1. Arithmétique élémentaire

Exercice 1. Calculer le pgcd de 341 et 672 puis écrire une relation de Bézout explicite pour ces deux nombres.

Exercice 2. Déterminer tous les couples d'entiers naturels dont le pgcd est 56 et dont le ppcm est 672.

Exercice 3. Soient a, b et c trois nombres entiers relatifs ; on suppose que a et b sont non nuls et on pose $d = \text{pgcd}(a,b)$.
1. Déterminer toutes les solutions entières de l'équation homogène $ax+by=0$.
2. Démontrer que l'équation inhomogène $ax+by=c$ admet une solution entière si et seulement si $d|c$.
3. Déterminer toutes les solutions entières de l'équation inhomogène $ax+by=c$ lorsque $d|c$.

Exercice 4. Résoudre les équations suivantes dans $\mathbb{Z}$:

a) $2x+3y=4$ b) $341x-672y=62$ c) $15x+51y=41$
d) $10x-8y=42$ e) $17x+19y=23$

Exercice 5. Exhiber trois nombres entiers p, a, b tels que $p|ab$ mais $p\nmid a$ et $p\nmid b$. Étant donné un nombre entier non nul p, à quelle condition l'assertion

$$\forall a,\ b\in\mathbb{Z},\ (p|ab \Longrightarrow p|a \ \text{ ou } \ p|b)$$

est-elle vraie ?

Exercice 6. Exhiber trois nombres entiers p, q, a tels que $p|a$ et $q|a$ mais $pq\nmid a$. Étant donnés des nombres entiers non nuls p,q, à quelle condition l'assertion

$$\forall a\in\mathbb{Z},\ (p|a \text{ et } q|a \Longrightarrow pq|a)$$

est-elle vraie ?

Exercice 7. Un général chinois livre bataille à la tête de deux mille hommes. À l'issue du combat, il demande aux rescapés de se grouper par 11 et note que cinq soldats restent isolés ; il leur demande ensuite de se grouper par 13 et note que trois soldats restent isolés ; il leur demande enfin de se grouper par 15 et note alors que 11 soldats restent isolés. Quelle perte doit-il annoncer à l'empereur ?

Exercice 8. Résoudre dans $\mathbb{Z}$ les systèmes suivants :

$$\begin{cases} x\equiv 3 \pmod 6\\ x\equiv 2 \pmod 5\\ x\equiv 6 \pmod 7\end{cases}$$

Exercice 9. Résoudre dans $\mathbb{Z}$ les systèmes suivants :

$$a)\begin{cases} 3x\equiv 2 \pmod 5\\ 5x\equiv 4 \pmod 9\end{cases}\qquad b)\begin{cases} 3x\equiv 1 \pmod 5\\ 4x\equiv 6 \pmod{14}\\ 5x\equiv 11 \pmod 3\end{cases}$$

Exercice 10. Résoudre dans $\mathbb{Z}$ les systèmes suivants :

$$a)\begin{cases} x\equiv 2 \pmod 4\\ x\equiv 3 \pmod 6\end{cases}\qquad \begin{cases} 5x\equiv 1 \pmod{12}\\ 4x\equiv 2 \pmod{15}\end{cases}$$

Exercice 11. (*Divisibilité par* 9) 1. Prouver que $10^k\equiv 1 \pmod 9$ pour tout $k\in\mathbb{N}$.
2. Prouver que 571356 est un multiple de 9.
3. Donner une condition nécessaire et suffisante pour qu'un nombre entier soit divisible par 9.

Exercice 12. (*Une infinité de nombres premiers, 1*) Soit $\mathscr{E}=\{p_1,\dots,p_n\}$ un ensemble fini de nombres premiers. Démontrer que le nombre $p_1p_2\dots p_n+1$ n'est divisible par aucun des nombres $p_1,\dots,p_n$ et en déduire qu'il existe une infinité de nombres premiers.

Exercice 13. (*Une infinité de nombres premiers de la forme* $4m+3$) 1. Vérifier que le produit de deux nombres entiers de la forme $4m+1$ est encore de cette forme.

2. En adaptant le raisonnement de l'exercice précédent, démontrer qu'il existe une infinité de nombres premiers de la forme $4m+3$ (*Indication : considérer* $2^2 p_1 p_2 \dots p_n - 1$).

Exercice 14. (*Une infinité de nombres premiers, 2*) Étant donné un entier $n \geq 1$, le n-ème *nombre de Fermat* est défini par $F_n = 2^{2^n} + 1$.

Quels que soient les entiers $n, k > 0$, démontrer que F_n divise $F_{n+k} - 2$. En déduire que F_n et F_{n+k} sont premiers entre eux, puis qu'il existe une infinité de nombres premiers.

Exercice 15. (*Une infinité de nombres premiers, 3*) Soit $\mathscr{P}$ l'ensemble des nombres premiers.

En utilisant l'identité $\frac{1}{1-p^{-1}} = \sum_{m \geq 0} p^{-m}$, démontrer que l'on a

$$\sum_{n=1}^{N} \frac{1}{n} \leq \prod_{p \in \mathscr{P},\ p \leq N} \frac{1}{1-p^{-1}}$$

pour tout entier naturel $N \geq 2$. En déduire que l'ensemble $\mathscr{P}$ est infini.

Exercice 16. (*Une infinité de nombres premiers, 4*) Soit $\mathscr{P}_h = \{p_1, \dots, p_h\}$ l'ensemble des h premiers nombres premiers. On note $\mathscr{N}_h$ l'ensemble des entiers naturels dont tous les facteurs premiers appartiennent à $\mathscr{P}_h$ et, pour tout nombre réel positif x, on note $N_h(x)$ le nombre d'éléments de $\mathscr{N}_h$ majorés par x.

1. Montrer que tout élément $n \in \mathscr{N}_h$ s'écrit d'une manière et d'une seule sous la forme $n = n_1^2 p_1^{\varepsilon_1} \dots p_h^{\varepsilon_h}$ avec $n_1 \in \mathscr{N}_h$ et $\varepsilon_1, \dots, \varepsilon_h \in \{0, 1\}$.

2. Si $n \leq x$, vérifier que l'on a $n_1 \leq \sqrt{x}$ et en déduire la majoration $N_h(x) \leq 2^h \sqrt{x}$.

3. Déduire de ce qui précède qu'il existe une infinité de nombres premiers.

4. Étant donné un nombre réel $x \geq 1$, on note $\pi(x)$ le cardinal de l'ensemble des nombres premiers majorés par x. En utilisant ce qui précède, démontrer que l'on a

$$\pi(x) \geq \frac{\log(x)}{2\log(2)}.$$

Cette minoration est-elle de bonne qualité ?

5. Démontrer que le n-ème nombre premier p_n est majoré par 4^n.

Exercice 17. (*Équation de Pythagore*) Le but de cet exercice est de déterminer l'ensemble $\mathscr{E}$ de tous les triplets d'entiers naturels (x, y, z) tels que

$$x^2 + y^2 = z^2.$$

0. Déterminer tous les triplets $(x, y, z) \in \mathscr{E}$ dans lesquels une coordonnée au moins s'annule.

À partir de maintenant, on ne considère que des triplets (x, y, z) *avec* $x, y, z \geq 1$.

1. Montrer que tout élément (x, y, z) de $\mathscr{E}$ est de la forme (dx', dy', dz'), où $d \in \mathbb{N}$ et (x', y', z') est un élément de $\mathscr{E}$ tel que x', y' et z' soient des entiers naturels premiers entre eux dans leur ensemble.

2. Prouver que les entiers x', y' et z' sont en fait premiers entre eux deux à deux.

À partir de maintenant, on considère un élément (x, y, z) *de* $\mathscr{E}$ *telle que* x, y *et* z *soient des entiers naturels premiers entre eux deux à deux.*

3. Démontrer que l'un des deux nombres x ou y est pair (*Indication : raisonner modulo* 4).

4. Supposons que x soit pair. Démontrer que les entiers $z+y$ et $z-y$ sont pairs, puis que

$$\frac{z+y}{2} \quad \text{et} \quad \frac{z-y}{2}$$

sont des carrés.

5. Déduire de ce qui précède que $\mathscr{E}$ est l'ensemble de tous les triplets (x, y, z) qui, à permutation près de x et y, sont de la forme

$$x = 2dab, \quad y = d(a^2 - b^2), \quad z = d(a^2 + b^2),$$

où $d \in \mathbb{N}$ et a, b sont deux entiers premiers entre eux, de parité différente et tels que $a > b > 0$.

6. Dresser la liste de tous les triplets $(x, y, z) \in \mathscr{E}$ tels que $\max\{x, y, z\} \leq 30$.