Université de Bordeaux
Mathématiques

Calcul formel – Master
2025–2026

FEUILLE D'EXERCICES n° 8

On rappelle la notion de nombre de Carmichael, et le critère pour les détecter. Sa preuve fait l'objet de l'exercice 4.

Définition 1. On appelle *nombre de Carmichael* tout nombre composé n vérifiant

$$a^{n-1} \equiv 1 \mod n \quad \text{pour tout } a \text{ premier à } n.$$

On admet le théorème suivant qui donne un critère pour déterminer si un nombre est de Carmichael.

Théorème 2 (Critère de Korselt)**.** *Un entier est un nombre de Carmichael si et seulement s'il est composé, sans facteur carré, et si pour tout premier p divisant n, l'entier $p-1$ divise $n-1$.*

Exercice 1 – [Test de Rabin-Miller]

On s'intéresse ici au test de Rabin-Miller, qui améliore le test de non primalité de Fermat vu au TD précédent.

On décompose $n-1$ sous la forme $n-1 = 2^e q$ avec q impair. Comme pour le test de Fermat, on prend des entiers a au hasard entre 2 et $n-2$. Si n est premier, on a alors deux cas :

(i) Soit $a^q \equiv 1 \mod n$,

(ii) Soit il existe i vérifiant $0 \leq i < e$ et $a^{2^i q} \equiv -1 \mod n$

Dès qu'un entier a ne vérifie ni (i) ni (ii), on sait que n est composé.

Programmez le test de Rabin-Miller et comparer les résultats obtenus avec ceux que donnaient le test de Fermat itéré du TD précédent.

Exercice 2 – [Factorisation]

Soit $n = 7639911$. On se propose de factoriser n via une méthode de crible *à la* Dixon. Pour cela on choisit une base de facteurs premiers raisonnable :

$$\mathcal{F} = \{2, 3, 5, 7, 11\}.$$

1) En partant de $\lceil \sqrt{n} \rceil$, collectez des x tels que $v = x^2 \mod n$ se décompose sur $\mathcal{F}$. Pensez à stocker les factorisations.

2) Pour chacune de ces relations, construisez le vecteur des exposants correspondants. Par exemple, si $v = 1508548^2 \mod n = 903168 = 2^{11} \times 3^2 \times 7^2$, alors le vecteur correspondant est

$$(11, 2, 0, 2, 0)$$

ou encore après réduction modulo 2 :

$$(1, 0, 0, 0, 0).$$

3) Construisez la matrice formée par les vecteurs précédemment construits.

4) En calculant un élément non nul du noyau à gauche, déterminez une relation de la forme

$$x^2 = y^2 \mod n$$

Si vous ne trouvez aucun vecteur non nul c'est que vos lignes sont linéairement indépendantes, donc que vous n'avez pas trouvé assez de relations.

5) En déduire une factorisation de n.

Exercice 3 – [Construction de grands nombres premiers]

On rappelle que n est premier si et seulement si $(\mathbb{Z}/n\mathbb{Z})^\times$ est un groupe cyclique de cardinal $n-1$. Ainsi, montrer que n est premier est équivalent à trouver un générateur de ce groupe, *i.e.* un élément d'ordre $n-1$. Un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$ est aussi appelé élément primitif modulo n. On va utiliser ce critère pour prouver la primalité d'un entier n (en renvoyant un *certificat* de primalité). On suppose que l'on connaît la factorisation de $n-1$, ou du moins la liste des facteurs premiers de $n-1$.

Algorithme 1. Algorithme de Lucas-Lehmer

Entrées: n : entier probablement non premier, $p_1, \ldots, p_r$ diviseurs premiers de $n-1$
Sorties: `Vrai` ou `Faux` ou `Echec`

$a \leftarrow \{1, \ldots, n-1\}$
`Si` $a^{n-1} \not\equiv 1 \mod n$:
    `Retourner Faux`
`Pour i de 1 à r:`
    `Si` $a^{(n-1)/p_i} \equiv 1 \mod n$:
        `Echec`
`Retourner Vrai et le certificat de primalité` a

---

1) En admettant pour l'instant le résultat ci-dessous, prouvez la correction de cet algorithme, c'est-à-dire que s'il n'échoue pas et termine, alors n est bien premier et a est bien une preuve de primalité (qu'on appelle certificat).

Soit G un groupe et soit $x \in G$. Montrez que x est d'ordre d si et seulement si les deux conditions suivantes sont vérifiées.

(1) $x^d = 1$

(2) Pour tout diviseur premier ℓ de d, on a $x^{d/\ell} \neq 1$.

2) Implémentez le test de Lucas-Lehmer.

3) On considère $n = 2.3.5.7.11^2.13.17.19+1 = 106696591$. Utilisez le test de Lucas-Lehmer pour montrer simultanément que n est premier et que 7 est un élément primitif modulo n.

4) Cherchez un nombre premier p de la forme

$$p = 2^{e_2}.3^{e_3}.5^{e_5}.7^{e_7}.11^{e_{11}}.13^{e_{13}}.17^{e_{17}}.n + 1$$

avec $e_i = 1$ ou $e_i = 2$. On pourra tester si p est un candidat à être premier grâce à l'égalité $2^{p-1} = 1 \bmod p$.

Attention, ne pas utiliser la commande : `2^B %p` celle-ci calcule d'abord 2^B, puis réduit modulo p. Déclarez d'abord l'anneau $\mathbb{Z}/p\mathbb{Z}$ par la commande : `R=IntegerModRing(p)` après quoi vous pouvez calculer 2^B dans $\mathbb{Z}/p\mathbb{Z}$ par `R(2)^B` .

5) Généralisez la stratégie ci-dessus pour fabriquer des nombres premiers de plus en plus grands. Créer une première liste L de petits nombres premiers (incluant 2 !), puis une deuxième liste P comportant des nombres premiers de plus en plus grands que vous aurez fabriqués petit à petit. Considérez l'entier impair :

$$N = 1 + \prod_{p \in L} p^{e_p} \prod_{p \in P} p$$

où l'exposant e_p vaut 1 ou 2, puis testez s'il est premier ou non. La commande `Subsets(L)` peut vous être utile : elle crée la liste de toutes les parties de L.

Si vous évitez de mettre $3, 5, 7$ dans la liste L, vous aurez, lorsque N est premier, une probabilité relativement proche de $1/2$ qu'un entier pris au hasard modulo N soit primitif et fournisse donc un témoin de primalité (pourquoi ?). La commande `randint(a,b)` vous fournit un entier choisi aléatoirement et uniformément entre a et b.

La probabilité que votre nombre N soit premier peut être évaluée empiriquement par le théorème des nombres premiers qui dit que le nombre de nombres premiers $\leqslant n$ est très proche de $n/\ln n$.

Fabriquez ainsi un nombre premier d'au moins mille chiffres décimaux.

6) Prouvez le résultat admis au début.

Exercice 4 – [Critère de Korselt]

1) Soit p un nombre premier et m un nombre naturel non nul. Soit $n = p^2m$. Montrer que

$$(1 + pm)^{n-1} \not\equiv 1 \mod n.$$

En déduire que tout nombre de Carmichael est sans facteur carré.

2) On rappelle que si p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique. Soit n un entier sans facteur carré.

a) On suppose que pour tout nombre premier p divisant n, l'entier $p-1$ divise $n-1$. Soit a un entier premier à n. Montrer que

$$a^{n-1} \equiv 1 \mod n.$$

b) On suppose que n est de Carmichael. Soit p un diviseur premier de n. Soit g un entier dont la classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^*$. Montrer qu'il existe un entier a premier à n tel que $a \equiv g \mod p$. En déduire que $p-1$ divise $n-1$.

3) En déduire une preuve du Critère de Korselt.

4) Montrer que tout nombre de Carmichael est impair et produit d'au moins trois nombres premiers distincts.

5) Vérifier que $561 = 3.11.17$, $1729 = 7.13.19$ et $29341 = 13.37.61$ sont des nombres de Carmichael.

6) Supposons que p, $2p-1$ et $3p-2$ soient tous trois premiers. Montrer que $p = 3$ ou $p \equiv 1 \mod 6$, et que dans ce dernier cas $p(2p-1)(3p-2)$ est un nombre de Carmichael.

7) Montrer que la Définition 1 est équivalente à la suivante.

Définition 3. On appelle *nombre de Carmichael* tout nombre composé n vérifiant $a^n \equiv a \pmod n$ pour tout a.