1. Arithmétique des entiers

Exercice 1.1 Trouver le PGCD de 341 et 527.

Exercice 1.2 Trouver tous les couples d'entiers positifs dont le PGCD est 56 et le PPCM est 672.

Exercice 1.3 Montrer que si les entiers a et b sont premiers entre eux, alors $a^2 + b^2$ et ab sont premiers entre eux. La réciproque est-elle vérifiée ?

Exercice 1.4 Soient a, b, c, n des entiers et $d = \mathrm{PGCD}(a, b)$.

1. Montrer que si c est divisible par a et b alors cd est divisible par ab :
$$(a \mid c \quad \text{et} \quad b \mid c) \quad \Longrightarrow \quad ab \mid cd.$$
2. Montrer que si a divise c, alors $n^a - 1$ divise $n^c - 1$.
3. Montrer à l'aide de l'algorithme d'Euclide que
$$\mathrm{PGCD}(n^a - 1, n^b - 1) = n^d - 1.$$
4. En déduire que si a et b sont premiers entre eux, alors $(n^a - 1)(n^b - 1)$ divise $(n^{ab} - 1)(n - 1)$.

Exercice 1.5 (Divisibilité par 9)

1. Montrer que pour tout $k \in \mathbb{N}$, on a $10^k \equiv 1 \pmod 9$.
2. Montrer que $4 \times 10^3 - 5 \times 10^2 + 8 \times 10 - 7$ est divisible par 9.
3. Montrer que 571356 est un multiple de 9.
4. Trouver une condition nécessaire et suffisante pour qu'un nombre soit divisible par 9.

Exercice 1.6 Soient a, b, c trois entiers relatifs. Montrer que si $a^3 + b^3 + c^3$ est divisible par 7, alors l'un des trois entiers a, b ou c est divisible par 7.

Exercice 1.7 Montrer qu'un entier de la forme $8k - 1$ n'est pas somme de trois carrés.

Exercice 1.8 Trouver l'inverse de 8 modulo 43.

Exercice 1.9 Résoudre dans $\mathbb{Z}$:

a) $2x + 3y = 4$ b) $341x - 527y = 62$ c) $10x - 8y = 42$
d) $15x + 51y = 41$ e) $17x + 19y = 23$

Exercice 1.10 Résoudre dans $\mathbb{Z}$:

a) $13x + 1 \equiv 8 \pmod{25}$ b) $207x \equiv 6 \pmod{18}$

c) $3x \equiv 10 \pmod{2003}$ d) $\begin{cases} 3x \equiv 2 & \pmod 5 \\ 5x \equiv 4 & \pmod 9 \end{cases}$

e) $\begin{cases} 3x \equiv 1 & \pmod 5 \\ 4x \equiv 6 & \pmod{14} \\ 5x \equiv 11 & \pmod 3 \end{cases}$

Exercice 1.11 (Triplets pythagoriciens) Le but de cet exercice est de trouver tous les triplets d'entiers positifs (x, y, z) tels que :

$$x^2 + y^2 = z^2. \tag{1}$$

1. Montrer que tout triplet solution de (1) est de la forme (dx', dy', dz'), où $d \in \mathbb{N}$ et $(x', y', z') \in \mathbb{N}^3$ est un triplet de nombres premiers entre eux dans leur ensemble et solution de (1).
2. Montrer qu'en fait x', y' et z' sont premiers entre eux deux à deux.
   On suppose désormais que x, y et z sont premiers entre eux deux à deux.
3. Montrer que z est impair. En déduire que x et y sont de parité différente.
   On suppose que x impair et y pair.
4. Montrer que $z + y$ et $z - y$ n'ont pas de diviseur premier commun. En déduire que ces deux nombres sont des carrés.
5. Montrer que toute solution de (1) est de la forme :

   $$x = kld, \quad y = \frac{k^2 - l^2}{2} d, \quad z = \frac{k^2 + l^2}{2} d,$$

   avec d un entier positif et k, l deux entiers impairs premiers entre eux tels que $k \geq l$.

Exercice 1.12 (Une infinité de nombres premiers 1.) Supposons, par l'absurde, qu'il n'y ait qu'un nombre fini de nombres premiers $\{p_1, \ldots, p_h\}$. On considère :

$$A = p_1 \cdots p_h + 1.$$

Démontrer qu'il n'est divisible par aucun des $p_1, \ldots, p_h$ et conclure.

Exercice 1.13 (Une infinité de nombres premiers 2.) Soit n un entier positif non nul, on pose :

$$F_n = 2^{2^n} + 1.$$

Montrer que si $m < n$, alors F_m et F_n sont premiers entre eux (indication : évaluer F_n en fonction de F_m). En déduire que l'ensemble des nombres premiers est infini.

Exercice 1.14 (Une infinité de nombres premiers 3.) Soit $\mathcal{P} = \{p_1, \ldots, p_h\}$ un ensemble de h nombres premiers distincts. Notons $\mathcal{N}$ l'ensemble des nombres entiers positifs dont tous les facteurs premiers sont dans $\mathcal{P}$, et $\nu(x)$ le nombre d'éléments de $\mathcal{N}$ qui sont $\leq x$.

1. Montrer que tout élément $n \in \mathcal{N}$ s'écrit de façon unique sous la forme :

   $$n = p_1^{c_1} \times \cdots \times p_h^{c_h} \times m^2, \qquad \text{avec } c_i \in \{0, 1\}\ (i = 1, \ldots, h) \text{ et } m \in \mathcal{N}.$$

2. Supposons que $n \leq x$, vérifier que $m \leq \sqrt{x}$ et en déduire que $\nu(x) \leq 2^h \sqrt{x}$.
3. Déduire de ce qui précède qu'il y a un nombre infini de nombres premiers.