Université Claude Bernard - Lyon 1 — **Semestre automne 2023–2024**

L1 — UE : Algèbre 1 (MATHS)

Devoir Surveillé 2 du 04/12/2023

Durée : 1 heure

Les documents et les téléphones/calculatrices/ordinateurs sont interdits.

Vous devrez faire attention à rédiger correctement. Toute rédaction incomplète ou imprécise sera sanctionnée même si le raisonnement est correct. **N'écrivez pas au crayon à papier.**

Exercice 1 Racines n^{eme} ($6 = 2+1+1+2$ pts)

Soit n un entier supérieur ou égal à 2.

1. Ecrire i et $-1+i$ sous forme exponentielle.
2. En déduire les racines n^{eme} de $-i$ et $-1+i$.
3. Résoudre dans $\mathbb{C}$ l'équation $z^2+z+1+i=0$.
4. En déduire les solutions de l'équation $z^6+z^3+1+i=0$.

Exercice 2 PGCD et PPCM (2 pts)

Calculer les pgcd et ppcm de 135 et 375.

Exercice 3 Nombres premiers ($6 = 2+2+2$ pts)

Soient p un nombre premier et $a \in \mathbb{N}$ un entier qui n'est pas divisible par p. Posons $R_p = \{1, 2, \cdots, p-1\}$. Soit $f : R_p \to R_p$ l'application définie par $f(i) = j$ où j est l'élément de R_p vérifiant $ai \equiv j \mod p$.

1. Montrer que l'application f est bijective. *Indication : Montrer que f est injective.*
2. Montrer que $a^{p-1}(p-1)!$ est congru à $(p-1)!$ modulo p.
   Indication : Montrer que $a^{p-1}(p-1)! \equiv f(1)\cdot f(2)\cdots f(p-1) \mod p$ et en déduire.
3. En déduire que $a^{p-1} \equiv 1 \mod p$ (le **petit théorème de Fermat**).

Exercice 4 Systèmes de congruences ($8 = 2+2+2+2$ pts)

1. Calculer le PGCD de 714 et 493.
2. Trouver une solution particulière $(x_0, y_0) \in \mathbb{Z}^2$ de l'équation $493x + 714y = 51$.
3. En déduire les solutions de l'équation diophantienne $29x + 42y = 3$.
4. Résoudre le système d'équation suivant :

$$\begin{cases} n \equiv 10 & \pmod{29} \\ n \equiv 7 & \pmod{42} \end{cases}$$

   Notons que $29 \cdot 42 = 1218$.

Exercice 5 BONUS (2 pts) Trouver le reste de la division euclidienne de $6^{321} - 4^{237}$ par 5.