

# Exercices Mathématiques pour l'informatique I :

## Arithmétique

1. Les nombres suivants divisent-ils 12 ? Justifiez.

$$a = 24 \quad ; \quad b = -6 \quad ; \quad c = 4 \quad ; \quad d = 12 \quad ; \quad e = 9.$$

2. Déterminez le quotient et le reste de la division euclidienne de 111 par 11 ; de 123 par 7 ; de 777 par 21 ; de 1434 par 13 ; de 1025 par 15 et de  $-38$  par 6.

3. Calculez :

$$7 \bmod 5 ; 789 \bmod 5672 ; 77 \bmod 11 ; 55 \bmod 7 ; 72 \bmod 13.$$

4. Montrez que pour tout  $n \in \mathbb{Z}$ ,  $(n+2)^2 - n^2$  est divisible par 4.

5. On fait la division euclidienne d'un entier  $n$  par 137 et par 143. Les quotients sont égaux et les restes respectifs sont 131 et 5. Quel est l'entier  $n$  ?

6. Déterminez tous les entiers naturels qui, dans la division euclidienne par 3, donnent un quotient égal au double du reste.

7. Prouvez les propositions suivantes :

- (a)  $\forall a \in \mathbb{Z}_0, \quad 1|a$ .
- (b)  $\forall a \in \mathbb{Z}_0, \quad a|0$ .
- (c)  $\forall a \in \mathbb{Z}_0, \quad a|a$ .
- (d)  $\forall a, b \in \mathbb{Z}_0, \quad a|b \Rightarrow (\forall c \in \mathbb{Z}_0 \quad a|(b.c))$ .
- (e)  $\forall a, b, c \in \mathbb{Z}_0, \quad (a|b \wedge b|c) \Rightarrow a|c$ .
- (f)  $\forall a, b, c \in \mathbb{Z}_0, \quad (a|b \wedge a|c) \Rightarrow a|(b+c)$ .
- (g)  $\forall a, b, c \in \mathbb{Z}_0, \quad (a|b \wedge a|c) \Rightarrow a|(b-c)$ .
- (h)  $\forall a, b, c \in \mathbb{Z}_0, \quad (a|b \vee a|c) \Rightarrow a|(b.c)$ .
- (i)  $\forall a, b, c, d \in \mathbb{Z}_0, \quad (a|b \wedge c|d) \Rightarrow (a.c)|(b.d)$ .

8. Déduisez de l'exercice 7 les deux propositions suivantes :

- (a)  $\forall a, b \in \mathbb{Z}_0, \quad a|b \Rightarrow (\forall c \in \mathbb{Z}_0 \quad a|(b+a.c))$ .
- (b)  $\forall a, b, c \in \mathbb{Z}_0, \quad (a|b \wedge a|c) \Rightarrow (\forall d, e \in \mathbb{Z}_0 \quad a|(d.b+e.c))$ .

9. Prouvez que pour tous  $a, b \in \mathbb{Z}_0$ , si  $a|b$  et  $b|a$ , alors  $a = b$  ou  $a = -b$ .

10. Prouvez que pour tous  $a, b, n, m \in \mathbb{N}$ , si  $n, m \geq 2$ ,  $n|m$  et  $a \equiv_m b$ , alors  $a \equiv_n b$ .

11. Prouvez que pour tout  $n \in \mathbb{N}$ , si  $n$  est impair, alors  $n^2 \equiv_8 1$ . De même, prouvez que pour tout  $n \in \mathbb{N}$ , si  $n$  est pair, alors  $n^2 \equiv_8 0$  ou  $n^2 \equiv_8 4$ .

12. Prouvez que la première proposition est *fausse* et que la deuxième est *vraie*.
- (a)  $\forall a, b, c \in \mathbb{Z}_0, \quad (a|c \wedge b|c) \Rightarrow (a.b)|c.$
- (b)  $\forall a, b, c \in \mathbb{Z}_0$  tels que  $a, b$  premiers entre eux,  $(a|c \wedge b|c) \Rightarrow (a.b)|c.$
13. Le nombre d'élèves dans l'auditoire est compris entre 100 et 200 élèves. Si l'on range les élèves par 3, par 5 ou par 7, il reste toujours 2 élèves. Combien y a-t-il d'élèves dans cet auditoire ? (aide : utilisez l'exercice 12).
14. On effectue la division euclidienne d'un entier  $a$  par 7, le reste est 4. Quel peut être le reste de la division euclidienne de  $a$  par 21 ?
15. En Belgique, un numéro de compte est toujours de la forme :

$$123 - 1234567 - 12.$$

Les trois premiers chiffres forment un code identifiant la banque, les sept chiffres suivants constituent réellement le numéro de compte du client et les deux derniers chiffres sont là pour vérifier les autres. Si le numéro de compte est un numéro valable, les deux derniers chiffres sont en fait le reste de la division par 97 du nombre composé des dix premiers chiffres (le code de la banque suivi du numéro de compte du client). Cette petite vérification, permet d'éviter un grand nombre d'erreurs de frappes, avant la validation un virement électronique. Vérifiez que les numéros de compte suivants sont des numéros de compte valide :

- Médecins Sans Frontières : 000 – 0000060 – 60.
- Amnesty International : 001 – 0520520 – 94.

16. Prouvez que les deux propositions suivantes sont *vraies* :
- (a)  $\forall a, b, c, d \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a \equiv_m b \wedge c \equiv_m d) \Rightarrow (a + c) \equiv_m (b + d).$
- (b)  $\forall a, b, c, d \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a \equiv_m b \wedge c \equiv_m d) \Rightarrow (a.c) \equiv_m (b.d).$
17. Prouvez que les deux propositions suivantes sont *fausses* :
- (a)  $\forall a, b, c, d \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a + c) \equiv_m (b + d) \Rightarrow (a \equiv_m b \wedge c \equiv_m d).$
- (b)  $\forall a, c, d \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a.c) \equiv_m (a.d) \Rightarrow c \equiv_m d.$
18. Déduisez de l'exercice 16 que les deux propositions suivantes sont *vraies* :
- (a)  $\forall a, b \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m.$
- (b)  $\forall a, b \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a.b) \bmod m = ((a \bmod m).(b \bmod m)) \bmod m.$
19. En utilisant la deuxième égalité de l'exercice 18, calculez  $3^{25} \bmod 1037$  (sans élever 3 à la puissance 25).
20. Soient  $a$  et  $b \in \mathbb{Z}$  tels que leurs restes modulo 11 sont 7 et 2 respectivement. Calculez le reste modulo 11 de  $a^2 - b^2$  (aide : utilisez l'exercice 18).
21. Déterminez les restes modulo 7 de  $10, 10^2, 10^3, 10^4$  et  $10^5$ . En déduire que 111111 est un multiple de 7. (aide : utilisez l'exercice 18).

22. Prouvez que les deux propositions suivantes sont *fausses* :
- (a)  $\forall a, b \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a + b) \bmod m = (a \bmod m) + (b \bmod m).$
  - (b)  $\forall a, b \in \mathbb{Z}, \forall m \in \mathbb{N}_0 \quad (a.b) \bmod m = (a \bmod m).(b \bmod m).$
23. Les affirmations suivantes sont-elles vraies ou fausses ? Justifiez.
- (a)  $\forall a, b \in \mathbb{Z} \quad (a \bmod 2) + (b \bmod 2) = (a + b) \bmod 2.$
  - (b)  $\forall a, b \in \mathbb{Z} \quad (a \bmod 2).(b \bmod 2) = (a.b) \bmod 2.$
24. Pour  $n \in \mathbb{N}$ , on note  $D_n$  l'ensemble des diviseurs naturels de  $n$  :  $D_n = \{x \in \mathbb{N} \text{ tel que } x|n\}$ .
- (a) Calculez  $D_{12}$  et  $D_{16}$ .
  - (b) Calculez  $|D_p|$  (le cardinal de  $D_p$ ) pour tout naturel  $p$  premier.
  - (c) Montrez que pour tout  $n \in \mathbb{N}$ ,  $D_n \neq \emptyset$ .
  - (d) Montrez que pour tout  $n \in \mathbb{N}$ ,  $|D_n|$  est pair ssi  $n$  n'est pas un carré parfait.
25. Un résultat connu en arithmétique est *l'identité de Bezout*. Ce théorème affirme que : étant donnés  $a, b \in \mathbb{Z}$  non tous deux nuls, il existe  $x, y \in \mathbb{Z}$  tel que :

$$ax + by = \text{pgcd}(a, b).$$

En utilisant ce résultat, montrez que, quels que soient  $m, n \in \mathbb{Z}$  et  $p$  un nombre premier, si  $p|m.n$ , alors  $p|m$  ou  $p|n$ .

Ce résultat est-il toujours vrai si  $p$  n'est pas premier ?

26. Utilisez l'exercice 25 pour démontrer le théorème fondamental de l'arithmétique.
27. Déterminez lesquels de ces nombres sont premiers : 21, 71, 111 et 143.
28. Décomposez les nombres suivants en nombres premiers : 88, 124, 289 et 402.
29. Calculez :  $\text{pgcd}(15, 36)$ ,  $\text{ppcm}(21, 49)$ ,  $\text{pgcd}(121, 125)$ ,  $\text{ppcm}(31, 81)$ .
30. Prouvez que le produit de trois entiers consécutifs est toujours divisible par 6.
31. Ecrivez en notation binaire les nombres suivants : 7, 9, 11, 31 et 65.
32. Ecrivez en notation hexadécimale les nombres suivants : 13, 31 et 65.
33. Convertissez les entiers suivants de l'hexadécimal au décimal :  $A0B1$  et  $F0A02$ .
34. Convertissez les entiers suivants de l'hexadécimal au binaire :  $ABBA$  et  $FACE$ .
35. Convertissez les entiers suivants du binaire en hexadécimal : 1111 1011 et 1001 1101.
36. Trouvez un inverse de 5 modulo 11, ainsi qu'un inverse de 3 modulo 7.
37. Prouvez que  $2^{340} \equiv_{11} 1$ .

38. Déterminez tous les entiers entre 1 et 20 vérifiant l'énoncé suivant :

*“Si  $n$  est pair, alors son successeur est premier.”*

(Rappel : soit  $n \in \mathbb{Z}$ , le successeur de  $n$  est  $n + 1$ .)

39. Pour chacune des équations suivantes, trouvez tous les entiers qui en sont solutions :

$$x \equiv_{37} 0 \quad ; \quad 3x \equiv_4 2 \quad ; \quad x^2 + 2x + 1 \equiv_2 1 \quad ; \quad x^2 + 1 \equiv_5 0 \quad ; \quad x^2 \equiv_4 x^2(x + 1).$$

40. Décidez si les affirmations suivantes sont vraies ou fausses. Justifiez votre réponse.

- (a) Tout entier est congru modulo 6 à un des entiers 0, 1, 2, 3,  $-1$  ou  $-2$ .
- (b) Soient  $a, b, c \in \mathbb{Z}_0$ , si  $a$  divise  $b$  et  $b$  ne divise pas  $c$ , alors  $a$  ne divise pas  $c$ .
- (c) Soit  $a \in \mathbb{Z}$ , si  $a|1$ , alors  $a = 1$ .
- (d) Soient  $a, b, p \in \mathbb{N}_0$ , si  $p|ab$ , alors  $p|a$  ou  $p|b$ .
- (e)  $2^{300} \equiv_{11} 2$ .
- (f) Soient  $x, y \in \mathbb{Z}$ , si  $x \neq 0$  et  $y \neq 0$ , alors  $x.y \not\equiv_6 0$ .
- (g) Soit  $p$  un nombre premier, le nombre  $p^2 - p$  n'est jamais premier.
- (h) Quels que soient  $a, b \in \mathbb{Z}$  et  $n \in \mathbb{N}_0$  :  $(a + b) \bmod n = (a \bmod n) + (b \bmod n)$ .
- (i) Soient  $p_1, p_2 \in \mathbb{N}$ , si  $p_1$  et  $p_2$  sont premiers, alors  $\text{pgcd}(p_1, p_2) = 1$ .
- (j) Tout nombre naturel dont le carré est premier est un multiple de sept.
- (k) Pour tout  $p \in \mathbb{N}$ , si  $p$  vérifie l'équation  $x^2 + 2 \equiv_5 1$ , alors  $p$  est premier.
- (l) Soient  $p$  un nombre premier et  $a, b \in \mathbb{N}$ , si  $1 \leq a, b \leq p - 1$ , alors  $ab \not\equiv_p 0$ .
- (m) Soient  $a, b, p \in \mathbb{N}$ , si  $1 \leq a, b \leq p - 1$ , alors  $ab \not\equiv_p 0$ .
- (n) Soient  $a, p \in \mathbb{N}$ ,  $a^2 \bmod p = (a \bmod p)^2$ .
- (o)  $\{b \in \mathbb{N} \mid \exists n \in \mathbb{N} \ b \equiv_7 4^n\} = \{1, 2, 4\}$ .
- (p)  $\{b \in \mathbb{N} \mid \exists n \in \mathbb{N} \ b = (4^n \bmod 7)\} = \{1, 2, 4\}$ .
- (q)  $\forall n \in \mathbb{Z}, |n| \leq n^2$ .
- (r)  $\forall a, b, c \in \mathbb{Z}, \forall m \in \mathbb{N}_0$ , on a  $(a + b \equiv_m a + c) \Rightarrow (b \equiv_m c)$ .
- (s)  $\forall a, b, c, m \in \mathbb{N}_0$ , tous premiers, on a  $(a \cdot b \equiv_m a \cdot c) \Rightarrow (b \equiv_m c)$ .
- (t)  $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, n \leq x \leq n + 1$ .

41. Pour  $n \in \mathbb{N}$ , on définit

$$X_n = \{x \in \mathbb{R} \mid n \bmod 2 \leq x \leq n \bmod 4\} \quad ; \quad Y_n = \{x \in \mathbb{N} \mid (2|n) \Rightarrow (x \leq n)\}.$$

- (a) Calculez  $X_0, X_1, X_2, X_3$  et  $X_{82}$ .
- (b) Calculez  $\bigcup_{n \geq 0} X_n$ .
- (c) Calculez  $\bigcup_{n \geq 0} Y_n$  et  $\bigcap_{n \geq 0} Y_n$ .

42. Un “truc” pour tester rapidement qu’un nombre naturel est divisible par 3 est de tester que la somme de ses digits dans son écriture en base 10 est divisible par 3. Par exemple, 123 est divisible par 3, car  $1 + 2 + 3 = 6$  est divisible par 3. Le but de cet exercice est d’essayer de comprendre ce “truc”.

- (a) Quel que soit  $k \in \mathbb{N}$ , calculez le reste de la division de  $10^k$  par 3.
- (b) Soit  $n \in \mathbb{N}$ , on sait que l’on peut écrire  $n$  en base 10 (vous ne devez pas le prouver) ; c’est-à-dire que l’on peut écrire  $n$  sous la forme suivante :

$$n = \sum_{k=0}^K a_k 10^k$$

pour un certain  $K \in \mathbb{N}$ , avec  $a_k \in \{0, 1, \dots, 9\}$ . Par exemple,  $123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$ . En utilisant cette écriture, formalisez (à l’aide d’une implication) qu’une condition nécessaire pour qu’un nombre naturel soit divisible par 3 est que la somme de ses digits dans son écriture en base 10 soit divisible par 3.

- (c) En utilisant le point (a), prouvez la propriété que vous avez formulée au point (b).
  - (d) Déterminez si la réciproque de la propriété que vous avez formulée au point (b) est vraie.
  - (e) Ce “truc” est-il vrai pour tester la divisibilité d’un naturel par un autre nombre que 3 ? Expliquez votre raisonnement !
43. Soit la fonction  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  définie ci-dessous :

$$f(n) = n \mod 5.$$

- (a) La fonction  $f$  est-elle injective ? Justifiez votre réponse.
  - (b) La fonction  $f$  est-elle surjective ? Justifiez votre réponse.
44. Soit  $k \in \mathbb{N}$  tel que  $k \geq 2$ . Soit la fonction  $f_k : \mathbb{Z} \rightarrow \{0, 1, \dots, k-1\}$  définie ci-dessous :

$$f_k(n) = n \mod k.$$

- (a) La fonction  $f_k$  est-elle injective ? Justifiez votre réponse.
  - (b) La fonction  $f_k$  est-elle surjective ? Justifiez votre réponse.
45. Soit la fonction  $f : \mathbb{N}_0 \rightarrow 2^{\mathbb{N}}$  définie ci-dessous :

$$f(n) = \{m \in \mathbb{N}_0 \text{ tel que } m|n\}.$$

- (a) La fonction  $f$  est-elle injective ? Justifiez votre réponse.
- (b) La fonction  $f$  est-elle surjective ? Justifiez votre réponse.

46. Soit la fonction  $f : \mathbb{N} \rightarrow 2^{\mathbb{N}}$  définie ci-dessous :

$$f(n) = \{m \in \mathbb{N}_0 \text{ tel que } m|n\}.$$

(a) La fonction  $f$  est-elle injective ? Justifiez votre réponse.

(b) La fonction  $f$  est-elle surjective ? Justifiez votre réponse.

47. Soit la fonction  $f : \mathbb{N} \rightarrow 2^{\mathbb{N}} \setminus \{\emptyset\}$  définie ci-dessous :

$$f(n) = \{m \in \mathbb{N}_0 \text{ tel que } m|n\}.$$

(a) La fonction  $f$  est-elle injective ? Justifiez votre réponse.

(b) La fonction  $f$  est-elle surjective ? Justifiez votre réponse.

48. Soit la fonction  $f : \mathbb{N} \rightarrow 2^{\mathbb{N}}$  définie ci-dessous :

$$f(n) = \{p \in \mathbb{N} \text{ tel que } p|n \text{ et } p \text{ est premier}\}.$$

(a) La fonction  $f$  est-elle injective ? Justifiez votre réponse.

(b) La fonction  $f$  est-elle surjective ? Justifiez votre réponse.