

Stage Liesse - Factorisation par les courbes elliptiques

15 mai 2018

Les exercices peuvent se résoudre avec SAGE, que l'on lance depuis un terminal en indiquant `sage -n jupyter`.

Les algorithmes de factorisation présentés ici reposent sur le théorème suivant.

Théorème 1 (Lagrange). *L'ordre d'un élément d'un groupe est un diviseur de l'ordre du groupe.*

En particulier, on retrouve le petit théorème de Fermat en se plaçant dans le groupe \mathbb{F}_p^\times :

$$\forall a \in \mathbb{F}_p^\times, \quad a^{p-1} \equiv 1 \pmod{p}.$$

Mise en route : l'algorithme $p - 1$ de Pollard

L'algorithme $p - 1$ est un algorithme inventé par John Pollard en 1974. Il repose sur l'idée suivante. Soit n un entier à factoriser et p l'un de ses facteurs premiers. Supposons que $p - 1$ divise un certain entier m . Alors, par le petit théorème de Fermat, pour tout entier a , $a^m \equiv a \pmod{p}$. Donc le $\text{pgcd}(a^m - 1, n)$ n'est pas trivial et peut fournir un diviseur de n .

Il nous reste à décider d'une valeur de m . Nous choisissons le PPCM de l'ensemble des entiers $\{1, 2, 3, \dots, b\}$ pour une certaine borne b .

Definition 2. On dit qu'un entier x est *b-friable* lorsque tous ses diviseurs premiers sont inférieurs à b .

On dit qu'un entier x est *b-ultrafriable* si toutes les puissances d'un nombre premier qui le divisent sont inférieures à b .

Ce choix de m permet d'attraper les facteurs premiers p de n tels que $p - 1$ est *b-ultrafriable*.

On obtient l'algorithme suivant :

Algorithme 1 : Méthode $p - 1$ de Pollard

Entrées : Entier n , borne de friabilité b , liste P des entiers premiers $\leq b$ **Sorties** : Diviseur propre de n ou « échec : pas de facteur p avec $p - 1$ qui soit b -ultrafriable »

```

1  $a \leftarrow$  Élément aléatoire de  $\llbracket 2, n - 1 \rrbracket$ .
2 si  $g = a \wedge n > 1$  alors
3    $\lfloor$  retourner  $g$ 
4 pour  $p \in P$  faire
5   Calculer le plus grand entier  $\alpha_p$  tel que  $p^{\alpha_p} \leq b$ 
6   pour  $j \in \llbracket 1, \alpha_p \rrbracket$  faire
7      $a \leftarrow a^p \pmod n$ 
8     si  $1 < g = (a - 1) \wedge n < n$  alors
9        $\lfloor$  retourner  $g$ 
10 retourner Échec

```

Bilan : soit n un entier que nous cherchons à factoriser. On suppose que n se décompose en un produit $n = pq$ où p et q sont deux entiers premiers entre eux. Alors, par le lemme chinois,

$$(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times.$$

La méthode $p - 1$ de Pollard révèle le facteur p lorsque l'on a obtenu dans l'algorithme les éléments $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ et m tels que

$$a^m = 1 \pmod p \quad a^m \neq 1 \pmod q. \quad (1)$$

Exercice 3. 1. Programmer l'algorithme $p - 1$ de Pollard.

2. Vérifier sur plusieurs exemples qu'il fonctionne quand n possède des facteurs ultrafriables et qu'il ne fonctionne pas sinon.

Les courbes elliptiques

Nous nous plaçons sur un corps fini \mathbb{F}_p avec p premier et > 3 . Une courbe elliptique \mathcal{E} est la réunion disjointe d'un point noté $0_{\mathcal{E}}$ (et dit point à l'infini) et l'ensemble des points affines (x, y) vérifiant

$$\mathcal{E}_{a,b} : y^2 = x^3 + ax + b$$

pour des coefficients a et b fixés tels que $4a^3 + 27b^2 \neq 0 \in \mathbb{F}_p$. Nous noterons $\mathcal{E}_{a,b}(\mathbb{F}_p)$ cette courbe.

On peut définir une loi d'addition sur $\mathcal{E}_{a,b}(\mathbb{F}_p)$ par les règles suivantes :

— le neutre est le point à l'infini $0_{\mathcal{E}}$,

- l'opposé d'un point affine $P(x_P, y_P)$ est son symétrique $(x_P, -y_P)$ par rapport à l'axe (Ox) ,
- trois points alignés sont de somme nulle.

Ainsi, pour calculer la somme $P + Q$, on recherche la troisième intersection de la droite (PQ) , ou de la tangente à \mathcal{E} en P , avec \mathcal{E} et on renvoie sa symétrie par rapport à l'axe (Ox) (voir figure 1).

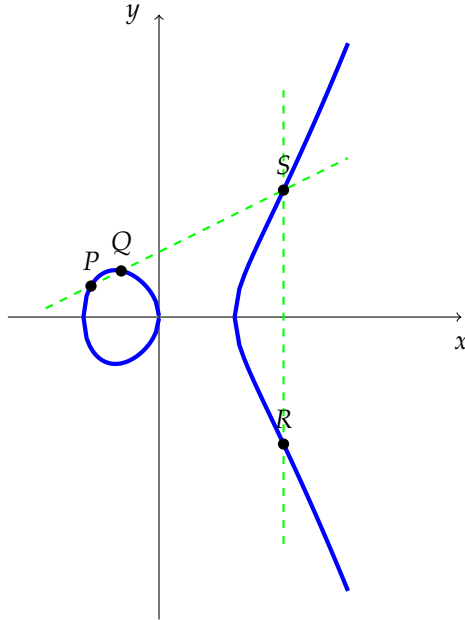


FIGURE 1: Somme de deux points :
 $P + Q = R$, $S = -R$.

Théorème 4. *Le groupe des points $\mathcal{E}_{a,b}(\mathbb{F}_p)$ est toujours de la forme*

$$\mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/s\mathbb{Z} \quad (\text{avec } r|s).$$

De plus, on a la borne suivante, dite de Hasse,

$$p + 1 - 2\sqrt{p} \leq |\mathcal{E}_{a,b}(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$$

Théorème 5. *Pour tout entier $m \in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$, il existe une courbe elliptique telle que $|\mathcal{E}_{a,b}(\mathbb{F}_p)| = m$.*

De plus, il existe $c > 0$ tel que si \mathcal{S} est un sous-ensemble de $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ de plus de 3 éléments, alors le nombre $N(\mathcal{S})$ de courbes elliptiques dont le cardinal est dans \mathcal{S} satisfait

$$N(\mathcal{S}) > \frac{c|\mathcal{S}|p^{3/2}}{\log p}.$$

Exemple 6. Le cryptosystème de Menezes & Vanstone est un protocole (aujourd'hui déconseillé) de cryptographie asymétrique qui permet à Alice de recevoir un message de Bob

Génération de clés Alice fixe une courbe elliptique $\mathcal{E}(\mathbb{F}_p)$, des points G, H et un entier m tel que $mG = H$.

Clé privée L'entier m est sa clé secrète.

Clé publique Elle publie la courbe et les points G et H .

Chiffrement Bob peut envoyer des messages $(x_1, x_2) \in \mathbb{F}_p^2$. Pour cela, il choisit un entier aléatoire k . Il calcule $Y = kG$. Il calcule $(c_1, c_2) = kH$. Il calcule enfin $s_1 = c_1x_1 \pmod p$ et $s_2 = c_2x_2 \pmod p$. Il envoie à Alice le triplet $(Y, s_1, s_2) \in \mathcal{E} \times \mathbb{F}_p \times \mathbb{F}_p$.

Déchiffrement Alice calcule $mY = mkG = kH = (c_1, c_2)$. À partir de c_1 et de c_2 , elle retrouve le message avec $m_1 = c_1^{-1}s_1 \pmod p$ et $m_2 = c_2^{-1}s_2 \pmod p$.

Exercice 7. On donne la cubique \mathcal{E} définie sur \mathbb{F}_{13} par

$$y^2 = x^3 + 4x + 7.$$

1. Vérifier qu'il s'agit d'une courbe elliptique et que $G = (4, 3)$ appartient à la courbe.
2. Alice et Bob utilisent le cryptosystème de Menezes et Vanstone pour communiquer, avec le point G et la clé secrète $m = 9$ (notation de l'exemple 6).
 - (a) Calculer le point H de la clé publique d'Alice.
 - (b) Bob veut envoyer le message $(2, 7)$ à Alice. Calculer son chiffré.
 - (c) Alice reçoit le message (Y, s_1, s_2) de la part de Bob avec $Y = (1, 5)$, $s_1 = 7$ et $s_2 = 2$. Retrouver le clair.

L'algorithmme ECM

L'algorithmme ECM (Elliptic Curve Method) a été inventé en 1985 par Lenstra. Il revisite la méthode $p-1$ de Pollard.

Soit $\mathcal{E}_{a,b} : y^2 = x^2 + ax + b$ une cubique sur $\mathbb{Z}/n\mathbb{Z}$ (avec $(4a^3 + 27b^2) \wedge n = 1$). Grâce au lemme chinois, on a une application naturelle

$$\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z}) \rightarrow \mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z}) \times \mathcal{E}_{a,b}(\mathbb{Z}/q\mathbb{Z})$$

entre les points affines de ces courbes (que l'on étend au point à l'infini par $0_{\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})} \mapsto (0_{\mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z})}, 0_{\mathcal{E}_{a,b}(\mathbb{Z}/q\mathbb{Z})})$). La méthode ECM consiste à trouver un point $A \in \mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ et un entier m tel que

$$\begin{cases} m \cdot A = 0_{\mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z})} & \text{dans } \mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z}) \\ m \cdot A \neq 0_{\mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z})} & \text{dans } \mathcal{E}_{a,b}(\mathbb{Z}/q\mathbb{Z}) \end{cases} \quad (2)$$

(comparer avec l'équation (1))

Dans cette situation, le calcul de $m \cdot A$ dans $\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ échoue. En effet, tous les calculs restent valable modulo p et montrent que $m \cdot A$ est le point $0_{\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})}$. Mais tous les calculs restent valable modulo q aussi et montrent que $m \cdot A$ ne peut pas être le point $0_{\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})}$. Calculer $m \cdot A$ dans $\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ revient à faire une suite d'opérations arithmétiques dans $\mathbb{Z}/n\mathbb{Z}$: elles peuvent toutes être réalisées sauf lorsqu'on cherche à diviser par un élément x de $\mathbb{Z}/n\mathbb{Z}$ non inversible. Mais dans ce cas, le pgcd de x et de n est non trivial et fournit un facteur de n .

En faisant le choix $m = \text{ppcm}\{1, 2, 3, \dots, b\}$, on obtient l'algorithme suivant :

Algorithme 2 : Factorisation par courbes elliptiques de Lenstra (ECM)

Entrées : Entier n premier avec 6 et qui n'est pas une puissance d'un nombre premier. Borne B .

Sorties : Diviseur non-trivial de n ou « échec »

```

1 Tirer au hasard  $a, x_0, y_0 \in \llbracket 0, n-1 \rrbracket$ 
2  $b \leftarrow y_0^2 - x_0^3 - ax_0$ 
3  $g \leftarrow \text{pgcd}(4a^3 + 27b^2, n)$ 
4 si  $1 < g < n$  alors
5   | retourner  $g$ 
6 sinon si  $g = n$  alors
7   | retourner Echec
8  $\mathcal{E} \leftarrow \mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ 
9  $A \leftarrow (x_0, y_0)$ 
10 pour  $p$  premier  $\leq B$  faire
11   | Trouver  $e$  maximal tel que  $p^e \leq B$ 
12   | essayer
13   |   |  $A \leftarrow p^e \cdot A$  dans  $\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ 
14   |   | excepté Erreur d'inversion
15   |   | retourner Facteur de  $n$  obtenu
16 retourner Echec

```

Choix de la borne de friabilité Il y a de l'ordre de $O(B)$ opérations dans $\mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z})$ pour une tentative d'application de l'algorithme. On peut estimer également la probabilité de trouver un point A dont l'ordre soit B -friable dans $\mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z})$ et ne le soit pas dans $\mathcal{E}_{a,b}(\mathbb{Z}/q\mathbb{Z})$ (en vérité, la deuxième condition est très improbable lorsque la première est satisfaite et peut être oubliée). On obtient une probabilité de friabilité de l'ordre de

$$\text{prob}(B) = c \cdot |\mathcal{S}| \cdot \frac{p^{3/2}}{\log p} \cdot \frac{1}{p^2}$$

où S est l'ensemble des nombres friables compris entre $p + 1 - 2\sqrt{2}$ et $p + 1 + 2\sqrt{2}$.

On peut ainsi optimiser la complexité de l'algorithme en minimisant $\frac{B}{\text{prob}(B)}$ (en s'appuyant sur des résultats de distribution des nombres friables). On obtient $L\left(1/2, \sqrt{2}/2 + \epsilon; \sqrt{p}\right)$ et une complexité en

$$L\left(1/2, \sqrt{2} + \epsilon; \sqrt{p}\right)$$

où

$$L(\alpha, \beta; N) = \exp\left(\beta(\log N)^\alpha (\log \log N)^{1-\alpha}\right).$$

Remarque 8. La complexité de ECM est liée à la taille du plus petit diviseur de n et non pas à n lui-même. Aussi, la méthode est particulièrement efficace pour éliminer les facteurs de n de taille moyenne. Elle peut être utilisée en complément à d'autres méthodes pour retirer de n les facteurs de petite et moyenne taille, le cas le plus défavorable étant le cas $n = pq$ avec p et q premiers de même taille.

Dans un cas pratique, le choix de la borne de friabilité B doit donc correspondre au temps que l'on est prêt à consacrer à la recherche de facteurs de n .

Exemple 9. Cherchons à factoriser $n = 3397$ par la méthode ECM. On tire au hasard la cubique d'équation

$$y^2 = x^3 + 4x + 25$$

et le point $P = (3, -8)$.

— On commence par calculer $2P$ selon les formules habituelles. On calcule la pente de la tangente en P qui vaut

$$\lambda = \frac{3x_P^2 + a}{2y_P} = \frac{31}{-16} = 635 \pmod{n}.$$

On en tire le point $2P$ de coordonnées :

$$x_{2P} = \lambda^2 - 2x_P = 2373 \quad y_{2P} = -y_P + \lambda(x_P - x_{2P}) = 3326.$$

— On calcule ensuite $3P = 2P + P$. La pente de la droite $(P, 2P)$ devrait être

$$\lambda = \frac{y_{2P} - y_P}{x_{2P} - x_P} = \frac{3326 - (-8)}{2373 - 3} = \frac{3334}{2370}.$$

Mais 2370 n'est pas inversible modulo n . En effet, le pgcd $2370 \wedge 3397$ vaut 79. Le calcul de λ échoue et révèle, ce faisant, un facteur de n , à savoir 79.

Exercice 10. On considère les paramètres

$$a = b = 4, \quad p = 47, \quad q = 59 \quad \text{et} \quad P = (1, 3).$$

On pose $n = pq$.

1. Quel est l'ordre ω_p et ω_q de P dans $\mathcal{E}_{a,b}(\mathbb{F}_p)$ et dans $\mathcal{E}_{a,b}(\mathbb{F}_q)$?
2. Soit ϕ_p la projection modulo p , à savoir $\phi_p : \mathcal{E}_{a,b}(\mathbb{Z}/n\mathbb{Z}) \rightarrow \mathcal{E}_{a,b}(\mathbb{F}_p)$. Quels sont les antécédants du point $(0 : 1 : 0)$ par ϕ_p ?
3. Que se passe-t-il si on cherche à calculer $\omega_p P$ et $\omega_q P$ dans $\mathcal{E}(\mathbb{Z}/n\mathbb{Z})$?

Afin d'implémenter l'algorithme ECM avec Sage, nous voulons redéfinir l'algorithme de division afin que le calcul de x/y dans $\mathbb{Z}/n\mathbb{Z}$ quand y n'est pas inversible lève une erreur qui indique le facteur de n que l'on a découvert. On définit

```
class FoundFactor(Exception):
    def __init__(self, value):
        self.value = value
    def __str__(self):
        return repr(self.value)
```

Exercice 11. Ecrire une fonction `division` qui prend en entrée deux éléments x et y de $\mathbb{Z}/n\mathbb{Z}$ et renvoie le quotient x/y lorsque celui-ci existe, une erreur `ZeroDivisionError` lorsque y est nul dans $\mathbb{Z}/n\mathbb{Z}$ et une erreur `FoundFactor` lorsque y est non nul mais n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 12. On désigne par (x_M, y_M) les coordonnées affines du point M .

1. Montrer que l'addition $R = P + Q$ de deux points distincts P et Q de la courbe $\mathcal{E}_{a,b}$ conduit aux formules

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}, \quad x_R = \lambda^2 - x_P - x_Q, \quad y_R = -y_P + \lambda(x_P - x_R)$$

où λ est la pente de la droite (PQ) .

2. Montrer que la duplication $R = 2P$ d'un point P de $\mathcal{E}_{a,b}$ conduit en général aux formules

$$\lambda = \frac{3x_P^2 + a}{2y_P}, \quad x_R = \lambda^2 - 2x_P, \quad y_R = -y_P + \lambda(x_P - x_R)$$

où λ est la pente de la tangente à \mathcal{E} en P . Que se passe-t-il si $y_P = 0$?

3. Comment faire pour calculer l'ensemble des points de 2-torsion de $\mathcal{E}_{a,b}$? Quelle structure du sous-groupe $\mathcal{E}[2]$ de 2-torsion peut-on obtenir ?
4. Écrire une fonction `addition` qui prend en entrée deux points P et Q d'une courbe elliptique et renvoie leur somme $P + Q$.
5. Comparer avec la méthode native de SAGE. On pourra prendre par exemple la courbe $\mathcal{E}_{a,1}(\mathbb{F}_q)$ et différents multiples du point P_0 de coordonnées $(0, 1)$.

Exercice 13. 1. Ecrire une fonction multiplication qui prend en entrée un point P d'une courbe elliptique et un scalaire λ et renvoie le produit $\lambda \cdot P$.

On pourra utiliser une méthode d'exponentiation rapide dont le principe est le suivant :

$$\forall \lambda \in \mathbb{N}, \quad \lambda \cdot P = \begin{cases} 0_{\mathcal{E}_{a,b}} & \text{si } \lambda = 0 \\ P & \text{si } \lambda = 1 \\ \frac{\lambda}{2} \cdot (P + P) & \text{si } \lambda \text{ est pair} \\ P + \frac{\lambda - 1}{2} \cdot (P + P) & \text{si } \lambda \text{ est impair} \end{cases}$$

2. Comparer avec la méthode native de SAGE.

Exercice 14. 1. Écrire une fonction ECM qui implante l'algorithme ECM de Lenstra.

2. Tester votre fonction sur différents exemples.

Exercice 15. On pose $n = 42857766101$. Quelle est la plus petite valeur de la borne de friabilité B telle que l'algorithme factorise n avec les paramètres $a = b = 4$ et $P = (1, 3)$? [Indication : factoriser les exposants des groupes $\mathcal{E}(\mathbb{F}_p)$ et $\mathcal{E}(\mathbb{F}_q)$ où p et q sont les deux diviseurs premiers de n .]

Corrigés de certains exercices

Solution 3. 1. Une implémentation de la méthode $p-1$ de Pollard :

```
def Pollard(n,b):
    Zn=Zmod(n)
    a=Zn.random_element()
    g = gcd(ZZ(a),ZZ(n))
    if g>1:
        return g
    for p in primes(b):
        c=1
        while(c<b):
            c*=p
            a=mod(a^p ,n)
            g=gcd(ZZ(a-1),ZZ(n))
            if g>1:
                return g
    return false
```

2. On peut fabriquer un entier composé réfractaire comme suit :

```
b=30
L = [p for p in primes(b+1,10*b) if max((p-1).prime_divisors()) >= b]
p=L[0]
q=L[1]
n=p*q
print factor(p-1), factor(q-1)
Pollard(n,b)
```

(Les entiers $p-1$ et $q-1$ sont bien b -ultrafriables!)

Solution 7. 1. Le discriminant est non nul.

2.(a) $H = (11,11)$.

(b) $k = 5$, donc $Y = kG = (11,2)$. $kH = (1,5)$. Donc $s_1 = x_1 = 2$ et $s_2 = 5x_2 = 9$.

(c) Le clair est $(5,8)$.

Solution 10. 1. On a $\omega_p = 3$ et $\omega_q = 4$.

```
p=47
E = EllipticCurve(Zmod(p), [4,4])
A = E(1,3)
A.order()
```

2. Il n'y a qu'un seul point : $(0 : 1 : 0)$

3. On doit avoir $\phi_p(\omega_p P) = (0 : 1 : 0)$ et $\phi_q(\omega_p P) \neq (0 : 1 : 0)$, ce qui implique (par la question précédente) que $\omega_p P = (0 : 1 : 0)$ et que $\omega_p P \neq (0 : 1 : 0)$. Contradiction. Calculer $\omega_p P$ déclenche une erreur.

```
p=47
q=59
n=p*q
E = EllipticCurve(Zmod(n), [4, 4])
A = E(1, 3)
3*A
4*A
```

Solution 11. On peut faire

```
def division(x,y):
    n = y.modulus()
    if ZZ(n).divides(ZZ(y)):
        raise ZeroDivisionError
    elif gcd(ZZ(y), ZZ(n))>1:
        raise FoundFactor(gcd(ZZ(y), ZZ(n)))
    else:
        return mod(x, n)/mod(y, n)
```

Solution 12. 1. L'équation de la droite (PQ) est clairement

$$y - y_P = \lambda(x - x_P)$$

Pour trouver S , on doit donc résoudre le système

$$\begin{cases} y - y_P = \lambda(x - x_P) \\ y^2 = x^3 + ax + b \end{cases}$$

qui conduit à l'équation

$$x^3 - \lambda^2 x^2 + [\dots] = 0.$$

Mais

$$x^3 - \lambda^2 x^2 + [\dots] = (x - x_P)(x - x_Q)(x - x_S).$$

Donc par identification

$$x_S = \lambda^2 - x_P - x_Q$$

La conclusion suit immédiatement.

2. On se souvient que la tangente en x_P a pour équation

$$\frac{\partial f}{\partial x}(P) \cdot (x - x_P) + \frac{\partial f}{\partial y}(P) \cdot (y - y_P) = 0$$

ce qui fournit bien la pente $\lambda = \frac{3x_P^2+a}{2y_P}$. Le reste du calcul est identique la question précédente. Si $y_P = 0$, on obtient une tangente verticale qui intersecte la courbe en $0_{\mathcal{E}}$. Donc $2P = 0_{\mathcal{E}}$.

3. Le sous-groupe $\mathcal{E}[2]$ de 2-torsion correspond aux points P tels que $2P = 0_{\mathcal{E}}$. On retrouve donc le point $0_{\mathcal{E}}$ et l'ensemble des points $(\sigma, 0)$ tels que $\sigma^3 + a\sigma + b = 0$. Il y en a 0, 1 ou 3, ce qui correspond aux groupes trivial, $\mathbb{Z}/2\mathbb{Z}$ ou $(\mathbb{Z}/2\mathbb{Z})^2$.
4. Algorithme d'addition

```
def addition(P,Q):
    if P[2]==0:
        return Q
    elif Q[2]==0:
        return P
    elif P[0]==Q[0] and P[1]==-Q[1]:
        return P.curve()(0)
    else:
        if P==Q:
            lamb = division( (3*P[0]^2+P.curve().a4()) , (2*P[1]))
        else:
            lamb = division(Q[1]-P[1], Q[0]-P[0])
        x = lamb^2-P[0]-Q[0]
        y = -P[1]+lamb*(P[0]-x)
        return P.curve()(x,y)
```

Solution 13. 1. Multiplication

```
def multiplication(lamb,P):
    E = P.curve()
    if lamb == 0:
        return E(0)
    elif lamb == 1:
        return P
    elif lamb%2 == 0:
        return multiplication(lamb/2,addition(P,P))
    else:
        Q = multiplication(ZZ((lamb-1)/2),addition(P,P))
        return addition(P,Q)
```

2.

Solution 14. 1. Algorithme ECM

```

def ECM(n,B):
    Zn = Zmod(n)
    a = Zn.random_element()
    x0 = Zn.random_element()
    y0 = Zn.random_element()
    b = y0^2-x0^3-a*x0
    g = gcd(ZZ(4*a^3+27*b^2),ZZ(n))
    if g==n:
        return False
    elif g>1:
        return g
    E = EllipticCurve(Zn, [a,b])
    A = E(x0,y0)
    for p in primes(B):
        c=1
        while (c<B):
            c*=p
            try:
                A = multiplication(p,A)
            except FoundFactor as FF:
                print 'Facteur trouvé :'
                return FF.value
    return False

```

2.

Solution 15. On peut faire

```

n = 42857766101
print factor(n)
p=63029
q=679969
Ep = EllipticCurve(GF(p),[4,4])
Eq = EllipticCurve(GF(q),[4,4])
Ep.abelian_group(), Eq.abelian_group()
Ep.cardinality().factor() , Eq.cardinality().factor()

```

On remarque alors que les deux groupes sont des groupes cycliques $\mathcal{E}(\mathbb{F}_p) = \mathbb{Z}/62896\mathbb{Z}$ et $\mathcal{E}(\mathbb{F}_q) = \mathbb{Z}/678501\mathbb{Z}$ et que, de plus,

$$62896 = 2^4 \cdot 3931 \quad \text{et} \quad 678501 = 3^2 \cdot 75389.$$

Comme le plus petit des plus grands facteurs de ces ordres est 3931, il faut donc aller génériquement jusqu'à la borne $B = 3931$ (inclusive).

Il se trouve que ici P est d'ordre $2^3 \cdot 3931$ (faire `Ep(Pn).order().factor()` pour s'en apercevoir). On peut confirmer la borne trouvée en faisant

```

n = 42857766101
En = EllipticCurve(Integers(n), [4, 4])
Pn = En(1, 3)

Q= Pn
for r in primes(3932):
    for i in range(log(n,r)+1):
        Q= r*Q

```

Remarque : le hasard aurait pu nous donner $P' = (21091706543, 38501272299)$ au lieu de P et qui est d'ordre 8 dans dans $\mathcal{E}(\mathbb{F}_p)$. Dans ce cas, calculer $8P'$ dans $\mathcal{E}(\mathbb{Z}/n\mathbb{Z})$ provoque déjà une erreur.