Correction DM

Exercice 1.

1. Ça se devine : on sait que $10 \cdot 2 = 20 \equiv 1[19]$. Sinon, on utilise l'algorithme d'Euclide :

$$\begin{aligned} 19 &= 10 \cdot 1 + 9 \\ 10 &= 9 \cdot 1 + 1 \end{aligned}$$

Qui donne le même résultat.

2. Par définition de c_0 et de D, l'entier N s'écrit $10D + c_0$, on a donc

$$\begin{aligned} N = 10D + c_0 &\equiv 10D + 1 \cdot c_0[19] \\ &= 10D + 10 \cdot 2 \cdot c_0[19] \\ &= 10(D + 2c_0)[19] \end{aligned}$$

Soit le résultat annoncé.

3. Par la question précédente, N est congru à $10(D+2c_0)$ modulo 19. Donc N est divisible par 19 si et seulement si $10(D + 2c_0)$ est divisible par 19. De plus, comme 10 est premier avec 19, on a que $10(D + 2c_0)$ est divisible par 19 si et seulement si $D + 2c_0$ est divisible par 19. D'où le critère voulu.

4. On pose $N_0 = 84721$, $D_0 = 8472$ son nombre de dizaines et $c_0 = 1$ son chiffre des unités. Par la question précédente, N est divisible par 19 si et seulement si $N_1 := D_0 + 2c_0 = 8474$ l'est.
On applique à nouveau le critère précédent à $N_1 = 8474$, on a $D_1 = 847$ et $c_1 = 4$. Donc N_1 est divisible par 19 si et seulement si $N_2 = 847 + 2 \cdot 4 = 855$ l'est.
On applique à nouveau le critère précédent à $N_2 = 855$, on a $D_2 = 85$ et $c_2 = 5$. Donc N_2 est divisible par 19 si et seulement si $N_3 = 85 + 2 \cdot 5 = 95$ l'est.
On applique à nouveau le critère précédent à $N_3 = 95$, on a $D_3 = 9$ et $c_3 = 5$. Donc N_3 est divisible par 19 si et seulement si $N_4 = 9 + 10 = 19$ l'est.
Comme 19 est évidemment divisible par lui-même, on trouve que N_2, N_1 et N_0 sont divisibles par 19.

5. L'hypothèse est que 10 soit inversible modulo m, autrement dit que m et 10 soient premiers entre eux.

6. On reprend le raisonnement de la question 2 : on a toujours $N = 10D + c_0$, et donc

$$\begin{aligned} N = 10D + c_0 &\equiv 10D + 1 \cdot c_0[m] \\ &= 10D + 10 \cdot \ell \cdot c_0[m] \\ &= 10(D + \ell c_0)[m] \end{aligned}$$

7. On reprend le raisonnement de la question 3 : comme $N \equiv 10(D + \ell c_0)[m]$, on a que N est divisible par m si et seulement si $10(D + \ell c_0)$ l'est. Or comme 10 est inversible modulo m, on a

$$10(D + \ell c_0) \equiv 0[m] \Leftrightarrow \ell \cdot 10(D + \ell c_0) \equiv D + \ell c_0[m]$$

D'où le critère suivant : N est divisible par m si et seulement si $D + \ell c_0$ est divisible par m.

Exercice 2.

On note 0 le jour présent, de sorte que l'indice de demain est 1 et celui d'hier est -1. Les jours x où Pompon

rentre chez lui sont régis par l'équation $x \equiv 7[23]$ car il viendra mercredi prochain (dans 7 jours) et il rentre tous les 23 jours. De même, les jours y que Aurélien passe chez lui sont régis par l'équation $y \equiv -1[7]$.

Les jours où Pompon et Aurélien sont chez eux le même jours sont donc les solutions d du système de congruence

$$\begin{cases} d \equiv 7[23] \\ d \equiv -1[7] \end{cases}$$

Comme 23 et 7 sont premiers entre eux, les solutions de ce système sont égales modulo $23 \vee 7 = 161$. On cherche une solution particulière à notre système : on pose donc $d = 7 + 23p = -1 + 7q$ et on obtient

$$-23p + 7q = 8$$

Pour trouver une solution à cette équation, on utilise l'algorithme d'Euclide :

$$23 = 7 \cdot 3 + 2$$
$$7 = 2 \cdot 3 + 1$$

On obtient $1 = 7 - 2 \cdot 3 = 7 - (23 - 7 \cdot 3) \cdot 3 = 7 - 23 \cdot 3 + 7 \cdot 9 = 7 \cdot 10 - 23 \cdot 3$. On pose donc $p = 8 \cdot -3 = -24$ ou $q = 10 \cdot 8 = 80$ (ça revient au même), et on a $d = -1 + 7q = -1 + 560 = 559$.

Les solutions du système sont exactement les entiers congrus à 559 modulo [161]. Le plus petit entier positif respectant cette dernière équation est $559 - 3 \cdot 161 = 76 + 775 = 76$. On obtient donc que Pompon et Aurélien se retrouverons dans 76 jours, et ensuite tous les 161 jours.

Exercice 3. (Frobenius)
1. On rappelle que

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

Comme p est un nombre premier, on a que p divise $\binom{p}{k}$ si et seulement si p divise $p!$ et p ne divise pas $k!(p-k)!$. Par le lemme d'Euclide, p divise $k!(p-k)$ si et seulement si il divise $k!$ ou $(p-k)!$. Or, si $k \notin \{0, p\}$, on a $k < p$ et $p - k < p$. Une fois encore par le Lemme d'Euclide, on trouve que si p divise $k!$, alors p divise un des facteurs de $k!$, donc un entier $< p$: c'est impossible, et de même pour $(p-k)!$. Ainsi, si $k \notin \{0, p\}$, p ne divise pas $k!(p-k)!$ et donc p divise $\binom{p}{k}$.

2. On commence par montrer que ϕ est un morphisme de groupes de $(A, +)$ vers lui-même : Soient $x, y \in A$, comme A est commutatif, on a la formule du binôme :

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Comme A est de caractéristique p, on a par définition $p(= p \cdot 1_A) = 0$ dans A. Or d'après la question précédente, $\binom{n}{k}$ est divisible par p si $k \notin \{0, p\}$, donc les termes correspondants de la somme sont en fait nuls dans A, d'où

$$(x+y)^p = \binom{p}{0} x^0 y^p + \binom{p}{p} x^p y^0 = x^p + y^p$$

et ϕ est bien un morphisme de groupes. Le reste de la définition de morphisme d'anneau se vérifie très facilement : $\phi(1_A) = 1_A^p = 1_A$ et $\phi(xy) = (xy)^p = x^p y^p$ car x et y commutent.
Dans $\mathbb{Z}/p\mathbb{Z}$, le morphisme de Frobenius est trivial : en effet le théorème de Fermat nous donne $a^p \equiv a[p]$ pour tout entier a, autrement dit $a^p = a$ dans $\mathbb{Z}/p\mathbb{Z}$.

3. Ça découle immédiatement de la question précédente : X et X^p sont deux polynômes distincts dans $\mathbb{Z}/p\mathbb{Z}[X]$ (ils n'ont pas le même degré), pourtant les fonctions

$$x \mapsto x \quad \text{et} \quad x \mapsto x^p$$

définies sur $\mathbb{Z}/p\mathbb{Z}$ sont égales. Les notions de "polynômes" et de "fonctions polynomiales" ne sont pas identiques sur les corps finis.

Exercice 4.

1. On utilise l'algorithme d'Euclide

$$\begin{aligned} 119 &= 32 \cdot 3 + 23 \\ 32 &= 23 \cdot 1 + 9 \\ 23 &= 9 \cdot 2 + 5 \\ 9 &= 5 \cdot 1 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 + 0 \end{aligned}$$

Donc $\frac{119}{32} = [3, 1, 2, 1, 1, 4]$. Pour $-\frac{46}{39}$, il faut faire attention comme il s'agit d'un nombre négatif : on commence par extraire sa partie entière

$$-2 = \frac{-78}{39} < \frac{-46}{39} < \frac{-39}{39} = -1$$

Donc le première terme du développement en fraction continue est -2, on prend ensuite

$$\frac{-46}{39} + 2 = \frac{32}{39}$$

ATTENTION ! Il ne faut pas faire le développement de $\frac{32}{39}$, mais celui de $\frac{39}{32}$, en effet

$$\frac{-46}{39} = -2 + \frac{32}{39} = -2 + \frac{1}{\frac{39}{32}} = \left[-2, \frac{39}{32}\right]$$

À nouveau algorithme d'Euclide :

$$\begin{aligned} 39 &= 32 \cdot 1 + 7 \\ 32 &= 7 \cdot 4 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

On a donc $\frac{39}{32} = [1, 4, 1, 1, 3]$ et $\frac{-46}{39} = [-2, 1, 4, 1, 1, 3]$.

2. On utilise la relation $[a, b, c] = \left[a, b + \frac{1}{c}\right]$ à répétitions :

$$\begin{aligned} [3, 1, 1, 4, 1, 3] &= \left[3, 1, 1, 4, 1 + \frac{1}{3}\right] = \left[3, 1, 1, 4, \frac{4}{3}\right] \\ &= \left[3, 1, 1, 4 + \frac{3}{4}\right] = \left[3, 1, 1, \frac{19}{4}\right] \\ &= \left[3, 1, 1 + \frac{4}{19}\right] = \left[3, 1, \frac{23}{19}\right] \\ &= \left[3, 1 + \frac{19}{23}\right] = \left[3, \frac{42}{23}\right] \\ &= \left[3 + \frac{23}{42}\right] = \frac{149}{42} \end{aligned}$$

$$\begin{aligned}[-5,1,3,2,4] &= \left[-5,1,3,2+\frac{1}{4}\right] = \left[-5,1,3,\frac{9}{4}\right] \\ &= \left[-5,1,3+\frac{4}{9}\right] = \left[-5,1,\frac{31}{9}\right] \\ &= \left[-5,1+\frac{9}{31}\right] = \left[-5,\frac{40}{31}\right] \\ &= -5+\frac{31}{40} = \frac{-169}{40}\end{aligned}$$

3. C'est une fraction continue finie, qui correspond donc à un nombre rationnel. Or π n'est pas rationnel.

4. En mettant $a+x=\sqrt{n}$ au carré, on obtient

$$\begin{aligned}(a+x)^2 = a^2+2ax+x^2 = n &\Leftrightarrow 2ax+x^2 = n-a^2 \\ &\Leftrightarrow (2a+x)x = n-a^2 \\ &\Leftrightarrow x = \frac{n-a^2}{2a+x}\end{aligned}$$

Bien-sûr, ceci est possible car $2a+x>0$ (en effet, $n \geqslant 1$ donne $\sqrt{n} \geqslant 1$). En posant $f(t) := \frac{n-a^2}{2a+t}$, on obtient $f(x)=x$, donc pour tout $i \in \mathbb{N}^*$, $f^i(x)=x$. Ainsi,

$$\sqrt{n} = a+x = a+f^i(x)\ \forall i \in \mathbb{N}^*$$

soit le résultat voulu.

5. On a $5^2 = 25 < 27 < 36 = 6^2$, donc la partie entière de $\sqrt{27}$ est 5. On a alors

$$\sqrt{27} = 5+(\sqrt{27}-5) = \left[5,\frac{1}{\sqrt{27}-5}\right]$$

Par l'expression conjuguée, on a

$$\frac{1}{\sqrt{27}-5} = \frac{\sqrt{27}+5}{27-25} = \frac{\sqrt{27}+5}{2}$$

Comme la partie entière de $\sqrt{27}$ est 5, celle de $\sqrt{27}+5$ est 10 et celle de $\frac{\sqrt{27}+5}{2}$ est 5, d'où

$$\left[5,\frac{1}{\sqrt{27}-5}\right] = \left[5,\frac{\sqrt{27}+5}{2}\right] = \left[5,5+\frac{\sqrt{27}-5}{2}\right] = \left[5,5,\frac{2}{\sqrt{27}-5}\right]$$

Toujours par expression conjuguée, on a

$$\frac{2}{\sqrt{27}-5} = \frac{2\sqrt{27}+10}{2} = \sqrt{27}+5$$

La partie entière de $\sqrt{27}+5$ est 10, et on a

$$\left[5,5,\frac{2}{\sqrt{27}-5}\right] = \left[5,5,\sqrt{27}+5\right] = \left[5,5,10,\frac{1}{\sqrt{27}-5}\right]$$

On retombe sur $\frac{1}{\sqrt{27}-5}$, que l'on a déjà traîté : on a vu

$$\frac{1}{\sqrt{27}-5} = \left[5,10,\frac{1}{\sqrt{27}-5}\right] = \left[\overline{5,10}\right]$$

et donc $\sqrt{27} = \left[5,\overline{5,10}\right]$.