Factorisation avec des courbes de genre 2

Romain Cosset

Sous la direction d'Emmanuel Thomé
Équipe: CACAO, laboratoire: LORIA

L'algorithme $p-1$

Soit un entier N et $p \mid N$. Nous voullons trouver p.

Soit $a \wedge N = 1$,
Fermat: si $p-1 \mid k$ alors $a^k \equiv 1 \bmod p$.

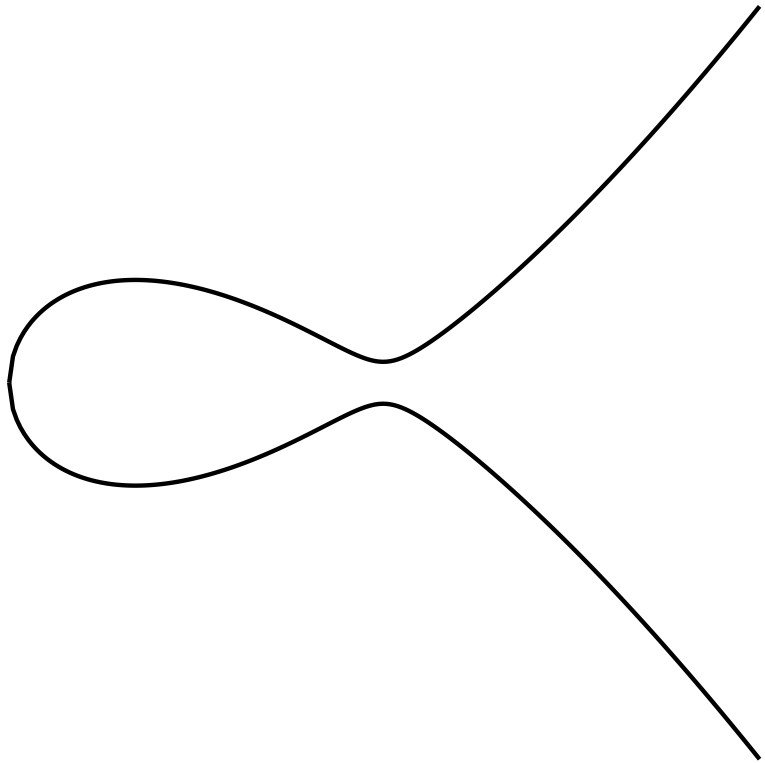
ALGORITHME: P-1 (entrée N et B_1)

1. Choisir au hasard a mod N premier avec N.
2. Calculer a^k mod N avec $k = ppcm(1, 2, \ldots, B_1)$.
3. Calculer $pgcd(a^k - 1, N)$.

Si $p-1$ est B_1-friable, l'algorithme renvoie p.

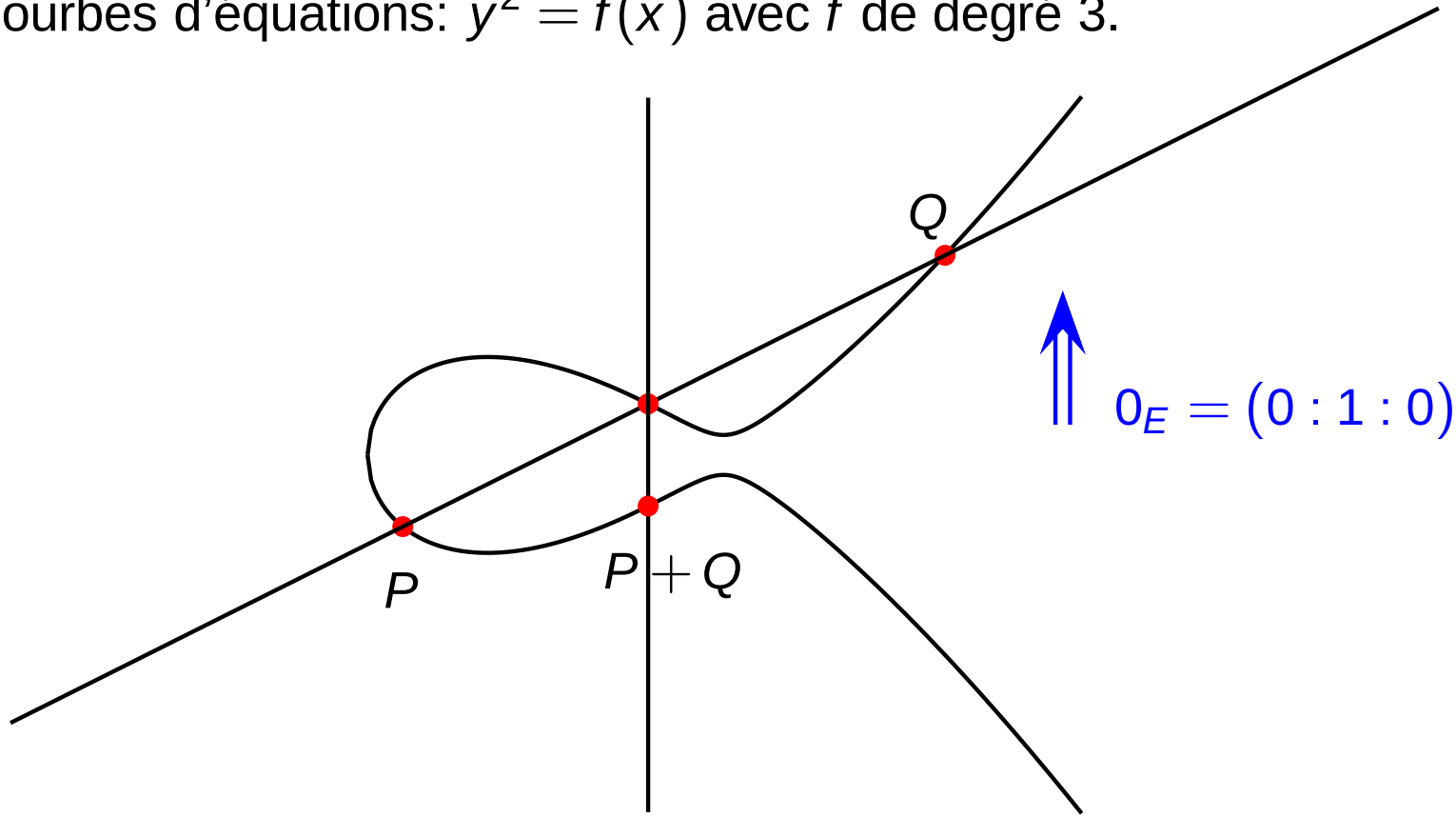
Courbes elliptiques

Courbes d'équations: $y^2 = f(x)$ avec f de degré 3.



Courbes elliptiques

Courbes d'équations: $y^2 = f(x)$ avec f de degré 3.



L'algorithme ECM

Soit un entier N et $p \mid N$. Nous voullons trouver p.

ALGORITHME: ECM (entrée N et B_1)

1. Choisir une courbe elliptique $\mathcal{E}$ sur $\mathbb{Z}/N\mathbb{Z}$ avec un point P dessus.
2. Calculer $k * P$ avec $k = ppcm(1, 2, \ldots, B_1)$
3. Espérer que $k * P = O_{\mathcal{E}}$ mod p.
4. Sinon revenir à 1.

Si $\#\mathcal{C}(\mathbb{F}_p)$ est B_1-friable, alors une division va rater et nous trouverons p.

L'algorithme ECM, détails

Améliorations classiques:

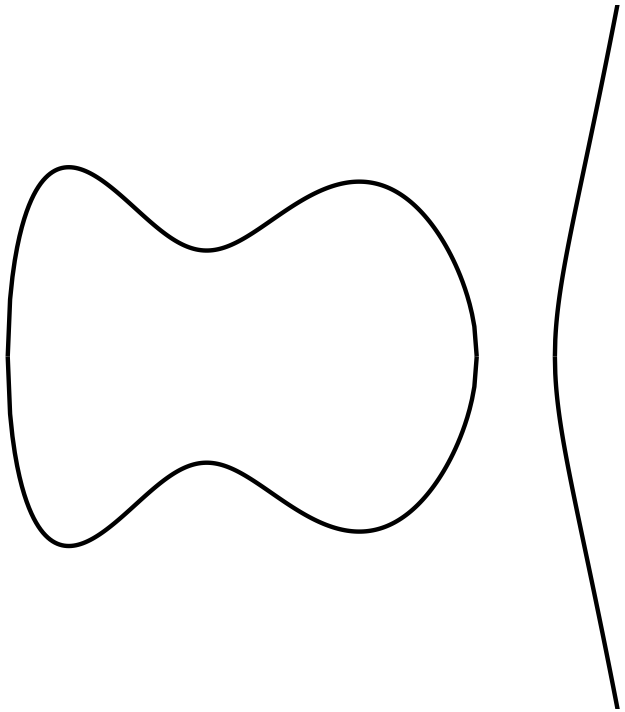
- Nous travaillons en coordonnées projectives $(x : y : z)$. À la fin nous calculons $pgcd(z, N)$.
- Nous utilisons seulement $(x :: z)$. Les formules de Montgomery permettent

$$\begin{aligned} \pm P &\longrightarrow \pm 2P \\ \pm P, \pm Q, \pm(P-Q) &\longrightarrow \pm(P+Q) \end{aligned}$$

- D'autres améliorations sont utilisées.

Courbes hyperelliptiques de genre 2

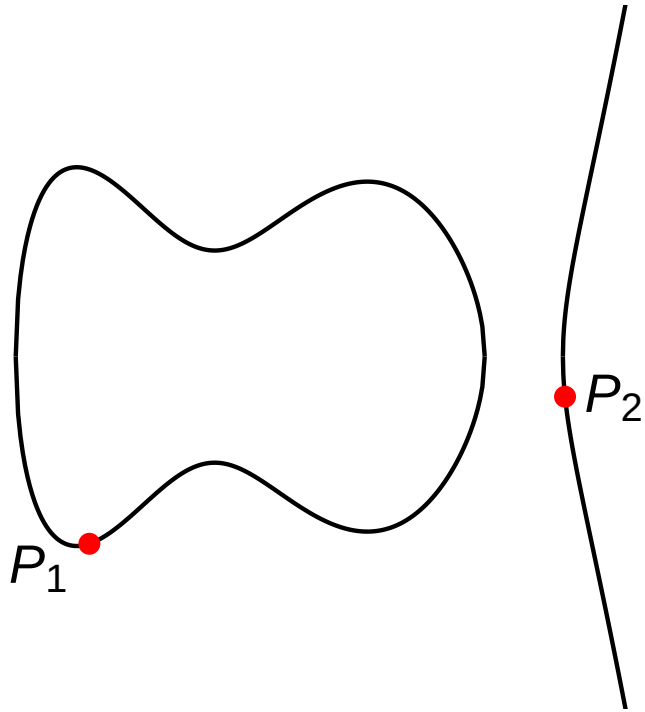
Courbes d'équations: $y^2 = f(x)$ avec f de degré 5.
On peut se ramener à $f(x) = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.



Courbes hyperelliptiques de genre 2

Courbes d'équations: $y^2 = f(x)$ avec f de degré 5.
On peut se ramener à $f(x) = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

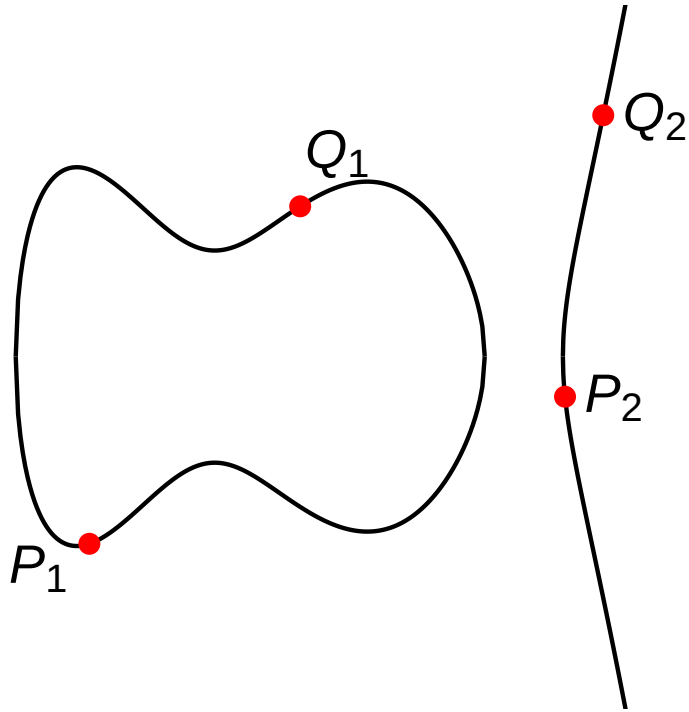
Les points sur la courbes ne forment plus un groupe. Il faut travailler dans la Jacobienne.



Courbes hyperelliptiques de genre 2

Courbes d'équations: $y^2 = f(x)$ avec f de degré 5.
On peut se ramener à $f(x) = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

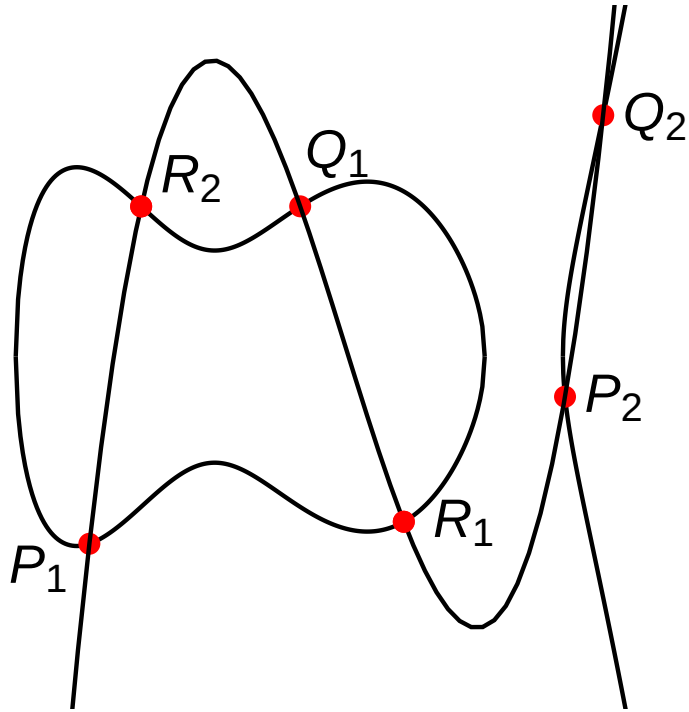
Les points sur la courbes ne forment plus un groupe. Il faut travailler dans la Jacobienne.



Courbes hyperelliptiques de genre 2

Courbes d'équations: $y^2 = f(x)$ avec f de degré 5.
On peut se ramener à $f(x) = x(x-1)(x-\lambda)(x-\mu)(x-\nu)$.

Les points sur la courbes ne forment plus un groupe. Il faut travailler dans la Jacobienne.



L'algorithme HECM

ALGORITHME: HECM (entrée N et B_1)

1. Choisir une courbe hyperelliptique avec un diviseur D dans sa Jacobienne.
2. Calculer $k * D$ avec $k = ppcm(1, 2, \ldots, B_1)$
3. Espérer que $k * D = O_{Jac}$ mod p.
4. Sinon revenir à 1.

Si $\#Jac(\mathbb{F}_p)$ est B_1-friable, alors nous trouverons $p \mid N$.

Pourquoi, en général, ECM est meilleur que HECM

Pour un facteur p possible de N,

- $\#\mathcal{E}(\mathbb{F}_p) \approx p$
- $\#Jac(\mathcal{C})(\mathbb{F}_p) \approx p^2$

La probabilité de succès de HECM sera plus faible que celle d'ECM.

Pourquoi, en général, ECM est meilleur que HECM

Pour un facteur p possible de N,

- $\#\mathcal{E}(\mathbb{F}_p) \approx p$
- $\#Jac(\mathcal{C})(\mathbb{F}_p) \approx p^2$

La probabilité de succès de HECM sera plus faible que celle d'ECM.

L'arithmétique sur une Jacobienne est plus lente que celle sur une courbe elliptique (définie sur le même corps).

Comment améliorer HECM

- **Probabilité de succès: courbes décomposables**
  Supposons l'existence d'une isogénie:

$$\psi : \mathit{Jac}(\mathcal{C}) \to \mathcal{E}_1 \times \mathcal{E}_2$$

  HECM avec ces courbes est équivalents à deux ECM simultanés.

Comment améliorer HECM

- **Probabilité de succès: courbes décomposables**
  Supposons l'existence d'une isogénie:

$$\psi : Jac(\mathcal{C}) \rightarrow \mathcal{E}_1 \times \mathcal{E}_2$$

  HECM avec ces courbes est équivalents à deux ECM simultanés.
- **Arithmétique: surfaces de Kummer**
  Elles fournissent le même type de formules que celles de Montgomery.

SURFACES DE KUMMER

Aperçu

Soit $\mathcal{K}_{\alpha,\beta,\gamma,\delta}$ la surface de $\mathbb{P}^3$ donnée par l'équation

$$\left(\left(X^2+Y^2+Z^2+T^2\right)-F\left(XT+YZ\right)-G\left(XZ+YT\right)\right.$$
$$\left.-H\left(XY+ZT\right)\right)^2-4E'^2\alpha\beta\gamma\delta XYZT=0$$

où E', F, G et H sont des constantes dépendant de α, β, γ, δ.

Aperçu

Soit $\mathcal{K}_{\alpha,\beta,\gamma,\delta}$ la surface de $\mathbb{P}^3$ donnée par l'équation

$$\left(\left(X^2+Y^2+Z^2+T^2\right)-F\left(XT+YZ\right)-G\left(XZ+YT\right)\right.$$
$$\left.-H\left(XY+ZT\right)\right)^2-4E'^2\alpha\beta\gamma\delta XYZT=0$$

où E', F, G et H sont des constantes dépendant de α, β, γ, δ.

Posons

$$\lambda := \frac{\alpha\gamma}{\beta\delta} \qquad \mu := \frac{\gamma\varepsilon}{\delta\phi} \qquad \nu := \frac{\alpha\varepsilon}{\beta\phi}$$

$$\mathcal{C}:\ y^2 = x\left(x-1\right)\left(x-\lambda\right)\left(x-\mu\right)\left(x-\nu\right)$$

alors

$$Jac(\mathcal{C})/\{\pm 1\} \simeq \mathcal{K}_{\alpha,\beta,\gamma,\delta}$$

Le morphisme est explicite (mais compliqué).

Pseudo-addition

Entrée: $P = (X, Y, Z, T)$ et $Q = (\underline{X}, \underline{Y}, \underline{Z}, \underline{T})$ sur $\mathcal{K}_{\alpha,\beta,\gamma,\delta}$ et $P - Q = (\bar{X}, \bar{Y}, \bar{Z}, \bar{T})$ avec $\bar{X}\bar{Y}\bar{Z}\bar{T} \neq 0$

Sortie: $P + Q$

1. $X' = (X + Y + Z + T)(\underline{X} + \underline{Y} + \underline{Z} + \underline{T})\frac{B}{A}$
2. $Y' = (X + Y - Z - T)(\underline{X} + \underline{Y} - \underline{Z} - \underline{T})$
3. $Z' = (X - Y + Z - T)(\underline{X} - \underline{Y} + \underline{Z} - \underline{T})\frac{B}{C}$
4. $T' = (X - Y - Z + T)(\underline{X} - \underline{Y} - \underline{Z} + \underline{T})\frac{B}{D}$
5. $x = (X' + Y' + Z' + T')^2$
6. $y = (X' + Y' - Z' - T')^2 \frac{\bar{X}}{\bar{Y}}$
7. $z = (X' - Y' + Z' - T')^2 \frac{\bar{X}}{\bar{Z}}$
8. $t = (X' - Y' - Z' + T')^2 \frac{\bar{X}}{\bar{T}}$
9. Renvoyer (x, y, z, t)

Coût: 4 carrés, 10 produits, 3 divisions*

Multiplication

Nous cherchons une chaîne de doublement et de pseudo-additions:

$$ex : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 7 \longrightarrow 10 \longrightarrow 17$$

Multiplication

Nous cherchons une chaîne de doublement et de pseudo-additions:

$$ex : \qquad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 7 \longrightarrow 10 \longrightarrow 17$$

$$n*P,\ (n+1)*P \longmapsto (2n)*P,\ (2n+1)*P,\ (2n+2)*P$$

À chaque étape nous choisissons le point qui doit être doublé selon le developpement binaire de k:

$$ex : \qquad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5 \longrightarrow 8 \longrightarrow 9 \longrightarrow 17$$

Multiplication

Nous cherchons une chaîne de doublement et de pseudo-additions:

$$ex : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 7 \longrightarrow 10 \longrightarrow 17$$

$$n*P,\ (n+1)*P \longmapsto (2n)*P,\ (2n+1)*P,\ (2n+2)*P$$

À chaque étape nous choisissons le point qui doit être doublé selon le developpement binaire de k:

$$ex : \quad 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 4 \longrightarrow 5 \longrightarrow 8 \longrightarrow 9 \longrightarrow 17$$

À chaque étape, $(n+1)*P - n*P = P$ donc $\frac{\bar{X}}{\bar{Y}}$, $\frac{\bar{X}}{\bar{Z}}$, $\frac{\bar{X}}{\bar{T}}$ peuvent être précalculées.

Le coût de l'algorithme est pour chaque boucle:

$$\begin{aligned} Doublement : &\quad 8\,S \quad + 6\,M \\ Pseudo-addition : &\quad 4\,S \quad + 10\,M \\ Total : &\quad 9\,S \quad + 16\,M \end{aligned}$$

Paramétrisation

Conditions

Il faut:

- $\mathcal{C}$ $(2,2)$-décomposable: $\lambda = \mu\frac{1-\nu}{1-\mu}$
- $\mathcal{E}_i$ définie sur $\mathbb{Z}/N\mathbb{Z}$: $\mu(\mu-\nu) = \square$
- Pouvoir travailler sur $\mathcal{K}$: $\alpha, \beta, \gamma, \delta$ *rationnels*

Conditions

Il faut:

- $\mathcal{C}$ $(2,2)$-décomposable: $\lambda = \mu\frac{1-\nu}{1-\mu}$
- $\mathcal{E}_i$ définie sur $\mathbb{Z}/N\mathbb{Z}$: $\mu(\mu-\nu) = \square$
- Pouvoir travailler sur $\mathcal{K}$: $\alpha, \beta, \gamma, \delta$ *rationnels*

Ces conditions imposent $\alpha = \delta$.

$$\alpha = 1 \qquad \beta = \frac{\mu}{\sqrt{\lambda\mu\nu}} \qquad \gamma = \frac{\sqrt{\lambda\mu\nu}}{\nu} \qquad \delta = 1$$

Conditions

Il faut:

- $\mathcal{C}$ $(2,2)$-décomposable: $\lambda = \mu\frac{1-\nu}{1-\mu}$
- $\mathcal{E}_i$ définie sur $\mathbb{Z}/N\mathbb{Z}$: $\mu(\mu-\nu) = \square$
- Pouvoir travailler sur $\mathcal{K}$: $\lambda\mu\nu = \square$

Conditions

Il faut:

- $\mathcal{C}$ $(2,2)$-décomposable: $\lambda = \mu\frac{1-\nu}{1-\mu}$
- $\mathcal{E}_i$ définie sur $\mathbb{Z}/N\mathbb{Z}$: $\mu(\mu-\nu) = \square$
- Pouvoir travailler sur $\mathcal{K}$: $\lambda\mu\nu = \square$

Nous obtenons une courbe elliptique sur $\mathbb{Q}(a)$:

$$y^2 = 1 + \left(-3a^2 + a^4\right)x^2 + a^2x^4$$

Comment choisir un point sur $\mathcal{K}$?

Deux solutions:

- Mettre une coordonnée à 0. Les autres sont sur une courbe paramétrable.
  Coût $k * P$: 10 S + 13 M par boucle.

Comment choisir un point sur $\mathcal{K}$?

Deux solutions:

- Mettre une coordonnée à 0. Les autres sont sur une courbe paramétrable.
  Coût $k * P$: 10 S + 13 M par boucle.
- Prendre deux coordonnées égales ou opposées.
  Coût $k * P$: 10 S + 12 M par boucle.

L'algorithme HECM

ALGORITHME: HECM (entrée N et B_1)

1. Choisir une courbe hyperelliptique décomposable avec un point P sur la surface de Kummer.
2. Calculer $k * P$ avec $k = ppcm(1, 2, \ldots, B_1)$
4. Calculer l'image $\psi(k * P)$ de $k * P$ sur les courbes elliptiques sous-jacentes
3. Espérer que $\psi(k * P) = O_{\mathcal{E}_i} \ mod \ p$.
4. Sinon revenir à 1.

Si $\#\mathcal{E}_1(\mathbb{F}_p)$ *ou* $\#\mathcal{E}_2(\mathbb{F}_p)$ est B_1-friable, alors nous trouverons $p \mid N$.

Travail futur

- Continuer de comparer HECM et ECM
- Utiliser des multiplications par de petits paramètres
- Est-il possible d'améliorer la probabilité de succès en améliorant la torsion?
- Que se passe t'il dans le cas d'autres courbes décomposables?