On the discrete logarithm problem in elliptic curves

Claus Diem

University of Leipzig

Some history

At ECC 2004 in Bochum, Pierrick Gaudry presented an index calculus algorithm for the ECDLP over extension fields:

Heuristic claim Let $n \in \mathbb{N}, n \geq 2$ be fixed. Then the ECDLP over fields of the form $\mathbb{F}_{q^n}$ can be solved in an expected time of

$$O(q^{2-\frac{2}{n}}) \ .$$

Some history

At ECC 2004 in Bochum, Pierrick Gaudry presented an index calculus algorithm for the ECDLP over extension fields:

Heuristic claim Let $n \in \mathbb{N}, n \geq 2$ be fixed. Then the ECDLP over fields of the form $\mathbb{F}_{q^n}$ can be solved in an expected time of

$$O(q^{2-\frac{2}{n}}) \ .$$

He mentioned that I have an $L[3/4]$-algorithm for elliptic curves over some fields.

Some history

At ECC 2004 in Bochum, Pierrick Gaudry presented an index calculus algorithm for the ECDLP over extension fields:

Heuristic claim Let $n \in \mathbb{N}, n \geq 2$ be fixed. Then the ECDLP over fields of the form $\mathbb{F}_{q^n}$ can be solved in an expected time of

$$O(q^{2-\frac{2}{n}}) \ .$$

He mentioned that I have an $L[3/4]$-algorithm for elliptic curves over some fields.

On the next day, I claimed:

Some history

Claim. There exists a randomized algorithm which takes as input a tuple $(q, n, E/\mathbb{F}_{q^n}, A, B)$, where q is a prime power, n a natural number, $E/\mathbb{F}_{q^n}$ an elliptic curve and $A, B \in E(\mathbb{F}_{q^n})$ with $B \in \langle A \rangle$, which computes the DLP with respect to A and B and has the following property:

Let us fix $a, b \in \mathbb{R}$ with $0 < a < b$ and let us consider all instances with

$$a \log_2(q) \leq n \leq b \log_2(q).$$

Then restricted to these instances, the algorithm has an expected running time of

$$O\left(2^{D \cdot (n \cdot \log_2(q))^{3/4}}\right) \quad \text{for } D = \frac{4b + \epsilon}{a^{3/4}} \ .$$

Some history

And I continued ...

Some history

And I continued ...

Please note.

1. I do not have a complete proof of this statement.
2. The algorithm is not practical.

The good (and the bad) news

- There is now a proven result:

The good (and the bad) news

- There is now a proven result:

  For fixed $a, b > 0$ and instances with

  $$a \log(q)^{1/3} \leq n \leq b \log(b)$$

  we have an expected time of

  $$e^{O((\log(q^n))^{3/4})} .$$

The good (and the bad) news

- There is now a proven result:

  For fixed $a, b > 0$ and instances with

  $$a \log(q)^{1/3} \leq n \leq b \log(b)$$

  we have an expected time of

  $$e^{O((\log(q^n))^{3/4})} .$$

- The algorithm is still not practical.

A preliminary algorithm

Let an instance $E/\mathbb{F}_{q^n}, A, B$ be given, E in Weierstraß-Form.

Let us for simplicity assume that $\#E(\mathbb{F}_{q^n})$ is prime.

Let $k := \mathbb{F}_q, K := \mathbb{F}_{q^n}$, and let $x : E \longrightarrow \mathbb{P}^1_K$ be as usual.

A preliminary algorithm

1. Determine $N := \#E(K)$.

A preliminary algorithm

1. Determine $N := \#E(K)$.
2. Determine some $m \leq n$ and $c \leq n$.
3. Choose some c-dimensional k-vector subspace U of K.
4. Define a so-called *factor base*

$$\mathcal{F} := \{P \in E(K) \mid x(P) \in U\}$$

Let $\mathcal{F} = \{F_1, \ldots, F_k\}$.

A preliminary algorithm

5. For $i = 1, \ldots, k+1$ do

   Repeat

   Choose $\alpha_i, \beta_i \in \mathbb{Z}/N\mathbb{Z}$ uniformly randomly and try to determine a *relation*

$$P_1 + \cdots + P_m = \alpha_i A + \beta_i B$$

   with $P_1, \ldots, P_m \in \mathcal{F}$.

   Until this was successful.

   Rewrite the relation as

$$\sum_{j=1}^{k} r_{i,j} F_j = \alpha_i A + \beta_i B \ .$$

A preliminary algorithm

6. Determine some $\underline{\gamma} \in (\mathbb{Z}/N\mathbb{Z})^{k+1}$: $\underline{\gamma}R = 0$, $\underline{\gamma} \neq \underline{0}$.

   We have

$$(\sum_i \gamma_i \alpha_i)a + (\sum_i \gamma_i \beta_i)b = 0$$

   and thus

$$b = \frac{-\sum_i \gamma_i \alpha_i}{\sum_i \gamma_i \beta_i} a \ .$$

Relation generation

Given $C\,(=\alpha A+\beta B)\in E(K)$, we want to find a relation

$$P_1+\cdots+P_m=C$$

with $P_1,\ldots,P_m\in\mathcal{F}$.

For this we try to solve systems of multivariate polynomial equations over k.

Relation generation

Idea. For $P_1, \ldots, P_m \in E(\overline{K})$, the condition $P_1 + \cdots + P_m = C$ can be expressed algebraically over K.

We try to find relations by solving systems of polynomial equations over k.

- The space of tuples $(P_1, \ldots, P_m) \in \mathcal{F}^m$ has mc degrees of freedom over k.
- The space of points $C \in E(K)$ has n degrees of freedom over k.

Relation generation

Idea. For $P_1, \ldots, P_m \in E(\overline{K})$, the condition $P_1 + \cdots + P_m = C$ can be expressed algebraically over K.

We try to find relations by solving systems of polynomial equations over k.

- The space of tuples $(P_1, \ldots, P_m) \in \mathcal{F}^m$ has mc degrees of freedom over k.
- The space of points $C \in E(K)$ has n degrees of freedom over k.

$\Longrightarrow$ Let $\delta := mc - n$. Then for fixed C the relations / solutions $(P_1, \ldots, P_m) \in \mathcal{F}^m$ with $P_1 + \cdots + P_m = C$ vary in a δ-dimensional space over k.

Relation generation

Idea. For $P_1, \ldots, P_m \in E(\overline{K})$, the condition $P_1 + \cdots + P_m = C$ can be expressed algebraically over K.

We try to find relations by solving systems of polynomial equations over k.

- The space of tuples $(P_1, \ldots, P_m) \in \mathcal{F}^m$ has mc degrees of freedom over k.
- The space of points $C \in E(K)$ has n degrees of freedom over k.

$\Longrightarrow$ Let $\delta := mc - n$. Then for fixed C the relations / solutions $(P_1, \ldots, P_m) \in \mathcal{F}^m$ with $P_1 + \cdots + P_m = C$ vary in a δ-dimensional space over k.

We want that $\delta = 0$ ...

A new preliminary algorithm

1. Determine $N := \#E(K)$.
2. Determine some $m \leq n$, let $c := \lceil \frac{n}{m} \rceil$ and $\delta := mc - n$. We thus have $n = mc - \delta = (m - \delta) \cdot c + \delta \cdot (c - 1)$.
3. Choose some c-dimensional k-vector subspace U of K and some $c - 1$-dimensional k-vector subspace U' of U.
4. Define a *factor base*

$$\mathcal{F} := \{P \in E(K) \mid x(P) \in U\}$$

and also

$$\mathcal{F}' := \{P \in E(K) \mid x(P) \in U'\} .$$

Let $\mathcal{F} = \{F_1, F_2, \ldots, F_k\}$.

A new preliminary algorithm

5. For $i = 1, \ldots, k+1$ do

   Repeat

   Choose $\alpha_i, \beta_i \in \mathbb{Z}/N\mathbb{Z}$ uniformly randomly and try to determine a *relation*

$$P_1 + \cdots + P_m = \alpha_i A + \beta_i B$$

   with $P_1, \ldots, P_\delta \in \mathcal{F}'$, $P_{\delta+1}, \ldots, P_m \in \mathcal{F}$.

   Until this was successful.

   Rewrite the relation as

$$\sum_{j=1}^{k} r_{i,j} F_j = \alpha_i A + \beta_i B \ .$$

A new preliminary algorithm

6. Determine some $\underline{\gamma} \in (\mathbb{Z}/N\mathbb{Z})^{k+1}$: $\underline{\gamma}R = 0$, $\underline{\gamma} \neq \underline{0}$.

   We have

$$(\sum_i \gamma_i \alpha_i)a + (\sum_i \gamma_i \beta_i)b = 0$$

   and thus

$$b = \frac{-\sum_i \gamma_i \alpha_i}{\sum_i \gamma_i \beta_i} a \ .$$

Decomposition

We need a procedure to compute relations or "decompositions".

Input. $C \in E(K)$.

Output. A relation

$$P_1 + \cdots + P_m = C$$

with

$$P_1, \ldots, P_\delta \in \mathcal{F}', P_{\delta+1}, \ldots, P_m \in \mathcal{F} \ ,$$

that is,

$$x(P_1), \ldots, x(P_\delta) \in U', x(P_{\delta+1}), \ldots, x(P_m) \in U \ .$$

Decomposition

Let $P_1, \ldots, P_m \in E(K)$.

Equivalent are:

- $P_1 + \cdots + P_m = C$

Decomposition

Let $P_1, \ldots, P_m \in E(K)$.

Equivalent are:

- $P_1 + \cdots + P_m = C$
- $(P_1) + \cdots + (P_m) + (-C) \sim (m+1) \cdot O$

Decomposition

Let $P_1, \ldots, P_m \in E(K)$.

Equivalent are:

- $P_1 + \cdots + P_m = C$
- $(P_1) + \cdots + (P_m) + (-C) \sim (m+1) \cdot O$
- $\exists f \in K(E)^* : (f) = (P_1) + \cdots + (P_m) + (-C) - (m+1) \cdot (O)$.
- $\exists f \in L((m+1) \cdot O - (-C)) :$
  $(f) = (P_1) + \cdots + (P_m) + (-C) - (m+1) \cdot (O)$.

Decomposition

Let $P_1, \ldots, P_m \in E(K)$. Let $P_1, \ldots, P_m, C, O$ be distinct. Equivalent are:

- $P_1 + \cdots + P_m = C$
- $(P_1) + \cdots + (P_m) + (-C) \sim (m+1) \cdot O$
- $\exists f \in K(E)^* : (f) = (P_1) + \cdots + (P_m) + (-C) - (m+1) \cdot (O)$.
- $\exists f \in L((m+1) \cdot O - (-C)) :$
  $(f) = (P_1) + \cdots + (P_m) + (-C) - (m+1) \cdot (O)$.
- $\exists f \in L((m+1) \cdot O - (-C)) : \forall i = 1, \ldots, m : f(P_i) = 0$.

Decomposition

Let $P_1, \ldots, P_m \in E(K)$. Let $P_1, \ldots, P_m, C, O$ be distinct.
Equivalent are:

- $P_1 + \cdots + P_m = C$
- $(P_1) + \cdots + (P_m) + (-C) \sim (m+1) \cdot O$
- $\exists f \in K(E)^* : (f) = (P_1) + \cdots + (P_m) + (-C) - (m+1) \cdot (O)$.
- $\exists f \in L((m+1) \cdot O - (-C)) :$
  $(f) = (P_1) + \cdots + (P_m) + (-C) - (m+1) \cdot (O)$.
- $\exists f \in L((m+1) \cdot O - (-C)) : \forall i = 1, \ldots, m : f(P_i) = 0$.

Now: Choose a basis of $L((m+1) \cdot O - (-C))$, expand this over k, restrict $x(P_i)$ to U or to U' ...

Decompositions

Let $C, P_1, \ldots, P_m \in E(K)$. Let $P_1, \ldots, P_m, C, O$ be distinct.
Let $b_1, \ldots, b_m$ be a basis of $L((m+1) \cdot O - (-C))$.
Equivalent are:

- $P_1 + \cdots + P_m = C$
- $\exists \alpha_1, \ldots, \alpha_m \in K : \forall i = 1, \ldots, m : (\sum_\ell \alpha_\ell b_\ell)(P_i) = 0$

For varying $P_1, \ldots, P_m$, we have

- $2m$ variables for the P_i and m equations of degree 3
- $m-1$ variables for the $\alpha_1, \ldots, \alpha_{m-1}$ and m equations of low degree.

Over k, we have

- $n\,m + n$ variables and $n\,m$ equations for the P_i
- $n\,m - n$ variables and $n\,m$ additional equations.

Solving the systems

Over k, we have

- $n\,m + n$ variables and $n\,m$ equations for the P_i
- $n\,m - n$ variables and $n\,m$ additional equations.

In total: $2nm$ variables and $2nm$ equations of low degree over k.

$\Longrightarrow$ We can expect that the system has 0-dimensional solution set.

Solving the systems

Over k, we have

- $n\,m + n$ variables and $n\,m$ equations for the P_i
- $n\,m - n$ variables and $n\,m$ additional equations.

In total: $2nm$ variables and $2nm$ equations of low degree over k.

$\Longrightarrow$ We can expect that the system has 0-dimensional solution set.

(Or maybe not?)

Solving the systems

There are algorithms to determine all k-rational *isolated* solutions of multivariate systems. (Details omitted.)

A point of an algebraic set / scheme is called *isolated* if it is equal to its connected component.

The expected running time is $e^{O(nm)} \cdot \log(q)^{O(1)}$. (Again details omitted.)

Assume that for varying $C \in E(K)$, "most" k-rational solutions are isolated. Then the expected running time for the relation generation is

$$m! \cdot e^{O(nm)} \cdot q^c \ .$$

Solving the systems

There are algorithms to determine all k-rational *isolated* solutions of multivariate systems. (Details omitted.)

A point of an algebraic set / scheme is called *isolated* if it is equal to its connected component.

The expected running time is $e^{O(nm)} \cdot \log(q)^{O(1)}$. (Again details omitted.)

Assume that for varying $C \in E(K)$, "most" k-rational solutions are isolated. Then the expected running time for the relation generation is

$$e^{O(nm+\frac{n}{m}\cdot\log(q))} .$$

The heuristic running time

We have

$$e^{O(nm+\frac{n}{m}\cdot\log(q))}\ .$$

for the relation generation and just $e^{O(\frac{n}{m}\cdot\log(q))}$ for the linear algebra.

For $m=\min(\lceil\sqrt{\log(q)}\rceil,n)$ we have

$$e^{O(\max(n\cdot\sqrt{\log(q)}\,,\log(q)))}\ .$$

Applications

Let us assume an expected running time of

$$e^{O(\max(n\cdot\sqrt{\log(q)}\,,\log(q)))}\,.$$

Then:

- For $n \leq b \cdot \sqrt{\log(q)}$ we have $q^{O(1)}$.
  For

  $$a\sqrt{\log(q)} \leq n \leq b\log(q)$$

  we have

  $$e^{O((\log(q^n))^{2/3})}\,.$$

Applications

Let us assume an expected running time of

$$e^{O(\max(n\cdot\sqrt{\log(q)}\,,\log(q)))}\,.$$

Then:

- For $n \leq b \cdot \sqrt{\log(q)}$ we have $q^{O(1)}$.
  For
  $$a\sqrt{\log(q)} \leq n \leq b\log(q)$$
  we have
  $$e^{O((\log(q^n))^{2/3})}\,.$$

$$q = e^{\log(q)} = e^{(\log(q)^{3/2})^{2/3}} = e^{(\sqrt{\log(q)}\cdot\log(q))^{2/3}} \leq e^{(\frac{1}{a}n\log(q))^{2/3}}$$

Applications

Let us assume an expected running time of

$$e^{O(\max(n\cdot\sqrt{\log(q)},\log(q)))}.$$

Then:

- For

  $$a\log(q) \leq n \leq b\log(q)$$

  we have

  $$e^{O((\log(q^n))^{3/4})}.$$

Geometry

Let $\mathrm{Res}_{K|k}(E)$ be the Weil restriction of E w.r.t. $K|k$. This is an n-dimensional abelian variety over k with

$$\mathrm{Res}_{K|k}(E)(k) \simeq E(K) \ .$$

More generally, for any k-scheme S,

$$\mathrm{Res}_{K|k}(E)(S) \simeq E(S \times_k K) \ .$$

Geometry

Let $\mathrm{Res}_{K|k}(E)$ be the Weil restriction of E w.r.t. $K|k$. This is an n-dimensional abelian variety over k with

$$\mathrm{Res}_{K|k}(E)(k) \simeq E(K) \ .$$

More generally, for any k-scheme S,

$$\mathrm{Res}_{K|k}(E)(S) \simeq E(S \times_k K) \ .$$

We also have $\mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ with

$$\mathrm{Res}_{K|k}(\mathbb{A}^1_K)(k) \simeq K \ .$$

We have $\mathrm{Res}_{K|k}(\mathbb{A}^1_K)(k) \simeq \mathbb{A}^n_k$. Such an isomorphism corresponds to an isomorphism $K \simeq k^n$.

Geometry

Let $E_a := x^{-1}(\mathbb{A}^1_K)$ be the "affine part" of E.

The covering $x : E_a \longrightarrow \mathbb{A}^1_K$ induces a covering

$$\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$$

of degree 2^n.

Geometry

Let $E_a := x^{-1}(\mathbb{A}^1_K)$ be the "affine part" of E.

The covering $x : E_a \longrightarrow \mathbb{A}^1_K$ induces a covering

$$\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$$

of degree 2^n.

$U \leq K$ corresponds to a subgroup-variety A of $\mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ with

$$A(k) = U \ .$$

Geometry

Let $E_a := x^{-1}(\mathbb{A}^1_K)$ be the "affine part" of E.

The covering $x : E_a \longrightarrow \mathbb{A}^1_K$ induces a covering

$$\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$$

of degree 2^n.

$U \leq K$ corresponds to a subgroup-variety A of $\mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ with

$$A(k) = U \ .$$

Likewise U' corresponds to a subgroup-variety A' of A with

$$A'(k) = U' \ .$$

Geometry

Let V be defined by the following diagram being Cartesian.

$$\begin{array}{ccc} V & \hookrightarrow & \mathrm{Res}_{K|k}(E_a) \\ \downarrow & & \downarrow \mathrm{Res}(x) \\ A & \hookrightarrow & \mathrm{Res}_{K|k}(\mathbb{A}^1_K) \end{array} .$$

We have $\mathcal{F} \simeq V(k)$.

Let V' be defined similarly. Then also $\mathcal{F} \simeq V'(k)$.

Geometry

The addition map $(\mathcal{F}')^{\delta} \times \mathcal{F}^{m-\delta} \longrightarrow E(K)$ corresponds to the addition map

$$V'(k)^{\delta} \times V(k)^{m-\delta}(k) \longrightarrow \mathrm{Res}_{K|k}(E)(k) \ .$$

Let

$$a_m : (V')^{\delta} \times V(k)^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

be the addition map.

Geometry

The addition map $(\mathcal{F}')^{\delta} \times \mathcal{F}^{m-\delta} \longrightarrow E(K)$ corresponds to the addition map

$$V'(k)^{\delta} \times V(k)^{m-\delta}(k) \longrightarrow \mathrm{Res}_{K|k}(E)(k) \ .$$

Let

$$a_m : (V')^{\delta} \times V(k)^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

be the addition map.

For $C \in E(K) \simeq \mathrm{Res}_{K|k}(E)(k)$ we want to study the preimage of C in $(V')^{\delta} \times V^{m-\delta}$.

Geometry

The addition map $(\mathcal{F}')^{\delta} \times \mathcal{F}^{m-\delta} \longrightarrow E(K)$ corresponds to the addition map

$$V'(k)^{\delta} \times V(k)^{m-\delta}(k) \longrightarrow \mathrm{Res}_{K|k}(E)(k) \ .$$

Let

$$a_m : (V')^{\delta} \times V(k)^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

be the addition map.

For $C \in E(K) \simeq \mathrm{Res}_{K|k}(E)(k)$ we want to study the preimage of C in $(V')^{\delta} \times V^{m-\delta}$.

This is called the *fiber* at C.

Geometry

Let still

$$a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

Main task. Let $C \in E(K)$ be uniformly distributed. Give now a suitable lower bound on the probability that the fiber of C contains an isolated k-rational point!

Geometry

Let still

$$a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

Main task. Let $C \in E(K)$ be uniformly distributed. Give now a suitable lower bound on the probability that the fiber of C contains an isolated k-rational point!

Note: $\mathrm{Res}_{K|k}(E)(k)$ and $(V')^{\delta} \times V^{m-\delta}$ have dimension n.

Geometry

Let still

$$a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

Main task. Let $C \in E(K)$ be uniformly distributed. Give now a suitable lower bound on the probability that the fiber of C contains an isolated k-rational point!

Note: $\mathrm{Res}_{K|k}(E)(k)$ and $(V')^{\delta} \times V^{m-\delta}$ have dimension n.

Question. Is $a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E)$ surjective?

Geometry

Let still

$$a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

Main task. Let $C \in E(K)$ be uniformly distributed. Give now a suitable lower bound on the probability that the fiber of C contains an isolated k-rational point!

Note: $\mathrm{Res}_{K|k}(E)(k)$ and $(V')^{\delta} \times V^{m-\delta}$ have dimension n.

Question. Is $a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E)$ surjective on every irreducibility component of $(V')^{\delta} \times V^{m-\delta}$?

Geometry

Let still

$$a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

Main task. Let $C \in E(K)$ be uniformly distributed. Give now a suitable lower bound on the probability that the fiber of C contains an isolated k-rational point!

Note: $\mathrm{Res}_{K|k}(E)(k)$ and $(V')^{\delta} \times V^{m-\delta}$ have dimension n.

Question. Is $a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E)$ surjective on every irreducibility component of $(V')^{\delta} \times V^{m-\delta}$?

Difficult!

Geometry

Let still

$$a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

Observation. Let $(P_1, \ldots, P_m) \in ((V')^{\delta} \times V^{m-\delta})(k)$, $C := P_1 + \cdots + P_m$.

Equivalent are:

- $(P_1, \ldots, P_m)$ is isolated and reduced in the fiber of C.
- a_m is unramified at $(P_1, \ldots, P_m)$.
- $(a_m)_* : T_{(P_1,\ldots,P_m)}((V')^{\delta} \times V^{m-\delta}) \longrightarrow T_C(\mathrm{Res}_{K|k}(E))$ is injective.

Moreover, “unramifiedness” is an open property ...

New algorithm

Choose a decomposition

$$K = \bigoplus_{i=1}^{m} U_i \ .$$

Let

$$\mathcal{F}_i := \{P \in E(K) \mid x(P) \in U_i\}$$

and

$$\mathcal{F} := \bigcup_{i=1}^{m} \mathcal{F}_i \ .$$

New algorithm

Choose a decomposition

$$K = \bigoplus_{i=1}^{m} U_i \ .$$

Let

$$\mathcal{F}_i := \{P \in E(K) \mid x(P) \in U_i\}$$

and

$$\mathcal{F} := \bigcup_{i=1}^{m} \mathcal{F}_i \ .$$

We want to find relations of the form

$$P_1 + \cdots + P_m = C \ \text{ with } P_i \in \mathcal{F}_i \ .$$

New algorithm

The decomposition

$$K = \bigoplus_{i=1}^{m} U_i$$

corresponds to a decomposition

$$\mathbb{A}_k^n \simeq \mathrm{Res}_{K|k}(\mathbb{A}_K^1) = \bigoplus_{i=1}^{m} A_i \ .$$

Let V_i be as V above. We thus have

$$V_i(k) \simeq \mathcal{F}_i \ .$$

New algorithm

Let $0 \in \mathbb{A}^1(K)$ be unramified and split under $x : E_a \longrightarrow \mathbb{A}^1_K$; let $P_0 \in E(K)$ be a preimage.

Now $\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ is unramified at $P_0 \in \mathrm{Res}_{K|k}(E)(k)$.

New algorithm

Let $0 \in \mathbb{A}^1(K)$ be unramified and split under $x : E_a \longrightarrow \mathbb{A}^1_K$; let $P_0 \in E(K)$ be a preimage.

Now $\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ is unramified at $P_0 \in \mathrm{Res}_{K|k}(E)(k)$.

We want to study the fibers of the map

$$a_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

New algorithm

Let $0 \in \mathbb{A}^1(K)$ be unramified and split under $x : E_a \longrightarrow \mathbb{A}^1_K$; let $P_0 \in E(K)$ be a preimage.

Now $\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ is unramified at $P_0 \in \mathrm{Res}_{K|k}(E)(k)$.

We want to study the fibers of the map

$$a_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

Claim. This map is unramified at $(P_0, \ldots, P_0) \in (V_1 \times \cdots \times V_m)(k)$.

$\Longrightarrow$ If the V_i are irreducible, the map is generically unramified, thus generically quasi-finite.

New algorithm

Proof of claim.

We have

$$a_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_{K|k}(E) \ .$$

This morphism is unramified at $(P_0, \ldots, P_0)$ if and only if the map

$$(a_m)_* : T_{(P_0,\ldots,P_0)}(V_1 \times \cdots \times V_m) \longrightarrow T_{mP_0}(\mathrm{Res}_{K|k}(E))$$

is injective.

New algorithm

We have

$$
\begin{array}{ccc}
T_{(P_0,\ldots,P_0)}(V_1 \times \cdots \times V_m) & \xrightarrow{(a_m)_*} & T_{mP_0}(\mathrm{Res}_{K|k}(E)) \\
\updownarrow & & \uparrow (\tau_{((m-1)P_0)})_* \\
T_{P_0}(V_1) \times \cdots \times T_{P_0}(V_m) & \xrightarrow{\Sigma} & T_{P_0}(\mathrm{Res}_{K|k}(E)) \\
\downarrow & & \downarrow \mathrm{Res}(x)_* \\
T_0(A_1) \times \cdots \times T_0(A_m) & \xrightarrow{\Sigma} & T_0(\mathrm{Res}_{K|k}(\mathbb{A}^1_K)) \\
\| & & \| \\
U_1 \times \cdots \times U_m & \xrightarrow{\Sigma} & K \ .
\end{array}
$$

New algorithm

Let now $(P_1, \ldots, P_m) \in V_1(k) \times \cdots \times V_m(k)$. Then the map

$$a_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_{K|k}(E)$$

is unramified at $(P_1, \ldots, P_m)$ if and only if we have

$$T_{P_0}(\mathrm{Res}_{K|k}(E)) = \bigoplus_{i=1}^{m} (\tau_{(P_0 - P_i)})_* (T_{P_i}(V_i)) \ .$$

This can be studied explicitly.

New algorithm

Let now $(P_1, \ldots, P_m) \in V_1(k) \times \cdots \times V_m(k)$. Then the map

$$a_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_{K|k}(E)$$

is unramified at $(P_1, \ldots, P_m)$ if and only if we have

$$T_{P_0}(\mathrm{Res}_{K|k}(E)) = \bigoplus_{i=1}^{m} (\tau_{(P_0 - P_i)})_* (T_{P_i}(V_i)) \ .$$

This can be studied explicitly.

- Let $\mathrm{char}(k)$ be odd. We have the holomorphic differential $\frac{dx}{y}$ and the holomorphic tangent vector field yt_x.

New algorithm

Let now $(P_1, \ldots, P_m) \in V_1(k) \times \cdots \times V_m(k)$. Then the map

$$a_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_{K|k}(E)$$

is unramified at $(P_1, \ldots, P_m)$ if and only if we have

$$T_{P_0}(\mathrm{Res}_{K|k}(E)) = \bigoplus_{i=1}^{m} (\tau_{(P_0 - P_i)})_* (T_{P_i}(V_i)) \ .$$

This can be studied explicitly.

- Let $\mathrm{char}(k)$ be even, E non-supersingular. We have $\frac{dx}{x}$ and xt_x.

New algorithm

Let now $(P_1, \ldots, P_m) \in V_1(k) \times \cdots \times V_m(k)$. Then the map

$$a_m : V_1 \times \cdots \times V_m \longrightarrow \mathrm{Res}_{K|k}(E)$$

is unramified at $(P_1, \ldots, P_m)$ if and only if we have

$$T_{P_0}(\mathrm{Res}_{K|k}(E)) = \bigoplus_{i=1}^{m} (\tau_{(P_0 - P_i)})_* (T_{P_i}(V_i)) \ .$$

This can be studied explicitly.

- Let $\mathrm{char}(k)$ be even and E supersingular. We have dx and t_x.

And some conditions

Additionally, we have some conditions:

- $\#V_i(k)$ should have at least $\frac{1}{4} \cdot q^{\dim(V_i)}$ elements.
- For odd characteristic, the V_i have to be irreducible.

The results

Theorem. The discrete logarithm problem in the groups of rational points of elliptic curves over fields $\mathbb{F}_{q^n}$ can be solved in an expected time of

$$e^{O(\max(\log(q),n\cdot\log(q)^{1/2},n^{3/2}))}.$$

Under the condition that q is even it can be solved in an expected time of

$$e^{O(\max(\log(q),n\cdot\log(q)^{1/2},n\cdot\log(n)^{1/2}))}.$$

My works

- Habilitation thesis: On arithmetic and the discrete logarithm problem in class groups of curves, 2008
- On the discrete logarithm problem in elliptic curves. Compositio Mathematica No. 147, 2011
- On the discrete logarithm problem in elliptic curves II. Submitted, 2011