Contrôle continu du 25 octobre 2022

Exercice 1. (sur 5 pts) *Calculs*

1. **i.** Lister l'ensemble des inversibles de $\mathbb{Z}/30\mathbb{Z}$.
   ii. Calculer l'ordre de $[7]_{30}$ dans $\mathbb{Z}/30\mathbb{Z}^\times$.
2. Calculer le PGCD et les coefficients de Bézout associés aux entiers 7 et 10.
3. Résoudre dans $\mathbb{Z}$ les systèmes suivants :

$$\begin{cases} z \equiv_2 1 \\ z \equiv_3 2 \\ z \equiv_5 4 \end{cases} \qquad \begin{cases} z \equiv_{10} 4 \\ z \equiv_7 3 \end{cases}$$

4. Soit $n_1, \dots, n_k$ des entiers premiers entre eux deux à deux et $N = n_1 \cdots n_k$. Montrer que $N-1$ est l'unique solution positive et $< N$ du système

$$\begin{cases} z \equiv_{n_1} n_1 - 1 \\ z \equiv_{n_2} n_2 - 1 \\ \quad \vdots \\ z \equiv_{n_k} n_k - 1. \end{cases}$$

Exercice 2. (sur 8 pts) *Les entiers de Gauss*

Soit $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ où $i^2 = -1$.

1. Montrer que $\mathbb{Z}[i]$ est un anneau.

Pour $z = a + ib \in \mathbb{Z}[i]$, on note $\bar{z} = a - ib$ son conjugué, et $N(z) = z\bar{z}$.

2. Montrer que $z \mapsto \bar{z}$ est un automorphisme d'anneau de $\mathbb{Z}[i]$.
3. **i.** Calculer $N(z)$ en fonction de a et b. En déduire que pour tout $z \in \mathbb{Z}$, $N(z) \geq 0$, et que $N(z) = 0$ si et seulement si $z = 0$.
   ii. Montrer que $z \in \mathbb{Z}[i]$ est inversible (pour la multiplication) si et seulement si $N(z) = 1$.
   iii. En déduire l'ensemble des éléments inversibles de $\mathbb{Z}[i]$.
4. **i.** Est-ce que $i \cdot \mathbb{Z} = \{ib : b \in \mathbb{Z}\}$ est un idéal de $\mathbb{Z}[i]$? Si oui, décrire l'anneau quotient $\mathbb{Z}[i]/i \cdot \mathbb{Z}$.
   ii. Est-ce que $i \cdot \mathbb{Z}[i] = \{iz : z \in \mathbb{Z}[i]\}$ est un idéal de $\mathbb{Z}[i]$? Si oui, décrire l'anneau quotient $\mathbb{Z}[i]/i \cdot \mathbb{Z}[i]$.

Exercice 3. (sur 8 pts) *Autour de l'algorithme de Miller-Rabin*

L'algorithme de Miller-Rabin implanté en TP combine deux idées : les tests de Fermat et des racines carrées.

1. **Test de Fermat**. On tire aléatoirement un entier k entre 2 et $N-1$; si $\text{PGCD}(k,N) \neq 1$ ou $k^{N-1} \bmod N \neq 1$, N est déclaré « non premier » et k est appelé un *témoin de non-primalité* ; sinon il est déclaré « premier ».

   i. Montrer que si N est premier, alors il n'admet aucun témoin de non-primalité.

   ii. Soit $M = \{[a]_N : \text{PGCD}(a,N) = 1, a^{N-1} \bmod N = 1\}$. Montrer que M est un sous-groupe (multiplicatif) de $\mathbb{Z}/N\mathbb{Z}^\times$.

   iii. Que dit le théorème de Lagrange sur l'ordre d'un sous-groupe d'un groupe fini ? En déduire que si $M \neq \mathbb{Z}/N\mathbb{Z}^\times$, alors $|M| \leq \varphi(N)/2$ où $\varphi(N)$ est l'indicatrice d'Euler.

   iv. En déduire que dès que N admet un témoin de non-primalité premier avec N, il en admet en fait au moins $N/2$.

   v. Pourquoi la question précédente ne suffit pas pour dire que le test de Fermat est correct ?

2. **Test des racines carrées.** Un entier $x \in \{1,\dots,N-1\}$ est une *racine carrée* de l'unité modulo N si $x^2 \bmod N = 1$.

   i. Montrer que 1 et $N-1$ sont toujours racines carrées de l'unité modulo N.

   ii. Montrer que si x est racine carrée de l'unité modulo N, alors N divise $(x-1)(x+1)$.

   iii. En déduire que si N est premier, alors $x = 1$ ou $x = N-1$.

   iv. Montrer que 1 et 7 ne sont pas les seules racines de l'unité modulo 8.