On Galois Representations in Theory and Praxis

SAGA Seminar
AMU Poznan
April 17/18 th, 2018

Gerhard Frey
University of Duisburg-Essen
gerhard.frey@gmail.com

1 Many Questions and Some Answers

A usual feature in the life of a mathematician is:
Someone, it may be a layman or a colleague, is asking a
(simple) question.
And very often, the embarrassing result is that one cannot give an answer.

Questions about **diophantine** problems are notorious for this feature, and for 350 years the most prominent example was

Fermat's Conjecture (**FLT**)

$$X^p + Y^p = 1$$

has only two solutions over the field of rational number $\mathbb{Q}$ if p is a prime > 2.

It is not clear why this specific claim became so important for number theory. For instance, it is reported that **C.F. Gauß** (after having tried to get results) said that he could state a problem as interesting as Fermat's claim every week.
He was wright in one sense, namely the importance of FLT as mathematical statement is not overwhelming.

But he was wrong in a deeper sense: It turned out that FLT was a wonderful testbed and triggered new theories like **Algebraic Number Theory**.

FERMAT

1.1 Some Answers

This gives a hint for strategies to answer questions:
Look for structural reasons why it can be true (or wrong), and then use these structures.
We know:

1. $$Y^2 = X^3 + 1$$

   has only finitely many points with coordinates in $\mathbb{Z}$.(**Siegel-Mahler**)

2. $$Y^2 = X^6 + 1$$

   has only finitely many points with coordinates in $\mathbb{Q}$ (**Faltings**)

3. $$X^p + Y^p = 1$$

   has, for $p > 2$ only two points with coordinates in $\mathbb{Q}$ (**Taylor–Wiles**)

4. The ***projective*** **curve**

   $$Y^2 Z = X^3 + A \cdot XZ^2 + B \cdot Z^3$$

   with

   $$\mathbf{A} = 7D5A0975FC2C3057EEF67530417AFFE$$
   $$7FB8055C126DC5C6CE94A4B44F330B5D9$$

   and

   $$\mathbf{B} \ = 26DC5C6CE94A4B44F330B5D9BBD77C$$
   $$BF958416295CF7E1CE6BCCDC18FF8C07B6$$

   has *modulo*

   $$\mathbf{p} = A9FB57DBA1EEA9BC3E660A909D838D7$$
   $$26E3BF623D52620282013481D1F6E5377$$

   exactly

   $$q = A9FB57DBA1EEA9BC3E660A909D838D7$$
   $$18C397AA3B561A6F7901E0E82974856A7$$

   points. p, q are numbers with 256 bits, i.e. $\approx$ 80 decimals, and are given in the hexadecimal system. We come nearer to the structural background by the

5. **Conjecture of Serre**($\sim$ 1986), which is now the

   Theorem 1.1 *(**Khare-Wintenberger-Kisin** ($\sim$ 2006)):*
   Odd two-dimensional irreducible (continuous) $\mathbb{F}_q$-representations ρ of the automorphism group $G_{\mathbb{Q}}$ of the algebraic numbers $\bar{\mathbb{Q}}$ are given by its operation on points of finite order of Jacobian varieties of a well-known "classical" family of curves, the modular curves $X_0(N)$.
   In addition, the minimal possible level N and the twist character (" neben type ") are obtained from the arithmetical data of ρ.

[1]

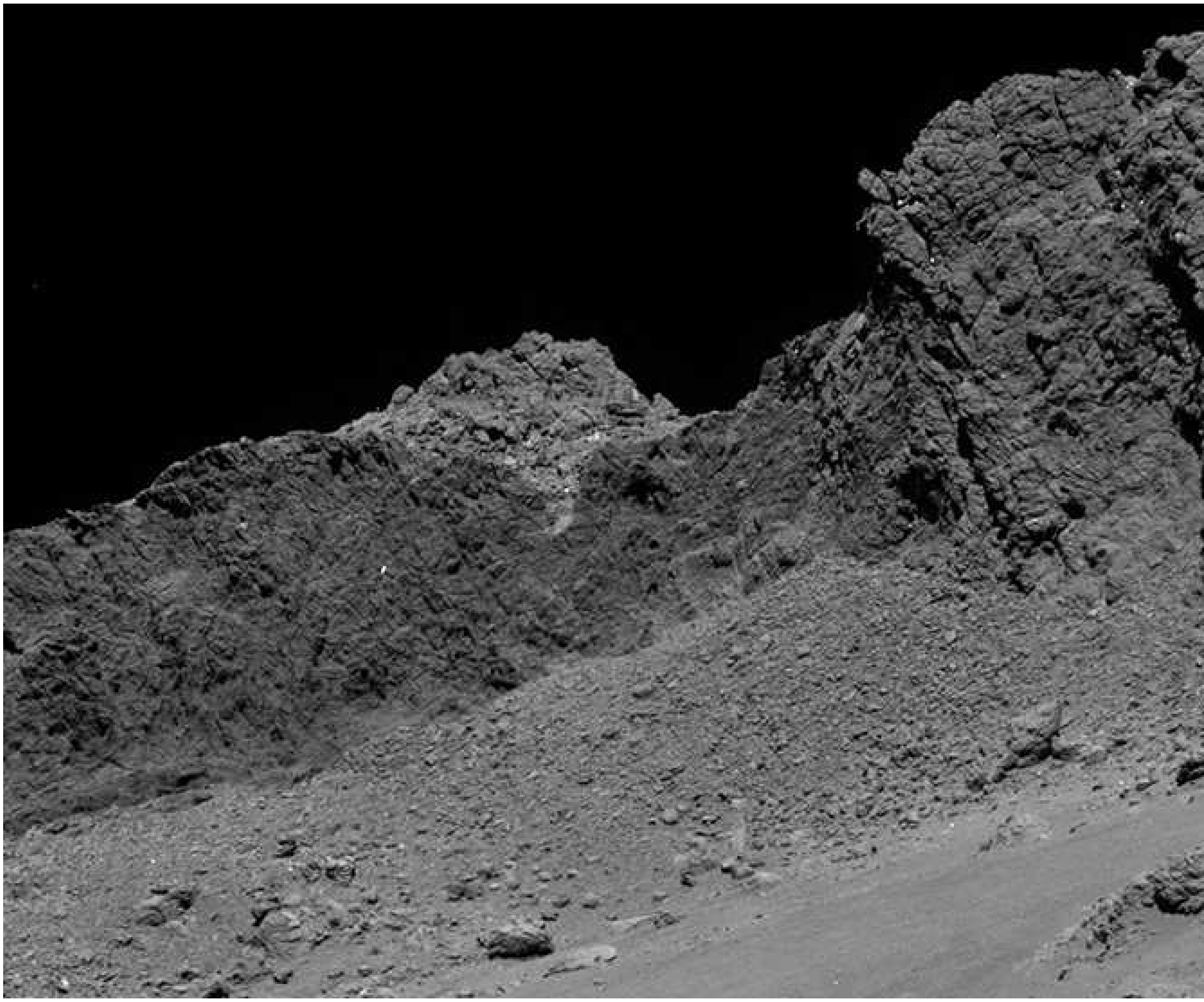
[1] FLT is just a footnote to this theorem.

1.2 So What?

A further experience of mathematicians:
Having answered a question after a long and often painful struggle your neighbor comments:
It is nice that you know now that Fermat was right.
But what it is good for?
G.H.Hardy's in his book : *"A Mathematician's Apology"* stresses the the "uselessness" of number theory and claims that its intrinsic beauty is enough to justify it.

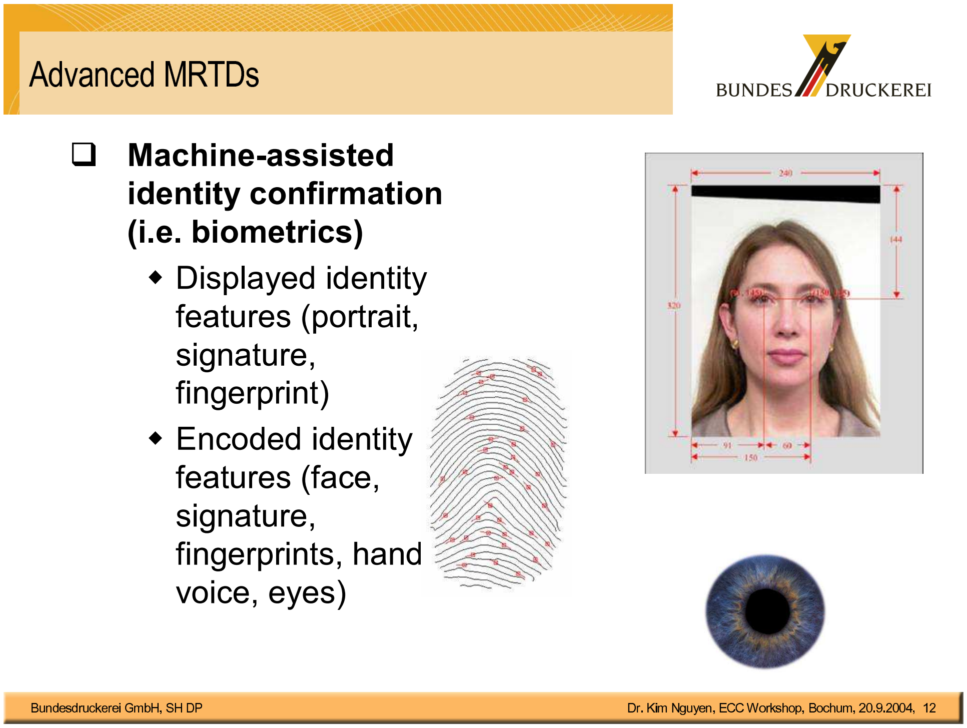
He was wrong about the uselessness:
Because of digitalization number theory plays a prominent role in communication theory and especially in data security.

2 Applications



Rosetta meets Churyumov-Gerasimenko, August 6th, 2014 from: Wikipedia This picture exists because of a first already classical topic application: ***Coding Theory***, which uses either arithmetically defined lattices or, very successfully, vector spaces constructed with curves over finite fields.

In this lecture we shall concentrate on a second topic: ***Cryptographic methods*** that enable to send messages via open channels secure against forging and maintaining privacy.
The result 4.) from above was constructed in this context, for example it is used for the German e-Passport.



Advanced MRTDs

BUNDES DRUCKEREI

- ❑ **Machine-assisted identity confirmation (i.e. biometrics)**
  - Displayed identity features (portrait, signature, fingerprint)
  - Encoded identity features (face, signature, fingerprints, hand voice, eyes)

Bundesdruckerei GmbH, SH DP

Dr. Kim Nguyen, ECC Workshop, Bochum, 20.9.2004, 12

from: Bundesdruckerei

2.1 Public Key Cryptography

We want 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.

2.2 Bits and Q-Bits

The possibility that quantum computing could be realizable in foreseeable time yields new aspects for the discussion of crypto primitives.
We shall describe below systems for which we have good reasons to believe that the bit-complexity is exponential.
But their q-bit complexity is subexponential or even polynomial.
New relations between crypto primitives arise. It seems that in this world the hidden subgroup problem and connected to it, the hidden shift problem related to groups G are central.
Here the state of the art is that for abelian G the problems can be solved in subexponential time and space, for dihedral groups there is "hope".

2.3 Diffie-Hellman Key Exchange

From now on we shall concentrate on the problem to exchange keys in open channels in the spirit of **Diffie-Hellman**. We shall begin with a rather abstract definition of Diffie-Hellman-like schemes.
At the end of the talk we shall discuss systems that could be more resistant against quantum computing and there the abstract setting will be useful.

2.3.1 Pushouts in Categories

Two partners P_1 and P_2 want to share a common secret.
Let $\mathcal{C}_i$; $i = 1, 2$ be two categories with objects $A_j^1 = A_j^2$; $j \in J$ and morphisms $B_{j,k}^i = \mathrm{Mor}^i(A_j, A_k)$ and base object A_0 such that

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

$$(A_l,\ \gamma_1 \in B^1(A_k, A_l),\ \gamma_2 \in B^2(A_j, A_l))$$

   with

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

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

Key Exchange (P_1 chooses φ, P_2 chooses ψ, they send A_j, A_k and $P(\psi)$ respectively $P(\varphi)$ and compute the ***common secret*** A_l.

Security The scheme is broken if the **Diffie-Hellman Computational Problem (DHCP)** is weak: For randomly given A_j, A_k determine A_l, which is the pushout of

$$A_0 \xrightarrow{\varphi} A_j$$

and

$$A_0 \xrightarrow{\psi} A_k.$$

2.3.2 Pushouts by morphisms

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 existing)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 be not uniquely determined by a.

Problem:

1. Find a “genuine” usable instance for the abstract setting!
2. What can one say about quantum computing security?

Example. Let G be a (semi-)group, and A a simple-transitive G-set.
For $g \in G$, define

$$t_g \in End_{set}(A)$$

by

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

Let G_1 be a semi-subgroup of G and $G_2 \subset Z(G_1)$ where $Z(G_1)$ is the centralizer of G_1 in G.
Since

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

we can use (A, G, G_1, G_2) for key exchange.

Hidden Shift Computations of translations t_g on G-sets are typical examples for hidden shifts.
In the example take the

$$f_0 : B_1 \to A \text{ with } f_0(g) = t_g \cdot a_0$$

and

$$f_1 : B_1 \to A \text{ with } f_1(g) = t_g \cdot (t_{g_1} \cdot a_0).$$

One can try to use quantum computer algorithms to determine g_1 and hence to break the key exchange protocol.
In fact, for B_1 abelian and finite there is an algorithm of **Kuperberg**, which solves this task in subexponential time.
We shall see an example of a system for which we can apply this result later on.

2.4 The "Classical" Case

(Totally insecure under QC)
$(C, +)$ is a cyclic group of prime order ℓ with a numeration by which it is embedded into $\mathbb{N}$.
$A \subset \mathbb{N}$ is the set of generators of C.
a_0 is a fixed generator.
Take

$$G_1 = G_2 = (\mathbb{Z}/\ell)^* = N_\ell^* \quad \text{mod } {}^*\ell$$

where N_ℓ^* are the natural numbers prime to ℓ and $t_b(a) = a + a \cdots + a$
(b summands: *Scalar multiplication* in C).
The **Discrete Logarithm** (**DL**) of $a \in A$ relative to the base point a_0 is

$$\log(a) = \min(z \in N_\ell^*;\ t_z(a_0) = a).$$

(A, a_0, N_ℓ^*) is a ***DL-System***. [2]

2.5 Tasks to be Done

In order that we can use (a family of) groups G for crypto systems based on discrete logarithms they have to satisfy three crucial conditions:

1. The elements in G can be stored in a computer in a compact way
(e.g. $O(log(\mid G \mid)$ bits needed)).

2. The group composition is given by an algorithm that is easily and efficiently implemented and very fast.

3. The computation of the DL in G (for random elements) is (to the best of our knowledge) very hard and so infeasible in practice (ideally exponential in $\mid G \mid$), in particular the group order of G has to be a large prime.

[2] **Maurer - Wolf**: Up to *subexponential* (probabilistic) algorithms the crypto primitive determining security of a DL-system is the **Discrete Logarithm.**

3 Arithmetic Geometry

The structural background used today for solving this task is

Arithmetic Geometry

a mathematical discipline that combines

- Algebraic Number Theory
- Algebraic Geometry
- Theory of Functions over $\mathbb{C}$

and culminates in
Modern Galois Theory, i.e. the arithmetical theory of representations of Galois groups.

3.1 Algorithmic Arithmetic Geometry

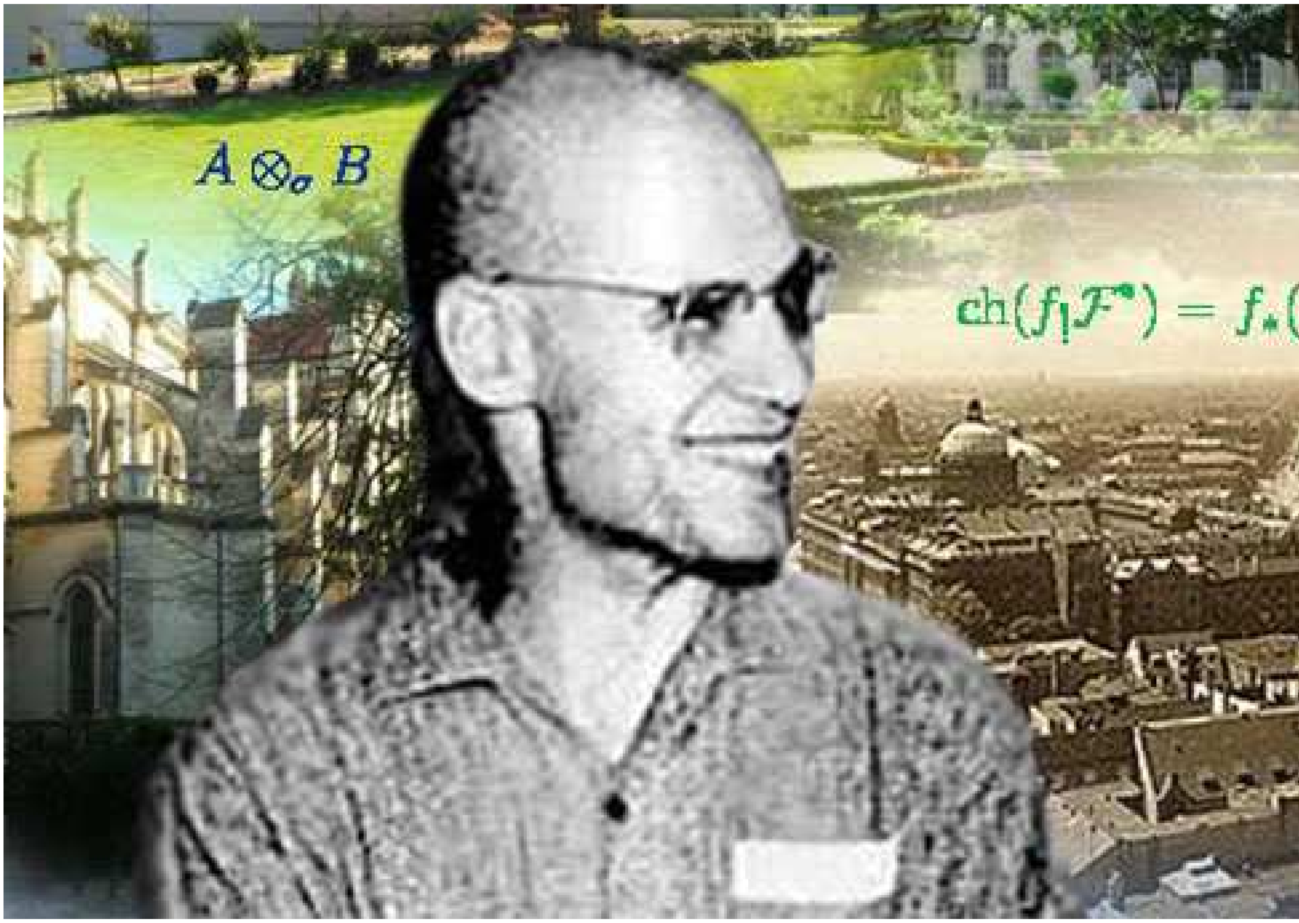
Besides the theoretical side there is a very exciting and rapidly proceeding algorithmic aspect of Arithmetic Geometry
It generalizes considerably both range and techniques of now classical Computational Number Theory

Examples are: Algorithms for modular forms and modular curves and related Galois representations
but of course also: **explicit theory** of varieties over finite fields
as counterpart to explicit theory of algebraic number fields.

3.2 Arithmetical Curves and Surfaces

The analogy between the arithmetic of number fields and function fields of one variable over finite fields has been known at least since the beginning of the twentieth century, and it had a stimulating effect on both topics.

The application of fundamental work of **Alexander Grothendieck** has deepened and widened this analogy enormously.



from: Wikipedia

3.2.1 Curves

Definition 3.1 *A curve is a scheme, such that the stalk in a closed point has Krull dimension 1.*

Arithmetical curves. Take K as number field with integers O_K. $\mathcal{C}_K$ is a ringed space to $\mathrm{Spec}(O_K)$: For finite $S \subset \mathrm{Spec}(O_K)$ and
$U = \mathrm{Spec}(O_K) \setminus S$ define

$$\mathcal{O}(U) := O_S = \{x \in K; x = y/z\}$$

with $z \notin P$ for $P \in U$.
The "function field" field of $\mathcal{C}_K$ is K.
The stalk $\mathcal{O}_P$ at $P \neq 0$ is a valuation ring .
The restriction of $f \in \mathcal{O}_P$ to P is the reduction modulo P.
A prime divisor $\mathfrak{P}$ of K is defined as equivalence class of valuations with ring $\mathcal{O}_P$.
Its degree is $\log(|O_K/P|$.

Geometric projective curves. Let K_0 be a *perfect* field with Galois group $G_{K_0} := \mathrm{Aut}_{K_0}(\overline{K_0})$.
An irreducible *projective* regular curve $\mathcal{C}$ over K_0 is a closed scheme of dimension 1 over $\mathrm{Spec}(K_0)$ embedded in $\mathbb{P}^n/K_0$. For finite $S \subset \mathcal{C}$ define

$$\mathcal{O}(U) := O_S$$

as holomorphic functions outside of S in the function field $K_{\mathcal{C}}$ of $\mathcal{C}$.
Regularity of $\mathcal{C}$ yields that G_{K_0}-orbits in $\mathcal{C}(\overline{K_0})$ correspond one-to-one to equivalence classes of valuations of $K_{\mathcal{C}}$, which are trivial on K_0.
A prime divisor $\mathfrak{P}$ of $\mathcal{C}$ is a Galois orbit of a point $P \in \mathcal{C}(ovK_0)$.
Its degree $\deg(\mathfrak{P})$ is $|\mathfrak{P}|$.

3.2.2 Arithmetical Surfaces

Take $\mathcal{S} = \mathrm{Spec}(O_K)$ where K is a number field. Let $\mathcal{C}_K$ be a projective curve over K.
After having chosen an embedding into a projective space we can extend $\mathcal{C}_K$ to a scheme $\mathcal{C}$ over $\mathcal{S}$.
$\mathcal{C}$ is two-dimensional and hence a *surface* with *fibers* over $\mathrm{Spec}(O_K)$.
The generic fiber is $\mathcal{C}_K$, for maximal ideals $P \subset O_K$ the fiber $\mathcal{C}_P$ is a projective curve over a finite field, the reduction $\mod P$ of $\mathcal{C}$.
This reduction may be neither regular nor irreducible (but connected) (bad reduction).
Hence we can study curves over number fields together with their reductions with the powerful methods of the theory of surfaces (e.g. minimal models, metrics).

3.2.3 Picard Groups of Curves

Let $\mathcal{C}$ be a regular curve.
The divisors group $\mathcal{D}_{\mathcal{C}}$ is the free abelian group generated by the set of prime divisors.
A principal divisor of $f \in K_{\mathcal{C}}^{*}$ is

$$(f) := \sum_{\mathfrak{P} \text{ prime divisor of } \mathcal{C}} v_{\mathfrak{P}}(f) \cdot \mathfrak{P}$$

where $v_{\mathfrak{P}}$ is the normalized valuation in $\mathfrak{P}$.

Definition 3.2

$$\mathrm{Pic}_{\mathcal{C}} := \mathcal{D}_{\mathcal{C}} / \mathcal{P}_{\mathcal{C}}.$$

Picard groups of projective curves Take $\mathcal{C}$ projective without singularities.

The degree of a divisor

$$D = \sum z_{\mathfrak{P}} \cdot \mathfrak{P}$$

is

$$\sum z_{\mathfrak{P}} \cdot \deg(\mathfrak{P}).$$

Divisors of degree 0 form a subgroup $\mathcal{D}_{\mathcal{C}}^{0}$ of $\mathcal{D}_{\mathcal{C}}$ containing principal divisors.

Definition 3.3

$$\mathrm{Pic}_{\mathcal{C}}^{0} := \mathcal{D}_{\mathcal{C}}^{0} / \mathcal{P}_{\mathcal{C}}$$

is the divisor class group of degree 0 *of* $\mathcal{C}$*.*

4 Algorithms in Picard Groups

The main question in this section is: Can we use Picard groups of curves for DL-systems useable in crypto systems, i.e.: Are the 4 items in Task 2.5 satisfied for a clever choice of curves?

4.1 The Theorem of Riemann-Roch

Let K be a number field.
The basic **Theorem of Minkowski** ensures that in every ideal class there is an ideal $\subset O_K$ with small norm, and so $\mathrm{Pic}(O_K)$ is a **finite abelian group**.
This result (and Dirichlet's theorem) is the key ingredient for ***Algorithmic Number Theory***.
It is possible to compute *explicitly and efficiently* with ideal classes using integral ideals with small norm. Fundamental for the arithmetic of curves $\mathcal{C}$ over K_0 is the

Theorem of Riemann-Roch.

4.1.1 Riemann-Roch Spaces

We define a partial ordering of elements in $\mathrm{Div}_{\mathcal{C}}(k)$ as follows; $D = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}}$ 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 4.1 *Let $D = \sum_{\mathfrak{p} \in \Sigma_{\mathcal{C}}(k)} z_{\mathfrak{p}} \in \mathrm{Div}_{\mathcal{C}}(k)$. The **Riemann-Roch space** associated to D is*

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

So 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 $D_1 \geq 0$.

Proposition 4.2 *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 $\ell(D) \sim \ell(D')$. In particular $\mathcal{L}(D)$ is a finite-dimensional K-vector space.

Definition 4.3 $\ell(D) := \dim_K(\mathcal{L}(D))$.

To compute $\ell(D)$ is a fundamental problem in the theory of curves.

Theorem 4.4 (Riemann) *For given curve $\mathcal{C}$ there is a minimal number $g_{\mathcal{C}} \in \mathbb{N} \cup \{0\}$ such that for all $D \in \mathrm{Div}_{\mathcal{C}}$ we have*

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

Definition 4.5 *$g_{\mathcal{C}}$ is the* genus *of $\mathcal{C}$.*

The theorem of Riemann can be refined (Roch-part) (and then reveals its true face: duality) by using divisors of differentials:

Theorem 4.6 *Let Ω be a canonical divisor of $\mathcal{C}$. For all $D \in \mathrm{Div}_{\mathcal{C}}(K)$ we have*

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

A differential ω is *holomorphic* if (ω) is an effective divisor. The set of holomorphic differentials is a K-vector space denoted by $\omega_{\mathcal{C}}^0$ which is equal to $\mathcal{L}(W)$.

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

Corollary 4.7 $\omega_{\mathcal{C}}^0$ *is a* $g_{\mathcal{C}}$*- dimensional* K*- vector space and* $\deg(W) = 2g_{\mathcal{C}} - 2$.

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

Corollary 4.8 *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.*

4.2 Applications of RR

4.2.1 Picard groups of curves over finite fields

A first **consequence** is: If $K_0 = \mathbb{F}_q$ then

$$\mathrm{Pic}_{\mathcal{C}}^0 \text{ is a finite abelian group}$$

and the elements can be presented with a number of bits depending polynomially on $g_{\mathcal{C}}$ and $\log q$.

But we get much more:

Theorem 4.9 ***(F.Heß, C. Diem)***
Let $\mathcal{C}$ *be a curve of genus* $g_{\mathcal{C}}$ *over* $\mathbb{F}_q$.
The addition in $\mathrm{Pic}_{\mathcal{C}}^0$ *can be executed (probabilistically) with a number of bit-operations, which is bounded (explicitly) polynomially in* $g_{\mathcal{C}}$ *(for q fixed) and* $\log(q)$ *(for* $g_{\mathcal{C}}$ *fixed).*

The proof of this theorem is modeled after an analogous result for addition in ideal classes of number fields, the theorem of Riemann-Roch replaces the theorem of Minkowski.

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 (which is assumed to be algebraically closed in F and isomorphic 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

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

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 4.10 *For $g \geq 3$ and $D = \omega_{\mathcal{C}}$ the space $\mathcal{L}(\omega) = \omega_{\mathcal{C}}^0$ is without base points, and so Φ_ω is a morphism from $\mathcal{C}$ to $\mathbb{P}^{g_C - 1}$.*

Φ_ω may not be an embedding but the only exception is that Phi_ω induces a cover to the projective line of degree 2, and then either the genus of $\mathcal{C}$ is 1 or $\mathcal{C}$ is *hyperelliptic.*

Theorem 4.11 *Let $\mathcal{C}$ be a curve of genus $g_{\mathcal{C}} > 2$ and assume that $\mathcal{C}$ is not hyperelliptic. Then Φ_ω is an embedding of $\mathcal{C}$ into $\mathbb{P}^{g_C - 1}$ 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 $\Phi_\omega(\mathcal{C})$. Φ_ω is the **canonical embedding** of $\mathcal{C}$.

Example 4.12 *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 $x \in k(C) \setminus k$ 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 canonical embedding for **non hyperelliptic** curves and general projections we can chose $G_h(X, Y, Z)$ as homogeneous polynomial of degree $2g_{\mathcal{C}} - 2$.

Remark 4.13 *In general this is not the minimal degree for plane curves of genus g,*

But in general, this is not

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: $\ell_i = i$. Hence $\mathcal{L}_1 =< 1 >$, $\mathcal{L}_2 =< 1, x >$ with a function $x \in K(\mathcal{E})$ with $(x)_\infty = 2\mathfrak{p}_\infty$, $\mathcal{L}_3 =< 1, x, y >$ with $(y)_\infty = 3\mathfrak{p}_\infty$ and $\mathcal{L}_5 =< 1, x, x^2, y, xy >$ 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

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

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 3 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 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 iff the discriminant with 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 4.14 *Elliptic curves defined over k correspond one-to-one the isomorphic classes of plane projective curves without singularities given by Weierstrass equations*

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

with non-vanishing discriminant X-discriminant.

Since we are dealing with isomorphism classes of such curves we can further normalize the equations and finally find invariants for the class of a given $\mathcal{E}$.
This is a bit tedious if $char(K)|6$. In this case we refer to J.Silverman: The Arithmetic of Elliptic Curves).
Assume that $char(k) \neq 2, 3$ then we can use Tschirnhausen transformations to get and equation

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

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 $\neq 0$, as well as

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

If K is algebraically closed then $j_{\mathcal{E}}$ determines the isomorphy class of $\mathcal{E}$.
For arbitrary K, E is determined up to a *twist*, which is quadratic if $char(k)$ is prime to 6 (see again Silverman's book)

Weierstrass equations for hyperelliptic curves: We apply the same strategy to hyperelliptic curves of genus ≥ 2. Let $\mathcal{C}$ be a curve over K of genus $g \geq 2$ with a cover

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

of degree 2. 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, $conorm(\mathfrak{p}_{0,\infty}) = 2 \cdot \mathfrak{p}_\infty$ and so η is ramified in Q_0, or $conorm(\mathfrak{p}_{0,\infty}) = \mathfrak{p}_\infty \cdot \mathfrak{p}'_\infty$. In any case $conorm(\mathfrak{p}_{0,\infty}) =: D$ 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 $\ell_1 = 2$.

Counting of dimensions for larger i yields:
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 and equation

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

and $\deg(h(x) \leq g + 1$, $\deg(f) \leq 2g + 2$.
The Hurwitz genus formula shows that the cover has exactly $2g + 2$ ramification points, and so $\deg(f) = 2g+1$ if the point at infinity is ramified, and $\deg(f) = 2g+2$ if this point is unramified.
The cover η is uniquely determined up to automorphisms of $\mathbf{P}^1$, and so the dimension of the hyperelliptic locus in the moduli scheme $\mathcal{M}_g$ of curves of genus g is $2g-1$. (Recall: The dimension of $\mathcal{M}_g$ is $3g - 3$ and so larger than $2g - 1$ for $g \geq 3$.)

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

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 $\mathcal{C}$.

4.2.4 Addition Laws for elliptic and hyperelliptic curves

Again we begin with elliptic curves.
Let $\mathcal{E}$ be a curve of genus 1 with rational point P_∞, hence by definition $\mathcal{E}$ is an elliptic curve.
By Riemann-Roch we find a regular Weierstraß equation theorem

$$E : Y^2Z + a_1YXZ + a_3YZ^2 =$$

$$X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and $P_\infty = (0 : 1 : 0)$.
In $c \in \mathrm{Pic}^0_E$ there is exactly one prime divisor $\mathfrak{P}$ of degree 1 and hence a point $P \in E(K_0)$ such that

$$c = \mathfrak{P} - \mathfrak{P}_\infty.$$

We identify $(\mathrm{Pic}^0_E, +)$ with $(E(K_0), \oplus)$.
Given $P_1, P_2 \in E(K_0)$ the line l_{P_1,P_2} through P_1, P_2 intersects $E(K_0)$ in a third point Q.
$\mathfrak{P}_1 + \mathfrak{P}_2 + \mathfrak{Q} - 3\mathfrak{P}_\infty = (l_{P_1,P_2\ |E})$ and so

$$P_1 \oplus P_2 \oplus Q = 0.$$

4.3 Addition in Picard groups of hyperelliptic curves

Inspired by the group law on elliptic curves and its geometric interpretation one finds an *explicit* algorithm for the group operations in Picard groups of hyperelliptic curves.

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

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

over k. We denote the prime divisor corresponding to $P_\infty = (0 : 1 : 0)$ by $\mathfrak{p}_\infty$.

We note that the affine coordinate ring of $W_{\mathcal{C}}$ is

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

and so prime divisors $\mathfrak{p}$ of degree d of $\mathcal{C}$ correspond to prime ideals $P \neq 0$ with $[\mathcal{O}/P : k] = d$. Mumford representation:In each divisor class $c \in \mathrm{Pic}^0(k)$ we find a unique *reduced* divisor

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

with $\sum_{i=1}^r n_i \deg(\mathfrak{p}_i) = d \leq g$, $\mathfrak{p}_i \neq \omega(\mathfrak{p}_j$ for $i \neq j$ and $\mathfrak{p}_i \neq \mathfrak{p}_i nfty$.

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

By algebra we get that the ideal I is a free $\mathcal{O}$-module of rank 2 and so

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

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

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

Theorem 4.15 (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?

To find u, v one solves (with High School Math) an interpolation problem.
Given two divisor classes in Mumford representation one has to find such a representation in the sum of these classes, and this is done by a reduction step: The **Cantor algorithm**:
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 $< u_1u_2, u_1(y - v_2), u_2(y - v_1), (y - v_1)(y - v_2) >$.
We have to determine a base, and this is done by Hermite reduction.
The resulting ideal is of the form $< u_3'(X), v_3'(X) + w_3'(X)Y >$ but not necessarily reduced.
To reduce it one uses recursively the fact that $u|(v^2 - hv - f)$.
For readers acquainted with algorithmic number theory it may be enlightening to compare this algorithm with the well known method to compute class groups of imaginary quadratic number fields, going back to Gauß and based on the theory of definite quadratic forms with fixed discriminant.

4.4 Picard groups of curves as DL - systems?

Conditions 1) and 2) of Task 2.5 are satisfied –**if** one finds curves $\mathcal{C}$, so that $\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$ contains a subgroup of large prime order. To check this one needs a fast algorithm for computing $|\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)|$.
In general this is unsolved.
But before going to tedious details we should discuss the expected security!
There are various attacks to DL-systems based on Picard groups but the worst one is Index-calculus.

5 Index-calculus

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

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

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 on Algebra by Kraichik (1922) ; in fact this is the index-calculus algorithm reinvented and refined in cryptography from 1980 till today, see in particular new work of A. Joux e al. As result one gets algorithms of subexponential complexity (with relatively small constants,), which are even dramatically faster if q is not a prime.
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. 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 lifting of elements in Abelian varieties over finite fields to number fields.

But unfortunately there are very effective variants of the index- calculus attack to Picard groups.

5.1 The Principle of 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 If the following holds

$$R_j : \oplus_{i=1}^{r} [n_i] g_i = 0_G. \tag{2}$$

Obviously R_j yields the relation

$$\sum_{i=1}^{r} n_i \log_{g_0}(g_i) \equiv 0 \mod N \tag{3}$$

for discrete logarithm.

We assume that we can find sufficiently many independent relations as in Eq. (2) for solving the system in Eq. (3) 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

$$G \cong \mathbb{Z}^r / < ..., R_j, ... > .$$

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 $e_1, .., e_r$ 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 $n\mathbb{N}$ is B-smooth if all prime divisors of n are $\leq B$, and results from analytic number theory by Canfield, Erdös, Pomerance state 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 a paper of A.Enge and P. Gaudry.
This principle is refined in concrete situations with enormous effect as we shall see below. Index calculus can be applied to a discrete logarithm in Jacobians of hyperelliptic curves.

Let $\mathcal{C}$ be a hyperelliptic curve of genus $g \geq 2$ over a finite field $\mathcal{F}_q$ of characteristic p and G a cyclic subgroup in $\mathrm{Pic}^0_{\mathcal{C}}$.

As factor base we choose points in $Pic^0_{\mathcal{C}}$ with $u(X)$ irreducible of degree bounded by 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.

Theorem 5.1 *For* $\log q \leq (2g+1)^{1-\epsilon}$*, there exists a constant* $c \leq 2.18$ *such that the discrete logarithms in* $Jac_{\mathcal{C}}(\mathbb{F}_q)$ *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 5.2 (Gaudry) *Let* $\mathcal{C}$ *be a genus* $g \geq 2$ *hyperelliptic curve defined over a finite field* $\mathcal{F}_q$*. If* $q > g!$ *then discrete logarithms in* $Jac_{\mathcal{F}_q}(\mathcal{C})$ *can be computed in expected time* $O(g^3 q^{2+\epsilon})$*.*

Since the expected size of $\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$ is q^g 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 (Diem, Gaudry, Thé riaut, Thomé)) one gets

Theorem 5.3 *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.*

5.2 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, and 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. member ship tests for zero-dimensional schemes) Diem succeeds to prove

Theorem 5.4 *Fix $d \geq 4$ such that d or $d-1$ is prime.*
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.

Remark 5.5 *The result may be a bit disappointing: Remaining candidates for DL-systems in the zoo of curves over finite fields are and so remaining candidates are:* ***elliptic curves****,* ***curves of genus 2*** *and* ***hyperelliptic curves of genus 3****, i.e. only curves curves given by equations (in char 0):*

$$Y^2 = X^n + \ldots.$$

with $3 \leq n \leq 8$. *Even in this case there are in rather a lot of cases transfers to systems known to be weak:*
Correspondences *to non-hyperelliptic curves for* $g = 3$
Duality *maps e.g. for supersingular curves*
Weil descent and related index-calculus *if $\mathbb{F}_q$ is not a prime field.*

So: Take for $\mathcal{C}$ an elliptic curve E or a curve of genus 2 (and avoid some weak instances) and , maybe, very special curves of genus 3 (e.g. with automorphisms of order 4) and for $\mathbb{F}_q$ a prime field $\mathbb{F}_p$.
Then we shall find (carefully chosen) elliptic curves defined over prime fields $\mathbb{F}_p$, which are, till today, exponentially secure under algorithms with classical computers. Example 3.) from above is a instance with security level of AES128.

But as said already, there will be no resistance against quantum computing.
But at the very end of the lecture we shall present two systems for key exchange in the spirit of Diffie-Hellman with more Q-bit security.

The main remaining task will be point counting on curves of small genus over $\mathbb{F}_q$. To do this we shall need more about Galois representations.

6 Fundamental groups and Galois representations

Comparing with the theory of Riemann surfaces we see that there is still an important tool missing: What are the analogues of fundamental groups and their operation on cohomology groups, how do topological and arithmetic objects combine? Obviously, the Zariski topology has to be replaced by a stronger topology.

The great idea of Grothendieck was a generalization of the theory of topological spaces by **Grothendieck topologies**:

Environments are replaced by *covers* with appropriate algebraic-geometric properties.

We only touch this fascinating area very superficially and look at the

Etale Topology: A $\mathcal{X}$ scheme is endowed with the system of étale (finite and unramified) covers

$$f : \mathcal{Y} \to \mathcal{X}$$

with the well known functorialities of such covers, i.e. under scalar extensions.

Projective limits are used to construct "universal" covers and fundamental groups (which are, in the profinite topology, compact by definition).

Example 1:

Be K a field.

Let L be a finite extension of K, and $f_L : \text{Spec}L \to \text{Spec}K$ given by the inclusion $i_L : K \hookrightarrow L$.

f_L is étale if and only if L/K is textbf separable.

The universal cover is K_s, the separable completion of K, and the fundamental group is

$$G_K = Aut_K(K_s).$$

Quotients of this group can be obtained by special covers, for example, the maximum abelian extension is K has the fundamental group $G_K/[G_K, G_K]$.

Example 2:

Let $X = \text{Spec}O_K$ be an arithmetic curve.

Then, the universal cover in étale topology is the ring of integers in the maximal unramified extension K_{nr} of K. The fundamental group is $G_(K_{nr}/K)$.

The fundamental group of $\mathbb{Z}$ is trivial (Minkowski). In general we do not know much about this group.

But if one goes to the maximal-abelian extension, one obtains a finite extension whose Galois group is isomorphic to Pic_K, and the *class theory theory* rules the game.

If one likes, one can formulate this theory completely in the language of *étale cohomology.*

Example 3:

Of particular interest is the case that $X = \mathcal{C}$ is a projective curve over a field K_0 with $\mathrm{Char}(K_0) = 0$.
In this case, the properties of K_0 interplay with those of the curve: On the one hand you have covers by constant field extensions of K_0, on the other hand, there are "geometric " covers with fixed constant fields. Unfortunately, such covers do not behave nicely under composition, and the situation is very well reflected by the exact (and, in general non-split) sequence of Galois groups:

$$1 \to G_{K_{\mathcal{C}\cdot\overline{K_0}}} \to G_{K_\mathcal{C}} \to G_{K_0} \to 1.$$

Etale topology is concerned with *unramified* extensions $\mathcal{D}$ of $\mathcal{C}$.
Since separable constant field extensions are unramified, we have the basic sequence

$$1 \to \Pi_1(\mathcal{C} \times \mathrm{Spec}(\overline{K_0})) \to \Pi_1(\mathcal{C}) \to G_{K_0} \to 1$$

where $\Pi_1(\mathcal{C} \times \mathrm{Spec}(\overline{K_0}))$ is the *geometric fundamental group.*

Remark 6.1 *(Anabel geometry according to Grothendieck)*

1. *The above sequence yields a Galois representation*

   $$\rho_\mathcal{C} : G_{K_0} \to \mathcal{OUT}(\Pi_{1,g}(\mathcal{C}))$$

   .

2. *If K_0 is contained in a $\mathfrak{p}$- adic field and if the genus of $\mathcal{C}$ is ≥ 2, then $\mathcal{C}$ is uniquely determined by $\rho_\mathcal{C}$ (**Mochizuki**).*

3. *If $K_0 = \mathbb{Q}$ and $g_\mathcal{C} \geq 2$ then $\rho_\mathcal{C}$ is injective.*
   So you can study the Galois group of $\mathbb{Q}$ using the fundamental groups of curves over $\mathbb{Q}$.

ℓ -adic Galois representations . Let ℓ be a prime different from char$((K_0)$. Following Grothendieck we can assume without loss of generality that $K_0 \subset \mathbb{C}$ and compare algebraic covers with analytic covers.

From the *Riemann existence theorem* it follows that every finite group can be realized as a Galois group over $K_{\mathcal{C}} \cdot \overline{K_0}(T)$ and that $\Pi_1(\mathcal{C} \times \mathrm{Spec}(\overline{K_0}))$ is the compactification in the Krull topology of a free group with $2g_{\mathcal{C}}$ generators modulo *one* commutator relation.

So the maximal-abelian pro- ℓ quotient $\Pi_1(\mathcal{C} \times \widetilde{\mathrm{Spec}(\overline{K_0})})_\ell$ as an abelian group is isomorphic to $\mathbb{Z}_\ell^{2gc}$ and $\rho_{\mathcal{C}}$ induces an ℓ -adic representation

$$\widetilde{\rho}_{\ell\mathcal{C}} : G_{K_0} \to Aut(\mathbb{Q}_\ell^{2gc}).$$

$\widetilde{\rho}_{\ell\mathcal{C}}$ is the ℓ -adic completion of $H^1(\mathcal{C})_{et}$.

Conjecture of Fontaine-Mazur: *Every* irreducible ℓ -adic Galois representation of a number field with only finitely many ramification points and satisfying a semi-stability condition "comes from" a cohomology group of a smooth projective variety.

"Geometric class theory theory": Tate modules of Picard groups .
We find a geometrically constructed representation space for $\widetilde{\rho}_{\ell\mathcal{C}}$:
G_{K_0} operates on $\mathrm{Pic}^0_{\mathcal{C}}(\overline{K_0})$ in a natural way.
For $n \in \mathbb{N}$ we denote by $\mathrm{Pic}^0{}_C(\overline{K_0})[\ell^n]$ the subgroup of elements whose order divides ℓ^n.
Fact: $\mathrm{Pic}^0_{\mathcal{C}}(\overline{K_0})[\ell^n]$ is isomorphic as *Galois module* to

$$\Pi_1(\mathcal{C} \times \widetilde{\mathrm{Spec}(\overline{K_0})})_\ell/\ell^n \times \pi_1(\mathcal{C} \times \widetilde{\mathrm{Spec}(\overline{K_0})})_\ell.$$

Definition 6.2 *The Tate module $\mathcal{T}_{\mathcal{C},\ell}$ is the G_{K_0} module*

$$\mathrm{proj-limPic^0_{\mathcal{C}}(\overline{K_0})[\ell^n]}.$$

$\widetilde{\rho}_{\ell\mathcal{C}}$ the Galois representation with representation space $\mathcal{T}_{\mathcal{C},\ell} \bigotimes \mathbb{Q}_\ell$, and the representation $\rho_{\mathcal{C},\ell^n} := \widetilde{\rho}_{\ell\mathcal{C}} \bigotimes \mathbb{Z}/\ell^n$ has as a representation module $\mathrm{Pic}^0_{\mathcal{C}}(\overline{K_0})[\ell^n]$.

7 Etale Isogenies of Elliptic Curves

Let $\mathcal{E}$ be an elliptic curve over K_0 and assume first that $K_0 = \overline{K_0}$.
Then $\Pi_1(\mathcal{E})$ is the profinite free abelian group with two generators. Finite quotients of $\Pi_1(\mathcal{E})$ are subgroups of $\mathbb{Z}/n \times \mathbb{Z}/n$ for large enough n.
By Galois theory these quotients correspond to unramified finite covers of curves

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

By the Hurwitz genus formula it follows that $\mathcal{E}'$ **is also an elliptic curve.**
We can assume that η maps $P_{\mathcal{E}',\infty}$ to $P_{\mathcal{E},\infty}$, and then η is a morphism of the projective group schemes $\mathcal{E}', \mathcal{E}$.
Hence the kernel $\mathrm{Ker}(\eta)$ is closed and so an étale group scheme.
In particular, $|\ker(\eta)(K_0)| = \deg(\eta)$. Now take K_0 arbitrary and $\mathcal{E}, \mathcal{E}'$ defined over K_0.
Then η is defined over K_0 iff $\ker(\eta)$ is G_{K_0}-invariant.
η is an example for the following definition:

Definition 7.1 *Elliptic curves $\mathcal{E}$ and $\mathcal{E}'$ are isogenous over K_0 iff there is a finite morphism $\eta : \mathcal{E}' \to \mathcal{E}$.*
If $\mathcal{E} = \mathcal{E}'$ then $\eta \in \mathrm{End}(\mathcal{E})$, the ring of endomorphisms.

Remark 7.2 *There are important* inseparable *and so non-étale isogenies of elliptic curves. These are detected by the "finite-flat" topology, their kernels are finite-flat group schemes (e.g. local group schemes).*

7.1 Isogeny graph

Let K_0 be arbitrary. As explained, G_{K_0} operates on the geometric fundamental group.
It follows: Let $\mathcal{E}, \mathcal{E}'$ be elliptic curves over K_0 and let

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

be a separable isogeny.
Then f is defined over K_0 if Ker(f) is invariant under G_{K_0}.
Let n be prime to the characteristic of K_0.
f is cyclic of order n if Ker(f) $\cong \mathbb{Z}$/n. Cyclic isogenies can be composed by isogenies of prime degree.

Definition 7.3 *The isogeny graph $\Sigma_{K_0}(\mathcal{E})$ of $\mathcal{E}$ over K_0 has as vertices the isomorphism classes (over $\overline{K_0}$ of elliptic curves $\mathcal{E}'$ isogenous to E over K_0, and as edges separable isogenies of prime degree.*

7.2 Modular Curves

We assume that $N \in \mathbb{N}$ is prime to $\mathrm{Char}(K_0)$ and study for over fields L of K isogenies η of elliptic curves E/L whose kernel C_N is cyclic of order N. The functor $L \mapsto \{(E, \eta_N)/L/\cong\}$ is a (coarse) moduli functor $\mathcal{F}_N$.

There is a classical explicit construction of the **modular curve** $X_0(N)$ as quotient of the complex upper half plane which presents this functor. **Explicit construction** over $\mathbb{C}$

$$\mathbb{H} := \{z \in \mathbb{C};\ \mathrm{Im}(z) > 0\}$$

and

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \infty.$$

$$\Gamma_0(N) := \left\{\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})\right\}$$

with $c \equiv 0 \mod N$
operates on $\mathbb{H}^*$ by

$$z \mapsto (az+b)/(cz+d).$$

$$X_0(N)_{\mathbb{C}} := \Gamma_0(N)\backslash\mathbb{H}^*.$$

$X_0(N)$ is a compact Riemann surface and hence a projective curve over $\mathbb{C}$.

By construction the curve presents the complex points of the moduli functor $\mathcal{F}_N$ and hence, By general principles, $X_0(N)$ is defined over $\mathrm{Spec}(\mathbb{Z})$.

This curve has a very rich algebraic and analytic structure, e.g. the Galois representations on torsion points of $\mathrm{Pic}^0(X_0)(N))$ are direct sums of odd two-dimensional representations of $G_{\mathbb{Q}}$.

7.2.1 Computational Aspect

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).

Result:(Vélu, Couveignes, Lercier, Elkies, Kohel, ...)

The cost for the computation of an isogeny of degree ℓ of an elliptic curve E over $\mathbb{F}_q$ is $\mathcal{O}(\ell^2 + \ell\log(\ell)\log(q))$.

7.3 Arithmetic of Galois Representations

Let K be a number field with absolute Galois group G_K, which is compact in the profinite topology.
Let R be a topological ring.
A Galois representation is a continuous homomorphis

$$\rho : G_K \to M_{k\times k}(R).$$

The most important example for R are $\mathbb{Z}/n$, $\mathbb{F}_q$ and $\mathbb{Z}_\ell$.
Because of continuouty it follows that $\mathrm{Ker}(\rho)$ is closed.
Define $K_\rho := \overline{K}^{\mathrm{Ker}(\rho)}$.
ρ is unramified in $\mathfrak{P} \in \mathrm{Spec}(O_K)$ if K_ρ/K is unramified in $\mathfrak{P}$.
Our standard assumption is: The set of ramified primes is finite.
The conductor N_ρ of ρ is "essentially" the product of the prime ideals (mayby with small exponents), which are ramified in ρ.
(ρ heißt **geometrisch** (s.o.)).

7.4 Semi-simple Representations

Definition 7.4 *For $\sigma \in G_K$ denote by*

$$\chi_{\rho(\sigma)}(T)$$

*the charakteristical polynomial of $\rho(\sigma)$.
ρ is semi-simple if ρ is determined by*

$$\{\chi_{\rho(\sigma)}(T); \sigma \in G_K\}$$

up to equivalence.

To emphasize the importance of this property we remark:
The key result for the proof of the Theorem of Faltings is that

$$\widetilde{\rho}_{\ell_{\mathcal{C}}}$$

attached to Tate modules of Picard grops of curves over K is semi-simple.

7.5 Frobeniusautomorphismen

The key for the intimate relation between arithmetic in number fields K with its Galois group G_K is the study of Frobenius automorphisms.

Definition 7.5 *Let* $\mathfrak{l}$ *be a prime ideal of* O_K *containing the prime number* ℓ*, and take* $\sigma \in G_K$*.*
σ *is a Frobeniusautomorphismus attached to* $\mathfrak{l}$ *if there is a prime ideal* $\mathfrak{l}'$ *in* $\bar{\mathbb{Z}}$ *containing* $\mathfrak{l}$ *such that for all* $x \in \bar{\mathbb{Z}}$ *we have:*

$$\sigma(x) - x^{\ell} \in \mathfrak{l}'.$$

For given $\mathfrak{l}$ there are (infinitely many) different Frobeniusautomorphismen , but they are all conjugate in G_K ,so their charakteristical polynomial attached to representations are equal. If the representations are semi-simple we can neglect the different possibilities and choose for $\mathfrak{l}$ one Frobeniusautomorphismus $\sigma_{\mathfrak{l}}$.

Theorem 7.6 ***Density Theorem of Čebotarev***
A semi-simple representation ρ *is determined by*

$$\{\chi_{\rho(\sigma_{\mathfrak{l}})}(T)\}_{\mathfrak{l}\in\mathrm{Spec}(O_K)\setminus S}$$

, where S *is an arbitrary finite set containing* (0)*.*

7.6 Two-dimensional odd Galois representations

In this section, we are interested in two-dimensional representations ρ.

Definition 7.7 *ρ is odd if for every complex conjugation $\tau \in G_K$ one has*

$$\det(\rho)(\tau) = -1$$

7.6.1 Representations on elliptic curves

Let E be an elliptic curve over K that we extend to a (minimal) curve $\mathcal{E}$ över O_K.
$\mathcal{E}$ has good reduction outside a finite set $S_{\mathcal{E}}$.
The conductor of $\mathcal{E}$ is $N_{\mathcal{E}} = \prod_{\mathfrak{P} \in S_{\mathcal{E}}} \mathfrak{P}^{e_{\mathfrak{P}}}$ with $e_{\mathfrak{P}} = 1$ if $\mathcal{E}$ is semi-stable in $\mathfrak{P}$.
It follows that $\widetilde{\rho}_{\ell \mathcal{E}}$ is a two-dimensional representation that is semi-simple and unramified outside of $N_{\mathcal{E}}$. G_K induces on $\mathcal{E}(\overline{K}[n])$ an odd (Weil pairing) representation

$$\rho_{n,\mathcal{E}} : G_K \to Aut(\mathbb{Z}/n \times \mathbb{Z}/n)$$

.

Theorem 7.8 *(special case of Faltings and Tate results)*
The following items are equivalent (with a number n_0 depending on $N_{\mathcal{E}}$)

1. *$\mathcal{E}$ is K- isogenous to $\mathcal{E}'$.*

2. $$\widetilde{\rho}_{\ell \mathcal{E}} \cong \widetilde{\rho}_{\ell \mathcal{E}'}$$

   for one (and therefore all) ℓ.

3. $$\chi_{\widetilde{\rho}_{\ell \mathcal{E}}}(\sigma_{\mathfrak{p}}) = \chi_{\widetilde{\rho}_{\ell \mathcal{E}'}}(\sigma_{\mathfrak{p}})$$

   for almost all prime ideals $\mathfrak{p} \in \mathrm{Spec}(O_K) \setminus (S_{\mathcal{E}} \cup \{\mathfrak{l};\, \ell \in \mathfrak{l}\}$.

4. *(Effective version of Čebotarev):*

   $$\chi_{\rho_{n,\mathcal{E}}} = \chi_{\rho_{n,\mathcal{E}'}}$$

   for an $n \geq n_0$.

7.6.2 The Frobenius Endomorphism

We are now motivated to **calculate** $\chi_{\widetilde{\rho_{\ell,\mathcal{E}}}}(\sigma_{\mathfrak{p}})$ for $\ell \notin \mathfrak{p}$.

1. ***" Hensel's Lemma "***: $\sigma_{\mathfrak{p}}$ can be identified in a natural way with the Frobenius automorphism $Frob_{p^d}$ of the field $O_K/\mathfrak{p} = \mathbb{F}_q$, which is a topological generator of $G_{\mathbb{F}_q}$, and
$$\chi_{\widetilde{\rho_{\ell,\mathcal{E}}}}(\sigma_{\mathfrak{p}}) = \chi_{\widetilde{\rho_{\ell,\mathcal{E}_{\mathfrak{p}}}}}(Frob_{p^d})$$
.

2. The Galois element $Frob_{p^d}$ has a **geometric** interpretation: It fixes the equation of $\mathcal{E}_{\mathfrak{p}}$ and operates on the points by exponentiation, so it induces the **Frobenius endomorphism** $\phi_{\mathfrak{p}} \in End(\mathcal{E}_{\mathfrak{p}})$.
$\phi_{\mathfrak{p}}$ is a purely inseparable isogeny of degree p^d.

3. Let $\ell \neq p$.
The characteristic polynomial of $\widetilde{\rho_{\ell,\mathcal{E}_{\mathfrak{p}}}}$ is an **integer** normalized polynomial
$$\chi_{\mathcal{E}_{\mathfrak{p}}}(T) = T^2 - Tr(\phi_{\mathfrak{p}})T + p^d$$
independent of ℓ, and for n prim to p we get
$$\chi_{\rho_{n,\mathcal{E}_{\mathfrak{p}}}}(\phi_{\mathfrak{p}})(T) \equiv \chi_{\mathcal{E}_{\mathfrak{p}}}(T) \mod n.$$

4. **Deuring:** $\phi_{\mathfrak{p}}$ can be interpreted as an imagina äry-quadratic number, and so
$$Tr(\phi_{\mathfrak{p}})^2 \leq 4p^d.$$

The isogeny $\phi_{\mathfrak{p}} - id$ is separable and its kernel is $\mathcal{E}_{\mathfrak{p}}(\mathbb{F}_q)$.

Corollary 7.9 [3]
$$|\mathcal{E}_{\mathfrak{p}}(\mathbb{F}_q)| = |p^d + 1 - Tr(\phi_{\mathfrak{p}})| \leq 2\sqrt{p^d}.$$

[3] This is the **Hasse** inequality analogous to the Riemann Hypothesis proved by **Weil** for $g > 1$.

7.7 Serre's Conjecture and FLT

Recall: The Conjecture of Serre($\sim$ 1986), which is now the

Theorem 7.10 ***(Khare-Wintenberger-Kisin*** *($\sim$ 2006)*:
Odd two-dimensional irreducible (continuous) $\mathbb{F}_q$-representations ρ of the automorphism group $G_{\mathbb{Q}}$ of the algebraic numbers $\bar{\mathbb{Q}}$ are given by its operation on points of finite order of the Picard groups of modular curves $X_0(N)$ with nebentype.
In addition, the minimal possible level N and the twist character are obtained from the arithmetical data of ρ.

Application: FLT:
For

$$A^p - B^p = C^p$$

and

$$E_{ABC} : Y^2Z = X(X - A^p)(X - B^p)$$

the representation $\rho_{p,\mathcal{E}_f}$ has conductor $2 \cdot p$, and so is presented by $\mathrm{Pic}^0(X_0(2)[p]$, which is a curve of genus 0!

7.8 Point counting on elliptic curves: The SAE Algorithm

The theoretical results together with the corollary 7.9 allow us to calculate $|\mathcal{E}_{\mathfrak{p}}(\mathbb{F}_q)|$ in **polynomial time**.
The idea of **R. Schoof** is:
Compute the operation from $\phi_{\mathfrak{p}}$ to $\mathcal{E}_{\mathfrak{p}}[\ell^k]$ for small ℓ, k with $\prod \ell^k \geq 2\sqrt{p^d}$ and use then CRT.
For this calculation, use the explicitly known " classical n-divisional polynomials " Ψ_n.
Disadvantage: $\deg(\Psi_n) \sim n^2$, and hence the Schoof algorithm is too slow.
Idea of Atkin-Elkies: Compute instead of points with cyclic groups, and use the the " classical modular polynomials " ϕ_n of degree $\sim n$.

Theorem 7.11 ***(SAE)***
$|\mathcal{E}_{\mathfrak{p}}(\mathbb{F}_q)|$ *can be calculated with complexity* $\mathcal{O}((d \log p)^4)$.

7.9 Point counting for curves of genus 2 and 3

As said, the other candidates for DL-systems are Picard groups of hyperelliptic curves of genus 2 and 3.

We can try to follow the ideas of SAE in order to determine $|\mathrm{Pic}^0_{\mathcal{C}}|$ for curves $\mathcal{C}$ over fields $\mathbb{F}_q$.

In principle, this is possible for general abelian varieties and a polynomial time algorithm is due to Pila in the spirit of Schoof.

But this algorithm is much too slow for applications. For curves of genus 2 there are (rudimentary) results for "modular" polynomials and for division polynomials. Gaudry and Schost use this and succeed (in rather a tour de force) to compute Picard groups of curves of genus 2 in cryptographically interesting ranges. For curves of genus 3 this seems to be hopeless nowadays.

But one can use curves with special properties, for instance, one looks for curves such the the ring of endomorphisms $\mathcal{O}_{\mathcal{C}}$ of the Jacobian variety is large: $\mathcal{C}$ has real multiplication and so $\mathcal{O}_{\mathcal{C}}$ contains an order in a totally real number field of degree $g_{\mathcal{C}}$, or even a CM-field, i.e. an imaginary quadratic field over a totally real field of degree $g_{\mathcal{C}}$. It is well-known that the latter case leads to classical class field theory (Shimura-Taniyama theory) and hence the Frobenius endomorphisms are given by prime ideals in $\mathcal{O}_{\mathcal{C}}$, and real multiplication can be used to accelerate the point counting algorithms immensely (work of Gaudry et.al.).

To construct such curves one first has to determine the period matrix of the Jacobian and then their (Shioda) invariants over the complex numbers. By reduction theory modulo p and by using Mestre's algorithm one then determines equations for $\mathcal{C}$ over $\mathbb{F}_q$.

The main source for curves with real multiplication are curves, whose Jacobian are $g_{\mathcal{C}}$-dimensional siple factors of the Jacobian variety $J_0(N)$ of the modular curve $X_0(N)$.

This method works very efficiently for curves of genus 2, and since they are equipped with a very fast addition and, as far as we know, as secure as elliptic curves, Picard groups of curves of genus 2 are a competitive alternative to elliptic curves.

For curves of genus 3 one has a big problem: Most curves of genus 3 are non-hyperelliptic (since the hyperelliptic locus is of co-dimension 1 in the moduli space of curves of genus 3) and so not usable for cryptography. Hence suggestions for curves of genus 3 are mostly restricted to curves $\mathcal{C}$ with complex multiplication field $R(\sqrt{-1})$ where R is a totally real cubic field with class number 1: The existence of an automorphism of order 4 on the Jacobian forces $\mathcal{C}$ to be hyperelliptic.

8 Diffie-Hellman Key Exchange with Isogenies

We end the lecture by sketching two Key Exchange systems based on elliptic curves but not on the discrete logarithm, which could be more resistant against quantum computers.
We have to use the theory of isogenies of elliptic curves over finite fields and beautiful theoretical results mainly due to **M. Deuring**.

8.1 Isogenies of Ordinary Elliptic Curves

Theorem 8.1 ***(Deuring)***
Let E be an elliptic curve over a field K_0.
E is ordinary iff $\mathrm{End}(E)$ is commutative.

1. *Assume that $\mathrm{Char}(K_0) = 0$. Then E is ordinary and $\mathrm{End}_{\overline{K_0}}(E) = \mathbb{Z}$ (generic case) or $\mathrm{End}_{\overline{K_0}}(E)$ is an order $O_E \subset \mathbb{Q}(\sqrt{-d_E})$, $d_E > 0$ (CM-case).*
   Take E with CM with order O_E.
   Let $\mathcal{S}_E$ be the set of $\mathbb{C}$-isomorphy classes of elliptic curves with endomorphism ring O_E.
   Then $\mathrm{Pic}(O_E)$ acts in a natural and simply transitive way on $\mathcal{S}_E$, hence $\mathcal{S}_E$ is a PHS under $\mathrm{Pic}(O_E)$:
   For $c \in \mathrm{Pic}(O_E)$, $\mathfrak{A} \in c$ and $\mathbb{C}/O_E = E_0$ we get
   $c \cdot [E_0]$ is the class of $\mathbb{C}/\mathfrak{A}$.

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

   (a) there is a prime $\mathfrak{p}$ of K with

   $$\mathcal{E}_{\mathfrak{p}} \cong E,$$

   and

   (b)

   $$\mathrm{End}(E) = \mathrm{End}(\mathcal{E}) = O_E$$

   with $O_E \subset$ an order in an imaginary quadratic field.

8.1.1 Key Exchange à la Couveignes-Stolbunov

Let E_0 be an ordinary elliptic curve over $\mathbb{F}_q$ with $\mathrm{End}(E_0) = O$.
Define S_{E_0} as set of isomorphy classes of elliptic curves over $\overline{\mathbb{F}_q}$ with ring of endomorphisms O.
Using Deuring's lifting and the theory of complex multiplication we get that S_{E_0} is a $\mathrm{Pic}(O)$-set.
Hence we can use it for **Key Exchange:**
The partner P choses $c \in \mathrm{Pic}(O)$ and publishes the j-invariant of $c \cdot E_0$.
The exchange is not as fast as DL but feasible since one finds enough isogenies that are composites of isogenies of small degree (smoothness).
The **security** depends on the hardness of the following problem:
Find an isogeny between two isogenous elliptic curves.
The best **"classical"** result I know is
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 with quantum computer this complexity is subexponential (**Childs-Jao-Soukharev**), and the used fact is that S_{E_0} is a G-set with the abelian group $G = \mathrm{Pic}(O)$.

8.2 Supersingular Elliptic Curves

We now assume that E is a supersingular.
Again, the following results are mostly due to Deuring.

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

8.2.1 The Key Exchange System of De Feo

Take

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

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

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

is a supersingular elliptic curve over $\mathbb{F}_{p^2}$.

Categories $\mathcal{C}_i$ $(i = 1, 2)$ Objects isomorphism classes of supersingular E over $\mathbb{F}_{p^2}$ isogenous to E_0 and hence with $|E(\mathbb{F}_{p^2})| = (r^a \cdot s^b \cdot f)^2$.
Morphisms in $\mathcal{C}_1$: φ with $|\ker(\varphi)|$ dividing r^a
Morphisms in $\mathcal{C}_2$: ψ with $|\ker(\psi)|$ dividing s^b.
In this category the pushouts exist.

For additional information choose P_1, P_2 of order r^a and Q_1, Q_2 of order s^b in $E_0(\mathbb{F}_{p^2})$.
Key Exchange: The Partner P_1 chooses $n_1, n_2 \in \mathbb{Z}/r^a$ and the isogeny

$$\eta : E_0 \to E_0/ < n_1P_1 + n_2P_2 >=: E_1.$$

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

$$\psi : E_0/ < m_1Q_1 + m_2Q_2 >=: E_2.$$

P_2 sends

$$(E_2, \psi(P_1), \psi(P_2)).$$

P_1 can compute the common secret, the pushout of η and ψ) as

$$E_3 := E_2/ < n_1\psi(P_1) + n_2\psi(P_2) >$$

Again **Security** depends on computing an isogeny of two elliptic curves.
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, a very small key size.

In contrast to the ordinary case the groups around like 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.
But of course, there is lot of theory around, e.g. maximal orders in $Quot(\mathrm{End}(E_0))$ correspond to definite ternary quadratic forms of discriminant p ...