Planche n° 23. Arithmétique. Corrigé

Exercice n° 1

Par récurrence double, pour tout $n \in \mathbb{N}^*$, $F_n \in \mathbb{N}^*$.

Soit $n \in \mathbb{N}^*$. Soit d un entier naturel non nul. Si d divise F_n et F_{n+1}, alors d divise F_{n+1} et $F_{n+1} + F_n = F_{n+2}$ et si d divise F_{n+1} et F_{n+2}, alors d divise F_{n+1} et $F_{n+2} - F_{n+1} = F_n$. Ainsi, F_{n+1} et F_{n+2} d'une part et F_n et F_{n+1} d'autre part ont même ensemble de diviseurs communs. En particulier, $\text{PGCD}(F_{n+1}, F_{n+2}) = \text{PGCD}(F_n, F_{n+1})$.

Mais alors, par récurrence simple, pour tout $n \in \mathbb{N}^*$, $\text{PGCD}(F_n, F_{n+1}) = \text{PGCD}(F_1, F_2) = \text{PGCD}(1, 1) = 1$. On a montré que pour tout $n \in \mathbb{N}^*$, F_n et F_{n+1} sont des entiers premiers entre eux.

Exercice n° 2

1) Puisque p est premier, $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un corps et en particulier un anneau intègre. Soit $x \in \mathbb{Z}/p\mathbb{Z}$.

$$\begin{aligned} x^2 = \widehat{1} &\Leftrightarrow x^2 - \widehat{1} = \widehat{0} \Leftrightarrow \left(x - \widehat{1}\right)\left(x + \widehat{1}\right) \\ &\Leftrightarrow x - \widehat{1} = \widehat{0} \text{ ou } x + \widehat{1} = \widehat{0} \text{ (par intégrité de } (\mathbb{Z}/p\mathbb{Z}, +, \times)) \\ &\Leftrightarrow x = \widehat{1} \text{ ou } x = -\widehat{1}. \end{aligned}$$

L'ensemble des solutions est $\left\{-\widehat{1}, \widehat{1}\right\}$ ou encore $\left\{\widehat{1}, \widehat{p-1}\right\}$.

2) Dans $\mathbb{Z}/12\mathbb{Z}$, l'équation admet pour solutions $-\widehat{1}$ et $\widehat{1}$. Mais il y a peut-être d'autres solutions.

$\widehat{0}^2 = \widehat{0}$.
$\widehat{1}^2 = \widehat{1} = \left(-\widehat{1}\right)^2 = \left(\widehat{11}\right)^2$
$\widehat{2}^2 = \widehat{4} = \left(\widehat{10}\right)^2$.
$\widehat{3}^2 = \widehat{9} = \left(\widehat{9}\right)^2$.
$\widehat{4}^2 = \widehat{4} = \left(\widehat{8}\right)^2$.
$\widehat{5}^2 = \widehat{1} = \left(\widehat{7}\right)^2$.
$\widehat{6}^2 = \widehat{0}$.

L'ensemble des solutions est $\left\{\widehat{1}, \widehat{5}, \widehat{7}, \widehat{11}\right\}$.

3) Si $x^7 = \widehat{1}$, alors $x \neq \widehat{0}$. Puisque 19 est un nombre premier, $(\mathbb{Z}/19\mathbb{Z} \setminus \{0\}, \times)$ est un groupe de cardinal 18.

Si $x^7 = 1$, alors l'ordre de x est un diviseur de 7 et donc égal à 1 ou 7. Mais l'ordre de x doit aussi diviser 18. Donc l'ordre de x est égal 1 ou encore $x = \widehat{1}$. Réciproquement, $\widehat{1}$ est solution de l'équation et donc l'ensemble des solutions de l'équation est $\left\{\widehat{1}\right\}$.

Exercice n° 3

L'algorithme d'Euclide appliqué à 418 et 223 s'écrit :

$$\begin{aligned} &418 = 1 \times 223 + 195. \\ &223 = 1 \times 195 + 28. \\ &195 = 6 \times 28 + 27. \\ &28 = 1 \times 27 + 1. \end{aligned}$$

Le dernier reste non nul est 1 et donc 223 et 418 sont premiers entre eux puis $\widehat{223}$ est inversible dans $(\mathbb{Z}/418\mathbb{Z}, +, \times)$. Ensuite,

$$\begin{aligned} 1 &= 28 - 27 \\ &= 28 - (195 - 6 \times 28) = 7 \times 28 - 195 \\ &= 7(223 - 195) - 195 = 7 \times 223 - 8 \times 195 \\ &= 7 \times 223 - 8(418 - 223) = 15 \times 223 - 8 \times 418, \end{aligned}$$

puis $\widehat{15} \times \widehat{223} = \widehat{1}$. L'inverse de $\widehat{223}$ dans $(\mathbb{Z}/418\mathbb{Z}, +, \times)$ est $\widehat{15}$.

Exercice n° 4

1) 19 est un nombre premier et donc $(\mathbb{Z}/19\mathbb{Z}, +, \times)$ est un corps. Toute classe non nulle est donc inversible et en particulier simplifiable pour $\times$.

Soit $(x, y) \in (\mathbb{Z}/19\mathbb{Z})^2$.

$$\left\{\begin{array}{l}\widehat{3}x + \widehat{4}y = \widehat{0} \\ \widehat{4}x + \widehat{3}y = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}\widehat{5}\left(\widehat{3}x + \widehat{4}y\right) = \widehat{5} \times \widehat{0} \\ \widehat{4}x + \widehat{3}y = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}-\widehat{4}x + y = \widehat{0} \\ \widehat{4}x + \widehat{3}y = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}y = \widehat{4}x \\ \widehat{4}x + \widehat{3}\left(\widehat{4}x\right) = \widehat{5}\end{array}\right.$$
$$\Leftrightarrow \left\{\begin{array}{l}y = \widehat{4}x \\ -\widehat{3}x = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}\widehat{6}\left(-\widehat{3}x\right) = \widehat{6} \times \widehat{5} \\ y = \widehat{4}x\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x = \widehat{11} \\ y = \widehat{6}\end{array}\right. .$$

L'ensemble des solutions est $\left\{\left(\widehat{11}, \widehat{6}\right)\right\}$.

2) 18 n'est pas premier. Les classes inversibles de l'anneau $(\mathbb{Z}/18\mathbb{Z}, +, \times)$ sont $\widehat{1}$, $\widehat{5}$, $\widehat{7}$, $\widehat{11} = -\widehat{7}$, $\widehat{13} = -\widehat{5}$, $\widehat{17} = -\widehat{1}$ (classes des entiers de $[\![1, 17]\!]$ qui sont premiers à 18.

Soit $(x, y) \in (\mathbb{Z}/18\mathbb{Z})^2$.

$$\left\{\begin{array}{l}\widehat{3}x + \widehat{4}y = \widehat{0} \\ \widehat{4}x + \widehat{3}y = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}\widehat{7}x + \widehat{7}y = \widehat{5} \text{ ((I + II)} \\ \widehat{4}x + \widehat{3}y = \widehat{5}\end{array}\right.$$

Ensuite, $18 = 2 \times 7 + 4$ puis $7 = 4 + 3$ puis $4 = 3 + 1$ et donc

$$1 = 4 - 3 = 4 - (7 - 4) = 2 \times 4 - 7 = 2(18 - 2 \times 7) - \times 7 = 2 \times 18 - 5 \times 7$$

puis $-\widehat{5} \times \widehat{7} = \widehat{1}$. L'inverse de $\widehat{7}$ dans $(\mathbb{Z}/18\mathbb{Z}, +, \times)$ est $-\widehat{5}$ ou encore $\widehat{14}$.

$$\left\{\begin{array}{l}\widehat{3}x + \widehat{4}y = \widehat{0} \\ \widehat{4}x + \widehat{3}y = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x + y = \widehat{7} \\ \widehat{4}x + \widehat{3}y = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}y = -x + \widehat{7} \\ \widehat{4}x + \widehat{3}\left(-x + \widehat{7}\right) = \widehat{5}\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x = \widehat{2} \\ y = \widehat{5}\end{array}\right. .$$

L'ensemble des solutions est $\left\{\left(\widehat{2}, \widehat{5}\right)\right\}$.

Exercice n° 5

1) Soient $n \geqslant 2$ puis d un diviseur de n. Posons donc $n = qd$ où $q \in \mathbb{N}^*$ ou encore posons $q = \dfrac{n}{d}$.

Soit $k \in [\![1, n]\!]$. Si $k \wedge n = d$, alors il existe $k' \in \mathbb{N}^*$ tel que $k = k'd$. De plus, $k \in [\![1, n]\!]$ et donc $k' \in \left[\!\!\left[1, \dfrac{n}{d}\right]\!\!\right]$.

Réciproquement, s'il existe $k' \in \left[\!\!\left[, \dfrac{n}{d}\right]\!\!\right]$ tel que $k = k'd$, alors $k \wedge n = d \Leftrightarrow (k'd) \wedge (qd) = d \Leftrightarrow k' \wedge q = 1$.

Donc, $E_d = \left\{k'd,\ k' \in \left[\!\!\left[, \dfrac{n}{d}\right]\!\!\right],\ k' \wedge \dfrac{n}{d} = 1\right\}$. E_d est ainsi en bijection avec $\left\{k' \in \left[\!\!\left[, \dfrac{n}{d}\right]\!\!\right],\ k' \wedge \dfrac{n}{d} = 1\right\}$ et donc

$$\operatorname{card}(E_d) = \varphi\left(\frac{n}{d}\right).$$

2) Pour tout entier $k \in [\![1, n]\!]$, $k \wedge n$ est un diviseur d de $[\![1, n]\!]$. Mais alors, tout entier $k \in [\![1, n]\!]$ est dans un et un seul des E_d où d est un diviseur de n. Par suite,

$$n = \operatorname{card}([\![1, n]\!]) = \sum_{d|n}^{n} \operatorname{card}(E_d) = \sum_{d|n} \varphi\left(\frac{n}{d}\right).$$

Enfin, si on note $\mathscr{D}(n)$ l'ensemble des diviseurs de n, $f : \begin{array}{ccc}\mathscr{D}(n) & \to & \mathscr{D}(n) \\ d & \mapsto & \dfrac{n}{d}\end{array}$ est une permutation de $\mathscr{D}(n)$ (car f est effectivement une application de $\mathscr{D}(n)$ vers lui-même qui est involutive). On a donc aussi

$$n = \sum_{d|n} \varphi(d).$$

Exercice n° 6

Pour $k \in [\![2, m+1]\!]$, posons $n_k = (m+1)! + k$. Les entiers n_k, $k \in [\![2, m+1]\!]$, sont m entiers consécutifs. De plus, pour tout $k \in [\![2, m+1]\!]$, n_k est divisible par k avec $k \geqslant 2$ et n'est donc pas un nombre premier.

Exercice n° 7

1) p divise n^2+1 ou encore $n^2 \equiv -1$ [p] puis $n^4 \equiv 1$ [p].
D'autre part, puisqu'il existe $k \in \mathbb{N}^*$ tel que $pK - n \times n = 1$, le théorème de Bézout permet d'affirmer que n et p sont premiers entre eux. Mais alors, d'après le petit théorème de Fermat $n^{p-1} \equiv 1$ [p].

D'après ce qui précède, dans $\mathbb{Z}/p\mathbb{Z}$, $\widehat{n}^4 = \widehat{1}$. $\widehat{n}$ est un élément de $(\mathbb{Z}/p\mathbb{Z})^*$ puisque $n \wedge p = 1$. L'ordre de $\widehat{n}$ dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est un diviseur de 4, à savoir 1, 2, ou 4. Si $\widehat{n} = \widehat{1}$, alors $\widehat{n}^2 = \widehat{1}$ ce qui est faux car, p étant impair, $-\widehat{1} \neq \widehat{1}$. Donc, $\widehat{n} \neq \widehat{1}$ et de même, $\widehat{n}^2 \neq \widehat{1}$ et finalement, $\widehat{n}$ est d'ordre 4.

Puisque $\widehat{n}^{p-1} = \widehat{1}$, $p-1$ est un multiple de l'ordre de $\widehat{n}$ à savoir 4. Donc, $p \equiv 1$ [4].

1) Puisque $5 \equiv 1[4]$, il existe au moins un nombre premier de la forme $4K+1$, $K \in \mathbb{N}^*$. Supposons par l'absurde qu'il existe un nombre fini de nombres premiers de la forme $4K+1$, $K \in \mathbb{N}^*$. Notons $p_1 < p_2 < \ldots < p_k$ ces nombres.

‘ Soit $N = 4p_1^2 \ldots p_k^2 + 1 = (2p_1 \ldots p_k)^2 + 1$. N est un entier impair supérieur ou égal à 2 et donc N admet un facteur premier impair que l'on note p. D'après la question précédente, $p \equiv 1$ [4]. Mais puisque p divise N, il existe K tel que $Kp - 4p_1^2 \ldots p_k^2 = 1$. Le théorème de Bézout permet d'affirmer que p est premier à chacun des p_i, $1 \leqslant i \leqslant k$ et en particulier p est un nombre premier de la forme $4K+1$, $K \in \mathbb{N}^*$, distinct de chacun des p_i, $1 \leqslant i \leqslant k$. Ceci est faux et il était donc absurde de supposer qu'il n'ya qu'un nombre fini de nombres premiers de la forme $4K+1$, $K \in \mathbb{N}^*$.

‘ On a montré qu'il existe une infinité de nombres premiers de la forme $4K+1$, $K \in \mathbb{N}^*$.

Exercice n° 8

Puisque $9 \wedge 13 = 1$, le théorème chinois montre que le système proposé a au moins une solution x_0 dans $\mathbb{Z}$. Mais alors, pour $x \in \mathbb{Z}$,

$$\begin{aligned}
\left\{\begin{array}{l} x \equiv 4\ [9] \\ x \equiv 2\ [13] \end{array}\right. &\Leftrightarrow \left\{\begin{array}{l} x \equiv x_0\ [9] \\ x \equiv x_0\ [13] \end{array}\right. \\
&\Leftrightarrow x - x_0 \in 9\mathbb{Z} \cap 13\mathbb{Z} \Leftrightarrow x - x_0 \in (9 \vee 13)\mathbb{Z} \Leftrightarrow x - x_0 \in (9 \times 13)\mathbb{Z} \\
&\Leftrightarrow \exists q \in \mathbb{Z}/\ x = x_0 + 117q.
\end{aligned}$$

Il reste à déterminer une solution particulière x_0 du système proposé. Soient $k \in \mathbb{Z}$ puis $x = 4 + 9k$.

$$\begin{aligned}
x \equiv 2\ [13] &\Leftrightarrow 4 + 9k \equiv 2\ [13] \Leftrightarrow 9k \equiv -2\ [13] \\
&\Leftrightarrow 3 \times 9k \equiv 3 \times (-2)\ [13]\ (\text{car } 9 \wedge 13 = 1) \\
&\Leftrightarrow k \equiv -6\ [13] \\
&\Leftarrow k = 7 \Leftarrow x = 67.
\end{aligned}$$

L'ensemble des solutions du système proposé est $\{67 + 117q,\ q \in \mathbb{Z}\}$.

Exercice n° 9

$12 = 2^2 \times 3$ et donc $\varphi(12) = 12\left(1 - \dfrac{1}{2}\right)\left(1 - \dfrac{1}{3}\right) = 4$. Ensuite, $5 \wedge 12 = 1$ et donc, d'après le théorème d'Euler, $5^4 \equiv 1$ [12]. Ensuite, $657 = 4 \times 164 + 1$ puis

$$5^{567} = \left(5^4\right)^{164} \times 5 \equiv 5\ [12]$$

et finalement, $5^{567} - 5$ est divisible par 12.