Elliptic Curves: Facts, Conjectures and Applications

Gerhard Frey
Institute for Experimental Mathematics
University of Essen
e-mail: frey@iem.uni-due.de
ECC 2010
Seattle

1 Prelude

Problems:

1. **Kronecker's Dream:**
   Let K be a field. Construct all abelian extensions in an explicit way!
2. **Number Theorist's Challenge:**
   Decide whether a number is a prime, if not, find prime factors, and do it quickly!
3. **Diffie-Hellman's Demand:**
   Find a large finite group with fast addition and hard Discrete Logarithm!

PART I. The Time before ECC

2 A Little History of Great Ideas, before 1985

- about 9×25 years ago C.F. Gauß starts his career and, during the next 10 years
  - makes experiments and discovers the prime number theorem
  - studies theoretically and practically elliptic curves and functions (key word: lemniscate) in the special case of the arc length on the *lemniscate*

    $$r^2 = cos(2\varphi)$$

    as elliptic integral

    $$\int_0^w \frac{1}{\sqrt{1-r^4}} dr,$$

  - defines and computes AGM.

- defines the "INDEX" of elements in finite fields (we say today: DL)
- begins with the theory of function fields over finite fields and states the first non-trivial example for the "Riemann hypothesis" (nearly forgotten Chapter VII of Disquisitiones Arithmeticae)

and does many other things, too.

- about 7×25 years ago C.G. Jacobi computes tables for indices for numbers ≤ 100 and primes < 1000
- about 5×25 years ago Kronecker had a Jugendtraum: realize abelian extensions of number fields by special values of transcendental functions and

- Frobenius proved a predecessor (density of primes with given decomposition type) of Čebotarev's density theorem (proved 1922)
- about 4×25 years ago Weber published the third volume of ALGEBRA

- about 3×25 years ago
  - E.Noether studied $Pic(O)$, developed ideal theory (commutative algebra) and her student Grete Herrmann developed effective (computational) ideal theory (theoretically)
  - Deuring and Hasse studied elliptic curves over finite fields and relations with classical theory (CM-theory). As result Hasse proved the Riemann hypothesis for elliptic curves over finite fields. This was "the begin of MODERN ARITHMETIC GEOMETRY"

– 2×25 years ago: kind of explosion!

– Grothendieck's monumental work on Arithmetic Geometry and in particular about Galois Theory: Schemes, Fundamental groups, étale and rigid cohomology, motives, relation with L-functions....
Collection: Dix Exposés sur la cohomologie des schemas

– Tate: Duality theorems

– Néron-Tate: Heights on abelian varieties

– Eichler-Shimura congruence Relation between modular forms, Galois representations (Eichler-Shimura congruence emerging) and elliptic curves (abelian varieties)

- Birch and Swinnerton-Dyer: using the insights from above, **and** massive computing with EDSAC computer state BSD for elliptic curves (Crelle's Journal 1963,1965) which turned out to be amongst the most seminal mathematical publications of all times.
  More conjectures emerged, all relying on the interplay of Galois Theory and analytic L-series:
- Tate-Sato Conjecture
  As precision, and a little later:
- The Lang-Trotter conjecture (1976)

Things culminated in the 70's (we are leaving our 25-years slots).
A high point was the Conference on Modular Forms in Antwerp 1972.
From now on arithmetic of modular forms, of Galois representations and of varieties over global fields interacted strongly.

For example: Around this time the Conjecture of Serre was stated in a vague form: Two dimensional odd representations over finite fields are attached to modular forms. This conjecture generalizes the Taniyama-Shimura conjecture enormously.

A golden age of arithmetic geometry could begin.

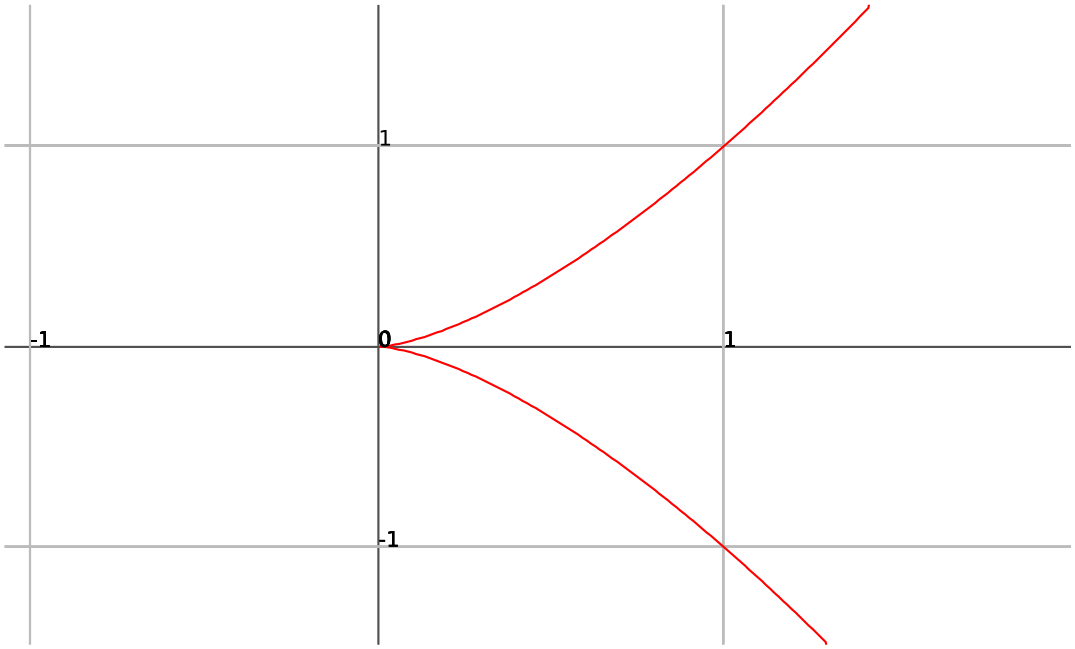
3 The Geometric Players

We want to come nearer to the tasks in the prelude by using ***arithmetic properties of geometric objects***.
We begin with the easiest geometric objects: rational curves, i.e. curves that are (maybe after a finite field) isomorphic to the projective line minus some points.

4 Plane Cubic Curves of Genus 0: $\mathbb{P}^1$ with Holes

4.1 The Additive Group as Cubic

$$Y^2Z = X^3.$$



is a plane projective curve with one singular point $(0, 0, 1)$ which is a *cusp*.

$$t \mapsto (t^{-3}, t^{-2}, 1); t \neq 0;\ 0 \mapsto (0, 1, 0)$$
$$0 \mapsto (0, 1, 0)$$

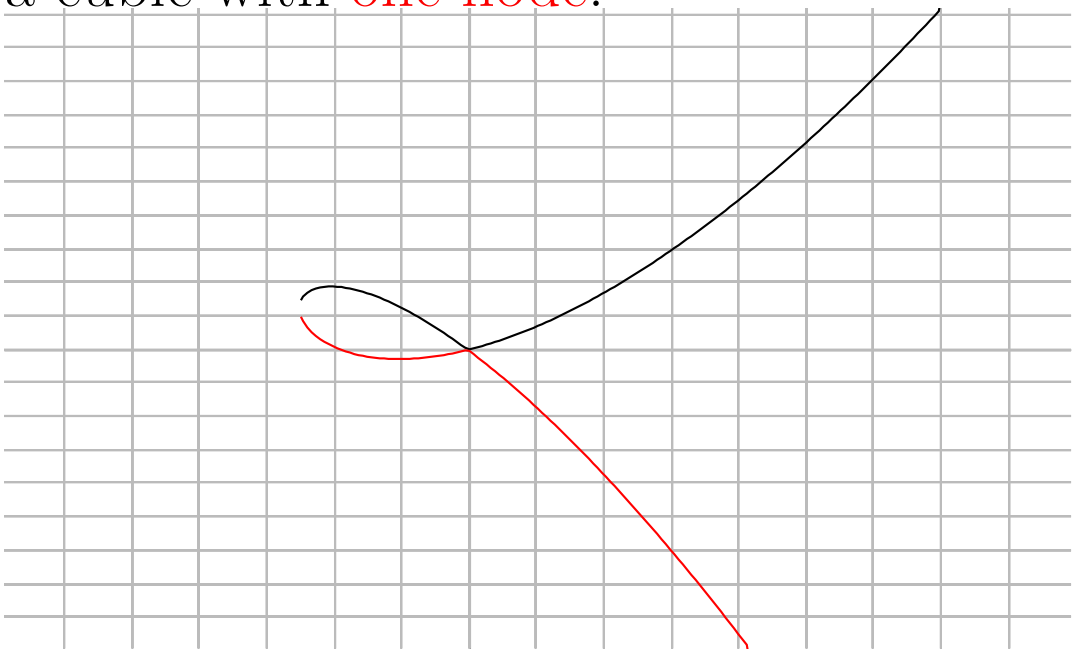
is an isomorphism from G_a to E_a^{reg}.
Exercise: Describe $+$!

4.2 The Multiplicative Group as Cubic

Take

$$E_m : Y^2Z + XYZ = X^3,$$

a cubic with one node.



By

$$u \mapsto (\frac{u}{(1-u)^2}, \frac{u^2}{(1-u)^3}) \text{ for } u \neq 1; 1 \mapsto (0,1,0)$$

we get an isomorphism from G_m to E_m^{reg}.
Again: Describe multiplication geometrically!

4.3 Applications of G_m

The Jugendtraum became true over $\mathbb{Q}$.

Theorem 1 ***(Kronecker-Weber)***

$$\mathbb{Q}^{ab} = \mathbb{Q}(G_m(\mathbb{Q}_s)_{tor})$$

and hence is generated by values of exp.

Characters of $G_{\mathbb{Q}}$ were studied successfully.
One spectacular result:
Kummer: Fermat's Last Theorem is true for regular primes (but there are infinitely many non-regular primes).

Prime number tests as well as algorithms for factoring numbers were developed (using $(\mathbb{Z}/p)^*$) but they are not as effective as desirable,
and the computation of discrete logarithms by index-calculus methods goes back at least to 1922.
Reasons for "Failure":

- Using $\mathbb{P}$ one finds (essentially) only G_a (which is good for Artin-Schreier-theory in characteristic $p > 0$) and G_m as algebraic-geometric objects.
- There are "too many" points on G_m, $\mathbb{Q}^*$ is not finitely generated and contains free subgroups of large rank(*"smooth" numbers*).

5 Elliptic Curves

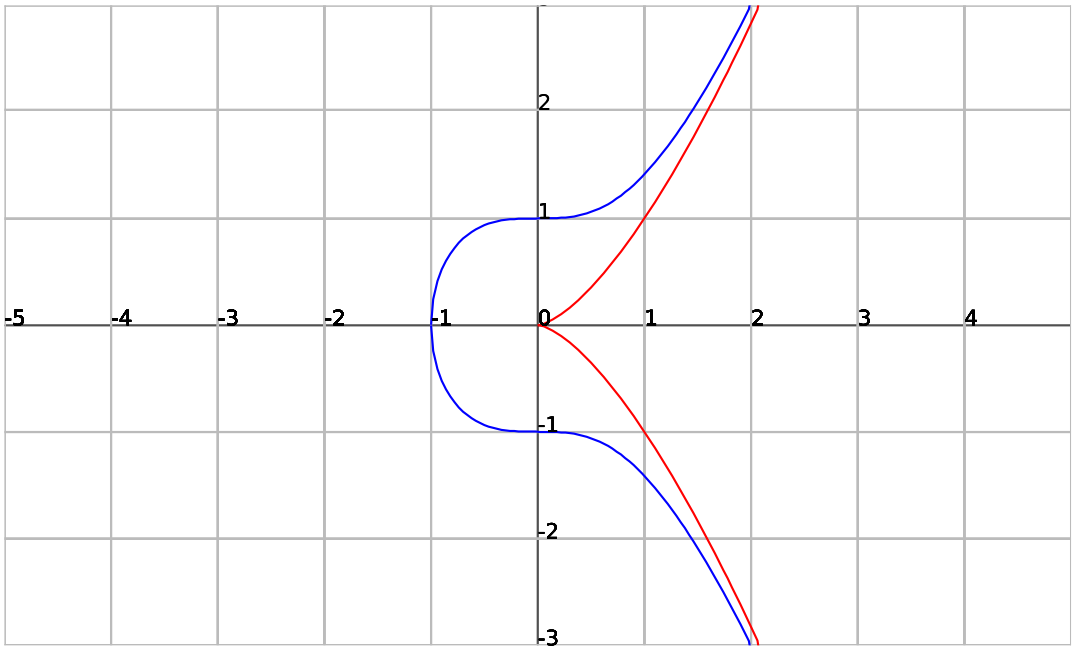
5.1 A Small Deformation Changes the World

We change the projective curves defining G_a and G_m a little bit:

$$Y^2Z = X^3$$

$$\mapsto$$

$$Y^2Z = X^3 + Z^3$$

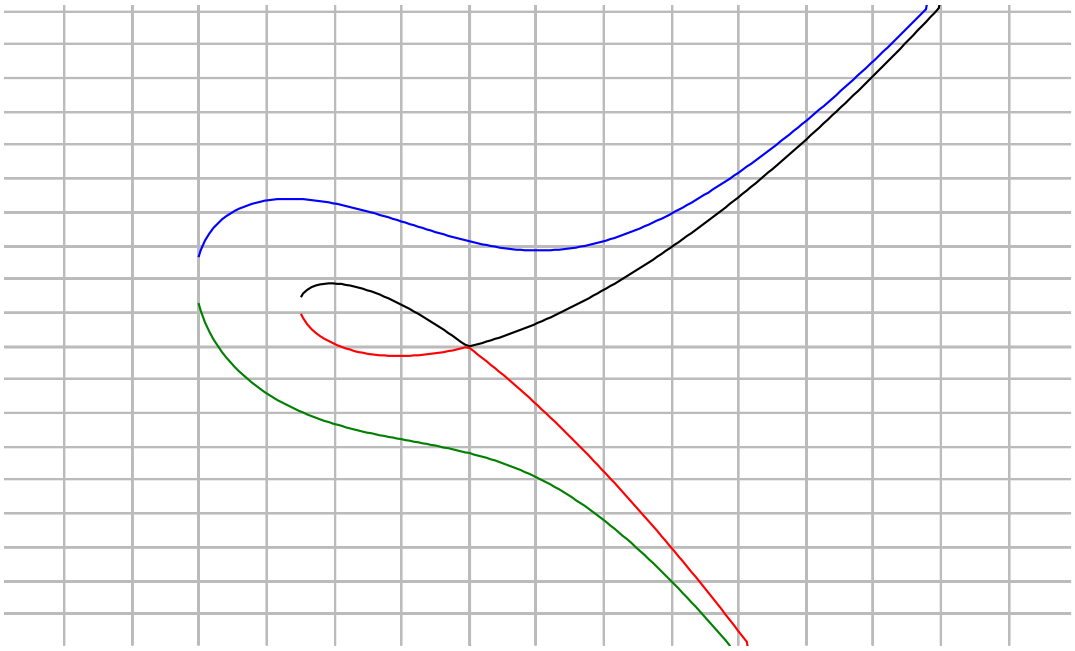


and

$$Y^2Z + XYZ = X^3$$

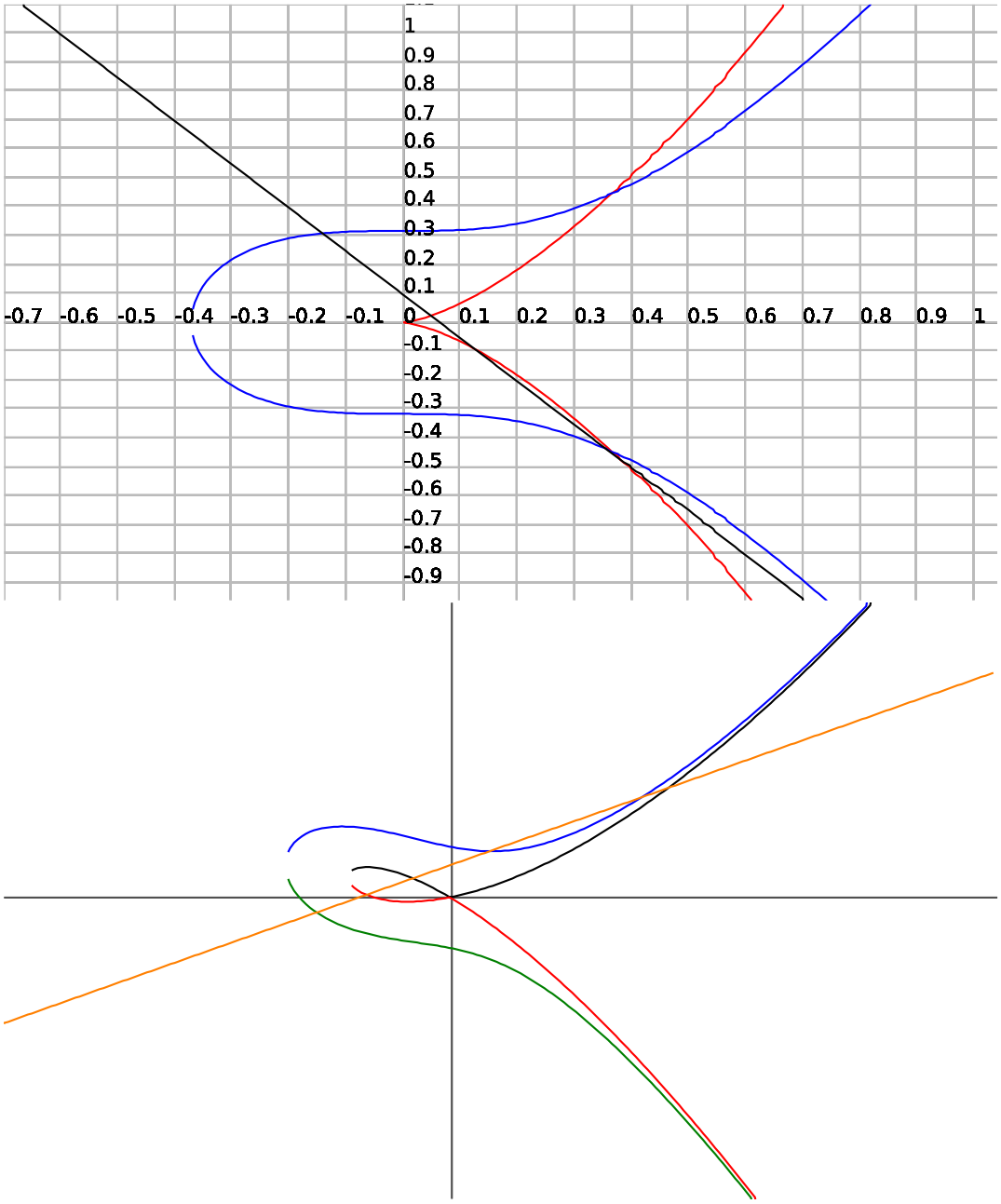
$$\mapsto$$

$$Y^2Z + XYZ = X^3 + Z^3$$



The singular points have vanished. The result is a plane regular projective cubic E.

We still can look at the geometric addition laws


1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
-0.7 -0.6 -0.5 -0.4 -0.3 -0.2 -0.1 0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1
-0.1
-0.2
-0.3
-0.4
-0.5
-0.6
-0.7
-0.8
-0.9

We note

- Composition makes sense for all pairs of points on the deformed curves.
- It is not difficult to give formulas for the composition.

Fact: E is a **connected projective** algebraic group of dimension 1.

Definition 5.1 *An elliptic curve E over a field K is a projective absolutely irreducible group scheme of dimension 1 defined over K, i.e. E is an abelian variety of dimension 1 over K.*

There are two big and obvious differences to the cubics with singular points:
Elliptic curves are projective and hence compact (in many senses), and there are "many" non-isomorphic elliptic curves.
In fact, the isomorphy class of E is, over K_s, determined by an element $j_E \in K$, the absolute invariant, and for every $j \in K$ there is an E with $j_E = j$.
Over K one needs in addition a (usually quadratic) character to determine the class of E. Every elliptic curve E can be given as plane cubic with Weierstraß equation

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

If char(K) $\neq 2$ we can assume that $a_1 = 0 = a_3$.
If char(K) prime to 6 we can assume in addition that $a_2 = 0$.

We get the short Weierstraß form

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Conversely

$$Y^Z + a_1XYZ + a_3YZ^2 =$$

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

defines an elliptic curve iff it has no singular points, i.e. there is no point on the curve (over the separable closure K_s of K) at which all partial derivatives vanish simultaneously, i.e. the discriminant $\Delta_E \neq 0$. If $\Delta_E = 0$ then the corresponding curve is (possibly after a quadratic extension of K) projectively isomorphic to G_a or G_m.

5.2 Addition Laws

Following the geometric picture above (and using Riemann-Roch theorem) it is an easy **Exercise** to write down ADDITION FORMULAS!

Remark 5.1 *We emphasize that the presentation of elliptic curves by Weierstraß equations is only one of many possibilities. It may be of theoretical or practical importance to choose other presentations, such as*

- *intersections of two quadrics in* $\mathbb{P}^3$
- ***Legendre*** *normal form (needed: rationality of points of order 2)*
- ***Hessian*** *form (rationality condition for flex points)*
- *quartic plane projective curve with rational singularity: "**Edwards Curves**".*

5.3 Torsion Structures

$0 \geq p = \mathrm{char(K)} \neq \ell \in \mathbb{P}$. K a field with separable closure K_s, absolute Galois group G_K and algebraic closure $\overline{K}$.

Definition 5.2 *For $n \in \mathbb{N}$ define the group scheme of n-torsion points of E by*

$$E[n] = \{P \in E(\overline{K});\ n \cdot P = O\} = ker(n \cdot id_E).$$

Facts 1

- *If $n = p^s$ then $E[p^s] = (\mathbb{Z}/p^s)^\delta$ with $\delta \in \{0, 1\}$.*
  $\delta = 0$: E supersingular, else ordinary.
- *If n is prime to p then $E[n] \subset E(K_s)$ and, as abelian group, $E[n]$ is isomorphic to $\mathbb{Z}/n \times \mathbb{Z}/n$.*
- *For $gcd(n, p) = 1$ $E[n]$ induces a 2-dimensional Galois representation $\rho_{E,n}$ over the ring $\mathbb{Z}/n$.*

- $$T_\ell(E) := proj - lim_{k\in\mathbb{N}} E[l^k]$$
  is the ℓ-adic Tate module of E.
  It is a free $\mathbb{Z}_\ell$-module of rank 2.
  G_K acts on $T_\ell(E)$ continuously with respect to the pro finite topology and induces the 2-dimensional ℓ-adic representation $\tilde{\rho}_{E,\ell}$. In a highbrow language: $T_\ell(E)$ is the first ℓ-adic étale cohomology group of E and $\tilde{\rho}_{E,\ell}$ is the attached ℓ-adic representation.
- *Let $End_K(E)$ be the ring of endomorpisms of E, and $End_K(E)^0 := End_K(E) \bigotimes \mathbb{Q}$.*
  $End_K(E)^0$ is a skew field (since E is a simple abelian variety) and by the action on $T_\ell(E)$, it is embedded into $M(2, \mathbb{Q}_\ell)$.
  Hence it is either equal to $\mathbb{Q}$ or is a quadratic field or a quaternion field.

5.3.1 Comparison with Rational Curves

For n prime to p then $G_m[n] = \mu_n =< \zeta_n >$ is isomorphic as abelian group to $\mathbb{Z}/n$. with ζ_n a primitive root of unity of order n.
G_K acts on μ_n and induces a one-dimension representation, the *cyclotomic character* :

$$\chi_n : G_K \longrightarrow \mathbb{Z}/n^*$$
$$\sigma \mapsto k_\sigma$$

with

$$\sigma(\zeta_n) = \zeta_n^{k_\sigma}.$$

cyclotomic character

Theorem 2

$$\det(\rho_{\mathrm{E,n}}) = \chi_{\mathrm{n}}.$$

Remark 5.2 *Behind the theorem is the duality of abelian varieties and, applied to torsion points, the Weil pairing.*
It follows that $\rho_{E,n}$ *is* odd.

5.4 Level Structures and Modular Curves

Definition 5.3 *Take n prime to p*

$$\alpha : E[n] \xrightarrow{\cong} \mathbb{Z}/n \times \mathbb{Z}/n$$

is a level-n-structure of E.

The **moduli problem**: "Classify isomorphy classes (E, α) of elliptic curves E with level n-structure α" is represented by the modular curve $X(n)$. Interesting subcovers:
Classify elliptic curves with a fixed point of order n: $X_1(n)$, and
Classify elliptic curves with a fixed cyclic subgroup of order n: $X_0(n)$.

To be more precise:
The moduli problem (E, α) is representable by a fine moduli space over (to avoid complications) $\mathbb{Z}[1/n, \zeta_n]$ which is the modular curve $X(n)$. (For experts: to get an irreducible curve one has to fix the determinant of α, e.g. take canonical level-n-structures.)
This means: For algebras R over $\mathbb{Z}[1/n, \zeta_n]$the set $X(n)(R)$ parameterizes the pairs of elliptic curves with level-n-structures rational over R.
$Gl(2, \mathbb{Z}/n)$ acts as group of automorphisms on $X(n)$.

To get subcovers take Γ as subgroup of $Gl(2, \mathbb{Z}/n)$ and define a new moduli problem: Classify pairs $(E,$ orbits of $\Gamma)$!
Again we get a moduli space (which may be coarse) by taking $X(n)/U$.
Examples:

$\Gamma_1(n) =:= \{\left(\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right)$ with $b \in \mathbb{Z}/n, d \in \mathbb{Z}/n^*\}$

and

$\Gamma_0(n)) := \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ with $ad \in \mathbb{Z}/n^*, b \in \mathbb{Z}/n\}$.

$\Gamma_1(n)$, $n > 2$ defines to the modular curve $X_1(n)$, a fine moduli space for pairs (E, P) with P a point (section) of order n.
$\Gamma_0(n)$ defines $X_0(n)$ which is a coarse moduli space for pairs (E, C_n), $C_n \subset E[n]$ cyclic of order n.

So elliptic curves (resp. torsion structures) are intimately related to *modular forms*. *Modular elliptic curves* are subcovers of $X_0(n)$: "Elliptic curves create elliptic curves" (**Taniyama-Shimura**).

6 Galois Representations in Arithmetical Environments

6.1 Hierarchy of Fields

The number field K carries various topologies induced by equivalence classes ("places") of valuations v. These valuations extend the p-adic valuations and the absolute value on $\mathbb{Q}$.
For $K = \mathbb{Q}$ they correspond to $\mathbb{P} \cup \{-\log(|.|)\}$.
The completion of K at v is the local field K_v.
If v is an extension of a p-adic valuation then the ring of integers O_K of K is contained in the valuation ring O_v, the residue field is $\mathbb{F}_v =: \mathbb{F}_q$.
For each v we choose an extension to K_s again denoted by v.

G_v consists of elements of G_K acting v-continuously and can be identified with G_{K_v}.

It has a canonical quotient group, the Galois group of the maximal unramified extension of K_v that is canonically isomorphic to $G_{\mathbb{F}_q}$ and topologically generated by the lift of the Frobenius automorphism ϕ_q.

Via these identification one can define (conjugacy classes of) Frobenius elements $\sigma_v \in G_K$.

6.2 Local-Global Principle for Galois Representations

Let ρ be a continuous presentation of G_K.
Let σ be an element of G_K.
By

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

we denote the characteristic polynomial of $\rho(\sigma)$.
Example:
For $k = 2$

$$\chi_{\rho(\sigma)}(T) = T^2 - Tr(\rho(\sigma))T + det(\rho(\sigma)).$$

Definition 6.1 *ρ is semi-simple if ρ is determined (up to equivalence) by $\{\chi_{\rho(\sigma)}(T); \sigma \in G_K\}$.*

6.2.1 Local-Global Law for Representations

There is a powerful **Local-Global-**principle yielded by *Čebotarev's density theorem* *(*1922*)* mentioned above as landmark.

Theorem 3 *If ρ is semi-simple then ρ is determined by*

$$\{\chi_{\rho(\sigma_\mathfrak{l})}(T); \mathfrak{l} \textit{ runs over almost all places of } K\}.$$

7 Elliptic Curves in Arithmetical Environments

We are interested in elliptic curves E over global fields K.
For simplicity we assume that K is a number field, and sometimes even that $K = \mathbb{Q}$. We follow the hierarchy from above and embed K in $\mathbb{C}$ and K_v.

7.1 Elliptic Curves over $\mathbb{C}$

Projective algebraic curves over $\mathbb{C}$ have a canonical complex structure which makes them to compact Riemann surfaces and vice-versa.
Elliptic curves are equal to their Jacobian variety, and so we get a parameterisation

$$\mathbb{C} \xrightarrow{\phi} E(\mathbb{C})$$

by

$$z \mapsto (\wp(z), \wp'(z))$$

where $\wp$ is the suitable normalized Weierstraß $\wp$-function.
The kernel of ϕ is a lattice Λ_E in $\mathbb{C}$. By normalizing we can assume that

$$\Lambda_E = \mathbb{Z} + \mathbb{Z}\tau$$

with $Im(\tau > 0$.

τ is determined modulo the action of $Sl(2,\mathbb{Z})$ on the complex upper half plane and is the *period* of E.
The absolute invariant j_E is the evaluation of the modular function j at τ.
Consequences:

- $E[n] = 1/n\Lambda_E/\Lambda_E \cong \mathbb{Z}/n \times \mathbb{Z}/n$ (this proves one of the facts from above for all fields of characteristic 0)
- The ring of endomorphisms $End(E)$ of E is commutative (hence this holds over all fields of characteristic 0).

- $End(E)$ is either $\mathbb{Z}$ (generic case) or an order in an imaginary quadratic field (CM case).

- In the CM case the invariant j_E is an algebraic integer.

7.2 Elliptic curves over K_v

Now assume that K_v is a complete with respect to a non-archimedean valuation v with ring of integers O_v, maximal ideal m_v and finite residue field $\mathbb{F}_q$. We call K_v a **local field**.
Let E_v be an elliptic curve over K_v.
We can try to imitate methods used over $\mathbb{C}$ in the realm of rigid geometry.
A first classical result (3×25 years old) is due to E. Lutz and states:
The group $E(K_v)$ contains a subgroup of finite index which is isomorphic to O_v.

Corollary 1 *The subgroup of torsion elements in $E(K_v)$ is finite.*
In particular: If K is a field of finite type then $E(K)_{tor}$ is finite.

But one can do much better.
Our knowledge about schemes (from $\sim$ $60'$s) allows to extend E to a group scheme $\mathcal{E}$ over O_v, and the special fiber $\mathcal{E}_v$ is a group scheme over $\mathbb{F}_v$, and there is a homomorphism, the reduction map, which maps $E(K_v)$ surjectively to $\mathcal{E}_v(\mathbb{F}_v)$.
The kernel of the reduction map is a pro-p-group where $p = \mathrm{char}(\mathbb{F}_\mathrm{v})$. It it contains only torsion points of p-power order.
We can do this in a best possible way to get the Néron model.
We allow unramified quadratic extensions and get :
The connected component of $\mathcal{E}_v$ is either

1. an elliptic curve
2. G_m
3. G_a

In the first case we say that E has good reduction modulo v.
In the second case we say that E has multiplicative reduction.
In both cases we call E semi-stable at v. An important theoretical and practical criterion is due to Néron-Ogg-Shafarevich:

Theorem 4 *E has good reduction modulo v iff for all n prime to p the adjunction of points of order n is unramified.*

7.3 Elliptic Curves over Finite Fields

Motivated by reduction theory we investigate elliptic curves E over finite fields $\mathbb{F}_q$. Of course, $E(\mathbb{F}_{q,s})$ consists only of torsion points.
The Frobenius automorphism ϕ_q generates $G_{\mathbb{F}_q}$ topologically and hence it determines $\tilde{\rho}_{E,\ell}$.
At the same time ϕ_q induces an *endomorphism* of E by raising coordinates to q-th powers.
It is not very difficult to see that the characteristic polynomial of this endomorphism (applied to Tate-modules of E) is the same as the one of $\tilde{\rho}_{E,\ell}$ for all ℓ, and so it is a polynomial in $\mathbb{Z}[T]$.

Definition 7.1 *The characteristic polynomial of* ϕ_q *is*

$$\chi_{q,E}(T) = T^2 - \mathrm{trace}(\phi_q)\mathrm{T} + \mathrm{q}$$

with $trace(\phi_q)$ *the trace of the Frobenius endomorphism (taken from the action on any Tate-module of* E*.*

Corollary 2

$$|E(\mathbb{F}_q)| = q + 1 - \mathrm{trace}(\phi_q)$$

The reason for this corollary is that $E(\mathbb{F}_q)$ is the kernel of the separable endomorphism $\phi_q - id_E$.

Corollary 3 ***(Tate)***
The isogeny class of E *over* $\mathbb{F}_q$ *is determined by* $\mathrm{trace}(\phi_q)$*.*

7.4 Information by Lifting

It is a very common feature of number theory that one tries to get information about global objects like solutions of equations by looking tat the problem modulo primes.
Here we will see that the inverse way works sometimes,too.

7.4.1 From Finite Fields to Local Fields

The key ingredient is Hensel's Lemma in various forms.

Proposition 1 *(ℓ-adic lifting)*
Let K_v be a local field with residue field $\mathbb{F}_q$.
Let E be an elliptic curve over $\mathbb{F}_q$ and $\tilde{E}$ an elliptic curve over K_v whose reduction modulo v is E. Take ℓ prime to p.
Then $\tilde{\rho}_{E,\ell} = \tilde{\rho}_{\tilde{E},\ell}$.

This result is not totally satisfying since there are many curves $\tilde{E}$ satisfying the condition, and the lifting refers to the Frobenius automorphism in the Galois group and not to the lifting of the Frobenius endomorphism of E.

But this is possible under one restriction: E is not supersingular!

7.4.2 From Finite Fields to Global Fields: The Work of Deuring

In a beautiful paper (*Die Typen der Multiplikatorenringe von Elliptischen Kurven*) M. Deuring classified the endomorphism rings of elliptic curves over finite fields and established a bridge to curves with complex multiplication in number fields.

Theorem 5 *Let E be an elliptic curve over $\mathbb{F}_q$.*

- *If E is supersingular then $End(E)$ is an order in the quaternion algebra which is ramified exactly at p and ∞.*

- *If $E_{/\mathbb{F}_q}$ is an ordinary elliptic curve then $End(E) \neq \mathbb{Z}$ and, given a valuation v on $\mathbb{Q}_s$ with residue field of characteristic p, there is (up to twists) exactly one elliptic curve $\tilde{E}$ defined over a number field K with*

$$End(\tilde{E}) = End(E)$$

and the reduction modulo v restricted to K is equal to $E_{/\mathbb{F}_q}$.

It follows that $\tilde{E}$ has complex multiplication and so $End(E)$ is an order in an imaginary quadratic field.

Definition 7.2 *$\tilde{E}$ is the canonical lift of E*

Corollary 4 *("Riemann Hypothesis") Let E be an ordinary elliptic curve over $\mathbb{F}_q$. Then the splitting field of $\chi_{q,E}(T) = T^2 - \mathrm{trace}(\phi_q)\mathrm{T} + \mathrm{q}$ is imaginary quadratic, and hence $(|E(\mathbb{F}_q)| - q - 1))^2 - 4q = \mathrm{trace}(\phi_q)^2 - 4\mathrm{q} < 0$.*
Hence

$$||E(\mathbb{F}_q)| - q - 1)| < 2\sqrt{q}.$$

(For supersingular E one gets the same inequality immediately).

8 Elliptic Curves over Global Fields: Global meets Local

8.1 Torsion points

Let E be an elliptic curve over a number field. and define $K_n := K(E[n])$
It is obvious that K_n/K is Galois with Galois group $G_n \subset Gl(2, \mathbb{Z}/n)$.
From above we know that $\zeta_n \in K_n)$ and that $G(K_n)/K(\zeta_n) \subset Sl(2, \mathbb{Z}/n)$.
We distinguish two cases:
1.) $End(E)$ is an order in $\mathbb{Q}(\sqrt{-d})$, $d \in \mathbb{N}$.
Kronecker's Dream becomes true for imaginary quadratic fields:
$\mathbb{Q}(\sqrt{-d})^{ab} = \mathbb{Q}(\sqrt{-d})(j_E, \bigcup_n E[n])$.
2.) $End(E) = \mathbb{Z}$.

Theorem 6 ***(Serre)***
For almost all ℓ we have $G_\ell = Gl(2, \mathbb{Z}/\ell)$.

8.2 The Group of Rational Points

From local theory follows:

- $E(K)_{tor}$ is finite (and easily estimated and computed)
- For all $n \in N$ the group $E(K)/nE(K)$ is finite (consequence of Theorem of Hermite-Minkowski)

To get more we need a new ingredient: the Néron - Tate height h_E. This is a *positive definite quadratic form* on $E(K) \bigotimes \mathbb{R}$. It is defined *locally* in a rather explicit way and can be computed effectively.
Putting local heights together one gets the global height. Roughly, it is the height of the X-coordinate of points.
Example: If $K = \mathbb{Q}$ and $P = (a/b, y)$ then $h(P) \approx \log(max(|a|, |b|))$.

Theorem 7 ***(Mordell-Weil)***
$E(K)$ is a finitely generated $\mathbb{Z}$-module, and $E(K) \bigotimes \mathbb{R}$ is an Euclidian space. Its dimension is the rank r_E of E.

Consequence:
Choose an affine Weierstraß equation for E.
For a given finite set S of places of K there are only finitely many points in $E(K)$ with X - coordinates integral outside of S.
Conjecture (Lang) The height of points on elliptic curves over K is bounded from below by $C \cdot height(\Delta_E)$.
This is proved (Silverman) for many curves.
We conclude that there are no infinite subgroups of "smooth" elements, and sets of points with small height tend to be linearly independent.
Problem: Compute r_E

8.3 The L-series of E

Above we have seen that the characteristic polynomial of Frobenius elements at places v of K count points on $\mathbb{F}_v$ and determine the reduction of E up to isogeny. Bringing all this information together (and having Čebotarev in mind) we can hope to get insight into the arithmetic of E.

8.4 The Isogeny Theorem and Mordell's Conjecture

Faltings proved: The ℓ-adic representation attached to Tate-modules of abelian varieties is semi-simple (1982). Hence E (A) is isogenous to E' (A') (i.e. there is a surjective morphism with finite kernel) iff for ℓ and for almost all places $\mathfrak{l} \in \Sigma_K$ the characteristic polynomials of the Frobenius automorphisms at $\mathfrak{l}$ are equal.
Effective variant: One can take as representation space the points of order n (for n large enough). As consequence Faltings could prove that on curves of genus > 1 there are only finitely many K-rational points (*Mordell's conjecture*).

8.5 The Conjecture of Taniyama-Hasse

One of the most fruitful principles of arithmetic geometry is the linking of Galois theory with analytic functions.
Of course the inspiring examples are the L-series of global fields, and key words are Eichler-Shimura congruences and Langlands' programme.
In our context we are interested in the L-series of elliptic curves and define them, for simplicity, for $K = \mathbb{Q}$.

Definition 8.1 *Let E be an elliptic curve over $\mathbb{Q}$ with (minimal) discriminant Δ_E.*

$$L_E(s) := \prod_{p|\Delta_E} (1 - a_p^{-s})^{-1}$$

$$\cdot \prod_{p \text{ prime to } \Delta_E} (1 - \mathrm{trace}(\phi_p) p^{-s} + p^{1-s})^{-1}$$

where , for $p|\Delta_E$ we have: $a_p = 0$ if E has additive reduction, $a_p = 1$ if p has split multiplicative reduction, and else $a_p = -1$.

Conjecture 1 *(**Hasse (?) and Taniyama**): $L_E(s)$ has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation.*

This was proved by Deuring for CM-curves, and by Shimura for modular elliptic curves.

8.6 The Conjecture of Birch and Swinnerton-Dyer

The motivation of this conjecture is the analytic formula for class numbers.
Behind the formulation lie extensive computations (1960) and keen and ingenious intuition.
Again we formulate the conjecture only over $\mathbb{Q}$.

Conjecture 2 ***(BSD)***
We assume that the Hasse-Taniyama conjecture is true for $E/\mathbb{Q}$.
Then

$$\frac{L_E^{(r_E)}(1)}{r_E!} = \frac{\#\mathrm{Sha}(E)\Omega_E R_E \prod_{p|\Delta_E} c_p}{(\#E(\mathbb{Q})_{tor})^2}.$$

In the formula we have some harmless factors: Ω_E is the real period of E, $\{c_p\}$ are the Tamagawa numbers determined by the Néron model of E, and $\#E(\mathbb{Q})_{tor}$ is easily computed (Mazur's theorem).
A difficult factor is R_E defined as volume of the lattice $E(Q) \bigotimes \mathbb{R}$ in the Euclidean space endowed with the Néron-Tate height.
It is important to get at least bounds for it in order to make the formula useable. It corresponds to the regulator of number fields attached to a system of fundamental units.
Totally mysterious is Sha(E), the Tate-Shafarevich group of E. It has no counterpart in the G_m-world. It measures the failure of the Hasse-principle for curves of genus 1 with Jacobian E.
It is conjectured that it is finite (obviously part of BSD).

If we stay in the time *before 1985* the only theoretical big result is due to Coates and Wiles (1976) for elliptic curves with CM: If $L_E(1) \neq 0$ then $E(\mathbb{Q})$ is finite.
The influence of BSD is immense. It has been vastly generalized, and the arithmetic interpretation of special values of L-series attached to geometric objects like motives is a central theme in arithmetic geometry.

8.7 The Distribution of Eigenvalues of Frobenius Endomorphisms

The Question:
Given a "random" elliptic curve over $\mathbb{F}_q$, what can we say about the structure of $E(\mathbb{F}_q)$?
We know the size of $|E(\mathbb{F}_q)|$: It is about q with an error of size $2\sqrt{q}$, because it must lie in the "Hasse interval".
But what is the exact order?
Is the group cyclic?
Is the order a prime number or, contrary, a smooth number?
A first step to answer such questions is to ask for probabilities.
There are two possible approaches: Either fix $\mathbb{F}_q$ and vary the curve or choose a curve, let us say, over $\mathbb{Q}$,vary the reduction place p and study the reduction $E^{(p)}$ of E.

For fixed $\mathbb{F}_q$ Deuring's work is again very useful: He relates the number of elliptic curves with given order with class numbers of binary quadratic forms, and there is a highly developed theory about this subject.

For fixed $E/\mathbb{Q}$ we have one special case: E has CM.

Then the Frobenius endomorphism is an element in an order of an imaginary quadratic field with norm p, and analytic number theory has results about the distribution of traces of these elements.

But what happens if E has no CM (and this is the generic case).
We know that $\mathrm{trace}(\phi_\mathrm{p}) = 2\sqrt{\mathrm{p}}\cos(\theta_\mathrm{p})$ and so the eigenvalues of ϕ_p are equal to $\sqrt{p} \cdot e^{i\theta_p}$ and $\sqrt{p} \cdot e^{-i\theta_p}$

Conjecture 3 ***(Tate,Sato)***
$\{\theta_p\}$ is equally distributed in $[0, \pi]$ with respect to the measure $\mu = 2/\pi sin^2(\theta)d\theta$.

Another typical question is: Given a non-torsion point P of $E(\mathbb{Q})$.
How often is $E^{(p)}(\mathbb{F}_q) =< P^{(p)} >$. This is an analogue of conjectures of Artin about primitive roots in $\mathbb{Z}/p$. More generally take a number A and ask "how often" we have $\mathrm{trace}(\phi_\mathrm{p}) = \mathrm{A}$?

Conjecture 4 ***(Lang-Trotter)***

$$|\{p \leq T; a_p = A\}| \sim c_{A,E}(2/\pi)\sqrt{T}/\log(T)$$

with a constant $c_{A,E}$ *which is not zero if there is no congruence obstruction (for instance, if* $E(\mathbb{Q})$ *has a point of order* 2 *then almost all* a_p *are divisible by* 2.*)*

PART II The Time after ECC

In 1985 everything was ready for a golden age for arithmetic geometry.

But at the same time there was a great impacton the algorithmic side, and number theory had its first really deep application to engineering. For this two new ideas were responsible: Use elliptic curves for factoring and for Discrete Logarithms!

Names of initiators of these fascinating ideas are dropped in the programme of this conference:

- Hendrik Lenstra about integer factorization using elliptic curves
- Victor Miller and Neal Koblitz about ECC
- Shafi Goldwasser and Joe Kilian about primality proving using elliptic curves
- Oliver Atkin and Francois Morain about primality proving using elliptic curves

To show how mighty the available machinery is we begin with highlights from theory.

9 Big Theorems

We begin with the most spectacular new result.
During the last five years the proof of Serre's conjecture was established which is a big step towards Langlands' programme and extends the Jugendtraum.
There are many names to mention but let me restrict myself to Wintenberger, Khare, Kisin, Taylor, Wiles, Diamond, Conrad,...:

Theorem 8 *Let $\mathbb{F}_q$ be a finite field. Let*

$$\rho : G_{\mathbb{Q}} \to GL(2, \mathbb{F}_q)$$

be a continuous, absolutely irreducible, twodimensional, odd repre sentation with Serre conductor N_ρ and Serre weight k_ρ. Then ρ is modular (with nebenty-pe) of level N_ρ and weight k_ρ.

Consequences:

Theorem 9 *The L-series of irreducible two-dimensional odd complex represen-tations ρ are holomorphic.*

Already proved before:

Theorem 10 *Every elliptic curve over $\mathbb{Q}$ is modular.*

FLT is just a footnote to this result!

Previous conditional results on elliptic curves are now true in general:

- Gross-Zagier:If $L_E(s)$ has a zero of order 1 at s = 1 then it has positive rank.
- Kolyvagin (1990): If $L_E(1) \neq 0$ then $r_E = 0$, and if $L_E(s)$ has a first-order zero at $s = 1$ then $r_E = 1$.
- Rubin (1991) showed for CM curves defined over the CM field: If $L_E(1) \neq 0$ then the p-part of the Tate-Shafarevich group had the predicted order for all primes $p > 7$.

Finally: The Tate-Sato conjecture was proved (announced 2010) at least for elliptic curves over $\mathbb{Q}$ by Barnet-Lamb, Geraghty, Harris and Taylor. (by proving that a certain L-series is holomorphic).

10 Cryptography

What has this to do with ECC?
Surely ECC will not need all the deep theory used for the proof of Serre's conjecture. But it uses astonishingly much, and the rest is for building up confidence!
For Neil Koblitz and Victor Miller the existing theory was a strong motivation to suggest elliptic curves as source for DL systems. One reason must have been that an index calculus attack like the one in the G_m-world was impossible because of the theory, here: the properties of the height.
I refer to the "Golden Shield"-Lecture of Koblitz at ECC 2000 and the analysis of the Xedni-attack he did in the paper with Jacobson, Silverman, Stein and Teske.
(Cf. the remarkable new result in the paper of Rosen and Silverman: Even Heegner points are independent!)

To make the approach practical one has to overcome difficulties. Most important is the fast construction of instances.
Encouraging statistical statements (partly heuristic or conjectural but partly proven now) were mentioned above.
Koblitz himself used Deuring's work to show that both smooth numbers and prime numbers occur sufficiently often as orders of $E(\mathbb{F}_q)$.

The next step is to count points.
The available theory was CM, and till today it is very efficient.
But next came a much more general approach using étale cohomology (Schoof) and modular curves (isogenies) leading to the very efficient Schoof-Elkies-Atkin - Algorithm.

The next wave (15 year later) was the introduction of p-adic lifting (Satoh: canonical lifting making Deuring effective, Mestre: AGM),
p-adic analysis (Kedlaya: making Dwork, Monski-Washnitzer effective)
and p-adic deformation (Lauder).

Some members of the big family of elliptic curves were excluded, many contributions to efficiency and security were added, and always reported during ECC conferences.

But the general picture is remarkably stable....

11 Apology

What I missed: More about p-adic cohomology
Duality Theory: Tate pairing et al...

Not miss to say: Thanks for Listening!