Arithmétique

1) Factorisation et diviseurs

Définition Pour $n, m \in \mathbb{N}$, on dit que n divise m, ce que l'on note $n \mid m$, s'il existe $k \in \mathbb{N}$ tel que $m = kn$.
On dit que $p \in \mathbb{N}$ est premier si $p \neq 1$ et si les seuls diviseurs de p sont 1 et lui-même.

Exemple Montrer que si $k \mid n$ et $k \mid m$, alors $k \mid n+m$ et $k \mid n-m$.

Parité

Exercice 1 Montrer que n est pair si et seulement si n^2 est pair.

Exercice 2 Soit n impair, et $a_1, \dots, a_n$ la suite des entiers $1, 2, \dots, n$ réordonnés. Montrer que $(a_1-1)(a_2-2)\dots(a_n-n)$ est pair.

Divisibilité

Exercice 3 Soit $n > 3$ un nombre premier. Montrer qu'il existe $m \in \mathbb{N}$ tel que $n = 6m+1$ ou $n = 6m-1$.

Exercice 4 Soit $n = \underline{abc}_{10}$ un nombre à trois chiffres. Montrer que $11 \mid n$ si et seulement si $11 \mid a-b+c$.

Factorisations

Exercice 5
1. En écrivant $a^4 + 4b^4 = a^4 + 4b^4 + 4a^2b^2 - 4a^2b^2$, factoriser $a^4 + 4b^4$.
2. Montrer que pour $n \in \mathbb{N}^*$, si $n \geq 2$, $n^4 + 4^n$ n'est pas un nombre premier.

Exercice 6
1. Vérifier que pour $a, b \in \mathbb{Z}$ et $m \in \mathbb{N}^*$, on a
$$a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \dots + a + 1) \quad \text{et} \quad a^m - b^m = (a-b)(a^{m-1} + a^{m-2}b + \dots + ab^{m-2} + b^{m-1}).$$
2. Montrer que pour $n \geq 2$, $3^{2n} - 2^n$ et $3^{2n+1} + 1$ ne sont pas premiers.
3. Montrer que pour $n \in \mathbb{N}^*$, si $2^n - 1$ est premier, alors n est premier.

Factorisations et équations diophantiennes

Exercice 7 Déterminer le nombre de solutions entières positives de l'équation $x^2 - y^2 = 100^2$.

Exercice 8 Déterminer les entiers $n \in \mathbb{N}^*$ tels que $2^n \mid 3^n - 1$.

Exercice 9
1. Soient $x, y \in \mathbb{N}$. On suppose que $y \geq 5$ et que $7^x - 3 \cdot 2^y = 1$. Montrer que x est pair, puis que $\frac{x}{2}$ est pair.
2. Déterminer tous les couples $(x, y) \in \mathbb{N}^2$ vérifiant $7^x - 3 \cdot 2^y = 1$.

Diviseurs

Exercice 10 Quels sont les entiers $n \in \mathbb{N}^*$ admettant un nombre impair de diviseurs ?

Exercice 11 Soit $a_0 \in \mathbb{N}$. Pour $n \in \mathbb{N}$, tant que a_n a au moins trois diviseurs autres que lui même, on définit a_{n+1} comme la somme de ses trois plus grands diviseurs, autres que lui-même.
1. Si a_0 est impair, montrer que le procédé termine.
2. Pour quels a_0 est-ce que le procédé ne termine jamais ?

2) Entiers premiers entre eux et diviseurs communs

Définition On dit que deux entiers n et m sont premiers entre eux si leur seul diviseur commun est 1.

Exercice 12 Soit $n \in \mathbb{N}^*$. Montrer que n et $n+1$ sont premiers entre eux. Montrer que $21n+4$ et $14n+3$ sont premiers entre eux.

Exercice 13 Montrer que $\text{pgcd}(1 + a + a^2 + \dots + a^{m-1}, a-1) = \text{pgcd}(a-1, m)$.

Exercice 14 Montrer que si a, b sont premiers entre eux, alors $a^2 - b^2$ et ab sont premiers entre eux

Exercice 15 On considère la suite de Fibonacci, définie par $F_0 = 1$, $F_1 = 1$ et pour tout $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$. Montrer que pour tout $n \in \mathbb{N}$, F_n et F_{n+1} sont premiers entre eux.

Théorème de Bézout

Propriété Soit $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Alors il existe $q \in \mathbb{N}$ et $r \in [\![0, b-1]\!]$ tel que $a = bq + r$. Cette écriture est unique.

Exercice 16 Soient $a, b \in \mathbb{N}$. On note A l'ensemble des entiers de $\mathbb{N}^*$ qui peuvent s'écrire sous la forme $au + bv$, avec $u, v \in \mathbb{Z}$.
1. Soit d le minimum de A. Montrer que si a, b sont premiers entre eux, alors $d = 1$. **Ind** : *Considérer des divisions euclidiennes.*
2. En déduire le théorème de Bézout : a, b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Applications

Exercice 17 Soit $x \in \mathbb{R}_+^*$ tel que x^{101} et x^{37} soient rationnels. Montrer que x est rationnel.

Exercice 18 Lemme de Gauss Montrer que si a, b sont premiers entre eux et $a \mid bc$ alors $a \mid c$.

Exercice 19 Soit $P(x) = ax^3 + bx^2 + cx + d$ un polynôme à coefficients entiers. Montrer que si $P\left(\frac{p}{q}\right) = 0$ avec $\frac{p}{q}$ une fraction irréductible, alors $p \mid d$ et $q \mid a$.

3) Nombres premiers

Exercice 20
1. Montrer qu'il existe une infinité de nombres premiers.
2. Montrer qu'il existe une infinité de nombres premiers de la forme $4k-1$.
Ind : *Le produit de deux entiers de la forme $4k+1$ est également de la forme $4k+1$.*

Décomposition en facteurs premiers

Théorème Tout entier $n \geq 2$ se décompose, de manière unique, comme produit de facteurs premiers : $n = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$.

Propriété Soient $n, m \geq 1$ deux entiers. On note $p_1, \dots, p_\ell$ les nombres premiers divisant n ou m. On écrit

$$n = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell} \quad \text{et} \quad m = p_1^{\beta_1} \dots p_\ell^{\beta_\ell}, \quad \text{où} \quad \alpha_i, \beta_i \geq 0.$$

Alors $n \mid m$ si et seulement si ...

Exercice 21 Quel est le nombre de diviseurs de $n = p_1^{\alpha_1} \dots p_\ell^{\alpha_\ell}$?

Exercice 22 Par combien de 0 l'écriture décimale de 2025! termine-t-elle ? Quel est le dernier chiffre non nul ?

Exercice 23 Soient $a, b \in \mathbb{N}^*$. On suppose que pour tout $k \in \mathbb{N}$, a^k divise b^{k+1}. Montrer que a divise b.

Exercice 24 ★ Pour quels entiers n est-ce que 2^{n-1} divise $n!$?

Répartition des nombres premiers

Exercice 25 Soit $n \geq 1$. En considérant $N = (n+1)!$, montrer que l'on peut trouver n entiers consécutifs dont aucun n'est premier.

Exercice 26 On considère la suite $(p_n)_{n\geq 1}$ des nombres premiers. On note, pour $n \in \mathbb{N}^*$, $\quad S_n = \dfrac{1}{p_1} + \dots + \dfrac{1}{p_n} = \displaystyle\sum_{k=1}^{n} \frac{1}{p_k}$.

L'objectif est de montrer que S_n tend vers $+\infty$.
On procède par l'absurde et on travaille sous l'hypothèse que $(S_n)_{n\in\mathbb{N}}$ est majorée. En particulier, il existe un entier n_0 tel que

$$\sum_{k=n_0+1}^{+\infty} \frac{1}{p_k} = \frac{1}{p_{n_0+1}} + \frac{1}{p_{n_0+2}} + \dots < \frac{1}{2}.$$

On appelle grands nombres premiers les p_k pour $k \geq n_0 + 1$, et petits nombres premiers les autres. Soit $N \in \mathbb{N}^*$.

1. On note N_g le nombre d'entiers $\leq N$ qui sont divisibles par un grand nombre premier. Montrer que $N_g < \frac{N}{2}$.
2. On note N_s le nombre d'entiers $\leq N$ qui sont ne sont divisibles par aucun grand nombre premier.
   Justifier que tout entier $n \geq 1$ peut s'écrire de manière unique comme $n = ab^2$, où $a, b \in \mathbb{N}^*$ et a n'est divisible par le carré d'aucun nombre premier. En déduire que $N_s \leq 2^{n_0}\sqrt{N}$.
3. Aboutir à une contradiction.

4) Ordre d'un élément

Fonction φ d'Euler

Définition Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers de $[\![1, n]\!]$ qui sont premiers avec n.

Exercice 27 Que dire de $\varphi(p)$ pour p un nombre premier ? De $\varphi(p^\alpha)$?

Exercice 28 Soit $n \in \mathbb{N}^*$. En réduisant les fractions $\frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n}$, sous forme irréductible, montrer que $\varphi(1) + \dots + \varphi(n) = n$.

Exercice 29 Montrer que pour tout $n \geq 3$, $\varphi(n)$ est pair.

Théorèmes de Fermat et d'Euler

Notation On note $a \equiv b[n]$ si a et b ont le même reste dans la division euclidienne par n, ou, de manière équivalente, si $n \mid b - a$.

Propriété Si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors $ab \equiv a'b'[n]$.

Exemple Déterminer le reste dans la division euclidienne de 7^{100} par 8.

Exercice 30 Théorème de Fermat Soit p un nombre premier et $a \in [\![1, p]\!]$ premier avec p.

1. Pour $k \in [\![1, p-1]\!]$, montrer que ak est premier avec p.
2. Montrer qu'il existe $\ell \in [\![1, p-1]\!]$ tel que $a\ell \equiv 1[p]$.
3. Pour $k_1, k_2 \in [\![1, p-1]\!]$ distincts, montrer que ak_1 et ak_2 sont distincts modulo p, c'est-à-dire $ak_1 \not\equiv ak_2[p]$.
4. En considérant les produits $\prod_{k=1}^{p-1} k = (p-1)!$ et $\prod_{k=1}^{p-1} ak$ modulo p, montrer que $a^{p-1} \equiv 1[p]$.

Pour $n \in \mathbb{N}^*$, en remplaçant $\prod_{k=1}^{p-1} k$ par le produit des entiers de $[\![1, n-1]\!]$ qui sont premiers avec n, on obtiendrait :

Théorème – d'Euler. Si a est premier avec n, on a $a^{\varphi(n)} \equiv 1[n]$.

Exercice 31 Soit a un entier premier avec 10. Montrer qu'il existe un multiple de a qui ne s'écrit qu'avec le chiffre 9.

Exercice 32 Montrer que pour $n \in \mathbb{N}^*$, on a $n \mid 2^{n!} - 1$.

Exercice 33 ★ Déterminer les entiers $n \in \mathbb{N}^*$ impairs tels que $n \mid 3^n + 1$.

Indication : Considérer le plus petit facteur premier p de n et le plus petit entier $o \in \mathbb{N}^*$ tel que $3^o \equiv 1[p]$.