# Exercices 17 — Arithmétique

## Divisibilité - Congruences

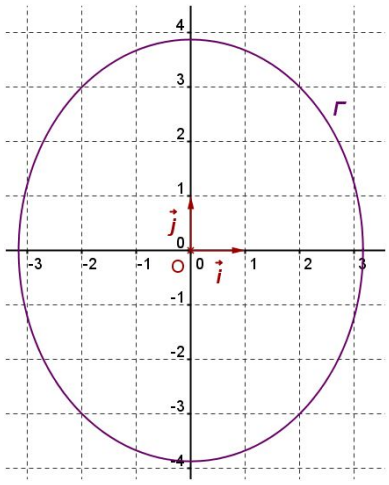
**Exercice 1.** — Montrer que l'équation $25x - 60y = 13$ n'admet pas de couple d'entiers solution.

**Exercice 2.** — Prouver que l'équation $12x + 15y^2 + 36xy = 3002$ n'admet pas de couple d'entiers relatifs solution.

**Exercice 3.** — Dans cet exercice, on cherche à résoudre l'équation diophantienne :

$$(E) \qquad 3x^2 + 2y^2 = 30$$

(c'est-à-dire que l'on cherche les couples $(x, y)$ d'entiers relatifs solutions de l'équation $(E)$).




1) Démontrer que si $(x, y)$ est un couple d'entiers relatifs solution de $(E)$, alors $(x, -y)$ est un autre couple solution.

   *Dans la suite de l'exercice, on admettra que si $(x, y)$ est solution de $(E)$, alors les couples $(-x, y)$ et $(-x, -y)$ sont également solutions.*

2) Soient $x$ et $y$ deux entiers naturels tels que $3x^2 + 2y^2 = 30$.

   a) Démontrer que $0 \leqslant x \leqslant 3$.

   b) En examinant les différents cas, déterminer tous les couples $(x, y)$ d'entiers naturels solutions de $(E)$.

3) Conclure en donnant la liste des couples d'entiers relatifs solutions de $(E)$.

**Exercice 4.** — Déterminer tous les entiers naturels $n$ tels que $(n - 1)$ divise $(n + 8)$.

**Exercice 5.** — Déterminer tous les entiers naturels $n$ tels que $(n - 4)$ divise $(3n + 24)$.

**Exercice 6.** — Montrer que le produit de deux entiers naturels consécutifs est pair.

**Exercice 7.** — Montrer que la somme de trois entiers naturels consécutifs est un multiple de 3.

**Exercice 8.** — Montrer que le produit de trois entiers naturels consécutifs est un multiple de 3.

**Exercice 9.** — Montrer que la somme de cinq entiers naturels consécutifs est un multiple de 5.

**Exercice 10.** — Montrer que : $11 \left| \left(2^{123} + 3^{121}\right) \right.$

**Exercice 11.** — Montrer que le produit de 62 entiers naturels consécutifs est multiple de 59.

**Exercice 12.** — La propriété : "pour tout entier naturel $n$, $5^{6n+1} + 2^{2n}$ est divisible par 5" est-elle vraie ?

**Exercice 13.** — Montrer que pour tout entier naturel $n$, $5^{6n+1} + 2^{3n+1}$ est divisible par 7.

**Exercice 14.** — Montrer que $1 + 2^{30} + 3^{30} + 4^{30}$ est multiple de 5.

**Exercice 15.** — Montrer que $1^{1001} + 2^{1001} + 3^{1001} + 4^{1001} + 5^{1001}$ est divisible par 5.

**Exercice 16.** — Montrer que pour tout entier relatif $n$ le nombre $A_n = n(n + 3)(n + 6)(n + 13)$ est divisible par 4.

**Exercice 17.** — Montrer que l'équation (E) : $5x^2 + 2y^4 = 135789$ n'admet aucun couple d'entiers relatifs solution.

**Exercice 18.** — On considère un polynôme $P$ de degré $n > 1$ à coefficients entiers relatifs. Explicitement, on suppose que P s'écrit : $P(x) = a_n x^n + \cdots + a_1 x + a_0$ avec $a_0, a_1, \ldots, a_n$ des entiers relatifs, et $a_n \neq 0$ et $a_0 \neq 0$.

1) Montrer que toute racine entière de $P$ divise $a_0$.

2) En déduire que le polynôme $x^3 + 2x^2 + 6x - 4$ n'a pas de racine entière.

**Exercice 19.** — Soient $x$ et $y$ deux entiers relatifs. Montrer que : $7 \left| x \right.$ et $7 \left| y \right. \iff 7 \left| x^2 + y^2 \right.$

**Exercice 20. — Critère de divisibilité par 3**

Pour $n$ un entier naturel, on peut noter : $\overline{a_p \cdots a_1 a_0}$ son écriture décimale, les $a_i$ désignant des entiers compris entre 0 et 9. Cette écriture signifie que : $n = a_p \times 10^p + \cdots + a_1 \times 10 + a_0$.

Etablir que $n$ est multiple de 3 si et seulement si $\sum_{i=0}^{p} a_i$ est multiple de 3.

**Exercice 21. — Critère de divisibilité par 11**

Mêmes notations que précédemment. Etablir que $n$ est multiple de 11 si et seulement si $\sum_{i=0}^{p} (-1)^i a_i$ est multiple de 11.

**Exercice 22. — Système chinois**

1) Déterminer tous les entiers $x$ congrus à 2 modulo 10. 2) Déterminer tous les entiers $x$ congrus à 5 modulo 13.

3) Résoudre dans $\mathbb{Z}$ le système : $\begin{cases} x \equiv 2 \ [10] \\ x \equiv 5 \ [13] \end{cases}$

## Division euclidienne

**Exercice 23. —** Déterminer tous les entiers naturels qui, divisés par 6, donnent un quotient égal au reste.

**Exercice 24. —** Déterminer le quotient et le reste dans la division euclidienne de $a = 3^{1000} + 28$ par 9.

**Exercice 25. —** Déterminer le quotient et le reste dans la division euclidienne de $A = 5^{2019} + 51$ par 25.

**Exercice 26. —** On divise un entier naturel $n$ par 243 et 248. Les quotients sont égaux, et les restes respectifs sont 130 et 10. Quel est cet entier naturel $n$ ?

**Exercice 27. —** Déterminer le reste dans la division euclidienne de $1234^{2019}$ par 7 (on pourra noter que $1234 \equiv 2 \ [7]$, et que $2019 = 3 \times 673$).

## PGCD, PPCM, relation de Bezout

**Exercice 28. —** Déterminer le PGCD et les "coefficients de Bezout" des entiers $a$ et $b$ suivants :

1) $a = 33$ et $b = 24$ 2) $a = 37$ et $b = 27$ 3) $a = 270$ et $b = 105$

**Exercice 29. —** Soit $n \in \mathbb{N}$. Montrer que le PGCD de $2n + 4$ et $3n + 3$ ne peut être que 1, 2, 3 ou 6.

**Exercice 30. —** Déterminer tous les couples d'entiers relatifs tels que : $\begin{cases} x \wedge y &= 15 \\ xy &= 900 \end{cases}$

**Exercice 31. —** Déterminer tous les couples d'entiers naturels tels que : $\begin{cases} x \wedge y &= 8 \\ x^2 - y^2 &= 5440 \end{cases}$

**Exercice 32. —** Déterminer tous les couples $(x, y)$ d'entiers naturels tels que : $\begin{cases} x \vee y = 18 \\ x + y = 15 \end{cases}$

**Exercice 33. —** Déterminer tous les couples d'entiers relatifs tels que : $\begin{cases} x \wedge y &= 5 \\ x \vee y &= 60 \end{cases}$

**Exercice 34. —** Déterminer tous les couples d'entiers relatifs tels que : $\begin{cases} x \wedge y &= 10 \\ x + y &= 100 \end{cases}$

**Exercice 35. —** Quel est le plus petit entier naturel congru à 5 modulo 27 et modulo 42 ?

**Exercice 36. —** Déterminer l'ensemble des couples d'entiers relatifs $(x,\ y)$ solutions de (E) : $7x - 6y = 1$.

**Exercice 37. —** Déterminer l'ensemble des couples d'entiers relatifs $(x,\ y)$ solutions de (E) : $16x - 3y = 4$.

**Exercice 38. —** Déterminer l'ensemble des couples $(x\ ;\ y) \in \mathbb{Z}^2$ solutions de $(E) : 3x + 7y = 10^n$ (où $n \in \mathbb{N}$).

**Exercice 39. —** Déterminer l'ensemble des couples d'entiers relatifs $(x,\ y)$ solutions de (E) : $18x + 7y = 12$.

**Exercice 40.** — On se propose de déterminer tous les entiers relatifs $N$ tels que : $\begin{cases} N & \equiv & 5 & [13] \\ N & \equiv & 1 & [17] \end{cases}$

1) Vérifier que 239 est solution de ce système.
2) Soit $N$ un entier relatif solution de ce système. Démontrer que $N$ peut s'écrire sous la forme $N = 1 + 17x = 5 + 13y$ où $x$ et $y$ sont deux entiers relatifs vérifiant la relation $17x - 13y = 4$.
3) Résoudre l'équation $17x - 13y = 4$ où $x$ et $y$ sont des entiers relatifs.
4) En déduire qu'il existe un entier relatif $k$ tel que $N = 18 + 221k$.
5) Démontrer l'équivalence entre $N \equiv 18 \quad [221]$ et $\begin{cases} N & \equiv & 5 & [13] \\ N & \equiv & 1 & [17] \end{cases}$.

**Exercice 41.** — On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie par : $u_0 = 0$, $u_1 = 1$ et $\forall\, n \in \mathbb{N},\ u_{n+2} = u_{n+1} + u_n$.

0) Révision : quelle est l'expression du terme général $u_n$ en fonction de $n$ ?
1) Montrer que : $\forall\, n \in \mathbb{N}^*,\ u_{n+1}u_{n-1} - u_n^2 = (-1)^n$.
2) En déduire que : $\forall\, n \in \mathbb{N}^*,\ u_{n+1} \wedge u_n = 1$.

**Exercice 42.** — Soient $a$ et $b$ deux entiers premiers entre eux. Montrer que $a$ et $a + b$ sont premiers entre eux.

**Exercice 43.** — Soit $n \in \mathbb{N}^*$. Montrer que $n^2 + n$ et $2n + 1$ sont premiers entre eux.

## Nombres premiers

**Exercice 44.** — Montrer que l'entier naturel $N = 2^{2022} - 49$ n'est pas premier.

**Exercice 45.** — 1) Pour vérifier que 977 est premier, on peut essayer de le diviser par les nombres premiers 2, 3, 5 et ainsi de suite jusqu'à un certain nombre premier $p_1$. Précisément, quelle est la valeur de $p_1$ ?
2) Déterminer tous les couples d'entiers naturels $(x, y)$ tels que : $x^2 - y^2 = 977$.

**Exercice 46.** — Soit $p$ un nombre premier, $p \geqslant 5$. Montrer que $p^2 - 1$ est divisible par 24.

**Exercice 47.** — Construire une liste de 2019 entiers consécutifs non premiers.

**Exercice 48.** — Existe t-il deux entiers relatifs non-nuls $a$ et $b$ tels que : $a\ln(3) + b\ln(7) = 0$ ?

**Exercice 49.** — Justifier que : $\forall\, n \in \mathbb{Z},\ 19 \,|\, n^{19} - n$.

**Exercice 50.** — **(Un nombre de Carmichael, 1879-1967)**. Justifier que : $\forall\, n \in \mathbb{Z},\ n^{1729} \equiv n\ [1729]$ (indication : $1729 = 7 \times 13 \times 19$).

**Exercice 51.** — **(Sur les nombres de Mersenne, 1588-1648)**. On suppose que $n$ est un entier $\geqslant 2$ tel que $2^n - 1$ est premier. Montrer que $n$ est premier.

**Exercice 52.** — **(Progression arithmétique de Dirichlet, 1805-1859)** Montrer qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

**Exercice 53.** — **(Théorème de Wilson, 1741-1793)** [*]
Soit $p$ un entier $\geqslant 2$. Etablir que : $p$ est premier SSI $(p-1)! \equiv -1\ [p]$.

**Exercice 54.** — **Indicatrice d'Euler (1707-1783).**
**Notations** : pour tout entier $n \geqslant 2$, on note $\phi(n)$ le nombre d'entiers naturels inférieurs à $n$ qui sont premiers avec $n$. On définit ainsi une application $\phi : \mathbb{N}\setminus\{0,1\} \longrightarrow \mathbb{N}^*$, appelée fonction **indicatrice d'Euler**.
Par exemple : $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$. On notera $\mathscr{P}$ l'ensemble des nombres premiers.

1) En justifiant brièvement vos réponses, donner les valeurs de $\phi(5)$, $\phi(9)$ et $\phi(12)$. [†]

---

∗. Selon la **loi d'éponymie de Stigler** : "une découverte scientifique ne porte jamais le nom de son auteur" (cette loi, énoncée par le statisticien Stephen Stigler en 1980, ne serait pas de Stigler lui-même !...). Cette loi s'applique en particulier au théorème de Wilson. Celui-ci fut énoncé initialement par un mathématicien Arabe nommé Alhazen (965-1039). Il fut connu à partir du XVIIe siècle en Europe, mentionné dans les travaux de Leibniz (1646-1716). Un peu plus tard, Wilson redécouvre ce qu'il croit être une conjecture et en partage la découverte avec son professeur Edward Waring, qui publie cette conjecture en 1770. Lagrange (1736-1813) en présente deux premières démonstrations en 1771, puis Euler une troisième en 1773. Utilisant les notations de l'arithmétique modulaire, Gauss (1777-1855) reformule la démonstration d'Euler et en donne une quatrième.

†. On pourra vérifier (après calculs et justifications) que $\phi(12) = \phi(3) \times \phi(4)$, et que $\phi(9) \neq \phi(3) \times \phi(3)$.

2) Soit $n$ un entier supérieur ou égal à 2, et soit $a \in \mathbb{Z}$. Redémontrer que :

$$[a \text{ est inversible modulo } n] \iff [a \wedge n = 1]$$

3) Soit $p \in \mathscr{P}$.

   a) Etablir que $\phi(p) = p - 1$.

   b) Soit $\alpha \in \mathbb{N}^*$. Soit $n$ un entier naturel. Montrer que : $[n \wedge p = 1] \iff [n \wedge p^\alpha = 1]$.

   c) En déduire que pour tout $\alpha \in \mathbb{N}^*,\ \phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

*A la lumière de la question 3-a, la conclusion de cette question peut être réécrite : $\forall n \in \mathbb{Z}\backslash p\mathbb{Z},\ n^{\phi(p)} \equiv 1\,[p]$. Cette assertion peut être généralisée à un entier $N$ non nécessairement premier ; il s'agit de l'énoncé ci-dessous.*

$$\boxed{\underline{\text{Théorème d'Euler}} :\quad \forall N \in \mathbb{N}\backslash\{0,1\},\ \forall n \in \mathbb{Z},\ [n \wedge N = 1] \Longrightarrow \left[n^{\phi(N)} \equiv 1\ [N]\right]}\ ^{\ddagger}$$

**Exercice 55. — Les bases du codage RSA, extrait du DS9 de 2018**

1) **Congruences et exponentiation rapide**

   a) Déterminer le PGCD et les coefficients de Bezout des entiers 27 et 112.

   b) On pose $a = 12$. Calculer $a^2$, puis $a^4$, puis $a^8$ et enfin $a^{16}$ modulo 145.

   c) Déduire de ce qui précède la valeur de $12^{27}$ modulo 145.

2) **Questions de cours**

   a) Rappeler la définition d'entiers premiers entre eux. Rappeler la définition de nombre premier.

   b) Soient $a$ et $b$ deux entiers. A quelle condition sur $a$ et $b$ l'entier $a$ est-il inversible modulo $b$ ? Donner, en justifiant brièvement votre réponse, un inverse de 27 modulo 112, ainsi qu'un inverse de 112 modulo 27.

   c) Etablir que si $p$ et $q$ sont deux nombres premiers distincts, alors ils sont premiers entre eux.

   d) Soit $p$ un nombre premier. Le petit théorème de Fermat affirme que : $\forall a \in \mathbb{Z},\ a^p \equiv a\ [p]$.

   Redémontrer alors que : $\forall a \in \mathbb{Z}\backslash p\mathbb{Z},\ a^{p-1} \equiv 1\ [p]$.

3) **Une nouvelle conséquence du théorème de Fermat**. Soient $p$ et $q$ deux nombres premiers distincts, et soit $N = pq$.

   a) Montrer que $a$ est premier avec $N$ si et seulement si $a$ est premier avec $p$ et avec $q$.

   b) On suppose que $a$ est premier avec $N$. Montrer que $a^{(p-1)(q-1)} \equiv 1\ [p]$ et $a^{(p-1)(q-1)} \equiv 1\ [q]$.

   c) Déduire de la question précédente que $a^{(p-1)(q-1)} \equiv 1\ [N]$.

4) On pose $\varphi(N) = (p-1)(q-1)$. Soit $e$ un entier naturel premier avec $\varphi(N)$. Justifier qu'il existe un entier $d$ tel que $ed \equiv 1\ [\varphi(N)]$.

5) Soit $m$ un entier naturel.

   a) Montrer que si $m$ est premier avec $N$, alors $m^{ed} \equiv m\ [N]$. [§]

   b) Montrer que pour tout entier $m$, on a $m^{ed} \equiv m\ [N]$.

   c) **"Vérification"**. Dans cette question, on prend $p = 5$, $q = 29$, $m = 12$ et $e = 27$. Donner sans justification la valeur de $d$. Déterminer la valeur de $m^e$ modulo $N$, puis détailler le calcul de $(m^e)^d$ modulo $N$.

---

‡. Pour l'anecdote, voici le même énoncé dans sa version originale :

Theorema II.

55. Si fuerit N ad x numerus primus, et n numerus partium ad N primarum, tum poteſtas $x^n$ vnitate ni inuta ſemper per numerum N erit diuiſibilis.

Ce théorème est extrait d'un article publié (par Euler, vous aviez suivi !) en 1763 dans une revue scientifique russe appelée "Novi Commentarii academiae scientiarum Petropolitanae" (traduit en français : "Nouveaux Mémoires de l'Académie Impériale des Sciences de St-Petersbourg"). Qu'un mathématicien suisse ait publié en latin dans un journal russe ne doit pas vous surprendre ; en premier lieu, le latin fut la langue prédominante (pour ne pas dire exclusive) des travaux scientifiques entre le XVème et le XVIIIème siècles. En second lieu, la deuxième moitié du XVIIIème siècle correspond au règne de la tsarine Catherine II, qui a énormément contribué au développement des arts, lettres et sciences en Russie. Elle a notamment incité Euler à s'installer à Saint-Petersbourg (où il repose désormais), et a entretenu des relations privilégiées avec Diderot et Voltaire pour ne citer qu'eux.

§. Où $e$ et $d$ sont ceux définis dans la question 4, et $N = pq$ avec $p$ et $q$ premiers distincts.