ALG 7 | Arithmétique dans $\mathbb{Z}$

Les démonstrations ne sont pas vraiment là pour vous convaincre que quelque chose est vrai – elles sont là pour vous montrer pourquoi c'est vrai.

Andrew Mattei Gleason

Portrait de Luca Pacioli, Jacopo de Barberi

I. Divisions et congruences

1 — *Une divisibilité* f

Montrer que, pour tout $n \in \mathbb{N}^*$, 16 divise $5^n - 4n - 1$.

2 — *Réciproque d'un résultat bien connu* f

Soit $(a, b) \in \mathbb{N}^2$. Montrer que si a^2 divise b^2, alors a divise b.

3 — *Calcul d'une valuation dyadique* f

Démontrer que, pour tout entier naturel n, $\nu_2\left(5^{2^n} - 1\right) = 2^{n+2}$.

4 — *X PC-2019* ff

Soit m, $d \in \mathbb{N}*$ et $q \in \mathbb{N}$ avec $q \geqslant 2$.

1. Montrer que, si m divise d, alors $q^m - 1$ divise $q^d - 1$.
2. Étudier la réciproque.

5 — *Puissances de a modulo b* ff

Soit a et b dans $\mathbb{N}^*$ tel que $a \wedge b = 1$.

1. Pour tout $k \in \mathbb{N}$, on note r_k le reste de la division euclidienne de a^k par b. Pourquoi l'application $\phi : k \mapsto r_k$ n'est-elle pas injective sur $\mathbb{N}$?
2. En déduire l'existence d'un entier naturel n non nul tel que $a^n \equiv 1\,[b]$.

II. Nombres premiers

6 — *Petit théorème de Fermat* f

Soit p un nombre premier et $a \in \mathbb{Z}$.

1. Soit $k \in [\![1, p-1]\!]$. Exprimer $\binom{p}{k}$ en fonction de $\binom{p-1}{k-1}$ et en déduire que p divise $\binom{p}{k}$.
2. Montrer que, pour tout $(a, b) \in \mathbb{Z}^2$, $(a+b)^p = a^p + b^p\,[p]$.
3. En déduire le petit théorème de Fermat : pour tout $a \in \mathbb{Z}$, $a^p = a\,[p]$.

4. Montrer que si p est un entier distinct de 2 et 5, alors il divise un des éléments de $\{1, 11, 111, 1111, \dots\}$.

7 — *Les carrés-cubes* ***f***

Soit $n \in \mathbb{N}$. On suppose qu'il existe $(x, y) \in \mathbb{N}^2$ tels que $n = x^2$ et $n = y^3$.

Montrer qu'il existe $z \in \mathbb{N}$ tel que $n = z^6$.

8 — *Une congruence remarquable* ***ff***

Soit p un nombre premier impair et $n \in \mathbb{N}$. Établir que $(1+p)^{p^n} \equiv 1 + p^{n+1} \left[p^{n+2}\right]$.

9 — *Mersenne en plus général, X-PC 2010* ***ff***

Soit $(a, b, n) \in [\![2, +\infty[\![^3$ tels que $a^n + b^n$ soit premier. Montrer que n est une puissance de 2.

10 — *Nombres de diviseurs positifs* ***fff***

Pour tout entier n supérieur ou égal à 1, on note $d(n)$ le nombre de diviseurs positifs de n.

1. On décompose $n \in \mathbb{N} \setminus \{0, 1\}$ en produit de facteurs premiers $n = p_1^{\mu_1} \cdots p_k^{\mu_k}$. Exprimer $d(n)$ à l'aide de μ_1 , …, μ_k.

2. En déduire que d est multiplicative, c'est-à-dire $\forall (a, b) \in \left(\mathbb{N}^*\right)^2 \quad , \quad a \wedge b = 1 \implies d(ab) = d(a)d(b)$.

3. Montrer que n est un carré d'entier *si et seulement si* $d(n)$ est impair.

4. Montrer que le produit de tous les diviseurs de n vaut $\sqrt{n^{d(n)}}$.

5. Montrer que le nombre de $(a, b) \in \mathbb{N}^2$ tels que $a \vee b = n$ est égal à $d\left(n^2\right)$.

11 — *Valuation p-adique* ***fff***

Soit p un entier premier. Pour tout $x \in \mathbb{Z}$, on note $\nu_p(x)$ l'exposant de p dans la décomposition de x en produit de facteurs premiers. On considère $n \in \mathbb{N}^*$.

1. Soit $m \in \mathbb{N}^*$. Déterminer le nombre de multiples de m appartenant à $[\![1, n]\!]$. On utilisera la partie entière.

2. En déduire que $\nu_p(n!) = \displaystyle\sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.

3. Application 1 : montrer que l'écriture décimale de 1000! se termine par 249 zéros.

4. Application 2 : soit n et m dans $\mathbb{N}$, montrer que $\dfrac{(2n)!(2m)!}{n!m!(n+m)!} \in \mathbb{N}$.

III. Équations

12 — *Une équation diophantienne sans solution*

En travaillant modulo 5, démontrer que $15x^2 - 7y^2 = 9$ n'admet aucune solution dans $\mathbb{Z}^2$.

13 — *Une équation de congruence*

Résoudre l'équation $5x \equiv 3\,[28]$ d'inconnue $x \in \mathbb{Z}$.

14 — *Une équation à deux inconnues*

On s'intéresse à l'équation $(a \wedge b)^2 + ab = 101$ d'inconnue $(a,b) \in \mathbb{N}^2$.

Démontrer que, si $(a,b) \in \mathbb{N}^2$ est solution, alors $a \wedge b = 1$. En déduire les solutions.

15 — *Équation diophantienne d'ordre un à trois inconnues* ***f***

Résoudre dans $\mathbb{Z}^3$ l'équation $5x - 3y + 8z = 1$.

16 — *Deux systèmes d'équations* ***f***

Résoudre les systèmes

1. $\begin{cases} x \wedge y = 3 \\ x \vee y = 135 \end{cases}$; **2.** $\begin{cases} x + y = 100 \\ x \wedge y = 10 \end{cases}$.

17 — *Une équation du type $a \vee x = b$* ***f***

Résoudre l'équation $28 \vee x = 140$ d'inconnue $x \in \mathbb{N}$.

18 — *Une équation classique* ***ff***

L'objectif de l'exercice est de déterminer toutes les solutions $(a,b) \in (\mathbb{N}^*)^2$ de l'équation

$$(\mathrm{E}) : a^b = b^a$$

On propose deux méthodes : la première fondée sur l'analyse et la seconde purement arithmétique.

1. Justifier que (E) admet une infinité de solutions.

2. On note $f : \mathbb{R}_+^* \to \mathbb{R}$ la fonction définie par $\forall x > 0,\ f(x) = \dfrac{\ln x}{x}$.

a. Étudier les variations et tracer le graphe de la fonction f.

b. En déduire toutes les solutions de (E).

3. Soit $(a,b) \in (\mathbb{N}^*)^2$ une solution de (E) telle que $b > a$.

a. Soit p un nombre premier. Établir que que $\nu_p(a)b = \nu_p(b)a$.

b. En déduire que a divise b.

c. Soit n et m des entiers naturels tels que $m \geqslant 3$ et $n \geqslant 2$. Montrer que $m^{n-1} > n$.

d. En déduire que $(a,b) = (2,4)$.

19 — *Une équation diophantienne* ***ff***

Soit $(m,n) \in \mathbb{N}^2$ tels que $n(n+1)(n+2) = m^2$.

1. Montrer que $n+1$ et $(n+1)^2 - 1$ sont des carrés parfait.

2. Déterminer toutes les solutions $(m,n) \in \mathbb{N}^2$ de l'équation $n(n+1)(n+2) = m^2$.

20 — *Une équation* ***fff***

Résoudre dans $(\mathbb{N}^*)^3$ l'équation $\dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = 1$.

IV. PGCD et PPCM

21 — *Un vieil exercice de concours de 1974* ***f***

On pose $u_n = 5^n + 6^n$ pour tout $n \in \mathbb{N}$. Montrer que $\forall n \in \mathbb{N},\ u_{n+1} \wedge u_n = 1$.

22 — *Une identité sur les pgcd* ***f***

Montrer que, pour tout $(a,b) \in \mathbb{N}^2$ et $n \in \mathbb{N}$, on a $a^n \wedge b^n = (a \wedge b)^n$.

23 — *Arithmétique et racines de l'unité* ***ff***

Montrer que, pour tout $(a,b) \in (\mathbb{N}^*)^2$, on a $\mathbb{U}_a \cap \mathbb{U}_b = \mathbb{U}_{a \wedge b}$.

24 — *Générateurs de $\mathbb{U}_n$* *ff*

Soit $n \in \mathbb{N}^*$, $k \in [\![1, n]\!]$ et $\omega := e^{\frac{2ki\pi}{n}}$. Démontrer que $\mathbb{U}_n = \{\omega^\ell ; \ell \in \mathbb{Z}\}$ *si et seulement si* $k \wedge n = 1$.

25 — *Nombres de Fermat* *ff*

Pour tout $n \in \mathbb{N}$, on note $F_n = 2^{2^n} + 1$ (n-ième nombre de Fermat).

1. Établir que, pour tout $n \in \mathbb{N}$, $\prod_{k=0}^{n} F_k = F_{n+1} - 2$.

2. En déduire que $F_m \wedge F_n = 1$ pour tout $(n, m) \in \mathbb{N}$ tel que $n \neq m$.

26 — *Nombres de Fibonacci* *fff*

On considère la suite (F_n) définie par ses premiers termes $F_0 = 0$ et $F_1 = 1$ et par la relation de récurrence $F_{n+2} = F_n + F_{n+1}$ pour $n \in \mathbb{N}$.

1. Montrer que $\forall n \in \mathbb{N}^*$, $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$. En déduire que, $\forall n \in \mathbb{N}$, $F_n \wedge F_{n+1} = 1$.

2. Montrer que pour tout couple $(n, p) \in \mathbb{N} \times \mathbb{N}^*$, $F_{n+p} = F_p F_{n+1} + F_{p-1}F_n$.

3. En déduire que $F_n \wedge F_p = F_{n+p} \wedge F_p$.

4. Démontrer que pour tout $(m, n) \in \mathbb{N}^2$, $F_m \wedge F_n = F_{m \wedge n}$.

V. Problèmes

27 — *Lemme de Hensel et carrés modulo p^n où $p \in \mathbb{P}$*

⇛ On note $\mathbb{Z}[X]$ l'ensemble des fonctions polynomiales de $\mathbb{R}$ dans $\mathbb{R}$ à coefficients dans $\mathbb{Z}$, i.e. des fonctions de la forme :

$$x \mapsto \sum_{i=0}^{n} a_i x^i \quad \text{où } n \in \mathbb{N} \text{ et } (a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$$

On remarquera que pour tout $P \in \mathbb{Z}[X]$, P' appartient aussi à $\mathbb{Z}[X]$.

⇛ On note $\mathbb{Z}[X, Y]$ l'ensemble des fonctions polynomiales de $\mathbb{R}^2$ dans $\mathbb{R}$ à coefficients dans $\mathbb{Z}$, i.e. des fonctions de la forme :

$$(x, y) \mapsto \sum_{0 \leqslant i,j \leqslant n} a_{i,j} x^i y^j \quad \text{où } n \in \mathbb{N} \text{ et } \forall (i, j) \in [\![0, n]\!]^2,\ a_{i,j} \in \mathbb{Z}$$

⇛ Soit $\ell \in \mathbb{N}$ et $x \in \mathbb{Z}$. On dit que x est inversible modulo ℓ s'il existe y dans $\mathbb{Z}$ tel que

$$xy \equiv 1\,[\ell]$$

Un tel nombre y est appelé un inverse de x modulo ℓ.

Partie I – Préliminaires sur $\mathbb{Z}[X]$ et l'inversion modulaire

Dans cette partie, on fixe un élément ℓ de $\mathbb{N}$ et P dans $\mathbb{Z}[X]$.

1. **a.** Démontrer l'existence de $Q \in \mathbb{Z}[X,Y]$ tel que

$$\forall (x,y) \in \mathbb{R}^2,\ P(x) - P(y) = (x-y)Q(x,y)$$

b. Démontrer que, pour tout $(x,y) \in \mathbb{Z}^2$, $x \equiv y\,[\ell] \implies P(x) \equiv P(y)\,[\ell]$.

c. Démontrer l'existence de $R \in \mathbb{Z}[X,Y]$ tel que

$$\forall (x,y) \in \mathbb{R}^2,\ P(x+y) = P(x) + P'(x)y + y^2 R(x,y)$$

INDICATION : Commencer par établir le résultat dans le cas où P est monomiale.

2. Soit $a \in \mathbb{Z}$.

a. Justifier que a est inversible modulo ℓ *si et seulement si* $a \wedge \ell = 1$.

b. On suppose que a est inversible modulo ℓ et on note α l'un de ses inverses modulo ℓ.

Vérifier que, pour tous x et y dans $\mathbb{Z}$, $ax \equiv y\,[\ell] \iff x \equiv \alpha y\,[\ell]$.

Partie II – Lemme de Hensel et technique de remontée modulaire

Dans cette partie, on fixe un élément ℓ de $\mathbb{N}$. On commence par étudier le cas particulier d'une équation affine (question 1.) avant de passer au cas général (question 2.).

1. Soit $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}$ tel que $a \wedge \ell = 1$ et α un inverse de a modulo ℓ.

a. Déterminer en fonction de b et α un entier relatif x_1 vérifiant $ax_1 + b \equiv 0\,[\ell]$.

b. Pour tout $n \in \mathbb{N}^*$, on pose $x_{n+1} := (1-\alpha a)x_n - \alpha b$.

Démontrer que, pour tout $n \in \mathbb{N}^*$, x_n vérifie $ax_n + b \equiv 0\left[\ell^n\right]$.

c. Expliciter x_n en fonction de $n \in \mathbb{N}^*$, α, a et b.

d. Application numérique. Résoudre dans $\mathbb{Z}$ l'équation $2x + 5 \equiv 0\left[3^3\right]$.

2. Dans cette question, on fixe $P \in \mathbb{Z}[X]$.

a. Soit $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$ tel que $P(x) \equiv 0\left[\ell^n\right]$ et $P'(x) \wedge \ell = 1$. On fixe un inverse α de $P'(x)$ modulo ℓ.

Trouver une solution de l'équation $P(z) \equiv 0\left[\ell^{n+1}\right]$ de la forme

$$z := x + \lambda P(x) \quad \text{où } \lambda \in \mathbb{Z}$$

INDICATION : Exploiter le I.1.c.

b. Soit $x_1 \in \mathbb{Z}$ tel que $P'(x_1) \wedge \ell = 1$ et $P(x_1) \equiv 0\,[\ell]$.

Justifier l'existence d'une suite $(x_n)_{n \geqslant 1}$ d'entiers relatifs telle que

$$\forall n \in \mathbb{N}^*,\ P(x_n) \equiv 0\left[\ell^n\right] \quad \text{et} \quad x_{n+1} \equiv x_n\left[\ell^n\right]$$

3. Application numérique. Résoudre $x^2 \equiv -1\,[125]$.

INDICATION : Commencer par déterminer une solution particulière avant de toutes les trouver.

Partie III – Dénombrement des carrés modulo p^n où $p \in \mathbb{P}$ est impair

Dans cette partie, on fixe un nombre premier p impair.

Pour $(a,\ell) \in \mathbb{Z}^2$, on dit que a est un carré modulo ℓ si il existe x dans $\mathbb{Z}$ tel que $x^2 \equiv a\,[\ell]$. Autrement dit et pour faire le lien avec la partie II :

a est un carré modulo $\ell \iff$ l'équation $x^2 - a \equiv 0\,[\ell]$ d'inconnue $x \in \mathbb{Z}$ admet au moins une solution

Pour tout $n \in \mathbb{N}$, on note

$$\mathscr{C}_n := \left\{ a \in [\![0, p^n - 1]\!] \,;\, a \text{ est un carré modulo } p^n \right\} \quad \text{et} \quad u_n := \left|\mathscr{C}_n\right|$$

Par exemple, dans le cas où $p = 3$, $u_0 = 1$ et l'on déduit des tableaux de congruences suivants que $u_1 = 2$ et $u_2 = 4$:

x	0	1	2
x^2	0	1	1

(modulo 3)

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1

(modulo 9)

On revient désormais au cas général.

1. Pour tous x et y dans $[\![0, p-1]\!]$, on note $x \mathscr{R} y$ si $x^2 \equiv y^2\,[p]$.

a. Vérifier que $\mathscr{R}$ est une relation d'équivalence sur $[\![0, p-1]\!]$.

b. Soit $x \in [\![0, p-1]\!]$. Déterminer la classe d'équivalence de x ainsi que son cardinal.

c. En déduire que $u_1 = \dfrac{p+1}{2}$.

2. Dans cette question, on cherche à expliciter u_n en fonction de p et n pour tout entier naturel n non nul.

a. Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ tel que $a \wedge p = 1$.

Déduire de II.2.b. que a est un carré modulo p *si et seulement si* a est un carré modulo p^n.

b. Démontrer que

$$\mathscr{C}_n \setminus p\mathbb{N} = \left\{ a + kp \,;\, (a,k) \in \mathscr{C}_1^* \times [\![0, p^{n-1} - 1]\!] \right\} \text{ où } \mathscr{C}_1^* := \mathscr{C}_1 \setminus \{0\}$$

c. Démontrer que, pour tout entier naturel n supérieur ou égal à 2, on a $p\mathbb{N} \cap \mathscr{C}_n = \left\{ kp^2 \,;\, k \in \mathscr{C}_{n-2} \right\}$.

d. En déduire que, pour tout entier naturel n tel que $n \geqslant 2$

$$u_n = \frac{p-1}{2}\, p^{n-1} + u_{n-2}$$

puis expliciter u_n en fonction de p et n pour tout entier naturel n non nul.

Partie IV – Carrés modulo 2^n

Dans cette partie $p := 2$ et nous reprenons les notations $\mathscr{C}_n$ et u_n introduites à la partie III pour $n \in \mathbb{N}$.

1. Déterminer $\mathscr{C}_0$, $\mathscr{C}_1$, $\mathscr{C}_2$ et $\mathscr{C}_3$. On vérifiera que $u_0 = 1$, $u_1 = u_2 = 2$ et $u_3 = 3$.

2. Dans cette question, on fixe $a \in \mathbb{Z}$ impair, $n \in \mathbb{N}$ tel que $n \geqslant 3$ et on pose $\mathrm{P}(x) := x^2 - a$ pour tout réel x.

a. On suppose dans cette question l'existence de x dans $\mathbb{Z}$ tel que $\mathrm{P}(x) \equiv 0 \left[2^n\right]$.

Démontrer que x est impair et en déduire que l'équation $\mathrm{P}(z) \equiv 0 \left[2^{n+1}\right]$ admet une solution $z \in \mathbb{Z}$.

INDICATION : On recherchera z sous la forme $z := x + \lambda 2^{n-1}$ avec $\lambda \in \mathbb{Z}$.

b. En déduire que a est un carré modulo 2^n *si et seulement si* a est un carré modulo 8.

c. Établir que $\mathscr{C}_n \setminus 2\mathbb{N} = \left\{1 + 8k\,;\, k \in [\![0, 2^{n-3} - 1]\!]\right\}$.

3. En déduire u_n pour tout n dans $\mathbb{N}^*$.

INDICATION : On pourra remarquer le résultat du III.2.c. reste valable dans le cas où $p = 2$.

VI. Indications

1

Poser $u_n := 5^n - 4n - 1$ pour tout n. Chercher une relation de récurrence.

2

Utiliser la caractérisation de la divisibilité via les p-valuations.

3

On peut raisonner par récurrence.

4

Pour la réciproque, on pourra partir de la division euclidienne de d par m.

5

L'application ϕ ne prend qu'un nombre fini de valeurs.

6

Revenir aux factorielles (par exemple) au 1. Le 1. suggère (peu subtilement) un angle d'attaque pour le 2.

7

INDICATION : On pourra s'intéresser aux valuations p-adiques de n.

8

Raisonner par récurrence en utilisant la formule du binôme.

9

Raisonner par contraposition. Se ramener à une expression du type $A^k + B^k$ avec k impair et factoriser.

10

On peut (par exemple) utiliser le 1. au 3.

11

On trouve $\left\lfloor \frac{n}{m} \right\rfloor$ au 1.

12

Si (x, y) est solution, alors $3y^2 \equiv 4\,[5]$. Conclure en examinant les différentes valeurs de y modulo 5.

13

Se ramener à l'équation $5x - 28y = 3$.

14

Remarquer que 101 est premier.

15

Résoudre $5X - 3y = 1 - 8z$ à $z \in \mathbb{Z}$ fixé.

16

Au 1., poser $d = x \wedge y$, $x = dx'$, $y = dy'$. En déduire un système équivalent : $x = 3x'$, $y = 3y'$, $x' \wedge y' = 1$ et $x'y' = 45$. Les solutions du (a) sont $(3,135)$, $(15,27)$, $(27,15)$ et $(135,3)$.
Même méthode au 2. : les solutions sont $(10,90)$, $(30,70)$, $(70,30)$ et $(90,10)$.

17

Utiliser (par exemple) les valuations p-adiques.

18

Au 2.a., (a,b) est solution de (E) *si et seulement si* $f(a) = f(b)$ et utiliser les variations de f pour conclure. Au 3.b., exploiter l'unicité dans la décomposition en facteurs premiers.

19

Procéder par analyse-synthèse au 3.

20

Quitte à permuter, on peut se ramener au cas où $x \leqslant y \leqslant z$. Remarquer alors que si (x,y,z) est une solution, alors x ne peut pas être « trop grand » (il reste à quantifier cela, ie trouver un entier simple a tel que $x \leqslant a$). Se lancer alors dans une disjonction de cas sur x (cas où $x = 1$, $x = 2$, …, $x = a$) afin de se ramener à une équation deux inconnues. On trouve que les solutions de composantes croissantes sont les triplets $(2,3,6)$, $(2,4,4)$, $(3,3,3)$.

21

On peut s'inspirer de l'algorithme d'Euclide : $u_{n+1} = 6u_n - 5^{n+1}$, d'où l'on tire $u_{n+1} \wedge u_n = u_n \wedge 5^{n+1}$. On conclut alors facilement.

22

Factoriser a et b par leur pgcd.

23

Une des inclusions est triviale, l'autre peut être démontrée via une relation de Bezout.

24

Utiliser le théorème de Bezout.

25

Au 2, commencez par supposer $m < n$ et remarquer grâce au 1. que $\mathrm{F}_m \wedge \mathrm{F}_n = \mathrm{F}_m \wedge 2$.

26

Récurrence au a. Récurrence sur n au b. Au c., montrer que les diviseurs communs de F_n et F_p sont les mêmes que ceux de F_{n+p} et F_p en utilisant le a. Au d., on peut supposer que $m \geqslant n$ puis effectuer (quand cela est possible) la division euclidienne de m par n : $m = nq + r$. En itérant le résultat de la question précédente, obtenir

$$\mathrm{F}_n \wedge \mathrm{F}_r = \mathrm{F}_n \wedge \mathrm{F}_{r+n} = \mathrm{F}_n \wedge \mathrm{F}_{r+2n} = \cdots = \mathrm{F}_n \wedge \mathrm{F}_{r+nq} = \mathrm{F}_n \wedge \mathrm{F}_m$$

Conclure grâce à l'algorithme d'Euclide.

27

Utiliser la factorisation de $x^i - y^i$ par $x - y$ au I.1.a.