

## Arithmétique, Groupes et Anneaux

JUSQU'AU début du vingtième siècle, l'algèbre désignait essentiellement l'étude de la résolution d'équations algébriques (en témoigne la dénomination du *théorème fondamental de l'algèbre*). Avec la résolution des équations algébriques apparut, de manière plus ou moins confuse, la notion de nombre complexe : on utilisa le symbole  $\sqrt{-1}$ . Parallèlement, la théorie des congruences se développa.

Ainsi, de nouveaux objets mathématiques entrèrent en scène. Bientôt, les mathématiciens y virent des analogies étroites qu'ils cherchèrent à expliquer : l'algèbre devint progressivement l'étude abstraite des structures algébriques, jusqu'à ce que connaît l'étudiant d'aujourd'hui.

### 1. Arithmétique sur les entiers

Nous supposons acquises les notions de base sur l'ensemble des entiers naturels  $\mathbb{N}$  et des entiers relatifs  $\mathbb{Z}$ , ainsi que les calculs dans l'anneau quotient  $\mathbb{Z}/n\mathbb{Z}$ . Une étude plus approfondie de ce dernier fait l'objet de la section 3 de ce chapitre.

#### 1.1. Divisibilité - pgcd, ppcm

DÉFINITION 1. Soient  $a$  et  $b$  deux entiers relatifs. On dit que  $a$  *divise*  $b$  (ou que  $b$  est un *multiple* de  $a$ ), et on note  $a \mid b$ , s'il existe un entier  $n$  tel que  $b = an$ . Si  $a$  ne divise pas  $b$ , on note  $a \nmid b$ .

PROPOSITION 1 (DIVISION EUCLIDIENNE). Soient  $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ . Il existe un unique couple  $(q, r) \in \mathbb{Z} \times \mathbb{N}$  tel que

$$a = bq + r, \quad \text{avec } 0 \leq r < b.$$

$q$  s'appelle le quotient,  $r$  le reste, de la division euclidienne de  $a$  par  $b$ .

#### Classes de congruence modulo $n$ .

DÉFINITION 2. Soit  $n$  un entier naturel non nul. On note  $n\mathbb{Z} = \{nk, k \in \mathbb{Z}\}$ . Si  $x$  et  $y$  sont deux entiers, on note  $x \equiv y \pmod{n}$  si  $x - y \in n\mathbb{Z}$ . et on dit alors que  $x$  et  $y$  sont *congrus modulo*  $n$ .

DÉFINITION 3. Soit  $n$  un entier naturel non nul. L'anneau quotient de  $\mathbb{Z}$  par  $n\mathbb{Z}$  est noté  $\mathbb{Z}/n\mathbb{Z}$ . On note généralement  $\bar{x}$  (ou  $\dot{x}$ ) la classe d'un entier  $x$  dans  $\mathbb{Z}/n\mathbb{Z}$ . Ainsi,  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ .

#### PGCD.

DÉFINITION 4. – Soient  $a_1, \dots, a_n$  des entiers. Il existe un unique entier naturel  $d$  tel que  $a_1\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$ . Ainsi défini,  $d$  s'appelle le *pgcd* de  $a_1, \dots, a_n$  et on note  $d = \text{pgcd}(a_1, \dots, a_n)$ . L'entier  $d$  est aussi le plus grand entier naturel divisant tous les  $a_i$  ( $1 \leq i \leq n$ ).

– Lorsque  $\text{pgcd}(a_1, \dots, a_n) = 1$ , on dit que les entiers  $a_1, \dots, a_n$  sont premiers entre eux *dans leur ensemble*. Lorsque  $\text{pgcd}(a_i, a_j) = 1$  dès que  $i \neq j$ , les entiers  $a_i$  sont dits premiers entre eux *deux à deux*.

*Remarque 1.* – Des entiers premiers entre eux deux à deux sont premiers entre eux dans leur ensemble.

– Il résulte de la définition du pgcd que les diviseurs communs à une famille d'entiers sont les diviseurs du pgcd.

– Lorsque  $a_1, \dots, a_n$  sont des entiers, on a

$$\forall a \in \mathbb{Z}, \quad \text{pgcd}(aa_1, \dots, aa_n) = |a| \text{pgcd}(a_1, \dots, a_n).$$

– Le pgcd de deux entiers  $a$  et  $b$  se note aussi  $a \wedge b$ .

→ THÉORÈME 1 (BEZOUT). *Des entiers  $a_1, \dots, a_n$  sont premiers entre eux dans leur ensemble si et seulement s'il existe des entiers  $u_1, \dots, u_n$  tels que  $u_1 a_1 + \dots + u_n a_n = 1$ .*

*Remarque 2.* Lorsque deux entiers  $a$  et  $b$  sont premiers entre eux, le théorème de Bezout assure l'existence d'un couple  $(u, v) \in \mathbb{Z}^2$  tel que  $au + bv = 1$ . Il existe un moyen pratique de calculer un tel couple  $(u, v)$ , appelé algorithme d'Euclide (voir l'exercice 2).

→ THÉORÈME 2 (GAUSS). *Soient  $a, b$  et  $c$  trois entiers. Si  $a$  divise le produit  $bc$  et si  $a$  et  $b$  sont premiers entre eux, alors  $a$  divise  $c$ .*

PROPOSITION 2. *Si un entier  $a$  est premier avec des entiers  $b_1, \dots, b_n$ , alors  $a$  est premier avec le produit  $b_1 \dots b_n$ .*

PROPOSITION 3. *Soient  $a_1, \dots, a_n$   $n$  entiers premiers entre eux deux à deux et  $b$  un entier. Le produit  $a_1 \dots a_n$  divise  $b$  si et seulement si pour tout  $i$ ,  $a_i$  divise  $b$ .*

### PPCM.

DÉFINITION 5. Soient  $a_1, \dots, a_n$  des entiers. Il existe un unique entier naturel  $d$  tel que  $a_1 \mathbb{Z} \cap \dots \cap a_n \mathbb{Z} = d \mathbb{Z}$ . Ainsi défini,  $d$  s'appelle le *ppcm* de  $a_1, \dots, a_n$  et on note  $d = \text{ppcm}(a_1, \dots, a_n)$ . L'entier  $d$  est aussi le plus petit entier naturel non nul multiple de tous les  $a_i$  ( $1 \leq i \leq n$ ).

*Remarque 3.* – Il résulte de cette définition que les multiples communs à une famille d'entiers sont les multiples de leur ppcm.

– On a facilement

$$\forall a \in \mathbb{Z}, \quad \text{ppcm}(aa_1, \dots, aa_n) = |a| \text{ppcm}(a_1, \dots, a_n).$$

– Le ppcm de deux entiers  $a$  et  $b$  se note aussi  $a \vee b$ .

PROPOSITION 4. *Soient  $a_1, \dots, a_n$  des entiers premiers entre eux deux à deux. Alors*

$$\text{ppcm}(a_1, \dots, a_n) = |a_1 \dots a_n|.$$

PROPOSITION 5. *Pour deux entiers  $a$  et  $b$ , on a  $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$ .*

## 1.2. Nombres premiers

DÉFINITION 6. On dit qu'un entier naturel  $p \geq 2$  est un *nombre premier* si ses seuls diviseurs sont  $p, -p, 1$  et  $-1$ .

→ THÉORÈME 3 (THÉORÈME FONDAMENTAL DE L'ARITHMÉTIQUE). *Tout entier naturel  $n \geq 2$  s'écrit de manière unique à l'ordre près sous la forme*

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \tag{*}$$

où les  $p_i$  sont des nombres premiers distincts et les  $\alpha_i$  des entiers naturels non nuls. La relation (\*) s'appelle la *décomposition* de  $n$  en facteurs premiers.

*Remarque 4.* – Tout entier  $n$ ,  $|n| \geq 2$ , est divisible par un nombre premier.

- Si  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  et  $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$ , où les  $p_i$  sont des nombres premiers distincts et les  $\alpha_i, \beta_i$  des entiers naturels, alors  $\text{pgcd}(n, m) = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$  et  $\text{ppcm}(n, m) = p_1^{\delta_1} \cdots p_k^{\delta_k}$  où  $\gamma_i = \inf(\alpha_i, \beta_i)$  et  $\delta_i = \sup(\alpha_i, \beta_i)$ .

PROPOSITION 6. Si un nombre premier  $p$  ne divise pas un entier  $a$ , alors  $p$  et  $a$  sont premiers entre eux.

PROPOSITION 7. Si un nombre premier divise un produit d'entiers  $a_1 \cdots a_n$ , il divise au moins l'un des facteurs  $a_i$  de ce produit.

PROPOSITION 8. L'ensemble des nombres premiers est infini.

*Démonstration.* Raisonnons par l'absurde et supposons qu'il y ait un nombre fini de nombres premiers. Soit  $N$  le plus grand d'entre eux. Posons  $M = N! + 1$  et désignons par  $p$  un nombre premier divisant  $M$ . Comme  $p \leq N$ , on a  $p \mid (N!)$ , donc  $p \mid (M - N!) = 1$ , ce qui est absurde.  $\square$

PROPOSITION 9. Soit  $p$  un nombre premier et  $k$  un entier,  $1 \leq k \leq p - 1$ . Alors  $p \mid \binom{p}{k}$ .

PROPOSITION 10. Soit  $n \geq 2$  un entier. L'anneau  $\mathbb{Z}/n\mathbb{Z}$  est un corps si et seulement si  $n$  est premier.

→ THÉORÈME 4 (FERMAT). Soit  $p \geq 2$  un nombre premier. Alors

$$\forall a \in \mathbb{Z}, \quad a^p \equiv a \pmod{p}$$

et

$$\forall a \in \mathbb{Z}, p \nmid a, \quad a^{p-1} \equiv 1 \pmod{p}.$$

THÉORÈME 5 (WILSON). Un entier  $p \geq 2$  est un nombre premier si et seulement si

$$(p - 1)! \equiv -1 \pmod{p}.$$

*Démonstration. Condition nécessaire.* Si  $p = 2$  ou  $p = 3$ , c'est évident. Pour traiter le cas  $p > 3$ , on commence par rechercher les éléments  $x$  du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$  égaux à leur inverse. Ils vérifient  $x^2 = \bar{1}$ , c'est-à-dire  $(x - \bar{1})(x + \bar{1}) = \bar{0}$ . Les seuls éléments de  $(\mathbb{Z}/p\mathbb{Z})^*$  égaux à leurs inverses sont donc  $x = \bar{1}$  et  $x = \overline{-1}$ . On range les autres  $\bar{2}, \bar{3}, \dots, \overline{p-2}$  en  $\frac{p-3}{2}$  paires d'éléments  $\{x_i, y_i\}$  telles que  $x_i y_i = \bar{1}$ . Si  $k = \frac{p-3}{2}$ , on peut écrire

$$\bar{2} \cdot \bar{3} \cdots \overline{p-2} = \prod_{i=1}^k (x_i y_i) = \bar{1} \quad \text{donc} \quad (p-1)! \equiv -1 \pmod{p}.$$

*Condition suffisante.* Supposons  $p$  non premier, et notons  $a$  un diviseur de  $p$  vérifiant  $1 < a < p$ . On a  $a \mid [(p-1)! + 1]$  par hypothèse, et  $a \mid (p-1)!$  puisque  $1 < a < p$ , donc  $a \mid 1$  ce qui est absurde.  $\square$

### 1.3. Exercices

EXERCICE 1. Déterminer les triplets  $(a, b, c) \in (\mathbb{N}^*)^3$  tels que

$$(i) \text{ppcm}(a, b) = 42 \quad (ii) \text{pgcd}(a, c) = 3 \quad (iii) a + b + c = 29.$$

*Solution.* D'après (ii),  $3 \mid a$  et  $3 \mid c$ , donc  $3 \mid (a + c)$ . Comme  $b = 29 - (a + c)$ ,  $b$  n'est pas un multiple de 3, et 3 étant premier,  $3 \wedge b = 1$ . En utilisant (i) on a  $b \mid 42 = 3 \times 14$  et d'après le théorème de Gauss,  $b \mid 14$ . Donc  $b \in \{1, 2, 7, 14\}$ . Mais  $29 - b = a + c$  est divisible par 3, ce qui restreint les valeurs possibles de  $b$  à 2 et 14.

- Si  $b = 2$ ,  $a \in \{21, 42\}$  d'après (i). Mais  $a \leq 29$  d'après (iii), donc  $a = 21$  et  $c = 6$  avec (iii).
- Si  $b = 14$ ,  $a \in \{3, 6, 21, 42\}$  d'après (i). La relation (iii) entraîne  $a \leq 29 - b = 15$ , d'où  $a \in \{3, 6\}$ . Si  $a = 3$ ,  $c = 12$  par (iii); si  $a = 6$ ,  $c = 9$ .

Nécessairement, on a donc  $(a, b, c) = (21, 2, 6)$ ,  $(3, 14, 12)$  ou  $(6, 14, 9)$ . Réciproquement, on vérifie facilement que ces triplets sont solution.

→ EXERCICE 2. 1/ Soient  $a$  et  $b \geq 2$  deux entiers naturels non nuls premiers entre eux. Montrer que

$$\exists!(u_0, v_0) \in \mathbb{N}^2, \quad u_0 a - v_0 b = 1, \quad \text{avec } u_0 < b \text{ et } v_0 < a \quad (*)$$

et exprimer en fonction de  $u_0, v_0, a$  et  $b$  tous les couples  $(u, v) \in \mathbb{Z}^2$  solutions de  $ua - vb = 1$ .

2/ Déterminer deux entiers  $u$  et  $v$  vérifiant  $47u + 111v = 1$ .

---

*Solution.* 1/ Le théorème de Bezout assure l'existence de deux entiers  $u_1$  et  $v_1$  vérifiant  $u_1 a - v_1 b = 1$ . On effectue ensuite la division euclidienne de  $u_1$  par  $b$  :  $u_1 = bq + u_0$ , avec  $0 \leq u_0 < b$ . On obtient  $(bq + u_0)a - v_1 b = 1 = u_0 a - v_0 b$ , avec  $v_0 = v_1 - aq$ . Donc  $-1 \leq v_0 b = u_0 a - 1 < u_0 a < ba$ , et en divisant par  $b \geq 2$ , on tire  $0 \leq v_0 < a$ . Ainsi, notre couple  $(u_0, v_0)$  vérifie l'assertion (\*). Ceci étant, considérons un couple  $(u, v)$  vérifiant  $ua - vb = 1$ . En retranchant à (\*), on obtient

$$(u - u_0)a = (v - v_0)b. \quad (**)$$

Ceci montre que  $a \mid (v - v_0)b$  et comme  $a$  et  $b$  sont premiers entre eux, le théorème de Gauss entraîne  $a \mid (v - v_0)$ . Soit  $k \in \mathbb{Z}$  tel que  $v = v_0 + ka$ . En remplaçant dans (\*\*), on obtient  $(u, v) = (u_0 + kb, v_0 + ka)$ . Ceci prouve que le couple  $(u_0, v_0)$  est bien l'unique couple vérifiant la propriété (\*), et réciproquement, on vérifie facilement que les couples de cette forme sont solutions de  $ua - vb = 1$ .

2/ Les nombres 47 et 111 sont premiers entre eux,  $u$  et  $v$  existent donc. Nous allons les déterminer grâce à l'algorithme d'Euclide. On effectue d'abord la division euclidienne de 111 par 47

$$111 = 47 \times 2 + 17,$$

puis on itère en divisant toujours le dividende par le reste, jusqu'à ce que le reste égale 1 :

$$47 = 17 \times 2 + 13, \quad 17 = 13 \times 1 + 4, \quad 13 = 4 \times 3 + 1.$$

On part maintenant de  $1 = 13 - 4 \times 3$  et on remonte :

$$1 = 13 - 4 \times 3 = 13 - (17 - 13 \times 1) \times 3 = 4 \times 13 - 3 \times 17 = 4 \times (47 - 17 \times 2) - 3 \times 17 = 4 \times 47 - 11 \times 17 = 4 \times 47 - 11 \times (111 - 47 \times 2) = 26 \times 47 - 11 \times 111, \text{ d'où le résultat avec } u = 26 \text{ et } v = -11.$$

*Remarque.* Il existe des résultats analogues sur les polynômes (voir l'exercice 3 page 60).

EXERCICE 3. a) Montrer que pour tout entier naturel  $n$ ,  $5 \mid (2^{3n+5} + 3^{n+1})$ .

b) Montrer que pour tout entier  $n$ ,  $30 \mid (n^5 - n)$ .

c) Quel est le reste de la division euclidienne de  $16^{(2^{1000})}$  par 7 ?

---

*Solution.* a) On a  $2^5 \equiv 2 \pmod{5}$  et  $2^{3n} \equiv 8^n \equiv 3^n \pmod{5}$  donc  $2^{3n+5} \equiv 2 \cdot 3^n \pmod{5}$  et  $2^{3n+5} + 3^{n+1} \equiv 2 \cdot 3^n + 3 \cdot 3^n \equiv 0 \pmod{5}$ .

b) D'après le théorème de Fermat,  $n^5 \equiv n \pmod{5}$ , c'est-à-dire  $5 \mid (n^5 - n)$ .

De même,  $n^3 \equiv n \pmod{3}$  donc  $n^5 \equiv n^3 \cdot n^2 \equiv n \cdot n^2 \equiv n^3 \equiv n \pmod{3}$ , i. e.  $3 \mid (n^5 - n)$ .

Les entiers  $n$  et  $n^5$  ayant même parité, on a aussi  $2 \mid (n^5 - n)$ .

De plus, 2, 3 et 5 sont premiers entre eux deux à deux, et finalement  $30 = 2 \cdot 3 \cdot 5$  divise  $(n^5 - n)$ .

c) Posons  $N = 16^{(2^{1000})}$ . Il s'agit de déterminer la classe de congruence de  $N$  modulo 7. Comme  $16 \equiv 2 \pmod{7}$ , on a déjà  $N \equiv 2^{2^{1000}} \pmod{7}$ . En vue d'utiliser la relation  $2^6 \equiv 1 \pmod{7}$  (théorème de Fermat), recherchons le reste de la division de  $2^{1000}$  par 6. La relation  $4^2 \equiv 4$

(mod 6) permet d'obtenir, par récurrence sur  $n$ , la relation  $4^n \equiv 4 \pmod{6}$ , vraie pour tout  $n$ . En particulier,  $2^{1000} \equiv 4^{500} \equiv 4 \pmod{6}$ , donc il existe un entier naturel  $q$  tel que  $2^{1000} = 6q + 4$ .

Il ne reste qu'à écrire

$$N \equiv 2^{6q+4} \equiv (2^6)^q \cdot 2^4 \equiv 1^q 2^4 \equiv 2^4 \equiv 2 \pmod{7},$$

et le reste recherché est 2.

**EXERCICE 4 (NOMBRES DE MERSENNE, NOMBRES DE FERMAT).** **a)** *Nombres de Mersenne.* Soient  $a \geq 2$  et  $n \geq 2$  deux entiers. Si  $a^n - 1$  est un nombre premier, montrer que  $a = 2$  et que  $n$  est un nombre premier (un nombre de la forme  $2^p - 1$  où  $p$  est un nombre premier, est appelé *nombre de Mersenne*).

**b)** *Nombres de Fermat.* Soit  $n \in \mathbb{N}^*$ . Si  $2^n + 1$  est un nombre premier, montrer que  $n$  est une puissance de 2.

*Solution.* **a)** L'identité  $x^n - 1 = (x - 1)(x^{n-1} + \dots + x + 1)$  montre que

$$\forall x \in \mathbb{N}, x \geq 2, \quad (x - 1) \text{ divise } (x^n - 1). \quad (*)$$

L'entier  $a^n - 1$  étant premier, on en déduit  $a - 1 = 1$ , c'est-à-dire  $a = 2$ .

Écrivons  $n = pq$  où  $p$  et  $q$  sont deux entiers naturels. On a  $a^n - 1 = 2^n - 1 = (2^q)^p - 1$  de sorte que  $(2^q - 1)$  divise  $a^n - 1$  d'après (\*), ce qui entraîne  $q = 1$  ou  $q = n$  puisque  $a^n - 1$  est premier. L'entier  $n$  est donc premier.

**b)** Lorsque  $n$  est impair, l'identité  $x^n + 1 = (x + 1)(x^{n-1} - \dots + x^2 - x + 1)$  entraîne

$$\forall x \in \mathbb{N}, \forall n \in \mathbb{N}, n \text{ impair}, \quad (x + 1) \text{ divise } (x^n + 1). \quad (**)$$

Si  $n$  n'est pas une puissance de 2,  $n$  a au moins un facteur impair  $p > 1$ . Écrivons  $n = pq$  avec  $q \in \mathbb{N}^*$ . L'entier  $2^n + 1 = (2^q)^p + 1$  est divisible par  $(2^q + 1)$  d'après (\*\*), donc non premier. Ainsi,  $n$  doit être une puissance de 2.

*Remarque.* La réciproque du résultat de la question a) est fautive. Par exemple,  $2^{11} - 1 = 23 \times 49$  n'est pas premier. Cependant, on peut tester facilement la primalité des nombres de Mersenne grâce au test suivant (test de Lucas).

Soit  $(Y_n)$  la suite définie par  $Y_0 = 2$  et  $Y_{n+1} = 2Y_n^2 - 1$ . Si  $n \geq 3$ ,  $2^n - 1$  est premier si et seulement si  $(2^n - 1) \mid Y_{n-2}$ .

Ce test a permis de trouver le plus grand nombre premier connu en 2020 :  $2^{82589933} - 1$ , nombre d'un peu moins de 25 millions de chiffres, établi en 2018 avec le test de Lucas. On ignore s'il y a une infinité de nombres de Mersenne premiers ou pas. Notons que les nombres de Mersenne apparaissent dans les nombres parfaits (voir l'exercice 10 page 16).

– *Nombres de Fermat.* Fermat avait vérifié que  $2^{2^n} + 1$  était premier pour  $0 \leq n \leq 4$  et pensait que  $2^{2^n} + 1$  était premier pour tout  $n$ . Mais Euler montra que  $2^{2^5} + 1 = 641 \times 6700417$ , et on a jusqu'ici trouvé aucun autre nombre de Fermat premier. On ne sait même pas s'il y en a ! Le sujet d'étude 2 page 49 donne un test de primalité simple des nombres de Fermat.

**EXERCICE 5.** Soit  $A$  la somme des chiffres de  $4444^{4444}$  (écrit dans le système décimal) et  $B$  la somme des chiffres de  $A$ . Que vaut  $C$ , la somme des chiffres de  $B$  ?

*Solution.* L'exercice repose essentiellement sur la remarque suivante.

Tout entier naturel  $N$  est congru à la somme de ses chiffres (en base 10) modulo 9. (\*)

En effet. On peut écrire  $N = a_0 + a_1 \cdot 10 + \dots + a_p \cdot 10^p$ , où les  $a_i$  sont des entiers compris entre 0 et 9. La congruence  $10 \equiv 1 \pmod{9}$  entraîne  $10^i \equiv 1 \pmod{9}$  pour tout  $i$  donc

$$N = \sum_{i=0}^p a_i 10^i \equiv \sum_{i=0}^p a_i \pmod{9}.$$

On applique maintenant ce résultat. On a  $C \equiv B \equiv A \equiv 4444^{4444} \pmod{9}$ . D'après (\*),  $4444 \equiv 16 \equiv -2 \pmod{9}$  donc  $4444^3 \equiv (-2)^3 \equiv 1 \pmod{9}$ , et comme  $4444 = 3 \cdot 1481 + 1$ , on a  $4444^{4444} = (4444^3)^{1481} \cdot 4444 \equiv 1 \cdot (-2) \equiv 7 \pmod{9}$ . Finalement,

$$C \equiv 7 \pmod{9}. \quad (**)$$

Majorons maintenant  $C$  de manière à montrer  $C = 7$ . Le nombre  $4444^{4444}$  étant inférieur à  $10000^{5000} = 10^{20000}$ , il a au plus 20000 chiffres. Donc  $A$  vaut au plus  $9 \times 20000 = 180000$ , donc a au plus 6 chiffres, donc  $B$  vaut au plus  $6 \times 9 = 54$ , donc  $C \leq 5 + 9 = 14$ . De (\*\*), on tire  $C = 7$ .

*Remarque.* C'est la propriété (\*) qui explique le principe de la preuve par 9 que l'on effectue dans les classes de l'école primaire.

EXERCICE 6. Soit  $P = X^n + c_1 X^{n-1} + \dots + c_{n-1} X + c_n$  un polynôme à coefficients entiers. Montrer qu'une racine rationnelle de  $P$  est nécessairement entière.

---

*Solution.* Soit  $x = a/b$  une racine rationnelle de  $P$  ( $a \in \mathbb{Z}$ ,  $b \in \mathbb{N}^*$ ,  $a \wedge b = 1$ ). On a

$$0 = b^n P\left(\frac{a}{b}\right) = a^n + c_1 a^{n-1} b + \dots + c_{n-1} a b^{n-1} + c_n b^n$$

donc

$$a^n = -b(c_1 a^{n-1} + \dots + c_{n-1} a b^{n-2} + c_n b^{n-1}),$$

ce qui montre que  $b$  divise  $a^n$ . Les entiers  $a$  et  $b$  étant premiers entre eux, ceci n'est possible que si  $b = 1$ , d'où le résultat.

*Remarque.* On en déduit en particulier que la racine  $n$ -ième de tout entier  $N$  est soit entière, soit irrationnelle (considérer le polynôme  $X^n - N$ ).

EXERCICE 7. Montrer qu'il y a une infinité de nombres premiers de la forme  $6k - 1$ ,  $k \in \mathbb{N}^*$ .

---

*Solution.* Raisonnons par l'absurde en supposant qu'il n'y en ait qu'un nombre fini. Désignons par  $N$  le plus grand d'entre eux. L'entier  $M = -1 + 6(N!)$  est impair donc  $2 \nmid M$ . De même,  $M \equiv -1 \pmod{3}$  donc  $3 \nmid M$ .

Soit  $p$  un facteur premier de  $M$ . Si  $p$  est de la forme  $6k - 1$ , alors  $p \leq N$  donc  $p \mid (6 \cdot N!)$ , d'où  $p \mid (6N! - M) = 1$ , ce qui est impossible. Le nombre  $p$  n'est donc pas de la forme  $6k - 1$ . De plus  $p \notin \{2, 3\}$  comme on l'a vu plus haut, donc  $p$  est de la forme  $6k + 1$ ,  $k \in \mathbb{N}^*$ . Dans la décomposition  $M = p_1^{\alpha_1} \dots p_n^{\alpha_n}$  de  $M$  en facteurs premiers, on a donc  $p_i \equiv 1 \pmod{6}$  pour tout  $i$ , d'où  $M \equiv 1 \pmod{6}$ , ce qui est absurde car  $M \equiv -1 \pmod{6}$  par construction.

*Remarque.* On peut démontrer de la même manière qu'il y a une infinité de nombres premiers de la forme  $4k - 1$ . Il existe un théorème plus général (théorème de Dirichlet, 1837) qui dit :

$\forall (a, b) \in (\mathbb{N}^*)^2$ ,  $a \wedge b = 1$ , il existe une infinité de nombres premiers de la forme  $ak + b$ ,  $k \in \mathbb{N}$ .

Malheureusement, ce résultat n'a encore jamais pu être obtenu par des moyens élémentaires et simples. On peut cependant le démontrer dans certains cas particuliers (voir le problème 5 page 40, la partie 6/ du sujet d'étude 2 page 49 ou le problème 11 page 99).

En notant  $\pi_{a,b}(x)$  le nombre de nombres premiers  $\leq x$  de la forme  $ak + b$ , le théorème de Dirichlet assure également que lorsque  $a \wedge b = 1$ , on a  $\pi_{a,b}(x) \sim_{x \rightarrow +\infty} \pi(x)/\varphi(a)$  (où  $\pi(x)$  désigne le nombre de nombres premiers  $\leq x$  et  $\varphi(a)$  l'indicateur d'Euler de  $a$ ).

**EXERCICE 8. a)** Montrer qu'il n'existe pas de polynôme  $P$  non constant à coefficients entiers, tel que  $P(n)$  soit premier pour tout entier  $n$  supérieur à un certain rang  $N$ .

**b)** On considère un polynôme  $P$  à  $k$  variables et à coefficients entiers. On pose  $f(n) = P(n, 2^n, 3^n, \dots, k^n)$ , et on suppose  $\lim_{n \rightarrow \infty} f(n) = +\infty$  (ceci pour éviter des fonctions comme  $f(n) = 2^n 5^n - 10^n + 7$ ). Montrer que  $f(n)$  ne peut pas être un nombre premier pour tout entier  $n$  supérieur à un certain rang  $N$ .

*Solution.* **a)** Supposons qu'un tel polynôme existe. Écrivons  $P = \sum_{k=0}^n a_k X^k$ . L'entier  $p = P(N) = \sum_{k=0}^n a_k N^k$  est premier. Or tout entier naturel  $r$  vérifie

$$P(N + rp) = \sum_{k=0}^n a_k (N + rp)^k \equiv \sum_{k=0}^n a_k N^k \equiv 0 \pmod{p},$$

autrement dit  $P(N + rp)$  est divisible par  $p$  pour tout entier naturel  $r$ . Comme  $P(N + rp)$  est premier, on a  $P(N + rp) = p$  pour tout entier naturel  $r$ . Ainsi, le polynôme  $P(X) - p$  a une infinité de racines, il est donc nul, ce qui est contraire aux hypothèses.

**b)** Supposons l'existence d'une telle fonction. Un peu d'attention montre que  $f$  peut se mettre sous la forme

$$f(n) = \sum_{r=1}^m \left( \sum_{s=0}^{q_r} c_{r,s} n^s \right) a_r^n,$$

où les  $a_r$  et  $c_{r,s}$  sont entiers, avec  $1 \leq a_1 < a_2 < \dots < a_m$ . Comme  $\lim_{n \rightarrow \infty} f(n) = +\infty$ , on peut supposer  $f(N) > a_m > \dots > a_1 \geq 1$  (quitte à augmenter  $N$ ). Notons  $p$  le nombre premier  $p = f(N)$ . On a

$$\forall \ell \in \mathbb{N}, \forall s \in \mathbb{N}, \quad [N + \ell p(p-1)]^s \equiv N^s \pmod{p},$$

et d'après le théorème de Fermat, lorsque  $1 \leq r \leq m$  on a

$$a_r^{p-1} \equiv 1 \pmod{p} \quad \text{donc} \quad \forall \ell \in \mathbb{N}, \quad a_r^{N + \ell p(p-1)} \equiv a_r^N \pmod{p}.$$

Finalement,

$$\forall \ell \in \mathbb{N}, \quad [N + \ell p(p-1)]^s a_r^{N + \ell p(p-1)} \equiv N^s a_r^N \pmod{p},$$

et ceci pour tous les entiers  $r, s$  donc  $f[N + \ell p(p-1)] \equiv f(N) \equiv 0 \pmod{p}$ . Ceci étant vrai pour tout entier naturel  $\ell$ , on aboutit à une absurdité.

**EXERCICE 9.** Pour tout entier naturel  $n$ , on pose  $F_n = 2^{2^n} + 1$  (nombres de Fermat).

**a)** Montrer que les nombres  $(F_n)_{n \in \mathbb{N}}$  sont premiers entre eux deux à deux.

**b)** En déduire une autre démonstration du fait qu'il y a une infinité de nombres premiers.

*Solution.* **a)** Si  $n \in \mathbb{N}$ ,  $k \in \mathbb{N}^*$ , il s'agit de montrer que  $F_n$  et  $F_{n+k}$  sont premiers entre eux. La relation

$$F_{n+k} - 1 = 2^{2^{n+k}} - 1 = (2^{2^n})^{2^k} - 1 = (F_n - 1)^{2^k}$$

entraîne

$$F_{n+k} - 1 \equiv (F_n - 1)^{2^k} \equiv (-1)^{2^k} \equiv 1 \pmod{F_n}$$

donc  $F_n \mid (F_{n+k} - 2)$ . Ainsi, le pgcd  $d$  de  $F_n$  et  $F_{n+k}$  divise  $F_{n+k} - 2$ . Comme de plus  $d \mid F_{n+k}$ ,  $d$  divise 2, et  $F_n$  étant impair, on a nécessairement  $d = 1$ .

**b)** Pour tout  $n \in \mathbb{N}$ , notons  $p_n$  un facteur premier de  $F_n$ . Les  $F_n$  étant premiers entre eux deux à deux, les  $(p_n)_{n \in \mathbb{N}}$  sont distincts deux à deux. On a donc trouvé une infinité de nombres premiers.

*Remarque.* Profitons en ici pour rappeler quelques résultats dans l'histoire des nombres premiers. Les grecs savaient déjà qu'il y en avait une infinité. Le gros résultat suivant fut le théorème des nombres premiers.

*Si  $\forall x > 0$ ,  $\pi(x)$  désigne le nombre de nombres premiers inférieurs à  $x$ , on a  $\pi(x) \sim x/\log(x)$  lorsque  $x$  tend vers l'infini.*

Il fut démontré pour la première fois et presque simultanément par J. Hadamard et C. De la Vallée Poussin en 1896. Les démonstrations les plus classiques de ce résultat font appel à la fonction  $\zeta$  de Riemann. Une preuve en est proposée en annexe du tome d'Analyse (à partir de la deuxième édition).

**EXERCICE 10 (NOMBRES PARFAITS).** **1/a)** Pour tout entier naturel non nul  $n$ , on note  $\sigma(n)$  la somme des diviseurs de  $n$ . Exprimer  $\sigma(n)$  en fonction des termes intervenant dans la décomposition de  $n$  en facteurs premiers. Montrer que

$$n \wedge m = 1 \implies \sigma(nm) = \sigma(n)\sigma(m). \quad (*)$$

**b)** On dit qu'un entier naturel non nul  $n$  est parfait s'il est égal à la somme de ses diviseurs autres que lui même (*i. e.* si  $\sigma(n) = 2n$ ). Si  $2^p - 1$  est un nombre premier, montrer que  $n = 2^{p-1}(2^p - 1)$  est un nombre parfait.

**c)** Réciproquement, démontrer qu'un nombre parfait pair  $n$  est de la forme  $2^{p-1}(2^p - 1)$ , où  $2^p - 1$  est nécessairement un nombre premier.

**2/ (Nombres parfaits impairs).** **a)** (Théorème d'Euler). Montrer que s'il existe un nombre parfait impair  $n$ , alors il est nécessairement de la forme

$$n = p^{1+4\alpha}Q^2 \quad \text{avec } p \text{ premier, } p \equiv 1 \pmod{4}, \alpha \in \mathbb{N}, \text{ et } Q \in \mathbb{N}^* \text{ avec } p \wedge Q = 1.$$

(Indication : à partir de la décomposition en facteurs premiers  $n = \prod p_i^{\alpha_i}$ , étudier la valeur de  $\sigma(p_i^{\alpha_i})$  modulo 4.)

**b)** Montrer qu'un nombre parfait impair a au moins 3 facteurs premiers distincts.

*Solution.* **1/a)** Si  $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$  est la décomposition de  $n$  en facteurs premiers, on a

$$\sigma(n) = \sum_{\substack{0 \leq \beta_1 \leq \alpha_1 \\ \vdots \\ 0 \leq \beta_k \leq \alpha_k}} p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = \prod_{i=1}^k (1 + p_i + \cdots + p_i^{\alpha_i}) = \prod_{i=1}^k \left( \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \right).$$

La propriété (\*) en découle immédiatement.

**b)** On applique les résultats de la question précédente pour écrire

$$\sigma(n) = \sigma[2^{p-1}(2^p - 1)] = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1)2^p = 2n.$$

**c)** La réciproque est plus délicate. Comme  $n$  est pair, il existe un entier  $p \geq 2$  tel que  $n = 2^{p-1}m$  avec  $m$  impair. Le fait que  $2^{p-1} \wedge m = 1$  nous autorise à utiliser (\*), de sorte que  $\sigma(n) = \sigma(2^{p-1})\sigma(m) = (2^p - 1)\sigma(m)$ . Or  $\sigma(n) = 2n = 2^p m$  donc  $(2^p - 1) \mid 2^p m$ , et comme  $(2^p - 1) \wedge 2^p = 1$ , d'après le théorème de Gauss on a  $(2^p - 1) \mid m$ . Autrement dit, il existe  $\ell \in \mathbb{N}^*$  tel que  $m = (2^p - 1)\ell$ . La relation  $2^p m = 2n = \sigma(n) = (2^p - 1)\sigma(m)$  entraîne  $\sigma(m) = 2^p \ell = m + \ell$ .

Si  $\ell > 1$ ,  $m$  a au moins trois diviseurs distincts qui sont 1,  $\ell$  et  $m$ , d'où  $\sigma(m) \geq m + \ell + 1$ , ce qui est absurde. Donc  $\ell = 1$ ,  $m = 2^p - 1$  et  $\sigma(m) = m + \ell = m + 1$ ; on en déduit que