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

L1 UE : Algèbre 1 (MATHS)

Devoir Surveillé 2 du 04/12/2023

Durée : 1 heure

CORRECTION

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.
   Correction. (2 pts) $-i = e^{\frac{3\pi}{2}i}$, $-1+i = \sqrt{2}e^{\frac{3\pi}{4}i}$.

2. En déduire les racines n^{eme} de $-i$ et $-1+i$.
   Correction. (1 pts) Racines n^{eme} de $-i$ sont $\{e^{\frac{3\pi i}{2n}}e^{\frac{2\pi ik}{n}}, k = 0, 1, \dots, n-1\}$.
   Racines n^{eme} de $-1+i$ sont $\{\sqrt{2}^{\frac{1}{n}}e^{\frac{3\pi i}{4n}}e^{\frac{2\pi ik}{n}}, k = 0, 1, \dots, n-1\}$.

3. Résoudre dans $\mathbb{C}$ l'équation $z^2 + z + 1 + i = 0$.
   Correction. (1 pts) Notons que $(z+i)\big(z-(-1+i)\big) = z^2+z+1+i$.
   Ainsi les racines de $z^2+z+1+i$ sont $-i$ et $-1+i$.

4. En déduire les solutions de l'équation $z^6 + z^3 + 1 + i = 0$.
   Correction. (2 pts) Soit $t = z^3$. Ainsi l'équation devient $t^2 + t + 1 + i = 0$.
   Par la question précédente, les solutions sont $t_1 = -i$, $t_2 = -1+i$.
   On veut de suite résoudre, $z^3 = t_i, i = 1, 2$, (c.a.d les racines 3^{eme} de $-i$ et de $-1+i$).
   Par la question 2, les racines 3^{eme} de $-i$ sont $\{e^{i(\frac{\pi}{2}+\frac{2\pi k}{3})}, k = 0, 1, 2\}$ et
   les racines 3^{eme} de $-1+i$ sont $\{\sqrt{2}^{\frac{1}{3}}e^{i(\frac{\pi}{4}+\frac{2\pi k}{3})}, k = 0, 1, 2\}$.
   Les 6 solutions de $z^6 + z^3 + 1 + i = 0$ sont donc - $\{e^{\frac{\pi i}{2}}, e^{\frac{7\pi i}{6}}, e^{\frac{11\pi i}{6}}, 2^{\frac{1}{6}}e^{\frac{\pi i}{4}}, 2^{\frac{1}{6}}e^{\frac{11\pi i}{12}}, 2^{\frac{1}{6}}e^{\frac{19\pi i}{12}}\}$.

Exercice 2 **PGCD et PPCM** (2 pts)

Calculer les pgcd et ppcm de 135 et 375.

Correction. Par divisions euclidiennes

$$\begin{aligned} 375 &= 2 \cdot 135 + 105 \\ 135 &= 1 \cdot 105 + 30 \\ 105 &= 3 \cdot 30 + 15 \\ 30 &= 2 \cdot 15, \end{aligned}$$

on a $\mathrm{PGCD}(375, 135) = 15$. On en déduit que

$$\mathrm{PPCM}(375, 135) = \frac{135 \cdot 375}{\mathrm{PGCD}(135, 375)} = \frac{135 \cdot 375}{15} = 9 \cdot 375 = 3375.$$

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.*

   Correction. Soient $i_1, i_2 \in R_p$ tels que $f(i_1) = f(i_2)$. Alors, comme $ai_1 \equiv ai_2 \mod p$, on a $ai_1 - ai_2 = a(i_1 - i_2) \equiv 0 \mod p$, i.e., p divise $a(i_1 - i_2)$. Puisque a est p sont premiers entres eux, le lemme de Gauss implique que $i_1 - i_2$ est un mutiple de p, d'où $i_1 = i_2$ par la définition de R_p, i.e., f est injective. Comme R_p est un ensemble fini, f est automatiquement bijective.

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.

   Correction. Comme $a^{p-1}(p-1)! = \prod_{k=1}^{p-1}(ak)$ et $ak \equiv f(k) \mod p$ par définition, on en déduit que $a^{p-1}(p-1)! = \prod_{k=1}^{p-1}(ak) \equiv \prod_{k=1}^{p-1} f(k) \mod p$.

3. En déduire que $a^{p-1} \equiv 1 \mod p$ (le **petit théorème de Fermat**).
   Correction. Puisque l'application f est injective les $(p-1)$-valeurs $f(1), f(2), \cdots, f(p-1) \in R_p$ sont toutes distinctes et que il n'y a que $(p-1)$-éléments dans R_p, on en déduit que l'ensemble $\{f(1), f(2), \cdots, f(p-1)\}$ coïncide avec R_p d'où $\prod_{k=1}^{p-1} f(k) = (p-1)!$. Ainsi, on obtient

   $$a^{p-1}(p-1)! \equiv \prod_{k=1}^{p-1} f(k) = (p-1)! \mod p \qquad \Longleftrightarrow \qquad (a^{p-1} - 1)(p-1)! \equiv 0 \mod p.$$

   Donc, le lemme de Gauss implique que $p \mid a^{p-1} - 1$, car p ne divise pas $(p-1)!$.

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

1. Calculer le PGCD de 714 et 493.
   Correction. (2 pts) L'algorithme d'Euclide nous donne $\mathrm{PGCD}(171, 48) = 17$

   $$\begin{aligned} 714 &= 1 \times 493 + 221 \\ 493 &= 2 \times 221 + 51 \\ 221 &= 4 \times 51 + 17 \\ 51 &= 3 \times 17. \end{aligned}$$

2. Trouver une solution particulière $(x_0, y_0) \in \mathbb{Z}^2$ de l'équation $493x + 714y = 51$.
   Correction. (2 pts) Calculons une identité de Bézout :

   $$\begin{aligned} 17 &= 221 - 4 \cdot 51 = 221 - 4 \cdot (493 - 2 \cdot 221) \\ &= (-4) \cdot 493 + 9 \cdot 221 = (-4) \cdot 493 + 9 \cdot (714 - 1 \cdot 493) \\ &= 9 \cdot 714 - 13 \cdot 493, \end{aligned}$$

   on en déduit que $493 \cdot (-13) + 714 \cdot 9 = 17$. Comme $51 = 17 \cdot 3$, multipliant l'identité de Bézout obtenu par 3, on obtient $493 \cdot (-39) + 714 \cdot 27 = 51$. Donc, $(x_0, y_0) = (-39, 27)$ est une solution particulière de l'équation $493x + 714y = 51$.

3. En déduire les solutions de l'équation diophantienne $29x + 42y = 3$.

Correction. (2 *pts*) Multipliant $\frac{1}{17}$ sur l'équation $493x+714y = 51$, on obtient $29x+42y = 3$, d'où la solution particulière (x_0, y_0) trouvée dans la question précédente donne une solution particulière de l'équation $29x + 42y = 3$, i.e., on a $29x_0 + 42y_0 = 3$, d'où

$$29x + 42y = (3 =)29x_0 + 42y_0 \qquad \Longleftrightarrow 29(x - x_0) = -42(y - y_0).$$

Comme 29 est un nombre premier et que $\mathrm{PGCD}(29, 42) = 1$, le lemme de Gauss implique que $29 \mid y - y_0$, i.e., il existe $k \in \mathbb{Z}$ tel que $y - y_0 = 29k$, d'où

$$29(x - x_0) = -42(y - y_0) = -42 \cdot 29k \qquad \Longrightarrow \qquad x - x_0 = -42k.$$

On en déduit que les solutions de l'équation $29x + 42y = 3$ sont

$$(x, y) = (x_0, y_0) + k(-42, 29) = (-39 - 42k, 27 + 29k) \qquad k \in \mathbb{Z}.$$

4. Résoudre le système d'équation suivant :

$$\begin{cases} n \equiv 10 & (\mathrm{mod}\ 29) \\ n \equiv 7 & (\mathrm{mod}\ 42) \end{cases}$$

Notons que $29 \cdot 42 = 1218$.

Correction. (2 *pts*) Par la première equation, il existe $x' \in \mathbb{Z}$ tel que $n = 29x' + 10$ et par la deuxième équation, il existe $y' \in \mathbb{Z}$ tel que $n = 42y' + 7$, d'où $29x' + 10 = 42y' + 7$, i.e., $29 \cdot (-x') + 42 \cdot y' = 10 - 7 = 3$. D'après la question 2., $(-x', y') = (-39, 27)$, i.e., $(x', y') = (39, 27)$ est une solution particulière de l'équation $29x'+10 = 42y'+7$. En particulier, $n = 42 \cdot 27+7 = 1141$ est une solution particulière du système. Comme $\mathrm{PGCD}(29, 42) = 1$, on a $\mathrm{PPCM}(29, 42) = 1218$. Donc, d'après le théorème de reste chinois, l'ensemble des solutions du système est $1141 + 1218\mathbb{Z}$.

Une autre solution. Par la première equation, il existe $x' \in \mathbb{Z}$ tel que $n = 29x' + 10$ et par la deuxième équation, il existe $y' \in \mathbb{Z}$ tel que $n = 42y' + 7$, d'où $29x' + 10 = 42y' + 7$, i.e., $29 \cdot (-x') + 42 \cdot y' = 10 - 7 = 3$. D'après la question précédente, il existe $k \in \mathbb{Z}$ tel que $(-x', y') = (-39 - 42k, 27 + 29k)$, i.e., $(x', y') = (39 + 42k, 27 + 29k)$. En particulier, ceci implique que les solution du système est donné par

$$n = 29x' + 10(= 42y' + 7) = 29(39 + 42k) + 10 = 1141 + 1218k \qquad k \in \mathbb{Z}.$$

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

Correction. (2 *pts*) Comme $6^2 = 36 \equiv 1\,[5]$ et $4^2 = 16 \equiv 1\,[5]$, on a

$$6^{321} - 4^{237} \equiv 6^1 - 4^1 \equiv 2 \mod 5.$$