

TD 22 – Arithmétique des entiers (Correction)

1 Divisibilité

dans

$\mathbb{N}$

Exercice 1 – Divisibilité. Dire si les relations de divisibilité suivantes sont vraies ou fausses.

a) $2 \mid 124$

b) $7 \mid 22$

c) $11 \mid 121$

d) $13 \mid 65$

a) $2 \mid 124$ car $124 = 2 \times 62$

b) $7 \mid 22$

c) $11 \mid 121$ car $121 = 11 \times 11$

d) $13 \mid 65$ car $65 = 13 \times 5$

Exercice 2 – Diviseurs. Donner la liste des diviseurs de 42.

1, 2, 3, 6, 7, 14, 21, 42

Exercice 3 – Divisibilité. Déterminer les entiers $n \in \mathbb{N}$ tels que $(n-1)|(n+11)$.

Soit $n \in \mathbb{N}$. On a

$$n+11 = n-1+12.$$

Donc

$$\begin{aligned}(n-1)|(n+11) &\iff (n-1)|12 \\ &\iff n-1 \in \{1, 2, 3, 4, 6, 12\} \\ &\iff n \in \{2, 3, 4, 5, 7, 13\}\end{aligned}$$

Donc

$$(n-1)|(n+11) \iff n \in \{2, 3, 4, 5, 7, 13\}$$

Exercice 4 – Montrer par récurrence que pour tout entier $n \geq 0$, le nombre $5^n - 1$ est divisible par 4.

On prouve le résultat par **récurrence**. Notons, pour tout $n \geq 1$, par $\mathcal{P}(n)$ la propriété suivante

$\mathcal{P}(n)$: « Le nombre $5^n - 1$ est divisible par 4 »

- **Initialisation** : Montrons que la propriété $\mathcal{P}(1)$ est vraie, c'est-à-dire que l'on cherche à montrer que

$$5^1 - 1 \text{ est divisible par 4 .}$$

On a $5^1 - 1 = 4 = 4 \times 1$. Donc $5^1 - 1$ est divisible par 4. Donc $\mathcal{P}(1)$ est vraie.

- **Hérédité** : Soit $n \geq 1$. On suppose que la propriété $\mathcal{P}(n)$ est vraie, c'est-à-dire que l'on suppose que

$$5^n - 1 \text{ est divisible par 4}$$

Montrons que la propriété $\mathcal{P}(n+1)$ est vraie, c'est-à-dire que

$$5^{n+1} - 1 \text{ est divisible par 4}$$

Par hypothèse de récurrence, $5^n - 1$ est divisible par 4 donc il existe un entier k tel que $5^n - 1 = 4 \times k$. Donc

$$\begin{aligned} 5^{n+1} - 1 &= 5 \times 5^n - 1 \\ &= 5 \times (4k + 1) - 1 \\ &= 5 \times 4k + 5 - 1 \\ &= 5 \times 4k + 4 \\ &= 4 \times (5k + 1) \end{aligned}$$

Donc $5^{n+1} - 1$ est divisible par 4. Donc $\mathcal{P}(n+1)$ est vraie.

- **Conclusion** : D'après le principe de récurrence, on a démontré que, pour tout $n \geq 1$, la propriété $\mathcal{P}(n)$ est vraie, c'est-à-dire

$\forall n \in \mathbb{N}, \quad 4 \mid 5^n - 1$
--

Exercice 5 – Montrer que, pour tout $n \in \mathbb{N}^*$, $3 \mid (7^n - 4^n)$ sans faire une récurrence.

Pour tout $n \in \mathbb{N}$,

$$7^n - 4^n = (7 - 4) \sum_{k=0}^{n-1} 7^k 4^{n-k-1} = 3 \underbrace{\sum_{k=0}^{n-1} 7^k 4^{n-k-1}}_{\in \mathbb{N}}.$$

Donc 3 divise $7^n - 4^n$.

Exercice 6 – Démontrer les propriétés suivantes.

1. Si $a \mid b$ et $b \mid c$ alors $a \mid c$.
2. Si $a \mid b$ et $b \mid a$ alors $a = b$.
3. Si $a \mid b$ et $c \mid d$ alors $ac \mid bd$.
4. Si $a \mid b$ alors pour tout $n \in \mathbb{N}$, $a^n \mid b^n$.
5. Si $a \mid b$ alors $a \mid bc$.
6. Si $ab \mid c$ alors $a \mid c$ et $b \mid c$.

1. Supposons que $a \mid b$ et $b \mid c$. Alors il existe $k_1 \in \mathbb{N}$ et $k_2 \in \mathbb{N}$ tels que $b = ak_1$ et $c = k_2b$. Donc $c = k_2b = k_2k_1a$ et $k_2k_1 \in \mathbb{N}$ donc $a \mid c$.
2. Supposons que $a \mid b$ et $b \mid a$. Si $b = 0$ alors $0 \mid a$ donc $a = 0$, et $a = b = 0$. Supposons alors $b \neq 0$. Alors $a \leq b$ et $b \leq a$ d'après la propriété précédente. Donc $a = b$.
3. Supposons que $a \mid b$ et $c \mid d$. Alors il existe $k_1 \in \mathbb{N}$ tel que $b = ak_1$ et il existe $k_2 \in \mathbb{N}$ tel que $d = ck_2$. Donc $bd = ack_1k_2$ et $k_1k_2 \in \mathbb{N}$. Donc $ac \mid bd$.
4. Par récurrence en utilisant le résultat précédent.
5. Supposons que $a \mid b$. Alors il existe $k \in \mathbb{N}$ tel que $b = ka$. Donc $bc = kca$ et $kc \in \mathbb{N}$. Donc $a \mid bc$.
6. Supposons que $ab \mid c$. Alors il existe $k \in \mathbb{N}$ tel que $c = kab$. Comme $ka \in \mathbb{N}$, $b \mid c$ et comme $kb \in \mathbb{N}$, $a \mid c$.

2 Division

euclidienne

Exercice 7 – Division euclidienne. Effectuer la division euclidienne de a par b pour

a) $a = 473$ et $b = 6$

$$473 = 6 \times 78 + 5$$

b) $a = 784$ et $b = 15$

$$784 = 15 \times 52 + 4$$

c) $a = 578$ et $b = 25$

$$578 = 25 \times 23 + 3$$

Exercice 8 – Soit $n \in \mathbb{N}$. On effectue la division euclidienne de n par 45. On trouve que le reste est égal au carré du quotient. Quelles sont les valeurs possibles de n ?

Soit $n \in \mathbb{N}$. Notons q le quotient de la division euclidienne de n par 45. D'après l'énoncé, on a alors

$$n = 45q + q^2 \quad \text{avec} \quad 0 \leq q^2 \leq 44$$

Comme $0 \leq q^2 \leq 44$, alors $q \in \{0, 1, 2, 3, 4, 5, 6\}$.

- Pour $q = 0$, on obtient $n = 0$.
- Pour $q = 1$, on obtient $n = 46$.
- Pour $q = 2$, on obtient $n = 94$.
- Pour $q = 3$, on obtient $n = 144$.
- Pour $q = 4$, on obtient $n = 196$.
- Pour $q = 5$, on obtient $n = 250$.
- Pour $q = 6$, on obtient $n = 306$.

Donc l'ensemble des valeurs de n possibles est

$$\{0, 46, 94, 144, 196, 250, 306\}$$

Exercice 9 – Soit $(a, b) \in \mathbb{N}^2$ tel que $0 < a < b$. On effectue les divisions euclidiennes de a par $b - a$ et de b par $b - a$. Comparer les restes et les quotients obtenus.

Notons q et r respectivement le quotient et le reste dans la division euclidienne de a par $b - a$.

On a alors

$$a = q(b - a) + r \quad \text{avec } 0 \leq r < b - a$$

Alors

$$b = a + b - a = q(b - a) + r + b - a = (q + 1)(b - a) + r \quad \text{avec } 0 \leq r < b - a$$

Donc le quotient et le reste dans la division euclidienne de b par $b - a$ sont respectivement

$$\boxed{q + 1} \text{ et } \boxed{r}.$$

3 PGCD,

PPCM

Exercice 10 – Calculer de tête les PCGD et PPCM suivants.

a) $\text{PCGD}(3, 12)$

b) $\text{PPCM}(3, 12)$

c) $\text{PCGD}(10, 8)$

d) $\text{PPCM}(10, 8)$

Exercice 11 – Calcul de PGCD avec l’algorithme d’Euclide. Calculer le PGCD de a et b pour :

a) $a = 255$ et $b = 141$

Algorithme d’Euclide et on ne garde que le dernier reste non nul

$$255 = 141 \times 1 + 114$$

$$141 = 114 \times 1 + 27$$

$$114 = 27 \times 4 + 6$$

$$27 = 6 \times 4 + 3$$

$$6 = 3 \times 2 + 0$$

Donc, $\boxed{\text{PGCD}(255, 141) = 3.}$

b) $a = 401$ et $b = 130$

Algorithme d’Euclide et on ne garde que le dernier reste non nul

$$401 = 130 \times 3 + 11$$

$$130 = 11 \times 11 + 9$$

$$11 = 9 \times 1 + 2$$

$$9 = 2 \times 4 + 1$$

$$4 = 4 \times 1 + 0$$

Donc, $\boxed{\text{PGCD}(401, 130) = 1.}$

c) $a = 3465$ et $b = 600$

Algorithme d’Euclide et on ne garde que le dernier reste non nul

$$3465 = 600 \times 5 + 465$$

$$600 = 465 \times 1 + 135$$

$$465 = 135 \times 3 + 60$$

$$135 = 60 \times 2 + 15$$

$$60 = 15 \times 4 + 0$$

Donc, $\boxed{\text{PGCD}(3465, 600) = 15.}$

Exercice 12 – Nombres premiers entre eux. Dire si les nombres suivants sont premiers entre eux.

a) 8 et 24

b) 3 et 12

c) 11 et 24

d) 401 et 130

Exercice 13 – Calcul de PPCM. On pose $a = 720$ et $b = 252$.

1. Calculer le PGCD de a et b .

$$\text{PGCD}(a, b) = \boxed{36}$$

2. En déduire le PPCM de a et b .

On sait que

$$\text{PGCD}(a, b) = 36$$

Or,

$$\text{PGCD}(a, b) \times \text{PPCM}(a, b) = a \times b$$

On en déduit que

$$\text{PPCM}(a, b) = \frac{ab}{\text{PGCD}(a, b)} = \boxed{5040}$$

3. En déduire la valeur de

$$\frac{1}{a} + \frac{1}{b}$$

On a,

$$\frac{1}{720} + \frac{1}{252} = \frac{7+20}{5040} = \frac{27}{5040} = \boxed{\frac{3}{560}}$$

Exercice 14 – Soit $(a, b) \in \mathbb{N}^*$. Montrer que $\text{PCGD}(a, b) = \text{PCGD}(a, b - a)$. On pourra montrer que les deux entiers se divisent mutuellement.

Notons $d = \text{PCGD}(a, b)$ et $d' = \text{PCGD}(a, b - a)$.

- Montrons que $d|d'$. On a $d|a$ et $d|b$ donc $d|(b - a)$. Donc, puisque $d|a$ et $d|(b - a)$, on a $d|d'$ car le pgcd est le plus grand diviseur commun au sens de la division.
- Montrons que $d'|d$. On a $d'|a$ et $d'|(b - a)$ donc $d'|(a + (b - a)) = b$. Donc $d'|d$.

Ainsi $d|d'$ et $d'|d$ et $d, d' \in \mathbb{N}$. Donc $\boxed{d = d'}$

Exercice 15 – Déterminer tous les entiers naturels $(a, b) \in (\mathbb{N}^*)^2$ tels que

$$\text{PCGD}(a, b) = 18 \quad \text{et} \quad a + b = 360.$$

On pourra commencer par se ramener à des nombres premiers entre eux.

Raisonnons par analyse-synthèse.

- *Analyse* : soit $(a, b) \in (\mathbb{N}^*)^2$ tel que $a \wedge b = 18$ et $a + b = 360$. Alors il existe $a', b' \in \mathbb{N}^*$ tels que $a' \wedge b' = 1$ et $a = 18a', b = 18b'$. Donc $a' + b' = 20$. On énumère alors les cas possibles :
 - $a' = 1$ et $b' = 19$ ce qui conduit à

$a = 18, b = 342$

 - $a' = 3$ et $b' = 17$ ce qui conduit à

$a = 54, b = 306$

 - $a' = 7$ et $b' = 13$ ce qui conduit à

$a = 126, b = 234$

 - $a' = 9$ et $b' = 11$ ce qui conduit à

$a = 162, b = 198$

 - $a' = 11$ et $b' = 9$ ce qui conduit à

$a = 198, b = 162$

 - $a' = 13$ et $b' = 7$ ce qui conduit à

$a = 234, b = 126$

 - $a' = 17$ et $b' = 3$ ce qui conduit à

$a = 306, b = 54$

 - $a' = 19$ et $b' = 1$ ce qui conduit à

$a = 342, b = 18$

- On vérifie que les couples donnés plus haut sont bien des solutions.

4 Nombres

premiers

Exercice 16 – Montrer que 167 est un nombre premier.

$12^2 = 144 < 167 < 169 = 13^2$. Donc $12 < \sqrt{167} < 13$. Donc les nombres premiers inférieurs à $\sqrt{167}$ sont 2, 3, 5, 7, 11. Or, aucun de ces nombres ne divisent 167. Donc 167 est premier.

Exercice 17 – Décomposition en facteurs premiers.

1. Décomposer en produit de facteurs premiers les nombres suivants.

a) 63

b) 70

c) 140

d) 280

On obtient,

a) $63 = 3^2 \times 7$

b) $70 = 2 \times 5 \times 7$

c) $140 = 2^2 \times 5 \times 7$

d) $280 = 2^3 \times 5 \times 7$

2. En déduire la liste des diviseurs de 63.

On a

$$63 = 3^2 \times 7$$

Donc les diviseurs de 63 sont

a) $3^0 \times 7^0 = 1$

b) $3^0 \times 7^1 = 7$

c) $3^1 \times 7^0 = 3$

d) $3^1 \times 7^1 = 21$

e) $3^2 \times 7^0 = 9$

f) $3^2 \times 7^1 = 63$

3. En déduire les valeurs suivantes.

a) PGCD(63, 70)

b) PPCM(63, 70)

c) PGCD(140, 63)

d) PPCM(140, 63)

On obtient,

a) $\text{PGCD}(63, 70) = 2^0 \times 3^0 \times 5^0 \times 7 = 7$

b) $\text{PPCM}(63, 70) = 2^1 \times 3^2 \times 5^1 \times 7 = 630$

c) $\text{PGCD}(140, 63) = 7$

d) $\text{PPCM}(140, 63) = 1260$

Exercice 18 – Crible d’Eratosthène. On peut dresser la liste des nombres premiers $p \leq n$ de manière algorithmique en utilisant le crible d’Eratosthène. Pour cela, on peut écrire tous les nombres compris entre 2 à n , puis procéder comme suit:

1. le plus petit nombre est 2 qui est premier, et tous les multiples stricts de 2 ne sont pas premiers, on élimine alors tous ces multiples,
2. le premier nombre restant est 3, qui est donc premier, et tous les multiples stricts de 3 ne sont pas premiers, on élimine alors tous ces multiples,
3. le premier nombre restant est 5, qui est donc premier, et tous les multiples stricts de 5 ne sont pas premiers, on élimine alors tous ces multiples,
4. on poursuit ainsi jusqu’à tomber sur un nombre supérieur à $\sqrt{n}$.

Les entiers non élimés sont alors exactement les nombres premiers inférieurs à n puisque les entiers non premiers inférieurs à n possèdent un diviseur premier inférieur à $\sqrt{n}$ et ont donc été éliminés. Appliquer l’algorithme pour déterminer tous les premiers compris entre 1 et 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Exercice 19 – Soit $n \geq 2$. Montrer qu'aucun des entiers compris entre $n! + 2$ et $n! + n$ n'est premier. Comment obtenir n entiers consécutifs non premiers ?

- Soit m un entier compris entre $n! + 2$ et $n! + n$. Alors il existe $k \in \{2, \dots, n\}$ tel que $m = n! + k$. Alors $k|k$ et $k|n!$ car $n! = n \times (n-1) \times \dots \times k \times \dots \times 2 \times 1$. Donc $k|m$ et $k \geq 2$. Donc m n'est pas premier.
- Pour obtenir n entiers consécutifs non premier, on considère l'intervalle d'entiers

$$\{(n+1)! + 2, \dots, (n+1)! + n + 1\}$$