Feuille de TD n° 6

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

7 décembre 2020

Hors TD. Si vous souhaitez vérifier vos connaissances.

1. Calculer $\operatorname{pgcd}(33, 28)$ par l'algorithme d'Euclide. En déduire $\operatorname{ppcm}(33, 28)$.
2. Décomposer 1260 en produit de facteurs premiers. En déduire $\operatorname{pgcd}(1260, 55)$ et $\operatorname{ppcm}(1260, 55)$.
3. Vrai ou faux : Soit $(a, b) \in \mathbb{Z}^2$.
   (a) Si d divise ab et d ne divise pas a alors d divise b.
   (b) $d = \operatorname{pgcd}(a, b)$ si et seulement s'il existe $(u, v) \in \mathbb{Z}^2$ tel que $d = au + bv$.
   (c) Un entier est divisible par 42 si et seulement s'il est divisible par 6 et 7.
   (d) Un entier est divisible par 48 si et seulement s'il est divisible par 6 et 8.

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 $(x, y) \in \mathbb{N}^2$
$$x^2 = y^2 + \operatorname{pgcd}(x, y) + 2.$$
5. Déterminer les nombres premiers p tels que $p + 2$ et $p + 4$ soient premiers.

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 $\sqrt{3} \notin \mathbb{Q}$.

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 $5x \equiv 3 \bmod 28$.

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.

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. $\begin{cases} x \equiv 3 \bmod 17 \\ x \equiv 4 \bmod 11 \\ x \equiv 5 \bmod 6 \end{cases}$.

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 isomorphe à un groupe que nous avons déjà rencontré.

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 ?

Indications

Exercice 1

1. Regarder $(3^5)^n + (5^5)^n \times 5 + (4^5)^n \times 4^2$ modulo 11.
2. Regarder les puissances de 2 modulo 7 :
   $2^0 \equiv ?$ mod 7, $2^1 \equiv ?$ mod 7, etc.
   En déduire par une division euclidienne bien choisie, à quoi est congru 2^{65362} modulo 7.
3. Regarder à quoi est congru $n^2 + 1$ modulo 3 selon que $n \equiv 0$ mod 3, $n \equiv 1$ mod 3, $n \equiv 2$ mod 3.
4. Poser $d = \text{pgcd}(x, y)$ et utiliser le fait qu'il existe x', y' tels que $x = dx'$, $y = dy'$ et $\text{pgcd}(x', y') = 1$. En déduire que d divise 2 puis déterminer les valeurs possibles pour x' et y' en fonction des valeurs possibles pour d.
5. Regarder à quoi sont congrus $p + 2$ et $p + 4$ modulo 3 selon que p est congru à 0, 1 ou 2 modulo 3. Conclure.

Exercice 2

Supposer que $\sqrt{n} \in \mathbb{Q}$. Alors $\sqrt{n} = \dfrac{p}{q}$ avec p et q premiers entre eux. En déduire que $q^2 n = p^2$. ...

Exercices 3 à 5 Applications du cours 12.