Contrôle du 22 novembre

La notation accordera la plus grande importance à la qualité de la rédaction.

Exercice 1 : Énoncez le petit théorème de Fermat.

Calculez $2^{12345678909876543212345678909876543212345678909} \bmod 101$.

Exercice 2 :

Factorisez 143.

Quelles sont les racines carrées de 36 mod 143 ?

Exercice 3 :

On pose $p = 127$. Montrez que p est un nombre premier.

Factorisez $p - 1$ en produit de facteurs premiers.

On vérifie que $2^{63} = 1 \bmod p$, $2^{18} = 16 \bmod p$, $2^{42} = 1 \bmod p$, $3^{63} = 126 \bmod p$, $3^{18} = 4 \bmod p$, $3^{42} = 107 \bmod p$.

2 est il un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$?

3 est il un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$?

6 est il un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$?

En utilisant l'algorithme d'Euclide étendu calculez deux entiers a et b tels que

$$101a + 126b = 1.$$

Résoudre l'équation $a^{101} = 3$ dans $\mathbb{Z}/127\mathbb{Z}$.

Exercice 4 :

Montrez que $f(x) = x^7 + x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ est irréductible.

On pose $\mathbf{K} = \mathbb{F}_2[x]/f(x)$. Montrez que $\mathbf{K}$ est un corps.

Montrez que $x \bmod f(x)$ est un générateur de $\mathbf{K}^*$.

Résoudre l'équation $a^{51} = x \bmod f(x)$ dans $\mathbb{F}_2[x]/f(x)$.

Exercice 5 :

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

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

Donnez la liste de tous les générateurs de $(\mathbb{Z}/13\mathbb{Z})^*$.

Exercice 6 :

Montrer qu'il existe une infinité de nombres premiers.

Soit $n = 2 \times 3 \times 5 \times 7 \times 11$. Montrer qu'il n'y a pas de nombre premier dans l'intervale $[n + 2, n + 13[$.

Montrer que la différence entre deux nombres premiers consécutifs peut être arbitrairement grande.

Exercice 7 :

Décrivez un protocole cryptographique reposant sur la difficulté de calculer une racine carrée modulo un entier $n = pq$.

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

Exercice 8 :

Donnez un entier n qui soit congru à 1 modulo 2, à 2 modulo 3, et à 1 modulo 7.

Exercice 9 : Parmi tous les entiers de 1 à 999999 dites

- combien il y a de nombres pairs ?
- combien il y a de nombres à six chiffres ?
- combien il y a de carrés ?

Exercice 10 :

Montrer qu'il existe une infinité de nombres premiers.

Soit $n = 2 \times 3 \times 5 \times 7 \times 11$. Montrer qu'il n'y a pas de nombres premiers dans l'intervale $]n+2, n+13[$.

Montrer que la différence entre deux nombres premiers consécutifs peut être arbitrairement grande.

Exercice 11 : On veut factoriser le nombre $N = 36103$ en utilisant le crible quadratique.

1 . On observe que $\sqrt{N} \simeq 190.007894$. Écrivez une congruence modulo N du type

$$(a+m)^2 \equiv a^2 + u_1 a + u_0 \bmod N$$

dépendant d'un paramètre entier a. Ici m, u_0, u_1 sont des constantes entières bien choisies.

2 . Cherchez des valeurs de a comprises entre -20 et 20 qui permettent d'obtenir une congruence entre un carré et un nombre 7-friable modulo N. On pourra utiliser le document ci-après.

```
for(a=-20,20,print([a,factor(a^2+380*a-3)]))
[-20, [-1, 1; 3, 1; 7, 4]]
[-19, [-1, 1; 2, 1; 47, 1; 73, 1]]
[-18, [-1, 1; 3, 1; 41, 1; 53, 1]]
[-17, [-1, 1; 2, 1; 3, 2; 7, 3]]
[-16, [-1, 1; 5827, 1]]
[-15, [-1, 1; 2, 1; 3, 1; 11, 1; 83, 1]]
[-14, [-1, 1; 3, 1; 1709, 1]]
[-13, [-1, 1; 2, 1; 7, 1; 11, 1; 31, 1]]
[-12, [-1, 1; 3, 2; 491, 1]]
[-11, [-1, 1; 2, 1; 3, 1; 677, 1]]
[-10, [-1, 1; 7, 1; 23, 2]]
[-9, [-1, 1; 2, 1; 3, 1; 557, 1]]
[-8, [-1, 1; 3, 2; 331, 1]]
[-7, [-1, 1; 2, 1; 1307, 1]]
[-6, [-1, 1; 3, 1; 7, 1; 107, 1]]
[-5, [-1, 1; 2, 1; 3, 1; 313, 1]]
[-4, [-1, 1; 11, 1; 137, 1]]
[-3, [-1, 1; 2, 1; 3, 4; 7, 1]]
[-2, [-1, 1; 3, 1; 11, 1; 23, 1]]
[-1, [-1, 1; 2, 1; 191, 1]]
```

```
[0, [-1, 1; 3, 1]]
[1, [2, 1; 3, 3; 7, 1]]
[2, Mat([761, 1])]
[3, [2, 1; 3, 1; 191, 1]]
[4, [3, 1; 7, 1; 73, 1]]
[5, [2, 1; 31, 2]]
[6, [3, 2; 257, 1]]
[7, [2, 1; 3, 1; 11, 1; 41, 1]]
[8, [7, 1; 443, 1]]
[9, [2, 1; 3, 1; 11, 1; 53, 1]]
[10, [3, 2; 433, 1]]
[11, [2, 1; 7, 1; 307, 1]]
[12, [3, 1; 1567, 1]]
[13, [2, 1; 3, 1; 23, 1; 37, 1]]
[14, [37, 1; 149, 1]]
[15, [2, 1; 3, 2; 7, 1; 47, 1]]
[16, [3, 1; 2111, 1]]
[17, [2, 1; 3373, 1]]
[18, [3, 1; 7, 1; 11, 1; 31, 1]]
[19, [2, 1; 3, 2; 421, 1]]
[20, [11, 1; 727, 1]]
```

3 . Écrivez proprement toutes les congruences intéressantes obtenues. Portez les signes et les valuations dans une matrice M à coefficients entiers.

4 . Calculez le noyau de la réduction modulo 2 de la matrice M. Donnez la dimension de ce noyau, ainsi qu'une base.

5 . Pour chaque élément de cette base écrivez une congruence entre deux carrés modulo N. En déduire une factorisation (éventuellement triviale) de N.