Exercices d'entraînement

Exercice 1 : Montrez qu'un nombre est divisible par 11 si et seulement si la somme alternée de ses décimales est divisible par 11.

Exercice 2 : Quelles sont les racines carrées de 16 mod 35 ?

Exercice 3 : Quels sont les entiers x qui vérifient $6x = 9 \bmod 15$ et $10x = 4 \bmod 8$?

Exercice 4 : Donnez une description (en pseudo code) de l'algorithme d'Euclide étendu.

En utilisant l'algorithme d'Euclide étendu, montrer que 126 est premier à 137 et calculer l'inverse de 126 modulo 137.

Exercice 5 :

Donnez un générateur g de $(\mathbb{Z}/13\mathbb{Z})^*$.

Écrire la table des exponentielles et des logarithmes discrets en base g.

Exercice 6 :

Calculer le pgcd de 1339 et 689.

Quel est le cardinal de $(\mathbb{Z}/2678\mathbb{Z})^*$.

Quel est l'exposant de ce groupe ?

Exercice 7 :

Décrivez un protocole cryptographique reposant sur la difficulté de distinguer les carrés modulo un entier $n = pq$.

Illustrer ce protocole sur un exemple simple (avec un petit entier n).

Exercice 8 :

Donnez un entier x tel que le symbole de Jacobi $\left(\dfrac{x}{35}\right)$ soit 1 et x ne soit pas un carré modulo 35. Un tel x est appelé un faux carré.

Soient p et q deux entiers premiers impairs. On note $n = pq$. On suppose que l'on a un générateur aléatoire qui retourne une valeur dans $\{0, 1\}$ avec probabilité uniforme. On peut utiliser ce générateur plusieurs fois de suite. Les réponses sont alors deux à deux indépendantes.

Décrivez un algorithme pour choisir un élément aléatoire de $\mathbb{Z}/n\mathbb{Z}$ avec probabilité uniforme.

Même question avec $(\mathbb{Z}/n\mathbb{Z})^*$.

Même question avec l'ensemble des carrés dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Même question avec l'ensemble des faux carrés dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Vous justifierez soigneusement vos réponses.

Exercice 9 : Prouvez que 701 est premier.

Exercice 10 :

Le code ci-dessous est supposé trouver un facteur non-trivial de l'entier impair n.

```
puiss=Mod(random(n-3)+2,n);
k=1;
fac=1;
until(fac>1,k=k+1;puiss=puiss^k;fac=gcd(lift(puiss)-1,n));
print(fac);
```

Expliquez l'algorithme sous-jacent.

Donnez une estimation du temps de calcul.

Exercice 11 : Soit p un entier premier impair. Soit r un entier premier à p tel que $r \bmod p$ ne soit pas un carré dans $(\mathbb{Z}/p\mathbb{Z})^*$. On pose $R = \mathbb{F}_p[x]/(x^2 - r)$.

Montrez que R est un corps. Quel est sont cardinal ?

On note $\xi = x \bmod x^2 - r$. Montrez que ξ est racine du polynôme $x^2 - r$ dans R.

Montrez que ξ^p est aussi racine de ce polynôme. Montrez que $\xi^p = -\xi$.

Soit $\sigma : R \to R$ l'application qui envoie $a + b\xi$ sur $a - b\xi$. Montrez que

$$\sigma(uv) = \sigma(u)\sigma(v) \text{ et } \sigma(u+v) = \sigma(u) + \sigma(v)$$

pour tous u et v dans R.

Montrez que tout u dans R on a

$$\sigma(u) = u^p.$$

Quels sont les éléments de R fixés par σ ?

Soit T le sous-ensemble de R défini par

$$T = \{a + b\xi | a^2 - rb^2 = 1\}.$$

Montrer que T est un sous-groupe de R^*. Quel est son ordre ? Quel est son exposant ?

En vous inspirant de l'exercice précédent, donnez un algorithme de factorisation qui détecte les facteurs premiers p d'un entier n tels que $p + 1$ soit friable.

Exercice 12 : En quoi pourrait consister une *large prime variation* des algorithmes décrits dans les deux exercices précédents ?