Université de Bordeaux
Mathématiques

Algèbre et calcul formel – Master
Année 2023–2024

FEUILLE D'EXERCICES n° 8

Travail sur machine

Exercice 1 – [Critère de Korselt pour les nombres de Carmichael]

Dans cet exercice on démontre le critère de Korselt :

Théorème 1 (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 $n-1$.*

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. 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) Soit n un entier composé, sans facteur carré, et tel que pour tout premier p divisant n, l'entier $p-1$ divise $n-1$. Montrez que n est un nombre de Carmichael.

4) Déduire des questions précédentes le théorème annoncé.

Exercice 2 – [Encore les nombres de Carmichael]

1) 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.

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

3) On suppose que n est de Carmichael. On applique le test de non-primalité de Rabin-Miller à n et on suppose qu'il est positif, i.e. qu'on dispose de $a \in \mathbb{Z}/n\mathbb{Z}$ qui est témoin de non-primalité. Montrer qu'on peut facilement en déduire un facteur non trivial de n.

Exercice 3 – [Construction de grands nombres premiers]

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

2) À l'aide du théorème de Lucas-Lehmer, chercher 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` .

3) Généraliser 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.