Contrôle du 9 novembre

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

Exercice 1 : En utilisant le fait que $10 = 1 \bmod 3$ calculez de tête le reste de la division euclidienne de 70101010101010101101010101010101054321 par 3.

Exercice 2 : Quelles sont les racines carrées de 25 mod 21 ?

Exercice 3 : Quelles sont les racines cubiques de 27 mod 29 ?
Quelles sont les racines cubiques de 27 mod 31 ?

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 $(\mathbb{Z}/11\mathbb{Z})^*$.
Écrire la table des exponentielles et des logarithmes discrets en base g.

Exercice 6 :
On note $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ le corps à deux éléments. Montrer que le polynôme $f(x) = x^3 + x + 1$ est irréductible dans $\mathbb{F}_2[x]$.
Donnez un générateur g de $(\mathbb{F}_2[x]/f(x)\mathbb{F}_2[x])^*$.
Écrire la table des exponentielles et des logarithmes discrets en base g.

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 congru à 0 modulo 2, à 1 modulo 3, à 2 modulo 5.

Exercice 9 : Parmi tous les entiers de 1 à 9999 dites
- combien il y a de nombres pairs ?
- combien il y a de nombres à quatre chiffres ?
- combien il y a de carrés ?
- combien il y a de nombres 2-friables ?

Exercice 10 :

Combien y a-t-il de carrés dans $\mathbb{Z}/101\mathbb{Z}$?
Combien y a-t-il de carrés dans $(\mathbb{Z}/101\mathbb{Z})^*$?
Combien y a-t-il de carrés dans $\mathbb{Z}/303\mathbb{Z}$?
Combien y a-t-il de carrés dans $(\mathbb{Z}/303\mathbb{Z})^*$?
Combien y a-t-il de carrés dans $\mathbb{Z}/606\mathbb{Z}$?
Combien y a-t-il de carrés dans $(\mathbb{Z}/606\mathbb{Z})^*$?

Exercice 11 : Soit $A = \mathbb{Z}[x]$ l'anneaux des polynômes à coefficients entiers.

Soit I l'ensemble des polynômes $f(x)$ tels que $f(0)$ est pair.
Montrer que I est un idéal de A.
Montrer que I n'est pas un idéal principal.

Exercice 12 :

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 arbitrairemet grande.
