the above arithmetic invariants. Moreover, the case of curves with automorphism group of order > 2 doesn't seem to have been considered. Nevertheless, it seems as this was not a problem for $N \leq 200$, which seems to suggest that no such genus two curves appear for such N.*

10.3. CM curves. We further specialize and want to use curves of genus 2 whose Jacobian has complex multiplication. We shall use class field theory and the theory of Taniyama-Shimura of CM-fields to find such curves over number fields.By reduction we find curves with CM over finite fields, and again class field theory of CM-fields reduces point counting modulo p to the computation of the trace of an element in the CM-field with norm p.

Choose a squarefree integer $d \in \mathbb{N}$ such that $K_0 := \mathbb{Q}(\sqrt{d})$ has class number one. Let $\alpha = a + b\sqrt{d}$ be squarefree and $\alpha > 0$. Thus $K = K_0(i\sqrt{\alpha})$ is a CM field of degree 4. We choose d and α such that $K/\mathbb{Q}$ is Galois with group V_4 (i.e. Klein four-group). Since $[K : \mathbb{Q}] = 4$ and K is CM field we have four distinct embeddings φ_i, $i = 1, \ldots, 4$ of K into $\mathbb{C}$. A tuple $(K, \Phi) = (K, \{\varphi_1, \varphi_2\})$ is called CM-type. For an ideal $I \subset \mathcal{O}_K$ we define

$$\Phi(I) = \{(\varphi_1(x), \varphi_2(x))^t, x \in I\}.$$

Then $\mathbb{C}^2/\Phi(I)$ is an Abelian variety with complex multiplication by $\mathcal{O}_K$. Conversely every abelian variety $\mathcal{A}$ of CM-type (K,Φ) with complex multiplication by $\mathcal{O}_K$ is isomorphic to an abelian variety $\mathcal{A}_{I,\Phi}$; see Shimura-Taniyama (1961) [**64**].

The period matrix of $\mathcal{A}_{I,\Phi}$ lies in the Siegel upper half plane $\mathbb{H}_2$ and therefore we can equip $\mathcal{A}_{I,\Phi}$ with a principal polarization determined by an element $\gamma \in K$.

10.3.1. *Class polynomials.* For elliptic curves with complex multiplication by $\mathcal{O}_K$ the j-invariant lies in the Hilbert class field of the imaginary quadratic field K. The case of $g = 1$ is simpler due to the fact that the *reflex CM-field* $\hat{K}$ is equal to K (see [**63**]), which is not true for higher genus. The following is mostly due to A. Weng [**74**].

THEOREM 40. *Let K be a CM-field such that $[K:\mathbb{Q}] = 4$.*

i) *For every genus 2 curve $\mathcal{C}$ with CM-type by $\mathcal{O}_K$, the absolute invariants $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are algebraic numbers that lie in a class field over the reflex CM-field $\hat{K}$.*

ii) *For two genus 2 curves $\mathcal{C}$ and $\mathcal{C}'$ with CM with $\mathcal{O}_K$ we have that $\mathbf{x}_i(\mathcal{C})$ and $\mathbf{x}_i(\mathcal{C}')$, for $i = 1,2,3$, are Galois conjugates.*

iii) *Let $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_s\}$ be a set of representatives of isomorphism classes of genus 2 curves whose Jacobians have CM with endomorphism ring $\mathcal{O}_K$. Denote by $\mathbf{x}_i^{(j)}$, the i-th absolute invariant of $\mathcal{C}_j$. The polynomials*

$$H_{K,i}(X) := \prod_{j=1}^{s} (X - \mathbf{x}_i^{(j)}),$$

for $i = 1,2,3$, have coefficients in $\mathbb{Q}$.

Polynomials $H_{K,1}$, $H_{K,2}$, $H_{K,3}$, are called the **class polynomials**.

THEOREM 41. *Let K be a CM-field of degree 4 and $p \geq 7$ a prime which does not divide the denominators of the class polynomials $H_i(X) := H_{K,i}(X)$, $i = 1,2,3$. Then the following hold:*

- *For all $w \in \mathcal{O}_K$ with $w\bar{w} = p$, $H_i(X)$ have a linear factor over $\mathbb{F}_p$ corresponding to w.*
- *For each $\alpha \in \mathbb{F}_p$ there are two $\mathbb{F}_p$-isomorphism classes $\mathcal{A}_{p,1}$ and $\mathcal{A}_{p,2}$ of principally polarized abelian varieties over $\mathbb{F}_p$ with absolute invariants $\mathbf{x}_i = \alpha$, for $i = 1,2,3$.*
- *The principally polarized abelian varieties $\mathcal{A}_{p,1}$ and $\mathcal{A}_{p,2}$ have CM by $\mathcal{O}_K$.*
- *The number of $\mathbb{F}_p$-rational points of $\mathcal{A}_{p,j}$, $j = 1,2$, is given by*

$$\prod_{r=1}^{4} \left(1 + (-1)^j w_r\right)$$

- *The equation $w\bar{w} = p$ for $w \in \mathcal{O}_K$ has (up to conjugacy and sign) at most two different solutions. Hence, for every CM-field of degree 4 there are at most four different possible orders of groups of $\mathbb{F}_p$-rational points of principally polarized abelian varieties defined over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$.*

Once we compute the class polynomials $H_{K,i}$ we can reduce them module p (for large enough p) and get $H_{K,i}(X) \mod p$. The roots of $H_{K,i}(X) \mod p$ are the absolute invariants of genus 2 curves $\mathcal{C}$ modulo p. Now that we know invariants of the curve we can determine its equation as in [**51**]. Then the reduced curve is defined over $\mathbb{F}_p$ or a quadratic extension.

For example, if we are in the first case of the above theorem, say we find elements $w_1, \bar{w}_1 \in \mathcal{O}_K$ such that $w_1\bar{w}_1 = p$ then there exists at most one second solution (up to conjugation) such that $w_2\bar{w}_2 = p$. We set $W := \{\pm w_1, \pm w_2\}$. Then the order of $\mathrm{Jac}(\mathcal{C} \mod p)$, over $\mathbb{F}_p$, is $\{\chi_w(1) \mid w \in W\}$, where $\chi_w(T)$ is the characteristic polynomial of w.

By using the CM-method for curves of genus 2 one gets a very efficient way to construct cryptographically strong DL-systems as extensive tables have shown in the thesis of A. Weng.

One could hope to use these results not only for DL-systems but also for isogeny graphs of Jacobians of dimension 2 and it could be worthwhile to investigate whether they could be used in the way we shall see in Section 11 below.

11. Elliptic curve cryptography

Finally we come to the most interesting and well-understood case. We shall use isogenies between elliptic curves and their computation quite often, and so we begin, for the convenience of the reader, with a fundamental result of J. Vélu; see [**70**].

PROPOSITION 10 (Vélu's formula). *Let E be an elliptic curve, defined over a field k, with equation*

$$E : y^2 = x^3 + ax + b$$

and $G \subset E(\bar{k})$ be a finite subgroup invariant under G_k. The separable isogeny $\phi : E \to E/G$, of kernel G, can be written as follows:

For any $P(x, y)$ we get

$$\phi(P) = \left(x + \sum_{Q \in G \setminus \{\mathcal{O}\}} x(P+Q) - x(Q),\ y + \sum_{Q \in G \setminus \{\mathcal{O}\}} y(P+Q) - y(Q) \right) \tag{19}$$

and the curve E/G has equation $y^2 = x^3 + a'x + b'$, where

$$a' = a - 5 \sum_{Q \in G \setminus \{\mathcal{O}\}} (3x(Q)^2 + a),$$

$$b' = b - 7 \sum_{Q \in G \setminus \{\mathcal{O}\}} (5x(Q)^3 + 3ax(Q) + b).$$

Thus, knowing a finite subgroup G of E we can explicitly construct the corresponding isogeny $E \to E' := E/G$.

11.1. Endomorphism ring of E. The following results are mostly due to **M. Deuring** and mainly contained in the beautiful paper [**15**].

DEFINITION 42. Let $\mathcal{E}$ be an elliptic curve over k. $\mathcal{E}$ is ordinary if and only if $\mathrm{End}(\mathcal{E})$ is commutative. $\mathcal{E}$ is supersingular if and only if $\mathrm{End}(\mathcal{E})$ is not commutative.

THEOREM 43 (Deuring). *Let $\mathcal{E}$ be an elliptic curve defined over a field k. The following hold:*

i) *If* $\mathrm{char(k)} = 0$, *then $\mathcal{E}$ 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 k-isomorphism 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 $\tilde{\mathcal{E}}$ with CM over a number field K such that*

- *there is a prime $\mathfrak{p}$ of K with $\tilde{\mathcal{E}}_{\mathfrak{p}} \cong \mathcal{E}$ with $\tilde{\mathcal{E}}_{\mathfrak{p}}$ the reduction of $\tilde{\mathcal{E}}$ modulo $\mathfrak{p}$, and*
- $\mathrm{End}(\tilde{\mathcal{E}}) = \mathrm{End}(\mathcal{E})_{\mathfrak{p}} = O_{\mathcal{E}}$*, 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.*

We remark that the endomorphism ring of an elliptic curve over a finite field $\mathbb{F}_q$ is 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 12 (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 field 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 13. $|n_{\mathbb{F}_q,\mathcal{E}} - q - 1| < 2\sqrt{q}$.

Using the result iii) in Thm. 43 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 Hasse-Weil bound for points on Jacobian varieties over finite fields (Thm. 12).

11.2. Point counting. Corollary 13 is the key fact for a polynomial time algorithm for computing the order of $\mathcal{E}(\mathbb{F}_q)$ for elliptic curves $\mathcal{E}$ defined over the field $\mathbb{F}_q$, 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 the 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.

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 (see Section 5) that we can interpret these isogenies with the help of points on an explicitly known curve, namely the modular curve $X_0(n)$. An explicit equation for an affine model of $X_0(N)$ is given by the classical modular polynomial $\phi(j, j_N)$. It allows an effective computation of isogenies (as functions including the determination of the image curve) at least if n is of moderate size).

THEOREM 44 (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*

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

The **Idea of Atkin-Elkies** is: Use *étale isogenies* of small degree of $\mathcal{E}$ instead of points, and use the modular polynomial ϕ_n of degree $\sim n$. The resulting *Schoof-Atkin-Elkies algorithm* is very fast, in particular if one assumes as "standard conjecture" the generalized Riemann hypothesis (GRH).

COROLLARY 14 (SAE). *$|\mathcal{E}(\mathbb{F}_q)|$ 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 $|\mathcal{E}(\mathbb{F}_p)| = k \cdot \ell$ 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).*

11.3. Looking for post-quantum security. As we have seen in Section 11.2 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. We shall discuss now how we can use isogenies of elliptic curves (and maybe, of curves of larger genus with convenient endomorphism rings) to find key exchange schemes staying in the frame of Diffie-Hellman type protocols as described in Section 6.

11.3.1. *The isogeny graph.*

DEFINITION 45. Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$. The **isogeny graph** of $\mathcal{E}$ is a graph where nodes are j-invariants of elliptic curves isogenous to $\mathcal{E}$ and edges are isogenies between the curves attached to the nodes.

For some applications one restricts the degree of the isogenies defining edges. Isogeny graphs of ordinary elliptic curves are discussed by using the lifting theorem of Deuring, identifying these graphs with graphs coming from ideal classes of orders in imaginary quadratic fields , and then using analytic number theory and properties of modular forms. The study of graphs of supersingular elliptic curves uses properties of maximal orders of quaternion algebras. In both cases one gets the following result due to D. Jao, S. D. Miller and R. Vekatesan [**12**, Prop. 2.1].

THEOREM 46. *The isogeny graph of $\mathcal{E}$ is a Ramanujan graph.*

A first application, also to be found in [**12**] is the following:

COROLLARY 15. *Assume the $\mathcal{E}, \mathcal{E}'$ are elliptic curves over $\mathbb{F}_q$ with $\mathrm{End}(\mathcal{E}) = \mathrm{End}(\mathcal{E}') = \mathcal{O}$. Then there exists a subexponential algorithm which relates the DLP in $\mathcal{E}(\mathbb{F}_q)$ to the DLP in $\mathcal{E}'(\mathbb{F}_q)$.*

Hence we cannot weaken the DLP by applying isogenies between elliptic curves with the same order.

11.3.2. *The system of Couveignes-Stolbunov.* A second application of isogeny graphs is constructive. We sketch in the following work of Stolbunov [**68**] and Couveignes [**9**]. We use the results of Thm. 43 for an ordinary elliptic curve $\mathcal{E}_0$ over $\mathbb{F}_q$ with ring of endomorphism $\mathrm{End}(\mathcal{E}_0) = O$, which is an order in a quadratic imaginary field.

In analogy to the notation Theorem 43 define $\mathcal{S}_{E_0}$ as 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. Hence, we can use it for *Key Exchange protocols* as in Section 6: *The partner P chooses* $c \in \mathrm{Pic}(O)$ *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 since one finds enough isogenies that are composites of isogenies of small degree (smoothness); for an example see [**68**]. The **security** depends on the hardness of the following problem:

Problem 1. *Find an isogeny between two given isogenous elliptic curves.*

The following gives an idea of the running time for the solution to this problem.

Proposition 11 (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*

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

But recall: We are in the situation where 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 in the Q-bit world for the key exchange scheme; see results of Childs, Jao, Soukharev in [**6**]. Comparing this with the situation we have nowadays with respect to the widely tolerated RSA-system this may be not so disastrous.

11.3.3. *The key exchange system of De Feo.* The suggestion is to use supersingular elliptic curves over $\mathbb{F}_{p^2}$ and their properties also stated in Thm. 43. Take

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

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

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

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 [**12**] in the frame we have introduced in Section 6.

The objects in the categories $\mathcal{C}_i \quad (i = 1, 2)$ have as **objects** the isomorphism classes of supersingular curves E over $\mathbb{F}_{p^2}$ isogenous to $\mathcal{E}_0$ and hence with

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

The **morphisms in** $\mathcal{C}_1$ are isogenies φ with $|\ker(\varphi)|$ dividing r^a.

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 $\mathcal{P}_1$ chooses $n_1, n_2 \in \mathbb{Z}/r^a$ and the isogeny
$$\eta : \mathcal{E}_0 \to \mathcal{E}_0/\langle n_1 P_1 + n_2 P_2\rangle =: \mathcal{E}_1.$$
- The Partner $\mathcal{P}_2$ chooses $m_1, m_2 \in \mathbb{Z}/s^b$ and computes the isogeny
$$\psi : \mathcal{E}_0 \to \mathcal{E}_0/\langle m_1 Q_1 + m_2 Q_2\rangle =: \mathcal{E}_2.$$
- $\mathcal{P}_2$ sends $(\mathcal{E}_2, \psi(P_1), \psi(P_2))$.
- $\mathcal{P}_1$ can compute the common secret, the pushout of η and ψ as
$$\mathcal{E}_3 := \mathcal{E}_2/\langle n_1\psi(P_1) + n_2\psi(P_2)\rangle.$$

An analogous procedure enables $\mathcal{P}_2$ to compute the isomorphy class of $\mathcal{E}_3$, which is the common secret of the partners.

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.

References

[1] Pierre-Jean Abelard Simon ; Gaudry Pierrick; Spaenlehauer, *Improved complexity bounds for counting points on hyperelliptic curves*, Foundations of Computational Mathematics (2018), to appear.

[2] L. Beshaj and S. Guest, *Weighted projective space of binary sextics*, Algebraic curves and cryptography, 2018.

[3] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, *Genus-2 curves and jacobians with a given number of points* (2014), available at `1403.6911`.

[4] Reinier Bröker and Kristin Lauter, *Modular polynomials for genus 2*, LMS J. Comput. Math. **12** (2009), 326–339, DOI 10.1112/S1461157000001546. MR2570930

[5] Gabriel Cardona and Jordi Quer, *Field of moduli and field of definition for curves of genus 2*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83, DOI 10.1142/9789812701640_0006. MR2181874

[6] Andrew Childs, David Jao, and Vladimir Soukharev, *Constructing elliptic curve isogenies in quantum subexponential time*, J. Math. Cryptol. **8** (2014), no. 1, 1–29, DOI 10.1515/jmc-2012-0016. MR3163097

[7] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. MR2162716

[8] Marc Coppens and Gerriet Martens, *Linear series on 4-gonal curves*, Math. Nachr. **213** (2000), 35–55, DOI 10.1002/(SICI)1522-2616(200005)213:1⟨35::AID-MANA35⟩3.3.CO;2-Q. MR1755245

[9] Jean-Marc Couveignes, *Hard homogeneous spaces*, 2006. Cryptology e-Print Arxive.

[10] Luca De Feo, *Fast algorithms for computing isogenies between ordinary elliptic curves in small characteristic*, J. Number Theory **131** (2011), no. 5, 873–893, DOI 10.1016/j.jnt.2010.07.003. MR2772477

[11] Luca De Feo, Cyril Hugounenq, Jérôme Plût, and Éric Schost, *Explicit isogenies in quadratic time in any characteristic*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 267–282, DOI 10.1112/S146115701600036X. MR3540960

[12] Luca De Feo, David Jao, and Jérôme Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, J. Math. Cryptol. **8** (2014), no. 3, 209–247, DOI 10.1515/jmc-2012-0015. MR3259113

[13] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109. MR0262240

[14] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques* (French), Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349. MR0337993

[15] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper* (German), Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272, DOI 10.1007/BF02940746. MR0005125

[16] C. Diem, *On arithmetic and the discrete logarithm problem in class groups of curves*, Ph.D. Thesis, 2008. Habilitationsschrift.

[17] Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory **IT-22** (1976), no. 6, 644–654, DOI 10.1109/tit.1976.1055638. MR0437208

[18] Ron Donagi and Ron Livné, *The arithmetic-geometric mean and isogenies for curves of higher genus*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **28** (1999), no. 2, 323–339. MR1736231

[19] Andreas Enge and Pierrick Gaudry, *A general framework for subexponential discrete logarithm algorithms*, Acta Arith. **102** (2002), no. 1, 83–103, DOI 10.4064/aa102-1-6. MR1884958

[20] Stéphane Flon, Roger Oyono, and Christophe Ritzenthaler, *Fast addition on non-hyperelliptic genus 3 curves*, Algebraic geometry and its applications, 2008, pp. 1–28. MR2484046

[21] Gerhard Frey, *Isogenies in theory and praxis*, Open problems in mathematics and computational science, Springer, Cham, 2014, pp. 37–68. MR3330877

[22] Gerhard Frey and Ernst Kani, *Correspondences on hyperelliptic curves and applications to the discrete logarithm*, 2011, pp. 1–19.

[23] Gerhard Frey and Ernst Kani, *Normal forms of hyperelliptic curves of genus 3*, Des. Codes Cryptogr. **77** (2015), no. 2-3, 677–712, DOI 10.1007/s10623-015-0122-2. MR3403171

[24] P. Gaudry, *Fast genus 2 arithmetic based on theta functions*, J. Math. Cryptol. **1** (2007), no. 3, 243–265, DOI 10.1515/JMC.2007.012. MR2372155

[25] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, J. Cryptology **15** (2002), no. 1, 19–46, DOI 10.1007/s00145-001-0011-x. MR1880933

[26] Pierrick Gaudry, David Kohel, and Benjamin Smith, *Counting points on genus 2 curves with real multiplication*, Advances in cryptology—ASIACRYPT 2011, Lecture Notes in Comput. Sci., vol. 7073, Springer, Heidelberg, 2011, pp. 504–519, DOI 10.1007/978-3-642-25385-0_27. MR2935020

[27] P. Gaudry and É. Schost, *Modular equations for hyperelliptic curves*, Math. Comp. **74** (2005), no. 249, 429–454, DOI 10.1090/S0025-5718-04-01682-5. MR2085901

[28] P. Gaudry, E. Thomé, N. Thériault, and C. Diem, *A double large prime variation for small genus hyperelliptic index calculus*, Math. Comp. **76** (2007), no. 257, 475–492, DOI 10.1090/S0025-5718-06-01900-4. MR2261032

[29] Pierrick Gaudry and Robert Harley, *Counting points on hyperelliptic curves over finite fields*, Algorithmic number theory (Leiden, 2000), 2000, pp. 313–332. MR1850614

[30] Pierrick Gaudry, David Kohel, and Benjamin Smith, *Counting points on genus 2 curves with real multiplication*, Advances in cryptology—ASIACRYPT 2011, Lecture Notes in Comput. Sci., vol. 7073, Springer, Heidelberg, 2011, pp. 504–519, DOI 10.1007/978-3-642-25385-0_27. MR2935020

[31] Pierrick Gaudry and David Lubicz, *The arithmetic of characteristic 2 Kummer surfaces and of elliptic Kummer lines*, Finite Fields Appl. **15** (2009), no. 2, 246–260, DOI 10.1016/j.ffa.2008.12.006. MR2494393

[32] Pierrick Gaudry and Éric Schost, *Genus 2 point counting over prime fields*, J. Symbolic Comput. **47** (2012), no. 4, 368–400, DOI 10.1016/j.jsc.2011.09.003. MR2890878

[33] Ki-ichiro Hashimoto and Naoki Murabayashi, *Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two*, Tohoku Math. J. (2) **47** (1995), no. 2, 271–296, DOI 10.2748/tmj/1178225596. MR1329525

[34] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445, DOI 10.1006/jsco.2001.0513. MR1890579

[35] Jun-ichi Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. (2) **72** (1960), 612–649, DOI 10.2307/1970233. MR0114819

[36] Jun-ichi Igusa, *On Siegel modular forms of genus two*, Amer. J. Math. **84** (1962), 175–200, DOI 10.2307/2372812. MR0141643

[37] Antoine Joux, Andrew Odlyzko, and Cécile Pierrot, *The past, evolving present, and future of the discrete logarithm*, Open problems in mathematics and computational science, Springer, Cham, 2014, pp. 5–36. MR3330876

[38] Naoki Kanayama, *Division polynomials and multiplication formulae of Jacobian varieties of dimension 2*, Math. Proc. Cambridge Philos. Soc. **139** (2005), no. 3, 399–409, DOI 10.1017/S0305004105008765. MR2177167

[39] Naoki Kanayama, *Corrections to "Division polynomials and multiplication formulae in dimension 2" [MR2177167]*, Math. Proc. Cambridge Philos. Soc. **149** (2010), no. 1, 189–192, DOI 10.1017/S0305004110000113. MR2651585

[40] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985. MR772569

[41] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586, DOI 10.1007/s00222-009-0206-6. MR2551764

[42] Mark Kisin, *Modularity of 2-adic Barsotti-Tate representations*, Invent. Math. **178** (2009), no. 3, 587–634, DOI 10.1007/s00222-009-0207-5. MR2551765

[43] M. Kraitchik, *Introduction à la théorie des nombres* (French), Gauthier-Villars, Paris, 1952. MR0051845

[44] Greg Kuperberg, *A subexponential-time quantum algorithm for the dihedral hidden subgroup problem*, SIAM J. Comput. **35** (2005), no. 1, 170–188, DOI 10.1137/S0097539703436345. MR2178804

[45] Serge Lang, *Abelian varieties*, Springer-Verlag, New York-Berlin, 1983. Reprint of the 1959 original. MR713430

[46] Frank Leitenberger, *About the group law for the Jacobi variety of a hyperelliptic curve*, Beiträge Algebra Geom. **46** (2005), no. 1, 125–130. MR2146447

[47] Davide Lombardo, *Computing the geometric endomorphism ring of a genus-2 Jacobian*, Math. Comp. **88** (2019), no. 316, 889–929, DOI 10.1090/mcom/3358. MR3882288

[48] David Lubicz and Damien Robert, *Computing isogenies between abelian varieties*, Compos. Math. **148** (2012), no. 5, 1483–1515, DOI 10.1112/S0010437X12000243. MR2982438

[49] David Lubicz and Damien Robert, *Computing separable isogenies in quasi-optimal time*, LMS J. Comput. Math. **18** (2015), no. 1, 198–216, DOI 10.1112/S146115701400045X. MR3349315

[50] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein, *The locus of curves with prescribed automorphism group*, Sūrikaisekikenkyūsho Kōkyūroku **1267** (2002), 112–141. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). MR1954371

[51] Andreas Malmendier and Tony Shaska, *A universal genus-two curve from Siegel modular forms*, SIGMA Symmetry Integrability Geom. Methods Appl. **13** (2017), Paper No. 089, 17, DOI 10.3842/SIGMA.2017.089. MR3731039

[52] J. Mandili and T. Shaska, *Computation of heights on weighted projective spaces*, Algebraic curves and cryptography, 2018.

[53] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[54] Loï c Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations, 1994, pp. 59–94. MR1322319

[55] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules* (French), Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334. MR1106431

[56] David Mumford, *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, 2008. With appendices by C. P. Ramanujam and Yuri Manin; Corrected reprint of the second (1974) edition. MR2514037

[57] Yoshihiro Ônishi, *Determinant expressions for hyperelliptic functions*, Proc. Edinb. Math. Soc. (2) **48** (2005), no. 3, 705–742, DOI 10.1017/S0013091503000695. With an appendix by Shigeki Matsutani. MR2171194

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

[59] E. Previato, T. Shaska, and G. S. Wijesiri, *Thetanulls of cyclic curves of small genus*, Albanian J. Math. **1** (2007), no. 4, 253–270. MR2367218

[60] Oded Regev, *New lattice-based cryptographic constructions*, J. ACM **51** (2004), no. 6, 899–942, DOI 10.1145/1039488.1039490. MR2145258

[61] Tanush Shaska and Jennifer L. Thompson, *On the generic curve of genus 3*, Affine algebraic geometry, Contemp. Math., vol. 369, Amer. Math. Soc., Providence, RI, 2005, pp. 233–243, DOI 10.1090/conm/369/06814. MR2126664

[62] Tony Shaska, *Genus 2 curves with* $(3,3)$*-split Jacobian and large automorphism group*, Algorithmic number theory (Sydney, 2002), 2002, pp. 205–218. MR2041085

[63] Goro Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton Mathematical Series, vol. 46, Princeton University Press, Princeton, NJ, 1998. MR1492449

[64] Goro Shimura and Yutaka Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Publications of the Mathematical Society of Japan, vol. 6, The Mathematical Society of Japan, Tokyo, 1961. MR0125113

[65] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original. MR1329092

[66] Benjamin Smith, *Computing low-degree isogenies in genus 2 with the Dolgachev-Lehavi method*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 159–170, DOI 10.1090/conm/574/11418. MR2961408

[67] Henning Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009. MR2464941

[68] Anton Stolbunov, *Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves*, Adv. Math. Commun. **4** (2010), no. 2, 215–235, DOI 10.3934/amc.2010.4.215. MR2654134

[69] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144, DOI 10.1007/BF01404549. MR0206004

[70] Jacques Vélu, *Isogénies entre courbes elliptiques* (French), C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241. MR0294345

[71] Xiang Dong Wang, 2*-dimensional simple factors of* $J_0(N)$, Manuscripta Math. **87** (1995), no. 2, 179–197, DOI 10.1007/BF02570470. MR1334940

[72] Hermann-Josef Weber, *Hyperelliptic simple factors of* $J_0(N)$ *with dimension at least* 3, Experiment. Math. **6** (1997), no. 4, 273–287. MR1606908

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

[74] Annegret Weng, *Constructing hyperelliptic curves of genus 2 suitable for cryptography*, Math. Comp. **72** (2003), no. 241, 435–458, DOI 10.1090/S0025-5718-02-01422-9. MR1933830

[75] Yuri G. Zarhin, *Families of absolutely simple hyperelliptic Jacobians*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 1, 24–54, DOI 10.1112/plms/pdp020. MR2578467

[76] Yuri G. Zarhin, *Endomorphism algebras of superelliptic Jacobians*, Geometric methods in algebra and number theory, Progr. Math., vol. 235, Birkhäuser Boston, Boston, MA, 2005, pp. 339–362, DOI 10.1007/0-8176-4417-2_15. MR2166091

Institut für Experimentelle Mathematik, Universität Duisburg-Essen, 45326 Essen, Germany

Email address: frey@iem.uni-due.de

Department of Mathematics and Statistics, Oakland University, Rochester, Michigan 48309

Email address: shaska@oakland.edu