Arithmetic Geometry: Deep Theory, Efficient Algorithms and Surprising Applications

Gerhard Frey, University of Duisburg-Essen

Colloquium

Rome Tre, Dec. 12, 2018

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 Claim (**FLT**) : For $p \neq 2$ the projective curve

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

has only two $\mathbb{Q}$-rational points.

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 right 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**.

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.
$$Y^2 = X^3 + d,\ d \in \mathbb{Z} \setminus \{0\}$$
has only finitely many points with coordinates in $\mathbb{Z}$.(**Siegel-Mahler**)

2.
$$Y^2 = X^6 + d,\ d \in \mathbb{Z} \setminus \{0\}$$
has only finitely many points with coordinates in $\mathbb{Q}$ (**Faltings**)

3. **Theorem 1.1** ***(Taylor-Wiles)*** *Fermat's Claim is true.*

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

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

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. ≈ 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 1.2 ***(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 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:
Because of digitalization number theory plays a prominent role in communication theory and especially in data security.

2 Applications

A by now classical application of number theory is Coding Theory.
In this lecture we shall concentrate on another topic:
Cryptographical 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.

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 discussions of crypto primitive.
We shall describe below crypto primitives, 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 in particular 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 to the problem to exchange keys in open channels in the spirit of Diffie-Hellman. In the lecture tomorrow we shall describe a setting using push-outs in categories. The motivation is that such an abstract setting can open the mind for finding systems resistant against quantum computing, and we shall present at the end of the talk and, in more detail, in the lecture tomorrow, a promising example.

2.3.1 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 partner P_i chooses b_i and publishes $a_i := b_i(a_0)$.

The common key of P_1, P_2 is $b_2(a_1)$.

The effectiveness of this exchange depends on how fast the value $b_i(b_j(a_0))$ can be evaluated (i.e., calculated and represented), for random $b_i \in B_i, b_j \in B_j$.

The security depends on the
Computational Diffie-Hellman Problem

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 $b_a(a_0) = a$.

Problem:

1. Find usable instances 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 examples of systems for which we can apply this result later on.

2.3.2 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

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

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

2.4 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. $O(\log(|\ G\ |)$ 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 $|\ G\ |$), in particular the group order of G is a large prime.

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, in particular in the theory of representations of fundamental 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.

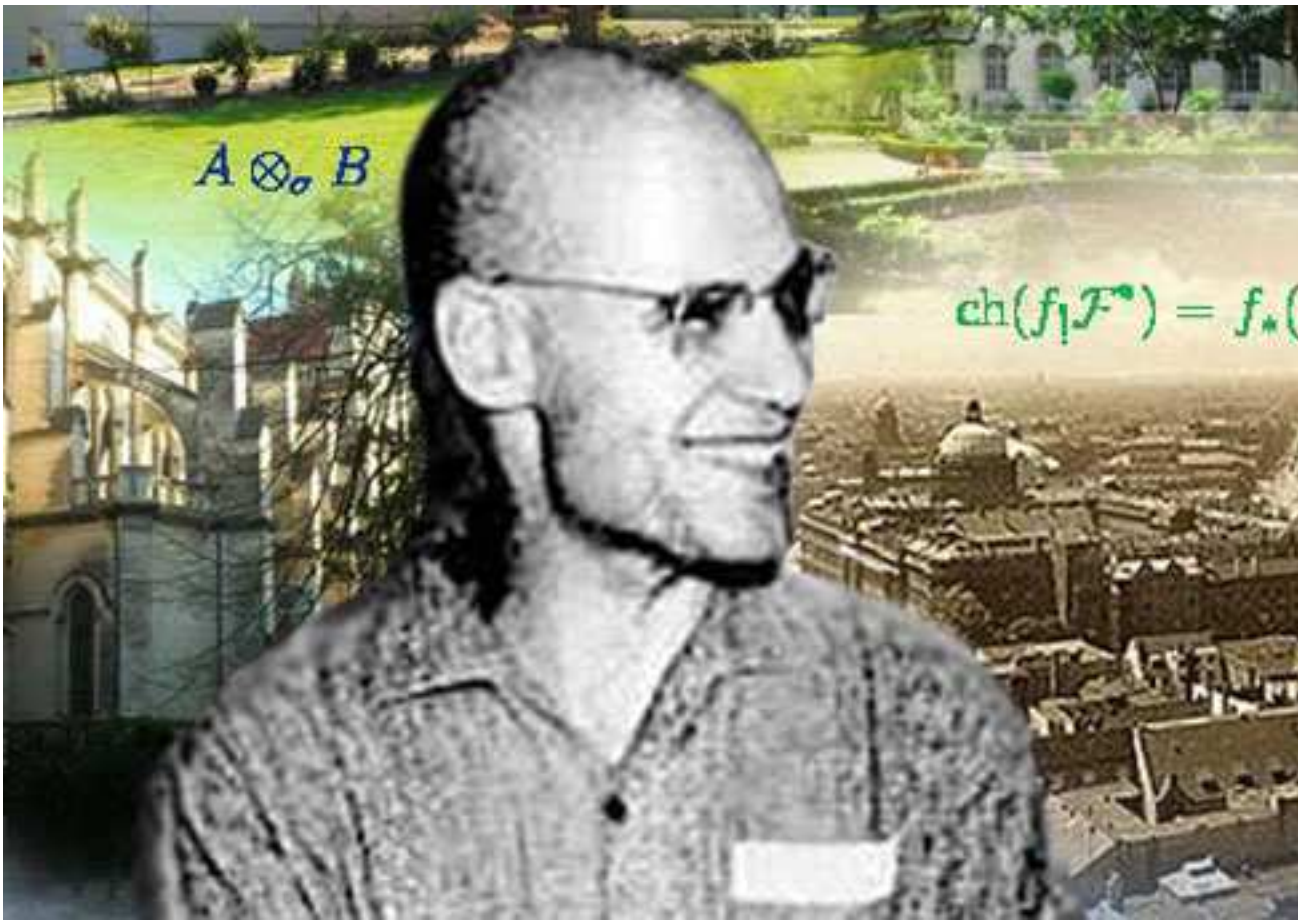
4 Curves and Galois Representations

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

4.1 Schemes

A scheme S consists of a collection of *affine schemes* X , which are "glued together".

An *affine scheme* belongs to a commutative ring R with 1, whose spectrum, i.e. the set of prime ideals becomes a topological space T by the Zariski topology.

The *structure sheaf* $\mathcal{O}_X$ associates to every open set $U \subset T$ the localization $\mathcal{O}_X(U)$ of "holomorphic functions" on U.

The stalk at a point P of T is a local ring $\mathcal{O}_P$ obtained as inductive limit of holomorphic functions at P.

Morphisms between schemes are given piecewise by affine morphisms, which are (local) ring homomorphisms between the structural sheaves.

Notation: $X = \mathrm{Spec}(R)$

Zero-dimensional schemes.

R: commutative noetherian ring with 1 whose prime ideals are maximal.

Examples

1) $R = \mathbb{Z}/n$ with $n \in \mathbb{N}$ (arithmetical prototype).

Points correspond to prime divisors of n.

2)$R = K_0[X]/(f(X))$ where K_0 is a field and $f(X) \in K_0[X] \setminus \{0\}$.

Points correspond to irreducible factors of f.

Caution: X is not determined by its points: $\mathrm{Spec}(\mathbb{F}_p[X]/(X^p - 1))$ is different from $\mathrm{Spec}(\mathbb{F}_p[X]/(X - 1))$.

3) $R = K$ where K is a field, $X = \mathrm{Spec}(K)$.

Curves

Definition 4.1 *A curve $\mathcal{C}$ is a scheme, such that the stalk $\mathcal{O}_P$ in a closed point has Krull dimension 1.*
A point P of $\mathcal{C}$ is regular (= non-singular) iff $\mathcal{O}_P$ is a discrete valuation ring.
$\mathcal{C}$ is regular iff all points of $\mathcal{C}$ are regular.

Case 1: Arithmetical curves: Take O_K as ring of integers in a #-field K.
$\mathrm{Spec}(O_K)$ is a regular affine curve.
$\mathcal{O}_P$ at $P \neq (0)$ is a valuation ring that is uniquely determined by P.
It defines a a prime divisor $\mathfrak{P}$ of K with $\deg(\mathfrak{P}) = \log(|O_K/P|$ and with normalized valuation $v_{\mathfrak{P}}$.
The restriction of "functions" to P is the reduction modulo $\mathfrak{P}$.

Case 2: Geometric projective curves.

Let K_0 be a *perfect* field with algebraic closure $\overline{K_0}$ and (absolute) Galois group $G_{K_0} := \mathrm{Aut}_{K_0}(\overline{K_0})$.

An irreducible *projective* curve $\mathcal{C}$ over K_0 is a scheme of dimension 1 over $\mathrm{Spec}(K_0)$ embedded in $\mathbb{P}^n/K_0$ as (projective) zero set (over $\overline{K_0}$) of a homogeneous prime ideal $I_{\mathcal{C}} \subset K_0[X_0, \ldots, X_N]$.

A typical open subscheme is an *affine part*

$$\mathcal{C}_S = \mathcal{C} \setminus S$$

where $S \subset \mathcal{C}(\overline{K_0})$ is finite and G_{K_0}-invariant.

$\mathcal{O}(U) := O_S$ is the ring functions without poles outside of S. It is an integral domain, and its quotient field is independent of the choice of S:
It is the function field $K_{\mathcal{C}}$ of $\mathcal{C}$.

We assume that $\mathcal{C}$ is projective irreducible and regular.
Fact: Galois orbits of points in $\mathcal{C}(\overline{K_0})$ correspond one-to-one to equivalent classes of valuations of $K_{\mathcal{C}}$, which are trivial on K_0.

Definition 4.2 *A prime divisor* $\mathfrak{P}$ *of* $\mathcal{C}$ *is a Galois orbit of a point* $P \in \mathcal{C}(\overline{K_0})$.
The number of points in this orbit is the degree $\deg(\mathfrak{P})$.

Arithmetical Surfaces

Let K be a number field and denote by $\mathcal{S}$ the curve corresponding to O_K.

Let $\mathcal{C}_K$ be a projective curve over K. By "clearing denominators" we can extend $\mathcal{C}_K$ to a scheme $\mathcal{C}$ over $\mathcal{S}$.

$\mathcal{C}$ is two-dimensional and hence a *surface* with curves as *fibers* over $\mathrm{Spec}(O_K)$.

The generic fiber is $\mathcal{C}_K$, for maximal ideals $P \subset O_K$ we get the reduction curve $\mathcal{C}_P$ over a finite field which may be neither regular nor irreducible but connected and projective.

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).

4.2 Fundamental Groups

One of Grothendieck's most seminal ideas is the **fundamental group** attached to a

Grothendieck topology.

Here neighborhoods in usual topologies are replaced by covers with special algebraic properties.
We can consider here only and very superficially the special case of the Etale Topology: For a schema $\mathcal{X}$ the neighborhoods are étale covers

$$\mathcal{Y} \to \mathcal{X}.$$

Projective limites give "universal covers" and fundamental groups Π_1 as projective limites of automorphisms.

Examples:

1. For a field K étale covers are separable algebraic extensions, the universal cover is K_s and the fundamental group is G_K.
2. For the curve attached to O_K étale covers are unramified ring extensions, and the universal cover has as quotient field the maximal unramified extension of K.
3. Let $\mathcal{C}_{|K_0}$ be a curve.
   Since K_0 is perfect constant field extensions are étale, and so

   $$1 \to \Pi_1(\mathcal{C}_{|\overline{K_0}}) \to \Pi_1(\mathcal{C}) \to G_{K_0} \to 1$$

   is exact.
   Hence we have a representation
   $\rho_{\mathcal{C}} : G_{K_0} \to \mathrm{Out}(\Pi_1(\mathcal{C}_{|\overline{K_0}}))$.

The exact sequence above is the starting point of the Anabelian Geometry (also due to Grothendieck).
It is interesting that we can define the genus $g_{\mathcal{C}}$ of $\mathcal{C}$ "via topology":
Let $0 \leq p = \mathrm{char}(K_0)$ and let $\Pi_1(\mathcal{C}_{|\overline{K_0}})'$ be the maximal quotient of $\Pi_1(\mathcal{C}_{|\overline{K_0}})$ with order (as profinite group) prime to p. Then classical theory of compact Riemann surfaces and liftings theorem due to Grothendieck/Serre yield that $\Pi_1(\mathcal{C}_{|\overline{K_0}})'$ is the quotient of a finitely generated free profinite group with $g_{\mathcal{C}}$ generators modulo one commutator relation.
Hence for primes ℓ different from p the maximal abelian pro-ℓ -quotient $\Pi_1(\mathcal{C}_{|\overline{K_0}})_\ell$ of $\Pi_1(\mathcal{C}_{|\overline{K_0}})'$ is isomorphic to $\mathbb{Z}_\ell^{2g_{\mathcal{C}}}$.
So one gets

4. ℓ-adic Galois representations.
   Let $\mathcal{C}$ be a projective regular curve of genus $g_{\mathcal{C}}$. Then $\rho_{\mathcal{C}}$ induces an ℓ-adic representation

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

Remark 4.3 *Generalizing the last example leads to the* ***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" an étale cohomology group of a smooth projective variety.*

In the next section we shall construct groups attached to curves, which give, amongst other things, representations spaces for $\widetilde{\rho}_{\ell\mathcal{C}}$.

4.2.1 Example: Elliptic Curves

Definition 4.4 *An elliptic curve $\mathcal{E}$ over K_0 is a projective regular curve of genus 1 with at least one K_0-rational point.*

It follows that $\Pi_1(\mathcal{E}_{|\overline{K_0}})'$ is a profinite free abelian group with two generators, and that

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

is a two-dimensional Galois representation.

Now assume that K_0 is algebraically closed.
Going to finite quotients of $\Pi_1(\mathcal{E})'$ it follows that every finite unramified cover

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

is abelian, and by the Hurwitz genus formula (well known for Riemann surfaces) it follows that C' has again genus 1, and since K_0 is algebraically closed, is an elliptic curve.
What happens if K_0 is not algebraically closed?
We shall come to this question in the frame of modular curves.

4.3 The Picard Functor of Curves

Let $\mathcal{C}$ be a regular projective curve.

Definition 4.5 • *The group of divisors* $\mathcal{D}_{\mathcal{C}}$ *is the free abelian group generated by the set of prime divisors of* $\mathcal{C}$.

- *For* $D = \sum z_{\mathfrak{P}} \cdot \mathfrak{P}$ *define*

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

- *For* $f \in K_{\mathcal{C}}^*$ *define*

$$(f) = \sum_{\mathfrak{P}} v_{\mathfrak{P}}(f) \cdot \mathfrak{P} \in \mathcal{P}_{\mathcal{C}}.$$

- $\mathcal{P}_{\mathcal{C}}$ *is a subgroup of the group* $\mathcal{D}_{\mathcal{C}}^0$ *of divisors of degree* 0.

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

  is the group of divisors classes of degree 0.

4.4 Tate modules of Picard groups

G_{K_0} operates on $\mathrm{Pic}^0_{\mathcal{C}_{|\overline{K_0}}}$.

From classical geometry over $\mathbb{C}$ and comparison theorems we get

$$\mathrm{Pic}^0_{\mathcal{C}_{|\overline{K_0}}}[\ell^n] \cong (\mathbb{Z}/\ell^n)^{2g_{\mathcal{C}}}.$$

Fact: $\mathrm{Pic}^0_{\mathcal{C}_{|\overline{K_0}}}[\ell^n]$ is as G_{K_0}-module isomorphic to $\Pi_1(\mathcal{C}_{|\overline{K_0}})_\ell/\ell^n$.

Definition 4.6 *The Tate module $\mathcal{T}_{\mathcal{C},\ell}$ is the G_{K_0}- module*

$$\varprojlim_n \mathrm{Pic}^0_{\mathcal{C}_{|\overline{K_0}}}[\ell^n].$$

Theorem 4.7 *$\widetilde{\rho}_{\ell\mathcal{C}}$ is 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 representation module $\mathrm{Pic}^0_{\mathcal{C}_{|\overline{K_0}}}[\ell^n]$.*

4.5 Addition in Picard Groups

Recall: If $\mathcal{C} = O_K$ is an arithmetic curve the addition in ideal classes is, in theory and practice, governed by the Theorem of Minkowski: In every ideal class is an integral ideal with small norm.
The analogous result equally fundamental for the arithmetic of *projective* curves $\mathcal{C}$ over K_0 is the

Theorem of Riemann-Roch.

We formulate a consequence:

Theorem 4.8 *Assume that $\mathcal{C}$ has a K_0-rational point P_∞ with corresponding prime divisor $\mathfrak{P}_\infty$.*
In every divisor class $c \in \mathrm{Pic}^0_{\mathcal{C}}$ there is a divisor

$$D_c = \sum n_{\mathfrak{P}} \mathfrak{P} - g_{\mathcal{C}} \cdot \mathfrak{P}_\infty \text{ with } n_{\mathfrak{P}} \geq 0.$$

Corollary 4.9 *If K_0 is a finite field then Pic^0_C is a finite abelian group.*

Hence we can represent two divisor classes c_i $(i = 1, 2)$ by divisors

$$D_i = \sum n_{\mathfrak{P}}^{(i)} \mathfrak{P} - g_{\mathcal{C}} \cdot \mathfrak{P}_\infty$$

and so the sum $c_1 \oplus c_2$ by

$$\sum_{i=1,2} (\sum n_{\mathfrak{P}}^{(i)} \mathfrak{P}) - 2g_{\mathcal{C}} \cdot \mathfrak{P}_\infty.$$

The explicit addition boils down to the task:

Find a function $f \in K_0(\mathcal{C})$ such that

$$\sum_{i=1,2} (\sum n_{\mathfrak{P}}^{(i)} \mathfrak{P}) - 2g_{\mathcal{C}} \cdot \mathfrak{P}_\infty =$$

$$(f) + \sum n_{\mathfrak{P}} \mathfrak{P} - g_{\mathcal{C}} \mathfrak{P}_\infty.$$

(Reduction step)

4.5.1 Example

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

$$E : Y^2Z + a_1YXZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

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 $(E(K_0), \oplus)$ and we remark that, after having fixed $\mathfrak{P}_\infty$, for every $L \supset K_0$ the set $\mathcal{E}(L)$ is an abelian group with neutral element $\mathfrak{P}_\infty$.

Explicitly: 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

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

Hence the addition is given by polynomial functions, and $\mathcal{E}$ has the structure of an Abelian variety of dimension 1.
More general: Abelian varieties $\mathcal{A}$ are absolutely irreducible regular projective varieties with a group scheme structure, i.e. they are equipped with an addition morphism

$$m : \mathcal{A} \times \mathcal{A} \to \mathcal{A}$$

such that the group axioms are satisfied.
Very important examples of Abelian varieties are Jacobian varieties $\mathcal{J}_\mathcal{C}$ of curves $\mathcal{C}$ representing Pic^0.

Homomorphisms

$$\eta : \mathcal{A}_1 \to \mathcal{A}_2$$

between abelian varieties are morphisms compatible with m

η is an isogeny and $\mathcal{A}_1$ is isogenous to $\mathcal{A}_2$ if η is (geometrically) surjective and has finite kernel

$$\ker(\eta) := \eta^{-1}(\{\mathcal{O}_{\mathcal{A}_2}\}).$$

It is a group scheme of dimension 0 of order $\deg(\eta)$.

η is separable or étale iff $|\ker(\eta)(\overline{K_0}| = \deg(\eta)$.

If so, then η is defined over K_0 iff $\ker(\eta)$ is invariant under G_{K_0}.

4.6 Modular Curves

Take K_0 arbitrary.
For $N \in \mathbb{N}$, prime to $\mathrm{Char}(K_0)$ and $L \supseteq K_0$ define the functor

$$L \to \{(E, \eta_N)/\cong\}$$

with $\mathcal{E}$ an elliptic curve over K_0 and η_N an isogeny of E with cyclic kernel of order N defined over L.
This 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 represents $\mathcal{F}_N$ over $\mathbf{C}$.

By general principles,
$X_0(N)$ is defined over $\mathrm{Spec}(\mathbb{Z})$ and represents $\mathcal{F}_N$ over $\mathbb{Z}[1/N]$.
$X_0(N)$ has a very rich algebraic and analytic structure used to prove Theorem 1.2.

5 A Excursion to Global Fields

5.1 Faltings' Proof of Mordell' Conjecture

Recall: A representation ρ is semi-simple iff it is, up to isomorphy, uniquely determined by the characteristic polynomials of the images of ρ. Let $\mathcal{C}$ be a projective irreducible curve over a number field K and ℓ a prime number.

Theorem 5.1 ***(Faltings):***
$\widetilde{\rho}_{\ell\mathcal{C}}$ is semi-simple and determines the isogeny class of the Jacobian variety of $\mathcal{C}$.

Work of **Tate and Parshin** imply:

Corollary 5.2 ***(Faltings***
If $g_{\mathcal{C}} \geq 2$ then $|C(K)|$ is finite.

For the proof Faltings used and developed the theory of arithmetic surfaces (including metrics from archimedean places).
A key role is played by the study of special elements of G_K, namely Frobenius automorphisms $\sigma_{\mathfrak{p}}$, which are attached to prime ideals $\mathfrak{p} \subset O_K$ and, a bit vaguely spoken, liftings of the Frobenius automorphism of the finite field $O_K/\mathfrak{p}$.

Theorem 5.3 *(**Chebotarev**): Semi-simple representations of G_K are determined by the characteristic polynomials of Frobenius elements.*

These polynomials are the local factors of the L-series of $\mathcal{C}$. More about their computation tomorrow.

6 Curves over Finite Fields

Now: $K_0 = \mathbb{F}_q$ with $q = p^d$.
Then

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

with short representation of elements.
Recall that the main part of the addition is a reduction step.

Theorem 6.1 ***(F.Heß, C. Diem)*** *Let $\mathcal{C}$ be a curve of genus $g_{\mathcal{C}}$ over $\mathbb{F}_q$.*
The reduction step and hence the addition in $\mathrm{Pic}^0_{\mathcal{C}}$ 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).

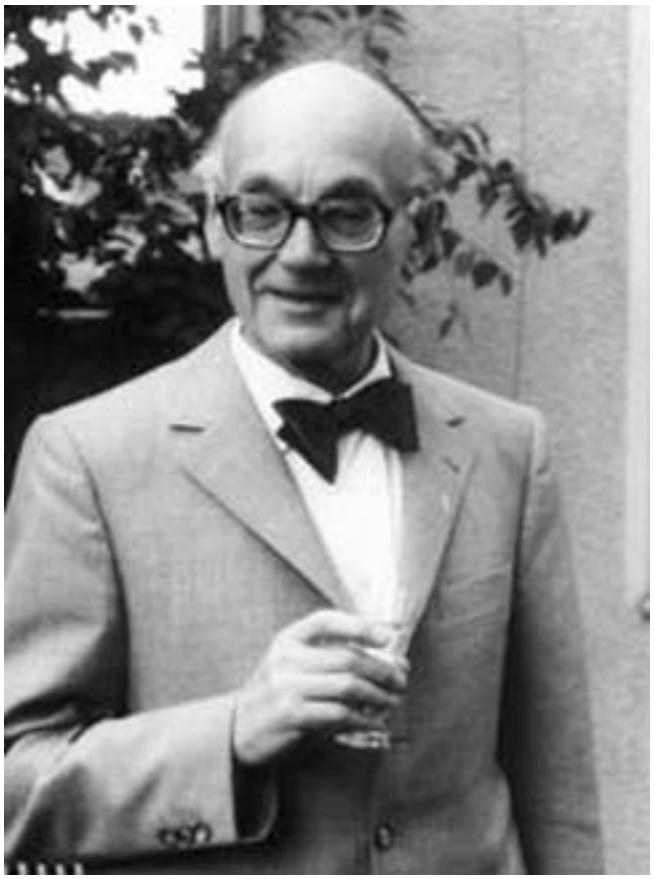
In special cases (e.g. if $\mathcal{C}$ is hyperelliptic) we get even better algorithms, which come near to the algorithms for elliptic curves.

Idea: Use Picard groups of curves as DL - systems!

Conditions 1) and 2) of Task 2.4 are satisfied –**if** one finds curves $\mathcal{C}$, so that $\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)$ contains a large set of prime numbers. To check this one needs a fast algorithm for computing $|\mathrm{Pic}^0_{\mathcal{C}}(\mathbb{F}_q)|$. In general this is unsolved.

But by looking at **security** one sees that for DL-systems, one should only use Picard groups of carefully chosen curves of genus 1 or 2 (and very restricted) curves of genus 3 over prime fields. **Keywords for attacks: Index-Calculus, Weil Descent**.

For the surviving curves we have methods to construct cryptographically interesting Picard groups. (More details in the lecture tomorrow.)



Max Deuring 1973

7 Isogenies of Elliptic Curves over Finite fields

In the following $\mathcal{E}$ and similar letters stand for elliptic curves over finite fields $\mathbb{F}_q$.

Basic for the arithmetic of $\mathcal{E}$ are isogenies

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

Etale isogenies can be decomposed into a chain of scalar multiplications and isogenies with cyclic kernel of prime order ℓ with ℓ a prime $\neq p$. As remarked, these latter ones belong to points on the modular curve $X_0(\ell)$.

Classical theory of elliptic functions and work of Deuring lead to an explicit equation for an affine model of $X_0(N)$ given by the classical modular polynomial $\phi(j, j_N)$.

Deurings work implies beautiful theoretical results, in particular one finds a close connection between elliptic curves over finite fields and class field theory of imaginary quadratic fields.

Theorem 7.1 *Assume that either* $q = p$ *or that* $\mathcal{E}(\overline{\mathbb{F}_q}[p] \neq \{0\}$ *(i.e.* $\mathcal{E}$ *is not supersingular). Then* $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E})$ *is an order* $\mathcal{O}$ *in an imaginary quadratic field, and the isomorphism classes* $\mathcal{S}_{\mathcal{E}}$ *of elliptic curves* $\mathcal{E}'$ *with endomorphism ring* $\mathcal{O}$ *form a principal homogeneous space with group* $\mathrm{Pic}_{\mathcal{O}}$.
If $\mathcal{E}$ *is supersingular and* $\mathbb{F}_q \supseteq \mathbf{F}_{p^2}$ *then* $\mathrm{End}_{\mathbb{F}_q}(\mathcal{E})$ *is an explicitly given maximal order in a Quaternion algebra.*

Next we state algorithmic results.

- The complexity of the computation of an isogeny of degree ℓ (as function and with explicit equation of the image curve) is

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

- Assume that $\mathcal{E}$ and $\mathcal{E}'$ have a commutative endomorphism ring $\mathcal{O}$.
To find an isogeny between $\mathcal{E}$ =and $\mathcal{E}'$ can be done with (expected)

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

bit-operations(due to **Kohel, Galbraith, Hess, Smart et al.**).

Surprise: Quantum Computing changes the complexity for finding an isogeny from exponential (in $\log(q)$) to subexponential.
The reason is that one can apply the hidden shift algorithms for the action of $\mathrm{Pic}_{\mathcal{O}}$ on $\mathcal{S}_{\mathcal{E}}$.

7.0.1 The Frobenius Endomorphism

The absolute Galois group $G_{\mathbb{F}_q}$ is topologically generated by the Frobenius automorphism $Frob_q$ with

$$\mathrm{Frob}_q(x) = x^q.$$

$Frob_q$ acts on the coordinates of point of $\mathcal{E}(\overline{\mathbb{F}_q})$ and so gives rise to a **geometric object**, the isogeny

$$\phi_q : E \to E \in \mathrm{End}(E),$$

which is purely inseparable of degree q.
Its ℓ-adic characteristic polynomial (as endomorphism) is equal to the characteristic polynomial $\chi_{\mathcal{E},\ell}(T)$ attached to the ℓ-adic Galois representation of Frob_q.

Theorem 7.2 *(**Hasse, Deuring, Weil, Tate**) There is a monic polynomial $\chi_{\mathcal{E}}(T) \in \mathbb{Z}[T]$ of degree 2 such that for all n prime to p we have*

1. $\chi_{\mathcal{E},n}(T) \equiv \chi_{\mathcal{E}}(T) \mod n$
2. *For all ℓ different from p we have*
$$\chi_{\mathcal{E}}(T) = \chi_{\mathcal{E},\ell}(T).$$
3. *The zeros of $\chi_{\mathcal{E}}(T)$ are algebraic integers with absolute value $q^{1/2}$.*
4. ***Tate**: $\chi_{\mathcal{E}}(T)$ determines $\mathcal{E}$ up to isogeny.*

Note: If $\tilde{\mathcal{E}}$ is an elliptic curve defined over a number field K such that $\mathcal{E}$ is the reduction modulo $\mathfrak{p}$ of $\tilde{\mathcal{E}}$ then the local factors of the $L-series$ of $\tilde{\mathcal{E}}$ belong to $\chi_{\mathcal{E},\ell}(T)$.

8 Application to Key Exchange

We close the gap for using elliptic curves for DL-systems.

8.1 Point Counting by AES

$\phi_q - id$ is separable and has kernel $\mathcal{E}(\mathbb{F}_q)$, hence

$$|\mathcal{E}(\mathbb{F}_q)| = \chi_{\mathcal{E}}(1) = q+1-Trace(\phi_q) \leq 2\sqrt{q}.$$

Compute $\chi_{\mathcal{E}}(T)$ by the action of Frob_q on $\mathcal{E}[n]$ (cf. Theorem 7.2) for small n and then use CRT (**Schoof**) (polynomial complexity but but too slow in practice.)

Idea of Atkin-Elkies: Use cyclic isogenies instead of points.

Theorem 8.1 ***(SAE)***
$|E(\mathbb{F}_q)|$ can be computed (probabilistically, with GRH) with complexity $\mathcal{O}((\log q)^4)$.

Conclusion We 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 an instance with security level of AES128.
So nowadays we are in a very comfortable situation.
But what about future with quantum computers ?

8.2 Post Quantum Crypto with Elliptic curves

We go away from DL-systems and use first $G - sets$.

1. The system of Couveignes-Stolbunov uses the set $\mathcal{S}_{\mathcal{E}}$ of a non-singular elliptic curve $\mathcal{E}$ with $\mathrm{Pic}_{\mathcal{O}}$ as G-set.
   The security is at most subexponential (not so bad!), but in even the most sophisticated versions the key exchange is very slow.
2. The system of Castryck et.al uses isogeny classes over $\mathbb{F}_p$ of a supersingular curve $\mathcal{E}$ over $\mathcal{F}_p$ with action of $\mathrm{Pic}_{\mathcal{O}}$ with $\mathcal{O} \subset \mathbb{Q}(\sqrt{-p})$.
   The security is again subexponential but the system needs only small key sizes and is very fast.

To come to exponential security **De Feo and Jao** went one step further and used supersingular elliptic curves over $\mathbf{F}_{p^2}$. Their key-exchange scheme needs only small key sizes and is much faster than the method of Couveignes-Stolbunov (but seemingly slower than the Castryck scheme).

It is most conveniently described in the categorical setting for Diffie-Hellman key exchange, and we shall describe it in more detail in tomorrows lecture.

For today:

THANK YOU VERY MUCH!

FLT The proof of FLT in five lines:

Take A, B, C with $A^p - B^p = C^p$.

$E : Y^2 = X(X - A^p)(X - B^p)$.

$G_{\mathbb{Q}}$ acts on $E[p]$ and induces ρ.

By [KWK] ρ comes from $\mathrm{Pic}^0_{X_0(2)}[p]$.

Since $X_0(2) \cong \mathbb{P}^1$ we get a Contradiction!