48 exercices en 6 parties, du plus simple au plus difficile : ★☆☆ facile · ★★☆ moyen · ★★★ difficile. Le corrigé détaillé est sur **benprofparticulier.fr**.

1. *Congruence modulo n : définition et reste*

À retenir : $a \equiv b\ [n]$ (module $n \geqslant 2$) $\Leftrightarrow n \mid a-b \Leftrightarrow$ même reste par n. Un reste r vérifie $0 \leqslant r \leqslant n-1$: $-9 = 4 \times (-3) + 3$, donc le reste vaut 3, même si $-9 \equiv -1\ [4]$. Et $a \equiv b\ [n]$ ne dit pas que b est le reste.

Ex. 1 ★☆☆ **Restes, y compris d'entiers négatifs** — Pour chaque entier, écris la division euclidienne $a = nq + r$ avec $0 \leqslant r \leqslant n-1$, puis donne le reste.

(a) Quel est le reste de 158 dans la division par 9 ?

(b) Quel est le reste de -31 dans la division par 8 ?

(c) Quel est le reste de -59 dans la division par 9 ?

(d) Quel est le reste de 1 000 dans la division par 19 ?

(e) Quel est le reste de -7 dans la division par 15 ?

(f) Que renvoie l'instruction Python `-86 % 11` ? Justifie par une division euclidienne.

Ex. 2 ★☆☆ **Congruence vraie ou fausse ?** — Dis si chaque congruence est vraie ou fausse. Justifie en calculant $a - b$.

(a) $71 \equiv 8\ [9]$ est-elle vraie ou fausse ? Justifie.

(b) $101 \equiv 1\ [10]$ est-elle vraie ou fausse ? Justifie.

(c) $62 \equiv 7\ [6]$ est-elle vraie ou fausse ? Justifie.

(d) $-19 \equiv 9\ [7]$ est-elle vraie ou fausse ? Justifie.

(e) $-40 \equiv -4\ [12]$ est-elle vraie ou fausse ? Justifie.

(f) $-11 \equiv 11\ [4]$ est-elle vraie ou fausse ? Justifie.

Ex. 3 ★★☆ **Les erreurs de Maëlle** — Maëlle a écrit cinq phrases sur sa copie. Chacune contient une erreur.

(a) « $77 \equiv 22\ [5]$, donc le reste de 77 par 5 vaut 22. » Où est l'erreur ? Corrige-la.

(b) « $-38 = 6 \times (-6) - 2$, donc le reste de -38 par 6 vaut -2. » Où est l'erreur ? Corrige-la.

(c) « $125 \equiv 5\ [8]$ est fausse, car $125 \neq 5 + 8$. » Où est l'erreur ? Corrige-la.

(d) « Tout entier a vérifie $a \equiv 0\ [1]$, donc je travaille modulo 1 pour simplifier. » Où est l'erreur ?

(e) « $x \equiv 3\ [4]$, donc $x = 3$. » Où est l'erreur ? Donne deux autres valeurs possibles de x.

Ex. 4 ★★☆ **Vrai ou faux pour tout entier** — a désigne un entier relatif et n un entier naturel. Dis si chaque affirmation est vraie ou fausse. Justifie par une démonstration ou un contre-exemple.

(a) Si $a \equiv 7\ [10]$, alors $a \equiv 2\ [5]$. Vrai ou faux ? Justifie.

(b) Si $a \equiv 2\ [5]$, alors $a \equiv 7\ [10]$. Vrai ou faux ? Justifie.

(c) a est impair si et seulement si $a \equiv -1\ [2]$. Vrai ou faux ? Justifie.

(d) Pour tout entier naturel n, $5n + 15 \equiv n + 3\ [4]$. Vrai ou faux ? Justifie.

Ex. 5 ★★☆ **Les vendredis de Yanis** — En 2027, Yanis numérote les jours de l'année de 1 (le 1er janvier) à 365 (le 31 décembre). Le 1er janvier 2027 est un vendredi.

(a) Justifie que le jour numéro j est un vendredi si et seulement si $j \equiv 1\ [7]$.

(b) Le 14 juillet 2027 porte le numéro 195. Détermine le jour de la semaine de cette date.

(c) Détermine tous les numéros j tels que $200 \leqslant j \leqslant 230$ qui sont des vendredis.

(d) Combien l'année 2027 compte-t-elle de vendredis ? Justifie.

Ex. 6 ★★★ **Tous les entiers congrus à 13 modulo 17** — Dans cet exercice, x désigne un entier relatif.

(a) Léo traduit $x \equiv 13\ [17]$ par « $x = 13 + 17$ ». Donne un entier congru à 13 modulo 17 qui contredit sa traduction, puis écris la bonne traduction.

(b) Détermine tous les entiers x de l'intervalle $[-60; 60]$ tels que $x \equiv 13\ [17]$.

(c) Combien d'entiers x de l'intervalle $[-1\,000; 1\,000]$ vérifient $x \equiv 13\ [17]$? Justifie.

(d) Traduis « x est impair » par une congruence. Démontre ensuite que : ($x \equiv 13\ [17]$ et x impair) $\iff$ $x \equiv 13\ [34]$.

(e) Déduis-en le nombre d'entiers impairs de l'intervalle $[-1\,000; 1\,000]$ qui sont congrus à 13 modulo 17.

Ex. 7 ★★★ **Opposés et restes** — Dans cet exercice, n désigne un entier naturel tel que $n \geqslant 2$, et a un entier relatif.

(a) On note r le reste de a dans la division par n et on suppose $1 \leqslant r \leqslant n-1$. Démontre que le reste de $-a$ vaut $n - r$. Que vaut ce reste si $r = 0$?

(b) Lila écrit : « le reste de $-2\,027$ par 13 est -12 ». Dis ce qui est juste et ce qui est faux dans sa phrase, puis donne le bon reste.

(c) Détermine tous les entiers $n \geqslant 2$ tels que $21 \equiv -21\ [n]$.

Ex. 7 **(suite)**

(d) On suppose n impair. Démontre que si $a \equiv -a\ [n]$, alors $a \equiv 0\ [n]$. Est-ce encore vrai si n est pair ? Justifie.

Ex. 8 ★★★ **Le pion de Sacha** — Un plateau circulaire a 12 cases numérotées de 0 à 11 ; les cases 0, 3, 6 et 9 sont rouges. Le pion de Sacha part de la case 0. Il avance ou recule selon ses déplacements, de somme s, et arrive sur la case r, reste de s dans la division par 12.

(a) Sur quelle case est le pion si $s = 125$? Et si $s = -50$?

(b) Sacha programme la fonction ci-dessous. Que renvoient `case(125)` et `case(-50)` ? Explique son erreur.

```
def case(s):
    if s >= 12:
        s = s - 12
    if s < 0:
        s = s + 12
    return s
```

(c) Corrige la fonction de Sacha sans utiliser l'opérateur `%`.

(d) Démontre que le pion est sur une case rouge si et seulement si $s \equiv 0\ [3]$.

(e) Après une partie, la somme s des déplacements de Sacha est impaire. Son pion peut-il être sur la case 4 ? Justifie.

2. *Compatibilité avec l'addition et la multiplication*

À retenir : Si $a \equiv b \pmod n$ et $c \equiv d \pmod n$, alors $a + c \equiv b + d$, $ac \equiv bd$ et $a^m \equiv b^m \pmod n$. On réduit la base, jamais l'exposant. On ne divise pas : $2 \times 3 \equiv 2 \times 0 \pmod 6$, mais $3 \not\equiv 0 \pmod 6$.

Ex. 9 ★☆☆ **Des représentants commodes** — Détermine le reste de la division euclidienne de chaque nombre par le module indiqué. Remplace d'abord chaque nombre par un représentant commode, négatif si c'est utile.

(a) 199×98 modulo 10.

(b) 49^3 modulo 50.

(c) 59×61 modulo 60.

(d) $(-17) \times 23$ modulo 6.

(e) 13^4 modulo 15.

(f) $2025^2 - 2023^2$ modulo 4.

Ex. 10 ★☆☆ **Le reste d'une expression en a** — L'entier a vérifie $a \equiv 5 \pmod{11}$. Détermine le reste de la division par 11 de chaque nombre.

(a) $3a + 7$.

(b) a^2.

(c) $a^2 - 2a + 6$.

(d) a^3.

(e) $2a^3 + a$.

(f) $a^4 + 10$.

Ex. 11 ★★☆ **Un produit nul sans facteur nul** — On étudie le reste de $6x$ modulo 8 pour x entier de 0 à 7.

x	0	1	2	3
$6x \equiv \dots \pmod 8$	0	…	…	…

x	4	5	6	7
$6x \equiv \dots \pmod 8$	…	…	…	…

(a) Complète le tableau. Détaille le calcul pour $x = 5$.

(b) Trouve dans le tableau un entier x de 1 à 7 tel que $6x \equiv 0 \pmod 8$. Déduis-en un produit de deux entiers non divisibles par 8 qui est divisible par 8.

(c) Détermine les entiers x de 0 à 7 tels que $6x \equiv 2 \pmod 8$, puis tous les entiers relatifs x qui vérifient cette congruence.

(d) L'équation $6x \equiv 5 \pmod 8$ a-t-elle des solutions dans $\mathbb{Z}$? Justifie.

Ex. 12 ★★☆ **Deux copies à corriger** — Inès écrit : « $11 \equiv 1 \pmod 5$, donc $2^{11} \equiv 2^1 = 2 \pmod 5$. » Malo écrit : « $4x \equiv 28 \pmod{10}$, donc $x \equiv 7 \pmod{10}$. »

(a) Calcule le reste de 2^{11} modulo 5 en partant de 2^2. Inès a-t-elle raison ? Justifie.

(b) Explique l'erreur d'Inès.

(c) Trouve un entier x de 0 à 9, différent de 7, tel que $4x \equiv 28 \pmod{10}$. Malo a-t-il raison ? Justifie.

(d) Détermine tous les entiers relatifs x tels que $4x \equiv 28 \pmod{10}$.

Ex. 13 ★★☆ **Une divisibilité pour tout n** — Dans cet exercice, n désigne un entier naturel.

(a) Démontre que, pour tout entier naturel n, $9^n \equiv 2^n \pmod 7$.

(b) Déduis-en que, pour tout entier naturel n, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

(c) Vrai ou faux : « Pour tout entier naturel n, $3^{2n+1} + 2^{n+2}$ est divisible par 14. » Justifie.

Ex. 14 ★★★ **Les deux derniers chiffres** — Les deux derniers chiffres d'un entier naturel sont donnés par son reste modulo 100. Par exemple, $3\,517 \equiv 17 \pmod{100}$.

(a) Détermine le reste de 99^{2027} modulo 100. Utilise un représentant négatif de 99.

(b) Calcule 49^2 modulo 100. Déduis-en le reste de 49^{2027} modulo 100.

(c) Déduis-en les deux derniers chiffres de $N = 99^{2027} + 49^{2027} + 52$.

(d) Démontre que, pour tout entier naturel n, $99^{2n} + 49^{2n} - 2$ est divisible par 100.

(e) Détermine les deux derniers chiffres de $99^n \times 49^n$ selon la parité de l'entier naturel n.

Ex. 15 ★★★ **Un vendredi et des puissances de 3** — Le 1er janvier 2027 est un vendredi. Une année compte 365 jours, ou 366 si elle est bissextile. Parmi 2027, 2028, 2029 et 2030, seule 2028 est bissextile. Les jours de la semaine reviennent tous les 7 jours.

(a) Détermine les restes de 365 et de 366 modulo 7. Déduis-en le jour de la semaine du 1er janvier 2031.

(b) Quel jour de la semaine sera-t-on 1 000 jours après le vendredi 1er janvier 2027 ?

(c) Calcule 3^3 modulo 7 avec un représentant négatif. Déduis-en le reste de 3^{100} modulo 7, puis le jour 3^{100} jours après le 1er janvier 2027.

(d) Yanis écrit : « $100 \equiv 2 \pmod 7$, donc $3^{100} \equiv 3^2 \equiv 2 \pmod 7$. » A-t-il raison ? Justifie.

(e) Pour tout entier naturel n, détermine le jour de la semaine 10^{6n} jours après un vendredi.

Ex. 16 ★★★ **Quand 12 divise-t-il un produit ?** — Pour tout entier naturel n, on pose $A_n = n^2 + 5n + 6$. Dans cet exercice, on travaille modulo 12.

(a) Vérifie que $A_n = (n+2)(n+3)$. Pour $n \equiv 7 \pmod{12}$, calcule le reste de A_n modulo 12 en remplaçant 7 par un représentant négatif.

(b) Démontre que, pour tout entier naturel n, A_n est pair. Raisonne selon le reste de n modulo 2.

(c) Explique pourquoi il suffit de tester les restes r de 0 à 11, puis détermine à la main ce qu'affiche ce programme.

```
def restes():
    L = []
    for r in range(12):
        if (r**2 + 5*r + 6) % 12 == 0:
            L.append(r)
    return L

print(restes())
```

(d) Gabin affirme : « Si $A_n \equiv 0 \pmod{12}$ et $n+3 \not\equiv 0 \pmod{12}$, alors $n+2 \equiv 0 \pmod{12}$. » Vrai ou faux ? Justifie.

(e) Déduis du programme tous les entiers naturels n tels que 12 divise A_n. Donne ceux compris entre 20 et 35.

3. *Restes des puissances : cycles*

À retenir : Je réduis la base (jamais l'exposant), je cherche la première puissance $a^k \equiv 1$ (ou -1), puis je divise l'exposant par k : $3^3 \equiv 1$ [13] donne $3^{91} \equiv 3$ [13]. Si 1 n'apparaît jamais, je pars de la première répétition.

Ex. 17 ★☆☆ **Restes de grandes puissances** — Sans calculer la puissance, réponds à chaque question en cherchant un cycle de restes.

(a) Détermine le reste de 4^{2018} dans la division par 7.

(b) Détermine le reste de 5^{1000} dans la division par 13.

Ex. 17 (suite)

(c) Détermine le reste de 17^{43} dans la division par 5.

(d) Détermine le reste de 4^{131} dans la division par 5.

(e) Détermine le reste de 10^{2025} dans la division par 11.

Ex. 18 ★☆☆ **Derniers chiffres** — Le chiffre des unités d'un entier naturel est son reste modulo 10 ; ses deux derniers chiffres forment son reste modulo 100.

(a) Détermine le chiffre des unités de 7^{1001}.

(b) Détermine le chiffre des unités de 13^{2028}.

(c) Détermine le chiffre des unités de 9^{2027}.

(d) Détermine les deux derniers chiffres de 7^{82}.

(e) Détermine les deux derniers chiffres de 51^{37}.

Ex. 19 ★★☆ **Trois copies à corriger** — Ben corrige trois copies. Pour chacune, explique l'erreur puis donne le bon résultat en le justifiant.

(a) Léa : « $3^4 = 81 \equiv 1 \pmod{16}$ et $2\,032 = 4 \times 508 + 0$: le reste est nul, donc $3^{2032} \equiv 0 \pmod{16}$. »

(b) Hugo : « $23 \equiv 2 \pmod 7$, donc $5^{23} \equiv 5^2 = 25 \equiv 4 \pmod 7$. »

(c) Nour : « D'après le petit théorème de Fermat, $2^{14} \equiv 1 \pmod{15}$; or $2\,030 = 14 \times 145$, donc $2^{2030} \equiv 1 \pmod{15}$. »

Ex. 20 ★★☆ **Une divisibilité pour tout entier** — Dans cet exercice, n désigne un entier naturel.

(a) Démontre que, pour tout entier naturel n, $3^{2n} - 2^n$ est divisible par 7.

(b) Complète

m	1	2	3
$2^m \equiv \ldots \pmod 7$	…	…	…

puis déduis-en le reste de 2^n modulo 7 selon le reste de n modulo 3.

(c) Déduis-en le reste de 3^{2026} dans la division par 7.

(d) Détermine les entiers naturels n tels que $3^{2n} + 2^n + 3$ soit divisible par 7.

Ex. 21 ★★☆ **Une fonction qui cherche le cycle** — Ben a écrit cette fonction, où `a` et `n` sont des entiers naturels avec $n \geqslant 2$.

```
def cycle(a, n):
    r = a % n
    m = 1
    while r != 1:
        r = (r * a) % n
        m = m + 1
    return m
```

(a) Que renvoie `cycle(3, 11)` ? Justifie en calculant les restes successifs.

(b) Déduis-en le reste de 3^{2033} dans la division par 11.

Ex. 21 **(suite)**

(c) Sans faire tourner la boucle, prévois ce que renvoient `cycle(12, 11)` et `cycle(14, 11)`. Justifie.

Ex. 22 ★★★ **Puissances de 2 : un cycle qui démarre en retard** — Dans cet exercice, on étudie les restes des puissances de 2 dans la division par 40.

m	1	2	3	4
$2^m \pmod{40}$	…	…	…	…

m	5	6	7	8
$2^m \pmod{40}$	…	…	…	…

(a) Complète les deux tableaux. Justifie ensuite qu'aucune puissance 2^m avec $m \geqslant 1$ n'est congrue à 1 modulo 40.

(b) Démontre que, pour tout entier naturel $m \geqslant 3$, $2^{m+4} \equiv 2^m \pmod{40}$.

(c) Déduis-en le reste de 2^{2026} dans la division par 40.

(d) Élodie écrit : « $2024 = 4 \times 506 + 0$, donc $2^{2024} \equiv 2^0 = 1 \pmod{40}$ ». Explique son erreur, puis donne le bon reste.

(e) Déduis de la question 3 le chiffre des unités de 2^{2026}.

Ex. 23 ★★★ **Modulo 11 : le signe moins et le théorème de Fermat** — On admet le petit théorème de Fermat : si p est un nombre premier qui ne divise pas l'entier a, alors $a^{p-1} \equiv 1 \pmod{p}$.

(a) Détermine le reste de $32^{2027} + 54^{2026}$ dans la division par 11.

(b) Max écrit : « 11 est premier, donc, d'après le petit théorème de Fermat, $33^{10} \equiv 1 \pmod{11}$ ». Explique son erreur, puis donne le bon reste.

(c) Détermine le reste de 13^{2040} dans la division par 11. Vérifie les hypothèses du théorème utilisé.

(d) Détermine tous les entiers naturels n tels que 11 divise $2^n + 1$.

Ex. 24 ★★★ **Un programme, un calendrier et une boucle sans fin** — Inès a écrit cette fonction, où `a` et `n` sont des entiers naturels avec $n \geqslant 2$.

```
def restes(a, n):
    liste = []
    r = a % n
    while r != 1:
        liste.append(r)
        r = (r * a) % n
    liste.append(r)
    return liste
```

(a) Que renvoie `restes(5, 7)` ? Justifie en calculant les restes successifs.

(b) Nous sommes un mercredi. Quel jour de la semaine sera-t-il dans 5^{2027} jours ? Justifie.

(c) Explique pourquoi l'appel `restes(4, 10)` ne s'arrête jamais.

Ex. 24 **(suite)**

(d) Inès remplace `while r != 1:` par `while r not in liste:` et supprime l'avant-dernière ligne. Que renvoie alors `restes(4, 10)` ? Justifie.

(e) Déduis-en le chiffre des unités de 4^{2027}.

4. *Critères de divisibilité et tableaux de congruences*

À retenir : $10 \equiv 1$ [9] : somme des chiffres. $10 \equiv -1$ [11] : somme alternée avec $+$ aux unités ($253 \equiv 3 - 5 + 2 = 0$ [11]). $100 \equiv 0$ [4] : deux derniers chiffres. Tableau : tous les restes de 0 à $n - 1$, puis conclure sur la ligne.

Ex. 25 ★☆☆ **Restes sans poser la division** — Réponds à chaque question avec un critère de divisibilité, sans poser la division.

(a) Donne le reste de 581 276 dans la division par 9.

(b) Donne le reste de 47 160 395 dans la division par 11.

(c) Détermine le plus grand multiple de 4 inférieur ou égal à 93 718.

(d) Détermine le plus petit entier naturel à ajouter à 40 863 pour obtenir un multiple de 25.

(e) Sachant que $1\,000 \equiv 0$ [8], justifie que $6\,024\,517 \equiv 517$ [8]. Déduis-en le reste de 6 024 517 dans la division par 8.

(f) Trouve le chiffre a pour que le nombre $\overline{5a732}$ soit divisible par 9.

(g) Trouve le chiffre b pour que le nombre $\overline{3b814}$ soit divisible par 11.

Ex. 26 ★☆☆ **Vrai ou faux sur les congruences** — Pour chaque affirmation, réponds par vrai ou faux et justifie.

(a) $10^5 \equiv 1$ [9].

(b) $10^5 \equiv 1$ [11].

(c) $5\,934 \equiv 4$ [4], car seul le chiffre des unités compte.

(d) Si $n \equiv 3$ [7], alors $n^2 \equiv 2$ [7].

(e) $-17 \equiv 3$ [7].

(f) Pour tout entier n, $n^2 - n$ est pair.

Ex. 27 ★★☆ **Démontrer les critères de 9, de 11 et de 4** — Soit N un entier naturel dont l'écriture décimale est $a_k \ldots a_1 a_0$, avec $k \geqslant 2$: $N = a_k \times 10^k + \cdots + a_1 \times 10 + a_0$, où chaque a_i est un chiffre entre 0 et 9.

(a) Justifie que $10 \equiv 1$ [9]. Démontre ensuite que $N \equiv a_k + \cdots + a_1 + a_0$ [9].

(b) Justifie que $10 \equiv -1$ [11]. Déduis-en que $N \equiv a_0 - a_1 + a_2 - \cdots + (-1)^k a_k$ [11].

(c) Justifie que $100 \equiv 0$ [4]. Démontre ensuite que $N \equiv 10a_1 + a_0$ [4].

Ex. 27 (suite)

(d) Pour trouver le reste de 5 293 modulo 11, Lina part de la gauche : $5 - 2 + 9 - 3 = 9$. A-t-elle raison ? Justifie.

Ex. 28 ★★☆ **Tableaux de congruences à exploiter** — Soit n un entier. Voici un tableau à compléter :

$n \equiv \ldots\,[3]$	**0**	**1**	**2**
$n(n+1)(n+2) \equiv \ldots\,[3]$	…	…	…

(a) Complète le tableau ci-dessus. Déduis-en que $n(n+1)(n+2)$ est divisible par 3 pour tout entier n.

(b) Démontre que $n(n+1)(n+2)$ est même divisible par 6 pour tout entier n.

(c) Dresse le tableau modulo 4 avec une ligne pour $2n^2$, une pour $3n$ et une pour $2n^2 + 3n + 1$. Déduis-en les entiers n tels que $4 \mid 2n^2 + 3n + 1$.

(d) Sami affirme : « Le carré d'un entier impair est toujours congru à 1 modulo 8. » Vrai ou faux ? Justifie avec le tableau des restes de n^2 modulo 8.

Ex. 29 ★★☆ **Choisir le bon modulo** — Les inconnues x et y sont des entiers relatifs.

(a) Dresse le tableau des restes de x^2 modulo 4.

(b) Démontre que l'équation $x^2 + 4y^2 = 2\,027$ n'a pas de solution entière.

(c) Malik étudie $x^2 = 3y + 2$ modulo 4 et ne peut pas conclure. Explique pourquoi, puis conclus avec un autre modulo.

(d) À l'aide des représentants $-3, \ldots, 3$, démontre que l'équation $x^3 = 7y + 3$ n'a pas de solution entière.

Ex. 30 ★★★ **Un critère de divisibilité par 7** — Soit N un entier naturel. On note a le quotient de N par 10 et b son chiffre des unités, donc $N = 10a + b$. On considère la fonction Python suivante.

```
def reduit(N):
    while N >= 100:
        a = N // 10
        b = N % 10
        N = a - 2 * b
    return N
```

(a) Justifie que $-20 \equiv 1\,[7]$. Déduis-en que $a - 2b \equiv -2N\,[7]$ pour tous entiers a et b.

(b) Démontre que $7 \mid N$ si et seulement si $7 \mid a - 2b$.

(c) Donne les valeurs successives prises par `N` lors de l'appel `reduit(59836)`, puis ce que la fonction renvoie. Conclus pour 59 836.

(d) Inès affirme : « N et $a - 2b$ ont toujours le même reste modulo 7. » Vrai ou faux ? Justifie.

(e) Démontre que $N \equiv 3(a - 2b)\,[7]$. Déduis-en le reste de 4 852 dans la division par 7, sans poser cette division.

Ex. 31 ★★★ **Les diviseurs de $n^2 + n + 1$** — D'après un sujet de bac. Pour tout entier naturel n, on pose $A = n^2 + n + 1$.

$n \equiv \ldots\,[5]$	**0**	**1**	**2**
$A \equiv \ldots\,[5]$	…	…	…

$n \equiv \ldots\,[5]$	**3**	**4**
$A \equiv \ldots\,[5]$	…	…

(a) Complète les deux tableaux de congruences ci-dessus. Déduis-en si A peut être un multiple de 5.

(b) Dresse le tableau des restes de A modulo 3. Déduis-en une condition nécessaire et suffisante sur n pour que $3 \mid A$.

(c) Détermine les restes de n modulo 7 pour lesquels $7 \mid A$.

(d) Déduis-en tous les entiers naturels $n < 21$ tels que A est divisible par 21.

(e) Démontre que A n'est divisible par 9 pour aucun entier naturel n.

Ex. 32 ★★★ **Les chiffres manquants d'un numéro de lot** — Dans un entrepôt de Nantes, chaque lot porte un numéro à cinq chiffres $N = \overline{4a52b}$, où a et b sont deux chiffres effacés. On cherche a et b à l'aide de critères de divisibilité.

(a) Démontre que tout entier naturel a le même reste modulo 25 que le nombre formé par ses deux derniers chiffres.

(b) Hugo calcule toujours la somme alternée en partant de la gauche. Démontre que, pour un nombre à cinq chiffres comme N, il obtient le même résultat qu'en partant des unités.

(c) Détermine tous les couples de chiffres $(a\,;b)$ tels que N soit divisible par 4 et par 11.

(d) Parmi ces numéros, lequel est divisible par 396 ? Justifie.

(e) Détermine les chiffres a et b pour que N soit divisible par 275.

5. *Résoudre $ax \equiv b\,[n]$, inverse modulo n, systèmes*

À retenir : Si $\text{pgcd}(a\,;n) = 1$, on multiplie par l'inverse u ($au \equiv 1\,[n]$) : $4x \equiv 3\,[7] \iff x \equiv 2 \times 3 = 6\,[7]$, soit $x = 6 + 7k$. Si $\text{pgcd}(a\,;n)$ ne divise pas b : aucune solution.

Ex. 33 ★☆☆ **Trouver un inverse par essais** — Dans chaque cas, dis si a admet un inverse modulo n. Si oui, donne cet inverse entre 0 et $n - 1$.

(a) $a = 3$ et $n = 11$.

(b) $a = 5$ et $n = 12$.

(c) $a = 9$ et $n = 13$.

Ex. 33 **(suite)**

(d) $a = 6$ et $n = 15$.

(e) $a = 10$ et $n = 17$.

(f) Inès affirme que l'inverse de 4 modulo 9 est 5, puisque $5 \equiv -4\ [9]$. A-t-elle raison ? Justifie, puis donne l'inverse de 4 modulo 9.

Ex. 34 ★☆☆ **Résoudre en multipliant par l'inverse** — Résous chaque équation, d'inconnue $x \in \mathbb{Z}$. Donne toutes les solutions sous la forme $x = r + nk$, $k \in \mathbb{Z}$, puis vérifie.

(a) $3x \equiv 5\ [7]$.

(b) $5x \equiv -7\ [9]$.

(c) $7x \equiv 5\ [12]$.

(d) $26x \equiv 6\ [11]$.

(e) $9x + 4 \equiv 9\ [16]$.

(f) Pour résoudre $2x \equiv 7\ [15]$, Noé écrit « $x \equiv \frac{7}{2}$ ». Explique son erreur, puis résous l'équation.

Ex. 35 ★★☆ **Un inverse par l'algorithme d'Euclide** — On veut résoudre l'équation $23x \equiv 7\ [60]$, d'inconnue $x \in \mathbb{Z}$.

(a) Justifie que 23 admet un inverse modulo 60.

(b) À l'aide de l'algorithme d'Euclide, trouve des entiers u et v tels que $23u + 60v = 1$. Déduis-en l'inverse de 23 modulo 60, entre 0 et 59.

(c) Résous l'équation $23x \equiv 7\ [60]$ et vérifie ta réponse.

(d) Sans refaire l'algorithme d'Euclide, déduis-en l'inverse de 37 modulo 60. Vérifie-le.

Ex. 36 ★★☆ **Quand pgcd(a ; n) n'est pas égal à 1** — On étudie les équations $12x \equiv b\ [20]$, d'inconnue $x \in \mathbb{Z}$, pour différentes valeurs de l'entier b.

(a) Démontre que l'équation $12x \equiv 9\ [20]$ n'a aucune solution.

(b) Démontre que $12x \equiv 8\ [20]$ équivaut à $3x \equiv 2\ [5]$.

(c) Résous $3x \equiv 2\ [5]$. Déduis-en les solutions de $12x \equiv 8\ [20]$ comprises entre 0 et 19.

(d) Détermine les entiers b compris entre 0 et 19 pour lesquels l'équation $12x \equiv b\ [20]$ a des solutions.

Ex. 37 ★★☆ **Les cartes de Sacha** — Sacha range sa collection de cartes. Par paquets de 7, il en reste 3. Par paquets de 9, il en reste 5. Elle possède entre 100 et 200 cartes. On note x ce nombre.

(a) Traduis la situation par deux congruences vérifiées par x.

(b) Justifie qu'il existe un entier k tel que $x = 3 + 7k$. Démontre alors que $7k \equiv 2\ [9]$.

(c) Résous $7k \equiv 2\ [9]$. Déduis-en toutes les solutions du système, sous la forme d'une classe modulo 63, et vérifie.

Ex. 37 **(suite)**

(d) Donne les nombres de cartes possibles. Sachant que ce nombre est impair, conclus.

Ex. 38 ★★★ **Un système aux modules non premiers entre eux** — On étudie le système $(S) : x \equiv 4\ \pmod 9$ et $x \equiv 7\ \pmod{12}$, d'inconnue $x \in \mathbb{Z}$. Les modules 9 et 12 ne sont pas premiers entre eux.

(a) Démontre que x est solution de (S) si et seulement si $x = 4 + 9k$, où l'entier k vérifie une congruence modulo 12 que tu préciseras.

(b) Calcule pgcd(9 ; 12). Déduis-en que la congruence vérifiée par k équivaut à une congruence modulo 4, puis résous-la.

(c) Déduis-en toutes les solutions de (S), sous la forme d'une classe modulo un entier à préciser, et vérifie.

(d) Yanis affirme que les solutions de (S) se répètent tous les $9 \times 12 = 108$ entiers. A-t-il raison ? Justifie.

(e) Démontre que le système $x \equiv 4\ \pmod 9$ et $x \equiv 6\ \pmod{12}$ n'a aucune solution.

Ex. 39 ★★★ **Les deux jets d'eau du parc** — Dans un parc de Lyon, le jet A se déclenche aux minutes 5, 13, 21, … (toutes les 8 minutes), et le jet B aux minutes 7, 22, … (toutes les 15 minutes). Les minutes sont comptées depuis l'ouverture, à 10 h. Les deux jets partent ensemble à la minute x lorsque $x \equiv 5\ \pmod 8$ et $x \equiv 7\ \pmod{15}$.

(a) Démontre que x vérifie les deux congruences si et seulement si $x = 5 + 8k$, où l'entier k vérifie une congruence modulo 15 que tu préciseras.

(b) Justifie que 8 admet un inverse modulo 15, puis trouve-le par essais. Résous ensuite la congruence vérifiée par k.

(c) Déduis-en que les solutions forment une seule classe, modulo un entier à préciser. Vérifie la plus petite solution positive.

(d) Léa affirme que les deux jets repartent ensemble toutes les $8 + 15 = 23$ minutes. A-t-elle raison ? Justifie.

(e) Le parc ferme à 22 h. Combien de fois les deux jets partent-ils ensemble dans la journée ? Donne les horaires.

Ex. 40 ★★★ **Chercher un inverse : essais ou Euclide ?** — Ben propose cette fonction Python, où a et n sont des entiers avec $n \geqslant 2$:

```
def inverse(a, n):
    for u in range(n):
        if (a * u) % n == 1:
            return u
    return -1
```

(a) Que renvoie `inverse(5, 18)` ? Justifie par un calcul.

(b) Que renvoie `inverse(12, 18)` ? Explique ce résultat à l'aide du critère d'existence d'un inverse.

(c) Écris une boucle qui affiche les entiers a de 1 à 17 ayant un inverse modulo 18. Combien y en a-t-il ?

Ex. 40 **(suite)**

(d) Hugo résout $5x \equiv 7 \pmod{18}$ à l'aide de la première question et conclut : « la solution est $x = 77$ ». Que manque-t-il à sa réponse ? Corrige-la et vérifie.

(e) Modulo 1000, la fonction peut faire 1000 essais. Détermine plutôt l'inverse de 43 modulo 1000 par l'algorithme d'Euclide, puis vérifie-le.

6. *Chiffrements et clés de contrôle*

À retenir : Chiffrement $y \equiv ax + b\ [26]$ avec A $= 0$: il est déchiffrable si $\text{pgcd}(a\,;26) = 1$. On déchiffre par $x \equiv a'(y - b)\ [26]$ où $aa' \equiv 1\ [26]$, jamais en divisant ($3 \times 9 = 27$ donne $a' = 9$). Une clé somme repère une erreur, pas une permutation.

Ex. 41 ★☆☆ **Chiffrer avec une clé affine** — On numérote les lettres A $= 0$, B $= 1$, …, Z $= 25$. La lettre de rang x est remplacée par la lettre de rang y, où $y \equiv 15x + 8 \pmod{26}$ et $0 \leqslant y \leqslant 25$.

(a) Chiffre la lettre E.

(b) Chiffre la lettre K.

(c) Justifie que $25 \equiv -1 \pmod{26}$, puis déduis-en le chiffré de Z sans calculer 15×25.

(d) Chiffre le mot AMI.

(e) Nora numérote A $= 1$, B $= 2$, … et prend $x = 2$ pour chiffrer B. Quelle lettre obtient-elle ? Explique son erreur et donne le bon chiffré de B.

Ex. 42 ★☆☆ **Calculer une clé de Luhn** — Algorithme de Luhn : en partant de la droite, on double un chiffre sur deux, en commençant par le deuxième. Si un double dépasse 9, on lui retire 9. On additionne tous les chiffres obtenus : le numéro est valide si cette somme est congrue à 0 modulo 10.

(a) Calcule la somme de Luhn du numéro 4 7 3 9, puis déduis-en s'il est valide.

(b) Calcule la somme de Luhn du numéro 5 8 2 1 6, puis déduis-en s'il est valide.

(c) Détermine le chiffre c pour que le numéro 6 5 7 8 c soit valide.

(d) Détermine le chiffre c pour que le numéro 3 5 2 9 4 1 7 c soit valide.

(e) Pour le numéro 7 2 4 6 c, Théo double les chiffres en partant de la gauche et trouve $c = 9$. A-t-il raison ? Justifie en calculant c.

Ex. 43 ★★☆ **Déchiffrer un message affine** — On numérote les lettres A $= 0$, …, Z $= 25$. Un message est chiffré par $y \equiv 21x + 11 \pmod{26}$, avec $0 \leqslant y \leqslant 25$.

(a) Justifie que 21 a un inverse modulo 26. Trouve-le en cherchant un multiple de 21 parmi 27, 53, 79, …

Ex. 43 **(suite)**

(b) Déduis-en des entiers c et d compris entre 0 et 25 tels que $y \equiv 21x + 11 \pmod{26} \iff x \equiv cy + d \pmod{26}$.

(c) Déchiffre le mot YPXU.

(d) Sacha déchiffre la lettre Y en calculant $\frac{24-11}{21}$. Explique pourquoi sa méthode ne fonctionne pas.

(e) Mila propose la clé $y \equiv 8x + 11 \pmod{26}$. Chiffre A et N avec cette clé, puis déduis-en qu'on ne peut pas déchiffrer avec cette clé.

Ex. 44 ★★☆ **Une clé qui ignore les permutations** — Une consigne de gare donne à chaque casier un code de quatre chiffres a, b, c, d, suivi d'une clé k : k est le reste de $a + b + c + d$ dans la division par 10.

(a) Calcule la clé du code 3 8 5 6.

(b) Démontre que si un seul chiffre du code est mal saisi, la clé change.

(c) Calcule la clé du code 8 3 5 6. Explique pourquoi cette clé ne détecte aucune permutation des chiffres.

(d) On prend maintenant pour clé le reste de $a + 2b + 3c + 4d$ dans la division par 11 (il peut valoir 10). Calcule la clé de 3 8 5 6, puis celle de 3 5 8 6.

(e) Avec cette nouvelle clé, démontre que l'échange de deux chiffres distincts du code, voisins ou non, change toujours la clé.

Ex. 45 ★★☆ **Un programme de chiffrement à corriger** — Avec A $= 0$, …, Z $= 25$, la fonction suivante chiffre un mot écrit en majuscules par $y \equiv ax + b\ [26]$.

```
def chiffre(mot, a, b):
    alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    resultat = ""
    for lettre in mot:
        x = alphabet.index(lettre)
        y = (a * x + b) % 26
        resultat = resultat + alphabet[y]
    return resultat
```

(a) Que renvoie `chiffre("LOUP", 7, 2)` ? Détaille le calcul.

(b) Lou écrit la ligne `y = a * x + b % 26`. Explique ce que calcule alors Python pour la lettre L avec $a = 7$ et $b = 2$, puis ce qui se passe.

(c) Noé écrit la ligne `x = alphabet.index(lettre) + 1`. Que renvoie alors `chiffre("A", 7, 2)` ? Explique l'erreur.

(d) Écris une fonction `dechiffre(mot)` qui déchiffre un mot chiffré avec $a = 7$ et $b = 2$. Justifie la formule que tu utilises.

Ex. 46 ★★★ **Retrouver la clé d'un espion** — On numérote les lettres A $= 0$, B $= 1$, …, Z $= 25$. Un espion chiffre la lettre de rang x par la lettre de rang y, où $y \equiv ax + b \pmod{26}$ et $0 \leqslant y \leqslant 25$. Ses entiers secrets a et b sont compris entre 0 et 25. On sait que E est chiffré Y et que S est chiffré W. La clé de l'espion doit permettre de déchiffrer.

(a) Traduis les deux informations connues par deux congruences vérifiées par a et b.

(b) Élimine b, puis démontre que a vérifie une congruence modulo 13. Résous-la.

(c) Déduis-en les deux valeurs possibles de a entre 0 et 25 et, pour chacune, la valeur de b.

(d) L'une des deux clés trouvées chiffre de la même façon deux lettres distinctes. Lesquelles ? Déduis-en la clé de l'espion.

(e) Détermine un inverse de 11 modulo 26, puis déchiffre le message intercepté LQDY.

Ex. 47 ★★★ **Le code ISBN-13 sous la loupe** — Un code ISBN-13 s'écrit avec 13 chiffres $a_1 a_2 \dots a_{13}$. On pose $S = a_1 + 3a_2 + a_3 + 3a_4 + \cdots + 3a_{12} + a_{13}$: le poids est 1 aux rangs impairs et 3 aux rangs pairs. Le code est valide lorsque $S \equiv 0 \pmod{10}$; le chiffre a_{13} est la clé.

(a) Le livre d'Inès, acheté à Rennes, porte le code 978270119384 suivi d'une clé effacée. Calcule la somme sans la clé, puis la clé.

(b) Démontre qu'une erreur sur un seul chiffre, remplacé par un autre chiffre, est toujours détectée.

(c) Deux chiffres voisins distincts c et d sont échangés. Détermine à quelle condition sur c et d l'erreur passe inaperçue.

(d) Dans le code complet du livre d'Inès, quels échanges de deux chiffres voisins passent le contrôle ? Vérifie un cas par le calcul.

(e) Une autre caisse utilise les poids 1 et 2 au lieu de 1 et 3. Montre, par un exemple pris sur le code d'Inès, qu'une erreur sur un seul chiffre peut alors passer inaperçue.

Ex. 48 ★★★ **Toutes les clés affines au banc d'essai** — Avec A $= 0$, …, Z $= 25$, on chiffre par $y \equiv ax + b \pmod{26}$, $0 \leqslant y \leqslant 25$. Le programme suivant teste toutes les valeurs de a :

```
def injective(a, b):
    images = []
    for x in range(26):
        y = (a * x + b) % 26
        if y in images:
            return False
        images.append(y)
    return True

n = 0
for a in range(26):
    if injective(a, 0):
        n = n + 1
print(n)
```

(a) Que renvoie `injective(13, 5)` ? Justifie en trouvant deux lettres chiffrées de la même façon.

(b) Démontre que, si a est pair, les lettres de rangs x et $x + 13$ ont la même image. Que renvoie alors `injective(a, b)` ?

(c) Démontre que, si $\text{pgcd}(a\,;26) = 1$, deux lettres distinctes ont toujours des images distinctes.

(d) Déduis-en ce qu'affiche le programme. Justifie.

(e) Pour $\text{pgcd}(a\,;26) = 1$, écris une fonction `dechiffre(mot, a, b)` qui cherche l'inverse de a par une boucle `while`. Que renvoie `dechiffre("QKX", 17, 20)` ?