Correction Partiel 2022-2023

Exercice 1.
(a) Ça se devine : on sait que $10 \cdot 3 = 30 \equiv -1[31]$, donc $10 \cdot (-3) \equiv -(-1) \equiv 1[31]$. Sinon, on utilise l'algorithme d'Euclide :

$$\begin{aligned} 31 &= 10 \cdot 3 + 1 \\ 10 &= 1 \cdot 10 + 0 \end{aligned}$$

Qui donne le même résultat.

(b) Par définition de c_0 et de D, l'entier N s'écrit $10D + c_0$, on a donc

$$\begin{aligned} N = 10D + c_0 &\equiv 10D + 1 \cdot c_0[31] \\ &= 10D + 10 \cdot (-3) \cdot c_0[31] \\ &= 10(D - 3c_0)[31] \end{aligned}$$

Soit le résultat annoncé.

(c) Par la question précédente, N est congru à $10(D-3c_0)$ modulo 31. Donc N est divisible par 31 si et seulement si $10(D - 3c_0)$ est divisible par 31. De plus, comme 10 est premier avec 31, on a que $10(D - 3c_0)$ est divisible par 31 si et seulement si $D - 3c_0$ est divisible par 31. D'où le critère suivant :
"Un entier est divisible par 31 si et seulement si son nombre de dizaines moins trois fois son chiffre des unités est divisible par 31.

(d) On pose $N_0 = 69750$, $D_0 = 6975$ son nombre de dizaines et $c_0 = 0$ son chiffre des unités. Par la question précédente, N est divisible par 31 si et seulement si $N_1 := D_0 - 3c_0 = 6975$ l'est.
On applique à nouveau le critère précédent à $N_1 = 6975$, on a $D_1 = 697$ et $c_1 = 5$. Donc N_1 est divisible par 31 si et seulement si $N_2 = 697 - 3 \cdot 5 = 682$ l'est.
On applique à nouveau le critère précédent à $N_2 = 682$, on a $D_2 = 68$ et $c_2 = 2$. Donc N_2 est divisible par 31 si et seulement si $N_3 = 68 - 3 \cdot 2 = 62$ l'est.
Or on a $62 = 31 \cdot 2$, donc N_3, N_2, N_1 et N_0 sont divisibles par 31.

(e) On peut généraliser cette méthode en remplaçant 31 par tout entier n premier avec 10 : Si n est un tel entier, il existe un entier ℓ avec $10\ell \equiv 1[n]$. Dans ce cas, pour tout $N \in \mathbb{N}$, on a $N \equiv 10(D + \ell c_0)[n]$ avec le même raisonnement qu'à la question (b). On trouve alors que N est divisible par n si et seulement si $D + \ell c_0$ l'est.

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 a où Alice va au cinéma sont régis par l'équation $a \equiv 0[25]$ car elle est allée au cinéma aujourd'hui et elle y va tous les 25 jours. De même, les jours b où Bob va au cinéma sont régis par l'équation $b \equiv -3[31]$.

Les jours où Alice et Bob vont au cinéma sont donc les solutions d du système de congruence

$$\begin{cases} d \equiv 0[25] \\ d \equiv -3[31] \end{cases}$$

Comme 25 et 31 sont premiers entre eux, les solutions de ce système sont égales modulo $25 \vee 31 = 775$. On cherche une solution particulière à notre système, il suffit pour cela de trouver une solution d' du système

$$\begin{cases} d' \equiv 0[25] \\ d' \equiv 1[31] \end{cases}$$

et de poser $d = -3d'$. On a

$$d' = 1 + 31p = 25q \Leftrightarrow 1 = 25q - 31p$$

On trouve une solution de cette équation de Bézout en utilisant l'algorithme d'Euclide :

$$31 = 25 \cdot 1 + 6$$
$$25 = 6 \cdot 4 + 1$$

Qui donne $1 = 25 - 6 \cdot 4 = 25 \cdot 5 - 31 \cdot 4$. On obtient donc une solution $d' = 125$ du deuxième système. Les solutions du premier système sont exactement les entiers congrus à -375 modulo $[775]$. Le plus petit entier positif respectant cette dernière équation est $-375 + 775 = 400$. On obtient donc que Alice et Bob iront au cinéma le même jour dans 400 jours, et ensuite tous les 775 jours.

Exercice 3.

(a) On cherche les racine du polynôme $X^2 - 1$ dans $\mathbb{Z}/n\mathbb{Z}$. On a $X^2 - 1 = (X - 1)(X + 1)$, donc

$$x^2 \equiv [n] \Leftrightarrow (x - 1)(x + 1) \equiv 0[n]$$

Comme n est premier, $Z/n\mathbb{Z}$ est intègre, donc ceci équivaut à $x - 1 \equiv 0[n]$ ou $x + 1 \equiv 0[n]$. On a donc deux solutions de $x^2 \equiv 1[n]$: $x = 1$ et $x = -1$. Notons que si n n'est pas premier, on peut avoir d'avantage de solutions : $4^2 = 1[15]$ alors que $4 \not\equiv 1, -1[15]$.

(b) Comme n est premier, tous les entiers de $\{1, \dots, n-1\}$ admettent un unique inverse modulo $\mathbb{Z}/n\mathbb{Z}$. On sait d'ailleurs que 1 et $n - 1$ sont leurs propres inverses modulo n (car $1^2 \equiv 1[n]$ et $(n-1)^2 \equiv (-1)^2 \equiv 1[n]$). Un entier $k \in \{2, \dots, n-2\}$ admet donc un unique inverse modulo n dans $\{2, \dots, n-2\}$, en effet, l'inverse de k ne peut être 1 où $n - 1$ car k n'est pas égal ni à 1, ni à $n - 1$.

En réordonnant le produit $2 \dots n-2$, on peut donc l'écrire comme des produits d'éléments de $\{2, \dots, k\}$ et de leurs inverses. Le produit est alors égal à 1 modulo n. On a alors $(n-1)! \equiv 1 \cdot (n-1)[n] \equiv -1[n]$

(c) Supposons que n est non premier, et soit p le plus petit diviseur de n non égal à 1. On pose $n = pq$.

- Si $p < q$, alors les entiers p et q apparaissent dans le produit $(n-1)!$, donc n divise $(n-1)!$ et $(n-1)! = 0$.
- Si $p = q$, alors $n = p^2$. Si $p = 2$, alors $n = 4$, et il est clair que $3! = 6 \equiv 2[4]$. Si $p > 2$ alors $p^2 = n > 2p$. Donc p et $2p$ sont deux entiers plus petit que $n - 1$, qui apparaissent donc dans le produit $(n-1)!$. Donc $2p^2 = 2n$ divise $(n-1)!$ et $(n-1)! \equiv 0[n]$.

(d) On a montré à la question (b) que si n est premier, alors $(n-1)! \equiv -1[n]$. Et on a montré à la question (c) que si n n'est pas premier, alors $(n-1)! \not\equiv -1[n]$.

Exercice 4.

(a) On utilise l'algorithme d'Euclide :

$$22 = 19 \cdot 1 + 3$$
$$19 = 3 \cdot 6 + 1$$
$$3 = 1 \cdot 3 + 0$$

Cet algorithme nous donne :

$$\frac{22}{19} = 1 + \frac{3}{19}, \quad \frac{19}{3} = 6 + \frac{1}{3}$$

On a donc

$$22/9 = \left[1 + \frac{3}{19}\right] = \left[1, \frac{19}{3}\right] = \left[1, 6 + \frac{1}{3}\right] = [1, 6, 3]$$

(b) On a $n < \sqrt{n^2 + 1} < n + 1$, en effet en passant le tout au carré, il est clair que

$$n^2 < n^2 + 1 < n^2 + 2n + 1$$

On calcule donc

$$\sqrt{n^2+1} = n + (\sqrt{n^2+1} - n) = \left[n, \frac{1}{\sqrt{n^2+1}-n}\right]$$

En utilisant la quantité conjugué, on a

$$\frac{1}{\sqrt{n^2+1}-n} = \frac{\sqrt{n^2+1}+n}{(\sqrt{n^2+1}-n)(\sqrt{n^2+1}+n)} = \frac{\sqrt{n^2+1}+n}{n^2+1-n^2} = \sqrt{n^2+1}+n$$

La partie entière de $\sqrt{n^2+1}+n$ est bien-sur $2n$, on a alors

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

En réappliquant le même raisonnement sur $\frac{1}{\sqrt{n^2+1}-n}$, on trouve par récurrence immédiate

$$\sqrt{n^2+1} = [n, \overline{2n}]$$

(c) On pose $x = [\overline{1,4}]$, on a

$$\begin{aligned} x = [\overline{1,4}] &= [1,4,x] \\ &= \left[1, 4 + \frac{1}{x}\right] \\ &= \left[1, \frac{4x+1}{x}\right] \\ &= 1 + \frac{x}{4x+1} \\ &= \frac{5x+1}{4x+1} \end{aligned}$$

Donc x respecte l'équation $x(4x+1) = 5x+1$, qui équivaut à $4x^2 - 4x - 1 = 0$. Les solutions de cette équation sont

$$\frac{4 \pm \sqrt{32}}{8} = \frac{1 \pm \sqrt{2}}{2}$$

Comme $\sqrt{2} > 1$, une seule de ces solutions est positive, c'est celle là qui est égale à x (le premier terme de la réduction en fraction continue de x est positif, donc x est positif).

D'après le paragraphe précédent, on a

$$[1, \overline{1,4}] = \left[1, \frac{1+\sqrt{2}}{2}\right] = 1 + \frac{2}{1+\sqrt{2}} = \frac{1+\sqrt{2}+2}{1+\sqrt{2}}$$