Examen de Cryptologie
1re session

10 mai 2022
Durée 2h

Auteurs
Valérie Ménissier-Morain, Maxime Roméas, Clémence Bouvier, Clara Pernot

Version du 10 mai 2022

Le seul document autorisé est une feuille manuscrite A4 recto-verso.
L'utilisation d'un appareil électronique est proscrite pendant toute la durée de l'épreuve.
Le barème sur 40 points est indicatif. La note finale sera le minimum entre les points obtenus et 20.

Exercice 1 – Théorème des restes chinois – 8 points

1. (**Algorithme d'Euclide étendu – 2 points**) En utilisant l'algorithme d'Euclide étendu, montrer que 7 est inversible mod 165 et calculer son inverse.

Solution :

On va appliquer l'algorithme d'Euclide étendu à $n = 165$ et $a = 7$.

Dans le tableau suivant chaque ligne à partir de la ligne $i = 1$ se lit :

- la partie gauche (colorée en rose), si $r_i \neq 0$, la division euclidienne de r_{i-1} par r_i est $r_{i-1} = q_i * r_i + r_{i+1}$ qui définit le quotient $q_i = \lfloor \frac{r_{i-1}}{r_i} \rfloor$ et le reste suivant $r_{i+1} = r_{i-1} - q_i * r_i$; sinon on s'arrête.
- pour la partie droite (colorée en jaune), $u_{i+1} = u_{i-1} - q_i * u_i$ et $v_{i+1} = v_{i-1} - q_i * v_i$
- avec l'initialisation (partie en haut, colorée en bleu) : $r_0 = a$, $r_1 = b$, $u_0 = v_1 = 1$, $v_0 = u_1 = 0$
- à chaque étape on a $r_i = u_i\, n + v_i\, a \quad \forall i$.

On exploite cette information sur les deux dernières lignes du tableau (cadres rouge et vert) :

- avant-dernière ligne (de numéro k), on trouve r_{k+1} (dans la cinquième colonne) le dernier reste positif, c'est-à-dire le pgcd de n et a et $r_{k+1} = u_{k+1}\, n + v_{k+1}\, a$ est une relation de Bézout.
  Si $r_{k+1} = 1$, alors v_{k+1} mod n est l'inverse de a modulo n, a n'est pas diviseur de zéro dans $\mathbb{Z}/n\mathbb{Z}$.
- à la dernière ligne (de numéro $k+1$ donc), on trouve $0 = r_{k+2} = n\, u_{k+2} + a\, v_{k+2}$.
  Si $r_{k+1} > 1$, alors a n'est pas inversible modulo n, c'est un diviseur de 0 dans $\mathbb{Z}/n\mathbb{Z}$, $|v_{k+2}| < n$ donc v_{k+2} est un témoin de diviseur de 0 pour a dans $\mathbb{Z}/n\mathbb{Z}$.

i	r_{i-1}	q_i	r_i	r_{i+1}	u_{i+1}	v_{i+1}
-1					1	0
0			165	7	0	1
1	165	23	7	4	1	-23
2	7	1	4	3	-1	24
3	4	1	3	1	2	-47
4	3	3	1	0	-7	165

Ici $k = 3$, on constate que $\text{pgcd}(7, 165) = r_{k+1} = 1$ donc 7 est inversible modulo 165. On a la relation de Bezout :

$$1 = 2 \times 165 - 47 \times 7$$

et $7^{-1} = -47 \bmod 165$.

2. (**2 points**) Soit $N = 2^{100}$. Montrer que

$$\begin{cases} N = 1 \bmod 3 \\ N = 1 \bmod 5 \\ N = 2 \bmod 7 \\ N = 1 \bmod 11 \end{cases}$$

Solution :

Méthode 1 : $2 \bmod 3 = -1$ donc $2^{100} = (-1)^{100} \bmod 3 = 1 \bmod 3$.
$2^2 = -1 \bmod 5$ donc $2^{100} = (2^2)^{50} = (-1)^{50} \bmod 5 = 1 \bmod 5$.
$2^3 = 1 \bmod 7$ donc $2^{100} = 2 \cdot (2^3)^{33} \bmod 7 = 2 \cdot 1^{33} \bmod 7 = 2 \bmod 7$.
$2^5 = 32 = -1 \bmod 11$ donc $2^{100} = (2^5)^{20} = 1 \bmod 11$.
Méthode 2 (qu'on peut adapter pour 3, 5 et 7) : 11 est premier donc, d'après le théorème de Lagrange, tout élément est d'ordre divisant $\varphi(11) = 11 - 1 = 10$ modulo 11. Donc $2^{100} = (2^{10})^{10} = 1^{10} \bmod 11 = 1 \bmod 11$.

3. (**1 point**) En déduire que $N = 1 \bmod 165$.

Solution :

$N = 1 \bmod 3, 5$ et 11 donc $N - 1$ est multiple de 3, 5 et 11 . Comme les modules sont premiers entre eux deux à deux , on a (corollaire de Gauss) que $N - 1$ est multiple de $3 \times 5 \times 11 = 165$. Donc $N = 1 \bmod 165$.
Corollaire de Gauss : Si a, b, c sont trois entiers tels que $\text{pgcd}(a, b) = 1$, $a \mid c$ et $b \mid c$ alors $ab \mid c$.

4. (**3 points**) Quel est le reste de la division euclidienne de 2^{100} par 1155 ?

Solution :

Dans la question 1, on a calculé la relation de Bezout suivante : $1 = 2 \times 165 - 47 \times 7$.
Dans les questions 2 et 3, on a montré que N satisfait les équations

$$\begin{cases} N = 1 \bmod 165 \\ N = 2 \bmod 7 \end{cases}$$

165 et 7 sont premiers entre eux , de produit $165 * 7 = 1155$.
D'après le CRT, la solution de ce système à deux équations qu'on cherche à résoudre est

$$\begin{aligned} & (2 \times 165) \times 2 + (-47 \times 7) \times 1 \bmod 1155 \\ = & \, 2 \times 165 + (2 \times 165 - 47 \times 7) \bmod 1155 \\ = & \, 2 \times 165 + 1 \bmod 1155 \\ = & \, 331 \bmod 1155 \end{aligned}$$

Donc le reste de la division euclidienne de $N = 2^{100}$ par 1155 est 331.

Exercice 2 – Courbe elliptique – 14,5 points

Dans tout cet exercice on s'intéresse au groupe additif E défini à partir des points rationnels de la courbe elliptique définie par l'équation $y^2 = x^3 + x + 3$ sur $\mathbb{F}_{11}$.

1. **(1 point)** Justifier que cette courbe est bien elliptique.

Solution :
La courbe est d'équation $y^2 = x^3 + ax + b$ définie sur $\mathbb{F}_p$ avec $p = 11$ premier, $a = 2$ et $b = 0$. Elle semble donc elliptique.
Elle est elliptique si, et seulement si, $\Delta = -16(4a^3 + 27b^2) \neq 0$. Or $4a^3 + 27b^2 = 4 \times 1 + 27 \times 3^2 = 4 + 5 \times (-2) = 3 - 6 \neq 0$ et $\Delta \neq 0$.

2. **(Points de la courbe – 3 points)** Donner, sous la forme d'un tableau comme vu en cours/TD, l'ensemble des points rationnels définissant E.

Solution :
On calcule $x^3 + x + 3$ mod 11 et y^2 mod 11 pour $x, y \in \mathbb{Z}/11\mathbb{Z}$. On regarde les collisions de ces deux listes et on déduit les points finis de la courbe.

y	y^2 mod 11
0	0
± 1	1
± 2	4
± 3	9
± 4	5
± 5	3

x	$x^3 + x + 3$ mod 11	collision	(x, y)
0	3	✓ $y = \pm 5$	$(0, \pm 5)$
1	5	✓ $y = \pm 4$	$(1, \pm 4)$
2	2		
3	0	✓ $y = 0$	$(3, 0)$
4	5	✓ $y = \pm 4$	$(4, \pm 4)$
5	1	✓ $y = \pm 1$	$(5, \pm 1)$
6	5	✓ $y = \pm 4$	$(6, \pm 4)$
7	1	✓ $y = \pm 1$	$(7, \pm 1)$
8	6		
9	4	✓ $y = \pm 2$	$(9, \pm 2)$
10	1	✓ $y = \pm 1$	$(10, \pm 1)$

3. **(Points d'ordre 2 – 0,5 point)** Quels sont les points d'ordre 2 de la courbe E ?

Solution :
Un point d'ordre 2 a une ordonnée nulle. Il y a un seul point d'ordonnée nulle : $(3, 0)$.

4. **(Cardinal – 1 point)** Vérifiez que la courbe est de cardinal $n = 18$.

Solution :
Les points rationnels de la courbe sont
- 8 paires symétriques $(0, \pm 5), (1, \pm 4), (4, \pm 4), (5, \pm 1), (6, \pm 4), (7, \pm 1), (9, \pm 2), (10, \pm 1)$
- 1 point sur l'axe des ordonnées $(3, 0)$

soit 17 points rationnels, auxquels il faut ajouter $\mathcal{O}$ le point à l'infini , ce qui fait donc 18 points au total.

5. **(Ordres possibles des éléments – 1 point)** Quels sont les ordres possibles des éléments de E.

Solution :
E est de cardinal, donc d'ordre, 18. D'après le théorème de Lagrange , l'ordre des éléments d'un groupe divise l'ordre du groupe. Par conséquent les ordres possibles des éléments de E sont les diviseurs de 18 : $1, 2, 3, 6, 9$ ou 18 .

6. (**Calcul dans E – 3 points**) Soient $P_1 = (5, 1)$ et $P_2 = (0, 6)$ deux points de E. Montrez que $[3]P_1 = P_2$.

Solution :
On vérifie que ces deux points figurent bien dans le tableau de la question 2.
- On calcule tout d'abord $[2]P_1$:

$$\lambda = \frac{3\,x_{P_1}^2 + a}{2\,y_{P_1}} = \frac{3 \times 5^2 + 1}{2 \times 1} = \frac{3 \times 3 + 1}{2 \times 1} = \frac{10}{2} = 5 \bmod 11$$

  donc $[2]P_1 = (x_{[2]P_1}, y_{[2]P_1})$ avec
  $x_{[2]P_1} = \lambda^2 - x_{P_1} - x_{P_1} = 5^2 - 5 - 5 = 3 - 5 - 5 = 4 \bmod 11$
  et $y_{[2]P_1} = \lambda\,(x_{P_1} - x_{[2]P_1}) - y_{P_1} = 5 \times (5 - 4) - 1 = 4 \bmod 11$.
- On calcule ensuite $[3]P_1 = P_1 + [2]P_1$:

$$\lambda = \frac{y_{[2]P_1} - y_{P_1}}{x_{[2]P_1} - x_{P_1}} = \frac{4 - 1}{4 - 5} = \frac{3}{-1} = -3 \bmod 11$$

  donc $P_1 + [2]P_1 = (x_{[3]P_1}, y_{[3]P_1})$ avec
  $x_{[3]P_1} = \lambda^2 - x_{P_1} - x_{[2]P_1} = (-3)^2 - 5 - 4 = 0 \bmod 11$
  et $y_{[3]P_1} = \lambda\,(x_{P_1} - x_{[3]P_1}) - y_{P_1} = (-3) \times (5 - 0) - 1 = 6 \bmod 11$.
- On constate par conséquent que $[3]P_1 = P_2$.

7. (**Structure du groupe – 3 points**) Quelle est la structure de E ? Vous justifierez votre réponse.

Solution :
- D'après le théorème de structure, E est isomorphe à $(\mathbb{Z}/d_1\mathbb{Z}, +) \times (\mathbb{Z}/d_2\mathbb{Z}, +)$ avec $d_1\,d_2 = n$, $d_1 \mid d_2$ et $d_1 \mid (p - 1)$.
- $p = 11$ donc d_1 doit être un diviseur de $11 - 1 = 10$, soit 1, 2, 5 ou 10.
- n n'est pas multiple de 5 ou 10 donc ces deux valeurs de d_1 sont écartées.
- Si $d_1 = 2$ alors d_2 est aussi multiple de 2 donc $d_1\,d_2$ doit être multiple de $2 \times 2 = 4$. Or $n = d_1\,d_2 = 18$ n'est pas multiple de 4 donc il nous faut aussi écarter la valeur 2 pour d_1.
- Il ne reste que $d_1 = 1$, $d_2 = 18$ et E est isomorphe à $(\mathbb{Z}/18\mathbb{Z}, +)$.

8. (**Maximalité de la courbe – 2 points**) Montrez qu'il n'existe pas de courbe elliptique de cardinal supérieur à 18 sur $\mathbb{F}_{11}$.

Solution :
D'après le théorème de Hasse, le cardinal d'une courbe elliptique sur $\mathbb{F}_p$ est inférieur à $p + 1 + 2\sqrt{p}$.
Soit N l'ordre d'une courbe elliptique de cardinal maximal, alors $N - p - 1$ est le plus grand entier inférieur à $2\sqrt{p}$, donc le plus grand entier i tel que $i^2 \leq (2\sqrt{p})^2 = 4p$.
Ici $p = 11$ donc $4p = 44$ est compris entre les deux carrés successifs $6^2 = 36 < 44 < 49 = 7^2$ donc $N - 11 - 1 = 6$ et $N = 18$ et il ne peut y avoir de courbe elliptique de cardinal supérieur à $N = 18$ sur $\mathbb{F}_{11}$.

Exercice 3 – Logarithme discret – 18 points

1. ($\mathbb{F}_{47}^{\times}$ **– 2 points**) Rappelez ce qu'est $\mathbb{F}_{47}^{\times}$. Quels sont ces éléments ? Quel est son cardinal ? Montrez que 16 est d'ordre 23 dans le groupe multiplicatif $\mathbb{F}_{47}^{\times}$.

Solution :
$\mathbb{F}_{47}^{\times}$ est le groupe des éléments inversibles de $\mathbb{F}_{47} = \mathbb{Z}/47\mathbb{Z}$, le corps fini à 47 éléments. Puisque 47 est premier , tous les éléments non nuls de $\mathbb{F}_{47}$ sont inversibles et $\mathbb{F}_{47}^{\times} = \mathbb{F}_{47} - \{0\}$ a 46 éléments .
D'après le théorème de Lagrange , l'ordre d'un élément divise l'ordre du groupe, ici 46, donc les ordres possibles dans le groupe multiplicatif $\mathbb{F}_{47}^{\times}$, sont les diviseurs de 46 : 1, 2, 23, 46 .
Montrons que $16^{23} = 1$. Pour cela on remarque que $16^{23} = (4^2)^{23} = 4^{46} = 1 \bmod 46$.
Il nous reste à montrer que 23 est le plus petit entier n tel que $16^n = 1$. Puisque $16^{23} = 1$, 23 est un multiple de l'ordre de 16 . Or 23 est premier et 16 n'est pas d'ordre 1. Donc 16 est bien d'ordre 23.

On va s'intéresser à la résolution de deux façons du DLP dans le sous-groupe de $\mathbb{F}_{47}^{\times}$ engendré par 16.

2. (**Baby-Step-Giant-Step – 5 points**)

   (a) (**Baby-Step-Giant-Step – 3 points**) En utilisant l'algorithme Baby-Step-Giant-Step, calculez le logarithme discret de 17 en base 16, c'est-à-dire le plus petit entier k tel que $16^k = 17 \bmod 47$.

Solution :
— On pose $s = \lceil \sqrt{47} \rceil = 7$. On va ensuite utliser la division euclidienne de k par s :

$$\exists!(q, r),\ k = q \cdot s + r \quad \text{avec } 0 \leq r < s$$

— Baby-Steps : on calcule les 16^i pour $0 \leq i \leq s - 1$

$$\begin{aligned}
16^0 &= 1 \bmod 47 \\
16^1 &= 16 \bmod 47 \\
16^2 &= 16 \times 16 = 256 = 21 \bmod 47 \\
16^3 &= 16 \times 21 = 336 = 7 \bmod 47 \\
16^4 &= 16 \times 7 = 112 = 18 \bmod 47 \\
16^5 &= 16 \times 18 = 288 = 6 \bmod 47 \\
16^6 &= 16 \times 6 = 96 = 2 \bmod 47
\end{aligned}$$

— Giant-Steps : on calcule les 17×16^{-js} pour $0 \leq j \leq s - 1$.
On va pré-calculer $16^{-s} \bmod 47$. Pour cela on a deux solutions :
  — calculer $16^7 = 16 \times 16^6 = 16 \times 2 = 32 \bmod 47$ puis utiliser l'algorithme d'Euclide étendu pour 32 et 47
  — ou bien, puisqu'on sait que $16^{23} = 1 \bmod 47$ et qu'on dispose de la valeur de plusieurs puissances de 16 modulo 47, alors $16^{-7} = 16^{16} \bmod 47 = (16^6)^2 \times 16^4 = (2^2) \times 18 = 72 = 25 \bmod 47$.

On commence donc à calculer les $17 \times 16^{-js} = 17 \times 25^j$ et on s'arrête dès qu'on retrouve une valeur de la liste précédente :

$$\begin{aligned}
17 \times 25^0 &= 17 \bmod 47 \\
17 \times 25^1 &= 425 = 2 \bmod 47
\end{aligned}$$

On a trouvé une collision pour $i = 6$ et $j = 1$ donc $k = js + i = 7 \times 1 + 6 = 13$.
Par conséquent, le logarithme discret de 17 en base 16 est 13.
On peut évidemment vérifier rapidement que $16^{13} = (16^6)^2 \times 16 = 2^2 \times 16 = 64 = 17 \bmod 47$, mais on va de toute façon vérifier à la question suivante.

(b) (**Exponentiation – 2 points**) Vous vérifierez le résultat de la question précédente en reprenant l'algorithme d'exponentiation Square-and-Multiply, dont vous donnerez la complexité.

Solution :
On rappelle que l'algorithme Square-and-Multiply permet de calculer $a^e \bmod n$ en utilisant l'écriture binaire de l'exposant $e = \sum_{i=0}^{\ell-1} e_i 2^i$ de la façon suivante :

```
function exp (a, e, n)
    x <- 1
    for i = ℓ − 1 to 0 do
        x <- x^2 mod n
        if e_i = 1 then x <- x × a mod n
        end if
    end for
    return x
end function
```

On réalise ainsi $\mathcal{O}(\log(e))$ multiplications
donc le coût de cet algorithme est : $\mathcal{O}(\log(e)\mathcal{M}(\log(n)))$.
On souhaite calculer $16^{13} \bmod 47$. En binaire, on a : $13 = (e_3e_2e_1e_0)_2 = (1101)_2$.

$$\begin{array}{ll} & x = 1 \\ e_3 = 1 & x = x^2 \times 16 = 16 \bmod 47 \\ e_2 = 1 & x = x^2 = 16^2 \times 16 = 21 \times 16 = 7 \bmod 47 \\ e_1 = 0 & x = x^2 = 7^2 = 2 \bmod 47 \\ e_0 = 1 & x = x^2 \times 16 = 2^2 \times 16 = 17 \bmod 47 \end{array}$$

Finalement, on a bien $16^{13} = 17 \bmod 47$.

3. (**Méthode ρ de Pollard – 11 points**)
On s'intéresse à présent à un autre algorithme permettant également de résoudre le problème du logarithme discret. Pour cela, on se place dans un sous-groupe $\langle h \rangle$ d'ordre q de $G = (\mathbb{Z}/p\mathbb{Z})^\times$, où p et q sont premiers.
Soit n un élément de $\langle h \rangle$, on définit l'application $f : \langle h \rangle \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \langle h \rangle \times \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ par :

$$f((x,a,b)) = \begin{cases} (hx, a+1, b) & \text{si } x = 0 \bmod 3 \\ (nx, a, b+1) & \text{si } x = 1 \bmod 3 \\ (x^2, 2a, 2b) & \text{si } x = 2 \bmod 3 \end{cases}$$

On construit la suite

$$\begin{cases} (x_0, a_0, b_0) = (1, 0, 0) \\ (x_{i+1}, a_{i+1}, b_{i+1}) = f((x_i, a_i, b_i)) \end{cases}$$

(a) (**Cycle – 1 point**) Sans effectuer de calcul expliquez pourquoi la suite $(x_i)_{i\in\mathbb{N}}$ possède un cycle.

Solution :
Les termes de la suite $(x_i)_{i\in\mathbb{N}}$, appartiennent à $\langle h \rangle$ qui est un sous-groupe d'ordre q. Le nombre de valeurs possibles pour les éléments de la suite étant majoré par q, la suite $(x_i)_{i\in\mathbb{N}}$ possède donc un cycle.

(b) (**Relation dans le triplet – 2 points**) Montrez que pour tout i, $x_i = h^{a_i} n^{b_i}$.

Solution :

Montrons par récurrence que pour tout i, $x_i = h^{a_i} n^{b_i}$.
Cas de base pour $i = 0$ on a, $x_0 = 1 = h^{a_0} n^{b_0}$.
Hérédité On suppose $x_i = h^{a_i} n^{b_i}$.
Si $x_i = 0 \bmod 3$, on a $(x_{i+1}, a_{i+1}, b_{i+1}) = (hx_i, a_i + 1, b_i)$. Donc

$$h^{a_{i+1}} n^{b_{i+1}} = hh^{a_i} n^{b_i} = hx_i = x_{i+1}$$

Si $x_i = 1 \bmod 3$, on a $(x_{i+1}, a_{i+1}, b_{i+1}) = (nx_i, a_i, b_i + 1)$. Donc

$$h^{a_{i+1}} n^{b_{i+1}} = nh^{a_i} n^{b_i} = nx_i = x_{i+1}$$

Si $x_i = 2 \bmod 3$, on a $(x_{i+1}, a_{i+1}, b_{i+1}) = (x_i^2, 2a_i, 2b_i)$. Donc

$$h^{a_{i+1}} n^{b_{i+1}} = (h^{a_i})^2 \left(n^{b_i}\right)^2 = x_i^2 = x_{i+1}$$

(c) **(Principe de résolution du DLP – 1,5 point)** Montrez que $c = (a_i - a_j)(b_j - b_i)^{-1} \bmod q$ donne le logarithme discret de n en base h, lorsque $x_j = x_i$, et $b_j - b_i$ est inversible modulo q.

Solution :
Si $x_j = x_i$, on a $h^{a_i} n^{b_i} = h^{a_j} n^{b_j}$.
Comme n est un élément de $\langle h \rangle$, il existe c tel que $n = h^c$. On a alors :

$$h^{a_i + c \cdot a_j} = n^{b_i + c \cdot b_j}.$$

Or $\langle h \rangle$ est d'ordre q donc : $a_i + c \cdot a_j = b_i + c \cdot b_j \bmod q$.
Puisque $b_j - b_i$ est inversible modulo q par hypothèse , on a bien $c = (a_i - a_j)(b_j - b_i)^{-1} \bmod q$.

(d) **(Cycle à exploiter – 1,5 point)** Justifiez qu'il existe un entier i tel que $x_i = x_{2i}$.

Solution :
Soit μ l'indice de premier élément du cycle et λ la période . Donc les $x_0, \ldots, x_{\mu+\lambda-1}$ sont tous distincts et pour tout $i \geq \mu$, on a $x_{i+\lambda} = x_i$ et par conséquent $x_{i+k\lambda} = x_i$ pour tout $k \geq 1$.
Soit $\ell \geq 1$ le plus petit entier tel que $\ell\lambda \geq \mu$, $x_{\ell\lambda+k\lambda} = x_{k\lambda}$ pour tout k. En particulier pour $k = \ell$, on obtient $x_{2\ell} = x_\ell$.

(e) **(Application – 3 points)** Mettez alors en application cet algorithme pour retrouver le logarithme discret de 17 en base 16.

Solution :
Ici $h = 16$, $n = 17$ et $q = 23$. On va dérouler les valeurs successives du triplet (x_i, a_i, b_i) à partir de $(x_0, a_0, b_0) = (1, 0, 0)$, jusqu'à trouver i tel que $x_i = x_{2i}$.

i	x_i	a_i	b_i	$x_i \bmod 3$
0	1	0	0	1
1	17	0	1	2
2	7	0	2	1
3	25	0	3	1
4	2	0	4	2
5	4	0	8	1
6	21	0	9	0
7	7	1	9	1
8	25	1	10	1
9	2	1	11	2
10	4	2	22	

On a une collision : $x_5 = x_{10}$.
De plus, $(b_{10} - b_5) = 22 - 8 = 14$ est inversible modulo 23, et son inverse est 5 puisque $5 \times 14 - 3 \times 23 = 1$.
Donc le logarithme discret de 17 en base 16 est donné par :

$$c = (a_5 - a_{10})(b_{10} - b_5)^{-1} = -2 \times 5 = 13 \bmod 23.$$

(f) **(Complexité – 2 points)** On suppose que la fonction f est suffisamment aléatoire pour trouver un cycle en $\mathcal{O}(\sqrt{q})$ itérations. Quelle est alors la complexité en temps de cet algorithme.

On calcule en parallèle les deux suites $(x_i)_{i\in\mathbb{N}}$ et $(x_{2i})_{i\in\mathbb{N}}$, jusqu'à trouver une collision. Combien d'éléments de $\langle h\rangle$ devez-vous stocker alors.

Comparez les complexités en temps et en espace de cet algorithme avec celles de l'algorithme Baby-Step-Giant-Step.

Solution :

L'algorithme présenté ici est l'algorithme ρ de Pollard.

Puisque la fonction f est suffisamment aléatoire pour trouver un cycle en $\mathcal{O}(\sqrt{q})$ itérations on a une complexité en temps en $\mathcal{O}(\sqrt{q})$, c'est-à-dire la complexité optimale en temps annoncée par le théorème de Shoup.

Si on calcule $(x_{i+1}, a_{i+1}, b_{i+1}) = f(x_i, a_i, b_i)$ et $(x_{2i+2}, a_{2i+2}, b_{2i+2}) = f(f(x_{2i}, a_{2i}, b_{2i}))$ à partir de (x_0, a_0, b_0), il suffit de garder les deux triplets de l'étape précédente pour passer à l'étape suivante et effectuer la comparaison, on a donc un nombre d'éléments de $\langle h\rangle$ constant à utiliser et une complexité en espace en $\mathcal{O}(1)$.

BSGS a une complexité en temps et en mémoire de $\mathcal{O}(\sqrt{q})$, alors que ρ de Pollard a une complexité en temps de $\mathcal{O}(\sqrt{q})$ et une complexité en mémoire de $\mathcal{O}(1)$, cet algorithme est plus utilisé en pratique tout simplement parce qu'il permet de traiter des DLP dans des groupes beaucoup plus gros là où Baby-Step-Giant-Step a rendu les armes depuis longtemps faute de mémoire pour stocker la table nécessaire à la recherche de collision.