

Corrections d'exercices sur l'arithmétique des entiers

Correction de l'exercice 1

Soit (a, b) un couple d'entiers convenable.

Nécessairement, b est un entier strictement supérieur à 17.

En faisant le programme Python suivant :

```
1 def Couples() :  
2     L=[]  
3     b=18  
4     a=24*b+17  
5     while a<=500 :  
6         L.append([a,b])  
7         b+=1  
8         a=24*b+17  
9     return L  
10  
11 print(Couples())
```

on obtient tous les couples convenables :

$(449, 18)$, $(473, 20)$ et $(497, 20)$.

Correction de l'exercice 2

On suppose que la quantité :

$$A = \frac{p^2 + q^2}{p^2 - q^2} \text{ est un entier.}$$

Or, $A = 1 + \frac{2q^2}{(p-q)(p+q)}$. La quantité :

$$B = \frac{2q^2}{(p-q)(p+q)} \text{ est entière.}$$

Quitte à diviser le numérateur et le dénominateur par $p \wedge q$, on peut supposer que les entiers p et q sont premiers entre eux, ce que l'on suppose par la suite.

Soit d un diviseur premier éventuel commun aux entiers $p - q$ et $p + q$. Alors, l'entier d divise la somme égale à $2p$ et la différence égale à $-2q$, donc l'entier d est égal à 2.

Les entiers $p - q$ et q^2 d'une part et les entiers $p + q$ et q^2 d'autre part, sont premiers entre eux car si par exemple δ est un nombre premier divisant éventuellement les entiers $p - q$ et q^2 , alors δ divise q , puis p , ce qui est impossible.

Dans l'égalité :

$$2q^2 = B \times (p - q)(p + q),$$

par le théorème de Gauss, on peut écrire que l'entier $p + q$ divise 2, ce qui n'est pas possible car $p + q > 2$.

Le quotient initial n'était pas un nombre entier.

Correction de l'exercice 3

Soit $(x, y) \in \mathbb{Z}^2$, une solution éventuelle à cette équation.

On en déduit en passant dans $\mathbb{Z}/5\mathbb{Z}$:

$$-2y^2 = 4.$$

Or, l'élément $-2 = 3$ est inversible dans $\mathbb{Z}/5\mathbb{Z}$, d'inverse 2. En multipliant par 2, on obtient :

$$y^2 = 8 = 3.$$

Or, voici la liste des carrés dans $\mathbb{Z}/5\mathbb{Z}$:

0	1	2	3	4
0	1	4	4	1

L'élément 3 n'est jamais un carré dans $\mathbb{Z}/5\mathbb{Z}$: contradiction et l'équation de départ n'admet aucune solution.

Correction de l'exercice 4

On travaille dans $\mathbb{Z}/19\mathbb{Z}$ et on calcule les puissances de 2 dans cet anneau.

Voici ces puissances de 2 :

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

La suite $(2^k)_{k \in \mathbb{N}}$ est 18-périodique et l'ensemble des entiers k tels que :

$$2^k \equiv 16 \pmod{19},$$

forme l'ensemble $4 + 18\mathbb{Z}$.

Il suffit maintenant de vérifier que pour tout entier $n \in \mathbb{N}$,

$$2^{6n+2} \in 4 + 18\mathbb{Z}.$$

On peut encore raisonner dans $\mathbb{Z}/18\mathbb{Z}$ en considérant les puissances de 2, ce qui donne le tableau :

0	1	2	3	4	5	6	7
1	2	4	8	16	14	10	2

La suite $(2^k)_{k \in \mathbb{N}}$ est 6-périodique à partir du rang 1 et l'ensemble des entiers k tels que $2^k \equiv 4$ [18] forme l'ensemble $2 + 6\mathbb{Z}$.

On en déduit que pour tout $n \in \mathbb{N}$, comme $6n + 2 \in 2 + 6\mathbb{Z}$, alors $2^{6n+2} \equiv 4$ [18], puis $2^{2^{6n+2}+3} \equiv 16$ [19] et finalement ce qu'il faut.

Correction de l'exercice 5

On note $\mathcal{D} = \{d_0, \dots, d_p\}$ l'ensemble des diviseurs positifs de l'entier n .

En utilisant la bijection $\varphi : \begin{cases} \mathcal{D} & \longrightarrow \mathcal{D} \\ k & \longmapsto \frac{n}{k} \end{cases}$, alors :

$$\begin{aligned} \left(\prod_{k=0}^p d_k \right)^2 &= \left(\prod_{\delta \in \mathcal{D}} \delta \right) \times \left(\prod_{\delta \in \mathcal{D}} \varphi(\delta) \right) \\ &= \prod_{\delta \in \mathcal{D}} (\delta \times \varphi(\delta)) \\ &= \prod_{\delta \in \mathcal{D}} n \\ &= n^{p+1}. \end{aligned}$$

Correction de l'exercice 6

On fonctionne dans $\mathbb{Z}/10\mathbb{Z}$.

Voici les puissances de 7 modulo 10 : 1, 7, 9, 3, 1, ...

La suite $(7^k)_{k \in \mathbb{N}}$ est 4-périodique.

On calcule maintenant les puissances de 7 modulo 4 : 1, 3, 1, 3, ...

On calcule maintenant les puissances de 7 modulo 2 : 1, 1, ...

Conclusion, $7^7 \equiv 1$ [2], donc $7^{7^7} \equiv 3$ [4], puis $7^{7^{7^7}} \equiv 3$ [10]. Le chiffre des unités est 3.

On procède de la même façon. La suite $(3^k)_{k \in \mathbb{N}}$ est 4-périodique dans $\mathbb{Z}/10\mathbb{Z}$.

Or, $5 \equiv 1$ [4], donc $5^{7^9} \equiv 1$ [4] et le chiffre des unités de $3^{5^{7^9}}$ est 3.

Correction de l'exercice 7

1. Soit $n \geq 2$ un entier. Une somme S de n entiers impairs consécutifs est de la forme :

$$\begin{aligned}
 S &= \sum_{k=n_0+1}^{n_0+n} (2k+1) \\
 &= \sum_{k=n_0+1}^{n_0+n} ((k+1)^2 - k^2) \\
 &= (n_0+n+1)^2 - (n_0+1)^2 \\
 &= n \times (2n_0+n+2)
 \end{aligned}$$

qui n'est pas un nombre premier.

2. On calcule les cubes modulo 9, ce qui donne le tableau :

0	1	2	3	4	5	6	7	8
0	1	8	0	1	8	0	1	8

Il est alors clair que dans $\mathbb{Z}/9\mathbb{Z}$, la somme de trois cubes consécutifs vaut $0+1+8=0$.

Correction de l'exercice 9

On procède par analyse / synthèse.

• Phase d'analyse.

Soit (x, y) une solution éventuelle à cette équation.

On pose $d = x \wedge y$, qui est un entier divisant $x \vee y$ et y , donc l'entier d divise 9.

On en déduit que l'entier d vaut 1, 3 ou 9. On distingue les cas.

→ si $d = 1$, alors les entiers x et y sont premiers entre eux et l'équation devient puisque $x \vee y = xy$:

$$xy - y = 8 \text{ ou encore } (x-1)y = 8.$$

On en déduit que

$$(x, y) \in \{(9, 1), (5, 2), (3, 4), (2, 8), (-7, -1), (-3, -2), (-1, -4), (-7, 1)\}.$$

Le plus simple est de ne garder ici que les couples dont les composantes sont premières entre elles – début de la synthèse...

→ si $d = 3$, alors l'équation devient :

$$xy - 3y = 18, \text{ car } x \vee y = \frac{xy}{3}.$$

Là encore, on liste tous les couples possibles.

—→ si $d = 9$, alors l'équation devient :

$$xy = 9y$$

et les seuls couples possibles sont $(9, 9k)$, où k est un entier.

• Phase de synthèse

La phase de synthèse a un peu été abordée en phase d'analyse.

On trouve une infinité de solutions en répertoriant les solutions des trois cas énoncés ci-dessus.

Correction de l'exercice 10

Soit p un nombre premier.

On écrit $a \times b = N^2$, où N est un entier strictement positif.

On obtient :

$$2\nu_p(N) = \nu_p(a) + \nu_p(b).$$

Comme les entiers a et b sont premiers entre eux, alors l'une des deux évaluations $\nu_p(a)$ ou $\nu_p(b)$ est nulle et donc l'autre vaut $2\nu_p(N)$.

On vient de montrer que chaque p -valuation dans a ou dans b est un nombre pair, ce qui suffit à répondre à la question.

Correction de l'exercice 11

Pour tout entier $N \in \mathbb{N}^*$, on notera $\mathcal{D}_N$ l'ensemble des diviseurs strictement positifs de l'entier N .

Soient n et m deux entiers premiers entre eux.

On montre que l'application :

$$\varphi : \begin{cases} \mathcal{D}_n \times \mathcal{D}_m & \longrightarrow \mathcal{D}_{nm} \\ (d_1, d_2) & \longmapsto d_1 \times d_2 \end{cases}$$

est une bijection.

Premièrement, cette application est bien définie car si d_1 divise n et d_2 divise m , alors le produit $d_1 \times d_2$ divisera nm .

Ensuite, si $\varphi(d_1, d_2) = \varphi(d'_1, d'_2)$, on en déduit :

$$d_1 d_2 = d'_1 d'_2.$$

Les entiers d_1 et d'_1 divisent n et les entiers d_2 et d'_2 divisent m . Les entiers d_1 et d'_2 sont premiers entre eux. On peut utiliser le théorème de Gauss pour avoir la divisibilité de d'_1 par d_1 .

De même, d'_1 divise d_1 . Les entiers naturels d_1 et d'_1 se divisent mutuellement donc sont égaux.

On fait de même entre d_2 et d'_2 .

L'application φ est injective.

Soit D un diviseur de nm .

On écrit :

$$\begin{aligned} D &= \prod_{p \in \mathcal{P}} p^{\nu_p(D)} \\ &= \left(\prod_{p \in \mathcal{P} \text{ et } p \mid n} p^{\nu_p(D)} \right) \times \left(\prod_{p \in \mathcal{P} \text{ et } p \mid m} p^{\nu_p(D)} \right) \end{aligned}$$

cette décomposition étant valable car n et m n'admettent aucun diviseur premier en commun.

Il est alors clair qu'en notant d_1 le premier produit et d_2 le second, alors :

$$\varphi(d_1, d_2) = D.$$

L'application φ est bijective.

On conclut par un changement d'indices :

$$\begin{aligned} \sigma(nm) &= \sum_{D \in \mathcal{D}_{nm}} D \\ &= \sum_{(d_1, d_2) \in \mathcal{D}_n \times \mathcal{D}_m} d_1 \times d_2 \\ &= \left(\sum_{d_1 \in \mathcal{D}_n} d_1 \right) \times \left(\sum_{d_2 \in \mathcal{D}_m} d_2 \right) \\ &= \sigma(n) \times \sigma(m). \end{aligned}$$

Correction de l'exercice 12

1. On fixe un entier naturel n .

On montre par récurrence l'assertion :

$\mathcal{P}(m)$: « l'entier F_n divise $F_m - 2$ ».

• Si $m = n + 1$, alors :

$$\begin{aligned} F_{n+1} - 2 &= (2^{2^n})^2 - 1 \\ &= (F_n - 1)^2 - 1 \\ &= F_n \times (F_n - 2) \end{aligned}$$

On obtient bien l'assertion $\mathcal{P}(n + 1)$.

- Supposons l'assertion $\mathcal{P}(m)$ vérifiée pour un certain rang $m > n$.

Au rang suivant, on remarque que :

$$F_{m+1} - 2 = F_m \times (F_m - 2)$$

est bien un multiple de $F_m - 2$, donc de F_n .

2. Soient $n \neq m$ deux entiers naturels. Par exemple, $n < m$.

Soit p un nombre premier divisant éventuellement F_n et F_m . Alors, l'entier p divise $F_m - 2$ par la question précédente, puis divise $2 = F_m - (F_m - 2)$.

Cependant, l'entier F_n est impair : contradiction.

3. Pour tout $n \in \mathbb{N}$, on peut choisir un diviseur premier p_n de l'entier F_n .

Par la question précédente, l'application $n \mapsto p_n$ est injective : l'ensemble des nombres premiers est infini, par le principe des tiroirs.

Correction de l'exercice 14

Soit a et b dans $\mathbb{Z}$. Le plus simple est de travailler dans $\mathbb{Z}/17\mathbb{Z}$.

L'élément 2 est inversible dans $\mathbb{Z}/17\mathbb{Z}$, d'inverse 9. L'élément 9 est inversible dans $\mathbb{Z}/17\mathbb{Z}$.

Ainsi, $2a + 3b$ est nul dans $\mathbb{Z}/17\mathbb{Z}$ si et seulement si $9^2 \times (2a + 3b)$ également.

Or, $9^2 \times (2a + 3b) = 9a + 9 \times 10b = 9a + 5b$.

Ceci termine l'exercice.

Correction de l'exercice 15

1. Par contraposé, supposons l'entier n non premier. On écrit :

$$n = rs, \text{ avec } r \geq 2 \text{ et } s \geq 2.$$

Or,

$$2^n - 1 = 2^{rs} - 1 = 2^{rs} - 1^s \text{ est factorisable par } 2^r - 1 \text{ avec } 2^n - 1 > 2^r - 1 \geq 2.$$

2. Par contraposé, si n n'est pas une puissance de 2, il existe un diviseur premier impair de n .

On écrit :

$$n = p \times s,$$

avec p un premier impair.

Ainsi,

$$2^n + 1 = 2^{ps} - (-1)^p$$

est factorisable par $2^s + 1$ avec $2 \leq 2^s + 1 < 2^n + 1$.

Correction de l'exercice 16

On suppose qu'il n'existe qu'un nombre fini de nombre premiers congrus à -1 modulo 4. On en dresse la liste :

$$p_1 < \cdots < p_s.$$

On considère l'entier :

$$N = \prod_{k=1}^s p_k^2 + 2.$$

L'entier N est divisible par un nombre premier q .

L'entier N est impair, donc q est impair.

Il est impossible que q soit congru à -1 modulo 4 car sinon q diviserait $\prod_{k=1}^s p_k^2$, donc 2.

On vient de montrer que tous les nombres premiers divisant N valent 1 dans $\mathbb{Z}/4\mathbb{Z}$. Leur produit et donc N vaut encore 1 dans $\mathbb{Z}/4\mathbb{Z}$.

Or, chaque p_k^2 vaut 1 modulo 4, ainsi que leur produit. L'entier N est congru à 3 modulo 4 : contradiction.

Correction de l'exercice 17

• Si a et b n'ont pas la même parité, le quotient $N = \frac{a^3 + b^3}{2}$ n'est pas un entier, donc n'est pas premier.

Si a et b ont la même parité, alors on peut factoriser $a^3 + b^3$ par $(a + b)$:

$$N = \frac{(a + b)}{2} \times (a^2 - ab + b^2).$$

Si a et b valent 0 ou 1, alors l'entier N vaut 0 ou 1 et n'est pas premier.

Sinon, on a $a \geq 2$ et $b \geq 2$ et l'entier N est factorisable par :

$$2 \leq \frac{a + b}{2} < N.$$

• La quantité $P = \frac{4^{2n+1} + 1}{5}$ est toujours un entier car dans $\mathbb{Z}/5\mathbb{Z}$,

$$4^{2n+1} = (-1)^{2n+1} = -1, \text{ donc } 4^{2n+1} + 1 = 0.$$

En développant :

$$(1 + 2^{2n+1})^2 - 2^r = 1 + 2^{2n+2} + 2^{4n+2} - 2^r,$$

on observe que :

$$P = \frac{(1 + 2^{2n+1})^2 - (2^{n+1})^2}{5} = \frac{1}{5} \times (1 + 2^{2n+1} - 2^{n+1}) \times (1 + 2^{2n+1} + 2^{n+1}).$$

Les entiers $1 + 2^{2n+1} - 2^{n+1} = 1 + 2^{n+1}(2^n - 1)$ et $1 + 2^{2n+1} + 2^{n+1}$ sont strictement supérieurs à 5 et strictement inférieurs à P . L'un de ces deux nombres est en outre multiple de 5.

L'entier P est donc divisible par un entier strictement supérieur à 1 et strictement inférieur à P .

Correction de l'exercice 18

1. Soit k le plus grand entier tel que $2^k \leq n$.

Alors, l'entier 2^k est de 2-valuation égale à k et est un entier compris entre 1 et n .

Soit p un entier de 2-valuation supérieure ou égale à k . Alors, p est multiple de 2^k : $p = 2^k \times m$.

Comme $2^{k+1} > n$, alors $m < 2$ et $m = 1$.

Conclusion, il n'y a qu'un seul entier de 2-valuation maximale : l'entier 2^k défini ci-dessus.

2. On écrit :

$$H_n = \frac{1}{2^k} + \sum_{i=1; i \neq 2^k} \frac{1}{i}.$$

On note S_n la deuxième somme. Chaque fraction $\frac{1}{i}$ est de la forme :

$$\frac{1}{2^\ell \times m},$$

où l'entier ℓ est compris entre 0 et $k-1$ et m est un entier impair.

On peut donc mettre la somme S_n sur le même dénominateur ce qui donne :

$$S_n = \frac{p}{2^{k-1} \times M},$$

où p est un entier et M est un entier impair, l'entier p étant éventuellement pair...

On en déduit :

$$H_n = \frac{1}{2^k} + \frac{p}{2^{k-1}M} = \frac{M + 2p}{2^k M}$$

est un nombre rationnel où le numérateur est impair et le dénominateur est pair, puisque $k \geq 1$ étant donné que l'entier n est supérieur ou égal à 2.

Correction de l'exercice 19

En faisant des essais, on devine la formule.

On montre par récurrence l'assertion :

$$\mathcal{P}(n) : \ll \nu_2(5^{2^n} - 1) = n + 2 \gg$$

- Lorsque $n = 0$, la formule devient $\nu_2(5 - 1) = 2$, ce qui est vrai.
- Supposons la formule vraie pour un certain entier naturel n .
- Au rang suivant, on pose :

$$5^{2^n} - 1 = 2^{n+2} \times m,$$

où l'entier m est impair.

On obtient :

$$\begin{aligned} 5^{2^{n+1}} - 1 &= (5^{2^n} - 1) \times (5^{2^n} + 1) \\ &= 2^{n+2} \times m \times (2^{n+2} \times m + 2) \\ &= 2^{n+3} \times m \times (2^{n+1} \times m + 1) \end{aligned}$$

de 2-valuation égale à $n + 3$.

On a la propriété au rang suivant.

Correction de l'exercice 20

1. Il y a exactement $k_0 = \left\lfloor \frac{n}{p^\alpha} \right\rfloor$ entiers dans $\llbracket 1, n \rrbracket$, dont voici la liste :

$$p^\alpha, 2p^\alpha, \dots, k_0 \times p^\alpha.$$

Les entiers de p -valuation égale à α sont les multiples de p^α et non multiples de $p^{\alpha+1}$.

Comme les multiples de $p^{\alpha+1}$ sont inclus dans les multiples de p^α , on trouve :

$$\left\lfloor \frac{n}{p^\alpha} \right\rfloor - \left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor$$

tels entiers.

2. On obtient déjà :

$$\nu_p(n!) = \sum_{k=1}^n \nu_p(k).$$

On regroupe les p -valuation selon leur valeur commune :

$$\begin{aligned} \nu_p(n!) &= \sum_{\alpha=0}^{+\infty} \left(\sum_{k=1 \text{ et } \nu_p(k)=\alpha}^n \nu_p(k) \right) \\ &= \sum_{\alpha=0}^{+\infty} \alpha \times \left(\left\lfloor \frac{n}{p^\alpha} \right\rfloor - \left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor \right) \\ &= \sum_{\alpha=0}^{+\infty} \alpha \times \left\lfloor \frac{n}{p^\alpha} \right\rfloor - \sum_{\alpha=0}^{+\infty} \alpha \times \left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor \end{aligned}$$

$$\begin{aligned}
&= \sum_{\alpha=1}^{+\infty} \alpha \times \left\lfloor \frac{n}{p^\alpha} \right\rfloor - \sum_{\alpha=1}^{+\infty} (\alpha - 1) \times \left\lfloor \frac{n}{p^\alpha} \right\rfloor \\
&= \sum_{\alpha=1}^{+\infty} \left\lfloor \frac{n}{p^\alpha} \right\rfloor.
\end{aligned}$$

3. On note N le nombre demandé de sorte que :

$$1000! = 10^N \times c,$$

où c est un entier dont le chiffre des unités n'est pas nul.

On en déduit que l'entier N est le minimum entre la 2-valuation et la 5-valuation dans $1000!$.

D'après la formule établie dans la question précédente, la formule est décroissante en α . Ainsi :

$$\begin{aligned}
N &= \nu_5(1000!) \\
&= \sum_{\alpha=1}^{+\infty} \left\lfloor \frac{1000}{5^\alpha} \right\rfloor \\
&= \left\lfloor \frac{1000}{5} \right\rfloor + \left\lfloor \frac{1000}{25} \right\rfloor + \left\lfloor \frac{1000}{125} \right\rfloor + \left\lfloor \frac{1000}{625} \right\rfloor \\
&= 249.
\end{aligned}$$

Il y a 249 zéros consécutifs à partir de la droite dans $1000!$.

4. Soient r et s dans $\mathbb{N}$. Soit p un nombre premier.

Il suffit de montrer que :

$$\nu_p((2r)!) + \nu_p((2s)!) - \nu_p((r+s)!) - \nu_p(r!) - \nu_p(s!) \geq 0.$$

En écrivant la formule de la question **Q.2** pour chaque p -valuation, il suffit de montrer que pour tout $\alpha \in \mathbb{N}^*$:

$$\left\lfloor \frac{2r}{p^\alpha} \right\rfloor + \left\lfloor \frac{2s}{p^\alpha} \right\rfloor - \left\lfloor \frac{r+s}{p^\alpha} \right\rfloor - \left\lfloor \frac{r}{p^\alpha} \right\rfloor - \left\lfloor \frac{s}{p^\alpha} \right\rfloor \geq 0.$$

Il suffit de montrer que pour tous réels x , et y positifs, :

$$\lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor \leq \lfloor 2x \rfloor + \lfloor 2y \rfloor.$$

Soient x et y deux réels positifs.

On pose $a = \lfloor x \rfloor$ et $b = \lfloor y \rfloor$.

Ainsi, $a + b \leq x + y < a + b + 2$, donc $\lfloor x + y \rfloor \in \{a + b, a + b + 1\}$.

Si $x + y < a + b + 1$, alors comme $2a \leq \lfloor 2x \rfloor$ et $2b \leq \lfloor 2y \rfloor$, on a ce qu'il faut.

Si $x + y \geq a + b + 1$, alors nécessairement $x \geq a + \frac{1}{2}$ ou $y \geq b + \frac{1}{2}$, donc $\lfloor 2x \rfloor \geq 2a + 1$ ou $\lfloor 2y \rfloor \geq 2b + 1$.

Quoiqu'il arrive, on a ce qu'il faut.

Correction de l'exercice 21

Le sens indirect est évident.

On établit le sens direct.

Dans toute la suite, pour toute partie A de $\{1, \dots, n\}$, on pose :

$$R_A = \prod_{k \in A} p_k.$$

On suppose $S_I = S_J$.

On pose les quatre ensembles :

$$I_1 = I \cap J, \quad I_2 = I \setminus J, \quad I_3 = J \setminus I \quad \text{et} \quad I_4 = \{1, \dots, n\} \setminus (I \cup J),$$

de sorte que les quatre ensembles I_1, I_2, I_3 et I_4 sont disjoints et :

$$S_I = R_{I_1} \times R_{I_2} + R_{I_3} \times R_{I_4} \quad \text{et} \quad S_J = R_{I_1} \times R_{I_3} + R_{I_2} \times R_{I_4}.$$

L'égalité $S_I = S_J$ devient :

$$(R_{I_1} - R_{I_4}) \times (R_{I_2} - R_{I_3}).$$

Par intégrité de $\mathbb{Z}$, l'une des deux parenthèses est nulle.

→ Si $R_{I_1} = R_{I_4}$, alors par unicité de la décomposition en facteurs premiers, R_{I_1} et R_{I_4} sont des produits vides, donc $I_1 = I_4 = \emptyset$.

Cela impose que $I \sqcup J = \{1, \dots, n\}$, donc $I = \{1, \dots, n\} \setminus J$.

→ Si $R_{I_2} = R_{I_3}$, alors toujours par unicité de la décomposition en facteurs premiers, R_{I_2} et R_{I_3} sont des produits vides, donc $I_2 = I_3 = \emptyset$.

Cela impose que $I = J$.

Correction de l'exercice 22

1. L'existence provient du développement par la formule du binôme en séparant les indices pairs ou impairs.

L'unicité provient de l'irrationalité de $\sqrt{2}$.

2. On aurait pu avoir l'existence par récurrence.

On a :

$$a_0 = 1 \quad \text{et} \quad b_1 = 0.$$

Si le couple (a_n, b_n) convient au rang n , au rang suivant :

$$(1 + \sqrt{2})^{n+1} = (1 + \sqrt{2}) \times (a_n + b_n \cdot \sqrt{2}) = a_{n+1} + b_{n+1} \cdot \sqrt{2},$$

en posant $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$.

On en déduit :

$$a_{n+1}^2 - 2b_{n+1}^2 = (a_n + 2b_n)^2 - 2(a_n + b_n)^2 = -(a_n^2 - 2b_n^2).$$

Conclusion, on a affaire à une suite géométrique de raison (-1) et :

$$a_n^2 - 2b_n^2 = (-1)^n(a_0^2 - 2b_0^2) = (-1)^n.$$

3. La formule :

$$a_n \times a_n - 2b_n \times b_n = \pm 1$$

apparaît comme une relation de Bezout entre a_n et b_n .

Correction de l'exercice 23

Les deux premiers points de cet exercice sont archi-classiques !! À retenir.

1. Soit k un entier entre 1 et $p-1$. On remarque que :

$$\binom{p}{k} \times k! \times (p-k)! = p!$$

est divisible par p .

Or, l'entier p est premier avec $k!$ et $(p-k)!$. Par le théorème de Gauss, le premier p divise le coefficient binomial.

2. On le montre par récurrence ascendante et descendante sur l'entier a .

Lorsque $a = 0$, l'égalité est immédiate.

Supposons que pour un certain entier a , l'entier $a^p - a$ soit multiple de p .

Au rang suivant, par le binôme,

$$(a+1)^p - (a+1) = \sum_{k=1}^{p-1} \binom{p}{k} a^k + (a^p - a)$$

qui est bien multiple de p par la première question et l'hypothèse de récurrence.

Au rang précédent, par le binôme,

$$(a-1)^p - (a-1) = \sum_{k=1}^{p-1} \binom{p}{k} (-1)^{p-k} a^k + (a^p - a) + (-1)^p + 1.$$

La somme est multiple de p , la quantité $a^p - a$ également.

Si $p = 2$, alors $(-1)^p + 1 = 2$ est multiple de $p = 2$.

Sinon, $(-1)^p + 1 = 0$ et on a ce qu'il faut.

3. (a) Soit $n \in \mathbb{N}$.

On sait que $n^5 - n$ est multiple de 5.

Or, $n^5 - n = n(n^4 - 1) = n(n - 1)(n + 1)(n^2 + 1)$ qui est encore multiple de 2 et de 3.

Le tout est multiple de $2 \times 3 \times 5$.

(b) idem

Correction de l'exercice 24

1. On sait que p_2 et p_3 sont impair. Leur différence r est paire.

La différence $p_2 - p_1$ est paire et $p_2 > 2$ est impair, ainsi que p_1 .

2. Si $n > p_1$, le terme p_{1+p_1} figure dans la $\mathcal{P}$ -suite.

Or, tout élément de la $\mathcal{P}$ -suite s'écrit :

$$p_k = p_1 + (k - 1)r.$$

On en déduit :

$$p_{1+p_1} = p_1 \times (1 + r) \text{ non premier.}$$

Donc $n \leq p_1$.

3. (a) Soient i et j deux entiers entre 1 et n .

Si $r_i = r_j$, alors en écrivant les divisions euclidiennes :

$$p_i = a_i q + r_i \text{ et } p_j = a_j q + r_j,$$

alors l'entier q divise $p_i - p_j$.

Or,

$$p_i - p_j = (i - j) \times r.$$

Le théorème de Gauss s'applique puisque le premier q est premier avec r .

Pour la réciproque, si q divise $(i - j)$, alors q divise $p_i - p_j$ et on a rapidement ce qu'il faut.

(b) Si i et j sont deux entiers différents entre 1 et q , alors l'entier q ne peut diviser $i - j$ car :

$$1 \leq |i - j| < q.$$

Par la question précédente, $r_i \neq r_j$.

(c) Les nombres $r_1, \dots, r_q$ sont q entiers différents dans l'ensemble $\llbracket 0, q - 1 \rrbracket$. Par égalité des cardinaux finis, on peut affirmer que :

$$\llbracket 0, q - 1 \rrbracket = \{r_1, \dots, r_q\}.$$

Il existe un entier s entre 1 et q tel que :

$$r_s = 0.$$

(d) Ainsi, l'entier p_s est un premier multiple de q : contradiction.

On a montré que la raison r est multiple du produit de tous les nombres premiers inférieurs à n .

Correction de l'exercice 25

1. Soit p vérifiant les hypothèses.

Voici la liste des diviseurs de E_p :

$$2^k \times (2^p - 1)^\varepsilon,$$

avec k un entier entre 1 et $p - 1$ et $\varepsilon \in \{0, 1\}$.

On peut calculer facilement la somme de ces nombres ce qui donne après calculs des sommes géométriques :

$$\lambda_{E_p} = 2E_p.$$

2. (a) Voici la liste des diviseurs de l'entier $n : 2^k \times d$, où k varie parmi les entiers entre 0 et r et d varie parmi les diviseurs de l'entier m .

On obtient rapidement la formule demandée par calcul de la somme géométrique à l'intérieur de la somme rectangulaire :

$$\sum_{k=0}^r 2^k = 2^{r+1} - 1.$$

(b) On en déduit :

$$2^{r+1}m = \lambda_n = \lambda_m \times (2^{r+1} - 1).$$

Comme 2^{r+1} et $2^{r+1} - 1$ sont des entiers premiers entre eux, on peut appliquer le théorème de Gauss : l'entier λ_m est multiple de 2^{r+1} . On pose c le quotient de ces deux nombres ce qui répond à la question en réinjectant.

(c) Les nombres 1, c , $2^{r+1} - 1$ et m divisent l'entier m .

Si $c \neq 1$, alors les nombres 1, c et m sont différents les uns des autres et la somme sur ces diviseurs est inférieure ou égale à λ_m .

Or, la somme sur ces trois entiers vaut déjà :

$$1 + c + m \Rightarrow 2^{r+1} \cdot c = 2^{r+1} \cdot c > \lambda_m.$$

Impossible !

Ainsi, $c = 1$ et $\lambda_m = 1 + m$. L'entier m n'admet que deux diviseurs strictement positifs : l'entier m est premier.

(d) En utilisant un autre exercice (le reconnaître !) de la feuille d'exercices, l'entier $r + 1$ est premier.

(e) immédiat.

Correction de l'exercice 26

1. Si (x, y, z) est un triplet pythagoricien, en prenant d le pgcd de ces trois entiers et en posant :

$$x' = \frac{|x|}{d}, \quad y' = \frac{|y|}{d} \text{ et } z' = \frac{|z|}{d},$$

alors le triplet (x', y', z') est un triplet pythagoricien à composantes positives.

De plus, si p est un diviseur premier éventuel de x' et de y' par exemple, alors p divisera $x'^2 + y'^2 = z'^2$, puis p divisera z' et donc le pgcd entre x' , y' et z' qui par construction vaut 1.

Deux des trois nombres x' , y' et z' sont toujours premiers entre eux : le triplet (x', y', z') est primitif.

Connaissant les triplets pythagoriciens primitifs, en multipliant les composantes par un même entier, on trouve tous les triplets pythagoriciens.

2. Si l'entier z est pair, alors les nombres x^2 et y^2 ont la même parité, ainsi que les entiers x et y .

Les entiers x et y ne peuvent être pairs car le triplet ne serait plus primitif.

Les entiers x et y sont donc impairs. On pose :

$$x = 2k + 1 \text{ et } y = 2\ell + 1,$$

de sorte que :

$$z^2 = x^2 + y^2 = 4k^2 + 4\ell^2 + 4k + 4\ell + 2 \equiv 2 \pmod{4}.$$

Or, comme z est pair, alors $z^2 \equiv 0 \pmod{4}$: contradiction.

L'entier z est impair.

3. Les nombres r et t sont bien des entiers.

Soit p un nombre premier divisant éventuellement r et t .

On en déduit que l'entier p divise la somme et la différence. L'entier p divise alors z et x : impossible.

4. On remarque que :

$$r \times t = \frac{z^2 - x^2}{4} = s^2.$$

D'après un autre exercice de la feuille – le reconnaître !! –, on sait que les entiers r et t sont des carrés parfaits.

5. On pose :

$$r = u^2 \text{ et } t = v^2,$$

donc :

$$x = u^2 - v^2 \text{ et } z = u^2 + v^2.$$

Or,

$$y^2 = z^2 - x^2 = 4u^2v^2,$$

donc $y = \pm 2uv$.

Si $y = 2uv$, alors le triplet est de la forme :

$$(x, y, z) = (u^2 - v^2, 2uv, u^2 + v^2).$$

Si $y = -2uv$, alors le triplet est de la forme :

$$(x, y, z) = (U^2 - V^2, 2UV, U^2 + V^2),$$

avec $U = u$ et $V = -v$ par exemple.

On vérifie que pour tout $(u, v) \in \mathbb{Z}^2$, le triplet $(u^2 - v^2, 2uv, u^2 + v^2)$ est un triplet pythagoricien primitif et par la première question, on a ce qu'il faut en multipliant les composantes par un même entier d .

Correction de l'exercice 27

1. Supposons $P(A) = P(B)$.

Par symétrie des rôles, il suffit de montrer l'inclusion $A \subset B$.

Soit $x \in A$. On pose :

$$x = \frac{r}{s},$$

où $r \in \mathbb{Z}$ et $s \in \mathbb{N}^*$ et $r \wedge s = 1$.

Soit p un nombre premier divisant s . Nous allons montrer que $s \in P(A)$.

En effet, on écrit une relation de Bezout entre r et s :

$$ru + sv = 1, \text{ donc en divisant par } s : xu + v = \frac{1}{s}.$$

L'ensemble A étant un sous-anneau de $\mathbb{Q}$ contient 1 donc tous les entiers.

Ainsi, xu qui est une somme (ou différence) de plusieurs fois l'élément x appartient à A , ainsi que v :

$$\frac{1}{s} \in A, \text{ donc aussi } : \frac{s}{p} \times \frac{1}{s} = \frac{1}{p}.$$

On en déduit que $p \in P(A) = P(B)$.

Tous les éléments $\frac{1}{p}$ appartiennent à l'anneau B , ainsi que leur produit : le quotient $\frac{1}{s}$ appartient encore à B , ainsi que :

$$r \times \frac{1}{s} = x.$$

2. On va montrer que l'ensemble :

$$A = \left\{ \frac{n}{m} \mid n \in \mathbb{Z}, m \in \mathbb{N}^*, m \text{ est un produit de premiers dans } P \right\}$$

répond à la question.

Il est facile de voir que $1 \in A$, que A est stable par produit et par différence en mettant la différence de deux quotients sur le même dénominateur.

On montre finalement que :

$$P(A) = P.$$

Soit $p \in P$. Alors, par définition de A :

$$\frac{1}{p} \in A, \text{ donc } p \in P(A).$$

Soit $p \in P(A)$. Alors, $\frac{1}{p} \in A$. Il existe une décomposition de la fraction $\frac{1}{p}$ sous la forme :

$$\frac{1}{p} = \frac{n}{q_1 \cdot q_2 \cdots q_r},$$

où n est un entier et les nombres q_k sont des éléments de P .

On en déduit :

$$pn = q_1 \cdot q_2 \cdots q_r.$$

Le nombre premier p divise le produit des premiers q_k : le premier p est l'un des facteurs q_k et donc le nombre p appartient bien à l'ensemble P .
