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

L1 — UE : Algèbre 1 (MATHS)

Exercices

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} Ici, on veut trouver tous les solutions de l'équation $(E) : z^8 + 4z^4 + 16 = 0$ par deux méthodes :

1. Voir l'équation (E) comme une équation sur z^4 ;
   (a) Trouver les valeurs de z^4.
   Correction On trouve $z^4 = -2 \pm 2\sqrt{3}i$.
   (b) Calculer les racines 4ème de ce que vous avez trouver dans la question précédente.
   Correction Les racines 4ème de $-2 \pm 2\sqrt{3}i = 4e^{\pm\frac{2\pi}{3}i}$ sont $2^{\frac{1}{2}}e^{\pm\frac{\pi}{6}i+\frac{k\pi}{2}i}$ avec $k = 0, 1, 2, 3$.
   (c) Conclure.
   Correction Les solutions de l'équation (E) sont $2^{\frac{1}{2}}e^{\pm\frac{\pi}{6}i+\frac{k\pi}{2}i}$ avec $k = 0, 1, 2, 3$.
2. À l'aide de $z^8 + 4z^4 + 16 = (z^8 + 8z^4 + 16) - 4z^4$,
   (a) Factoriser $z^8 + 4z^4 + 16$. On précisera les deux équations sur z^2 ainsi obtenues.
   Correction Comme $z^8 + 4z^4 + 16 = (z^4 + 4)^2 - (2z^2)^2 = (z^4 + 2z^2 + 4)(z^4 - 2z^2 + 4)$,
   on a $z^4 + 2z^2 + 4 = 0$ et $z^4 - 2z^2 + 4 = 0$.
   (b) Résoudre ces deux équation algébriques. Ensuite, calculer les racines carrées de ces solutions.
   Correction Les solutions de l'équation $z^4+2z^2+4 = 0$ (resp. $z^4-2z^2+4 = 0$) sont $-1\pm\sqrt{3}i$ (resp. $1\pm\sqrt{3}i$). Les racines carrées de $-1\pm\sqrt{3}i = 2e^{\pm\frac{2\pi i}{3}}$ (resp. $1\pm\sqrt{3}i = 2e^{\pm\frac{\pi i}{3}}$) sont $2^{\frac{1}{2}}e^{\pm\frac{\pi i}{3}}$ et $2^{\frac{1}{2}}e^{\pm\frac{4\pi i}{3}}$ (resp. $2^{\frac{1}{2}}e^{\pm\frac{\pi i}{6}}$ et $2^{\frac{1}{2}}e^{\pm\frac{7\pi i}{6}}$).
   (c) Conclure.
   Correction Les solutions de l'équation (E) sont $2^{\frac{1}{2}}e^{\pm\frac{\pi i}{6}}$, $2^{\frac{1}{2}}e^{\pm\frac{\pi i}{3}}$, $2^{\frac{1}{2}}e^{\pm\frac{2\pi i}{3}}$ et $2^{\frac{1}{2}}e^{\pm\frac{5\pi i}{6}}$.

Exercice 2 Équation diophantienne et Théorème des restes chinois

1. Calculer le PGCD de 720 et 252.
   Correction Par les divisions euclidiennes successives $720 = 2 \cdot 252 + 216$, $252 = 1 \cdot 216 + 36$ et $216 = 6 \cdot 36$, on a $\text{pgcd}(720, 252) = 36$.
2. Trouver une solution particulière $(x_0, y_0) \in \mathbb{Z}^2$ de l'équation $720x + 252y = 108$.
   Correction Remontant les divisions euclidiennes ci-dessus :
   $36 = 252 - 1 \cdot 216 = 252 - 1 \cdot (720 - 2 \cdot 252) = (-1) \cdot 720 + 3 \cdot 252$.
   Comme $108 = 3 \cdot 36$, on voit que $(x_0, y_0) = 3(-1, 3) = (-3, 9)$
   est une solution particulière de l'équation $720x + 252y = 108$.
3. En déduire les solutions de l'équation diophantienne $20x + 7y = 3$.
   Correction Comme $720 = 36 \cdot 20$ et $252 = 36 \cdot 7$, on voit que
   l'équation $720x + 252y = 108$ est équivalent à l'équation $20x + 7y = 3$.
   En particulier, (x_0, y_0) de la question précédente est une solution particulière de l'équation $20x + 7y = 3$, i.e., il vérifie $20x_0 + 7y_0 = 3$, d'où $20(x - x_0) + 7(y - y_0) = 0$, i.e., $20(x - x_0) = -7(y - y_0)$. Le deuxième membre étant un multiple de 7, $7|20(x - x_0)$.

D'après le lemme de Gauss, il existe $7|(x-x_0)$. Donc, il existe $k \in \mathbb{Z}$ tel que $x-x_0 = 7k$, i.e., $x = x_0+7k$. Ceci implique que $7(y-y_0) = -20(x-x_0) = -140k$ d'où $y = y_0-20k$. Donc, les solutions sont $(x, y) = (x_0, y_0) + k(7, -20)$ avec $k \in \mathbb{Z}$.

4. Résoudre le système d'équation suivant :

$$\begin{cases} n \equiv 9 & \pmod{20} \\ n \equiv 6 & \pmod{7} \end{cases}$$

Correction L'équation $n \equiv 9[20]$ implique qu'il existe $x' \in \mathbb{Z}$ tel que $n = 20x' + 9$ et l'équation $n \equiv 6[7]$ implique qu'il existe $y' \in \mathbb{Z}$ tel que $n = 7y' + 6$. On en déduit que $(n =)20x' + 9 = 7y' + 6$, i.e., $20(-x') + 7y' = 3$. D'après la question précédente, on en déduit que $(-x', y') = (x_0, y_0) + k(7, -20) = (-3, 9) + k(7, -20)$ avec $k \in \mathbb{Z}$. d'où $n = 7y' + 6 = 7(9 - 20k) + 6 = 69 - 140k$ avec $k \in \mathbb{Z}$.

Exercice 3 Arithmétique Soit p un nombre premier supérieur à 2.

1. Pour tout entier k entre 1 et $p - 1$, montrer que le coefficient binomial $\binom{p}{k}$ est divisible par p.

Correction Le coefficient binomial $\binom{p}{k} = \dfrac{p!}{k!(p-k)!}$ étant un entier, l'entier $k!(p-k)!\binom{p}{k} = p!$ est un multiple de p. Par hypothèse, p ne peut diviser $k!(p-k)!$, d'où le lemme de Gauss implique que $\binom{p}{k}$ est un multiple de p.

2. Montrer, par récurrence, que $p|a^p - a$ pour tout entier naturel a.

Correction (Initialisation) : $0^p - 0 = 0$ est un multiple de p, donc l'énoncé est vrai. (Héridité) : Supposons que $a^p - a$ est un multiple de p pour un $a \in \mathbb{N}$. En rang $a + 1$,

$$\begin{aligned}(a+1)^p - (a+1) =& \sum_{k=0}^{p} \binom{p}{k} a^k - (a+1) = \sum_{k=1}^{p-1} \binom{p}{k} a^k + (a^p + 1^p) - (a+1) \\ =&(a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k.\end{aligned}$$

Comme la question précédente implique que $\sum_{k=1}^{p-1} \binom{p}{k} a^k$ est un multiple de p et que $p|a^p - a$ par l'hypothèse de récurrence, on en déduit que $(a+1)^p - (a+1)$ l'est aussi.

3. En déduire que si a et p sont premier entre eux, $a^{p-1} - 1$ est divisible par p. (Petit théorème de Fermat)

Correction Comme le nombre premier p divise $a^p - a = a(a^{p-1} - 1)$ et que a et p sont premiers entre eux par hypothèse, le lemme de Gausse implique que p divise $a^{p-1} - 1$.

Exercice 4 Nombres premiers

1. Vérifier que, pour tout entier $0 \leqslant n \leqslant 40$, l'entier $n^2 - n + 41$ est un nombre premier et que pour $n = 41$ et 42, ils ne le sont pas.

Correction Par calcul direct. Voici le tableau $(0 < n \leqslant 40)$:

n	1	2	3	4	5	6	7	8	9	10
$f(n)$	41	43	47	53	61	71	83	97	113	131
n	11	12	13	14	15	16	17	18	19	20
$f(n)$	151	173	197	223	251	281	313	347	383	421
n	21	22	23	24	25	26	27	28	29	30
$f(n)$	461	503	547	593	641	691	743	797	853	911
n	31	32	33	34	35	36	37	38	39	40
$f(n)$	971	1033	1097	1163	1231	1301	1373	1447	1523	1601

On peut vérifier que les $f(n)$ dans ce tableau sont tous premiers ! Le critère suivant est à utiliser :

Si un entier $n \in \mathbb{N}^*$ n'est pas divisible par les nombres premiers p entre 1 et $\sqrt{n}$,
n est un nombre premier.

Cet énoncé est évident car si n a un diviseur d vérifiant $\sqrt{n} \leqslant d < n$, alors, l'entier $\frac{n}{d}$ est un diviseur de n vérifiant $1 < \frac{n}{d} \leqslant \sqrt{n}$.
Reste à savoir que les nombres premiers entre 1 et 40 sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37$.
Bien évidemment, $f(41) = 41^2 - 41 + 41 = 41^2 (= 1681)$ et $f(42) = 42^2 - 42 + 41 = 42(42-1) + 41 = 41(42+1) = 41 \cdot 43 (= 1763)$ ne sont pas premiers... BON COURAGE !!!

2. Existe-t-il un entier K tel que $n^2 - n + K$ est un nombre premier pour tout $n \in \mathbb{N}$ sauf $n = K, K+1$? Justifier votre réponse.

   Correction On constante que, par exemple, pour $m \in \mathbb{N}^*$,

   $$f(mK) = (mK)^2 - mK + K = K(mK^2 - m + 1)$$

   ne peut être un nombre premier. Donc, un tel entier K n'existe pas.

Exercice 5 **Congruence** Calculer 16^{2023} mod 11 et 16^{2023} mod 13.

Correction Comme $16 \equiv 5[11]$, on a $16^{2023} \equiv 5^{2023}[11]$. Étudions les puissances de 5. Par calcul direct,

$$5^2 = 25 \equiv 3[11], \quad 5^3 \equiv 15 \equiv 4[11], \quad 5^4 \equiv 20 \equiv 9[11], \quad 5^5 \equiv 45 \equiv 1[11].$$

Comme $2023 = 404 \cdot 5 + 3$, on en déduit que

$$5^{2023} = (5^5)^{404} \cdot 5^3 (\equiv 1^{404} \cdot 5^3) \equiv 5^3 \equiv 4[11].$$

De même, $16 \equiv 3[13]$ implique que $16^{2023} \equiv 3^{2023}[13]$ et

$$3^2 = 9, \quad 3^3 = 27 \equiv 1[13].$$

(On peut aussi calculer comme $3^2 = 9 \equiv -4[13]$ et $3^3 \equiv -12 \equiv -12 + 13 \equiv 1[13]$.)
Comme $2023 = 674 \cdot 3 + 1$, on en déduit que

$$3^{2023} = (3^3)^{674} \cdot 3^1 (\equiv 1^{674} \cdot 3^1) \equiv 3^1 \equiv 3[13].$$

On obtient

$$16^{2023} \equiv 4[11], \qquad 16^{2023} \equiv 3[13].$$