Corrigé du TD n° 6

Arithmétique dans $\mathbb{Z}$ et groupes d'isométries.

8 décembre 2020

Exercice 1.

1. Soit $n \in \mathbb{N}$. Démontrer que $11 \mid 3^{5n} + 5^{5n+1} + 4^{5n+2}$.
2. Déterminer le reste de la division euclidienne de 2^{65362} par 7.
3. Soit $n \in \mathbb{N}$. Montrer que 3 ne divise pas $n^2 + 1$.
4. Déterminer les solutions de l'équation d'inconnues $(x, y) \in \mathbb{N}^2$
$$x^2 = y^2 + \text{pgcd}(x, y) + 2.$$
5. Déterminer les nombres premiers p tels que $p + 2$ et $p + 4$ soient premiers.

---

1. *Version 1.*
• On a $3^2 \equiv -2 \bmod 11$, donc $3^4 \equiv (-2)^2 \equiv 4 \bmod 11$, puis $3^5 \equiv 4 \times 3 \equiv 1 \bmod 11$. Donc, comme $3^{5n} = (3^5)^n$, on en déduit que $3^{5n} \equiv 1^n \equiv 1 \bmod 11$.
• On a $5^2 \equiv 3 \bmod 11$, donc $5^4 \equiv 3^2 \equiv 9 \bmod 11$, puis $5^5 \equiv 9 \times 5 \equiv 45 \equiv 1 \bmod 11$. Donc comme $5^{5n+1} = (5^5)^n \times 5$, on en déduit que $5^{5n+1} \equiv 1^n \times 5 \equiv 5 \bmod 11$.
• On a $4^2 \equiv 5 \bmod 11$, donc $4^4 \equiv 5^2 \equiv 3 \bmod 11$, puis $4^5 \equiv 3 \times 4 \equiv 1 \bmod 11$. Donc comme $4^{5n+2} = (4^5)^n \times 4^2$, on en déduit que $4^{5n+2} \equiv 1^n \times 16 \equiv 5 \bmod 11$.
Finalement, $3^{5n} + 5^{5n+1} + 4^{5n+2} \equiv 1 + 5 + 5 \equiv 11 \equiv 0 \bmod 11$.
Donc 11 divise $3^{5n} + 5^{5n+1} + 4^{5n+2}$.

Version 2. On démontre le résultat par récurrence. Notons pour tout $n \in \mathbb{N}$, (H_n) la propriété « $11 \mid 3^{5n} + 5^{5n+1} + 4^{5n+2}$ ».
• Initialisation. Pour $n = 0$, on a $3^{5n} + 5^{5n+1} + 4^{5n+2} = 1 + 5 + 4^2 = 22$ et 11 divise 22. Donc (H_0) est vraie.
• Hérédité. Soit $n \in \mathbb{N}$. Supposons (H_n) et montrons (H_{n+1}).
On a $3^{5(n+1)} + 5^{5(n+1)+1} + 4^{5(n+1)+2} = 3^{5n} \times 3^5 + 5^{5n+1} \times 5^5 + 4^{5n+2} \times 4^5$.
On montre comme précédemment que $3^5 \equiv 1 \bmod 11$, $5^5 \equiv 1 \bmod 11$ et $4^5 \equiv 1 \bmod 11$.
Il existe donc k_1, k_2 et k_3 des éléments de $\mathbb{Z}$ tels que $3^5 = 1 + 11k_1$, $5^5 = 1 + 11k_2$ et $4^5 = 1 + 11k_3$.
Donc
$$\begin{aligned} 3^{5(n+1)} + 5^{5(n+1)+1} + 4^{5(n+1)+2} &= 3^{5n}(1 + 11k_1) + 5^{5n+1}(1 + 11k_2) + 4^{5n+2}(1 + 11k_3) \\ &= 3^{5n} + 5^{5n+1} + 4^{5n+2} + 11(3^{5n}k_1 + 5^{5n+1}k_2 + 4^{5n+2}k_3). \end{aligned}$$
Par hypothèse de récurrence, 11 divise $3^{5n} + 5^{5n+1} + 4^{5n+2}$, et comme 11 divise $11(3^{5n}k_1 + 5^{5n+1}k_2 + 4^{5n+2}k_3)$, on en déduit que 11 divise leur somme, égale à $3^{5(n+1)} + 5^{5(n+1)+1} + 4^{5(n+1)+2}$.
D'où (H_{n+1}).
Ainsi, pour tout $n \in \mathbb{N}$, 11 divise $3^{5n} + 5^{5n+1} + 4^{5n+2}$.

2. On a $2^0 \equiv 1 \bmod 7$, $2^1 \equiv 2 \bmod 7$, $2^2 \equiv 4 \bmod 7$, $2^3 \equiv 1 \bmod 7$. *Maintenant que l'on est retombé sur le* 1*, on va raisonner sur l'exposant modulo* 3*.*
Or $65362 = 3 \times 21787 + 1$.
Donc $2^{65362} = (2^3)^{21787} \times 2$. D'après les calculs précédents, $2^3 \equiv 1 \bmod 7$, donc $2^{65362} \equiv 1 \times 2 \equiv 2 \bmod 7$.
Comme $0 \leq 2 < 7$, on en déduit que le reste de la division euclidienne de 2^{65362} par 7 vaut 2.

3. On sait que n est congru à 0, 1 ou 2 modulo 3 (*reste de la division euclidienne de n par* 3).
-1er cas : $n \equiv 0 \bmod 3$. Alors $n^2 \equiv 0 \bmod 3$ et donc $n^2 + 1 \equiv 1 \bmod 3$.
-2ème cas : $n \equiv 1 \bmod 3$. Alors $n^2 \equiv 1 \bmod 3$ et donc $n^2 + 1 \equiv 2 \bmod 3$.
-3ème cas : $n \equiv 2 \bmod 3$. Alors $n^2 \equiv 4 \equiv 1 \bmod 3$ et donc $n^2 + 1 \equiv 2 \bmod 3$.
Donc dans tous les cas, $n^2 + 1$ n'est pas congru à 0 modulo 3. Donc 3 ne divise pas $n^2 + 1$.

4. *Version 1 :* Soit $(x,y) \in \mathbb{N}^2$. On suppose que $x^2 = y^2 + \text{pgcd}(x,y) + 2$. Alors $(x,y) \neq (0,0)$. Posons $d = \text{pgcd}(x,y) > 0$. On sait qu'il existe $(x',y') \in \mathbb{Z}^2$ tel que $x = dx'$, $y = dy'$ et $\text{pgcd}(x',y') = 1$. On a donc
$$d^2x'^2 = d^2y'^2 + d + 2.$$
Donc $d(dx'^2 - dy'^2 - 1) = 2$ et d divise donc 2. Donc $d = 1$ ou $d = 2$.
-1er cas : $d = 1$. Alors $x'^2 = y'^2 + 3$, soit encore $(x' - y')(x' + y') = 3$. Or 3 est un nombre premier et $x' - y' \leq x' + y'$ puisque $y' \geq 0$, donc nécessairement $x' - y' = 1$ et $x' + y' = 3$. Donc $x' = 2$ et $y' = 1$, et finalement $x = 2$ et $y = 1$.
-2nd cas : $d = 2$. Alors en divisant par 4, on obtient $x'^2 = y'^2 + 1$, soit encore $(x' + y')(x' - y') = 1$. Donc nécessairement $x' + y' = 1$ et $x' - y' = 1$. Donc $x' = 1$ et $y' = 0$, et finalement $x = 2$ et $y = 0$.
Réciproquement, on vérifie que les couples $(2,1)$ et $(2,0)$ vérifient l'équation :
$$2^2 = 1^2 + 1 + 2 \quad \text{et} \quad 2^2 = 0^2 + 2 + 2.$$
D'où l'ensemble des solutions de l'équation est $\{(2,1),(2,0)\}$.

Version 2 : Soit $(x,y) \in \mathbb{N}^2$. Supposons que $x^2 = y^2 + \text{pgcd}(x,y) + 2$. Posons $d = \text{pgcd}(x,y)$. Comme d divise x et d divise y, l'égalité modulo d donne $2 \equiv 0 \bmod d$. Donc d divise 2 et $d = 1$ ou $d = 2$. De plus, on a $(x+y)(x-y) = d+2$.
Si $d = 1$, on résout $(x + y)(x - y) = 3$ comme précédemment et on trouve $(x,y) = (2,1)$.
Si $d = 2$, on a alors $(x + y)(x - y) = 4 = 2^2$. Comme x et y sont pairs, $x + y$ et $x - y$ le sont également, donc nécessairement $x + y = 2$ et $x - y = 2$. D'où $x = 2$ et $y = 0$.
Réciproquement, on vérifie que les couples $(2,1)$ et $(2,0)$ sont bien solutions de l'équation.

5. *Version 1 :* Soit p un nombre premier tel que $p + 2$ et $p + 4$ soient également premiers.
-1er cas : p est congru à 0 modulo 3. Alors 3 divise p et p étant premier, on a nécessairement $p = 3$. De plus, $p + 2 = 5$ et $p + 4 = 7$ sont premiers.
-2ème cas : p est congru à 1 modulo 3. Alors $p + 2 \equiv 3 \equiv 0 \bmod 3$. Donc 3 divise $p + 2$. Or $p + 2$ est strictement supérieur à 3 (puisque $p \geq 2$), ce qui contredit le fait que $p + 2$ soit premier. Donc p n'est pas congru à 1 modulo 3.
-3ème cas : p est congru à 2 modulo 3. Alors $p + 4 \equiv 6 \equiv 0 \bmod 3$. Donc 3 divise $p + 4$. Comme précédemment, ceci contredit le fait que $p + 4$ soit premier. Donc p n'est pas congru à 2 modulo 3.
Donc finalement, 3 est le seul nombre premier p tel que $p + 2$ et $p + 4$ soient premiers.

Version 2 : Pour tout nombre $p \in \mathbb{N}^*$, les classes de $p - 1$, p et $p + 1$ sont les trois éléments de $\mathbb{Z}/3\mathbb{Z}$, donc les classes de $p + 2$, p et $p + 4$. Par hypothèse, $p + 2$ et $p + 4$ sont des nombres premiers ≥ 4, ils ne sont pas divisibles 3. On en déduit que $p \equiv 0[3]$, et comme p est premier, $p = 3$.

Exercice 2.

1. Soit $n \in \mathbb{N}$. Montrer que $\sqrt{n} \in \mathbb{Q}$ si et seulement s'il existe $m \in \mathbb{N}$ tel que $n = m^2$.
2. En déduire que $\sqrt{2} \notin \mathbb{Q}$ et $\sqrt{3} \notin \mathbb{Q}$.

---

1. *Version 1 :* $\Rightarrow$ Supposons que $\sqrt{n} \in \mathbb{Q}$. Alors il existe $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $\sqrt{n} = \dfrac{p}{q}$ et $\text{pgcd}(p,q) = 1$.
On a donc $q^2 n = p^2$. Comme $qn \in \mathbb{N}$, on en déduit que q divise $p^2 = p \times p$. Or p et q sont premiers entre eux. Donc, d'après le théorème de Gauss, q divise $p = p \times 1$, puis en appliquant à nouveau le théorème de Gauss, q divise 1. Donc $q = 1$ et donc $n = p^2$. *(On pourrait également utiliser que q et p^2 sont premiers entre eux car q et p le sont et obtenir que q divise 1 en appliquant une seule fois le théorème de Gauss).*
$\Leftarrow$ Réciproquement, s'il existe $m \in \mathbb{N}$ tel que $n = m^2$ alors $\sqrt{n} = m \in \mathbb{Q}$.
D'où le résultat.

Version 2 : De même, on écrit $\sqrt{n} = \dfrac{p}{q}$ avec p et q premiers entre eux. D'après le théorème de Bézout, il existe $(\alpha,\beta) \in \mathbb{Z}^2$ tel que $\alpha p + \beta q = 1$. D'où $\alpha p \equiv 1[q]$ et $\alpha^2 p^2 \equiv 1[q]$.
De plus, comme $\alpha^2 p^2 = \alpha^2 q^2 n$, il vient $\alpha^2 p^2 \equiv 0[q]$.
On en déduit $1 \equiv 0[q]$, c'est-à-dire $q = 1$. Donc $n = p^2$.

2. 2 ne s'écrit pas sous la forme $2 = m^2$ avec $m \in \mathbb{N}$ (par exemple, $1 = 1^2 < 2 < 2^2 = 4$) donc, d'après la question précédente, $\sqrt{2} \notin \mathbb{Q}$. De même pour 3.
Remarque : un entier n qui s'écrit sous la forme $n = m^2$ s'appelle un carré parfait. Par exemple, 4, 9, 16 sont des carrés parfaits.

Exercice 3 (Équations dans $\mathbb{Z}/n\mathbb{Z}$)**.**

1. Résoudre dans $\mathbb{Z}/10\mathbb{Z}$ l'équation $\overline{3}x + \overline{5} = \overline{0}$.
2. Résoudre dans $\mathbb{Z}$ l'équation $5x \equiv 3 \bmod 28$.

Uniquement la réponse. Correction détaillée dans le document Alg1Geo1-TD6-Notes-Ex1à5

1. L'équation admet une unique solution, $\overline{5}$.
2. L'ensemble des solutions de l'équation est $\mathcal{S} = \{23 + 28k \mid k \in \mathbb{Z}\}$.

Exercice 4 (Équations diophantiennes)**.** Résoudre les équations d'inconnues $(x,y) \in \mathbb{Z}^2$ suivantes :

1. $20x - 53y = 3$,
2. $162x + 207y = 27$,
3. $x^3 + 5 = 117y^3$. *On pourra réduire modulo* 9.

Uniquement la réponse. Correction détaillée dans le document Alg1Geo1-TD6-Notes-Ex1à5

1. L'ensemble des solutions est $\mathcal{S} = \{(24 + 53k, 9 + 20k) \mid k \in \mathbb{Z}\}$.
2. L'ensemble des solutions est $\mathcal{S} = \{(27 + 23k, -21 - 18k) \mid k \in \mathbb{Z}\}$.
3. L'équation n'admet pas de solutions.

Exercice 5 (Théorème des restes chinois)**.** Résoudre les systèmes de congruences suivants :

1. $\begin{cases} x \equiv 2 \bmod 10 \\ x \equiv 5 \bmod 13 \end{cases}$,
2. $\begin{cases} x \equiv 3 \bmod 17 \\ x \equiv 4 \bmod 11 \\ x \equiv 5 \bmod 6 \end{cases}$.

Uniquement la réponse. Correction détaillée dans le document Alg1Geo1-TD6-Notes-Ex1à5

1. L'ensemble des solutions est $\mathcal{S} = \{122 + 130k, k \in \mathbb{Z}\}$.
2. L'ensemble des solutions est $\mathcal{S} = \{785 + 1122k \mid k \in \mathbb{Z}\}$.

Exercice 6. Soit A, B et C trois points du plan euclidien deux à deux distincts non alignés : $A \notin (CD)$. On appelle triangle (ABC), la partie du plan $[AB] \cup [AC] \cup [C, D]$.

1. Montrer que les trois médiatrices de $[AB]$, $[AC]$ et $[BC]$ se coupent en un même point Ω. On dit que les droites sont concourantes.
2. Le triangle (ABC) est équilatéral si $AB = AC = BC$. Trouvez le groupe G des isométries du plan qui conservent un triangle équilatéral. On pourra se placer dans le repère $(\Omega, \overrightarrow{i}, \overrightarrow{j})$.
3. Montrer que G est ismorphe à un groupe que nous avons déjà rencontré.

---

1. On procède par analyse-synthèse : Si Ω existe, Ω est le point d'intersection des médiatrices de $[AB]$ et de $[BC]$. Synthèse, les droites (AB) et (AC) sont distinctes, les médiatrices de $[AB]$ et $[A, C]$ se coupent en un point Ω. Par définition de la médiatrice, $\Omega A = \Omega B$ et $\Omega B = \Omega C$, donc $\Omega A = \Omega C$ et Ω appartient aussi à la médiatrice de $[AC]$. Ce qui montre que les trois médiatrices se coupent en Ω.
2. Soit $\mathcal{C}$ cercle de Ω et de rayon $r = \Omega A = \Omega B = \Omega C$. Si (ABC) est invariant par une isométrie s, alors $\mathcal{C}$ est invariant par s. On a vu en cours que s est alors une rotation de centre Ω ou une réflexion d'axe passant par Ω. En particulier, Ω est un point fixe. De plus, $\Omega s(A) = \Omega s(B) = \Omega s(C) = r$ montre que l'image d'un sommet est un sommet.
   (a) Si $s(A) = A$, alors s est soit une réflexion τ d'axe (ΩA) soit l'identité.
   (b) Si $s(A) = B$, alors s est soit la rotation r de centre Ω et d'angle $\dfrac{2\pi}{3}$ (on oriente le plan de sorte que l'angle soit correctement orienté) ; soit $\sigma^{-1} \circ s$ admet A pour point fixe et n'est pas l'identité, donc $s = r \circ \tau$.
   (c) Si $S(A) = C$, alors s est soit la rotation r^2 soit $r^{-2} \circ s = \tau$ et donc $s = r^2 \circ \tau$.
3. On vérifie facilement que r et τ laissent bien invariant (ABC) et $G = \{id, r, r^2, \tau, r \circ \tau, r^2 \circ \tau\}$. On remarque que $r^3 = id$. De plus, $\tau \circ r(A) = s(B) = C$ et $r \circ \tau \circ r(A) = A$, donc $r \circ \tau \circ r$ est soit l'identité (impossible car sinon $\tau = id$) soit τ et donc $\tau \circ r = r^2 \circ \tau \neq r \circ \tau$. Le groupe n'est pas abélien.
4. On remarque qu'une isométrie de G est uniquement déterminée par l'image des sommets A, B et C. On construit un isomorphisme entre G et S_3 de la manière suivante : on pose $\alpha(A) = 1$, $\alpha(B) = 2$ et $\alpha(C) = 3$ puis
$$\varphi : G \to S_3,\ s \mapsto \begin{pmatrix} 1 & 2 & 3 \\ \alpha(s(A)) & \alpha(s(B)) & \alpha(s(C)) \end{pmatrix}.$$
   L'application est bijective, il reste à vérifier que c'est un morphisme, ce qui ne ose pas de problème.

Exercice 7 (Le groupe dihedral, \二面体群\)**.** Soit $\mathcal{P}$ le plan euclidien rapporté au repère $(O, \overrightarrow{i}, \overrightarrow{j})$ et $n \in \mathbb{N}$, $n \geq 3$. Pour tout $k \in [\![0, n-1]\!]$, on pose $z_k = \exp\left(\dfrac{2ik\pi}{n}\right)$ et A_k le point du plan euclidien $\mathcal{P}$ d'affixe z_k. On s'intéresse au groupe D_n des isométries du plan qui conservent $\mathcal{A} = \{A_0, \cdots, A_{n-1}\}$.

1. Montrer que si $\varphi \in D_n$, alors $\varphi(O) = O$.
2. Trouver toutes les rotations appartenant à D_n et montrer que l'ensemble des rotations forme un sous-groupe cyclique de D_n.

3. Vérifier que la réflexion s d'axe (Ox) appartient à D_n.
4. Décrire les éléments de D_n.
5. Le groupe D_n est-il abélien ?

---

1. Pour tout $k \in [\![0, n-1]\!]$, $OA_k = 1$. Donc O appartient à toutes les médiatrices des segments $[A_k A_{k'}]$ pour $k \neq k'$. Si $s \in D_n$, on a encore $s(O)$ appartient à toutes les médiatrices des segments $[A_k A_{k'}]$ pour $k \neq k'$. On en déduit que $S(O) = 0$.
2. Toute rotation de D_n est donc de centre O et si r est la rotation de centre 0 d'angle $\dfrac{2i\pi}{n}$, alors la rotation r^k, vérifie $r^k(A_0) = A_k$. On en déduit que $\{id, r, \cdots, r^{n-1}\}$ est un ensemble de n rotations qui conservent $\mathcal{A}$.
   De plus, si s est une rotation de D_n telle que $s(A_0) = A_k$, alors $r^{-k} \circ s(A_0) = A_0$ est une rotation avec au moins deux points fixes, c'est l'identité donc $s = r^k$.
   Nous avons donc montré que $\{id, r, \cdots, r^{n-1}\}$ est l'ensemble des rotations qui conservent $\mathcal{A}$, c'est un sous-groupe cyclique engendré par r.
3. En termes d'affixes, s correspond à l'application $z \mapsto \bar{z}$ et z_k étant les racines n-ième de l'unité, on a bien $\bar{z}_k \in \mathcal{A}$. Donc $s \in D_n$.
4. Si $t \in D_n$ avec $t(A_0) = A_k$, alors $r^{-k} \circ t(A_0) = A_0$ donc $r^{-k} \circ t$ est soit l'identité et ainsi $t = r^k$, soit la réflexion d'axe (OA_0), c'est-à-dire s et ainsi $t = r^k \circ t$.
   On en déduit que $D_n = \{id, r, \cdots, r^{n-1}, s, \cdots, r^{n-1} \circ s\}$. C'est un groupe d'ordre $2n$.
5. $s \circ r(A_0) = A_{n-1}$ d'où $s \circ r = r^{n-1} \circ s$ et D_n n'est pas commutatif pour $n \geq 3$.

Il existe donc des groupes non abélien dordre $2n$ pour tout $n \geq 3$. le cas impair est beaucoup plus délicat. Nous avons déjà vu que tout groupe d'ordre p premier est cyclique (donc abélien). On peut vérifier qu'il en est de même si G d'ordre pq avec p et q premiers : G est encore cyclique.