Université Paris 8 Année 2021–2022

Master Mathématiques et applications

Algorithmes arithmétiques II — Devoir à la maison

à rendre pour le mercredi 17 novembre 2021

Documents à fournir. Vous devez rendre :

1. Par email **ou** en cours : vos réponses à la partie théorique (partie 1).
2. Par email **nécessairement** : une archive (format `.zip`) contenant vos programmes (partie 2).
3. Par email **nécessairement** : un rapport contenant vos réponses à la partie analyse (partie 3). Ce rapport sera obligatoirement au format `.pdf`.

L'email sera adressé à `julien.lavauzelle@univ-paris8.fr`.

Barème. Les trois parties ont sensiblement le même poids dans la note finale. Le **soin** et les **justifications** apportées à vos réponses seront évaluées. On notera également le soin apporté à l'implantation (commentaires, lisibilité, etc.).

Remarques. Lors de vos implantations, vous allez manier de grands entiers. Certains langages comme `python` les supportent nativement. Pour d'autres, comme `C`, il faut importer une bibliothèque externe (GMP pour `C`, par exemple).

Ressources. Comme aide à la programmation, on donnera à l'adresse

`https://www.math.univ-paris13.fr/~lavauzelle/teaching/2021-22/docs/AA/dm/docs.html`

des fichiers auxiliaires contenant des listes de premiers p de taille particulière, ou des listes des nombres premiers p tels que $p+1$ est B-superfriable pour des bornes B particulières.

La méthode $p+1$ de Williams pour la factorisation

Dans ce sujet, on considère la méthode de factorisation dite « $p+1$ » de Williams. Cette méthode permet de trouver des facteurs p d'un entier N à factoriser, tels que $p+1$ a une forme particulière, dite *superfriable*, que l'on définira plus tard.

1) Partie théorique

On suppose dans cette partie de l'énoncé que p est un diviseur premier impair de N, le nombre à factoriser. Pour $D \in \mathbb{Z}$, on note

$$\mathcal{A}^D := \{(x,y) \in (\mathbb{Z}/N\mathbb{Z})^2 \mid x^2 - y^2 D \equiv 1 \mod N\} \subseteq (\mathbb{Z}/N\mathbb{Z})^2 .$$

Puis, on note $\mathcal{A}_p^D$ la réduction de cet ensemble modulo p :

$$\mathcal{A}_p^D := \{(x \mod p, y \mod p) \mid (x,y) \in \mathcal{A}^D\} \subseteq (\mathbb{Z}/p\mathbb{Z})^2 .$$

Question 1.– Calculer $\mathcal{A}^D$ et $\mathcal{A}_p^D$ pour $p = 5$, $N = 15$ et $D = 2$. Expliquer votre méthode.

Lorsque D est un non-carré modulo p, on rappelle que $\mathbb{F}_p[X]/(X^2 - D)$ est un corps que l'on note $\mathbb{F}_p(\sqrt{D})$, où $\sqrt{D}$ représente la classe de X dans $\mathbb{F}_p[X]/(X^2 - D)$. On note enfin ψ l'isomorphisme d'espace vectoriel :

$$\begin{array}{rccc} \psi : & (\mathbb{Z}/p\mathbb{Z})^2 & \to & \mathbb{F}_p(\sqrt{D}) \\ & (x, y) & \mapsto & x + y\sqrt{D} \end{array}$$

Question 2.– Démontrer que $\psi(\mathcal{A}_p^D)$ est un sous-groupe multiplicatif de $\mathbb{F}_p(\sqrt{D})$, d'ordre $p + 1$.

On note maintenant $\mathcal{U} \coloneqq \psi(\mathcal{A}_p^D)$. Pour $u = x + y\sqrt{D} \in \mathcal{U}$, on note

$$x(u) \coloneqq x \quad \text{et } y(u) \coloneqq y\,.$$

Question 3.– Soit $u \in \mathcal{U}$. Calculer u^2 puis exprimer $x(u^2)$ en fonction de $x(u)$.

Question 4.– Soit $u \in \mathcal{U}$. Démontrer que pour tout $n \geq 1$, on a :

$$\begin{aligned} x(u^{2n}) &\equiv 2x(u^n)^2 - 1 \mod p, \\ x(u^{2n+1}) &\equiv x(u^n)x(u^{n+1}) - x(u) \mod p. \end{aligned}$$

Pour ce faire, on pourra s'aider du calcul de $y(u^{2n})$.

Soit maintenant $a \in \mathbb{Z}/N\mathbb{Z}$ et $(a_n)_{n\geq 1}$ la suite dans $\mathbb{Z}/N\mathbb{Z}$ définie par $a_1 = a$ et pour tout $n \geq 1$:

$$\begin{aligned} a_{2n} &\equiv 2a_n^2 - 1 \mod N, \\ a_{2n+1} &\equiv a_n a_{n+1} - a \mod N. \end{aligned}$$

Question 5.– Supposons qu'il existe $b \in \mathbb{Z}/N\mathbb{Z}$ et D non-carré modulo p tel que l'élément $u = a + b\sqrt{D} \in \mathcal{U}$ existe et vérifie

$$a_n = x(u^n), \quad \forall n \geq 1\,.$$

Démontrer que si $M \geq 1$ est un multiple de $p + 1$, alors p divise $a_M - 1$.

Question 6.– **[BONUS]** Estimer la probabilité qu'en tirant a aléatoirement, il existe $b \in \mathbb{Z}/N\mathbb{Z}$ et D non-carré modulo p tel que l'élément $a + b\sqrt{D} \in \mathcal{U}$.

2) Partie implantation

De la partie précédente, on peut déduire une méthode générale pour trouver un diviseur p de N dans le cas où $p + 1$ est *superfriable*. Voici une définition de cette notion.

Définition. Soit $B \geq 2$. On dit qu'un entier $x \geq 2$ est B-superfriable si tout entier de la forme c^e qui divise x (avec c un nombre premier et $e \geq 1$) est plus petit ou égal à B.

Exemple. L'entier $16 = 2^4$ n'est pas 9-superfriable, mais l'entier $72 = 2^3 \times 3^2$ l'est.

Question 7.– Implanter une fonction `is_powersmooth(x, B)` qui prend en entrée deux entiers x et B, et qui teste si l'entier x est B-superfriable.

Question 8.– Implanter une fonction `compute_bound(B)` qui calcule le plus efficacement possible la valeur $M = \text{ppcm}(2, \ldots, B)$. Pour vous aider, vous pourrez trouver dans le fichier annexe `liste_petits_premiers.txt` la liste de tous les nombres premiers plus petits que 10 000.

La méthode « $p+1$ » de Williams repose sur le calcul d'une suite $(x_n)_{n\geq 1}$ définie par les relations de récurrence suivantes :

$$\begin{cases} x_{2n} & = 2x_n^2 - 1 \mod N \\ x_{2n+1} & = 2x_n x_{n+1} - x_1 \mod N \end{cases} \quad \text{pour } n \geq 1$$

Ainsi, si z_n désigne le couple (x_n, x_{n+1}), on peut déduire (z_{2n}, z_{2n+1}) de x_1 et z_n. Cela signifie qu'on peut **adapter la méthode d'exponentiation binaire** au calcul de x_n.

Exemple. Si $M = 18$, l'écriture de M en base de M est $(10010)_2$. Les troncations de cette écriture forment les entiers $1 = (1)_2$, $2 = (10)_2$, $4 = (100)_2$, $9 = (1001)_2$ et $18 = (10010)_2$. Donc, on va successivement calculer x_1, x_2, x_4, x_9 et x_{18}.

Il est facile de passer de x_1 à x_2 et de x_2 à x_4, par l'équation $x_{2n} = 2x_n^2 - 1 \mod N$ donnée plus haut. En revanche, pour calculer x_9, on a besoin à la fois de x_4 et de x_5. Dans l'algorithme de calcul de la suite (x_n), il faudra donc maintenir la connaissance de $z_n = (x_n, x_{n+1})$.

Pour $x_1 = 2$, on doit obtenir les valeurs suivantes

n	x_n	x_{n+1}
1	2	7
2	7	26
4	97	362
9	70226	262087
18	9863382151	–

Question 9.– Implanter une fonction `calcule_x(x1, M, N)` qui prend en entrée un élément $x_1 \in \{1, \ldots, N-1\}$ et qui calcule la valeur de $x_M \mod N$ par une méthode analogue à l'exponentiation binaire.

On s'intéresse maintenant à l'Algorithme 1, dit méthode de factorisation « $p+1$ » de Williams.

Algorithme 1 : Méthode $p+1$ de Williams

Entrée : un entier $B \geq 3$ et un entier composé impair $N \geq 15$ possédant un facteur premier impair p tel que $p+1$ est B-superfriable
Sortie : un diviseur d de N

Initialiser $d \leftarrow N$.
Tant que $d = N$ **faire**
  Calculer $M \leftarrow \text{ppcm}\{2, \ldots, B\}$.
  Tirer aléatoirement x_1 dans $\{1, \ldots, N-1\}$.
  Calculer $d \leftarrow \text{pgcd}(x_1, N)$.
  Si $d \neq 1$
    Retourner d
  Calculer $x_M \leftarrow$ `calcule_x`(x_1, M, N).
  Calculer $d \leftarrow \text{pgcd}(x_M - 1, N)$.
Retourner d.

Question 10.– Implanter un algorithme qui calcule de pgcd de deux entiers. Cet algorithme devra supporter des entrées de taille importante (plusieurs centaines de chiffres).

Question 11.– Implanter l'Algorithme 1. Tester votre implantation avec certaines valeurs données en annexe.

3) Partie analyse

Question 12.– En utilisant la partie théorique, expliquer pourquoi l'Algorithme 1 calcule bien un diviseur p de N tel que $p+1$ est B-superfriable. La qualité de l'argumentation sera évaluée.

Question 13.– Donner une estimation de la complexité de la méthode $p+1$ de Williams en fonction de B et N. La qualité de l'argumentation sera évaluée.

Question 14.– Calculer **expérimentalement** la complexité de la méthode $p+1$ de Williams. Commenter les résultats obtenus (même s'ils ne sont pas convaincants).

Pour cela, on tracera des graphes du temps de calcul (ou du nombre d'opérations comptées) en fonction de N et/ou de la borne de friabilité B choisie. On pourra également s'aider des entiers donnés dans les fichiers auxiliaires, ou implémenter son propre générateur d'entiers composés (de taille et forme particulière).

Rappelons enfin que :

— pour vérifier qu'une fonction $f(x)$ se comporte comme un polynôme en x, c'est-à-dire $\beta x^\alpha + o(x^\alpha)$, on trace $\log(f(x))$ en fonction de $\log(x)$,

— pour vérifier qu'une fonction $g(x)$ se comporte comme une exponen.tielle en x, c'est-à-dire $(\delta + o(1))\gamma^x$, on trace $\log(f(x))$ en fonction de x

Annexe

Pour vous aider à tester vos programmes, voici ci-dessous quelques valeurs de N, p et q qui doivent mener à une factorisation quasi-immédiate de N.

$N = pq$	facteurs p, q tels que $p+1$ est B-superfriable		B
8435923	2243	3761	20
433214017981	526679	822539	20
668877085585453	20540519	32563787	20
29601945037090540097	4302501839	6880170223	60
2202930212280802191504287	1099511799979	2003553042653	150
1434606164092147949243688378019	1125899906956109	1274186235586991	400
168373945511479629236199196552692028 3	1152921504620379229	1460411180090875927	1000

TABLE 1 – Exemples de factorisations « faciles » effectuées par l'algorithme $p+1$ de Williams.

Quelques exemples de taille plus conséquente, mais que l'algorithme $p+1$ règle toujours très rapidement (< 1 seconde si l'implantation est bonne) :

- $N = 10562256276314677189367086699051860083179133005474255536770513713410152272327$
  $p = 80694878738093144866358575156611462449$
  $q = 13089128382726742425590053490410316402 3$
  où $p+1$ est 100-superfriable.

- $N = 62168737006042231928510814222178349101156309737965504752177410010962889443724567730 7...$
  $...16203710521739874848738315366444050483000922241076559240303096972312 29$
  $p = 67370446184902616587480990283695167230411304043318606176733774562163367914599$
  $q = 92278945036843081009237393938740885814972681387747472129904570310056540085371$
  où $p+1$ est 200-superfriable.

- $N = 75335665860992821169105470726766540912231610419365378084109059906708119860068536707...$
  $...23673944387751725757220297910047314599198514346142077537459486353899376688526034522045 70...$
  $...46051949701511230965455078708866820795617315314721680376760845 13$
  $p = 25859751346998904721315154541135445772069592027081540466915141922132646156251 8...$
  $...12286986260376922317805736767051853068 79$
  $q = 29132401487586512476354570916689568474194168376146508296871732993914796687724 5...$
  $...60484143488960272064176130757946206028 47$
  où $p+1$ est 300-superfriable.