Méthode arithmético-géométrique pour le comptage de points d'une courbe elliptique définie sur $\mathbf{F}_{2^d}$

V. Vitse

UVSQ - MA^2

Plan

Motivations

Approche standard du comptage de points

Algorithmique sur $\mathbf{Z}_q$

Approche AGM en caractéristique 2

Motivations

- Courbes elliptiques naturellement munies d'une loi de groupe où le problème du log discret est difficile.
- ECC introduit par Miller (1985) puis Koblitz (1987) : systèmes cryptographiques sur courbes elliptiques définies sur des corps finis (protocole d'échange de clés de Diffie-Hellman, signatures El Gamal plus courtes...) $\Rightarrow$ trouver des sous-groupes cycliques dont l'ordre est divisible par un grand nombre premier, calcul de cardinalité du groupe.
- Algorithmes de comptage de points :
  - Shoof (1985) : 1er algo de complexité polynomiale $O(n^{4+\epsilon})$ puis améliorations apportées par Elkies et Atkin (SEA), Couveignes...
  - En 2000, nouvelle famille d'algorithmes (Satoh, Vercauteren...) : méthode p-adiques, temps en $O(n^{3+\epsilon})$ et consommation mémoire en $O(n^2)$
  - Etude de l'algorithme AGM dû à Mestre.

Plan

Motivations

Approche standard du comptage de points

Algorithmique sur $\mathbf{Z}_q$

Approche AGM en caractéristique 2

Points rationnels

E courbe elliptique ordinaire définie sur $\mathbf{F}_q$, $q = p^d$, p premier, $d \in \mathbf{N}^*$
Soit $\Phi_q \in End(E)$ le q-ième Frobenius,

Propriété

Soit $P \in E$ un point de la courbe, alors P est rationnel sur $\mathbf{F}_q$ si et seulement si $\Phi_q(P) = P$.
En particulier,

$$\#E(\mathbf{F}_q) = \#\ker([1] - \Phi_q) = \deg([1] - \Phi_q)$$

$\Rightarrow$ comptage de points ramenés au calcul de $\deg([1] - \Phi_q)$

Action de Φ_q sur le module de Tate

Définition

- *Anneau des l-adiques :* $\mathbf{Z}_l = \varprojlim \mathbf{Z}/l^n\mathbf{Z}$
- *Module de Tate :* $T_l(E) = \varprojlim E[l^n]$ *où* $E[l^n]$ *groupe de* l^n*-torsion*

Proposition

Si $l \neq p$ *premier, alors*

$$T_l(E) \simeq \mathbf{Z}_l \times \mathbf{Z}_l$$

et il existe un morphisme naturel

$$\begin{array}{ccc} End(E) & \rightarrow & End(T_l(E)) \simeq \mathcal{M}_2(\mathbf{Z}_l) \\ \varphi & \mapsto & \varphi_l \end{array}$$

$$\Rightarrow \chi(\Phi_{q,l})(X) = X^2 - \mathrm{Tr}(\Phi_{q,l})X + \det(\Phi_{q,l}) \in \mathbf{Z}_l[X]$$

Conjecture de Weil

Théorème

- $\det(\Phi_{q,l}) = \deg(\Phi_q) = q$ *et* $\mathrm{Tr}(\Phi_{q,l}) = 1 + q - \deg([1] - \Phi_q)$.
- $\forall n \in \mathbf{Z},\ \deg([n] - \Phi_q) = \chi(\Phi_q)(n) = n^2 - n\,\mathrm{Tr}(\Phi_q) + \det(\Phi_q)$

dont on déduit le théorème de Hasse :

Théorème (Hasse)

$$|\mathrm{Tr}(\Phi_q)| \leq 2\sqrt{\det \Phi_q}$$

En particulier, on peut approximer le nombre de points rationnels de la courbe E :

$$1 + q - 2\sqrt{q} \leq \#E(\mathbf{F}_q) \leq 1 + q + 2\sqrt{q}$$

$\Rightarrow$ il suffit de connaitre $\mathrm{Tr}(\Phi_q)$ modulo $2^2 p^{\lceil \frac{d}{2} \rceil}$

Relèvement canonique, q-adiques

E courbe elliptique ordinaire définie sur $\mathbf{F}_q$, $q = p^d$.

- Idée de Satoh : se placer sur une courbe définie sur un corps local de caractérique nulle qui "relève bien" la courbe elliptique E
  $\Rightarrow$ introduire q-adiques $(\mathbf{Z}_q, \mathbf{Q}_q)$ et $\mathcal{E}$ le relèvement canonique défini sur $\mathbf{Q}_q$
- Calcul de la trace :

Théorème (Satoh)

Soit $\mathcal{E}$ une courbe elliptique définie sur un corps de caractéristique 0, et soit ω une forme différentielle holomorphe sur $\mathcal{E}$. Pour tout $f \in End(\mathcal{E})$, on définit $\lambda_f = \frac{f^*(\omega)}{\omega}$. Alors λ_f est une racine du polynôme caractéristique de f et en particulier,

$$\mathrm{Tr}(f) = \lambda_f + \frac{\deg(f)}{\lambda_f}$$

Corps des p-adiques

Anneau des p-adiques

Définition

- *Entier p-adique :* $x = (x_1, x_2, \ldots)$ *où* $x_n \in \mathbf{Z}/p^n\mathbf{Z}$, $x_{n+1} = x_n \bmod p^n$.
- *Anneau des p-adiques :* $\mathbf{Z}_p$ *où somme/produit sont définis coordonnées par coordonnées de manière naturelle.*

Propriété

- $\mathbf{Z}_p$ *est un anneau de valuation discrète de corps résiduel* $\mathbf{F}_p$ *et de caractéristique* 0.
- $x \in \mathbf{Z}_p^*$, $x = up^n$ *où* $u \in \mathbf{Z}_p^*$ *et* $n \in \mathbf{N}$
  $\nu_p(x) = n$ *est la valuation p-adique*

Corps des p-adiques

Norme p-adiques

Définition

- *Corps des p-adiques :* $\mathbf{Q}_p = Frac(\mathbf{Z}_p)$
- *Valuation p-adique se prolonge sur* $\mathbf{Q}_p$ *:* $\nu_p(\frac{1}{x}) = -\nu_p(x)$
- *Norme p-adique :*

$$|.|_p : \mathbf{Q}_p \to \mathbf{R}_+,\ x \to |x|_p = p^{-\nu_p(x)}$$

Proposition

- $\mathbf{Z}_p = \{x \in \mathbf{Q}_p : |x|_p \leq 1\}$ *anneau de valuation de* $\mathbf{Q}_p$
- $\mathbf{Q}_p$ *est le complété de* $\mathbf{Q}$ *pour la norme* $|.|_p$

Corps des q-adiques

Définition

Soit $K = \mathbf{Q}_p[X]/(P)$ *(*$P \in \mathbf{Z}_p[X]$ *irréductible de degré* d*, de contenu* 1*) une extension de* $\mathbf{Q}_p$ *de degré* d*.*
K *est dite* **non ramifiée**, *si* $\deg(P) = \deg(P_N)$, $\forall N \in \mathbf{N}$ *où* $P_N \in (\mathbf{Z}/p^N\mathbf{Z})[X]$ *tels que* $P_N = P \bmod p^N$*.*

Proposition

Il existe une unique (à isomorphisme près) extension non ramifiée de degré d *de* $\mathbf{Q}_p$*, notée* $\mathbf{Q}_q$ *où* $q = p^d$*. Cette extension est galoisienne, de groupe de Galois cyclique.*
ν_p *et* $|.|_p$ *se prolongent de façon unique à* $\mathbf{Q}_q$*.*

Entiers q-adiques, lien $\mathbf{F}_q/\mathbf{Q}_q$

Définition

$\mathbf{Z}_q = \{x \in \mathbf{Q}_q : |x|_p \leq 1\}$ *est l'anneau de valuation de* $\mathbf{Q}_q$.

Propriété

(i) $\mathbf{Z}_q$ *est un anneau local, d'idéal maximal* $p\mathbf{Z}_q$, *son corps résiduel est* $\mathbf{F}_q$.

(ii) $\mathbf{Z}_q$ *est une extension de* $\mathbf{Z}_p$: $\mathbf{Z}_q \simeq \mathbf{Z}_p[X]/(P)$

(iii) $\mathbf{Z}_q = \varprojlim \mathbf{Z}_q/p^N\mathbf{Z}_q = \varprojlim(\mathbf{Z}/p^N\mathbf{Z})[X]/(P_N)$

Théorème

$Gal(\mathbf{Q}_q/\mathbf{Q}_p) \simeq Gal(\mathbf{F}_q/\mathbf{F}_p)$ *(donné par la réduction modulo p)*
$Gal(\mathbf{F}_q/\mathbf{F}_p) =< \sigma >$ *où* $\sigma : x \mapsto x^p$ *(petit Frobenius)*
$\Rightarrow Gal(\mathbf{Q}_q/\mathbf{Q}_p) =< \Sigma >$ *(*Σ *substitution de Frobenius).*

Relevé canonique et substitution de Frobenius

Définition

Un relevé canonique de la courbe elliptique ordinaire E définie sur $\mathbf{F}_q$ est une courbe elliptique $\mathcal{E}$ définie sur $\mathbf{Q}_q$ satisfaisant :

- *la réduction de $\mathcal{E}$ modulo p est E,*
- *$End(\mathcal{E}) \simeq End(E)$ isomorphisme induit par la réduction modulo p.*

En particulier, le q-ième Frobenius $\Phi_q : E \to E$ se relève en un endomorphisme $\mathcal{F}_q : \mathcal{E} \to \mathcal{E}$, et on a $\operatorname{Tr} \mathcal{F}_q = \operatorname{Tr} \Phi_q$.

Théorème (Deuring)

Le relevé canonique $\mathcal{E}$ de E existe et est unique à isomorphisme près.

Relèvement p-ième Frobenius et calcul de la trace

E courbe elliptique définie sur $\mathbf{F}_q \simeq \mathbf{F}_{p^d}$

- Le p-ième Frobenius $\Phi_p : E \to E^\sigma$ induit un cycle d'isogénie sur E

$$E \xrightarrow{\Phi_{p,0}} E^\sigma \xrightarrow{\Phi_{p,1}} E^{\sigma^2} \xrightarrow{\Phi_{p,2}} \ldots \xrightarrow{\Phi_{p,d-1}} E^{\sigma^d} = E$$

Théorème

$\Phi_p : E \to E^\sigma$ se relève en une isogénie $\mathcal{F}_p : \mathcal{E} \to \mathcal{E}^\Sigma$, où Σ est la substitution de Frobenius.

En appliquant successivement ce résultat, on peut relever le cycle d'isogénies

$$E \xrightarrow{\Phi_{p,0}} E^\sigma \xrightarrow{\Phi_{p,1}} E^{\sigma^2} \xrightarrow{\Phi_{p,2}} \ldots \xrightarrow{\Phi_{p,d-1}} E^{\sigma^d} = E$$

en un cycle d'isogénies

$$\mathcal{E} \xrightarrow{\mathcal{F}_{p,0}} \mathcal{E}^\Sigma \xrightarrow{\mathcal{F}_{p,1}} \mathcal{E}^{\Sigma^2} \xrightarrow{\mathcal{F}_{p,2}} \ldots \xrightarrow{\mathcal{F}_{p,d-1}} \mathcal{E}^{\Sigma^d} = \mathcal{E}$$

et $\mathrm{Tr}(\mathcal{F}_q) = \mathrm{Tr}(\mathcal{F}_{p,d-1} \circ \ldots \circ \mathcal{F}_{p,0})$.

Plan

Motivations

Approche standard du comptage de points

Algorithmique sur $\mathbf{Z}_q$

Approche AGM en caractéristique 2

Calculs à la précision N

On suppose désormais $p = 2$ et $q = 2^d$.

- Notion de précision : $a \in \mathbf{Z}_2$ représenté par $a_N = a \bmod 2^N$ (un élément de $\mathbf{Z}_2$ à la précision N nécessite donc $O(N)$ bits mémoire)
- Choix d'implémentation : travail dans $\mathbf{Z}_q$ à la précision $N \leftrightarrow$ travail dans $(\mathbf{Z}/2^N\mathbf{Z})[X]/(P_N)$ où $P_N = P \bmod 2^N$ (un élément de $\mathbf{Z}_q$ à la précision N nécessite donc $O(dN)$ bits mémoire).
- Complexité des opérations usuelles :
  - Addition : $O(dN)$
  - Multiplication naïve : $O(d^2N^2)$
- Accéleration des calculs modulo P_N : on part de $P_1 \in \mathbf{F}_2[X]$ polynôme irréductible creux (trinomial ou pentanomial), qu'on relève en $P \in \mathbf{Z}_2[X]$

Bibliothèques utilisées

- Norme de sécurité : extensions de degré $d \simeq 160$, précision de l'ordre de 80 bits pour le calcul de la trace.
  $\Rightarrow$ utilisation de GMP pour l'arithmétique sur les grands entiers
- Calcul modulaire dans $\mathbf{Z}_2[X]$ rendu possible avec NTL :
  - pas de classe préexistante pour les q-adiques (pour le changement de précision), mais multiplications très efficaces dans $(\mathbf{Z}/2^N\mathbf{Z})[X]/(P_N)$ (Karatsuba, Schönhage-Strassen) en $O((dN)^\mu)$
  - on utilise la classe ZZ_X (polynômes à coeff grands entiers)
  - on travaille avec des polynômes de degré $d-1$ à coefficients dans $[\![0; 2^N - 1]\!]$.
  - addition/multiplication modulo P_N de la classe ZZ_X, puis troncature des bits dans la classe ZZ pour ramener les coeff dans l'intervalle $[\![0; 2^N - 1]\!]$.
- Autres opérations usuelles (inverse, racine carrée) basées sur un analogue dans $\mathbf{Z}_q$ des itérations de Newton.

Calcul d'inverse dans $\mathbf{Z}_q$

ENTRÉE : $a \in \mathbf{Z}_q$ inversible, $N \in \mathbf{N}$ la précision
SORTIE : z l'inverse de a à la précision N

1. **si** $N = 1$ **alors**
2. $\quad z \leftarrow \frac{1}{a} \bmod 2$
3. **sinon**
4. $\quad z \leftarrow \text{Inverse}\left(a, \left\lfloor \frac{N+1}{2} \right\rfloor\right)$
5. $\quad z \leftarrow z + z(1 - az) \bmod 2^N$
6. **fin si**
7. **retourner** z

Remarques :

- ligne 1 : dans AGM on s'épargne le calcul d'inverse à la précision 1 dans $\mathbf{F}_q$ (on prendra 1 comme inverse approché)
- algorithme donnant une preuve constructive du fait qu'un élément est inversible dans $\mathbf{Z}_q$ si et seulement si il est inversible (non nul) mod 2.
- **Complexité** : $O((dN)^\mu)$

Calcul de racine carrée dans $\mathbf{Z}_q$

ENTRÉE : $a \in \mathbf{Z}_q$ carré inversible, z_0 approximation initiale de $\frac{1}{\sqrt{a}}$ à l'ordre 2, $N \in \mathbf{N}$ la précision

SORTIE : z l'inverse de la racine carrée de a à la précision N

1. **si** $N \leq 2$ **alors**
2. $\quad z \leftarrow z_0$
3. **sinon**
4. $\quad N' \leftarrow \left\lfloor \frac{N+2}{2} \right\rfloor$
5. $\quad z \leftarrow \text{RacineCarreeInverse}(a, z_0, N')$
6. $\quad x \leftarrow 1 - az^2 \bmod 2^{N+1}$
7. $\quad z \leftarrow z + \frac{zx}{2} \bmod 2^N$
8. **fin si**
9. **retourner** z

Remarques :

- approximation de $\frac{1}{\sqrt{a}}$ à l'ordre 2 non problématique dans AGM
- un élément inversible est un carré dans $\mathbf{Z}_q$ si et seulement si il admet une racine carrée approchée mod 4 (preuve constructive)
- **Complexité** : $O((dN)^\mu)$

Plan

Motivations

Approche standard du comptage de points

Algorithmique sur $\mathbf{Z}_q$

Approche AGM en caractéristique 2

Restriction du problème

- En caractéristique 2, une courbe elliptique ordinaire (j-invariant non nul) a pour équation :

$$E \ : \ y^2 + xy = x^3 + a_2x^2 + a_6 \quad \text{où } a_6 \in \mathbf{F}_q^*$$

et son j-invariant ne dépend que de a_6
$\Rightarrow$ on se restreint aux courbes d'équations

$$E' \ : \ \tilde{y}^2 + \tilde{x}\tilde{y} = \tilde{x}^3 + a_6 \quad \text{où } a_6 \in \mathbf{F}_q^*$$

- Un isomorphisme entre E et E' est de la forme

$$\begin{cases} x = \tilde{x} \\ y = \tilde{y} + s\tilde{x} \end{cases} \quad \text{où } s \text{ vérifie } s^2 + s - a_2 = 0 \text{ dans } \mathbf{F}_q$$

Deux cas possibles :
  - E et E' ont le même nombre de points dans $\mathbf{F}_q$
  - E et E' ont le même nombre de points dans $\mathbf{F}_{q^2}$ (E' est appelée "tordue" de E) : on déduit la cardinalité de E connaissant celle de E'

Contexte AGM

$$E: \quad y^2 + xy = x^3 + c \qquad\qquad c \in \mathbf{F}_q^*$$

Théorème (Relevé canonique de E)

Il existe un unique relevé $\mathcal{E}$, appelé canonique, de E dans $\mathbf{Q}_q$ vérifiant :

(i) *$\mathcal{E}$ admet une bonne réduction modulo 2*

(ii) *$End(\mathcal{E}) \simeq End(E)$*

En particulier,

- $\Phi_2 : E \to E^\sigma \leftrightsquigarrow \mathcal{F}_2 : \mathcal{E} \to \mathcal{E}^\Sigma$
- $\Phi_{2,k} : E^{\sigma^k} \to E^{\sigma^{k+1}} \leftrightsquigarrow \mathcal{F}_{2,k} : \mathcal{E}^{\Sigma^k} \to \mathcal{E}^{\Sigma^{k+1}}$.
- $\Phi_q \in End(E) \leftrightsquigarrow \mathcal{F}_q \in End(\mathcal{E})$ *tel que*

$$\begin{cases} \mathcal{F}_{2,d-1} \circ \ldots \circ \mathcal{F}_{2,0} = \mathcal{F}_q \\ \mathrm{Tr}(\mathcal{F}_q) = \mathrm{Tr}(\Phi_q) \end{cases}$$

Action de $\mathcal{F}_q^*$ sur la différentielle holomorphe de $\mathcal{E}$

Théorème (Satoh)

Soit $c \in \mathbf{Q}_q$ tel que $\mathcal{F}_q^* \omega = c\,\omega$ où ω est une différentielle holomorphe sur $\mathcal{E}$. Alors

$$\mathrm{Tr}(\mathcal{F}_q) = c + \frac{q}{c}$$

- On suppose que $\mathcal{E}$ est isomorphe à la courbe $\mathcal{E}_{a,b}$ d'équation :

$$\mathcal{E}_{a,b} : \quad y^2 = x(x - a^2)(x - b^2) \tag{1}$$

  $\omega = \frac{dx}{y}$ différentielle holomorphe définie sur $\mathcal{E}_{a,b}$.
- Calcul $\mathcal{F}_q^*(\omega) = \mathcal{F}_{2,0}^* \circ \ldots \circ \mathcal{F}_{2,d-1}^*(\omega)$?
  On introduit la suite arithmético-géométrique $(a_k, b_k)_{k \geq 0}$ et un isomorphisme entre $\mathcal{E}^{\Sigma^k}$ et $\mathcal{E}_{a_k,b_k}$: $\quad y^2 = x(x - a_k^2)(x - b_k^2)$

Suite arithmético-géométrique

Soient $\alpha, \beta \in \mathbf{Z}_q$ tels que

$$\begin{cases} \alpha, \beta \in 1 + 4\mathbf{Z}_q \\ \dfrac{\alpha}{\beta} \in 1 + 8\mathbf{Z}_q \end{cases} \tag{2}$$

On définit récursivement une suite arithmético-géométrique (α_k, β_k) par

$$\begin{cases} (\alpha_0, \beta_0) = (\alpha, \beta) \\ (\alpha_{k+1}, \beta_{k+1}) = \left(\dfrac{\alpha_k + \beta_k}{2}, \sqrt{\alpha_k \beta_k} \right) \end{cases} \tag{3}$$

Lemme

- $c \in 1 + 8\mathbf{Z}_q \Rightarrow \exists ! e \in 1 + 4\mathbf{Z}_q,\ e^2 = c$
- *Si* (α_k, β_k) *vérifie* (2), *alors* $(\alpha_{k+1}, \beta_{k+1})$ *vérifie* (2).

Suite arithmético-géométrique

L'itération AGM donne des 2-isogénies entre les courbes :

Théorème

Soient $\alpha, \beta \in 1 + 4\mathbf{Z}_q$ *et* $(\alpha', \beta') = AGM(\alpha, \beta)$.
Alors $\mathcal{E}_{\alpha,\beta} : y^2 = x(x - \alpha^2)(x - \beta^2)$ *et* $\mathcal{E}_{\alpha',\beta'} : y^2 = x(x - \alpha'^2)(x - \beta'^2)$ *sont 2-isogènes :*

$$\begin{array}{rccl} \psi : & \mathcal{E}_{\alpha,\beta} & \to & \mathcal{E}_{\alpha',\beta'} \\ & (x, y) & \mapsto & \left(\dfrac{(x + \alpha\beta)^2}{4x}, y\dfrac{(x - \alpha\beta)(x + \alpha\beta)}{8x^2} \right) \end{array}$$

$$\psi^* \left(\frac{dx'}{y'} \right) = 2\frac{dx}{y}$$

Le noyau de ψ *est composé de deux points :*

$$\ker(\psi) = \{(0, 0); O_{\mathcal{E}_{\alpha,\beta}}\}$$

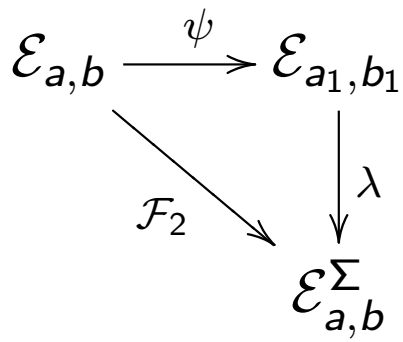
Lien AGM - relevé canonique

Proposition

Soit $\mathcal{F}_2 : \mathcal{E}_{a,b} \to \mathcal{E}^{\Sigma}_{a,b} = \mathcal{E}_{\Sigma(a),\Sigma(b)}$ *le 2-ième morphisme de Frobenius,* $\psi : \mathcal{E}_{a,b} \to \mathcal{E}_{a_1,b_1}$ *où* $(a_1, b_1) = AGM(a, b)$.

$$\ker(\mathcal{F}_2) = \ker(\psi)$$

En particulier, il existe un unique isomorphisme $\lambda : \mathcal{E}_{a_1,b_1} \to \mathcal{E}_{\Sigma(a),\Sigma(b)}$ *tel que* $\mathcal{F}_2 = \lambda \circ \psi$ *:*



Calcul de la trace

Théorème

Soient (a_k, b_k) la suite AGM initialisée par (a, b), alors on a le diagramme commutatif suivant :

$$\begin{array}{ccccccccc}
\mathcal{E}_{a,b} & \xrightarrow{\psi_0} & \mathcal{E}_{a_1,b_1} & \xrightarrow{\psi_1} & \mathcal{E}_{a_2,b_2} & \xrightarrow{\psi_2} & \cdots & \xrightarrow{\psi_{d-1}} & \mathcal{E}_{a_d,b_d} \\
\downarrow{\scriptstyle Id} & & \downarrow{\scriptstyle \lambda_1} & & \downarrow{\scriptstyle \lambda_2} & & \downarrow & & \downarrow{\scriptstyle \lambda_d} \\
\mathcal{E}_0 & \xrightarrow{\mathcal{F}_{2,0}} & \mathcal{E}_1 & \xrightarrow{\mathcal{F}_{2,1}} & \mathcal{E}_2 & \xrightarrow{\mathcal{F}_{2,2}} & \cdots & \xrightarrow{\mathcal{F}_{2,d-1}} & \mathcal{E}_d \simeq \mathcal{E}_0
\end{array}$$

où $\mathcal{E}_k = \mathcal{E}_{\Sigma^k(a),\Sigma^k(b)}$, $\mathcal{F}_{2,k} : \mathcal{E}_k \to \mathcal{E}_{k+1}$ (relevé de Φ_2) et $\lambda_k : \mathcal{E}_{a_k,b_k} \to \mathcal{E}_k$ sont des isomorphismes.

En particulier, $\lambda_d : \mathcal{E}_{a_d,b_d} \to \mathcal{E}_{a_0,b_0}$ isomorphisme tel que

- $\lambda_d(x', y') = \left(\left(\frac{a_0}{a_d} \right)^2 x', \pm \left(\frac{a_0}{a_d} \right)^3 y' \right)$
- $\mathcal{F}_q = \lambda_d \circ \psi_{d-1} \circ \ldots \circ \psi_1 \circ \psi_0$.

Calcul de la trace

Avec le théorème de Satoh, on en déduit le calcul de la trace avec une approximation suffisante (cf th. de Hasse) :

Théorème

$$\mathrm{Tr}(\mathcal{F}_q) = \mathrm{Tr}(\Phi_q) = \frac{a_0}{a_d} \bmod 2^{\lceil \frac{d}{2} \rceil + 2}$$

Remarques :

- il suffit de trouver a'_0 et a'_d approximant les valeurs a_0 et a_d à la précision $N - 1 = \lceil \frac{d}{2} \rceil + 2$
- en pratique (lemme technique) : prendre $a'_0, b'_0 \in \mathbf{Z}_q$ tels que $(a'_0, b'_0) = (a, b) \bmod 2^N$ où $N = \lceil \frac{d}{2} \rceil + 3$, alors $(a'_k, b'_k) = (a_k, b_k) \bmod 2^{N-1}$ et $\frac{a'_0}{a'_d} = \frac{a_0}{a_d} \bmod 2^{N-1}$ (approximation suffisante pour le calcul de la trace)

Précision nécessaire pour l'approximation du relevé canonique

Deux problèmes subsistent :

- comment trouver les approximations (a'_0, b'_0) à la précision N de (a, b) ?
- justifier le fait que $\mathcal{E}$ est bien isomorphe à une courbe $\mathcal{E}_{a,b}$ avec (a, b) vérifiant (2)

Proposition

Soit $n \in N^*$. Soient (α, β) et (α', β') vérifiant les hypothèses (2). Alors on a équivalence entre

(i) $j(\mathcal{E}_{\alpha',\beta'}) = j(\mathcal{E}_{\alpha,\beta}) \bmod 2^n$

(ii) $\frac{\alpha'}{\beta'} = \left(\frac{\alpha}{\beta}\right)^{\pm 1} \bmod 2^{n+3}$

Pour initialiser le calcul de la trace, il suffit donc de trouver (a'_0, b'_0) vérifiant les hypothèses (2), et tels que $j(\mathcal{E}_{a'_0,b'_0}) = j(\mathcal{E}) = j(\mathcal{E}_{a,b}) \bmod 2^{N-3}$.

Approximation du relevé canonique

Théorème (Approximation du relevé canonique)

Soient $\alpha_0 = 1$ *et* $\beta_0 = 1 + 8\bar{c}$ *où* $\bar{c} \in \mathbf{Z}_q$ *est un relevé de* $c \in \mathbf{F}_q^*$. *On note* (α_k, β_k) *la suite AGM initialisée à* (α_0, β_0) *et* $\mathcal{E}_{\alpha_k,\beta_k}$ *la courbe elliptique correspondante.*
Les courbes $\mathcal{E}_{\alpha_k,\beta_k}$ *approximent le relevé canonique* $\mathcal{E}$ *de la courbe* $E : y^2 + xy = x^3 + c$ *au sens suivant :*

$$j(\mathcal{E}_{\alpha_k,\beta_k}) = \Sigma^{k+1}(j(\mathcal{E})) \bmod 2^{k+1}$$

$\Rightarrow$ on peut prendre $(a'_0, b'_0) = (\alpha_{N-4}, \beta_{N-4})$.
Mieux : on peut encore limiter la précision du calcul de la première suite AGM (α_k, β_k), en prenant la suite (α'_k, β'_k) telle que :

$$\begin{cases} (\alpha'_0, \beta'_0) = (\alpha_0, \beta_0) \bmod 2^4 \\ (\alpha'_k, \beta'_k) = AGM(\alpha'_{k-1}, \beta'_{k-1}) \bmod 2^{k+4} \end{cases}$$

Remarques sur l'approximation

- Si on prend $(a'_0, b'_0) = (\alpha_{N-4}, \beta_{N-4})$, $\mathcal{E}_{a'_0,b'_0}$ approxime $\mathcal{E}^{\Sigma^{N-3}}$
  $\Rightarrow$ on va calculer $\#(E^{\sigma^{N-3}}(\mathbf{F}_q))$ (non gênant puisque $\Phi_2^{N-3} : E(\mathbf{F}_q) \to E^{\sigma^{N-3}}(\mathbf{F}_q)$ est bijectif)
- Bien que la suite AGM ne converge pas, elle fournit une approximation de $\mathcal{E}$: on peut en extraire une sous-suite convergente $(\alpha_{\varphi(k)}, \beta_{\varphi(k)})$ telle que

$$\lim_{k\to\infty} j(\mathcal{E}_{\alpha_{\varphi(k)},\beta_{\varphi(k)}}) = j(\mathcal{E}) = j(\mathcal{E}_{\alpha_\infty,\beta_\infty})$$

ce qui justifie l'hypothèse sur la forme du relevé canonique faite en (1).

Algorithme AGM

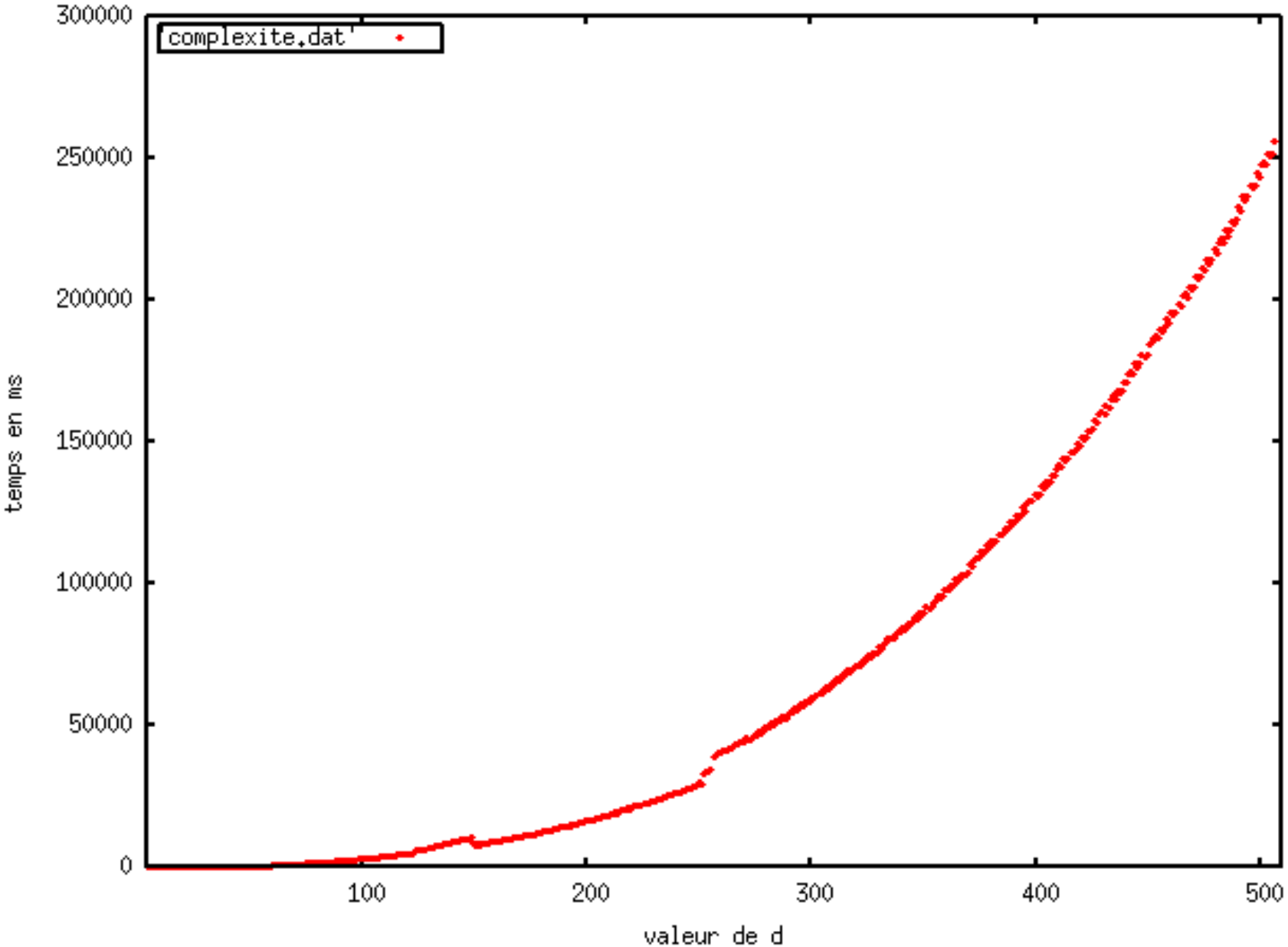
ENTRÉE : $E : y^2 + xy = x^3 + c$, $c \in \mathbf{F}_{2^d}^*$
SORTIE : nombre de points rationnels de $E(\mathbf{F}_{2^d})$
VARIABLES : N (précision), $a, b \in \mathbf{Z}_{2^d}$ (AGM), t (trace)

1. $N \leftarrow \left\lceil \frac{d}{2} \right\rceil + 3$
2. $a \leftarrow 1 \bmod 2^4$
3. $b \leftarrow 1 + 8c \bmod 2^4$
4. **pour** $i = 5$ à N **faire**
5. $\quad (a, b) \leftarrow \left(\frac{a+b}{2}, \sqrt{ab} \right) \bmod 2^i$
6. **fin pour**
7. $a_0 \leftarrow a$
8. **pour** $i = 0$ à $d - 1$ **faire**
9. $\quad (a, b) \leftarrow \left(\frac{a+b}{2}, \sqrt{ab} \right) \bmod 2^N$
10. **fin pour**
11. $t \leftarrow \frac{a_0}{a} \bmod 2^{N-1}$
12. **si** $t^2 > 2^{d+2}$ **alors**
13. $\quad t \leftarrow t - 2^{N-1}$
14. **fin si**
15. **retourner** $2^d + 1 - t$

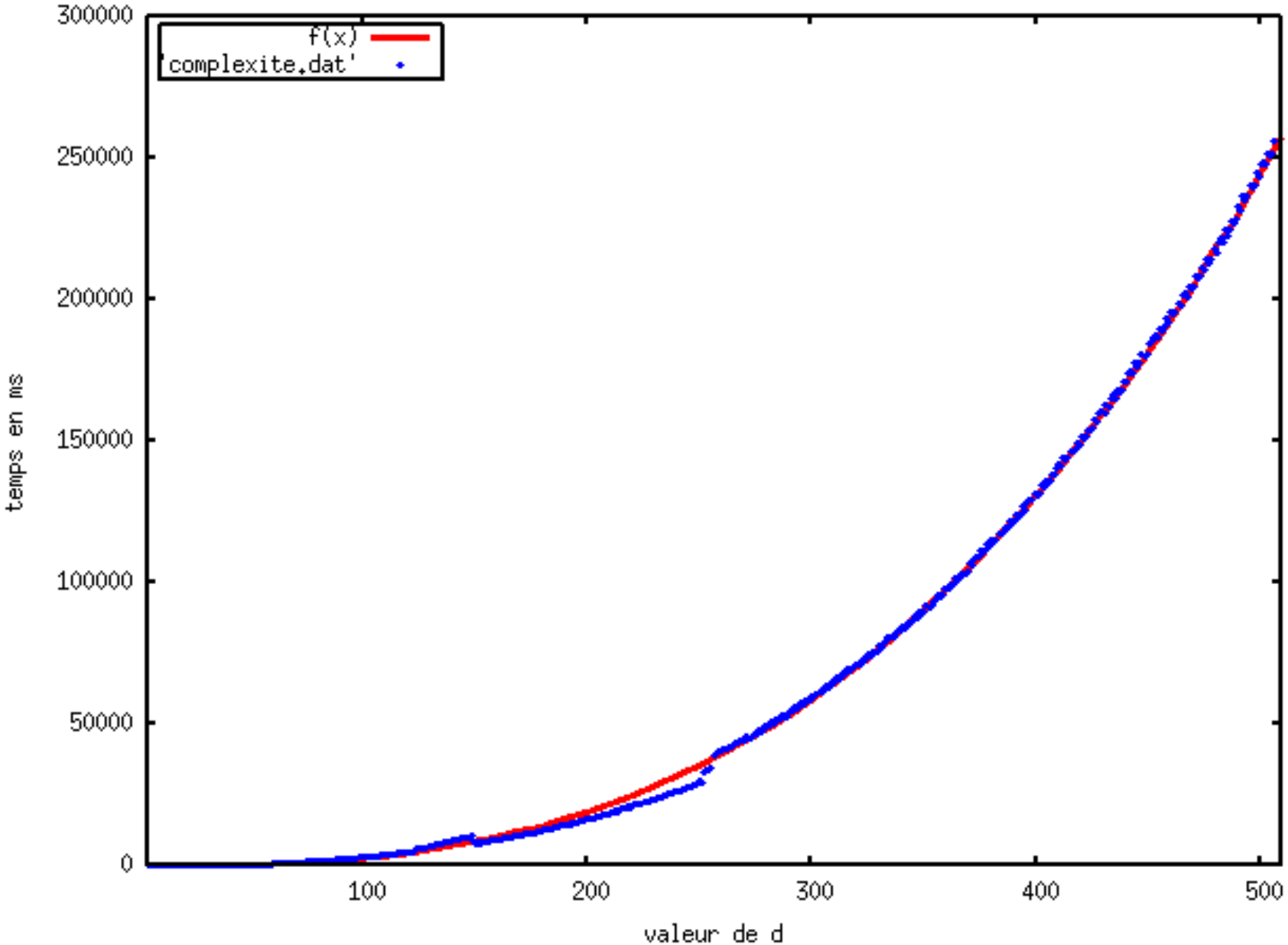
Vérification des résultats et complexité

- on vérifie que l'ordre d'un point P rationnel de la courbe dont l'abscisse a été choisie aléatoirement, est bien un diviseur du nombre de points rationnels trouvé
- Complexité en mémoire : on stocke $O(1)$ éléments de $\mathbf{Z}_q$ à la précision $N = O(d)$ (ayant donc d coefficients dans $\mathbf{Z}/2^N\mathbf{Z}$), soit une complexité en $O(d^2)$.
- Complexité en temps : on effectue de l'ordre de $2d$ calculs de racines carrés et produits avec un coût en $O((dN)^\mu) = O(d^{2\mu})$, soit une complexité totale en $O(d^{2\mu+1})$.

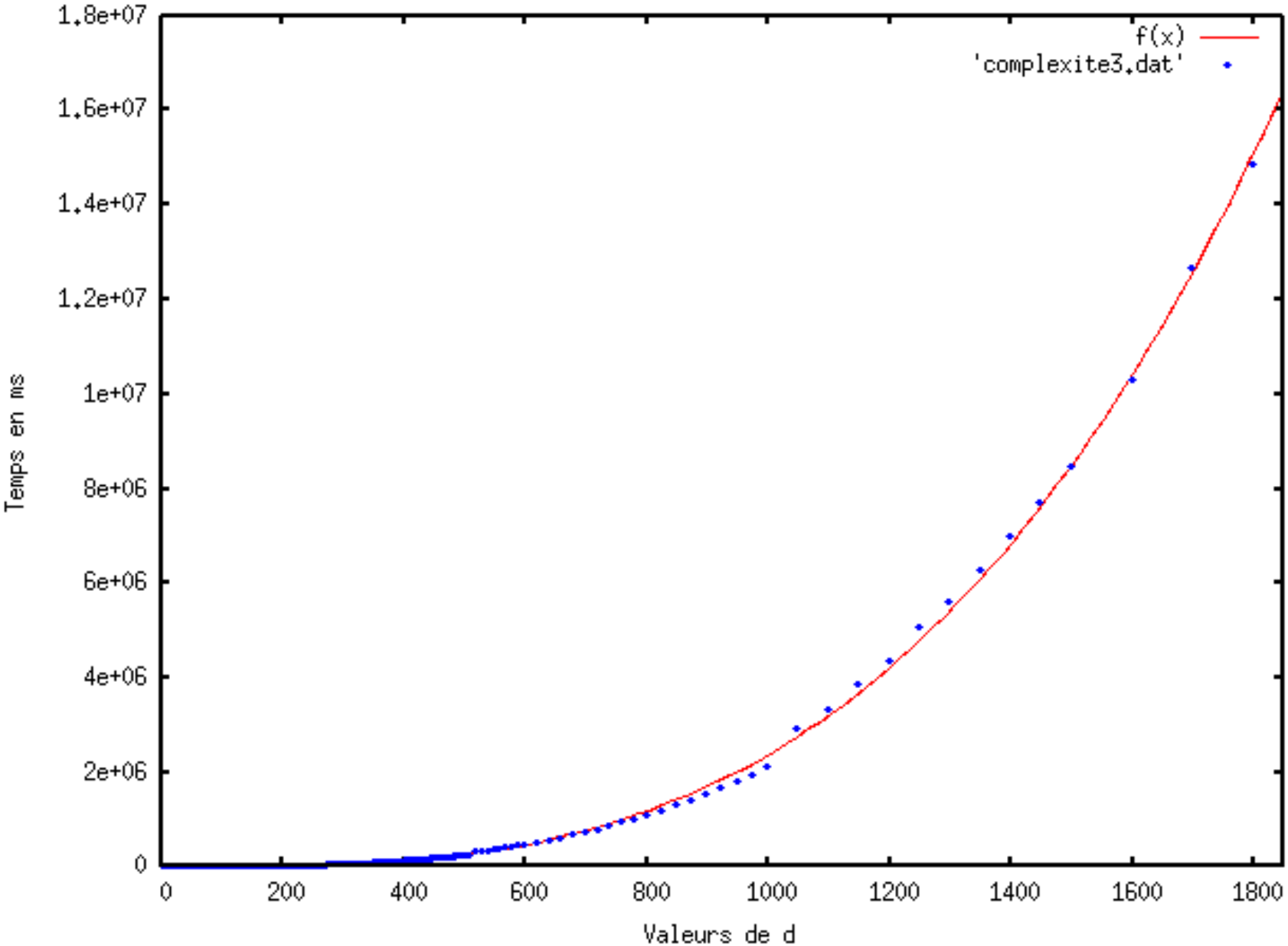
Résultats de l'implémentation



Résultats de l'implémentation



Résultats de l'implémentation



Interprétation des résultats

- Régression non linéaire sous Gnuplot : on retrouve bien la complexité en $d^{3.148}$
- Plusieurs décrochements de la courbe aux valeurs $d = 256, 512, 1024....$ Cette perte de performance s'explique certainement par un saut dans la façon de stocker les valeurs en mémoire.
- Un décrochement plus mystérieux en $d = 150$, probablement dû à un changement d'algorithme de multiplication dans NTL.