Chapter 15 Arithmétique des entiers

15.1 Divisibilité

Exercice 15.1

Démontrer par récurrence que pour tout $n \in \mathbb{N}$, 7 divise $3^{6n} - 6^{2n}$.

Exercice 15.2 (***) *Une majoration de σ (ENS MP)*

Pour $n \in \mathbb{N}^\star$, on note $\sigma(n)$ la somme des diviseurs de n. Montrer que

$$\sigma(n) \leq n + n \ln n.$$

Exercice 15.3

Les nombres a, b, c, d étant des éléments non nuls de $\mathbb{Z}$, dire si les propriétés suivantes sont vraies ou fausses, en justifiant la réponse.

1. Si a divise b et c, alors $c^2 - 2b$ est multiple de a.
2. Si a divise $b + c$ et $b - c$, alors a divise b et a divise c.
3. Si a est multiple de b et si c est multiple de d, alors $a + c$ est multiple de $b + d$.
4. Si 4 ne divise pas bc, alors b ou c est impair.
5. Si a divise b et b ne divise pas c, alors a ne divise pas c.

Exercice 15.4

Déterminer les entiers $n \in \mathbb{N}$ tels que :

1. $n | n + 8$.
2. $n - 1 | n + 11$.
3. $n - 3 | n^3 - 3$.

Exercice 15.5

Déterminer l'ensemble E des $n \in \mathbb{Z}$ tels que $n^2 + 7 \,\Big|\, n^3 + 5$.

Exercice 15.6

Soit $n \in \mathbb{N}^\star$.

1. Montrer que tout élément de $[\![1, n]\!]$ a au moins un multiple dans $[\![n + 1, 2n]\!]$.
2. En déduire que l'ensemble E des multiples communs à $1, 2, \ldots, 2n$ est égal à l'ensemble E' des multiples communs à $n + 1, n + 2, \ldots, 2n$.

15.2 Division euclidienne

15.3 Les nombres premiers

Exercice 15.7

Montrer que pour tout $n \in \mathbb{N}$, l'intervalle $[\![n! + 2, n! + n]\!]$ ne contient aucun nombre premier.

Exercice 15.8 (***) *Infinité des nombres premiers congrus à 3 modulo 4, (X MP)*

Montrer que l'ensemble $\mathcal{P}$ des nombres premiers est infini. Montrer qu'il en est de même de l'ensemble des nombres premiers congrus à 3 modulo 4.

15.4 Plus grand commun diviseur, algorithme d'Euclide

Exercice 15.9

Les nombres a, b, c, d étant des éléments non nuls de $\mathbb{Z}$, dire si les propriétés suivantes sont vraies ou fausses, en justifiant la réponse.

1. Si a divise b et b divise c, alors a divise c.
2. Si a divise b et a divise c, alors a divise $2b + 3c$.
3. S'il existe u et v entiers tels que $au + bv = 4$ alors $\text{pgcd}(a, b) = 4$.
4. Si $7a - 9b = 1$ alors a et b sont premiers entre eux.
5. Si a divise b et b divise c et c divise a, alors $|a| = |b|$.
6. Si a divise c et b divise d, alors ab divise cd.
7. Si 9 divise ab et si 9 ne divise pas a, alors 9 divise b.
8. Si a divise b ou a divise c, alors a divise bc.
9. Si a divise b, alors a n'est pas premier avec b.
10. Si a n'est pas premier avec b, alors a divise b ou b divise a.

Exercice 15.10

Soient a et b des entiers > 0 et premiers entre eux. Montrer qu'il existe un et un seul couple d'entiers (c, d) tel que

$$ac + bd = 1 \qquad\qquad 0 \leq c < b, \tag{1}$$

et que les autres solutions (u, v) de l'égalité de Bézout $ua + vb = 1$ sont $u = c + kb$ et $v = d - ka$, k parcourant $\mathbb{Z}$.

Exercice 15.11

Soient $n \in \mathbb{N}^\star$. Pour $q \in \mathbb{Z}$, on considère l'application

$$\begin{array}{rccc} \varphi_q : & \mathbb{U}_n & \to & \mathbb{U}_n \\ & z & \mapsto & z^q \end{array}.$$

1. Soient $p, q \in \mathbb{Z}$. Calculer $\varphi_p \circ \varphi_q$.
2. On suppose que n et q sont premiers entre eux. Vérifier que l'application φ_q est bijective.
3. Réciproquement, on suppose l'application φ_q bijective. Montrer que n et q sont premiers entre eux.

Exercice 15.12 (***)

Pour tout entier $m \geq 1$, notons $\varphi(m)$ le nombre d'entiers $k \in [1, m]$ premiers avec m.

La fonction $\varphi : \mathbb{N}^\star \to \mathbb{N}$ ainsi définie s'appelle *indicatrice d'Euler*. Démontrer, pour tout entier $n \geq 1$, l'égalité

$$\sum_{d \mid n} \varphi(d) = n, \tag{1}$$

la somme étant étendue à tous les diviseurs $d > 0$ de n.

Exercice 15.13

Les nombres a, b étant des éléments non nuls de $\mathbb{Z}$, dire si les propriétés suivantes sont vraies ou fausses, en justifiant la réponse.

1. Si 19 divise ab, alors 19 divise a ou 19 divise b.

2. Si 91 divise ab, alors 91 divise a ou 91 divise b.

3. Si 5 divise b^2, alors 25 divise b^2.

4. Si 12 divise b^2, alors 4 divise b.

5. Si 12 divise b^2, alors 36 divise b^2.

Exercice 15.14

Montrer que si $p > 3$ est premier, alors $24|p^2 - 1$.

Exercice 15.15 (**) *Multiples formésde* 1

Soit n un entier naturel non nul. On se propose de montrer qu'il existe un multiple de n dont l'écriture en base 10 est composée uniquement de 1 si, et seulement si n est premier avec 10.

1. Montrer que la condition $\text{pgcd}(n, 10) = 1$ est nécessaire.

2. Réciproquement, on suppose $\text{pgcd}(n, 10) = 1$.

   - Justifier que l'application $\mathbb{N} \to [\![0, n-1]\!]$ qui à r associe le reste de la division euclidienne de 10^r par n n'est pas injective.
   - En déduire qu'il existe deux entiers distincts u, v tels que $10^u - 10^v$ soit divisible par n, puis l'existence d'un entier r tel que $10^r - 1$ soit divisible par n.
   - Montrer alors que $\frac{10^{9r}-1}{9}$ est un entier, multiple de n et de la forme souhaitée.

3. Trouver le plus petit multiple de 49 formé uniquement de chiffres 1.

Exercice 15.16

Calculer $\text{pgcd}(424, 68)$ par l'algorithme d'Euclide.

Exercice 15.17

Calculer par l'algorithme d'Euclide $\text{pgcd}\,(18480, 9828)$.

Exercice 15.18 *Une équation avec un PGCD et un PPCM*

Résoudre l'équation suivante, d'inconnues $(a, b) \in \mathbb{N}^2$:

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

Exercice 15.19

Soit $n \in \mathbb{N}$. Déterminer, en discutant éventuellement suivant les valeurs de n, le pgcd des entiers suivants.

$$A = 9n^2 + 10n + 1 \qquad \text{et} \qquad B = 9n^2 + 8n - 1.$$

Exercice 15.20

Soit $u = (u_n)_{n\in\mathbb{N}}$ la suite numérique définie par

$$u_0 = 0, \qquad u_1 = 1, \qquad \text{et} \qquad \forall n \in \mathbb{N}, u_{n+2} = 3u_{n+1} - 2u_n.$$

1. Calculer les termes u_2, u_3, u_4, u_5, u_6 de la suite u.

2. Montrer que la suite u vérifie

   $$\forall n \in \mathbb{N}, u_{n+1} = 2u_n + 1.$$

   En déduire le plus grand diviseur commun de deux termes consécutifs de cette suite u.

3. Montrer que la suite u vérifie

$$\forall n \in \mathbb{N}, u_n = 2^n - 1.$$

Les nombres $2^n - 1$ et $2^{n+1} - 1$ sont-ils premiers entre eux pour tout entier naturel n ?

4. Vérifier que, pour tout couple d'entiers naturels $(n, p) \in \mathbb{N} \times \mathbb{N}$,

$$u_{n+p} = u_n \left(u_p + 1\right) + u_p.$$

En déduire que, pour tout couple d'entiers naturels $(n, p) \in \mathbb{N} \times \mathbb{N}$,

$$\text{pgcd}\left(u_n, u_{n+p}\right) = \text{pgcd}\left(u_n, u_p\right). \tag{1}$$

5. Soient a et b deux entiers naturels non nuls, r est le reste de la division euclidienne de a par b. Déduire de la propriété (1)

$$\text{pgcd}\left(u_b, u_r\right) = \text{pgcd}\left(u_a, u_b\right)$$

et que

$$\text{pgcd}\left(u_a, u_b\right) = u_{\text{pgcd}(a,b)}.$$

6. Calculer alors $\text{pgcd}\left(u_{1982}, u_{312}\right)$.

Exercice 15.21

On considère l'équation (E) : $26x + 15y = 1$ dans laquelle les inconnues x et y sont des entiers relatifs.

1. Écrire l'algorithme d'Euclide pour les nombres 26 et 15.

2. En déduire une solution particulière de (E) puis l'ensemble des solutions de (E).

3. Utiliser ce qui précède pour résoudre l'équation $26x + 15y = 4$.

Exercice 15.22

Résoudre dans $\mathbb{Z}^2$ les équations

1. $1260x + 294y = 3814$.

2. $1260x + 294y = 2814$.

Exercice 15.23 *Développement de* $(1 + \sqrt{2})^n$

1. Monter

$$\forall n \in \mathbb{N}, \exists!(a_n, b_n) \in \mathbb{Z}^2, \left(1 + \sqrt{2}\right)^n = a_n + b_n\sqrt{2}.$$

2. Calculer $\text{pgcd}(a_n, b_n)$ pour tout $n \in \mathbb{N}$.

Exercice 15.24 (***) *Suite de Farey*

Soit $n \in \mathbb{N}^\star$. Considérons tous les nombres rationnels *mis sous forme irréductible* appartenant à $[0, 1]$, et dont le dénominateur est au plus égal à n. En les rangeant par ordre croissant, on obtient une suite $\mathcal{F}_n$, appelée *suite de Farey d'ordre n*. Voici par exemple $\mathcal{F}_7$:

$$\frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}.$$

1. Montrer que, si $x = \frac{a}{b}$ et $y = \frac{c}{d}$ sont deux termes consécutifs de $\mathcal{F}_n$ $(x < y)$, on a $bc - ad = 1$.

2. Déduire de ce qui précède que, si $x = \frac{a}{b}$, $y = \frac{c}{d}$, $z = \frac{e}{f}$ sont trois termes consécutifs de $\mathcal{F}_n$, on a $y = \frac{a+e}{b+f}$.

15.5 Décomposition en facteurs premiers

Exercice 15.25
Combien 15! admet-il de diviseurs positifs ?

Exercice 15.26
Résoudre l'équation $xy + 6x - 3y = 40$ d'inconnue $(x, y) \in \mathbb{Z}^2$.

Exercice 15.27
Soit $n \in \mathbb{N} \setminus \{ 0, 1 \}$ dont la décomposition en facteurs premiers s'écrit

$$n = \prod_{k=1}^{r} p_k^{\alpha_k}$$

avec $p_1, \dots, p_r$ des nombres premiers deux à deux distincts.

On note $d(n)$ le nombre de diviseurs positifs de n et $\sigma(n)$ la somme de ceux-ci. Montrer

$$d(n) = \prod_{k=1}^{r} \left(\alpha_k + 1\right) \quad \text{et} \quad \sigma(n) = \prod_{k=1}^{r} \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Exercice 15.28
Soient $a \in \mathbb{N}^\star$ et N le nombre de diviseurs positifs de a. Déterminer une condition nécessaire et suffisante portant uniquement sur N pour que a soit un carré parfait.

Exercice 15.29 (***) *Un théorème de Kurshchak*
Pour $a \in \mathbb{N}^\star$, la valuation 2-adique de a est

$$v_2(a) = \max \left\{ \, k \in \mathbb{N} \, \middle| \, 2^k \, \middle| \, a \, \right\}.$$

Soit $m > n > 0$ deux entiers.

- Montrer qu'il existe dans $[\![n, m]\!]$ un seul entier de valuation 2-adique maximale.
- En déduire que $\sum_{k=n}^{m} \frac{1}{k}$ n'est jamais un entier.

15.6 La relation de congruence

Exercice 15.30
Quel est le reste de la division euclidienne de 3^{2024} par 11.

Exercice 15.31
Calculer 2000^{2000} modulo 7 et 2^{500} modulo 3.

Exercice 15.32 *Reste de la division euclidiene du carré d'un entier par* 8

1. Soit $a \in \mathbb{Z}$. Montrer que le reste de la division euclidienne de a^2 par 8 est égal à 0, 1 ou 4.
2. Soit $n \in \mathbb{N}$. Montrer que, si 8 divise $n - 7$, alors n ne peut pas être la somme de trois carrés d'entiers.

Exercice 15.33
Déterminer les nombres entiers x tels que $x^2 - 2x + 2$ soit divisible par 17.

Exercice 15.34
Déterminer les solutions entière de $x^2 + y^2 = 11z^2$.

Exercice 15.35
Résoudre les équations suivantes.

1. $5x \equiv 3$ [17].

2. $10x \equiv 6$ [34].

3. $10x \equiv 5$ [34].

Exercice 15.36 (**)

Résoudre les systèmes suivants d'inconnue $(x, y) \in \mathbb{Z}^2$:

1. $\begin{cases} x & \equiv 6 \pmod 9 \\ x & \equiv 7 \pmod{10} \end{cases}$.

2. $\begin{cases} x & \equiv 3 \pmod{11} \\ x & \equiv 2 \pmod{14} \end{cases}$.

Exercice 15.37

15 pirates chinois se partagent un butin constitué de pièces d'or. Mais une fois le partage (équitable) effectué, il reste 3 pièces. Que va-t-on en faire ? La discussion s'anime. Bilan : 8 morts. Les 7 survivants recommencent le partage, et il reste cette fois ci 2 pièce ! Nouvelle bagarre à l'issue de laquelle il ne reste que 4 pirates. Heureusement, ils peuvent cette fois ci se partager les pièces sans qu'il n'en reste aucune.

Sachant que 32 Tsing-Tao (bière chinoise) coûtent une pièce d'or, combien (au minimum) de Tsing-Tao pourra boire chaque survivant ?

Exercice 15.38 (**) *Le petit théorème de Fermat*

Soit p un nombre premier.

1. Montrer que pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.

2. En déduire que pour tout $(a, b) \in \mathbb{N}^2$, $(a+b)^p \equiv a^p + b^p \pmod p$.

3. Montrer par récurrence que : $\forall a \in \mathbb{N}$, on a $a^p \equiv a \pmod p$.

4. En déduire que si p ne divise pas $a \in \mathbb{Z}$, alors,

$$a^{p-1} \equiv 1 \pmod p.$$

Exercice 15.39 (***) *Étude de l'irréductibilité d'une fraction*

1. Montrer que pour tout $n \in \mathbb{N}$, la fraction $\dfrac{5^{n+1} + 6^{n+1}}{5^n + 6^n}$ est irréductible.

2. Trouver une condition nécessaire et suffisante sur $(\lambda, \mu, \alpha, \beta) \in \mathbb{N}^4$ pour que la fraction $\dfrac{\lambda\alpha^{n+1} + \mu\beta^{n+1}}{\lambda\alpha^n + \mu\beta^n}$ soit irréductible pour tout $n \in \mathbb{N}$.