Chapitre 1

Arithmétique modulaire

Au fond, en mathématiques, tout sort de l'itération obstinée et stupide de l'opérateur $n \mapsto n+1$

René Thom (Médaille Fields 1958).

La mathématique est la reine des sciences, mais la théorie des nombres est la reine des sciences mathématiques.

Carl-Friedrich Gauss (1777-1855).

I Introduction hors-programme

L'arithmétique est l'étude des **nombres entiers**, qui progressivement s'est généralisée pour devenir l'étude des *anneaux* et de leurs *idéaux*. De nos jours, des constructions rigoureuses des entiers ont été proposées, par exemple en utilisant les axiomes de Peano :

Axiomes de Peano, 1889 pour $\mathbf{N}$ (HP) :
Il existe un ensemble $\mathbf{N}$ dont les éléments sont appelés les entiers naturels, un élément $0 \in \mathbf{N}$ appelé zéro et une application $s : \mathbf{N} \to \mathbf{N}$, dite application successeur, vérifiant les propriétés suivantes :

- 0 n'est le successeur d'aucun entier ;
- deux nombres entiers qui ont le même successeur sont égaux ;
- si une partie A de $\mathbf{N}$ contient 0 et est stable par s alors $A = \mathbf{N}$ (Principe de récurrence).

À partir de ces axiomes, on peut définir sur $\mathbf{N}$ une addition ($+$) et une multiplication ($\times$), qui coïncident avec l'idée naturelle que vous en avez. On définit ensuite une relation d'ordre ($\leqslant$), et cela permet d'ordonner tous les entiers naturels, comme vous les connaissez. De toute cette construction très formelle, il faut seulement retenir le théorème qu'on admettra et qui nous sera utile pour définir la division euclidienne :

Théorème 1.1 (HP, admis) — $\mathbf{N}$ *est* ***bien ordonné****, c'est-à-dire que toute partie non vide de* $\mathbf{N}$ *admet un plus petit élément.*

Une fois tout cela défini... On finit par construire $\mathbf{Z}$ en "ajoutant" les entiers négatifs aux positifs.

II Divisibilité

Définition 1 (Divisibilité) — Soient a et b deux entiers relatifs. On dit que a **divise** b lorsqu'il existe un entier k tel que $b = ka$.
Dans ce cas, on note $a|b$ et on dit de manière équivalente :
- a est un **diviseur** de b ;
- b est un **multiple** de a.

L'ensemble des **multiples de** a est noté $a\mathbf{Z}$.

☞ **Exemple 1**

1) 3 divise 36 car $36 = 3 \times 12$. On peut remarquer qu'on en déduit également que 12 divise 36. Les diviseurs fonctionnent par paire. L'ensemble des diviseurs de 36 est

$$D(36) = \{-36, -18, -12, -9, -4, -3, -2, -1, 1, 2, 3, 4, 9, 12, 18, 36\}.$$

2) 1 et -1 sont des diviseurs de tout entier a car $a = 1 \times a = (-1) \times (-a)$. De même, pour tout entier a, a et $-a$ divisent a.

3) Tout entier a divise 0 car $0 = a \times 0$. En revanche, 0 ne divise que 0.

Proposition 1.2 — *Si a et b sont des entiers relatifs, on a les équivalences suivantes :*

$$a|b \quad \Leftrightarrow \quad -a|b \quad \Leftrightarrow \quad -a|-b \quad \Leftrightarrow \quad a|-b.$$

Proposition 1.3 — *Soit a et b deux entiers, si $a|b$ et si $b \neq 0$ alors $|a| \leqslant |b|$.*

Proposition 1.4 (Ensemble fini de diviseurs) — *Par corollaire, tout entier relatif n non nul possède un nombre fini de diviseurs, qui sont compris entre $-|n|$ et $|n|$.*

Proposition 1.5 — *Soient a et b deux entiers. Si $a|b$ et $b|a$, alors $|a| = |b|$.*
En particulier, si a et b sont deux entiers ***naturels*** *tels que $a|b$ et $b|a$, alors $a = b$.*

Proposition 1.6 (Transitivité) — *Soient a, b et c trois entiers. Si $a|b$ et $b|c$, alors $a|c$.*

Proposition 1.7 (Combinaison linéaires) — *Soient a, b et c trois entiers. Si $a|b$ et $a|c$ alors pour tous entiers u et v, $a|ub+vc$.*

III Division euclidienne

La structure de l'ensemble des entiers $\mathbf{Z}$ est donnée en grande partie par le fait que muni des opérations usuelles $+$ et $\times$, il est ce qu'on appelle un **anneau euclidien**, autrement dit, il existe une **division euclidienne** :

Théorème 1.8 (Division euclidienne sur Z) — *Si $(a,b) \in \mathbf{Z} \times \mathbf{N}^*$, alors il existe un unique couple $(q,r) \in \mathbf{Z} \times \mathbf{N}$ tels que :*

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

- *a est appelé le* ***dividende****;*
- *b est appelé le* ***diviseur****;*
- *q est appelé le* ***quotient****;*
- *r est appelé le* ***reste*** *de cette division euclidienne.*

Proposition 1.9 — *Si $(a,b) \in \mathbf{Z} \times \mathbf{N}^*$, alors $b|a$ si et seulement si le reste de la division euclidienne de a par b est nul.*

Proposition 1.10 — *Si b est un entier naturel supérieur à deux, alors tout entier a s'écrit sous une seule des formes suivantes où q est un entier :*

$$bq, \quad bq+1, \quad ..., \quad bq+b-1$$

☞ **Exemple 2** Soit un entier n. Montrons que $n(n^2+5)$ est divisible par 3.

1) Si $n = 3q$ alors 3 divise n donc 3 divise $n(n^2+5)$.

2) Si $n = 3q+1$ alors $n^2+5 = 3(3q^2+2q+2)$ et $3q^2+2q+2$ est un entier donc 3 divise n^2+5, donc 3 divise $n(n^2+5)$.

3) Si $n = 3q+2$ alors $n^2+5 = 3(3q^2+4q+3)$ et $3q^2+4q+3$ est un entier donc 3 divise n^2+5, donc 3 divise $n(n^2+5)$.

IV Congruences

L'idée de l'arithmétique modulaire est de raisonner sur les restes et non sur les nombres en eux-mêmes. Cela est justifié par le fait que les opérations passent aux congruences comme on le verra avec la dernière proposition.

Définition 2 (Congruences modulo m) — Soit m un entier naturel non nul et $(a,b) \in \mathbf{Z}^2$. On dit que a et b sont **congrus modulo** m et on note

$$a \equiv b \mod m \quad \text{ou} \quad a \equiv b \pmod m \quad \text{ou} \quad a \equiv b \ (m) \quad \text{ou encore} \quad a \equiv b \ [m]$$

si m **divise** $b-a$.

☞ **Exemple 3** 17 est congru à 2 modulo 3 car $17-2 = 15$ et 3 divise 15.
On a aussi $17 \equiv -1 \pmod 3$ car $17-(-1) = 18$ et 3 divise 18.

☞ **Exemple 4** Deux entiers a et b sont toujours congrus modulo 1 car 1 divise toujours $b-a$.

☞ **Exemple 5** Un entier, modulo 2 est congru à 0 (s'il est pair) ou 1 (s'il est impair).

Proposition 1.11 — *Avec les notations précédentes :*

- $a \equiv b \mod m$ *si et seulement a et b ont même reste dans leur division par m ;*
- $a \equiv 0 \mod m$ *si et seulement si m divise a.*

Proposition 1.12 (La congruence est une *relation d'équivalence*) — *Si a, b et c sont des entiers et m est un entier naturel non nul, alors :*

1) $a \equiv a \mod m$ *(la congruence est réflexive);*

2) *si* $a \equiv b \mod m$ *alors* $b \equiv a \mod m$ *(la congruence est symétrique);*

3) *si* $a \equiv b \mod m$ *et* $b \equiv c \mod m$*, alors* $a \equiv c \mod m$ *(la congruence est transitive);*

Proposition 1.13 (Compatibilité avec les opérations) — *Si a, b, a' et b' sont des entiers tels que* $a \equiv b \mod m$ *et* $a' \equiv b' \mod m$ *où m est un entier naturel non nul, alors :*

1) $a + a' \equiv b + b' \mod m$

2) $a - a' \equiv b - b' \mod m$

3) $aa' \equiv bb' \mod m$

4) *Si* $n \in \mathbf{N}^*$, $a^n \equiv b^n \mod m$.

Remarque importante : attention, cela ne fonctionne pas avec la division : $63 \equiv 45 \mod 3$ mais on n'a pas $7 \equiv 5 \mod 3$!

Définition 3 — m étant un entier naturel non nul, un entier a est dit **inversible modulo** m s'il existe un entier b tel que $ab \equiv 1 \mod m$.

V Exercices

Divisibilité

♦ **AM.1** Compléter par les mots *multiple* ou *diviseur* :

- 250 est un ... de 50 ;
- 37 est un ... de 0 ;
- 0 est un ... de 12 ;
- -4 est un ... de 4 ;

♦ **AM.2** (**Premières méthodes**)

1) Donner la liste des diviseurs de 15.

2) Déterminer l'ensemble des entiers naturels n tels que $2n+3$ divise 15.

♦ **AM.3** Déterminer l'ensemble des entiers naturels n tels que 15 divise $n+22$.

♦ **AM.4** Déterminer l'ensemble des entiers naturels n tels que $n+15$ divise $2n+3$.

♦ **AM.5** Déterminer l'ensemble des entiers relatifs n tels que $4n+1$ divise 13.

♦ **AM.6** Déterminer l'ensemble des entiers relatifs n tels que 13 divise $n+2$.

♦ **AM.7** Déterminer l'ensemble des entiers relatifs n tels que $n+2$ divise $4n+1$.

♦ **AM.8** Résoudre les équations suivantes dans $\mathbf{N}$:

- $x^2+y^2=5$;
- $x^2-y^2=12$;
- $x^2-y^2=-15$;
- $x+y=2xy$.

☞ **Indications exercice 8 :** Pour le dernier, distinguer les cas $x=y$, $x>y$ et $y>x$.

♦ **AM.9** On considère dans le plan, l'hyperbole $\mathcal{H}$ d'équation $y=\dfrac{12}{x}$.

Combien de points à coordonnées entières possède $\mathcal{H}$?

Division euclidienne

♦ **AM.10** Démontrer que pour tout entier naturel n,

$$2n(n+1)(n+2)$$

est divisible par 3.

♦ **AM.11** On a $337=27\times12+13$.

1) Donner le reste de la division euclidienne de 337 par 27.

2) Donner le reste de la division euclidienne de 337 par 12.

3) Déterminer le quotient et le reste de la division euclidienne de -337 par 12.

♦ **AM.12** Montrer que si $n\in\mathbf{N}$, $n(n+1)$ est un nombre pair, puis en déduire que $3n^2+3n$ est un multiple de 6.

♦ **AM.13** Dans chaque cas, déterminer le reste r dans la division euclidienne de A par B :

1) $A=1789$ et $B=14$;

2) $A=-2025$ et $B=11$;

3) $A=n^2+2n+3$ et $B=n+1$ où $n\in\mathbf{N}$;

4) $A=5n+1$ et $B=2n+1$ où $n\in\mathbf{N}$.

♦ **AM.14** On considère la suite (u_n) définie par :

$$\begin{cases} u_0=7 \\ u_{n+1}=3u_n+14 \quad \text{pour tout entier naturel } n. \end{cases}$$

On admet que pour tout entier naturel n, $u_n\in\mathbf{N}$.

1) Montrer par récurrence que pour tout entier naturel n, u_n est un multiple de 7.

2) Montrer par récurrence que pour tout entier naturel n, u_n est impair.

3) On considère la suite v où pour tout entier naturel n, $v_n=u_n+7$.

a) Montrer que (v_n) est géométrique.

b) En déduire u_n en fonction de n.

c) En déduire, suivant les valeurs de n, le reste de la division euclidienne de u_n par 9.

♦ **AM.15** (**Nombres amicaux**) Les nombres amicaux vont par deux : ce sont des entiers naturels où chacun est égal à la somme des diviseurs positifs stricts de l'autre.

1) Vérifier que 220 est l'ami d'un autre nombre.

2) Vérifier que 496 est son propre ami.

3) Écrire un programme permettant de déterminer tous les nombres amicaux inférieurs à 2000.

♦ **AM.16** On choisit un entier s'écrivant avec quatre chiffres, et on l'écrit à l'envers, puis on ajoute les deux nombres obtenus.

1) Essayer avec 7892.

2) Obtient-on toujours un multiple de 11 ?

♦ **AM.17** Quel est le chiffre des dizaines du carré d'un entier ayant pour chiffre des unités 5 ?

♦ **AM.18** (*)

1) Soit $m\in\mathbf{Z}$. Montrer que si 3 divise $4m$ alors 3 divise m.

2) Déterminer les racines du polynôme X^2-6X+4, qu'on note r_1 et r_2 (où $r_1 < r_2$).

3) On pose, pour tout entier naturel n, $u_n = r_1^n + r_2^n$.

a) Calculer u_0, u_1 et u_2.

b) Montrer que pour tout entier naturel n, on a :

$$u_{n+2} = 6u_{n+1} - 4u_n.$$

c) Démontrer par récurrence que pour tout entier naturel n, u_n est entier.

d) Démontrer que pour tout entier naturel n, 2^n divise u_n.

4) On pose pour tout entier naturel n, $v_n = u_{2n}$ et $w_n = u_{2n+1}$.

a) Démontrer par récurrence que pour tout entier naturel n, w_n est un multiple de 3.

b) Montrer que pour tout entier naturel n non nul, si 3 divise v_n alors 3 divise v_{n-1}.

c) En déduire que pour tout entier naturel n, v_n n'est pas un multiple de 3.

5) Existe-t-il un entier naturel n tel que 5 divise u_n ?

♦ **AM.19** Soit n un entier naturel impair. La somme de n entiers consécutifs est-elle toujours divisible par n ?

Congruences

*Les exercices **AM.20** à **AM.24** sont là pour vous apprendre les méthodes de base qui servent dans la plupart des autres exercices.*

♦ **AM.20** Démontrer que, pour tout entier naturel n, $10^n - 1$ est divisible par 9.

♦ **AM.21** Démontrer que, pour tout $n \in \mathbf{N}$, $n(n^2+5)$ est divisible par 3 en utilisant le tableau des restes modulo 3 :

Reste de n modulo 3	0	1	2
Reste de n^2+5 modulo 3			
Reste de $n(n^2+5)$ modulo 3			

♦ **AM.22** Déterminer l'ensemble des entiers x tels que $2x \equiv 4 \pmod 5$ en utilisant un tableau des restes modulo 5.

♦ **AM.23** Étudier les restes possibles pour un carré modulo 8 en complétant le tableau ci-dessous et en déduire que l'équation $x^2 - 5y^2 = 2014$ n'admet pas de solution dans $\mathbf{Z}^2$.

Reste de x modulo 8	0	1	...	7
Reste de x^2 modulo 3				

♦ **AM.24** Déterminer le chiffre des unités de $N = 2025^{2026}$ en remarquant que ce chiffre est le reste de la division de N par 10 et que $N \equiv 3 \pmod 1 0$, puis que $2014 = 4 \times 503 + 2$.

Remarque 1 Ce qu'il faut surtout retenir, c'est qu'on a écrit la division euclidienne de 2014 par 4 parce que $3^4 \equiv 1 \pmod{10}$ (et ça, il faut parfois le cherche seul).

♦ **AM.25** Soit $n \in \mathbf{N}$.

1) Démontrer que $3^{2n} \equiv 2^n \pmod 7$ et que $2^{4n} \equiv 2^n \pmod 7$.

2) En déduire que 7 divise $3^{2n+1} + 2^{4n+2}$.

♦ **AM.26** Déterminer le reste de la division euclidienne de $2016 \times 2017 \times ... \times 2026$ par 11.

♦ **AM.27** Déterminer les solutions (dans $\mathbf{Z}$) de l'équation :

$$3x \equiv 0 \pmod 8.$$

♦ **AM.28** En raisonnant modulo 4, démontrer que l'équation :

$$7x^2 - 4y^2 = 1$$

n'admet pas de solutions entières.

♦ **AM.29** Soient a et b deux entiers. Démontrer que si $7|a^2+b^2$, alors $7|a$ et $7|b$.

♦ **AM.30** Montrer que pour tout entier naturel n, $7^{2n+1} + 6^{2n+1}$ est divisible par 13.

♦ **AM.31**

1) Démontrer que pour tout $n \in \mathbf{N}$, $9^n - 2^n$ est divisible par 7.

2) Déterminer, pour tout entier naturel n, un diviseur commun aux nombres $2^{3n} - 3^n$.

♦ **AM.32** (**Critères de divisibilité**) En utilisant le fait qu'un nombre entier s'écrive comme somme de puissances de 10 (par exemple $358 = 3 \times 10^2 + 5 \times 10^1 + 8$), démontrer les critères de divisibilité suivants :

1) Un nombre entier est divisible par 2 si et seulement si son chiffre des unités est divisible par 2 ;

2) un nombre entier est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3 ;

3) un nombre entier est divisible par 5 si et seulement si son chiffre des unités est 0 ou 5 ;

Déterminer un critère de divisibilité par 9, puis par 11.

♦ **AM.33** (**Irrationalité de $\sqrt{3}$**) En raisonnant sur les congruences modulo 5 de a^2 et $3b^2$, démontrer qu'il n'existe pas d'entiers a et b tels que $\sqrt{3} = \frac{a}{b}$ (en supposant la fraction irréductible).

♦ **AM.34** (**Irrationalité de $\sqrt{2}+\sqrt{3}$, ***)

1) Démontrer par l'absurde que $\sqrt{6}$ est irrationnel.

☞ **Indications exercice 34 :** On pourra résonner sur les restes de p^2 et $6q^2$ modulo 7.

2) Démontrer que si un nombre x est rationnel, alors x^2 est rationnel.

3) En déduire par l'absurde que $\sqrt{2}+\sqrt{3}$ est irrationnel.

♦ **AM.35** Existe-t-il des entiers naturels n tels que 9 divise $7^n - n^6$?

♦ **AM.36** (*) Soit p un nombre premier supérieur à 7. Démontrer que 24 divise p^2-1.

☞ **Indications exercice 36 :** On pourra commencer par justifier que 2 divise $p-1$ et $p+1$, puis raisonner modulo 4 et modulo 3.

♦ **AM.37** Soit $a \in \mathbf{Z}$. Résoudre dans $\mathbf{N}^3$ l'équation

$$x^2+y^2=(4a+3)z^2,$$

d'inconnue (x,y,z).

♦ **AM.38** On pose $A = 7^{7^{7^7}}$.

1) Déterminer le reste modulo 10 de 7^n où $n \in \mathbf{N}$.

2) Déterminer le reste de 7^m modulo 4 en fonction de la parité de m.

3) Quelle est la parité de 7^{7^7} ?

4) En déduire le chiffre des unités dans l'écriture décimale de A.

♦ **AM.39** On considère l'équation $(E) : x^4+y^4=4^n$ d'inconnue $(x,y,n) \in \mathbf{N}^3$.
Le but de l'exercice est de démontrer que si $(x,y,n) \in \mathbf{N}^3$ est une solution de (E) alors $x=0$ ou $y=0$.

1) Déterminer les solutions de (E) de la forme $(x,y,0)$.

2) Soit $(x,y,n) \in \mathbf{N}^3$ est solution de (E) telle que $n \neq 0$. On suppose que $x \neq 0$ et $y \neq 0$.

a) En raisonnant modulo 4, démontrer que x et y sont pairs.

b) Justifier qu'il existe un plus grand entier naturel α tel que 2^α divise x et un plus grand entier naturel β tel que 2^β divise y.

c) Justifier qu'alors, si $x=2^\alpha u$ et $y=2^\beta v$, u et v sont des entiers impairs.

d) Démontrer que $n-2\alpha \geqslant 0$ et que $u^4+4^{2(\beta-\alpha)}v^4=4^{n-2\alpha}$.

e) En raisonnant modulo 4, montrer que $n=2\alpha$.

f) Aboutir à une contradiction et conclure.

♦ **AM.40** Dans tout cet exercice, lorsqu'on écrit « la somme des chiffres de x » , il faut comprendre « la somme des chiffres dans l'écriture décimale de x » .

1) a) Démontrer que, pour tout entier naturel non nul n, $10^n \equiv 1 \mod 9$.

b) Soit N un entier naturel S la somme des chiffres de N. Démontrer que $N \equiv S \mod 9$.

On pose $A = 2015^{2015}$ et on note B la somme des chiffres de A, C la somme des chiffres de B et D la somme des chiffres de C.

2) Démontrer que $A \equiv 8 \mod 9$ puis que $D \equiv 8 \mod 9$.

3) a) Démontrer que A s'écrit avec au plus 8 060 chiffres et en déduire que $B \leqslant 72\,540$.

b) De la même façon, montrer que $C \leqslant 45$.

4) Déduire des questions précédentes la valeur de D.

♦ **AM.41** Le but de l'exercice est de répondre à la question suivante :

Étant donné un entier n supérieur ou égal à 2, existe-t-il trois entiers x, y et z tels que :

$$x^2+y^2+z^2 \equiv 2^n-1 \mod 2^n \quad ?$$

Partie A - Cas particuliers

1) Dans cette question, on suppose que $n=2$.
Montrer que 1, 3 et 5 fournissent une solution au problème.

2) Dans cette question, on suppose que $n=3$.

a) Soit m un entier naturel.
Dresser un tableau donnant les restes possibles de m et m^2 modulo 8.

b) Peut-on trouver trois entiers naturels x, y et z tels que $x^2+y^2+z^2 \equiv 7 \mod 8$?

Partie B - Cas général $n \geqslant 3$

Supposons qu'il existe trois entiers naturels x, y et z tels que $x^2+y^2+z^2 \equiv 2^n-1 \mod 2^n$.

1) Justifier que l'on est dans l'un des deux cas suivants :

- Ou bien x, y et z sont tous les trois impairs ;
- ou bien exactement deux des trois entiers x, y et z sont pairs.

2) On suppose dans cette question que x et y sont tous les deux pairs et que z est impair.

a) Montrer que $x^2+y^2+z^2 \equiv 1 \mod 4$.

b) En déduire une contradiction.

3) On suppose dans cette question que x, y et z sont tous les trois impairs.

a) Démontrer que, pour tout entier naturel k, l'entier k^2+k est pair.

b) En déduire que $x^2+y^2+z^2 \equiv 3 \mod 8$.

c) Conclure en s'inspirant de la question 2.b.

4) Quelle réponse peut-on apporter à la question posée en préambule ?