# Introduction à l'arithmétique

Dans ce document, on se propose de donner un tour d'horizon des fondamentaux de l'arithmétique élémentaire des nombres entiers usuels. Il n'y a que peu de prérequis:

- Connaître le principe de récurrence.
- Pour les partie XI et XV uniquement: connaître le signe somme $\sum$ et savoir le manipuler.
- Pour la partie X uniquement: avoir quelques notions de géométrie du plan (pente d'une droite, équation d'un cercle).
- Pour la partie XIII uniquement: savoir ce qu'est un polynôme et son degré.

Toutes les autres notions abordées sont introduites au fil du problème. Les parties ne sont pas indépendantes. En revanche, il est parfaitement possible d'aborder une nouvelle partie en admettant les résultats des précédentes. Les parties sont numérotées en ordre grossièrement croissant de difficulté.

## Table des matières



## Partie I — Divisibilité des entiers

On que l'entier $n \neq 0$ divise l'entier $m$ lorsque $\frac{m}{n}$ est un entier (autrement dit, s'il existe $k \in \mathbb{Z}$ tel que $m = kn$). On note alors $n \mid m$. On dit aussi que $n$ est un diviseur de $m$.

(1) Pour chacune des propriétés suivantes, dire si elle est vraie ou fausse, en donner une preuve si elle est vraie, et un contre-exemple si elle est fausse.

(a) Si $n \mid m$ et $m \mid \ell$ alors $n \mid \ell$
(b) Si $n \mid m$ alors pour tout $k \in \mathbb{Z}$, $n \mid km$.
(c) Si $n \mid m$ et $\ell \mid m$ alors $n\ell \mid m$
(d) $n > 1$ admet au moins deux diviseurs.
(e) Si $n \mid m$ et $n \mid \ell$ alors $n \mid m + \ell$.
(f) Si $n, m > 0$, $n \mid m$ et $m \mid n$ alors $n = m$

(2) On appelle *plus grand commun diviseur (PGCD)* de deux entiers naturels $n$ et $m$ non simultanément nuls le plus grand entier $k \geq 1$ tel que $k \mid n$ et $k \mid m$. On le note $n \wedge m$
(a) Montrer que si $n, m > 0$, alors $n \wedge m \leq n$ et $n \wedge m \leq m$.
(b) Si $n \mid m$, que vaut $n \wedge m$ ? En déduire la valeur de $n \wedge 0$ pour $n > 0$.
(c) Montrer que si $n, m$ sont des entiers, alors

$$\frac{n}{n \wedge m} \wedge \frac{m}{n \wedge m} = 1$$

(3) On dit que deux entiers $n$ et $m$ sont *premiers entre eux* lorsque $n \wedge m = 1$.
   (a) Les entiers 12 et 15 sont ils premiers entre eux ? Et les entiers 9 et 11 ?
   (b) Montrer que pour tout $n > 1$, $n$ et $n - 1$ sont premiers entre eux.
   (c) (Lemme de Gauss) Montrer que si $k \mid \ell m$ et $k \wedge \ell = 1$ alors $k \mid m$.

# Partie II — Nombres premiers

(1) On dit qu'un entier $p > 1$ est *premier* si ses seuls diviseurs positifs sont 1 et $p$.
   (a) Lesquels des nombres suivants sont premiers ? $7, 9, 14, 17, 19, 21, 57$.
   (b) Montrer que $p$ est premier si et seulement si pour tout $m > 1$ qui n'est pas un multiple de $p$, on a $p \wedge m = 1$
   (c) Montrer que $p$ est premier si et seulement si pour tout $a, b \in \mathbb{Z}$ tels que $p$ divise $ab$, $p$ divise $a$ ou $p$ divise $b$.
   (d) Soit $n > 1$. Montrer que le plus petit diviseur $d > 1$ de $n$ est premier.
   (e) Soient $p, q$ deux nombres premiers distincts. Montrer que $p \wedge q = 1$.
   (f) Donner la valeur de $p^n \wedge p^m$ lorsque $p$ est premier et $1 \leq n < m$.

(2) Supposons qu'il y a un nombre fini de nombres premiers, que l'on note $p_1, \cdots, p_n$. En considérant le nombre

$$p_1 p_2 \cdots p_n + 1,$$

montrer qu'il existe un nombre premier $p$ ne figurant pas dans la liste $p_1, \cdots, p_n$. En déduire qu'il y a un nombre infini de nombres premiers.

(3) Soit $n > 1$. Montrer par récurrence forte[1] que $n$ s'écrit comme un produit $p_1 \cdots p_k$ de nombres premiers, éventuellement répétés. Indication: exploiter le résultat de la question (4.c). En déduire que tous les entiers $n > 1$ s'écrivent sous la forme

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

où $k \geq 1, p_1, \cdots, p_k$ sont des nombres premiers deux à deux distincts, $a_1, \cdots, a_k \geq 1$ sont des entiers ($k$ et les $p_i, a_i$ dépendent de $n$). On dit que c'est une *décomposition de $n$ en facteurs premiers.*

(4) Supposons que $n$ admet les deux décompositions en facteurs premiers suivantes:

$$n = p_1^{a_1} \cdots p_k^{a_k} = q_1^{b_1} \cdots q_r^{b_r}.$$

On suppose par ailleurs que les $p_i$ et les $q_i$ sont triés en ordre croissant. Montrer que $r = k$ et que pour tout $1 \leq i \leq k$, $p_i = q_i$ et $a_i = b_i$. On en déduit que chaque entier naturel $n \geq 1$ admet une *unique* décomposition en facteurs premiers.

Indication: Calculer $p_i \wedge n$ et $p_i^{a_i} \wedge n$.

# Partie III — Division euclidienne et algorithme d'Euclide

(1) Soient $n \geq 1$ et $q > 1$ deux entiers. Montrer qu'il existe un entier $k$ et un *unique* entier $r$ tel que $0 \leq r < q$ et $n = qk + r$. On parle de *division euclidienne de $n$ par $q$*. On appelle $r$ le *reste* et $k$ le *quotient dans la division euclidienne.*

[1] Dans une récurrence forte, au lieu de supposer dans l'hérédité la propriété vraie au rang précédent, on suppose la propriété vraie à tous les rangs précédents ($\mathcal{P}_k$ vraie pour tout $k < n$). Le principe de récurrence forte est équivalent au principe de récurrence (il n'y a donc rien à vérifier « en plus » d'une récurrence classique).

Indication: Commencer par montrer que $r$ existe (par exemple, par récurrence). Montrer ensuite l'unicité en supposant que $r_1$ et $r_2$ conviennent (déduire $r_1 = r_2$).

(2) Soient $n > 1$ et $m > 1$ deux entiers. On suppose que $n > m$.
   (a) On note $n = qm + r$ la division euclidienne de $n$ par $m$. Montrer que $n \wedge m = m \wedge r$
   (b) On définit une suite $(r_k)$ de la manière suivante:
      - $r_0 = n$
      - $r_1 = m$
      - $r_{k+1}$ est le reste de la division de $r_{k-1}$ par $r_k$, lorsque $r_k \neq 0$. Si $r_k = 0$, alors la suite s'arrête.

      Montrer que la suite $(r_k)$ est strictement décroissante. En déduire que c'est une suite finie (elle atteint 0), et en déduire que le dernier terme non-nul vaut $n \wedge m$.

      On appelle cette méthode de calcul du PGCD l'*algorithme d'Euclide*.
   (c) Appliquer l'algorithme d'Euclide pour calculer $33 \wedge 12$.

(3) Avec un raisonnement par récurrence, montrer que $r_k$ s'écrit $a_k n + b_k m$ pour des entiers $a_k, b_k$. En déduire qu'il existe $u, v \in \mathbb{Z}$ tels que

$$n \wedge m = un + vm.$$

   On appelle cette relation la *relation de Bézout*.

(4) (a) Montrer que $k \mid n, m$ si et seulement si $k \mid n \wedge m$.
   (b) Soient $n, m, \ell$ trois entiers, $\ell \neq 0$. Montrer que $n\ell \wedge m\ell = \ell(n \wedge m)$

(5) Soit $d \geq 1$ tel qu'il existe $u, v \in \mathbb{Z}$ satisfaisant $d = un + vm$. Montrer que $n \wedge m \mid d$.

# Partie IV — Congruences des entiers relatifs

On définit la relation de congruence $\equiv$ modulo $n$ sur $\mathbb{Z}$ de la manière suivante. Soit $n > 1$ un entier. Alors pour tous $a, b \in \mathbb{Z}$,

$$a \equiv b \pmod{n} \iff n \mid a - b$$

(1) Montrer que $n \mid m$ si et seulement si $m \equiv 0 \pmod{n}$.

(2) Montrer que si $a_1 \equiv a_2 \pmod{n}$ et $b_1 \equiv b_2 \pmod{n}$ alors $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$. Ainsi, la relation de congruence est compatible avec l'addition

(3) Montrer que si $a_1 \equiv a_2 \pmod{n}$ et $b_1 \equiv b_2 \pmod{n}$ alors $a_1 b_1 \equiv a_2 b_2 \pmod{n}$. Ainsi, la relation de congruence est compatible avec la multiplication. Un travail similaire montre (on l'admettra donc) que la relation de congruence est compatible avec toutes les propriétés des opérations usuelles sur les entiers (distributivité, soustraction, etc).

(4) Soit $n > 1$ et $m \in \mathbb{Z}$. Montrer qu'il existe un unique entier $0 \leq k < n$ tel que $m \equiv k \pmod{n}$. On dit que $k$ est le *résidu* de $m$ modulo $n$. Donner les résidus de $-1, 10$ et $-4$ modulo 5.

(5) Soient $n$ et $m$ deux nombres entiers positifs premiers entre eux. Montrer qu'il existe $k$ tel que

$$mk \equiv 1 \pmod{n}.$$

   On dit alors que $m$ est *inversible* modulo $n$, et $k$ est son *inverse modulaire*.

(6) Montrer que $m$ est inversible modulo $n$ si et seulement si $m$ et $n$ sont premiers entre eux.

# Partie V — Congruences modulo un nombre premier

Dans toute cette partie, $p$ est un nombre premier impair.

(1) Montrer que tous les entiers non multiples de $p$ sont inversibles modulo $p$.

(2) Soit $a$ non multiple de $p$.
   (a) Soient $u, v$ des entiers compris entre 0 et $p-1$ (bornes incluses). Montrer que
   $$ua \equiv va \pmod{p} \iff u = v$$
   (b) En déduire que la liste des résidus de $a, 2a, 3a, \cdots, (p-1)a$ est une permutation de la liste $(1, \cdots, p-1)$.
   (c) Montrer que
   $$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$
(3) (Petit théorème de Fermat) Déduire de ce qui précède que pour tout entier $n \in \mathbb{Z}$,
   $$n^p \equiv n \pmod{p}.$$
   Indication: Séparer les cas $n \equiv 0 \pmod{p}$ et $n \not\equiv 0 \pmod{p}$. Dans le second cas, montrer $a^{p-1} \equiv 1 \pmod{p}$.

# Partie VI — Théorème de Wilson

Dans cette partie, on veut montrer le théorème de Wilson: $p$ est premier si et seulement si
$$(p-1)! \equiv -1 \pmod{p}.$$

(1) Montrer que le théorème est vérifié pour $p = 2$.
(2) Supposons que $(p-1)! \equiv -1 \pmod{p}$. Montrer que tous les entiers non multiples de $p$ sont inversibles, et en déduire que $p$ est premier.
(3) Supposons maintenant que $p$ est un nombre premier impair.
   (a) Montrer que seuls $-1$ et 1 sont leur propre inverse modulaire.
   (b) Conclure.
(4) On donne $10! = 3\ 628\ 800$. D'après le théorème, 11 est-il premier ?

# Partie VII — Valuations $p$-adiques

Soit $p$ un nombre premier. On appelle *valuation $p$-adique* d'un entier $n \neq 0$ le plus grand entier $k$ tel que $p^k \mid n$. On la note $v_p(n)$. On prend la convention $v_p(0) = +\infty$.

(1) Montrer que $v_p(ab) = v_p(a) + v_p(b)$ pour tous $a, b > 0$.
(2) Montrer que si $b \mid a$, alors $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$
(3) Montrer que $v_p(a+b) \geq \min\big(v_p(a), v_p(b)\big)$
(4) Soient $a_1, b_1, a_2, b_2$ des entiers, $b_1$ et $b_2$ non nuls, tels que $a_1 b_2 = a_2 b_1$. Montrer que
   $$v_p(a_1) - v_p(b_1) = v_p(a_2) - v_p(b_2).$$
   En déduire que si $x = \frac{a}{b} \in \mathbb{Q} \setminus \{0\}$ pour $a, b \in \mathbb{Z} \setminus \{0\}$, on peut définir $v_p(x) = v_p(a) - v_p(b)$ sans que cette définition ne dépende du choix de $a$ et $b$. Ainsi, la valuation $p$-adique est définie sur $\mathbb{Q}$.

On appelle *partie entière* du réel $x \in \mathbb{R}$ l'unique entier $k \in \mathbb{N}$ tel que
$$x - 1 < k \leq x.$$

On la note $\lfloor x \rfloor$. On souhaite montrer la *formule de Legendre*, valable pour tout $p$ premier et pour tout entier naturel non nul $n$:

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots$$

(5) Montrer qu'il s'agit d'une somme finie: à partir d'un certain rang, tous les termes sont nuls.
(6) Montrer qu'il y a $\left\lfloor \frac{n}{p} \right\rfloor$ multiples de $p$ dans l'ensemble $\{1, 2, \cdots, n\}$. Combien y a-t-il de multiples de $p^2$ ?
(7) En utilisant $n! = 1 \times \cdots \times n$, montrer la formule de Legendre.

## Partie VIII — Équations diophantiennes linéaires

On appelle équation diophantienne toute équation donc on ne cherche que des solutions entières. Une équation diophantienne linéaire à $n$ variables $x_1, \cdots, x_n$ est une équation du type

$$a_1 x_1 + \cdots + a_n x_n = c$$

où $a_1, \cdots, a_n, c$ sont des entiers et pour laquelle on cherche des solutions $x_1, \cdots, x_n \in \mathbb{Z}$.

(1) Dans cette question, on note $(E)$ l'équation

$$ax + by = c,$$

où $a, b, c$ sont des entiers, $a$ et $b$ sont non nuls. On note $(E_h)$ l'équation $\frac{a}{d}x + \frac{b}{d}y = 0$ avec $d = a \wedge b$, que l'on appelle équation *homogène réduite* associée à $(E)$.
   (a) Montrer que $(E)$ admet une solution si et seulement si $a \wedge b$ divise $c$.
   (b) On suppose désormais que l'on connait une solution de $(E)$ notée $(x_0, y_0)$. Montrer que $(x + x_0, y + y_0)$ est solution de $(E)$ si et seulement si $(x, y)$ est solution de $(E_h)$.
   (c) Supposons que $(x, y)$ est solution de $(E_h)$. Montrer que $\frac{b}{d}$ divise $x$ et $\frac{a}{d}$ divise $y$. En déduire qu'il existe $k$ tel que

$$x = \frac{b}{d}k, \quad y = -\frac{a}{d}k.$$

   (d) Montrer que pour tout $k \in \mathbb{Z}$.

$$x = \frac{b}{d}k, \quad y = -\frac{a}{d}k$$

   est solution de $(E_h)$.
   (e) En déduire que les solutions de $(E)$ sont exactement les couples de la forme

$$\left(\frac{b}{d}k + x_0, -\frac{a}{d}k + y_0\right), \quad k \in \mathbb{Z}.$$

(2) Résoudre $-12x + 16y = 20$.

## Partie IX — Descente infinie dans une équation diophantienne

Soit $p$ un nombre premier et $n \geq 3$. On s'intéresse à l'équation diophantienne suivante:

$$x^n + py^n = p^2 z^n$$

(1) Montrer que $(0, 0, 0)$ est solution. On note $N(x, y, z) = |x| + |y| + |z|$. Montrer que si $(x, y, z) \neq (0, 0, 0)$, alors $N(x, y, z) > 0$.
(2) On suppose qu'il existe une solution différente de $(0, 0, 0)$. Montrer qu'il existe une solution $(x, y, z) \neq (0, 0, 0)$ telle que $N(x', y', z') \geq N(x, y, z)$ pour toute solution non nulle $(x', y', z')$. Dans la suite, $(x, y, z)$ désigne une telle solution.
(3) Montrer que $p$ divise $x^n$. En déduire qu'il existe $x'$ tel que

$$p^{n-1}x'^n + y^n = pz^n.$$

(4) Montrer que $p$ divise $y$ puis que $p$ divise $z$. En déduire qu'il existe une solution $(x', y', z')$ telle que $N(x', y', z') < N(x, y, z)$.
(5) Conclure que l'équation n'a qu'une seule solution.

# Partie X — Triplets pythagoriciens

On appelle *triplet pythagoricien* toute solution entière $(x, y, z)$ de l'équation diophantienne

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

On dit qu'un triplet pythagoricien $(x, y, z)$ est *primitif* lorsque $x \wedge y \wedge z = 1$.

(1) Soit $(x, y, z)$ un triplet pythagoricien et $d = x \wedge y \wedge z$. Montrer que $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ est un triplet pythagoricien primitif.
(2) (a) Soit $(x, y, z)$ un triplet pythagoricien primitif. Montrer que $x \wedge y = y \wedge z = x \wedge z = 1$.

Indication: Montrer que si un premier $p$ divise deux termes, alors il divise le troisième.

(b) Soit $(x, y, z)$ un triplet pythagoricien primitif. Montrer que $x$ et $y$ ont des parités différentes[2].

Indication: Montrer que si $x$ et $y$ sont impairs, alors $z^2 \equiv 2 \pmod 4$. Est-il possible pour un carré de valoir 2 modulo 4 ?

(c) Montrer que deux entiers naturels premiers entre eux dont le produit est un carré parfait (c'est à dire $k^2$ pour un entier $k$) sont eux-même des carrés parfaits.

Indication: Montrer que dans les décompositions en facteurs premiers, les exposants sont pairs.

(3) On va montrer que l'ensemble des triplets primitifs positifs $S$ pour lesquels $y$ est pair est donné par

$$(x, y, z) \in S \iff \exists m, n \in \mathbb{N}, m > n, m \wedge n = 1, m \not\equiv n \pmod 2, \begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases}$$

Soit $(x, y, z)$ un triplet primitif positif avec $y$ pair.

(a) Montrer que $z + x$ et $z - x$ sont pairs. En déduire que $r = \frac{z+x}{2}$ et $s = \frac{z-x}{2}$ sont premiers entre eux, puis que ce sont des carrés parfaits. On note $r = m^2$ et $s = n^2$.
(b) Montrer que

$$\begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases}$$

et que $m \wedge n = 1$. Montrer que $m$ et $n$ n'ont pas la même parité.
(c) Conclure.

On va maintenant adopter une approche géométrique pour résoudre le même problème.

(4) Montrer que $(x, y, z)$ est un triplet pythagoricien non nul si et seulement si $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$. En déduire qu'il y a une correspondance entre les triplets pythagoriciens non nuls primitifs et les points rationnels[3] $(x, y)$ du cercle unité.
(5) On note désormais $I$ le point $(-1, 0)$. Montrer que si $P = (x, y)$ est un point rationnel du cercle unité, alors la droite $(IP)$ a une pente rationnelle.
(6) Pour $t \in \mathbb{Q}$, on note $\mathcal{D}_t : y = t(x + 1)$.

[2] Parités différentes: l'un est pair, l'autre impair.
[3] Le point $(x, y)$ est rationnel lorsque $x, y \in \mathbb{Q}$

(a) Montrer que toutes les droites de pente rationnelles passant par $I$ s'écrivent $\mathcal{D}_t$ pour un $t \in \mathbb{Q}$.

(b) Soit $P = (x, y)$ un point d'intersection de $\mathcal{D}_t$ et du cercle unité $x^2 + y^2 = 1$. Montrer que

$$(x+1)\big((x-1) + t^2(x+1)\big) = 0.$$

En déduire que

$$x = -1 \quad \text{ou} \quad x = \frac{1-t^2}{1+t^2}.$$

Montrer que si $x = -1$, alors $P = I$. Sinon, montrer que $P$ a les coordonnées

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

(c) Montrer que pour $t \in \mathbb{Q}$, les points d'intersection de $\mathcal{D}_t$ et du cercle unité sont rationnels. En déduire que les points rationnels du cercle unité sont $I$ et tous les points

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right), \quad t \in \mathbb{Q}.$$

(d) Soit $t \in \mathbb{Q}$. Comme $t$ est rationnel, il s'écrit $t = \frac{m}{n}$ avec $m \in \mathbb{Z}$, $n \in N^*$, $m \wedge n = 1$. Montrer que

$$(m^2 - n^2, 2mn, m^2 + n^2)$$

est un triplet pythagoricien.

# Partie XI — Indicatrice d'Euler

On appelle indicatrice d'Euler la fonction $\varphi$ dont la définition est la suivante: pour tout $n > 0$ entier, $\varphi(n)$ est le nombre d'entiers entre 1 et $n-1$ qui sont premiers avec $n$.

(1) Soit $p$ un nombre premier.

(a) Montrer que $\varphi(p) = p - 1$

(b) Montrer pour tout $k > 1$, $\varphi\big(p^k\big) = (p-1)p^{k-1}$.

(2) Soit $p$ un nombre premier et $n$ un entier premier avec $p$. Soit $k \geq 1$ un entier. On appelle $E$ et $E'$ les ensembles suivants:

$$E = \big\{x \in \mathbb{N}^*, \quad x \wedge p^k n = 1 \quad \text{et} \quad x \leq p^k n\big\}$$
$$F = \big\{x \in \mathbb{N}^*, x \wedge n = 1 \quad \text{et} \quad x \leq p^k n\big\}$$

(a) Montrer que $E$ est inclus dans $F$.

(b) Montrer que $F$ possède $p^k\varphi(n)$ éléments.

(c) Montrer que $F \setminus E$ possède $p^{k-1}\varphi(n)$ éléments.

(d) En déduire que $\varphi\big(p^k n\big) = \varphi\big(p^k\big)\varphi(n)$

(3) Soient $u, v$ premiers entre eux. Montrer que $\varphi(uv) = \varphi(u)\varphi(v)$. On dit que $\varphi$ est *multiplicative*.

(4) Montrer que si $n = p_1^{k_1} \cdots p_r^{k_r}$ alors

$$\varphi(n) = n \times \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

(5) Dans cette question, on souhaite montrer l'identité suivante:

$$\forall n \in \mathbb{N}^*, \quad n = \sum_{d \mid n} \varphi(d),$$

où la somme porte sur l'ensemble des diviseurs $d$ de $n$.

(a) Montrer que l'identité est vérifiée pour $n = p$ avec $p$ un nombre premier, et pour $n = p^k$ pour $p$ premier et $k > 1$.

(b) Soient $m, n > 0$ deux entiers premiers entre eux. On suppose que la formule est vraie pour $m$ et pour $n$. Montrer que

$$mn = \sum_{d \mid mn} \varphi(d).$$

Indication: Montrer que les diviseurs de $mn$ s'écrivent de manière unique comme un produit $d_1 d_2$ où $d_1 \mid m$ et $d_2 \mid n$. Que dire de $d_1 \wedge d_2$ ?

(c) En déduire l'identité pour tout $n \in \mathbb{N}^*$.

(6) Dans cette question, pour $n > 1$ fixé et $x$ un entier, on note $\overline{x}$ le résidu de $x$ modulo $n$.

(a) Montrer que l'ensemble des résidus inversibles modulo $n$ est un ensemble $U = \{x_1, \cdots, x_k\}$ de taille $\varphi(n)$.

(b) Montrer que $xU := \{\overline{xx_1}, \overline{xx_2}, \cdots, \overline{xx_k}\} = U$. Indication: Montrer que chacun des $\overline{xx_i}$ est inversible modulo $n$ et que $\overline{xx_i} \neq \overline{xx_j}$ lorsque $i \neq j$.

(c) En déduire que $x_1 \cdot x_k \equiv x^k \cdot x_1 \cdots x_k \pmod{n}$

(d) Démontrer le *Théorème d'Euler*: pour tout $n > 1$ et tout $x$ premier avec $n$, $x^{\varphi(n)} \equiv 1 \pmod{n}$.

# Partie XII — Ordre multiplicatif

Soit $n > 1$ et $x$ un entier. On appelle *ordre multiplicatif* de $x$ modulo $n$ le plus petit entier $k \geq 1$ tel que $x^k \equiv 1 \pmod{n}$, lorsqu'un tel entier existe. Dans ce cas, on dit que $x$ admet un ordre modulo $n$, et on note $o_n(x)$ cet ordre.

(1) Supposons que $x$ et $n$ sont premiers entre eux.

(a) Montrer qu'il existe $1 \leq k_1 < k_2$ deux entiers tels que $x^{k_1} \equiv x^{k_2} \pmod{n}$.

(b) En déduire que $x^{k_2 - k_1} \equiv 1 \pmod{n}$. Conclure que $x$ admet un ordre modulo $n$.

(2) Supposons que $x$ et $n$ ne sont pas premiers entre eux. Est-il possible pour $x$ d'admettre un ordre modulo $n$ ?

(3) Soit $x$ un entier premier avec $n$.

(a) Supposons que $m$ est un multiple de $o_n(x)$. Montrer que $x^m \equiv 1 \pmod{n}$.

(b) Supposons désormais que $x^m \equiv 1 \pmod{n}$. Montrer que $o_n(x)$ divise $m$.

Indication: Faire la division euclidienne de $m$ par $o_n(x)$, et exploiter la minimalité de $o_n(x)$.

(c) Montrer que $o_n(x)$ divise $\varphi(n)$.

# Partie XIII — Racines primitives modulo un nombre premier

On appelle *racine primitive* modulo $n$ tout entier $x$ admettant un ordre modulo $n$ tel que $o_n(x) = \varphi(n)$. Dans toute cette partie, on prendra $n = p$ un nombre premier.

(1) Supposons que $g$ est une racine primitive modulo $p$.

(a) Montrer que pour tout $x$ premier avec $p$, il existe $0 \leq r < p - 1$ tel que $g^r \equiv x \pmod{p}$.

(b) Soit $k > 1$. Montrer que si $x$ admet un ordre, alors

$$o_p(x^k) = \frac{o_p(x)}{o_p(x) \wedge k}$$

(c) En déduire que $1 \leq x \leq p-1$ est générateur si et seulement si $r \wedge (p-1) = 1$ où $r$ est tel que $g^r \equiv x \pmod{p}$.

(d) Conclure qu'il y a exactement $\varphi(p-1)$ racines primitives modulo $p$.

Dans la question précédente, on a montré que s'il existe une racine primitive, alors il y en a exactement $\varphi(p-1)$. Il nous reste à montrer qu'il en existe bien une. Pour cela, on va montrer le résultat préliminaire suivant, appelé *Théorème de Lagrange*: Si $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ est un polynôme de degré $n \geq 1$ à coefficients entiers et tel que $a_n$ n'est pas multiple de $p$, alors $f(X)$ admet *au plus* $n$ racines non congrues[4] modulo $p$.

(2) On va montrer le théorème par récurrence sur $n$.

(a) Montrer que le théorème est vrai pour $n = 1$.

(b) Supposons que le théorème est vrai au rang $n-1$, et soit $f(X)$ un polynôme comme dans l'énoncé du théorème, de degré $n$. Supposons que $f(X)$ admet $n+1$ racines non congrues modulo $p$ que l'on note $c_0, \cdots, c_n$.

(i) Montrer

$$\begin{aligned} f(X) - f(c_0) = a_n(X-c_0)(X^{n-1} + X^{n-2}c_0 + \cdots + Xc_0^{n-2} + c_0^{n-1}) \\ + \quad a_{n-1}(X-c_0)(X^{n-2} + \cdots + Xc_0^{n-3} + c_0^{n-2}) \\ + \quad \vdots \\ + \quad a_1(X-c_0) \end{aligned}$$

puis en déduire qu'il existe un polynôme $g(X)$ de degré $n-1$ de coefficient dominant $a_n$ tel que $f(X) - f(c_0) = (X-c_0)g(X)$.

Indication: utiliser l'identité $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.

(ii) Montrer que $c_1, \cdots, c_n$ sont des racines de $g(X)$ modulo $p$.

(iii) Conclure en montrant que l'hypothèse selon laquelle $f(X)$ admet $n+1$ racines non congrues modulo $p$ est absurde.

(c) Conclure

On peut désormais montrer l'existence de racines primitives modulo $p$. On appelle *l'exposant* modulo $p$ l'entier $\lambda$ correspondant au maximum des valeurs de $o_p(k)$ pour $1 \leq k < p$.

(3) (a) On appelle *plus petit commun multiple*[5] *(PPCM)* de $m$ et $n$ des entiers non nuls la quantité

$$m \vee n = \frac{mn}{m \wedge n}.$$

Montrer que si $a$ et $b$ sont des entiers naturels tels que $o_p(a) = m$ et $o_p(b) = n$, alors

$$o_p(a \times b^{m \wedge n}) = m \vee n$$

Indication: On pourra exploiter la relation (1.b)

(b) Montrer que $\lambda$ vaut $o_p(1) \vee o_p(2) \vee \cdots \vee o_p(p-1)$ (on admet que l'ordre n'a pas d'importance dans le calcul du PPCM). En déduire qu'il existe $g$ un entier naturel tel que $o_p(g) = \lambda$, et donc que $\lambda \leq \varphi(p)$.

(c) Montrer que le polynôme $f(X) = X^\lambda - 1$ admet $p-1$ racines non congrues modulo $p$. En déduire $\lambda \geq p-1$.

(d) Conclure que $g$ est d'ordre $\varphi(p)$.

(4) Conclure sur le nombre de racines primitives modulo $p$.

[4] Autrement dit, il existe au plus $n$ entiers $0 \leq k < p$ tels que $f(k) \equiv 0 \pmod{p}$.

[5] On l'admettra: comme son nom l'indique, il désigne bien le plus petit entier multiple à la fois de $n$ et de $m$.

# Partie XIV — Racines primitives modulo une puissance d'un nombre premier

On a montré l'existence de racines primitives modulo un nombre premier $p$. On va montrer que pour $k > 1$, il existe une racine primitive modulo $p^k$.

(1) (Prérequis sur les polynômes[6]) Montrer que pour tout $N > 1$, il existe un polynôme $Q(X)$ à coefficients entiers tel que

$$(1+X)^N = 1 + NX + X^2 Q(X)$$

(2) Montrer que pour tout $n \in \mathbb{N}$,

$$(1+p)^{p^n} \equiv 1 + p^{n+1} \pmod{p^{n+2}}.$$

Indication: procéder par récurrence sur $n$.

(3) On rappelle que $\varphi(p^k) = (p-1)p^{k-1}$ (voir Partie XI).

(b) Montrer que $1+p$ est d'ordre $p^{k-1}$ modulo $p^k$. Indication: Calculer $(1+p)^{p^{k-2}}$ et $(1+p)^{p^{k-1}}$ modulo $p^k$.

(c) Soit $g$ une racine primitive modulo $p$. Montrer que pour tout $0 < \ell < p-1, p^k \nmid g^\ell - 1$, et que $p \mid g^{p-1} - 1$. En déduire qu'il existe $\ell$ tel que $g^\ell$ est d'ordre $p-1$ modulo $p^k$.

(d) Montrer que $(p-1) \wedge p^{k-1} = 1$. En déduire qu'il existe une racine primitive modulo $p^k$.

# Partie XV — Convolutions et inversion de Möbius

On appelle *fonction arithmétique* toute fonction $f : \mathbb{N}^* \longrightarrow \mathbb{R}$. Si $f$ et $g$ sont des fonctions arithmétiques, on définit leur convolution de la manière suivante:

$$\forall n \in \mathbb{N}^*, \quad (f \star g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

(1) Montrer que si $f$ et $g$ sont des fonctions arithmétiques, $f \star g = g \star f$.

(2) On note $\delta_1$ la fonction arithmétique telle que $\delta_1(1) = 1$ et $\delta_1(n) = 0$ pour tout $n > 1$. Soit $f$ une fonction arithmétique. Montrer que $f \star \delta_1 = f$.

(3) On note $\mathbb{1}$ la fonction arithmétique constante égale à 1 et $\mu$ la fonction arithmétique appellée *fonction de Möbius* définie par

$$\forall n \in \mathbb{N}^*, \mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par un carré parfait différent de 1} \\ 1 & \text{si } n \text{ est produit d'un nombre pair de nombres premiers distincts} \\ -1 & \text{si } n \text{ est produit d'un nombre impair de nombres premiers distincts.} \end{cases}$$

(a) Si $E$ est un ensemble fini, on note $\mathrm{card}(E)$ sa cardinalité (sa taille). Montrer que si $P = \{p_1, ..., p_r\}$ est un ensemble fini de nombres premiers deux à deux distincts, alors

$$\mu(p_1 \cdots p_r) = (-1)^{\mathrm{card}(P)}.$$

(b) Soit $n > 1$ un entier dont la décomposition en facteurs premiers est $p_1^{k_1} \cdots p_s^{k_s}$. Montrer que les diviseurs $d$ de $n$ tels que $\mu(d) \neq 0$ sont exactement les produits $p'_1 \cdots p'_r$ avec $\{p'_1, \cdots, p'_r\}$ un sous ensemble de $\{p_1, \cdots, p_s\}$.

(c) Notons $P$ l'ensemble des nombres premiers divisant $n > 2$. Montrer que

$$\sum_{d|n} \mu(d) = \sum_{D \subset P} (-1)^{\mathrm{card}(D)}$$

[6] Le lecteur ayant connaissance de la formule du binôme de Newton reconnaîtra immédiatement qu'il s'agit ici d'un énoncé plus faible de celle ci.

(d) En déduire que

$$\sum_{d|n} \mu(d) = k - \ell$$

où $k$ est le nombre de sous-ensembles de $P$ de cardinal pair et $\ell$ est le nombre de sous-ensenbles de $P$ de cardinal impair.

(e) Soit $p \in P$ fixé. On forme des couples $(S, S \cup \{p\})$ de sous-ensembles de $P$, avec $S$ un sous ensemble de $P$ ne contenant pas $p$. Montrer que chaque sous-ensemble de $P$ figure dans l'un des couples et uniquement dans celui ci, et que chaque couple contient un ensemble de cardinal pair et un ensemble de cardinal impair.

En déduire que $k = \ell$.

(f) Montrer que $\mu \star \mathbb{1} = \delta_1$.

(4) Soient $f, g, h$ trois fonctions arithmétiques. Montrer que $(f \star g) \star h = f \star (g \star h)$.

(5) En déduire la formule d'inversion de Möbius:

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} f(d) \iff \forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

(6) Montrer l'identité

$$\forall n \in \mathbb{N}^*, \quad \varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}.$$

# Partie XVI — Résidus quadratiques et symbole de Legendre

On appelle résidu quadratique modulo $n > 1$ les entiers $0 \leq k < n$ tels qu'il existe $x \in \mathbb{N}$ satisfaisant $x^2 \equiv k \pmod{n}$. On dit que $x$ est une racine carrée de $k$ modulo $p$.

Dans toute la suite, $p$ et $q$ sont des nombre premier **impairs**.

(1) Montrer que pour tout $a, b$ entiers,

$$ab \equiv 0 \pmod{p} \Rightarrow a \equiv 0 \pmod{p} \quad \text{ou} \quad b \equiv 0 \pmod{p}.$$

(2) En déduire que pour $k \in \mathbb{N}$, $x^2 \equiv k \pmod{p}$ admet au plus deux solutions dans l'ensemble $\{0, \cdots, p-1\}$.

(3) Soit $g$ une racine primitive modulo $p$.

(a) Montrer que le résidu modulo $p$ de $g^{2m}$ est un résidu quadratique modulo $p$ pour tout $m \geq 0$. Combien il y a-t-il de résidus de cette forme ?

(b) Montrer que le résidu modulo $p$ de $g^{2m+1}$ n'est pas un résidu quadratique modulo $p$, pour tout $m \geq 0$. Combien y a-t-il de résidus de cette forme ?

(c) En déduire qu'il y a exactement $\frac{p-1}{2}$ résidus quadratiques.

(d) Montrer que pour un résidu non nul $k$, on a

$$k^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} \text{ si } k \text{ est un résidu quadratique modulo } p \\ -1 \pmod{p} \text{ si } k \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

Indication: Montrer que $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Lorsque $p$ est un nombre premier impair, et $k$ un entier non multiple de $p$, on appelle *symbole de Legendre* l'entier défini par

$$\left(\frac{k}{p}\right) = \begin{cases} 1 & \text{si le résidu de } k \text{ est un résidu quadratique modulo } p \\ -1 & \text{si le résidu de } k \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

(4) Montrer les relations suivantes:
   (a) Pour $a, b$ non nuls modulo $p$,
   $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$
   (b)
   $$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod 4 \\ -1 & \text{si } p \equiv 3 \pmod 4 \end{cases}$$

(5) On va montrer le *lemme de Gauss* pour les symboles de Legendre: Si $a$ est un entier non multiple de $p$ et si $s$ est le nombre de résidus modulo $p$ des entiers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ qui sont strictement supérieurs à $\frac{p}{2}$, alors
   $$\left(\frac{a}{p}\right) = (-1)^s.$$
   On note $u_1, \cdots, u_s$ les résidus des entiers $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ qui sont supérieurs (strictement) à $\frac{p}{2}$. On note $v_1, \cdots, v_t$ les résidus restants.
   (a) Montrer que les $u_i, v_i$ sont inversibles modulo $p$, puis que les $u_i$ sont deux à deux distincts, de même que les $v_i$ sont deux à deux distincts.
   (b) Montrer qu'il n'existe pas de couple $(i, j)$ tel que $p - u_i \equiv v_j \pmod p$. En déduire que les entiers $p - u_1, \cdots, p - u_s, v_1, \cdots, v_s$ sont exactement les entiers $1, 2, \cdots, \frac{p-1}{2}$ (éventuellement dans le désordre).
   (c) Montrer que
   $$(-1)^s u_1 u_2 \cdots u_s v_1 v_2 \cdots, v_t \equiv \left(\frac{p-1}{2}\right)! \pmod p.$$
   (d) Montrer que
   $$u_1 \cdots u_s v_1 \cdots v_t \equiv a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p.$$
   (e) Conclure.

(6) Nous allons montrer que
   $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-8}{2}}.$$
   (a) Montrer que
   $$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor}.$$
   Indication: Utiliser le lemme de Gauss.
   (b) Montrer que nour tout entier $n$,
   $$\frac{n-1}{2} - \left\lfloor \frac{n}{4} \right\rfloor = \frac{n^2-1}{8} \pmod 2 \iff \frac{(n+8)-1}{2} - \left\lfloor \frac{n+8}{4} \right\rfloor \equiv \frac{(n+8)^2-1}{8} \pmod 2.$$
   (c) En déduire que pour tout entier impair $n$,

$$\frac{n-1}{2} - \left\lfloor \frac{n}{4} \right\rfloor = \frac{n^2-1}{8} \pmod 2.$$

(d) Conclure.

# Partie XVII — Loi de réciprocité quadratique

Dans toute cette partie, $p$ et $q$ désignent des premiers impairs distincts. L'objectif est de montrer le résultat suivant, connu sous le nom de *loi de réciprocité quadratique*:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

(1) (*Lemme préliminaire*) Dans cette question, $a$ est un entier **impair** non divisible par $p$. On va montrer

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)},$$

avec

$$T(a,b) = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor.$$

On reprend les notations utilisées pour le lemme de Gauss (question (XVI.5)): on note $u_1, \cdots, u_s$ (resp. $v_1, \cdots, v_t$) les résidus modulo $p$ des entiers $a, 2a, \cdots, \frac{p-1}{2}a$ supérieurs à $\frac{p}{2}$ (resp. inférieurs à $\frac{p}{2}$).

(a) Montrer que

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j.$$

Indication: Faire la division euclidienne de $ja$ par $\left\lfloor \frac{ja}{p} \right\rfloor$, pour chaque $j$.

(b) Montrer

$$\sum_{j=1}^{\frac{p-1}{2}} j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j$$

(c) En déduire que

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} j = pT(a,p) - ps + 2\sum_{k=1}^{s} u_j$$

(d) Conclure en montrant que $T(a,p) \equiv s \pmod 2$.

(2) (*Preuve de la loi de réciprocité quadratique*) Soient $p, q$ deux premiers impairs distincts

(a) Montrer qu'il y a $\frac{p-1}{2} \cdot \frac{q-1}{2}$ paires d'entiers $(x,y)$ telles que $1 \leq x \leq \frac{p-1}{2}$ et $1 \leq y \leq \frac{q-1}{2}$.

(b) Montrer que pour de telles paires, on a jamais $qx = py$.

(c) Montrer qu'il y a $T(q,p)$ paires telles que $qx > py$.

(d) En déduire que

$$T(q,p) + T(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

(e) Conclure.

(3) Montrer que $103x + 78 = y^2$ n'a pas de solutions entières $(x, y)$. On admettra que 103 est un nombre premier.

# Partie XVIII — Lifting the exponent

On appelle *Lifting the exponent lemma* ou *lemme LTE* le résultat suivant: si $p$ est un premier impair divisant $a - b$ mais ne divisant ni $a$ ni $b$, alors

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n).$$

On rappelle l'identité suivante: pour tous $a, b$ et tout $n > 0$,

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

(1) Donner une justification rapide de l'identité rappelée.

(2) Dans cette question, $p \nmid n$, et satisfait les conditions du lemme LTE. Montrer que

$$a^{n-1} + a^{n-2}b + \cdots + b^{n-1} \equiv na^{n-1} \pmod{p}.$$

En déduire que $p$ ne divise pas $a^{n-1} + a^{n-2}b + \cdots + b^{n-1}$, et conclure que le lemme LTE est vrai lorsque $p$ ne divise pas $n$.

(3) Soit $p$ un premier impair divisant $a - b$ mais ne divisant ni $a$ ni $b$.

(a) Montrer que $p$ divise $a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$.

(b) Notons $k = \frac{b-a}{p}$ (c'est un entier). Montrer que pour $1 \leq t < p$, on a

$$b^t a^{p-1-t} \equiv a^{p-1} + tkpa^{p-2} \pmod{p^2}.$$

Indication: Utiliser la question (XIV.1) avec $X = \frac{kp}{a}$

(c) En déduire que

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \not\equiv 0 \pmod{p^2}$$

puis que le lemme LTE est vrai pour $n = p$.

Indication: On pourra utiliser librement que $1 + 2 + \cdots + (p - 1) = \frac{p(p-1)}{2}$.

(d) Notons $\alpha = v_p(n)$. Montrer que

$$v_p(a^n - b^n) = v_p(a^{p^\alpha} - b^{p^\alpha}).$$

En déduire que le lemme LTE est vrai pour tout $n$.