Université Paris 7 — Année 2008/09
Licence 2 - MI4 — Groupes & Arithmétique

Feuille d'exercices n°5

Nombres pseudo-premiers
Nombres de Carmichael
Symboles de Legendre et Jacobi
Cryptographie

Exercice 1. On considère un entier $n > 1$ non premier. On note d le pgcd de $n-1$ et $\varphi(n)$.

Montrer que n est pseudo-premier de base a si et seulement si a est premier avec n et d'ordre divisant d dans $\mathcal{U}(\mathbb{Z}/n\,\mathbb{Z})$.

Exercice 2. Nombres de Poulet.

Les nombres de Poulet sont les nombres pseudo-premiers de base 2.

a) Déterminer l'ordre de 2 dans les groupes $(\mathbb{Z}/11\ \mathbb{Z})^\times$, $(\mathbb{Z}/31\ \mathbb{Z})^\times$ et $(\mathbb{Z}/341\ \mathbb{Z})^\times$. En déduire que 341 est un nombre de Poulet.

b) Soit n un nombre de Poulet et $n' = 2^n - 1$. Montrer que $n | n' - 1$.
En utilisant que $a|b \Rightarrow 2^a - 1 | 2^b - 1$, montrer que n' est un nombre de Poulet.

c) Les nombres de Poulet sont-ils en nombre fini ou infini ?

d) Montrer qu'un nombre de Mersenne $M_p = 2^p - 1$ non premier est un nombre de Poulet.

e) Montrer qu'un nombre de Fermat $F_n = 2^{2^n} + 1$ non premier est un nombre de Poulet.

Exercice 3. Déterminer $3^{10} \bmod 31$.

L'entier 341 est-il pseudo-premier de base 3 ? Est-ce un nombre de Carmichael ?

Exercice 4. Pour quelles bases 15 est-il pseudo-premier ?

Exercice 5. Proposer un algorithme qui fournit, pour un entier n non premier donné, la liste des dases pour lesquelles n est pseudo-premier.

Exercice 6. Rappeler les caractérisations des nombres de Carmichael.

Exercice 7. Exemples de nombres de Carmichael.

a) Vérifier que les nombres suivants sont de Carmichael : 1729, 6601 et 278545.

b) Montrer que si $6\,m+1$, $12\,m+1$ et $18\,m+1$ sont tous trois premiers, alors leur produit $n = (6\,m+1)\,(12\,m+1)\,(18\,m+1)$ est un nombre de Carmichael.

Exercice 8. Montrer par l'absurde que tout nombre de Carmichael a au moins trois facteurs premiers.

Exercice 9. Calculer les symboles de Legendre suivants : $\left(\frac{5}{17}\right)$, $\left(\frac{28}{11}\right)$, $\left(\frac{2009}{17}\right)$, $\left(\frac{10}{89}\right)$, $\left(\frac{-42}{97}\right)$.

Exercice 10. Soit $p \geqslant 3$ un nombre premier.

a) Montrer que le nombre de racines carrées d'un entier $\alpha \in \mathbb{Z}$ dans $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$ est $1 + \left(\frac{\alpha}{p}\right)$.

b) Soient a, b, $c \in \mathbb{Z}$ avec $p \nmid a$. Montrer que l'équation $a\,x^2 + b\,x + c = 0$ possède $1 + \left(\frac{\Delta}{p}\right)$ solutions dans $\mathbb{F}_p$, où $\Delta = b^2 - 4\,a\,c$.

c) Déterminer le nombre de solutions dans $\mathbb{Z}/83\,\mathbb{Z}$ des équations suivantes : $x^2 + 1 = 0$, $x^2 + x + 1 = 0$, $x^2 - 4\,x + 13 = 0$, $x^2 + x + 21 = 0$.

Exercice 11. Soient n_1 et n_2 deux entiers premiers entre eux.

Montrer qu'un entier a est un résidu quadratique modulo $n = n_1\, n_2$ si et seulement si a est un résidu quadratique modulo n_1 et modulo n_2.

Exercice 12. Résoudre l'équation $x^2 = 1$ dans $\mathbb{Z}/15\,\mathbb{Z}$, $\mathbb{Z}/21\,\mathbb{Z}$ et $\mathbb{Z}/60\,\mathbb{Z}$.

Exercice 13. Proposer un algorithme qui permet de calculer les symboles de Legendre.

Exercice 14. Soit $p \geqslant 3$ un nombre premier.

À quelle condition -1 est-il un résidu quadratique modulo p ?

On suppose $p \equiv 1 \bmod 4$. À l'aide du théorème de Wilson, montrer que $(\frac{p-1}{2})!$ est une racine carrée de -1 dans $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$.

Exercice 15. Soit $p \geqslant 3$ un nombre premier et $a \in \mathbb{Z}$ un entier premier à p. On souhaite déterminer les racines carrées de a dans $\mathbb{F}_p = \mathbb{Z}/p\,\mathbb{Z}$.

a) Montrer que si $p \equiv 3 \bmod 4$, les racines carrées de a dans $\mathbb{F}_p$ sont $\pm a^{\frac{p-1}{4}} \bmod p$.

b) On suppose que $p \equiv 5 \bmod 8$. Montrer que $a^{\frac{p-1}{4}} \equiv \pm 1 \bmod p$.

Si $\varepsilon = 1$, montrer que les racines carrées de a dans $\mathbb{F}_p$ sont $\pm a^{\frac{p+3}{8}} \bmod p$.

Si $\varepsilon = -1$, déterminer ces racines carrées en utilisant l'exercice précédent.

Exercice 16. On utilise l'algorithme suivant pour crypter un mot : on remplace chaque lettre par sa position dans l'alphabet (a par 1, b par 2, ...), on multiplie cette position par 7 puis on prend le reste de la division euclidienne par 26.

a) Coder le mot "JAZZ".

b) Expliquer pourquoi deux mots différents seront cryptés différemment.

c) Expliquer comme s'effectue le décryptage.

Exercice 17. On considère le système cryptographique RSA.

Calculer les clefs secrètes associées aux clefs publiques $(77, 7)$, $(77, 13)$ et $(69, 3)$.

Exercice 18. On considère le système cryptographie El Gamal.

Les triplets (p, g, A) suivants sont-ils des clés publiques : $(29, 2, 25)$, $(29, 5, 2)$?

Alice calcule $A = 2^6 \bmod 29$ et choisit la clé publique $(29,\ 2,\ A)$. Elle reçoit les messages cryptés (B, m') suivants : $(3, 4)$, $(4, 14)$, $(5, 11)$. Effectuez leur décryptage pour Alice.