Mathématiques pour l'informatique. L1 Informatique I23.

TD 7. Arithmétique [1]

EXERCICE 1. Déterminez les entiers naturels n tels que $n \mid n+8$.

Solution. Soit $n \in \mathbb{N}$ tel que $n \mid n+8$. Par définition de la relation de divisibilité sur $\mathbb{N}$, il existe un entier naturel k tel que $k\,n = n+8$. On en déduit que $n\,(k-1) = 8$ et donc que n divise 8. Il existe 4 diviseurs de 8, les entiers 1, 2, 4 et 8.

EXERCICE 2. Déterminez les entiers naturels n tels que leur division euclidienne par 3 donne un quotient égal au double du reste.

Solution. Soit $n \in \mathbb{N}$. Le théorème de la division euclidienne nous fournit un couple (q, r) tel que $n = 3\,q + r$ et $0 \leqslant r < 3$, et l'hypothèse de l'énoncé $q = 2\,r$. On en déduit que $n = 7\,r$ avec les 3 restes possibles $r = 0$, $r = 1$ ou $r = 2$, aboutissant respectivement aux 3 solutions $n = 0$, $n = 7$ ou $n = 14$.

EXERCICE 3. Déterminez les entiers naturels n tels que les quotients de la division euclidienne de n par 65 et par 79 sont identiques et les restes respectifs sont 63 et 7 ?

Solution. On note q le quotient commun aux deux divisions euclidiennes de n, par 65 et 79. On a donc :

$$n = 65q + 63$$
$$n = 79q + 7$$

Par transitivité de l'égalité, on en déduit que $65q + 63 = 79q + 7$ soit $14q = 56$. Comme $14 \mid 56$, on en déduit qu'il y a une solution avec le quotient $q = 4$ qui donne $n = 323$.

1. version du 18 mai 2023, 09 : 42

EXERCICE 4. Démontrez que la relation de divisibilité dans $\mathbb{Z}$ définie par *"a divise b, noté $a \mid b$, si et seulement s'il existe $c \in \mathbb{Z}$ tel que $ac = b$"* est réflexive, transitive mais n'est ni symétrique ni antisymétrique (ce n'est donc ni une relation d'équivalence, ni une relation d'ordre).

Solution. La relation est réflexive puisque pour tout entier relatif a on a $a.1 = a$. Elle est également transitive puisque si a, b et c sont trois entiers relatifs tels que $a \mid b$ et $b \mid c$, alors il existe $(k, l) \in \mathbb{Z} \times \mathbb{Z}$ tel que $ak = b$ et $bl = c$, donc $(ak)l = a(kl) = c$, ce qui montre que soit a divise c. En revanche elle n'est pas symétrique puisque $2 \mid 4$ mais $4 \nmid 2$ ni antisymétrique, car pour tout entier naturel $n \neq 0$, $n \mid (-n)$ et $(-n) \mid n$ et pourtant $n \neq (-n)$.

EXERCICE 5. Soit $n \in \mathbb{N}$. Démontrez qu'un entier $x \in \mathbb{Z}$ est un multiple de n si et seulement si le reste de la division euclidienne de x par n est nul.

Solution. Supposons que $x \in \mathbb{Z}$ soit un multiple de n. Alors il existe un entier $q \in \mathbb{Z}$ tel que $x = n\,q$, autrement dit d'après le théorème de la division euclidienne, q est le quotient de la division de x par n et le reste est nul. Réciproquement, si on note q le quotient de la division euclidienne de x par n et que le reste est nul alors $x = n\,q$ et x est bien un multiple de n.

EXERCICE 6. Soit n un entier naturel. Démontrez que la relation de congruence modulo n définie sur $\mathbb{Z}$ par *"x est congru à y modulo n, noté $x \equiv y \pmod{n}$, si et seulement si $y - x \in n\mathbb{Z}$"* est compatible avec l'addition dans $\mathbb{Z}$.

Solution. Rappelons que les relations d'équivalence compatibles avec une loi de composition interne sur un groupe $(G, +)$ sont nécessairement de la forme $y - x \in H$ où H est un sous-groupe normal de G (cf. théorème), or on sait que le groupe $(\mathbb{Z}, +)$ est commutatif et par conséquent tous ses sous-groupes $n\mathbb{Z}$ sont normaux.

Preuve alternative : soit $(x, x', y, y') \in \mathbb{Z}^4$ tels que $x \equiv x' \pmod{n}$ et $y \equiv y' \pmod{n}$:

$$\exists (k, \ell) \in \mathbb{Z}^2 \quad (x' - x = k\,n) \ \wedge \ (y' - y = \ell\,n). \tag{1}$$

Il faut montrer que $(x+y) \equiv (x'+y') \pmod{n}$, c'est-à-dire qu'il existe $m \in \mathbb{Z}$ tel que $(x'+y')-(x+y) = m\,n$. En additionnant les deux égalités de (1), on obtient

$$(x'-x)+(y'-y) = k\,n+\ell\,n$$
$$(x'+y')-(x+y) = (\underbrace{k+\ell}_{m})\,n.$$

EXERCICE 7. Démontrez les assertions suivantes :

(1) $\forall (a,b,c) \in \mathbb{Z}^3 \quad a \mid b \;\Rightarrow\; a \mid bc$,

(2) $\forall (a,b,c) \in \mathbb{Z}^3 \quad \big((a \mid b) \wedge (a \mid c)\big) \;\Rightarrow a \mid (b+c)$,

(3) $\forall (a,a',b,b') \in \mathbb{Z}^4 \quad \big((a \mid a') \wedge (b \mid b')\big) \;\Rightarrow ab \mid a'b'$,

(4) $\forall (a,b) \in \mathbb{Z}^2 \;\forall n \in \mathbb{N} \quad a \mid b \;\Rightarrow\; a^n \mid b^n$.

Solution. **(1)** On a $a \mid b \Leftrightarrow \exists k \in \mathbb{Z}\; a\,k = b$, donc $\forall c \in \mathbb{Z}$, $a\,k\,c = b\,c$, i.e. $a \mid b\,c$.

(2) On a $(a \mid b) \wedge (a \mid c) \Leftrightarrow \exists (k,\ell) \in \mathbb{Z}^2 \;\; a\,k = b \;\wedge\; a\,\ell = c$. En sommant ces deux égalités, on obtient $a\,(k+l) = b+c$ ce qui prouve que $a \mid (b+c)$.

(3) On a $(a \mid a') \wedge (b \mid b') \Leftrightarrow \exists (k,\ell) \in \mathbb{Z}^2 \;\; a\,k = a' \;\wedge\; b\,\ell = b'$. Cette fois on fait le produit des deux égalités pour obtenir $a\,b\,k\,\ell = a'\,b'$ ce qui prouve que $a\,b \mid a'\,b'$.

(4) Soit $(a,b) \in \mathbb{Z}^2$ et le prédicat $P(k)$ défini par $a \mid b \Rightarrow\; a^k \mid b^k$. On a trivialement $P(1)$. Soit $k \in [\![0, n-1]\!]$. D'après l'hypothèse de récurrence on a $a^n \mid b^n$ et il suffit d'appliquer le résultat précédent sur $a \mid b \wedge a^n \mid b^n$ pour conclure que $P(n+1)$ est vrai.

EXERCICE 8. La somme des âges (non-nuls) de trois frères est égale à 39, l'aîné a deux fois l'âge du benjamin (le plus jeune donc). Quels sont les âges des trois frères ? Indication : ne pas faire une étude de cas directe, utiliser la division euclidienne.

Solution. On peut modéliser aisément le problème avec trois entiers naturels A, B et C codant respectivement l'âge de l'aîné, du benjamin et du cadet, et on déduit de l'énoncé que ces entiers doivent satisfaire le système suivant :

$$A+B+C = 39$$
$$A = 2B$$

Rappelons qu'être le cadet est une notion *relative* (on est le cadet de quelqu'un), autrement dit on peut être à la fois cadet et benjamin. Donc par défaut, on a

$$A \geqslant C \geqslant B \geqslant 0. \tag{2}$$

Mais on peut affiner ces inégalités, en effet l'âge du benjamin est strictement positif, sans quoi l'aîné aurait également un âge nul et la somme des trois âges ne pourrait être égale à 39. D'autre part, si l'âge du cadet était égal à celui du benjamin, i.e. $C = B$, alors $A+B+C = 4C$ or $4 \nmid 39$. De la même manière, si l'âge de l'aîné était égal à celui du cadet, i.e. $A = C$, alors $A+B+C = 5B$ et $5 \nmid 39$, on a donc

$$A > C > B > 0. \tag{3}$$

En remplaçant A par $2B$ dans la première égalité, on obtient

$$3B + C = 39. \tag{4}$$

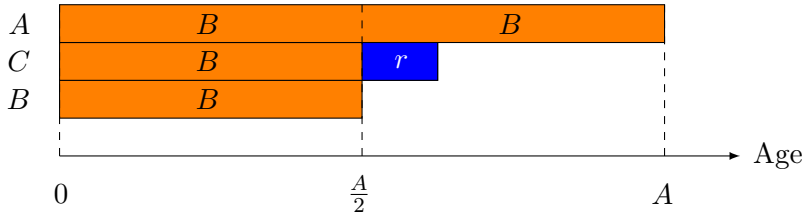

Figure 1. Les âges des trois frères.

Nous ne disposons que d'une équation pour deux inconnues, on ne peut pas conclure. La première démarche qui vient à l'esprit est de faire une étude de cas, mais il faut réaliser que si les valeurs numériques étaient plus grandes, cette approche serait fastidieuse voire impossible. Comme $A = 2B$, on déduit de (2) que $B < C < 2B$ et d'après le théorème de la division euclidienne, il existe un unique r tel que $C = B + r$ avec $0 \leqslant r < B$, et même $0 < r < B$ puisque le reste ne peut pas être nul ici. La figure 1 met en évidence les rapports d'âge entre les frères, on en tire

$$39 = 4B + r. \tag{5}$$

Il faut donc trouver tous les couples (B,r) avec $0 < r < B$ qui satisfont l'équation (5), ce qui nous conduit à considérer la division euclidienne de 39 par B sachant que le quotient vaut 4 (attention il est tentant ici de

considérer la division euclidienne par 4, mais ici $r < B$ et pas $r < 4$). Puisque $0 < r < B$, on déduit de (5) que

$$4B \leqslant 39 < 5B.$$

Donc $\lfloor \frac{39}{5} \rfloor < B \leqslant \lfloor \frac{39}{4} \rfloor$, soit $7 < B \leqslant 9$ et il ne reste que les valeurs $B = 8$ et $B = 9$ à tester ce qui nous donne les triplets $(A, C, B) = (16, 15, 8)$ et $(A, C, B) = (18, 12, 9)$ solutions du problème.

EXERCICE 9. Quel est le nombre de diviseurs positifs de 1 296 ? Indication : décomposez ce nombre en produit de facteurs premiers. Généralisez le résultat à un entier naturel quelconque.

Solution. On a $1\,296 = 2^4\,3^4$. La décomposition en produits de facteurs premiers d'un diviseurs de 1 296 s'écrit donc $2^k\,3^\ell$ avec $0 \leqslant k \leqslant 4$ et $0 \leqslant \ell \leqslant 4$, il y a donc 25 diviseurs distincts. Plus généralement,

$$n = \prod_{i=1}^{k} p_i^{n_i} \;\Rightarrow\; \#\{k \in \mathbb{N} \mid k|n\} = \prod_{i=1}^{k} (n_i + 1).$$

EXERCICE 10. Calculez $(294, 350)$ en décomposant ces deux nombres en produits de facteurs premiers puis utilisez l'algorithme du PGCD d'Euclide.

Solution. On a $294 = 2.3.7^2$ et $350 = 2.5^2.7$. On en déduit que leur plus grand diviseur commun $(294, 350) = 2.7 = 14$. Il faut remarquer que cette technique est totalement inefficace, la décomposition naïve en produit de facteurs premiers d'un entier naturel n nécessitant un nombre de divisions euclidiennes proportionnel à n, si l'on excepte quelques rares petits diviseurs (2, 3, 5, 9, 11) pour lesquels les critères de divisibilité évitent la division.

Ici l'algorithme du PGCD d'Euclide ne demande que 4 divisions euclidiennes en comparaison :

$$\begin{aligned} 294 &= 350 \times 0 + 294 \\ 350 &= 294 \times 1 + 56 \\ 294 &= 56 \times 5 + 14 \\ 56 &= 14 \times 4 + 0. \end{aligned}$$

EXERCICE 11. **(1)** Soit n un entier naturel non-nul. Démontrez que pour trouver tous les diviseurs d de n, on peut se contenter de tester la divisibilité des valeurs de l'intervalle $[\![2, \lfloor \sqrt{n} \rfloor]\!]$ dans l'ordre croissant.

(2) Un entier naturel $n \leqslant 160$ n'est divisible par aucun des 5 premiers nombres premiers. Est-il premier ?

Solution. **(1)** Si d est un diviseur de n, alors il existe $d' \in \mathbb{N}$ tel que $d\,d' = n$ et d' est également un diviseur de n. Si $d > \sqrt{n}$ alors $d' < \sqrt{n}$, or si l'on a testé tous les diviseurs de n inférieurs à $\sqrt{n}$, on a déjà testé d'.

(2) Il est inutile de tester les diviseurs premiers p de 160 si $p^2 > 160$, on peut donc s'arrêter à $p = 11$ puisque $13^2 = 169$. Or les 5 premiers nombres premiers sont $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ et $p_5 = 11$, donc n est premier.

EXERCICE 12. On note $(p_i)_{i \in \mathbb{N}^*}$ la suite croissante des nombres premiers, i.e. $p_1 = 2$, $p_2 = 3$, etc. Soit $n \in \mathbb{N}$ et $n \geqslant 1$. On définit le produit partiel π_n des nombres premiers

$$\pi_n := \prod_{i=1}^{n} p_i.$$

Quelle est la plus petite valeur a de n telle que $\pi_n + 1$ n'est pas un nombre premier ? Quelle est la décomposition en produit de facteurs premiers de $1 + \pi_a$?

Solution. On résume les calculs dans la table ci-dessous en notant π_i le produit des p_k pour tout $k \in [\![1, i]\!]$:

i	1	2	3	4	5	6	7
p_i	2	3	5	7	11	13	17
π_i	2	6	30	210	2 310	30 030	510 510
$\pi_i + 1$	3	7	31	211	2 311	30 031	510 511
primalité	p_2	p_4	p_{11}	p_{47}	p_{344}	59×509	

TABLE 1. Premières valeurs de π_n.

La plus petite valeur est donc $a = 6$.

EXERCICE 13. † Soit k un entier naturel impair. Démontrez que

$$\forall n \in \mathbb{N}\backslash\{0\} \quad \sum_{i=1}^{n} i^k \quad \text{est divisible par } \frac{n(n+1)}{2} \tag{6}$$

Indication : en notant $S(n,k)$ la somme de la proposition (6) calculez la somme $S(n,k)+S(n,k)$ dans $\mathbb{Z}/n\mathbb{Z}$ en appariant les termes i^k et $(n-i)^k$ puis en appariant les termes i^k et $(n-i+1)^k$.

Solution. On écrit la somme $S(n,k)$ une première fois dans le sens croissant des indices et une autre dans le sens décroissant avant de sommer :

$$\begin{array}{rcccccccc} S(n,k) & = & 0^k & + & 1^k & + & \cdots & + & n^k \\ S(n,k) & = & n^k & + & (n-1)^k & + & \cdots & + & 0 \\ 2S(n,k) & = & \underbrace{0^k+n^k}_{\equiv 0 \pmod n} & + & \underbrace{1^k+(n-1)^k}_{\equiv 0 \pmod n} & + & \cdots & + & \underbrace{n^k+0^k}_{\equiv 0 \pmod n} \end{array}$$

Mais dans $\mathbb{Z}/n\mathbb{Z}$, $(n-i)^k = (-i)^k$ et si k est impair, on a $(-i)^k = -(i^k)$, donc $2S(n,k) = 0$ dans $\mathbb{Z}/n\mathbb{Z}$ ce qui prouve que $n \mid 2S(n,k)$. On refait le même raisonnement mais cette fois en regroupant les termes i^k et $(n-i+1)^k$ pour prouver que $(n+1) \mid 2S(n,k)$ et donc que $n(n+1) \mid 2S(n,k)$ soit

$$\frac{n(n+1)}{2} \mid \sum_{i=0}^{n} i^k.$$

EXERCICE 14. On suppose que les représentants de $\mathbb{Z}/26\mathbb{Z}$ sont les entiers de l'intervalle $[\![0,25]\!]$. On note $\mathscr{A} := \{A, B, \ldots, Z\}$ l'alphabet latin et on définit l'application $f : \mathbb{Z}/26\mathbb{Z} \to \mathscr{A}$ par $f(i) :=$ $(i+1)$-ème lettre de $\mathscr{A}$.

(1) On munit $\mathbb{Z}/26\mathbb{Z}$ de l'ordre $\leqslant$ induit par $\mathbb{Z}$ et $\mathscr{A}$ de l'ordre alphabétique $\leqslant_{\mathscr{A}}$. Démontrer que f est un isomorphisme d'ensembles ordonnés.

(2) Démontrez que l'application $a_k : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ définie par $a_k(x) = x+k$ est une bijection. Quelle est sa bijection réciproque ?

(3) Formalisez le chiffrement de César avec un décalage circulaire de k lettres à l'aide d'une application $e_k : \mathscr{A} \to \mathscr{A}$ définie à partir de la bijection f qui identifie les ensembles $\mathscr{A}$ et $\mathbb{Z}/26\mathbb{Z}$ et de l'application a_k.

(4) Écrivez les fonctions *Python* `f(x)`, `g(x)` (pour l'application réciproque f^{-1}), `a(k,x)` et `e(k,x)` qui calculent les fonctions définies précédemment.

(5) Montrez que e_k est une permutation de $\mathfrak{S}(\mathscr{A})$.

(6) Combien existe-t-il d'orbites suivant la permutation e_k ?

Solution. **(1)** L'application f est évidemment injective puisque deux indices distincts donnent deux lettres distinctes, elle est donc bijective puisque les ensembles de départ et d'arrivée sont finis et de même cardinal. Pour tout $(i,j) \in (\mathbb{Z}/26\mathbb{Z})^2$ on a $(i \leqslant j) \Leftrightarrow (f(i) \leqslant_{\mathscr{A}} f(j))$, où $\leqslant_{\mathscr{A}}$ désigne l'ordre alphabétique, l'application f et sa réciproque f^{-1} sont donc croissantes. Comme f est de surcroît bijective, c'est donc un *iso*morphisme d'ensembles ordonnés.

(2) On vérifie immédiatement que $a_k \circ a_{-k} = \mathrm{Id}_{\mathbb{Z}/26\mathbb{Z}}$, ce qui prouve à la fois que a_k est bijective et que sa bijection réciproque $a_k^{-1} = a_{-k}$.

(3) Le diagramme commutatif de la figure 2 illustre que le chiffrement de César consiste à transformer une lettre en un nombre, à ajouter k à ce nombre et à convertir la valeur obtenue en lettre. On en déduit que $e_k = f \circ a_k \circ f^{-1}$.

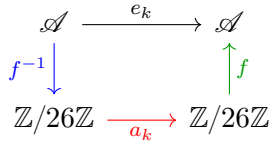

FIGURE 2. Diagramme commutatif pour le chiffrement de César.

(4) La conversion d'une lettre en nombre se fait grâce à la fonction `ord()` du *Python*, mais il faut soustraire le code numérique du caractère `'A'` pour s'aligner en 0. La conversion d'un nombre en lettre se fait avec la fonction réciproque `chr()`. L'addition par k dans $\mathbb{Z}/26\mathbb{Z}$ se fait grâce au reste de la division euclidienne par 26.

```
def f(x):
    return (chr(x + ord('A')))

def a(k,x):
    return (x + k) % 26
```

```
def g(x):
    return(ord(x) - ord('A'))

def e(k,x):
    return f(a(k,g(x)))
```

(5) Nous avons déjà montré que e_k est une bijection, elle permute donc les lettres de l'alphabet $\mathscr{A}$.

(6) L'étude se fait sur l'application a_k en transportant la permutation des lettres sur la permutation des entiers modulo 26 via f. Si $k \equiv 0 \pmod{26}$, alors $a_k = \mathrm{Id}$ et il y a autant d'orbites que de points fixes, à savoir 26, sinon le nombre d'orbites dépend du PGCD de k et 26. En effet, la taille de l'orbite d'un élément x de $\mathbb{Z}/26\mathbb{Z}$ est égal à son ordre dans $\mathfrak{S}(\mathbb{Z}/26\mathbb{Z})$, c'est-à-dire le plus petit entier non-nul p tel que $a_k^p(x) = x$, autrement dit tel que

$$x + p.k = x$$

En simplifiant par x, on cherche donc le plus petit entier p non-nul tel que

$$p.k = 0$$

et k et p sont donc des diviseurs de zéro dans $\mathbb{Z}/26\mathbb{Z}$. Un entier $k \in \mathbb{Z}/26\mathbb{Z}$ non-nul est un diviseur de zéro si et seulement s'il n'est pas premier avec 26. On en déduit *a contrario* que si $(k, 26) = 1$, il n'est pas un diviseur de 0, donc a_k est un 26-cycle et il n'y a qu'une seule orbite de cardinal 26. Sinon, l'ordre de tout élément non-nul de $\mathbb{Z}/26\mathbb{Z}$ est égal à $\frac{26}{(k,26)}$ et il y a donc $(k, 26)$ orbites. Par exemple pour $k = 4$, on a $(4, 26) = 2$, on a donc 2 orbites de taille 13, les valeurs paires dans l'une, impaires dans l'autre.

EXERCICE 15. Le premier janvier 2000 était un samedi. Quel jour de la semaine était le 275-ème jour de l'année 2000 ?

Solution. Les samedis sont donc les jours dont les restes par la division euclidienne par 7 est égal à 1. On a $275 = 39.7 + 2$, le reste étant égal à 2 il s'agit d'un dimanche.

EXERCICE 16. Le compas d'un bateau à la dérive tourne de 7° dans le sens horaire toutes les 8 minutes. Quelle direction indique le compas après 3 jours, 2 heures et 32 minutes si la direction initiale était de 23° ?

Solution. Le bateau dérive de 7° toutes les 8 minutes, on exprime la durée de la dérive en minutes et on divise par 8 :

$$3 \times 24 \times 60 + 2 \times 60 + 32 = 4\,472 \text{ minutes.}$$

Comme $4\,472 = 559 \times 8 + 0$, le compas a donc tourné 559 fois de 7° durant cette période, soit de $(559 \times 7° = 3\,913°$ ce qui nous donne un angle de $3\,913 \equiv 313 \pmod{360}$ degrés à rajouter aux 23° degré de départ, soit 336°.

EXERCICE 17. Vérifiez que $\forall a \in \mathbb{Z}\backslash\{0\}\ \ (a, 0) = a$ et que $\forall a \in \mathbb{Z}\ \ (a, 1) = 1$.

Solution. Par définition $(a, 0)$ est le plus grand commun diviseur de a et 0, et comme a divise a et 0, on a $(a, 0) = a$. L'entier 1 est le plus grand diviseur de 1 et divise a, on a $(a, 1) = 1$.

EXERCICE 18. Calculez le PGCD de 231 et 182 avec l'algorithme d'Euclide.

Solution. On a $(231, 182) = 7$:

$$\begin{aligned} 231 &= 182 \times 1 + 49 \\ 182 &= 49 \times 3 + 35 \\ 49 &= 35 \times 1 + 14 \\ 35 &= 14 \times 2 + 7 \\ 14 &= \boxed{7} \times 2 + 0 \end{aligned}$$

EXERCICE 19. Montrez qu'il n'existe pas d'entiers naturels a et b tels que leur somme est égale à 101 et dont le pgcd est égal à 3.

Solution. Par l'absurde, supposons que $a + b = 101$ et $(a, b) = 3$. Alors $3 \mid a$ et $3 \mid b$ ce qui se traduit par l'existence de deux entiers k et l tels que $a = 3\,k$ et $b = 3\,l$ que l'on remplace dans $a + b = 101$ pour obtenir $3(k + l) = 101$. Mais $1 + 0 + 1 = 2$ donc 101 n'est pas divisible par 3 ce qui contredit l'hypothèse.

EXERCICE 20. Pour un examen, on a réparti 367 étudiants dans 9 salles de même capacité en remplissant chaque salle avant d'en ouvrir une autre. Quelle était la capacité des salles et combien d'étudiants composeront dans la dernière salle d'examen ?

Solution. Il y a donc 8 salles pleines et une 9-ème pour les étudiants restants. On en déduit que la division euclidienne de 367 par 8 devrait fournir un reste non-nul si les valeurs sont cohérentes dans l'énoncé. On calcule la division euclidienne $367 = 8.45 + 7$, les 8 salles ont donc chacune une capacité de 45 places et la 9-ème salle accueille le 7 étudiants qui restent.

EXERCICE 21. † Un chef de chantier essaie d'organiser la construction d'une villa dans le Var. Il doit faire intervenir deux artisans le même jour. Le premier n'est disponible qu'un jour sur 6, l'autre une fois tous les 11 jours. Le chef de chantier a pu rencontrer le premier artisan le mardi 12 mars et le second le jeudi 14 mars. Quel jour doit-il leur donner rendez-vous pour leur faire effectuer les travaux le plus tôt possible ?

Solution. En notant P (resp. S) le jour où il peut rencontrer le premier artisan (resp. le second artisan), on déduit de l'énoncé les deux congruences suivantes :

$$P \equiv 12 \equiv 0 \pmod 6$$
$$S \equiv 14 \equiv 3 \pmod{11}$$

Ce qui se traduit par l'existence de deux entiers k et l tels que $P = 6\,k$ et $S = 11\,l + 3$. Pour assurer l'égalité $P = S$, il faut résoudre l'équation diophantienne

$$6\,k - 11\,l = 3. \tag{7}$$

Comme $(6, 11) = 1$, il existe un couple solution (a, b) solution de l'équation $6\,a - 11\,b = 1$ et le couple $(k, l) := 3(a, b)$ sera solution de (7). On applique l'algorithme d'Euclide étendu au couple $(6, -11)$:

$$-11 = (-2).6 + 1$$
$$6 = 6.\boxed{1} + 0$$

On en déduit que $6.2 - 11 = 1$ et que $(k, l) = 3.(2, 1) = (6, 3)$ d'où $P = S = 36$ et le rendez-vous est à fixer le $36 - 12 = 24$ jours après le 12 mars.

EXERCICE 22. Calculez l'ordre du sous-groupe de $(\mathbb{Z}/16\mathbb{Z}, +)$ engendré par 6.

Solution. On calcule successivement les éléments de ce sous-groupe :

$$6 + 6 \equiv 12 \pmod{16} \quad 12 + 6 \equiv 2 \pmod{16} \quad 2 + 6 \equiv 8 \pmod{16}$$
$$8 + 6 \equiv 14 \pmod{16} \quad 14 + 6 \equiv 4 \pmod{16} \quad 4 + 6 \equiv 10 \pmod{16}$$
$$10 + 6 \equiv 0 \pmod{16}$$

On a donc $\mathrm{gr}(6) = \{0, 6, 12, 2, 8, 14, 4, 10\}$ sous-groupe d'ordre $8 \mid 16$.

EXERCICE 23. Démontrez la proposition suivante :
Soit $n \in \mathbb{N}\backslash\{0\}$, alors $\forall (a, b, c, d) \in \mathbb{Z}^4$, on a

$$\begin{cases} a \equiv b \pmod n \\ c \equiv d \pmod n \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \pmod n \\ ac \equiv bd \pmod n \end{cases}$$

Solution. Soit $(a, b, c, d) \in \mathbb{Z}^4$, tels que $a \equiv b \pmod n$ et $c \equiv d \pmod n$. Il existe donc deux entiers k et l tels que $a - b = kn$ et $c - d = ln$ et en additionnant les deux égalités on obtient $(a+c)-(b+d) = (k+l)n$ ce qui prouve que $a + c \equiv b + d \pmod n$. D'autre part, $a = b + kn$ et $c = d + ln$ et en faisant le produit on obtient :

$$\begin{aligned} ac &= (b + kn)(d + ln) \\ &= bd + lbn + kdn + kln^2 \\ &= bd + (lb + kd + kln)n \end{aligned}$$

ce qui prouve que $a.c \equiv bd \pmod n$.

EXERCICE 24. Comment lire dans la table de multiplication de $\mathbb{Z}/n\mathbb{Z}$ si un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est inversible ? Dans ce cas, comment trouver son inverse ? Quel est l'inverse de 7 modulo 25 ? Quel est l'inverse de 11 modulo 26 ?

Solution. Il suffit de chercher si la valeur 1 apparaît sur la ligne correspondant à x. Dans ce cas le nombre sur la colonne où apparaît ce 1 est son inverse.
L'inverse de 7 modulo 25 est égal à 18. L'inverse de 11 modulo 26 est égal à 19. Notons que l'existence de ces inverses est assurée par $(7, 25) = 1$ et $(11, 26) = 1$.

EXERCICE 25. † Retrouvez les critères de divisibilité d'un nombre a (représenté en base 10) par un nombre n pour $n \in \{2, 3, 5, 9, 10, 11\}$.

Solution. On rappelle que la surjection canonique $\varphi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux, donc l'image d'une somme ou d'un produit est la somme ou le produit des images. Par conséquent, si l'on note $(a_i)_{i\in[\![0,k]\!]}$ les $k + 1$ chiffres de a dans son écriture en base 10, on a

$$a = \sum_{i=0}^{k} a_i 10^i \;\Rightarrow\; \varphi_n(a) = \sum_{i=0}^{k} \left(\varphi_n(a_i)\varphi_n(10)^i\right). \tag{8}$$

Le nombre a est divisible par n si le reste de la division euclidienne de a par n est nul, et dans ce cas son image $\varphi_n(a)$ dans l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ est égale à 0.

Calculons l'image de a dans l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ pour les trois valeurs $n \in \{2, 5, 10\}$. Toutes les puissances non-nulles de 10 ont un reste modulo 2, 5 ou 10 égal à 0, on a donc $\varphi_n(10^i) = 0$ pour tout $i > 0$ et bien sûr $\varphi_n(1O^0) = \varphi_n(1) = 1$. Par conséquent, pour ces 3 valeurs particulières, $\varphi_n(a) = \varphi_n(a_0)$, autrement dit l'image de a dans l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ ne dépend que du chiffre des unités a_0 de a. Le nombre a est donc divisible par 2 si a_0 est pair, divisible par 5 si $a_0 \in \{0, 5\}$ et divisible par 10 si $a_0 = 0$.

Faisons de même pour les valeurs $n \in \{3, 9\}$. Le reste de la division euclidienne d'une puissance de 10 par 9 est toujours égal à 1, donc $\forall i \in \mathbb{N}\ \varphi_n(10^i) = 1$ et ainsi :

$$\varphi_n(a) = \sum_{i=0}^{k} \varphi_n(a_i) = \varphi_n(\sum_{i=0}^{k} a_i).$$

Donc a est divisible par 3 (resp. 9) si la somme de ses chiffres est divisible par 3 (resp. par 9).

C'est à peine plus compliqué pour $n = 11$, il nous faut calculer $\varphi_{11}(10^i)$. On a $\varphi_{11}(10) = 10 = -1$, en effet $\overline{-1} = \overline{10}$ puisque 10 et -1 sont deux représentants de la même classe de congruence. On en déduit que $\varphi_{11}(10^i) = (-1)^i$ et donc que

$$\varphi_{11}(a) = \sum_{i=0}^{k} (-1)^i \varphi_{11}(a_i) = \varphi_{11}\left(\sum_{i=0}^{k} (-1)^i a_i\right).$$

Donc a est divisible par 11 si en additionnant tous les chiffres de rang pair et en soustrayant tous les chiffres de rang impair, le résultat est divisible par 11. Exemple : $a = 2\,409$, on a $2 - 4 + 0 - 9 = -11$, donc $11 \mid a$.

EXERCICE 26. Soit n un entier naturel.

(1) Montrez que si n est impair alors $n^2 \equiv 1 \pmod 4$ et $n^2 \equiv 1 \pmod 8$.

(2) Montrez que si n est pair alors $n^2 \equiv 0 \pmod 4$ et dans ce cas que $n^2 \equiv 0 \pmod 8$ ou $n^2 \equiv 4 \pmod 8$.

Solution. (1) Si n est impair, il existe un entier naturel k tel que $n = 2k+1$, on a donc

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 4(k^2 + k) + 1 \\ &= \underbrace{4.k(k+1)}_{h} + 1 \end{aligned}$$

Le reste de la division euclidienne par 4 est donc égal à 1, i.e. $n^2 \equiv 1 \pmod 4$, mais k ou $k+1$ est pair, ainsi h est un multiple de 8 et donc $n^2 \equiv 1 \pmod 8$.

(2) Si $n = 2k$, on a $n^2 = 4k^2$ ce qui prouve que n^2 est *toujours* un multiple de 4, i.e. $n^2 \equiv 0 \pmod 4$, mais on peut être plus précis. En effet, si k est pair, disons $k = 2l$ dans ce cas $k^2 = 4l^2$ et n est divisible par 16 et *a fortiori* par 8, sinon les restes modulo 8 des multiples de 4 sont 0 ou 4.

EXERCICE 27. Alice et Bob surveillent l'examen terminal de I23 qui se déroule de 9h00 à 12h00. Alice s'est couchée trop tard la veille et somnole 1 minute toutes les 28 minutes tandis que Bob regarde fixement sa montre pendant 1 minute tous les quarts d'heure car les surveillances d'examens l'ennuient. Les étudiants ont vu Alice bailler à 09h08 la première fois, alors que Bob a regardé sa montre dès 09h02.

(1) Si t désigne le temps écoulé en minutes depuis le début de l'épreuve, quelle congruence satisfait t pour correspondre aux moments d'inattention d'Alice ? Même question pour Bob ?

(2) Justifiez, sans faire de calculs, l'existence de solutions au système de congruences ci-dessus.

(3) à quelle(s) heure(s) les étudiants peuvent-ils espérer tricher à l'examen sans être remarqués par les deux surveillants ?

Solution. (1) On note A et B les deux entiers relatifs représentant les minutes écoulées depuis le début de l'épreuve à 9h 00). On a $A \equiv 8 \pmod{28}$ et $B \equiv 2 \pmod{15}$.

(2) On en déduit qu'il existe deux entiers relatifs k et l tels que $A = 28k+8$ et $B = 15l + 2$ et on veut résoudre l'équation diophantienne

$$28k + 8 = 15l + 2 \Leftrightarrow -28k + 15l = 6.$$

Comme $(28, 15) = 1$ et que $1 \mid 6$ alors l'identité de Bezout nous permet d'affirmer qu'il existe un couple (k, l) tel que $-28k + 15l = 6$.

(3) On calcule $(28, 15)$ avec l'algorithme d'Euclide et on réécrit les différentes égalités sous forme d'identités de Bézout à droite :

$$\begin{aligned} 28 &= 15.(1) + 13 & 28.(1) + 15.(-1) &= 13 \\ 15 &= 13.(1) + 2 & 15.(1) + 13(-1) &= \boxed{2} \\ 13 &= 2.(6) + 1 & 13.(1) + \boxed{2}.(-6) &= 1 \end{aligned}$$

L'algorithme d'Euclide étendu consiste à remonter le PGCD obtenu dans la dernière identité de proche en proche pour le faire apparaître en partie droite de la première identité. On multiplie l'avant dernière identité par -6 pour pouvoir remplacer $2.(-6)$ par $1 - 13.(1)$ ce qui donne le nouveau système :

$$\begin{aligned} 28.(1) + 15.(-1) &= 13 \\ 15.(-6) + 13(6) &= \boxed{2}.(-6) \\ \boxed{2}.(-6) &= 1 - 13.(1) \end{aligned}$$

Tout ceci devient :

$$\begin{aligned} 28.(1) + 15.(-1) &= \boxed{13} \\ 15.(-6) + \boxed{13}.(7) &= 1 \end{aligned}$$

On continue en multipliant cette fois la première identité par 7 :

$$\begin{aligned} 28.(7) + 15.(-7) &= \boxed{13}.(7) \\ \boxed{13}.(7) &= 1 - 15.(-6) \end{aligned}$$

Et on obtient finalement

$$\begin{aligned} -28.(-7) + 15.(13) &= 1 \\ -28.(-42) + 15.(-78) &= 6 \end{aligned}$$

On sait d'après ce théorème qu'il existe une infinité de solutions à l'équation diophantienne. Nous cherchons celles qui sont compatibles avec le problème, c'est-à-dire dont les valeurs sont positives et dans l'intervalle de temps de l'examen. Les couples solutions sont de la forme

$$(-42 - k.15, -78 - k.28)$$

Pour $k = -3$, on a le couple solution $(3, 6)$ et on en déduit $A = B = 92$ minutes, donc le premier moment d'inattention des deux enseignants est à 10h32. La solution compatible suivante pour $k = -4$ donne $A = 512$ mais dépasse la durée de l'examen.

EXERCICE 28. Calculez l'inverse de 7 modulo 2 018 s'il existe. Même question pour 451 modulo 1 236.

Solution. Comme $(2018, 7) = 1$, l'entier 7 admet un inverse modulo 2018 que l'on note u. Ceci se traduit par

$$\begin{aligned} 7u &\equiv 1 \pmod{2018} \\ 7u - 1 &\equiv 0 \pmod{2018} \end{aligned}$$

donc il existe $v \in \mathbb{Z}$ tel que $7u - 1 = 2\,018v$. On a donc à résoudre l'équation $7u + 2\,018(-v) = 1$ et l'algorithme d'Euclide étendu donne un couple solution (u, v) :

$$7 \times \underbrace{865}_{u} + 2\,018 \times \underbrace{(-3)}_{v} = 1.$$

Et dans $\mathbb{Z}/2018\mathbb{Z}$, cette égalité devient

$$7 \times 865 = 1.$$

Autrement dit, l'entier 865 est un représentant de l'inverse de 7 modulo 2018.

Avec un raisonnement similaire on obtient $451u - 1\,236v = 1$ et l'algorithme d'Euclide étendu donne après calculs, $451.(-581) + 1\,236.212 = 1$ donc -581 ou $-581 + 1\,236 = 655$ sont des représentants de l'inverse de 451 modulo 1 236.

EXERCICE 29. Calculez le reste de la division euclidienne de 2^{2021} par 17.

Solution. Le nombre 17 étant premier, on a $\varphi(17) = 16$. D'autre part $(17, 2) = 1$ et le petit théorème de Fermat nous donne $2^{16} \equiv 1 \pmod{17}$. Or $2021 = 16 \times 126 + 5$ donc

$$\begin{aligned} 2^{2021} &= 2^5.(2^{16})^{126} \\ &\equiv 32 \pmod{17} \end{aligned}$$

EXERCICE 30. † Démontrez les propositions suivantes :

(1) Il existe une infinité d'entiers naturels n tels que $5 \mid 2^n - 3$.

(2) Il existe une infinité d'entiers naturels n tels que $13 \mid 2^n - 3$.

(3) Démontrez qu'il n'existe aucun entier naturel n tel que $65 \mid 2^n - 3$.

Solution. **(1)** Notons q et r le quotient et le reste de la division de n par 4, i.e. $n = 4q + r$ avec $0 \leqslant r < 3$, ou de manière équivalente $n \equiv r \pmod 4$. On a

$$\begin{aligned} 2^n - 3 &= 2^{4q+r} - 3 \\ &= 2^r.(2^4)^q - 3 \end{aligned}$$

Donc $2^n - 3 \equiv 2^r - 3 \pmod 5$ car $2^4 \equiv 1 \pmod 5$ d'après le petit théorème de Fermat. On a :

$$\begin{aligned} 2^0 - 3 &\equiv 3 \pmod 5 & 2^2 - 3 &\equiv 1 \pmod 5 \\ 2^1 - 3 &\equiv 4 \pmod 5 & 2^3 - 3 &\equiv 0 \pmod 5 \end{aligned}$$

Finalement il y a une infinité d'entiers naturels n tels que $2^n - 3$ est divisible par 5. En effet $5 \mid 2^n - 3$ si et seulement si $n \equiv 3 \pmod 4$.

(2) Avec un raisonnement similaire et en reprenant les mêmes notations, on montre que $2^n - 3 \equiv 2^r - 3 \pmod{13}$ avec $0 \leqslant r < 12$ et

$$\begin{array}{llll} 2^0 - 3 \equiv 11 \pmod{13} & 2^4 - 3 \equiv 0 \pmod{13} & 2^8 - 3 \equiv 2 \pmod{13} \\ 2^1 - 3 \equiv 12 \pmod{13} & 2^5 - 3 \equiv 3 \pmod{13} & 2^9 - 3 \equiv 7 \pmod{13} \\ 2^2 - 3 \equiv 1 \pmod{13} & 2^6 - 3 \equiv 9 \pmod{13} & 2^{10} - 3 \equiv 4 \pmod{13} \\ 2^3 - 3 \equiv 5 \pmod{13} & 2^7 - 3 \equiv 6 \pmod{13} & 2^{11} - 3 \equiv 11 \pmod{13} \end{array}$$

Il y a donc une infinité d'entiers naturels n tels que $2^n - 3$ est divisible par 13. En effet $13 \mid 2^n - 3$ si et seulement si $n \equiv 4 \pmod{12}$.

(3) Comme $65 = 5 \times 13$, si $65 \mid 2^n - 3$, alors $5 \mid 2^n - 3$ et $13 \mid 2^n - 3$. D'après les résultats précédents, il faut donc que

$$\begin{aligned} n \equiv 3 \pmod 4 &\iff \exists k \in \mathbb{Z} \quad n = 4k + 3 \\ n \equiv 4 \pmod{12} &\iff \exists\, l \in \mathbb{Z} \quad n = 12l + 4 \end{aligned}$$

autrement dit, il faut que

$$\begin{aligned} 4k + 3 &= 12l + 4 \\ 4k - 12l &= 1 \end{aligned} \tag{9}$$

Or $(12, 4) = 4$ et $4 \nmid 1$, le théorème de Bézout nous permet d'affirmer qu'il n'existe pas de couple (k, l) satisfaisant l'équation (9).

EXERCICE 31. † Trois comètes passent à proximité de la Terre. La première passe tous les 5 ans et est passée l'an dernier, la deuxième passe tous les 8 ans et a été observée il y a deux ans, et la troisième passe tous les 11 ans et a été observée il y a trois ans. Quelle est la prochaine année où l'on pourra les observer toutes les trois ?

Solution. C'est en substance le même problème que celui du cuisinier chinois. En notant A l'année de cette conjonction, on déduit de l'énoncé les trois congruences suivantes :

$$\begin{aligned} A &\equiv -1 \pmod 5 \\ A &\equiv -2 \pmod 8 \\ A &\equiv -3 \pmod{11} \end{aligned}$$

Les trois entiers $n_1 := 5$, $n_2 := 8$ et $n_3 := 11$ sont premiers entre eux et d'après le premier corollaire du théorème des restes chinois le système de congruences ci-dessus admet une unique solution dans $\mathbb{Z}/n\mathbb{Z}$ où $n := 5.8.11 = 240$. L'algorithme qui permet de trouver cette solution s'appuie sur l'application de l'algorithme d'Euclide étendu sur trois équations diophantiennes. On calcule tout d'abord $\widetilde{n}_i = \frac{n}{n_i}$ pour $i \in \{1, 2, 3\}$:

$$\widetilde{n}_1 = 88, \quad \widetilde{n}_2 = 55, \quad \widetilde{n}_3 = 40.$$

Il faut à présent calculer les trois couples (u_i, v_i) qui satisfont les identités de Bézout suivantes :

$$\begin{aligned} 88.u_1 + 5.v_1 = 1 &\quad\Rightarrow\quad 88.u_1 \equiv 1 \pmod{440} \\ 55.u_2 + 8.v_2 = 1 &\quad\Rightarrow\quad 55.u_2 \equiv 1 \pmod{440} \\ 40.u_3 + 11.v_3 = 1 &\quad\Rightarrow\quad 40.u_3 \equiv 1 \pmod{440} \end{aligned}$$

et on obtient dans l'ordre les couples $(2, -35)$, $(-1, 7)$ et $(-3, 11)$. La solution A au système de congruences est donnée par

$$\begin{aligned} A &= 88.2.(-1) + 55.(-1).(-2) + 40.(-3).(-3) \\ &= 294. \end{aligned}$$

qui est bien le plus petit représentant positif de sa classe modulo 440. Il faudra donc attendre l'année 2317 pour observer ces trois comètes à nouveau.