Sur le problème du logarithme discret dans les courbes elliptiques

Claus Diem

Un peu d'histoire

Le problème du logarithme discret classique

On considère le problème du logarithme discret dans les groupes $\mathbb{F}_p^*$, p premier.

Un peu d'histoire

Le problème du logarithme discret classique

On considère le problème du logarithme discret dans les groupes $\mathbb{F}_p^*$, p premier.

Avec l'algorithme $\ll$ Baby-Step-Giant-Step $\gg$ on peut le résoudre en temps

$$\tilde{O}(\sqrt{p}) \ .$$

Un peu d'histoire

Le problème du logarithme discret classique

On considère le problème du logarithme discret dans les groupes $\mathbb{F}_p^*$, p premier.

Avec l'algorithme « Baby-Step-Giant-Step » on peut le résoudre en temps

$$\tilde{O}(\sqrt{p}) \, .$$

Théorème (Pomerance, 1987) Ce problème peut être résolu en temps

$$e^{O((\log(p)\cdot\log\log(p))^{1/2})}$$

avec un algorithme randomisé.

Un peu d'histoire

Le problème du logarithme discret classique

On considère le problème du logarithme discret dans les groupes $\mathbb{F}_p^*$, p premier.

Avec l'algorithme « Baby-Step-Giant-Step » on peut le résoudre en temps

$$\tilde{O}(\sqrt{p}) \ .$$

Théorème (Pomerance, 1987) Ce problème peut être résolu en temps

$$e^{O((\log(p)\cdot\log\log(p))^{1/2})}$$

avec un algorithme randomisé.

On utilise la méthode de « calcul d'index ».

Un peu d'histoire

1985

Victor Miller et Neal Koblitz proposent de considérer le problème du logarithme discret dans les courbes elliptiques sur les corps finis pour des applications cryptographiques.

Un peu d'histoire

1985

Victor Miller et Neal Koblitz proposent de considérer le problème du logarithme discret dans les courbes elliptiques sur les corps finis pour des applications cryptographiques.

Victor Miller argumente que cela devrait être plus efficace que l'utilisation du problème du logarithme discret classique ...

Un peu d'histoire

1985

Victor Miller et Neal Koblitz proposent de considérer le problème du logarithme discret dans les courbes elliptiques sur les corps finis pour des applications cryptographiques.

Victor Miller argumente que cela devrait être plus efficace que l'utilisation du problème du logarithme discret classique ...

... parce qu'il devrait être difficile d'appliquer la méthode du calcul d'index à ces groupes.

Un peu d'histoire

2004

Suivant un preprint de Igor Semaev, Pierrick Gaudry obtient un algorithme de calcul d'index dans les courbes elliptiques sur les corps finis non premiers.

Assertion heuristique Soit $n \in \mathbb{N}, n \geq 2$ fixé. Alors le problème du logarithme discret dans les courbes elliptiques sur les corps $\mathbb{F}_{q^n}$ peut être résolu en temps

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

avec un algorithme randomisé.

Un peu d'histoire

2004

Suivant un preprint de Igor Semaev, Pierrick Gaudry obtient un algorithme de calcul d'index dans les courbes elliptiques sur les corps finis non premiers.

Assertion heuristique Soit $n \in \mathbb{N}, n \geq 2$ fixé. Alors le problème du logarithme discret dans les courbes elliptiques sur les corps $\mathbb{F}_{q^n}$ peut être résolu en temps

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

avec un algorithme randomisé.

$$n = 3 : \qquad \frac{4}{3} < \frac{3}{2}$$

Mes résultats

Considérons le problème du logarithme discret dans les courbes elliptiques sur les corps finis $\mathbb{F}_{q^n}$.

Mes résultats

Considérons le problème du logarithme discret dans les courbes elliptiques sur les corps finis $\mathbb{F}_{q^n}$. Alors :

- Soient $a, b > 0$ fixés. Alors restreint aux instances avec

$$a \log(q)^{1/2} \leq n \leq b \log(q)^{1/2}$$

on peut résoudre le problème en temps

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

avec un algorithme randomisé.

Mes résultats

Considérons le problème du logarithme discret dans les courbes elliptiques sur les corps finis $\mathbb{F}_{q^n}$. Alors :

- Soient $a, b > 0$ fixés. Alors restreint aux instances avec

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

on peut résoudre le problème en temps

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

avec un algorithme randomisé.

Mes résultats

Considérons le problème du logarithme discret dans les courbes elliptiques sur les corps finis $\mathbb{F}_{q^n}$. Alors :

- Soient $n \in \mathbb{N}, n \geq 2$ fixé. Alors restreint à ces instances on peut résoudre le problème en temps

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

avec un algorithme randomisé.

Un algorithme préliminaire

Soit un instance $E/\mathbb{F}_{q^n}, A, B \in E(\mathbb{F}_{q^n}), B \in \langle A \rangle$ donné,
E en forme de Weierstraß.

Supposons pour simplifier que $\#E(\mathbb{F}_{q^n})$ est premier.

Soit $k := \mathbb{F}_q$ et $K := \mathbb{F}_{q^n}$ et soit $x : E \longrightarrow \mathbb{P}^1_K$ comme d'habitude.

Un algorithme préliminaire

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

Un algorithme préliminaire

1. Calculer $N := \#E(K)$.
2. Déterminer $m \leq n$ et $c \leq n$.
3. Choisir un sous-espace vectoriel U de K sur k de dimension c.
4. Définir la *base de facteurs*

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

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

Un algorithme préliminaire

5. Pour $i = 1, \ldots, k+1$:

   Répéter

   Choisir $\alpha_i, \beta_i \in \mathbb{Z}/N\mathbb{Z}$ uniformément randomisés et essayer de trouver une *relation*

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

   Jusqu'à en trouver une.

   Réécrire la relation comme

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

Un algorithme préliminaire

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

   [Nous avons

$$(\sum_i \gamma_i \alpha_i) A + (\sum_i \gamma_i \beta_i) B = 0 \ .]$$

7. Si $\sum_i \gamma_i \beta_i \neq 0$, sortir $-\dfrac{\sum_i \gamma_i \alpha_i}{\sum_i \gamma_i \beta_i}$.

Génération des relations

Etant donné $C(= \alpha A + \beta B) \in E(K)$, nous voulons trouver une relation / « décomposition »

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

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

Pour cela nous essayons de résoudre des systèmes d'équations polynomiales sur k.

Génération de relations / décompositions

Idée. Pour $P_1, \ldots, P_m, C \in E(\overline{K})$, la condition $C = P_1 + \cdots + P_m$ peut être exprimée algébriquement sur K.

Nous essayons de trouver des relations en résolvant des systèmes d'équations polynomiales sur k.

Génération de relations / décompositions

Idée. Pour $P_1, \ldots, P_m, C \in E(\overline{K})$, la condition $C = P_1 + \cdots + P_m$ peut être exprimée algébriquement sur K.

Nous essayons de trouver des relations en résolvant des systèmes d'équations polynomiales sur k.

Considérations heuristiques :

- L'espace des tuples $(P_1, \ldots, P_m) \in \mathcal{F}^m$ a mc « degrés de liberté » sur k.
- L'espace des points $C \in E(K)$ a n « degrés de liberté » sur k.

$\overset{?}{\Longrightarrow}$ Soit $\delta := mc - n$. Alors pour C fixé les relations / solutions $(P_1, \ldots, P_m) \in \mathcal{F}^m$ avec $C = P_1 + \cdots + P_m$ varient dans un espace δ-dimensionnel sur k.

Génération de relations / décompositions

Idée. Pour $P_1, \ldots, P_m, C \in E(\overline{K})$, la condition $C = P_1 + \cdots + P_m$ peut être exprimée algébriquement sur K.

Nous essayons de trouver des relations en résolvant des systèmes d'équations polynomiales sur k.

Considérations heuristiques :

- L'espace des tuples $(P_1, \ldots, P_m) \in \mathcal{F}^m$ a mc « degrés de liberté » sur k.
- L'espace des points $C \in E(K)$ a n « degrés de liberté » sur k.

$\overset{?}{\Longrightarrow}$ Soit $\delta := mc - n$. Alors pour C fixé les relations / solutions $(P_1, \ldots, P_m) \in \mathcal{F}^m$ avec $C = P_1 + \cdots + P_m$ varient dans un espace δ-dimensionnel sur k.

Nous voulons que $\delta = 0$ ...

Un algorithme nouveau

1. Calculer $N := \#E(K)$.
2. Déterminer un $m \leq n$, soit $c := \lceil \frac{n}{m} \rceil$ et $\delta := mc - n$.
   [Nous avons donc $n = mc - \delta = (m - \delta) \cdot c + \delta \cdot (c - 1)$.]
3. Choisir un sous-espace vectoriel U de K sur k de dimension c et un sous-espace vectoriel U' de U de dimension $c - 1$.
4. Définir la *base de facteurs*

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

et de plus

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

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

Un algorithme nouveau

5. Pour $i = 1, \ldots, k+1$:

   Répéter

   Choisir $\alpha_i, \beta_i \in \mathbb{Z}/N\mathbb{Z}$ uniformément randomisés et essayer de déterminer une *relation*

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

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

   Jusqu'à en trouver une.

   Réécrire la relation comme

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

Un algorithme préliminaire

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

   [Nous avons

$$(\sum_i \gamma_i \alpha_i) A + (\sum_i \gamma_i \beta_i) B = 0 \ .]$$

7. Si $\sum_i \gamma_i \beta_i \neq 0$, sortir $-\dfrac{\sum_i \gamma_i \alpha_i}{\sum_i \gamma_i \beta_i}$.

Décomposition

Nous avons besoin d'un procédure pour calculer des relations / décompositions.

Entrée. $C \in E(K)$.

Sortie. Une relation / décomposition

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

avec

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

i.e.

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

Ou « rien ».

Décomposition

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

Décomposition

Soient $P_1, \ldots, P_m \in E(K)$. Soient $P_1, \ldots, P_m, C, O$ différents.

Conditions équivalentes :

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

Décomposition

Soient $P_1, \ldots, P_m \in E(K)$. Soient $P_1, \ldots, P_m, C, O$ différents.

Conditions équivalentes :

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

Maintenant : Choisir une base de $L((m+1) \cdot O - (-C))$, l'étendre sur k, restreindre $x(P_i)$ à U ou à U'.

Décomposition

Soient $C, P_1, \ldots, P_m \in E(K)$. Soient $P_1, \ldots, P_m, C, O$ différents. Soit $b_1, \ldots, b_m$ une base de $L((m+1) \cdot O - (-C))$.

Conditions équivalentes :

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

Pour $P_1, \ldots, P_m$ variables nous avons

- $2m$ variables pour les P_i et m équations de degré 3
- $m-1$ variables pour les $\alpha_1, \ldots, \alpha_{m-1}$ et m équations de bas degré.

Résoudre les systèmes

Sur k, nous avons

- $n\,m + n$ variables et $n\,m$ équations pour les P_i
- $n\,m - n$ variables et $n\ m$ équations de plus.

En total : $2nm$ variables et $2nm$ équations de bas degré sur k.

$\Longrightarrow$ Nous nous attendons à ce que l'espace de solutions du système soit 0-dimensionnel.

Résoudre les systèmes

Sur k, nous avons

- $n\,m + n$ variables et $n\,m$ équations pour les P_i
- $n\,m - n$ variables et $n\ m$ équations de plus.

En total : $2nm$ variables et $2nm$ équations de bas degré sur k.

$\Longrightarrow$ Nous nous attendons à ce que l'espace de solutions du système soit 0-dimensionnel.

Ou peut-être pas ?

Résoudre les systèmes

Théorème (Canny, 1987) Il y a un algorithme randomisé avec les propriétés suivantes :

Entrée. $f_1, \ldots, f_n \in \mathbb{F}_q[x_1, \ldots, x_n]$.

Sortie. Toutes les solutions k-rationnelles isolées.

Temps de calcul. $(\deg(f_1) \cdots \deg(f_n) \cdot \log(q))^{O(1)}$.

Un point d'un ensemble algébrique / d'un schéma est appelé *isolé* s'il est égal à sa composante connexe.

Résoudre les systèmes

Pour nous, le temps de calcul est $e^{O(nm)} \cdot \log(q)^{O(1)}$ avec une variante de cet algorithme pour des systèmes creux. (Nous utilisons un algorithme de Maurice Rojas reposant sur les résultants toriques.)

Supposons que pour $C \in E(K)$ variable $\ll$ la plupart $\gg$ des solutions sont isolées.

$\Longrightarrow$ Le temps pour la génération des relations est

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

Résoudre les systèmes

Pour nous, le temps de calcul est $e^{O(nm)} \cdot \log(q)^{O(1)}$ avec une variante de cet algorithme pour des systèmes creux. (Nous utilisons un algorithme de Maurice Rojas reposant sur les résultants toriques.)

Supposons que pour $C \in E(K)$ variable $\ll$ la plupart $\gg$ des solutions sont isolées.

$\Longrightarrow$ Le temps pour la génération des relations est

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

alors

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

Le temps de calcul heuristique

Nous avons :

- $e^{O(nm+\frac{n}{m}\cdot\log(q))}$ pour la génération des relations

Le temps de calcul heuristique

Nous avons :

- $e^{O(nm+\frac{n}{m}\cdot\log(q))}$ pour la génération des relations

  et
- $e^{O(\frac{n}{m}\cdot\log(q))}$ pour l'algèbre linéaire.

Le temps de calcul heuristique

Nous avons :

- $e^{O(nm+\frac{n}{m}\cdot\log(q))}$ pour la génération des relations

  et
- $e^{O(\frac{n}{m}\cdot\log(q))}$ pour l'algèbre linéaire.

Avec $m = \min(\lceil\sqrt{\log(q)}\rceil, n)$ nous avons

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

Applications

Supposons un temps de calcul de

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

Applications

Supposons un temps de calcul de

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

Alors :

- Avec $n \leq b \cdot \sqrt{\log(q)}$ nous avons $q^{O(1)}$.

Applications

Supposons un temps de calcul de

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

Alors :

- Avec $n \leq b \cdot \sqrt{\log(q)}$ nous avons $q^{O(1)}$.

  Pour

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

  nous avons

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

Applications

Supposons un temps de calcul de

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

Alors :

- Avec $n \leq b \cdot \sqrt{\log(q)}$ nous avons $q^{O(1)}$.

  Pour

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

  nous avons

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

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

Applications

Supposons un temps de calcul de

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

Alors :

- Pour

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

nous avons

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

Géométrie

Soit $\mathrm{Res}_{K|k}(E)$ la restriction de Weil de E relative à $K|k$.
C'est une variété abélienne de dimension n sur k avec :
Pour tout k-schéma S,

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

Géométrie

Soit $\mathrm{Res}_{K|k}(E)$ la restriction de Weil de E relative à $K|k$.
C'est une variété abélienne de dimension n sur k avec :
Pour tout k-schéma S,

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

En particulier,

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

Géométrie

A chaque espace vectoriel de dimension finie W sur k on peut associer fonctoriellement un espace affine dans la catégorie de groupes algébriques sur k

$$\mathbb{A}_k[W]$$

avec

$$\mathbb{A}_k[W](k) = (W, +)$$

et

$$T_0(\mathbb{A}_k[W]) = W \ .$$

Géométrie

A chaque espace vectoriel de dimension finie W sur k on peut associer fonctoriellement un espace affine dans la catégorie de groupes algébriques sur k

$$\mathbb{A}_k[W]$$

avec

$$\mathbb{A}_k[W](k) = (W, +)$$

et

$$T_0(\mathbb{A}_k[W]) = W\ .$$

On a

$$\mathrm{Res}_{K|k}(\mathbb{A}^1_k)(k) = (K, +)$$

et

$$\mathrm{Res}_{K|k}(\mathbb{A}^1_k) = \mathbb{A}_k[K]\ .$$

Géométrie

Soit $E_a := x^{-1}(\mathbb{A}^1_K)$, la « partie affine » de E.

Le revêtement $x : E_a \longrightarrow \mathbb{A}^1_K$ induit un revêtement

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

de degré 2^n.

Géométrie

Soit $E_a := x^{-1}(\mathbb{A}^1_K)$, la « partie affine » de E.

Le revêtement $x : E_a \longrightarrow \mathbb{A}^1_K$ induit un revêtement

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

de degré 2^n.

L'inclusion $U \hookrightarrow K$ induit une immersion fermée

$$\mathbb{A}_k[U] \hookrightarrow \mathbb{A}_k[K]$$

Géométrie

Soit $E_a := x^{-1}(\mathbb{A}^1_K)$, la « partie affine » de E.
Le revêtement $x : E_a \longrightarrow \mathbb{A}^1_K$ induit un revêtement

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

de degré 2^n.

L'inclusion $U \hookrightarrow K$ induit une immersion fermée

$$\mathbb{A}_k[U] \hookrightarrow \mathbb{A}_k[K] \,,$$

de même

$$\mathbb{A}_k[U'] \hookrightarrow \mathbb{A}_k[K] \,.$$

Géométrie

Soit V défini par le diagramme cartésien

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

Nous avons $\mathcal{F} \simeq V(k)$.

Soit V' défini similairement. Alors on a aussi $\mathcal{F}' \simeq V'(k)$.

Géométrie

L'application d'addition $(\mathcal{F}')^{\delta} \times \mathcal{F}^{m-\delta} \longrightarrow E(K)$ correspond à l'application d'addition

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

Soit

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

le morphisme d'addition.

Géométrie

L'application d'addition $(\mathcal{F}')^{\delta} \times \mathcal{F}^{m-\delta} \longrightarrow E(K)$ correspond à l'application d'addition

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

Soit

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

le morphisme d'addition.

Pour $C \in E(K) \simeq \mathrm{Res}_{K|k}(E)(k)$ nous voulons étudier l'image réciproque de C dans $(V')^{\delta} \times V^{m-\delta}$.

Géométrie

L'application d'addition $(\mathcal{F}')^{\delta} \times \mathcal{F}^{m-\delta} \longrightarrow E(K)$ correspond à l'application d'addition

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

Soit

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

le morphisme d'addition.

Pour $C \in E(K) \simeq \mathrm{Res}_{K|k}(E)(k)$ nous voulons étudier l'image réciproque de C dans $(V')^{\delta} \times V^{m-\delta}$.

Autrement dit : nous voulons étudier la *fibre* sur C.

Géométrie

Soit encore

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

But principal. Pour $C \in E(K) \simeq \mathrm{Res}_{K|k}(E)(k)$ distribué uniformément, donner une borne inférieure sur la probabilité que la fibre sur C contient un point k-rationnel isolé !

Géométrie

Soit encore

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

But principal. Pour $C \in E(K) \simeq \mathrm{Res}_{K|k}(E)(k)$ distribué uniformément, donner une borne inférieure sur la probabilité que la fibre sur C contient un point k-rationnel isolé !

Remarquons : $\mathrm{Res}_{K|k}(E)$ et $(V')^{\delta} \times V^{m-\delta}$ sont de dimension n.

Question. A-t-on $a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E)$ surjective ?

Géométrie

Soit encore

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

But principal. Pour $C \in E(K)$ distribué uniformément, donner une borne inférieur sur la probabilité que la fibre de C contient un point k-rationnel isolé !

Remarquons : $\mathrm{Res}_{K|k}(E)(k)$ et $(V')^{\delta} \times V^{m-\delta}$ sont de la dimension n.

Question. A-t-on $a_m : (V')^{\delta} \times V^{m-\delta} \longrightarrow \mathrm{Res}_{K|k}(E)$ surjective sur toutes les composantes irréductibles de $(V')^{\delta} \times V^{m-\delta}$?

Difficile !

Géométrie

Soit encore

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

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

Conditions équivalentes :

- $(P_1, \ldots, P_m)$ est isolé et réduit dans la fibre de C.
- a_m est non-ramifié à $(P_1, \ldots, P_m)$.
- $(a_m)_* : T_{(P_1,\ldots,P_m)}((V')^{\delta} \times V^{m-\delta}) \longrightarrow T_C(\mathrm{Res}_{K|k}(E))$ est injective.

De plus, « être non-ramifié » est une propriété ouverte ...

Algorithme final

- Garantir que $0 \in \mathbb{A}^1(K)$ est non-ramifié et décomposé par rapport à $x : E_a \longrightarrow \mathbb{A}^1_K$.
- Choisir une décomposition

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

Soient

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

et

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

- Chercher des relations de la forme

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

Analyse d'algorithme

Comme avant soit V_i défini par le diagramme cartésien

$$\begin{array}{ccc} V_i & \hookrightarrow & \mathrm{Res}_{K|k}(E_a) \\ \downarrow & & \downarrow \mathrm{Res}(x) \\ \mathbb{A}_k[U_i] & \hookrightarrow & \mathbb{A}_k[K] = \mathrm{Res}_{K|k}(\mathbb{A}^1_K)\ . \end{array}$$

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

Analyse d'algorithme

Soit $P_0 \in E(K)$ un antécédent de $0 \in \mathbb{A}^1_K(K)$.

Maintenant $\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ est non-ramifié en $P_0 \in \mathrm{Res}_{K|k}(E)(k)$.

Analyse d'algorithme

Soit $P_0 \in E(K)$ un antécédent de $0 \in \mathbb{A}^1_K(K)$.

Maintenant $\mathrm{Res}(x) : \mathrm{Res}_{K|k}(E_a) \longrightarrow \mathrm{Res}_{K|k}(\mathbb{A}^1_K)$ est non-ramifié en $P_0 \in \mathrm{Res}_{K|k}(E)(k)$.

Nous voulons étudier les fibres du morphisme

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

Proposition Ce morphisme est non-ramifié en $\overline{(P_0, \ldots, P_0)} \in (V_1 \times \cdots \times V_m)(k)$.

$\Longrightarrow$ Si les V_i sont irréductibles, le morphisme et génériquement non-ramifié est alors génériquement fini.

Analyse d'algorithme

Preuve de la proposition

Nous avons

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

Ce morphisme est non-ramifié à $(P_0, \ldots, P_0)$ si et seulement si l'application

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

est injective.

Analyse d'algorithme

Nous avons

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

Analyse d'algorithme

Soit maintenant $(P_1, \ldots, P_m) \in V_1(k) \times \cdots \times V_m(k)$. Alors le morphisme

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

est non-ramifié à $(P_1, \ldots, P_m)$ si et seulement si

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

Cette condition peut être étudiée explicitement.

Analyse d'algorithme

Soit maintenant $(P_1, \ldots, P_m) \in V_1(k) \times \cdots \times V_m(k)$. Alors le morphisme

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

est non-ramifié à $(P_1, \ldots, P_m)$ si et seulement si

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

Cette condition peut être étudiée explicitement.

- Si $\mathrm{char}(k)$ est impair, nous avons le différentiel holomorphe $\frac{dx}{y}$ et le champ tangentiel holomorphe yt_x.
- Si $\mathrm{char}(k)$ est pair et E non-supersingulière, nous avons $\frac{dx}{x}$ et xt_x.
- Si $\mathrm{char}(k)$ est pair et E supersingulière, nous avons dx et t_x.

Et quelques conditions de plus ...

- $\#V_i(k)$ devrait avoir au moins $\frac{1}{4} \cdot q^{\dim(V_i)}$ éléments.
- En caractéristique impaire, les espaces V_i doivent être irréductibles.

Le résultat principal

Théorème Le problème du logarithme discret dans les groupes rationnels des courbes elliptiques sur les corps $\mathbb{F}_{q^n}$ peut être résolu en temps

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

avec un algorithme randomisé.

Sur la condition que q est pair, il peut être résolu en temps

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

avec un algorithme randomisé.

Mes travaux

- Mémoire d'habilitation : 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. Accepté par Algebra and Number Theory