Arithmétique dans $\mathbb{Z}$ - Exercices

Exercice 1.

1. Calculer PGCD$(888, 264)$ et PGCD$(729, 54)$.
2. Déterminer les décompositions en facteurs premiers de 660 et 192. En déduire le pgcd et le ppcm de ces deux entiers.
3. Soit $n \in \mathbb{N}$, $a = 2n+3$ et $b = 5n-2$. Déterminer PGCD(a, b) en fonction de n.
4. Déterminer le nombre de diviseurs positifs de 10!.
5. Déterminer tous les entiers naturels x, y avec $x \leq y$ et PGCD$(x, y) = 18$ et PPCM$(x, y) = 252$.

Exercice 2 (Petit théorème de Fermat). Soit p un nombre premier.

1. Soit $k \in [\![1, p-1]\!]$. Montrer que p divise $\binom{p}{k}$.
2. En déduire que p divise $n^p - n$ pour tout entier relatif n.
3. En déduire que si p ne divise pas n, alors p divise $n^{p-1} - 1$.

Exercice 3.

1. Soit $n \geq 2$ un entier. Déterminer le reste de la division euclidienne de $n^2 + 3n + 1$ par $n - 1$.
2. Déterminer les entier naturels n tels que $n + 1 | n^2 + 1$.
3. Montrer par récurrence sur $n \in \mathbb{N}$ que 7 divise $3^{2n+1} + 2^{n+2}$.

Exercice 4. Soit $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$. On dit que a est **congru à** b **modulo** n si $n|(b-a)$. On note alors $a \equiv b\,[n]$.

1. Montrer que : $\forall (a, b) \in \mathbb{Z}^2$, $a \equiv b\,[n] \iff b \equiv a\,[n]$.
2. Montrer que : $\forall (a, b, c) \in \mathbb{Z}^3$, $(a \equiv b\,[n]$ et $b \equiv c\,[n]) \Rightarrow a \equiv c\,[n]$.
3. Montrer que : $\forall (a, b, c, d) \in \mathbb{Z}^4$, $(a \equiv b\,[n]$ et $c \equiv d\,[n]) \Rightarrow a + c \equiv b + d\,[n]$.
4. Montrer que : $\forall (a, b, c, d) \in \mathbb{Z}^4$, $(a \equiv b\,[n]$ et $c \equiv d\,[n]) \Rightarrow ac \equiv bd\,[n]$.
5. Montrer que : $\forall (a, b, k) \in \mathbb{Z}^2 \times \mathbb{N}$, $a \equiv b\,[n] \Rightarrow a^k \equiv b^k\,[n]$.
6. Soit $m \in \mathbb{N}$. On note s la somme de ses chiffres. Montrer que $m \equiv s\,[3]$. Comment peut-on tester si un entier est divisible par 3 ?
7. Montrer qu'un nombre est divisible par 11 si et seulement si la différence entre la somme des ses chiffres de rangs pairs et ceux de rangs impairs est divisible par 11.

Exercice 5. Pour tout $n \in \mathbb{N}^*$, on pose $z_n = (1+2i)^n$ et on note $a_n = \mathrm{Re}(z_n)$ et $b_n = \mathrm{Im}(z_n)$.

1. Montrer que pour tout $n \geq 2$, $b_{n+1} = 2b_n - 5b_{n-1}$.
2. En déduire que pour tout $n \in \mathbb{N}^*$, b_n est un entier qui n'est pas divisible par 5.
3. Justifier alors que pour tout $n \in \mathbb{N}^*$, $z_n \notin \mathbb{R}$.

Indications - Solutions

Exercice 1 :

1. $\mathrm{PGCD}(888,264)=24$ et $\mathrm{PGCD}(729,54)=27$.
2. $660=2^2\cdot3\cdot5\cdot11$ et $192=2^6\cdot3$. $\mathrm{PGCD}(660,192)=2^2\cdot3=12$ et $\mathrm{PPCM}(660,192)=2^6\cdot3\cdot5\cdot11=10560$.
3. $\mathrm{PGCD}(a,b)=\mathrm{PGCD}(a,b-2a)=\mathrm{PGCD}(2n+3,n-8)=\mathrm{PGCD}(2n+3-2(n-8),n-8)=\mathrm{PGCD}(19,n-8)$. Comme 19 est premier, ce pgcd vaut soit 19 si $n-8$ est divisible par 19 et 1 sinon.
4. On compte les diviseurs positifs. $10!=2^8\cdot3^4\cdot5^2\cdot7$. Un diviseur correspond au choix de quatre puissances pour chacun des premiers 2, 3, 5 et 7. On a donc autant de diviseurs que d'éléments de $[\![0,8]\!]\times[\![0,4]\!]\times[\![0,2]\!]\times[\![0,1]\!]$: il y a 270 diviseurs.
5. On a $18=2\cdot3^2$ et $252=2^2\cdot3^2\cdot7$. Les deux entiers sont des multiples de 18 et divisent 252 : on a 18, 36, 126 et 252. On obtient $(18,252)$, $(36,126)$ comme solutions.

Exercice 2 :

1. On a $\binom{p}{k}=\dfrac{p!}{k!(p-k)!}=\dfrac{p(p-1)\cdots(p-k+1)}{k!}$. Donc p divise $k!\binom{p}{k}$. Or si $k!=\prod p_i^{\alpha_i}$ et $\binom{p}{k}=\prod q_j^{\beta_j}$ sont les décompositions en facteurs premiers, par unicité, $k!\binom{p}{k}=\prod p_i^{\alpha_i}\prod q_j^{\beta_j}$ est la décomposition en facteurs premiers. Or, p apparaît dans la décomposition en facteurs premiers de $k!\binom{p}{k}$. Puis, pour chaque entier $j\in[\![2,k]\!]$, p n'apparaît pas dans la décomposition en facteurs premiers de j. Par unicité de la décomposition, p apparaît donc dans la DFP de $\binom{p}{k}$. Donc p divise $\binom{p}{k}$.
2. On montre par récurrence sur $n\geq0$.
   - Initialisation : p divise bien 0^p-0.
   - Hérédité : soit $n\geq0$. On suppose que p divise n^p-n. Alors $(n+1)^p-(n+1)=n^p+\binom{p}{p-1}n^{p-1}+\cdots+\binom{p}{1}n+1-n-1=n^p-n+\binom{p}{p-1}n^{p-1}+\cdots+\binom{p}{1}n$. D'après la question précédente, p divise tous les coefficients binomiaux, donc par HR, p divise toute la somme précédente. Ainsi, p divise $(n+1)^p-(n+1)$.

   On conclut par récurrence.
3. Supposons que p ne divise pas n. Alors p divise $n(n^{p-1}-1)$, donc p divise $n^{p-1}-1$ d'après Euclide.

Exercice 3 :

1. On a $n^2+3n+1=n(n-1)+4n+1=n(n-1)+4(n-1)+5=(n+4)(n-1)+5$. Si $n>6$, alors $n-1>5$, donc le reste cherché vaut 5. Traitons les cas $n=2,3,4$ et 5 à part :
   - si $n=2$, $n^2+3n+1=11$ et $n-1=1$, donc le reste vaut 0 ;
   - si $n=3$, $n^2+3n+1=19$ et $n-1=2$, donc le reste vaut 1 ;
   - si $n=4$, $n^2+3n+1=29$ et $n-1=3$, donc le reste vaut 2 ;
   - si $n=5$, $n^2+3n+1=41$ et $n-1=4$, donc le reste vaut 1.
2. On a $n^2+1=n(n+1)-n+1=n(n+1)-(n+1)+2=(n+1)(n-1)+2$. Donc, si $n+1>2$, $n+1$ ne divise pas n^2+1 car le reste de la DE vaut 2. On vérifie facilement que pour $n=0$ et $n=1$, $n+1|n^2+1$.

Exercice 4 :

1. Soit $(a,b)\in\mathbb{Z}^2$. $a\equiv b\,[n]\iff n|b-a\iff n|a-b\iff b\equiv a\,[n]$.
2. Soit $(a,b,c)\in\mathbb{Z}^3$. Supposons que $a\equiv b\,[n]$ et $b\equiv c\,[n]$. Alors $n|(b-a)$ et $n|(b-c)$, donc $n|((b-a)-(b-c))$ et $n|(c-a)$. Donc $a\equiv c\,[n]$.
3. Soit $(a,b,c,d)\in\mathbb{Z}^4$. Supposons que $a\equiv b\,[n]$ et $c\equiv d\,[n]$. Alors $n|(b-a)$ et $n|(d-c)$, donc $n|(b-a+d-c)$, et $n|((b+d)-(a+c))$. Ainsi, $a+c\equiv b+d\,[n]$.
4. Soit $(a,b,c,d)\in\mathbb{Z}^4$. Supposons que $a\equiv b\,[n]$ et $c\equiv d\,[n]$. Alors $n|(b-a)$ et $n|(d-c)$. Or $bd-ac=b(d-c)+bc-ac=b(d-c)+(b-a)c$. Donc $n|(bd-ac)$ et $ac\equiv bd\,[n]$.
5. On procède par récurrence en utilisant la propriété précédente.
6. Notons $m=\overline{a_na_{n-1}\dots a_1a_0}$ les chiffres de m. On a donc $m=a_0+a_1\times10+a_2\times10^2+\cdots+a_n\times10^n$. Or comme $10\equiv1\,[3]$, on a pour tout $k\in\mathbb{N}$, $10^k\equiv1\,[3]$. Ainsi, $m\equiv a_0+a_1+\cdots+a_m\,[3]$. Ainsi, m est divisible par 3 ssi la somme de ses chiffres l'est.

7. On a $10 \equiv -1\,[11]$, donc $10^{2k} \equiv 1\,[11]$ et $10^{2k+1} \equiv -1\,[11]$ pour tout entier $k \in \mathbb{N}$. On reprend les notations de la question précédente : $m \equiv a_0 + a_2 + \cdots - a_1 - a_3 \cdots\,[11]$. On trouve bien la condition donnée dans l'énoncé.

Exercice 5 :

1. Soit $n \geq 2$. $z_{n+1} = (1+2i)z_n = z_n + 2iz_n$, donc $a_{n+1} + ib_{n+1} = a_n + ib_n + 2ia_n - 2b_n$. Ainsi, $b_{n+1} = b_n + 2a_n$. Or, de même, $a_n + ib_n = a_{n-1} - 2b_{n-1} + i(b_{n-1} + 2a_{n-1})$, donc $b_{n+1} = b_n + 2a_{n-1} - 4b_{n-1}$ et $b_n = b_{n-1} + 2a_{n-1}$, ce qui donne $2a_{n-1} = b_n - b_{n-1}$. En conclusion, $b_{n+1} = b_n + b_n - b_{n-1} - 4b_{n-1} = 2b_n - 5b_{n-1}$.
2. On procède par récurrence double :
   - Initalisation : $b_1 = 2$ et $b_2 = 4$ qui sont des entiers non divisibles par 5.
   - Hérédité : soit $n \geq 2$ et supposons que b_n et b_{n-1} sont des entiers non divisibles par 5. Alors $b_{n+1} = 2b_n - 5b_{n-1}$ est bien un entier. De plus, comme 5 est premier et ne divise ni 2 ni b_n, 5 ne divise pas $2b_n$. Comme $2b_n = b_{n+1} + 5b_{n-1}$, 5 ne peut pas diviser b_{n+1}.
3. Pour tout $n \in \mathbb{N}^*$, b_n est un entier qui n'est pas divisible par 5. En particulier, $b_n \neq 0$ (qui est divisible par 5). Donc $z_n \notin \mathbb{R}$.