Kapitel 1

Galois Operation

1.1 Point counting

1.1.1 Find a Curve!

The tasks are:
Find a finite field k, a curve C defined over k and a prime number p dividing $\mid Pic(O_C) \mid$, a point $P_0 \in Pic(O_C)$ such that we get a secure DL-system.
The determination of P_0 is not difficult if C is known.
To find (k, C) one uses the following strategy:

- Prove (e.g. by analytic number theory techniques) that good pairs occur with a reasonable large probability.
- Choose random (k, C) and count the elements in $Pic(O_C)$.

The second task is solved by determining the characteristic polynomial of the Frobenius automorphism Π acting on vector spaces related to the geometry of C and J_C:
Computation of the L-series of $C_{/k}$.
Examples for representation spaces are spaces of holomorphic differentials or more generally of differentials with prescribed poles and cohomology groups. De Rham cohomology, étale cohomology and crystalline cohomology are especially interesting.

There are most important theorems (Hasse, Deligne-Weil, Lefschetz) saying:

- Let Π operate on the étale or crystalline cohomology groups above. Then its characteristic polynomial is independent of the choice of the cohomology and is a monic polynomial with coefficients in $\mathbb{Z}$.
- If we choose the first cohomology groups then this polynomial is of degree $2 \cdot dim(A)$ and its zeroes are algebraic integers with absolute value $p^{n/2}$. It is called the L-series of A.
- The value of the L-series at the place 1 is equal to the order of $A(\mathbb{F}_{p^n})$.

We shall assume that p is a prime and that n_0 is a divisor of n.

1.1.2 Methods of counting on abelian varieties

Given:
An abelian variety A (elliptic curve, Jacobian of a hyperelliptic curve,...) over a finite field $\mathbb{F}_{p^n}$ with Frobenius automorphism Problem:
Count the number of points (and determine the group structure) of the $\mathbb{F}_{p^n}$-rational points on it.
Use:
The Galois operation by Π induces an endomorphism on A denoted by the same symbol.

Methods:

1. Brute force,
   (possible if $p^{n \cdot dimA} < 10^{12}$),
2. index-calculus or Pollard-ρ
   type algorithms,
3. compute the L-series of the Frobenius endomorphism Π

The methods 1 and 2 can only be used for auxiliary constructions since if they succeed the DL-problem can be solved by the same methods.

So we concentrate on the third method.

A variant of 1. and 2. is
Let A be defined over $\mathbb{F}_{p^{n_0}}$. Then Π (as endomorphism of A) is equal to π^{n/n_0}.

Now take A over $\mathbb{F}_{p^{n_0}}$ and count points on $A(\mathbb{F}_{p^{n_0}})$ by one of the methods mentioned above. Then we can compute $A(\mathbb{F}_{p^n})$ rather easily (method of constant field extensions).

To realize these representations mentioned above one uses the result that the étale cohomology is isomorphic to the Tate modules of A w.r.t. primes l different from p, and the crystalline cohomology is isomorphic to the **Dieudonné module** of A.

By definition Tate-modules T_lA mod l are the $l-$torsion points of A, and on this fact the strategy of Schoof's algorithm relies:
compute the Frobenius action modulo small primes (and their powers if possible) and then use the Chinese remainder theorem to determine the L-series. This algorithm is in general *in principle* polynomial (in $n \cdot logp$) but in practise not working fast enough without further tricks (Atkin-Elkies for elliptic curves) so that nowadays we can use it only to count the points on randomly chosen elliptic curves in cryptographic relevant regions. The reason for the higher efficiency in the elliptic curve case is that we can "easily" decide whether elliptic curves have isogenies of a given degree (and they have many!).

1.2 Lifting strategies

We could use more machinery (e.g. analytic ones) if we could lift the whole situation to characteristic 0 and determine the Frobenius explicitly.
Note: Π acts in two manners: As Galois automorphism **and** as endomorphism! It is not difficult to lift Π as Galois group element, but very difficult to do this as endomorphism.
For general liftings of A this is not possible. We need **canonical liftings**, and

they exist for abelian varieties with special properties ("ordinary varieties") due to deep theorems from arithmetic geometry. Take $A = E$ an elliptic curve. If E is supersingular we cannot lift Π such that we get non trivial information. (Fortunately it is very easy to determine the L-series of E forb supersingular elliptic curves.)
But assume that E is not supersingular and so $End(E)$ is an order O in an imaginary quadratic field. Then (**Deuring**) there is an elliptic curve $\tilde{E}$ defined over a number field with $End(\tilde{E}) = O$. In practice this does not help for randomly chosen elliptic curves.

Reason:
The order O will have a discriminant of a size $\sim 10^{60}$ and so E is defined over a number field of degree $\sim 10^{30}$!
But the situation changes if we replace the global number fields by their $p-$adic completion! This idea works (surprisingly good) for **small** p (and so for large n).

1.2.1 Elliptic Curves: Work of Satoh

(Very) short sketch:
Take p small, let E be an elliptic curve over $\mathbb{F}_{p^n}$.
We can assume that E is not supersingular. A consequence of class field theory is that the minimal polynomial of the j-invariant of the canonical lifting $\mathcal{E}$ has (all) zeroes in the minimal extension $W(\mathbb{F}_{p^n}) =: K_p$ of $\mathbb{Q}_p$ which is unramified with residue field $\mathbb{F}_{p^n}$.

First step: Determine the invariant of $\mathcal{E}$ (in a sufficiently good approximation) and so $\mathcal{E}$.
Then we know that Π has a lifting to $End_{K_p}(\mathbb{E})$.
Now comes the trick:
We have to compute how Π operates on torsion points (or another nice representation space). And so we can use the p-**power** torsion points which had vanished during the reduction process i.e. which are in the formal group of $\mathcal{E}$.
And then we can use p-adic power series to do this (Newton-type iteration).
The only problem is that the Frobenius automorphisms is not acting in a

non-trivial way on this group. But there is the dual map called **Verschiebung** which acts nicely (separably) and which has the same trace (all what we need).
Practical remarks:

- By the theorem of Hasse we know the order of $E(\mathbb{F}_{q^n})$ up to an error term of size $2 \cdot q^{n/2}$ and so it is enough to compute everything with (easy to estimate) p-adic precision.
- In fact one does not use Π but the action of π (or the corresponding Verschiebung) on the Weil restriction , and since p is small one use explicit formulas for isogenies.
- The complexity of this algorithm is polynomial in p (bad) but also in n both in space ($O(n^2)$ by a new result of Vercauteren) and time ($O(n^{5+\epsilon})$.

  Generalization:
  For $p = 2$ a very efficient version and a generalization to hyperelliptic curves of genus 2 (and 3) was given by Mestre and is called the AGM-method.

1.2.2 Counting on Curves: Work of Kedlaya

There is a theoretically more involved method which is surprisingly easy to be implemented.

It avoids to lift abelian varieties canonically but uses a $p-$adic version of de Rham cohomology to find a representation space for Π. The background is the work of Monsky-Washnitzer on Lefschetz fixed points formulas on these spaces, the paper is written by Kedlaya. Till now we have only discussed the case that we want to count points on abelian varieties. Now we shall count on an **affine** curve, from this it is easy to get the number of points of corresponding projective curves and then by using properties of Zeta-functions of curves and their relations to class group numbers on gets the result for the

Jacobian of the projective curve.

Note: To do this for curves of genus g one has to count the points on the curve over $\mathbb{F}_{p^{gn}}$.

De Rham cohomology

We assume now for the moment that C is an affine curve defined over a field K of characteristic 0 with ring of coordinate ring A (e.g. $A = K[X,Y]$). If we remove finitely many points from C we get again an affine curve C_1 with coordinate ring A_1.
Let Ω_1 be the the A_1-module of holomorphic differentials on C_1. Inside of Ω_1 there is the module of exact differentials, i.e. the image of A_1 under "differentiation" denoted by B_1.

$$H^1(C_1) := \Omega_1\,/B_1$$

is the first de Rham cohomology of C_1 which is a finite dimensionalb $K-$vectorspace.

The relevant example

Let C' be a projective hyperelliptic curve of genus g with a rational Weierstraß point which we choose as point at infinity. Let C be given as the affine part, an equation is

$$Y^2 \;=\; f(X)$$

where f is a polynomial of degree $2g+1$.
Let C_1 be the sub curve obtained by removing the zeroes of Y.
Then

$$A_1 = K[X,Y,Y^{-1}]/(Y^2 - f(X))$$

and we can give an explicit base of $H^1(C_1)$:

$$\begin{aligned} H^1(C_1) &=< X^i dX/Y; i = 0, \cdots, 2g-1 > \\ &\oplus < X^i dX/Y^2; i = 0, \cdots, 2g-1 > \end{aligned}$$

(we get a decomposition under the action of the hyperelliptic involution) and we can compare this cohomology with the étale cohomology (on which we

have a Galois action (Tate-modules!) of the absolute Galois group of K **and** the action of endomorphims of the Jacobian). Now assume that $K = K_p$ (for simplicity p odd), change notation $C \mapsto \mathcal{C}$ and assume that C is the reduction modulo p of $\mathcal{C}$. Then:
If Π would act on $H^1(\mathcal{C}_1)$ as endomorphism we could compute the L-series and so we could compute the number of points on $C_1(\mathbb{F}_{p^n})$.
This will be not possible in general but we always have an obvious action if we replace A_1 by its formal p-adic completion A_∞.
Reason: The map

$$X \mapsto X^{p^n}$$

extends to

$$Y \mapsto$$

$$Y^{p^n}((1 + (f(X)^{\Pi} - f(X)^{p^n})/f(X)^{p^n})^{1/2}$$

as series converging in the p-adic topology very rapidly.
This induces an action (explicitly given) on the de Rham cohomology of A_∞.

Check (Kedlaya): This formal cohomology is finitely generated with the same set of generators as $H^1(\mathcal{C}_1)$.
Then by the Theorem of Monsky-Washnitzer we get:
the fixed point theorem for Π holds on this formal cohomology group, and we are done.

In fact there a quite efficient implementations of this algorithm (Vercauteren) and generalizations to more general varieties (Lauder, Wan), see thesis of R. Gerkmann (Essen 2003).

1.2.3 Global lifting

Remaining open case: We want to count the element of $Pic(O)$ for underlying curves of genus larger than 1 in large characteristics.
The only working method today is a lifting to global fields in very special cases:
C is such that its Jacobian has a lifting to a number field of small degree over $\mathbb{Q}$ with a ring of endomorphism which contains either a lifting of Π or is at least not for away from it.

This means: C (resp. J_C) is the reduction mod $\mathfrak{p}$ of a curve (an abelian variety) which has **real** or **complex** multiplication with an order in a number field of small class number. $\mathbb{F}_q$ so following an idea of Atkin one
begins with an appropriate endomorphism ring, construct a corresponding global curve and the uses for C the reduction of this curve. This idea can be applied to Jacobians of curves of genus 2,3
(A. Weng). $g = 1$:
Class field theory of imaginary fields applied to elliptic curves is used till today. It works very efficiently, the hardest computational problem is the factorization of polynomials of degree ≤ 1000 over $\mathbb{F}_q$. $g = 2$:
This is implemented by A.Weng (Preprint IEM Essen 2000) in a very efficient way and uses

1. *class field theory* of fields of degree 2 over real quadratic fields (non-Galois over $\mathbb{Q}$), [1]
2. *Invariant theory* which is explicit and "easy" and
3. Mestre's method intersecting invariant forms

Example (Weng):
(g=2) Consider the CM-field

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}\left(i\sqrt{7 + 2\frac{-1+\sqrt{33}}{2}}\right).$$

It has class number two and two
polarizations.
The class polynomials are given by

$$\begin{aligned}
\mathbf{H_1}(X) &= w^4 + 125426939904w^3 + 2064831408683107614 72w^2 \\
&\quad -37777358525311935278890 35264w \\
&\quad +48802878644309442250486942594 49856, \\
\mathbf{H_2}(X) &= w^4 + 660000960w^3 + 106952268616185600w^2 \\
&\quad +272554661493753384 96000w
\end{aligned}$$

[1] to avoid non-necessary automorphisms

$$+837300145473346170101760000,$$

$$\mathbf{H_3}(X) = w^4 + 189766368w^3 + 7505309625975360w^2$$

$$+43463155606584303513 6w - 453298071903765088 29696.$$

For

$$p = 5900018603715467611181989109202421$$

the corresponding curve is

$$C : y^2 = t^5 + 2251831303237605767657618195346350t^4$$

$$+1395987570926578077980910550381755t^3$$

$$+3449986084090239803090552184527208t^2$$

$$+1071704234696277993751073168935 95t$$

$$+2770857204236068378720416405312357.$$

with

$$\mid J_C(\mathbb{F}_p) \mid =$$

is

$$= 3481021952418861785390626980854276431541396337102367100426394773063 2$$

$$= 8 \cdot q_{prime} \, (67 \text{ digits}).$$

3.) For $g \geq 3$ invariant theory becomes more complicated.
A.Weng is able to find curves with CM with 4 automorphisms.

Example (g=3)
For

$$p = 1234567765432112361 73$$

the Jacobian of the curve

$$C : y^2 = x^7 + 7x^5 + 14x^3 + 7x.$$

has complex multiplication by

$$K = \mathbb{Q}(i)K_0$$

where K_0 is generated by $w^3 - w^2 - 2w + 1$.
The group order is
$n = 188167580186437989111433953556453880527469259476859068821184$8
$= 8l$ with l a prime with 60 digits.

1.3 Pairings

1.3.1 Bilinear Structures

We shall use properties of abelian varieties with Galois action to build up a bilinear structure related to our DL-system in special cases.

Assume that the DL-system $A, \circ$ is given and that there is a group A' in which we can compute "as fast" as in A.
Assume moreover that $(B, \circ)$ is another DL system and that a map

$$Q(a_1, a_2) : A \times A' \to B$$

is computable in polynomial time (this includes that the elements in B need only $O(log \mid A \mid)$ space

with

- for all $n_1, n_2 \in \mathbb{N}$ and random elements $a_1, a_2' \in A \times A'$ we have

$$Q(n_1 \circ a_1, n_2 \circ a_2') = n_1 \cdot n_2 \circ Q(a_1, a_2')$$

- $Q(.,.)$ is non degenerate and hence for random $a' \in A'$ we have $Q(a_1, a') = Q(a_2, a')$ iff $a_1 = a_2$.

Then we call (A, Q) a DL-system with bilinear structure.
There are two immediate consequences:

- The DL-system $(A, \circ)$ is at most as secure as the system $(B, \circ)$.

- Assume moreover that $A = A'$.
  Given a (random) element a
  and $a_1, a_2, a_3 \in \mathbb{N} \circ a$ one can decide in polynomial time (in $log \mid B \mid$)
  whether (simultaneously)

$$a_1 = n_1 \circ a, a_2 = n_2 \circ a, a_3 = (n_1 \cdot n_2) \circ a$$

  holds.

This are negative aspects of bilinear DL-systems but very interesting protocols due to Joux (tripartite key exchange) and Boneh-Franklin use such structures in a positive way.

1.4 Tate Duality of Abelian Varieties

In this section we shall discuss a bilinear structure on points of order p inside of the rational points of the Jacobian variety of a curve C with a rational point P_0 defined over a finite field k of characteristic l_0 with values in the **Brauer group** of a local field which can weaken our system in some cases.

We distinguish now two cases:
1.) $p = l_0$ and
2.) $p \neq l_0$
and begin our discussion with the first case. We follow closely a paper of Rück.

1.4.1 The Artin-Schreier case

We use the following result about algebraic function fields with positive characteristic(Serre 1956):

Proposition 1 *Let k be a field of characteristic p, C a projective curve of genus g defined over k and $\Omega^1(C)$ the $k-$vector space of holomorphic differentials on C. Then there is an isomorphismus from $Pic_0(C)[p]$ into*

$\Omega^1(C)$ given by the following rule:
Choose a divisor D with $p \cdot D = (f)$ where f is a function on C. Then the divisor class $\bar{D}$ of D is mapped to the holomorphic differential df/f.(We have to use that char(K)= p!)

Next we describe differentials by their power series expansion at P_0.
Let t be a local parameter of C at P_0. Let $(a_0, a_1, ..., a_{2g-2})(f)$ be the tupel whose coordinates are first coefficients of the power series expansion of

$$(\partial f/\partial t)/f$$

at P_0. Hence we have to evaluate a function at a point. The problem is that the degree of f is very large.
The Riemann-Roch theorem implies that $(a_0, a_1, ..., a_{2g-2})(f)$ determines df/f completely . Hence

$$\Phi : Pic_0(C)[p] \to k^{2g-1}$$

given by

$$\bar{D} \mapsto (a_0, a_1, ..., a_{2g-2})(f)$$

is an injective map.

Hence: Φ transfers the DL- problem from $Pic_0(C)[p]$ into k^{2g-1} with its additive group structure. As remarked in example 1 this means that the DL-system is broken if the computation of Φ can be done in polynomial time. We leave this as an open problem for a moment and go to the second case:

1.4.2 The Kummer case

We begin by discussing a more general situation.
Let K be a field with absolute Galois group G_K and A a principally polarized abelian variety over K, p prime to char(K).
By μ_p we denote the group of p-th roots of unity in the separable closure K_s of K (regarded as G_K module).
We have the exact sequence of G_K-modules (Kummer sequence)

$$0 \to A(K_s)[p] \to A(K_s) \xrightarrow{\cdot p} A(K_s) \to 0.$$

Application of Galois cohomology gives the exact sequence

$$0 \to A(K)/pA(K) \xrightarrow{\delta} H^1(G_K, A(K_s)[p])$$

$$\stackrel{\alpha}{\to} H^1(G_K, A(K_s))[p] \to 0.$$

Next we use that $A(K_s)[p]$ is as G_K-module self dual (since A is principally polarized) and so we can use the cup product to get the **Tate-pairing**

$$<,>_K: A(K)/pA(K) \times H^1(G_K, A(K_s))[p]$$
$$\to H^2(G_K, \mu_p)$$

given by

$$< P + pA(K), \gamma >_K = \delta(P + pA(K)) \cup \alpha^{-1}(\gamma).$$

$H^2(G_K, \mu_p)$ is a very important group for the arithmetic of K, it is isomorphic to $H^2(G_K, K_s^*)[p]$ and hence consists of the elements of order dividing p of the **Brauer group** $Br(K)$ of K.
The information we can get out of the Tate-pairing depends on the information given by the Brauer group and on its degree of non-degeneracy.

For instance if $K = k$ is a finite field the Brauer group is $\{0\}$.
The situation changes if we take K as an $\mathfrak{l}-$adic field with residue field k.

Theorem 1 (Tate)
$<,>_K$ is non-degenerate.

Hence for principally polarized abelian varieties over $\mathfrak{l}$-adic fields we have transferred the DL- problem in $A(K)[p]$ to the corresponding problem in $Br(K)[p]$ provided that we can evaluate the pairing in polynomial time. This means especially that we can describe and compute in $H^1(G_K, A(K_s))[p]$ and $Br(K)[p]$.
Let us assume that K **contains the** $p-$**th root of unity** ζ_p,, i.e.
$p \mid (q-1)$.
Standard calculations with cohomology groups yield:
Let L_p be a ramified extension of K of degree p.

Corollary 1 *There is a non-degenerate pairing $<,>$:*

$$A(K)/p \cdot A(K) \times \mathrm{Hom}(G(L_p/K), A(K)[p])$$
$$\to Br(K)[p]$$

induced by the Tate pairing.

1.4.3 Application to Jacobian Varieties over Finite Fields

We continue to assume that k is a finite field of order $q = l_0^f$ and that$p$ is a prime dividing $q-1$. Let C be a projective curve defined over k and let A be its Jacobian. We lift (C, A) to $(\tilde{C}, \tilde{A})$ over an $\mathfrak{l}$-adic field K with residue field k and apply Corollary 1 to $\tilde{A}$.

Now we invest what is known about the Brauer group of K and get

Proposition 2 (Lichtenbaum) *Let τ be a generator of $G(L_p/K)$. Let P_1, P_2 be points of $\tilde{A}(K)$ with P_2 a point of order p. Let φ be the homomorphism of $G(L_p/K)$ to $J_C(k)[p]$ mapping τ to P_2. Represent $P_i - P_0$ by coprime divisors D_i in the divisor class group, and let f_2 be a function on $\tilde{C}$ with divisor $p \cdot D_2$. Then*

$$< P_1 + p \cdot \tilde{A}(K), \varphi >= f_2(D_1) \cdot N_{L_p/K}/(L^*).$$

$\tilde{A}(K)[p]$ is isomorphic to $A(k)[p]$, $\tilde{A}(K)/p{\cdot}A(K)$ is isomorphic to $A(k)/p{\cdot}A(k)$ and $K*/N(L_p/K)(L_p^*)$ is isomorphic to k^*/k^{*p}, so:

Corollary 2 *There is a non-degenerate pairing*

$$<,>_k\colon A(k)/p \cdot A(k) \times A(k)[p]) \rightarrow k^*/k^{*p}$$

given by the the following rule:
Let P_1, P_2 be points of $\tilde{A}(k)$ with P_2 a point of order p. Represent $P_i - P_0$ by coprime divisors D_i in the divisor class group of C, and let f_2 be a function on C with divisor $p \cdot D_2$.
Then

$$< P_1 + p \cdot J_C(k), P_2 >= f_2(D_1) \cdot k^*/k^{*p}.$$

As in the additive case we can transfer the DL-problem in $J_C(k)[p]$ to the discrete logarithm in a group related to k provided that we can compute $f_1(D_2)$ fast enough.
But there are two crucial differences: In the multiplicative case we end up in the *multiplicative group* of k, and in this group only sub exponential attacks are known, and secondly we can transform the original Tate duality pairing into a computable version only under the condition that k *contains the $p-th$ roots of unity.* This last condition is rather difficult to satisfy (or easy to avoid).

1.4.4 Computation of the duality pairing

In both cases the computation of the Tate-Lichtenbaum pairing boils down to the evaluation of a function f on C at a divisor E of C. The problem is that the degree of the zero- resp. pole divisor of f and the degree of the negative (and positive) part of D are very large (about p) and so a direct approach to do this evaluation is not possible. The way out was found by V. Miller for elliptic curves (applied to the Weil pairing). We use the theory of Mumford‘s Theta groups which explicitly describes extensions of (finite subgroups of) abelian varieties by linear groups.
We restrict ourselves to the multiplicative case.
The basic step for the computation is:
For given positive divisors A_1, A_2 of degree g find a positive divisor A_3 of degree g and a function h on C such that

$$A_1 + A_2 - A_3 - gP_0 = (h).$$

We can assume that this step can be done fast for otherwise we could not use J_C for DL-systems.
As measure for the complexity of our algorithm we shall take the needed amount of such steps.

We recall that we have a canonical birational morphism, ϕ_g, between the g-fold symmetric product of C and J_C.
Let S be a subset of $J_C(k)$. A divisor E of C is called prime to S if it is prime to all divisors in $\phi^{-1}(s); s \in S$.
Now assume that S is a finite subgroup of J_C, and that E is prime to S.
Define the following group law on
$S \times k^*$:

$$(s_1, a_1) \circ (s_2, a_2) := (\phi_g(A_3), a_1 a_2 \cdot h(E))$$

where A_3, h are computed as above with $A_i = \phi^{-1}(s_i)$.
The assumption for E guarantees that $h(E) \in k^*$. The degree of h is at most g, and so the evaluation is polynomial in $g \cdot log \mid k \mid$.

We apply this in the following situation:
$\bar{D}$ is an element of order p in $J_C(k)$ and $D \in \bar{D}$ is a divisor of the form

$D = A - gP_0$ where A is a positive divisor of degree g on C. Furthermore E is a divisor of degree 0 on C which is prime to the group generated by $\bar{D}$ in $J_C(k)$.
Then the $p-$fold application of $\circ$ gives the result

$$(\underline{0}, f(E))$$

where f is a function on C with $(f) = pD$.
This is easily seen by induction for evaluating the application of $\circ$ l times gives

$$(\phi_g(A_{l-1}), h_{l-1}(E))$$

with a positive divisor A_{l-1} of degree g and a function h_{l-1} whose divisor is equal to

$$lA - A_{l-1} - (l-1)gP_0.$$

Since $\bar{D}$ is a $p-$torsion point A_{p-1} equals gP_0 and so h_{p-1} has the divisor $pA - lgP_0$.

Now we can use the group structure on $< \bar{D} > \times k^*$ and apply the square-and multiply algorithm to evaluate f at E in $O(log(p))$ addition steps.
CONSEQUENCE:
We can reduce the discrete logarithm in $A(K)/pA(K)$ to the discrete logarithm in $Br(K)_p$ with the costs $O(log(\mid \mathbb{F}_q(\mu_p) \mid)$.

Remark:
In general the conditions that K and hence the residue field $\mathbb{F}_q$ contains $p-$th roots of unity **and** that A has points of order p rational over $\mathbb{F}_q$ which are cryptographically interesting will not be satisfied at the same time.
For elliptic curves we can formulate this more precisely:

Proposition 3 *Let E be an elliptic curve defined over $\mathbb{F}_q$ and p a prime. Let π be the Frobenius automorphismus of $\mathbb{F}_q$.
Then $\mathbb{Z}/p$ can be embedded into $E(\mathbb{F}_{q^f})$ iff the trace of π^f is congruent to $q^f + 1$ modulo p and the corresponding discrete logarithm in $E(\mathbb{F}_{q^f})$ can be reduced to the discrete logarithm in μ_p in the field $\mathbb{F}_{q^{fm}}$ where m is the smallest integer such that the trace of π^{fm} becomes congruent to 2 modulo p.*

Sometimes one can enforce these conditions (after a small extension).

Corollary 3 *Assume that there is an endomorphism η of A with*

- $$< P_0 + pA(k), \eta(P_0) >= \zeta_p$$
- *η can be computed in polynomial time.*

Then the decision problem related to P, Q, R reduces in polynomial time to the equality test of $< R + pA(k), \eta(P_0) >$ and $< P + pA(k), \eta(Q) >$ in k.

Example 1 *Let E be a supersingular elliptic curve and assume that $\mathbb{F}_q$ has odd degree over $\mathbb{Z}/p$. Assume moreover that there is an endomorphism of E which is not contained in $\mathbb{Z} \cdot id_E$ and whose restriction to the points of order p can be computed in polynomial time (e.g. $E : Y^2 = X^3 - X$ and $\eta : X \mapsto -X, Y \mapsto \sqrt{-1}Y$). Then the conditions of the corollary are satisfied.*

1.5 Classical Discrete Logarithms: Computing in Brauer groups

Cyclic Algebras

$c \in Br(K)_p$ can be identified with algebras C over K which become isomorphic to the $p \times p-$matrices after tensorizing with some cyclic extension field L of degree p, i.e. we can determine c by a pair

$$(\sigma, a)$$

with $< \sigma >= G(L/K)$ and $a \in K^*/N_{L/K}L^*$:
c is the class of $f_{\sigma,a} : G \times G \to L^*$, with

$$f_{\sigma,a}(\sigma^i, \sigma^j) = \begin{cases} a & : \quad i+j \geq p \\ 1 & : \quad i+j < p. \end{cases}$$

1.5.1 Local fields

Notation

Let K be complete with a discrete valuation v, a finite residue field k with $q = l_0^d$ elements and with Galois group G_K. For instance: $K = \mathbb{Q}_{l_0}$ and $k = \mathbb{Z}/l_0$.
Let π be the Frobenius automorphism of k.
Let L_u be the unique unramified extension of K of degree p. We can lift π in a canonical way to an element of the Galois group of L_u/K.

Invariants

The key results of local class field theory are:

1. Every element of c in $Br(K)[p]$ is equivalent to a cyclic algebra with respect to L_u/K.
2. Let c be given by (π, a). Then c is uniquely determined by $v(a)$ modulo p.

$v(a) \in \mathbb{Z}/p\mathbb{Z}$ is the
invariant $inv(c)$
of c.
Hence the computing in $Br(K)[p]$ would be trivial if we could compute invariants since then we transfer it to $\mathbb{Z}/p$. For cyclic algebras two cases occur:
1)c is given by a pair (τ, a) and τ is another generator of $G(L_u)/K$. We have to determine n with

$$\tau^n = \pi.$$

2)c is given by (σ, a) with σ a generator of a ramified extension of degree p. We have to find an equivalent pair of the form (π, b).
(This is the case coming out of the Tate pairing.)
For both cases we have to solve discrete logarithms in finite fields.

1.5.2 Global fields

The Hasse-Brauer-Noether sequence

Let K be a global field (number field) with
localisations K_v and
with decomposition groups G_v.

We get the most important exact sequence

$$0 \to Br(K)[p] \stackrel{\oplus_{v' \in \Sigma_K} \rho_{v'}}{\longrightarrow} \bigoplus_{v' \in \Sigma_K} Br(K_{v'})[p] \stackrel{\Sigma_{v' \in \Sigma_K} inv_{v'}}{\longrightarrow} \mathbb{Z}/p \to 0.$$

where Σ_K is the set of equivalence classes of valuations of K.

1.5.3 Index-Calculus in Brauer groups

Assume that A_v is a cyclic algebra corresponding to $c_v \in Br(K_v)_p$.
Lift A_v to a cyclic algebra A defined over K and use the equation

$$-\Sigma_{v' \in \Sigma_K \setminus v}\ inv_{v'}(\rho_{v'}(A)) = inv_v(A_v).$$

to get relations.
For the lifting we need
existence theorems
for cyclic extensions of K with prescribed ramification delivered by
global class field theory
(in an explicit way e.g. by CM theory).

1.5.4 Example: $K = \mathbb{Q}$

The global class field theory of $\mathbb{Q}$ is completely determined by the theorem
by Kronecker and Weber:

Theorem 2 (Kronecker–Weber) *Every abelian extension $K/\mathbb{Q}$ of $\mathbb{Q}$ is contained in a easily determined cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.*
There exists an extension $K/\mathbb{Q}$ of degree l ramified exactly at p iff $l|p-1$ holds. If it exists it is uniquely determined.

We have a complete control of the decomposition laws of primes.

1.5.5 The Algorithm

Consider a global algebra A of the form $A = (K/\mathbb{Q}, \sigma, a)$. If a can be factored in the form $a = \prod p^{n_p}$ the theorem by Hasse–Brauer–Noether leads to a relation of the form

$$inv_p(a) + \sum_{q \neq p} f_q n_q \equiv 0 \bmod l. \qquad (1.1)$$

Here the factors f_q are defined as follows:
Let $K_q/\mathbb{Q}_q$ denote the extension of local fields belonging to K/Q. We can identify $G(K_q, \mathbb{Q}_q)$ with the decomposition group G_q. Since G has prime order l, it is obvious that G_q is either trivial (if q splits completely in K) or is equal to G (if q is inert in K). If $K_q/\mathbb{Q}_q$ is unramified (i.e. $q \neq p$) we can identify $G(K_q/\mathbb{Q}_q)$ with the Galois group $G(k_q/\mathbb{F}_q)$ of the extensions of residue class fields.

Let σ denote the fixed generator of G.

Define f_q by $\pi_q = \sigma^{f_q}$ (π_q the Frobenius at q) modulo l.

(1.1) can be seen as a linear equation relating the indeterminates $\{f_q, inv_p(a)$. Hence we have to produce enough equations of this form in order to apply linear algebra modulo l to compute "enough" factors f_q.

Definition 1.5.1 *A natural number $n \in \mathbb{N}$ is M–smooth iff the following holds:*

$$q\, prime, q|n \Rightarrow q \leq M.$$

Let $\psi(x, y)$ denote the number of natural numbers $n \leq x$ which are y–smooth.

Theorem 3 *Let ε be an arbitrary positive constant, then we have uniformly for $x \geq 10$ and $y \geq (\log x)^{1+\varepsilon}$:*

$$\psi(x,y) = xu^{-u+o(u)} \quad \textit{für}\, x \to \infty \tag{1.2}$$

where $u = (\log x)/(\log y)$.

One algorithm for $K = \mathbb{Q}$

Choose a smoothness bound M and compute the factor basis S consisting of the primes less or equal to M.

Let d be the smallest number $\geq \sqrt{p}$.
For $\delta \in L := [0, ..., l]$ take
$a_1(\delta) := d + \delta$.
$a_2(\delta) := c_0 + 2\delta \cdot d + \delta^2)$
$(\equiv a^2$ modulo $p)$
with $c_0 = d^2 - p$.
Assume that for $\delta \in L$ both $a_1(\delta)$ and $a_2(\delta)$ are $M-$smooth. Then we get a relation for the f_q for q in the factor base.
To find such $\delta \in L$ we can use sieves.
Having enough relations for a large enough factor base we can proceed as usual: For random a we take small powers of a and hope that modulo p such a power yields a smooth number. Then we can compute the invariant of the corresponding algebra and so the invariant of a and use this for computing discrete logarithms.

This approach unifies methods and results obtained by various authors
(Coppersmith, ElGamal,
Schirokauer,Adleman-Huang)
using different and quite complicated methods for different cases. The most advanced amongst them are called number field sieve and function field sieve. All these methods can be explained by Brauer groups and so class field theory of global fields is the right background for the DL in finite fields. That point of view could open new possibilities for more advanced attacks for instance by lifting from local Brauer groups to global Brauer groups in a more intelligent way.

1.6 Scalar Restriction

Another example to use the
extra structure:
Frobenius endomorphism
is the scalar restriction.
It is applied to curves which are not defined over prime fields.
It can be used to transfer DL's in many elliptic curves to DL's in Jacobians of curves for which the index-calculus method works.

1.6.1 Descent

In a lecture at the ECC 1998 I proposed to look at the following well known fact:
An abelian variety of dimension d over $\mathbb{F}_q$ corresponds to an abelian variety of dimension $f \cdot d$ over $\mathbb{F}_{l_0}$.

Mathematical procedure: Take a field K and a finite separable field extension L/K. Let V be a quasi-projective variety (i.e. V can be embedded into a projective space) defined over L.
Then there is a quasi-projective variety W_V defined over K with
$W_V(K) = V(L)$ and $W_V \times L \simeq V^{[L:K]}$. Recipe:
Choose coordinate functions $X_1, \cdots, X_n$ of V over L and a basis $(u_1, \cdots, u_m)$ of L/K. Define the $n \cdot m$ variables $Y_{i,j}$ by

$$X_i = u_1 Y_{1,i} + \cdots + u_m Y_{m,i},$$

Plug these expressions into the relations defining V. Next express the coefficients of the resulting relations as linear combinations of the basis $(u_1, \cdots, u_m)$ and order these relations according to this basis to get the relations of the coordinate functions $Y_{1,1}, \cdots, Y_{m,n}$ of W_V over K.

For quasi-projective varieties one has to choose an appropriate cover of V by affine varieties, apply the descent recipe to them and then glue together the resulting affine varieties over K.

The Case of Finite Fields

Take $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$ and let A be an abelian variety of dimension d defined over $\mathbb{F}_{q^m}$.

The Weil restriction W_A is an abelian variety defined over $\mathbb{F}_q$ and its group of $\mathbb{F}_q$-rational points is in a natural way isomorphic to $A(\mathbb{F}_{q^m})$.

So the DL-problem on $A/\mathbb{F}_{q^m}$ is equivalent with the DL-problem on the $m \times d-$dimensional abelian variety W_A over $\mathbb{F}_q$. But W_A has more geometric structure: We find $\mathbb{F}_q$-rational subvarieties like curves and hypersurfaces on W_A which are not on A.

It seems that "in general" these subvarieties are rather complicated. For instance take an elliptic curve E. Then "in general" one expects that the minimal genus of curves on W_E is $\approx 2^m$ and so at least till now we cannot apply this additional information (positively or negatively) to the DL-problem if m is large. But for small m or special fields $\mathbb{F}_q$ one has to expect a different picture.

It seems to be clear that it does not work for random curves or for extensions of large prime degree (which is not a Mersenne prime). **How to use it...:**
Variant 1: Let L be a finite Galois extension of the field K.
Assume that C is a curve defined over L, D a curve defined over K and

$$\varphi : D \times L \to C$$

a non constant morphism defined over L.
Then we have a correspondence map

$$\phi : Pic^0(C) \to Pic^0(D)$$

$$\phi := Norm_{L/K} \circ \varphi^*.$$

Assumption: $ker(\phi)$ is small.
Then the (cryptographically relevant) part of $Pic^0(C)$ is mapped injectively into $Pic^0(D)$ and we have a transfer of the DL-problem in $Pic^0(C)$ into a (possibly easier) DL-problem.

It seems that this variant works
surprisingly well if C is a (hyper-)elliptic curve not defined over K in characteristic 2.
cf. work of Galbraith, Smart, Hess, Gaudry,Diem,...
Key word: **GHS attack**

It relates the DL-problem to the highly interesting theory of fundamental groups of curves over non algebraically closed ground fields.

It certainly would be worth while to study this approach for non projective curves like curves of genus 0 with singularities. Variant 2:
Again assume that C is defined over L.
We apply scalar restriction from L to K to the (generalized) Jacobian variety of C and get a $[L : K]-$dimensional (group scheme) Abelian variety A over K.
Now we look for curves D in $K-$simple factors B of A.
As B is a factor of $Jac(D)$ we can hope to transfer the DL-problem from $Jac(C)$ to $Jac(D)$.

It is not clear whether this variant can be used in practise.
But it leads to interesting mathematical questions:

- Which group schemes have curves of small genus as sub schemes?
- Investigate the Jacobian of modular curves!
- Which curves have the scalar restriction of an abelian variety (e.g. an elliptic curve) as Jacobian?

To the last question: Bouw, Diem and Scholten have found families of such curves!

1.6.2 Trace 0

As always one can find positive aspects, too.
Scalar restriction can be used for constructing abelian varieties as parts of

Jacobians on which one can compute fast.
One begins with a curve over $\mathbb{F}_q$, extends the scalars to $\mathbb{F}_{q^n}$ and takes the part A of the Weil restriction to $\mathbb{F}_q$ on which the trace of Π is equal to 0.

Examples:

1.)Take $C = E$ and $n = 3$.
Then $dim(A) = 2$.
2.)Take $C = E$ and $n = 5$.
Then $dim(A) = 4$
3.) Take C as curve of genus 2 and $n = 3$.
Then $dim(A) = 4$.

In all cases (and the appropriate environments) we get systems which are more efficient than similar systems with elliptic curves.
And, most important: The examples 2.) and 3.) are more resistant against the index-calculus attack and hence more secure than Jacobians of curves of genus 4.