Examen du 15 janvier 2021, durée 2 heures.
Calculatrice autorisée, feuille A4 recto-verso manuscrite autorisée.

1. Puissances modulo un nombre premier (10 points)

Dans cet exercice on fixe un entier $t \geq 1$ et on recherche des nombres premiers p de la forme $p = k2^t + 1$ et des entiers z vérifiant

$$z^{(2^{t-1})} \equiv -1 \ [p] \quad (*)$$

Les questions 1 à 4 présentent un exemple lorsque $t = 12$ et $k = 3$ donc $p = 3 \times 2^{12} + 1 = 12289$, on y recherche z tel que

$$z^{(2^{11})} \equiv -1 \ [p] \quad (**)$$

Les questions 6(a) et 6(b) sont indépendante des questions 1 à 5.

(1) Expliquer comment on peut vérifier que $p = 12289$ est premier. Attention, on ne demande pas de faire tous les calculs nécessaires, et on admettra dans la suite sans avoir fait toutes les vérifications que 12289 est premier.

(2) Soit a un élément inversible de $\mathbb{Z}/p\mathbb{Z}$ pour $p = 12289$. Montrer que l'ordre de a dans $(\mathbb{Z}/p\mathbb{Z})^*$ est soit 2^n soit 3×2^n pour $n \geq 0$. Quelle est la valeur maximale possible pour n ?

(3) Toujours pour $p = 12289$, on a effectué le calcul suivant :

$$11^{(2^{11})} \equiv 6241 \ [p]$$

(a) Expliquez comment on peut faire ce calcul efficacement (*mais ne faites pas les calculs vous-même*), et indiquez combien de divisions par p sont nécessaires.

(b) En déduire les valeurs de

$$11^{(2^{12})} \ [p], \quad 11^{(3\times 2^{11})} \ [p]$$

(c) $\overline{11}$ est-il un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$?

(4) Toujours pour $p = 12289$, déterminer un entier z tel que

$$z^{(2^{11})} \equiv -1 \ [p] \quad (**)$$

(5) Soit p un nombre premier. Montrer que si un couple (z, p) vérifie (*) alors p est de la forme

$$p = k2^t + 1, \quad \text{pour } k \in \mathbb{N}$$

Indication : calculer $z^{(2^t)} \ [p]$ et l'ordre de la classe de z dans $(\mathbb{Z}/p\mathbb{Z})^*$.

(6) On suppose qu'on dispose d'une commande `isprime(n)` qui renvoie un booléen vrai si n est un nombre premier.

(a) Écrire un algorithme `premiers(N,t)` renvoyant une liste de `N` nombres premiers p de la forme $k2^t + 1$.

(b) Modifier l'algorithme précédent en une fonction `premiers_fft(N,t)` pour trouver N couples (z, p) vérifiant (*).

(c) Peut-on améliorer l'algorithme de la question (b) si on dispose d'une commande `generateur(p)` renvoyant un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$?

Remarque : les couples d'entiers (z, p) vérifiant (*) sont très utiles pour implémenter des algorithmes de multiplication rapide de polynômes (par Fast Fourier Transform).

2. CRYPTAGE MATRICIEL À CLEF SECRÈTE (10 POINTS)

Pour coder des messages pouvant contenir des caractères de diverses langues, on représente chaque caractère par un entier sur 16 bits (codage UTF16 par exemple). On décide ensuite de crypter le message par blocs de 2 caractères, en multipliant chaque vecteur v des 2 entiers représentant un bloc par une matrice carrée A de taille 2 modulo un entier p qui sera supposé premier dans les questions 1 à 6. La matrice A est tenue secrète, c'est la clef secrète du système de cryptage.

(1) Dans quel intervalle se trouve un entier sur 16 bits ?
On suppose que p est un nombre premier qui permet de représenter de manière unique tous les entiers sur 16 bits par leur classe dans $\mathbb{Z}/p\mathbb{Z}$. Quel est le nombre minimal de bits de p ?

(2) On admettra que $p = 65537$ est bien premier. On pose :

$$p = 65537, \quad A = \begin{pmatrix} 263 & 4122 \\ 1 & 1799 \end{pmatrix}$$

Crypter le vecteur v correspondant aux deux caractères "intégrale double" et "intégrale triple" représentés respectivement par les entiers 8748 et 8749, i.e. calculer $w = Av$ modulo p

(3) Déterminer tous les vecteurs z à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ tels que $Az = Av$ modulo p pour $p = 65537$.
En déduire tous les vecteurs z à coefficients entiers qui vérifient $Az = Av$ modulo p.
Si on impose que les coordonnées de z sont dans l'intervalle du codage sur 16 bits, combien y-a-t-il de solutions ?

(4) Que se passerait-il si on avait choisi la même matrice mais $p = 6551$?

(5) Expliquer comment on peut décrypter, i.e. étant donné w quelconque, comment on trouve v tel que $Av = w$ modulo p.

(6) Quel est le nombre de matrices A possibles pour $p = 65537$? Cela vous parait-il suffisant pour résister à une attaque de la clef secrète A par force brute ? Peut-on imaginer un autre type d'attaque ? Comment pourrait-on renforcer la sécurité ?

(7) Dans cette question, on suppose que $p = 2^{16}$ et n'est donc pas premier. Peut-on appliquer l'algorithme du pivot de Gauss pour résoudre $Az = w = Av$ si on travaille modulo p bien que p ne soit alors pas premier ?
En est-il de même pour la matrice

$$p = 65536, \quad A = \begin{pmatrix} 262 & 4122 \\ 1 & 1799 \end{pmatrix}$$

(8) Quel(s) avantage(s) et inconvénient(s) y-a-t-il à travailler modulo 2^{16} par rapport à $p = 65537$?