Arithmétique

1. Division euclidienne
Quels que soient $x \in \mathbb{R}$ et $n \in \mathbb{N}^*$, il existe deux entiers q et r tels que
$$\lfloor x \rfloor = nq + r.$$
En déduire que, pour tout $m \in \mathbb{N}$,
$$\left\lfloor \frac{x+m}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + m}{n} \right\rfloor.$$

I
Congruences

2. La somme et le produit de trois entiers consécutifs sont divisibles par 3.

3. L'entier $2^{123} + 3^{121}$ est divisible par 11.

4. Les entiers $1 + 2^{30} + 3^{30} + 4^{30}$ et
$$1^{1001} + 2^{1001} + 3^{1001} + 4^{1001} + 5^{1001}$$
sont divisibles par 5.

5. Pour tout $n \in \mathbb{N}$, les entiers
$$5^{6n+1} + 2^{3n+1} \quad \text{et} \quad 5^{n+2} + 3^{n+1}.5^{2n}$$
sont divisibles par 7.

6. L'entier $n = 10d + u$ est divisible par 7 si, et seulement si, $3d + u$ est divisible par 7.
Comme $3 \times 5 = 1 \mod 7$, on en déduit que n est divisible par 7 si, et seulement si, $d + 5u$ est divisible par 7. Cela équivaut au fait que $d - 2u$ soit divisible par 7.
L'entier 2654 est-il divisible par 7 ? (Non.)

7. Quel que soit $n \in \mathbb{N}$, l'entier
$$n(n+3)(n+6)(n+13)$$
est divisible par 4.

8. Pour tout entier $n \in \mathbb{N}$,
$$\begin{aligned} 5n^3 + n &= -n^3 + n \mod 6 \\ &= n(n-1)(n+1) = 0 \mod 6. \end{aligned}$$

9. Pour tout entier $p \in \mathbb{N}$,
$$p(p^2+2) = p(p-1)(p+1) = 0 \mod 3.$$
Par conséquent,
$$3p^3 + 6p = 3p(p^2+2) = 0 \mod 9$$
et $n^3 + (n+1)^3 + (n+2)^3$ est divisible par 9 pour tout entier $n \in \mathbb{N}$.

10. Pour tout $n \in \mathbb{N}$, on pose
$$b_n = 4^{2n+2} - 15n - 16.$$

10.1 Pour tout $n \in \mathbb{N}$, l'entier $4^{2n+2} - 1$ est divisible par 15.
10.2 Pour tout $n \in \mathbb{N}$, la différence $b_{n+1} - b_n$ est divisible par $225 = 15^2$. Donc tous les entiers b_n sont divisibles par 225.

11. Pour tout $n \in \mathbb{N}$,
$$4^n = 1 + 3n \mod 9$$
et par conséquent l'entier $2^{2n} + 15n - 1$ est divisible par 9.

12. Pour quelles valeurs de $n \in \mathbb{N}$ l'entier
$$5^{6n+1} + 2^{2n}$$
est-il divisible par 5 ?

13. Résoudre l'équation $x^2 - 5y^2 = 3$ dans $\mathbb{Z}^2$. (Réduire modulo 5.)

14. Si $x = 5 \mod 6$, alors $x = -1 \mod 3$. La réciproque est fausse.

15. Carrés et cubes
15.1 Si $x = 1 \mod 5$, alors $x^2 = 1 \mod 5$.
15.2 Pour tout $x \in \mathbb{Z}$,
$$\begin{aligned} &x^2 \neq 2 \mod 3, \\ &x^2 = 0 \text{ ou } 1 \mod 4, \\ &x^3 = 0, \ 1 \text{ ou } 8 \mod 9. \end{aligned}$$
15.3 Si $n = x^2 + y^2$, alors $n \neq 3 \mod 4$.
15.4 Quels que soient les entiers relatifs a et b,
$$a^3 - b^3 = 0 \mod 3 \iff a - b = 0 \mod 3.$$
15.5 Si 9 divise $a^3 + b^3 + c^3$, alors a, b et c sont multiples de 3.
15.6 Si 7 divise $a^3 + b^3 + c^3$, alors abc est un multiple de 7.

16. Carrés modulo 7
Quels sont les carrés modulo 7 ? En déduire que les deux entiers x et y sont divisibles par 7 si, et seulement si, $x^2 + y^2$ est divisible par 7.

17. Soit $n \in \mathbb{N}$. Si n est impair, alors
$$7^n + 1 = 0 \mod 8$$
et si n est pair, alors
$$7^n + 1 = 2 \mod 8.$$

18. On cherche les couples $(m, n) \in \mathbb{N}^2$ tels que
$$2^m - 3^n = 1.$$
18.1 Quel que soit l'entier $k \in \mathbb{N}$,
$$3^{2k} + 1 = 2 \mod 8 \quad \text{et} \quad 3^{2k+1} + 1 = 4 \mod 8.$$
18.2 On en déduit que, si (m, n) est une solution, alors $m \leqslant 2$.
18.3 Les solutions sont donc $(1, 0)$ et $(2, 1)$.

19. Équation du second degré
On cherche les entiers relatifs n tels que
$$n^2 - 3n + 6 = 0 \mod 5.$$
19.1 Calculer $n^2 - 3n + 6$ pour tout $n \in \mathbb{Z}/5\mathbb{Z}$.
19.2 Quel est l'élément $a \in \mathbb{Z}/5\mathbb{Z}$ tel que $2a = 1 \mod 5$? En déduire que
$$n^2 - 3n + 6 = (n+1)^2 \mod 5$$
et conclure.

20. Puissances modulo 8

20.1 Si l'entier x est impair, alors $x^2 = 1 \mod 8$.

20.2 Si l'entier x est pair, alors $x^2 = 0$ ou $4 \mod 8$.

20.3 On suppose que les entiers a, b et c sont impairs.

1. Que vaut $a^2 + b^2 + c^2$ modulo 8 ? Et $2(ab + bc + ca)$?
2. En déduire que l'entier $a^2 + b^2 + c^2$ n'est pas un carré et que l'entier impair $ab + bc + ca$ n'est pas non plus un carré.

21. On note X, l'ensemble des nombres premiers p tels que

$$p = 3 \mod 4.$$

21.1 L'ensemble X n'est pas vide.

21.2 Si p et q sont deux nombres premiers congrus à 1 modulo 4, alors $pq = 1 \mod 4$.

21.3 On suppose que X est un ensemble fini :

$$X = \{p_1, \dots, p_n\}$$

et on pose

$$a = 4p_1 \cdots p_n - 1.$$

1. L'entier a admet un facteur premier appartenant à X.
2. L'entier a est premier à tous les éléments de X.
3. Conclure !

22. On considère l'entier

$$N = 4444^{4444}.$$

22.1 L'entier 4444 est congru à 4 modulo 10 et à 7 modulo 9. L'entier N est donc congru à 6 modulo 10 et à 7 modulo 9.

22.2 Pour tout entier $n \in \mathbb{N}^*$, on note $\sigma(n)$, la somme des chiffres de n (dans la représentation en base 10) et on pose

$$A = \sigma(N), \quad B = \sigma(A), \quad C = \sigma(B).$$

1. Si $n < 10^k$, alors $\sigma(n) \leqslant 9k$.

Comme $N < 10^{4 \times 4444}$, alors $0 \leqslant C \leqslant 18$.

2. Comme $N = A = B = C \mod 9$, alors $C = 6$ ou $C = 16$.
3. Une estimation plus précise (à l'aide de exp...) nous donne $A < 150000$, donc $B \leqslant 41$ et $C \leqslant 12$. Donc $C = 6$.

II

Facteurs premiers

23. Décompostion en facteurs premiers

$612 = 2^2.3^2.17$	$663 = 3.13.17$
$680 = 2^3.5.17$	$629 = 17.37$
$945 = 3^3.5.7$	$738 = 2.3^2.41$
$532 = 2^2.7.19$	$828 = 2^2.3^2.23$
$2145 = 3.5.11.13$	$2793 = 3.7^2.19$
$5418 = 2.3^2.7.49$	$5448 = 2^3.3.227.$

24. Soient x et y, deux entiers naturels. On note d et m, leur pgcd et leur ppcm et on suppose que

$$m - d = 3 \quad \text{et que} \quad m \mid 243 = 3^5.$$

Comme d divise 3^5, il faut que d soit une puissance de 3. Comme le ppcm $m = 3^p + 3$ est divisible par le pgcd $d = 3^p$, il faut que $p \in \{0, 1\}$.
Les seules possibilités sont donc

$$\{x, y\} = \{1, 4\} \quad \text{et} \quad \{x, y\} = \{3, 6\}.$$

25. Soient $x < y$, deux entiers. On suppose que leur pgcd est égal à 5 et leur ppcm à 60. Alors $(x, y) = (15, 20)$ ou $(x, y) = (5, 60)$.

26.1 Pour tout entier $p \geqslant 3$,

$$\frac{(p-1)^3 + (p+1)^3}{4} = \frac{p(p+3)}{2}.$$

L'un des deux facteurs est pair et supérieur à 4, donc le quotient est un entier et, après simplification, les deux facteurs sont supérieurs à 2.

26.2 Pour tout entier $n \geqslant 2$, le quotient

$$\frac{n^3 + (n+2)^3}{4}$$

est un entier composé.

27. Soit p, un nombre premier supérieur à 5. Alors l'entier

$$p^2 - 1 = (p-1)(p+1)$$

est divisible par 24. (Le facteur manquant, p, n'est pas un multiple de 3.)

28. Somme géométrique et nombres de Mersenne

1. Quels que soient les entiers p et q, les entiers $2^p - 1$ et $2^q - 1$ divisent $2^{pq} - 1$.
2. Si $2^n - 1$ est premier, alors l'exposant n est premier.
3. Cependant, $n = 11$ est premier alors que

$$2^{11} - 1 = 2047 = 23 \times 89.$$

29. Si les entiers a et b sont premiers entre eux et si le produit ab est un carré, alors a et b sont des carrés.

30.1 Si $x = a^2 = b^3$, alors il existe un entier c tel que $x = c^6$ et

$$x = 0 \quad \text{ou} \quad 1 \mod 7.$$

30.2 S'il existe deux entiers a et b tels que

$$x = a^n = b^m$$

où les exposants m et n sont premiers entre eux, alors il existe un entier c tel que

$$a = c^m \quad \text{et} \quad b = c^n.$$

31. Soit $n \in \mathbb{N}^*$.

31.1 Combien existe-t-il de diviseurs de n ?

31.2 Le nombre de diviseurs de n est impair si, et seulement si, n est un carré.

32. Nombres parfaits

Un entier $N \in \mathbb{N}$ est **parfait** si, et seulement si, la somme de ses diviseurs *stricts* est égale à N.
Pour tout entier $N \in \mathbb{N}$, on note $\sigma(N)$, la somme des *tous* les diviseurs de N.

32.1 L'entier N est parfait si, et seulement si, $\sigma(N) = 2N$.

32.2 Si $N = p_1^{m_1} \cdots p_r^{m_r}$, alors

$$\sigma(N) = \prod_{k=1}^{r} (1 + p_k + \cdots + p_k^{m_k}).$$

Simplifier cette expression.

32.3 Si a et b sont premiers entre eux, alors $\sigma(a)\sigma(b) = \sigma(ab)$.

32.4 Si l'entier $2^{n+1} - 1$ est premier, alors l'entier

$$2^n(2^{n+1} - 1)$$

est parfait.

32.5 On suppose que x est un entier parfait *pair*.

1. Il existe un entier $k \in \mathbb{N}^*$ et un entier impair m tels que $x = 2^k.m$.

2. Comme N est parfait,

$$\sigma(N) = 2N = 2^{k+1}q = \sigma(2^k)\sigma(q).$$

Il existe donc $r \in \mathbb{N}^*$ tel que

$$\sigma(q) = 2^{k+1}r \quad \text{et} \quad q = (2^{k+1}-1)r.$$

3. Comme $r = 1$, alors $\sigma(q) = q+1$, donc

$$x = 2^k \cdot (2^{k+1}-1)$$

où $q = 2^{k+1}-1$ est premier.

III

Théorème de Bézout (et de Gauss)

33. Si a divise c, si b divise c et si a et b sont premiers entre eux, alors le produit ab divise c.
Si a et b ne sont pas premiers entre eux, alors $a \vee b$ divise c (par définition du ppcm).

34. S'il existe trois entiers d, α et β tels que

$$a = d.\alpha, \quad b = d.\beta \quad \text{et} \quad \alpha \wedge \beta = 1,$$

alors $d = a \wedge b$ et $d.\alpha.\beta = a \vee b$.

35. Si a divise le produit $b.c$ et si a et b sont premiers entre eux, alors a divise c.

36. Soit p, un nombre premier. Pour tout entier $1 \leqslant k < p$,

$$k \times \binom{p}{k} = p \times \binom{p-1}{k-1}.$$

Le membre de gauche est donc divisible par p et le facteur k est premier à p. Donc p divise le coefficient binomial $\binom{p}{k}$.

37. Soit $p \geqslant 2$, un entier. Alors

$$\binom{2p+2}{p+1} = 2 \times (2p+1) \times \frac{\binom{2p}{p}}{p+1}$$

et comme l'entier $(p+1)$ est premier à 2 et à $(2p+1)$, alors il divise le coefficient binomial $\binom{2p}{p}$.
On en déduit par récurrence que $\binom{2p}{p}$ est pair pour tout entier $p \in \mathbb{N}^*$.

38.1 Si on considère n entiers consécutifs, l'un d'eux est divisible par n.

38.2 Soient $a \geqslant 2$ et b, deux entiers. Lorsque l'entier k varie de 0 à $(n-1)$, l'un des entiers $ak+b$ est divisible par n si, et seulement si, a et n sont premiers entre eux.

38.3 Trouver (s'il en existe) un point à coordonnées entières sur la droite d'équation $ax+by=c$.

$$\begin{array}{ccc} 2x-3y+1=0 & 5x+2y-2=0 & -3x+6y+2=0 \\ 8x+12y-4=0 & 6x-10y+8=0 & 7x+4y-2=0 \end{array}$$

39.

1. Résoudre les équations suivantes.

$$\begin{array}{cc} 95x+71y=46 & 20x-53y=3 \\ 71x+31y=2 & 12x+15y+20z=7 \end{array}$$

2. Résoudre les équations suivantes après avoir simplifié.

$$\begin{array}{l} 325x+299y=39 \\ 2520x-3960y=6480 \end{array}$$

40. Soit d, le pgcd de deux entiers a et b. Alors il existe deux entiers α et β, premiers entre eux, tels que

$$a = d\alpha \quad \text{et} \quad b = d\beta.$$

Il existe donc deux entiers u et v, premiers entre eux, tels que

$$au + bv = d.$$

a		b		d	α	β	u	v
120	$2^3.3.5$	450	$2.3^2.5^2$	30	4	15	4	-1
525	$3.5^2.7$	220	$2^2.5.11$	5	105	44		
2574	$2.3^2.11.13$	588	$2^2.3.7^2$	6	429	98		
2139	3.23.31	1615	5.17.19	1				

41.1 Pour tout entier $n \in \mathbb{N}$, les entiers $a, b \in \mathbb{Z}$ tels que

$$5a + 6b = n$$

sont de la forme

$$(a,b) = (-n+6k,\ n-5k). \qquad (k \in \mathbb{Z})$$

Pour $n \geqslant 30$, on peut choisir a et b dans $\mathbb{N}$.

41.2 On dispose de 59 euros en pièces de 2 euros et en billets de 5 euros. Combien de pièces et de billets ?

41.3 Si a et b sont premiers entre eux, alors pour tout $x \geqslant ab$, il existe deux entiers *naturels* u et v tels que

$$au + bv = x.$$

42. Soit $n \in \mathbb{N}$.

42.1 Quels que soient les entiers k et ℓ,

$$(a,b,c) = (-n+2k,\ n-3k+3\ell,\ n-5\ell)$$

est une solution de l'équation

$$15a + 10b + 6c = n.$$

42.2 Le triplet (a,b,c) appartient à $\mathbb{N}^3$ si, et seulement si,

$$k \geqslant \frac{n}{2}, \quad \ell \leqslant \frac{n}{5} \quad \text{et} \quad k - \ell \leqslant \frac{n}{3}.$$

Il faut donc que l'entier $k-\ell$ vérifie

$$\frac{3n}{10} \leqslant k - \ell \leqslant \frac{n}{3}.$$

Réciproquement, si on choisit deux entiers $d \in \mathbb{Z}$ et $\ell \in \mathbb{N}$ tels que

$$\frac{3n}{10} \leqslant d \leqslant \frac{n}{3} \quad \text{et} \quad \ell \leqslant \frac{n}{5},$$

alors $k = d + \ell$ est un entier naturel tel que

$$k \geqslant \frac{n}{2}.$$

42.3 Pour tout $n \geqslant 30$, il existe au moins un triplet $(a,b,c) \in \mathbb{N}^3$ tel que

$$15a + 10b + 6c = n.$$

43.1 Les entiers $70 = 2.5.7$, $75 = 3.5^2$ et $54 = 2.3^3$ sont premiers dans leur ensemble et

$$4.54 - 2.70 - 1.75 = 1.$$

43.2 Autres exemples

$$\begin{aligned} 2.82 - 3.88 + 99 &= -1 \\ -7.47 + 1.54 + 3.92 &= 1 \\ -33.73 + 33.67 + 1.71 &= 1 \end{aligned}$$

44. Trouver les entiers relatifs x tels que

$$x = 2 \mod 140 \quad \text{et} \quad x = -3 \mod 99.$$

45. Le nombre d'étudiants en première année est compris entre 500 et 1000. Qu'on les rassemble en groupes de 18, de 20 ou de 24, il reste toujours 9 étudiants. Quel est le nombre d'étudiants ?

46. L'équation $ax = b \mod n$ admet au moins une solution $x \in \mathbb{Z}$ si, et seulement si, $a \wedge n$ est un diviseur de b.

47. Si a et b sont premiers entre eux, alors

$$a \wedge (a+b) = b \wedge (a+b) = 1$$

et donc $(ab) \wedge (a+b) = 1$.
La réciproque est vraie aussi.

48. Quel que soit $n \in \mathbb{N}^*$,

$$n \wedge (n+1) = n \wedge (2n+1) = (n+1) \wedge (2n+1) = 1,$$

donc $(n^2+n) \wedge (2n+1) = 1$.

49. Pour tout entier n, les entiers $(n+1)$ et $(3n^2+2n)$ sont premiers entre eux.

50. Pour tout entier $n \in \mathbb{N}$, on pose $F_n = 2^{2^n} + 1$.

1. Soient $0 \leqslant n < n$. Pour $K = 2^{m-n}$, on a

$$(F_n - 1)^K = F_m - 1.$$

2. Comme K est pair, on en déduit qu'il existe un entier a tel que

$$a.F_n - F_m = -(-1)^K - 1 = -2.$$

Donc le pgcd de F_n et F_m divise 2.

3. Comme F_n et F_m sont impairs, ils sont premiers entre eux.

51.1 Quel que soit l'entier n, il existe un unique couple $(a_n, b_n) \in \mathbb{N}^2$ tel que

$$(1+\sqrt{2})^n = a_n + b_n\sqrt{2}.$$

51.2 On a alors

$$(1-\sqrt{2})^n = a_n - b_n\sqrt{2}$$

et on en déduit que

$$a_n^2 - 2b_n^2 = (-1)^n.$$

Par conséquent, les entiers a_n et b_n sont premiers entre eux.

IV

Mélanges

52. Soit P, un polynôme de degré $n \geqslant 1$ à coefficients dans l'anneau $\mathbb{Z}$:

$$P = a_n X^n + \cdots + a_1 X + a_0.$$

52.1 Si $x \in \mathbb{Z}$ est une racine de P, alors x divise a_0.

52.2 Si $x = {}^p/_q \in \mathbb{Q}$ (écrit sous forme irréductible) est une racine de P, alors p divise a_0 et q divise a_n.

52.3 Le polynôme $X^3 + 2X^2 + 6X - 4$ n'a donc pas de racine rationnelle.

52.4 Le polynôme

$$X^4 - X^3 - 17X^2 + 23X - 12$$

admet une racine entière :

$$(X^3 + 3X^2 - 5X + 3)(X - 4).$$

52.5 Le polynôme

$$2X^4 + 3X^3 + X^2 - 21X + 9$$

admet une racine rationnelle :

$$(X^3 + 3X^2 + 5X - 3)(2X - 3).$$

52.6 Le polynôme

$$3X^4 - 8X^3 + 7X^2 + 10X - 8$$

admet une racine rationnelle :

$$(X^3 - 2X^2 + X + 4)(3X - 2).$$

53. Pour tout $n \in \mathbb{N}$, on pose

$$u_n = (3+\sqrt{5})^n + (3-\sqrt{5})^n.$$

Alors

$$\forall\, n \in \mathbb{N}, \quad u_{n+2} - 6u_{n+1} + 4u_n = 0$$

et 2^n divise u_n pour tout $n \in \mathbb{N}$.

54. Théorème des nombres premiers
On **admet** que le nombre d'entiers premiers p inférieurs à x est équivalent, lorsque x tend vers $+\infty$, à $\frac{x}{\ell \mathrm{n}\, x}$.
Pour tout entier $n \in \mathbb{N}^*$, on note p_n, le n-ième nombre premier et on pose

$$\forall\, n \in \mathbb{N}^*, \quad d_n = p_{n+1} - p_n.$$

54.1

$$p_n \underset{n \to +\infty}{\sim} n\,\ell\mathrm{n}\, n$$

54.2

$$\sum_{1 < n \leqslant x} \frac{d_n}{\ell\mathrm{n}\, n} \underset{x \to +\infty}{\sim} x$$

54.3

$$\liminf_{n \to +\infty} \frac{d_n}{\ell\mathrm{n}\, n} \leqslant 1 \leqslant \limsup_{n \to +\infty} \frac{d_n}{\ell\mathrm{n}\, n}$$