Un **anneau $\boldsymbol{A}$ est ordonné par** $\leq$ ssi $\begin{cases} \forall x,y,z \in A\ x \leq y \Rightarrow x+z \leq y+z \\ \forall x,y \in A\ \ 0 \leq x \text{ et } 0 \leq y \Rightarrow 0 \leq x \times y \end{cases}$

Un **anneau $\boldsymbol{A}$ est totalement ordonné par** $\leq$ ssi $(A, \leq)$ est ordonné et $\leq$ ordre total.

Un **anneau $\boldsymbol{A}$ est archimédien** ssi $\forall \varepsilon \in A | \varepsilon > 0\ \ \forall a \in A\ \exists n \in \mathbb{Z}\ \ n\varepsilon \geq a$

Modèle de $\mathbb{Z}$.

Existence : $\exists (\mathbb{Z}, +, \times, \leq)$ vérifiant les propriétés :

$(\mathbb{Z}, +, \times, \leq)$ est un anneau commutatif, intègre, totalement ordonné, archimédien.

Toute partie non vide de $\mathbb{Z}$ majorée admet un maximum pour $\leq$.

TODO vérifier que ce sont bien les propriétés fondamentales.

Arithmétique dans $\mathbb{Z}$

En posant $\mathbb{N} = \{n \in \mathbb{Z} \mid n \geq 0\}$, $s : \mathbb{N} \to \mathbb{N} : n \mapsto n+1$

$(\mathbb{N}, 0, s)$ est un modèle de Peano valide. $+_{|\mathbb{N}\times\mathbb{N}} = +_{\mathbb{N}}$, $\times_{|\mathbb{N}\times\mathbb{N}} = \times_{\mathbb{N}}$, $\leq_{|\mathbb{N}\times\mathbb{N}} = \leq_{\mathbb{N}}$

$\mathbb{N} \subseteq \mathbb{Z}$

$\mathbb{Z} = \mathbb{N} \cup -\mathbb{N}$

Toute partie non vide de $\mathbb{Z}$ majorée admet un maximum pour $\leq$.

Toute partie non vide de $\mathbb{Z}$ minorée admet un minimum pour $\leq$.

$\mathbb{Z}$ n'est ni majoré ni minoré pour $\leq$.

$\forall x \in \mathbb{Z}\ \ x \in \{-1,1\} \Leftrightarrow \exists\, !\, x^{-1} \in \mathbb{Z}\ x \times x^{-1} = x^{-1} \times x = 1$

$1^{-1} = 1,\ (-1)^{-1} = -1$

Régularité

Si $x = y$ alors $x + z = y + z$ et réciproquement.

Si $x = y$ alors $x - z = y - z$ et réciproquement.

Si $x = y$ alors $xz = yz$. Réciproque fausse si $z = 0$.

Si $xz = yz$ et $z \neq 0$ alors $x = y$

Si $x \leq y$ alors $x + z \leq y + z$ et réciproquement.

Si $x \leq y$ alors $x - z \leq y - z$ et réciproquement.

Si $x \leq y$ et $z \geq 0$ alors $xz \leq yz$. Réciproque fausse si $z = 0$.

Si $xz \leq yz$ et $z > 0$ alors $x \leq y$.

Si $x < y$ alors $x + z < y + z$ et réciproquement.

Si $x < y$ alors $x - z < y - z$ et réciproquement.

Si $x < y$ et $z > 0$ alors $xz < yz$.

Si $xz < yz$ et $z > 0$ alors $x < y$.

Valeur absolue.

Pour $x \in \mathbb{Z}$, $|x| = \begin{cases} x \text{ si } x \geq 0 \\ -x \text{ si } x < 0 \end{cases}$

$\forall x \in \mathbb{Z}\ \ |x| \geq 0$

Deux entiers $x, y \in \mathbb{Z}$ sont de même signe ssi $xy = |x||y|$

Deux entiers $x, y \in \mathbb{Z}$ sont de signe contraire ssi $xy = -|x||y|$

Divisibilité.

Un entier non nul $\boldsymbol{b} \in \mathbb{Z}^*$ **divise** $\boldsymbol{a} \in \mathbb{Z}$ **/** $\boldsymbol{b}|\boldsymbol{a}$ **/** $\boldsymbol{a}$ **est un multiple de** $\boldsymbol{b}$ **/** $\frac{\boldsymbol{a}}{\boldsymbol{b}} \in \mathbb{Z}$ ssi $\exists q \in \mathbb{Z}\ qb = a$.

Dans ce cas q est unique, est appelé **quotient de $\boldsymbol{a}$ par $\boldsymbol{b}$**, et noté $q = \frac{\boldsymbol{a}}{\boldsymbol{b}}$

L'ensemble des diviseurs d'un entier $n \in \mathbb{Z}$ est $\boldsymbol{D}(\boldsymbol{n}) = \{d \in \mathbb{Z}^* \mid\ d|n\}$

L'ensemble des diviseurs positifs d'un entier $n \in \mathbb{Z}$ est $\boldsymbol{D}^+(\boldsymbol{n}) = \{d \in \mathbb{N}^* \mid d|n\}$

L'ensemble des diviseurs négatifs d'un entier $n \in \mathbb{Z}$ est $\boldsymbol{D}^-(\boldsymbol{n}) = \{d < 0 \mid d|n\}$

$\left(D^+(n), D^-(n)\right)$ est une partition de $D(n)$. $D^-(n) = -D^+(n)$ donc $|D^+(n)| = |D^-(n)|$

L'ensemble des multiples d'un entier $n \in \mathbb{Z}$ est $\boldsymbol{n}\mathbb{Z} = \{m \in \mathbb{Z}^* \mid n|m\} = \{kn : k \in \mathbb{Z}\}$

L'ensemble des multiples positifs d'un entier $n \in \mathbb{Z}$ est $n\mathbb{N} = \{kn : k \geq 0\}$

L'ensemble des multiples négatifs d'un entier $n \in \mathbb{Z}$ est $-n\mathbb{N} = \{-kn : k \geq 0\}$

$a \in b\mathbb{Z} \Leftrightarrow \frac{a}{b} \in \mathbb{Z} \Leftrightarrow b|a \Leftrightarrow b \in D(a)$

$D(a) = D(a') \Leftrightarrow a = \pm a'$

$a\mathbb{Z} = a'\mathbb{Z} \Leftrightarrow a = \pm a'$

Division euclidienne. Pour $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, $\exists\,!\,(q,r) \in \mathbb{Z}^2$ $\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$

q est **le quotient de la division euclidienne de $\boldsymbol{a}$ par $\boldsymbol{b}$**, r est **le reste de la division euclidienne de $\boldsymbol{a}$ par $\boldsymbol{b}$**. On note $q = a \,\mathbf{quo}\, b, r = a \,\mathbf{mod}\, b$.

Congruences.

Un entier $a \in \mathbb{Z}$ est congru à un entier $b \in \mathbb{Z}$ modulo un entier $n \in \mathbb{N}^*$, et on note $\boldsymbol{a \equiv b \bmod n}$ ssi $a - b \in n\mathbb{Z}$ ssi $n|(a-b)$

Etre congru modulo $n \in \mathbb{N}^*$ est une relation d'équivalence sur $\mathbb{Z}$.

Si $a \equiv b \bmod n$ alors $a + c \equiv b + c \bmod n$

Si $a \equiv b \bmod n$ alors $a - c \equiv b - c \bmod n$

Si $a \equiv b \bmod n$ alors $ac \equiv bc \bmod n$

Si $\begin{cases} a \equiv b \bmod n \\ c \equiv d \bmod n \end{cases}$ alors $ac \equiv bd \bmod n$

Si $a \equiv b \bmod n$ alors $\forall k \in \mathbb{N}\ a^k \equiv b^k \bmod n$

Si $r = a \bmod b$ est le reste de la DE de a par b, alors $a \equiv r \bmod n$

Si $a^p \equiv 1 \bmod n$ avec $p \in \mathbb{N}^*$ alors $\forall k \in \mathbb{N}\ \ a^k \equiv a^r \bmod n$ avec r reste de la DE de k par p.

PGCD.

Le plus grand diviseur commun (PGCD) de deux entiers non nuls $a, b \in \mathbb{Z}^*$ est noté $\boldsymbol{a \wedge b}$ et peut se définir par l'une des définitions équivalentes suivantes :

$\exists!\, a \wedge b \in \mathbb{Z}\ \ a \wedge b = \max D(a) \cap D(b)$

$\exists!\, a \wedge b \in \mathbb{N}\ \ D(a) \cap D(b) = D(a \wedge b)$

$\exists!\, a \wedge b \in \mathbb{Z}\ \ a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$

Le PGCD est toujours strictement positif. $a \wedge b \in \mathbb{N}^*,\ \ a \wedge b = |a| \wedge |b|$

Le PGCD est associatif et commutatif. $(a \wedge b) \wedge c = a \wedge (b \wedge c).\ \ a \wedge b = b \wedge a.$

On peut donc généraliser la définition du PGCD pour n variables. $\bigwedge_{i=1}^{n} a_i$

$\bigwedge_{i=1}^{n} a_i = \max \bigcap_{i=1}^{n} D(a_i), \quad \bigcap_{i=1}^{n} D(a_i) = D(\bigwedge_{i=1}^{n} a_i),\ \sum_{i=1}^{n} a_i\mathbb{Z} = (\bigwedge_{i=1}^{n} a_i)\mathbb{Z}$

Etre un diviseur commun, c'est diviser le PGCD. $\forall d \in \mathbb{Z}^*\ \ d|a$ et $d|b \Rightarrow d|(a \wedge b)$

$\forall k \in \mathbb{Z}^*\ \ ka \wedge kb = |k|(a \wedge b)$

PPCM.

Le plus petit multiple commun (PPCM) de deux entiers non nuls $a, b \in \mathbb{Z}^*$ est noté $\boldsymbol{a \vee b}$ et peut se définir par l'une des définitions équivalentes suivantes :

$\exists!\, a \vee b \in \mathbb{Z}\ \ a \vee b = \min a\mathbb{Z} \cap b\mathbb{Z} \cap \mathbb{N}^*$

$\exists!\, a \vee b \in \mathbb{Z}\ \ a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$

$\exists!\, a \vee b \in \mathbb{Z}\ \ a \vee b = \frac{|a||b|}{a \wedge b}$

Le PPCM est toujours strictement positif. $a \vee b \in \mathbb{N}^*,\ \ a \vee b = |a| \vee |b|$

Le PPCM est associatif et commutatif. $(a \vee b) \vee c = a \vee (b \vee c).\ \ a \vee b = b \vee a.$

On peut donc généraliser la définition du PPCM pour n variables. $\bigvee_{i=1}^{n} a_i$

$\bigvee_{i=1}^{n} a_i = \min \mathbb{N}^* \cap \bigcap_{i=1}^{n} a_i\mathbb{Z}, \quad \bigcap_{i=1}^{n} a_i\mathbb{Z} = (\bigvee_{i=1}^{n} a_i)\mathbb{Z}$

Etre un multiple commun, c'est être multiple du PPCM. $\forall m \in \mathbb{Z}^*\ \ a|m$ et $b|m \Rightarrow (a \vee b)|m$

$\forall k \in \mathbb{Z}^*\ \ ka \vee kb = |k|(a \vee b)$

$(a \wedge b)(a \vee b) = ab$

Nombres premiers entre eux.

Deux entiers $a, b \in \mathbb{Z}^*$ sont premiers entre eux ssi $a \wedge b = 1$ ssi $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$

n entiers $(a_i)_{1 \leq i \leq n} \in \mathbb{Z}^{*n}$ sont premiers entre eux dans leur ensemble ssi $\bigwedge_{i=1}^{n} a_i = 1$ ssi $\sum_{i=1}^{n} a_i\mathbb{Z} = \mathbb{Z}$

Théorème de Bézout. $a \wedge b = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}\ \ au + bv = 1$

Théorème de Bézout n. $\bigwedge_{i=1}^{n} a_i = 1 \Leftrightarrow \exists u_1, \dots, u_n \in \mathbb{Z}\ \ a_1u_1 + \cdots + a_nu_n = 1$

Etre des nombres premiers entre eux dans leur ensemble, signifie avoir une combinaison linéaire qui donne 1.

Relation de Bézout. $d = a \wedge b \Leftrightarrow \exists u, v \in \mathbb{Z}\ \begin{cases} au + bv = d \\ d|a \text{ et } d|b \end{cases}$

Relation de Bézout n. $d = \bigwedge_{i=1}^{n} a_i \Leftrightarrow \exists u_1, \dots, u_n \in \mathbb{Z}\ \begin{cases} a_1u_1 + \cdots + a_nu_n = d \\ \forall i\ \ d|a_i \end{cases}$

Caractérisation du PGCD. $d = a \wedge b \Leftrightarrow \exists a', b' \in \mathbb{Z}\ \begin{cases} a = a'd,\ b = b'd \\ a' \wedge b' = 1 \end{cases}$

Caractérisation du PGCD n. $d = \bigwedge_{i=1}^{n} a_i \Leftrightarrow \exists a'_1, \dots, a'_n \in \mathbb{Z}\ \begin{cases} \forall i\ \ a_i = a'_i d \\ \bigwedge_{i=1}^{n} a'_i = 1 \end{cases}$

Théorème de Gauss. $\forall a, b, c \in \mathbb{Z}^*$ si $\begin{cases} a|bc \\ a \wedge b = 1 \end{cases}$ alors $a|c$

Autrement dit si $\frac{b \times \dots}{a} \in \mathbb{Z}$ et $a \wedge b = 1$, alors $\frac{\dots}{a} \in \mathbb{Z}$

Si un entier divise un produit, et est premier avec l'un des facteurs, alors il divise le produit des autres facteurs.

Corollaire 1 de Gauss. $\begin{cases} a \wedge d = 1 \\ b \wedge d = 1 \end{cases} \Leftrightarrow ab \wedge d = 1$

Corollaire 1 de Gauss n. $\forall i\ \ a_i \wedge d = 1 \Leftrightarrow (\prod_{i=1}^{n} a_i) \wedge d = 1$

Un entier est premier avec chacun des entiers d'une famille, ssi il est premier avec leur produit.

Corollaire 2 de Gauss. Si $\begin{cases} a \wedge b = 1 \\ a|m \text{ et } b|m \end{cases}$ alors $ab|m$

Corollaire 2 de Gauss n. Si $\begin{cases} \bigwedge_{i=1}^{n} a_i = 1 \\ \forall i\ \ a_i|m \end{cases}$ alors $ab|m$

Un multiple commun à des entiers premiers entre eux dans leur ensemble, est un multiple de leur produit.

Algorithme d'Euclide. Permet de calculer le PGCD de 2 entiers.

Pour $a, b \in \mathbb{N}^*, 0 < b \leq a$, on peut construire une suite $(r_k)_{k \in \mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ par récurrence :

$r_0 = a,\ r_1 = b$

$\forall k \geq 2$ on pose $\begin{cases} r_k = 0 \text{ si } r_{k-1} = 0 \\ r_k \text{ reste de la DE de } r_{k-2} \text{ par } r_{k-1} \text{ si } r_{k-1} \neq 0 \end{cases}$

$\exists! n \in \mathbb{N}^*\ \ r_n \neq 0$ et $r_{n+1} = 0$. L'algorithme d'Euclide s'arrête toujours. $\forall k \geq n+1\ r_k = 0$.

$r_n = a \wedge b$

Nombres premiers.

Un **entier $n \in \mathbb{Z}$ est inversible** ssi $n \in \{-1, 1\}$.

Deux éléments x, y de $\mathbb{Z}$ sont associés ssi $y = \pm x$ ssi il existe un inversible λ tel que $y = \lambda x$

$\forall n \in \mathbb{N}$ 1 divise n, et n divise n càd $\{1, n\} \subseteq D^+(n)$

Un **entier naturel $p \in \mathbb{N}^*$ est premier/irréductible**

ssi $p \geq 2$ et $\forall d \in \mathbb{N}^*\ \ d|p \Rightarrow d = 1$ ou $d = p$.

ssi $p \geq 2$ et $D^+(p) = \{1, p\}$ càd il est ≥ 2 et ses seuls diviseurs positifs sont 1 et lui-même.

ssi $|D^+(p)| = 2$ càd il a exactement 2 diviseurs positifs.
ssi $\forall n \in \mathbb{N}^*\ \neg(p|n) \Rightarrow p \wedge n = 1$ càd il est premier avec tout entier naturel qu'il ne divise pas.
ssi $\forall n \in [\![1, p-1]\!]\ p \wedge n = 1$ càd il est premier avec tous les naturels non 0 strictement inférieurs.
On peut généraliser ces définitions à $\mathbb{Z}$.
Un **entier $p \in \mathbb{Z}^*$ est premier/irréductible**
ssi $p \in \mathbb{N}$ est un naturel premier, ou $-p \in \mathbb{N}$ est un naturel premier.
ssi $|D^+(p)| = 2$
ssi $p \notin \{1, -1\}$ et $\forall x, y \in \mathbb{Z}\ \ p = xy \Rightarrow x = \pm 1$ ou $y \pm 1$ càd p est non inversible et en écrivant p comme produit de deux facteurs, l'un doit être inversible, et l'autre doit être associé à p.
ssi $p \notin \{1, -1\}$ et $\forall x, y \in \mathbb{Z}$ si $p|xy$ alors $p|x$ ou $p|y$
ssi l'idéal $p\mathbb{Z}$ est premier.
Ces définitions peuvent encore se généraliser dans des anneaux.
En général, les questions de divisibilité ne dépendent pas du signe. On se restreint à définir et étudier les premiers uniquement dans $\mathbb{N}$.

Propriétés des nombres premiers.

On note $\mathcal{P}$ l'ensemble des entiers naturels premiers.
Un entier premier est ≥ 2 n'a pour diviseurs positifs que lui-même et 1, donc exactement deux.
Un entier premier est premier avec tout entier naturel qu'il ne divise pas.
Un entier premier est premier avec tous les naturels non nuls strictement inférieurs.
Lemme d'Euclide. Un entier premier qui divise un produit, divise l'un des facteurs.
L'ensemble des nombres premiers est infini.
Tout entier ≥ 2 (en valeur absolue) admet au moins un diviseur premier.
La valuation p-adique d'un entier $n \in \mathbb{Z}$, notée $v_p(n)$ est la plus grande puissance de p qui divise n, elle vaut 0 ssi p ne divise pas n.

Décomposition en facteurs premiers.

$$\forall n \in \mathbb{N}^* |\ n \geq 2\ \ \exists! r \in \mathbb{N}\ \exists! p_1, \dots, p_r, \alpha_1, \dots, \alpha_r \in \mathbb{N} \text{ tels que } \begin{cases} r \geq 1 \\ \forall i \in [\![1, r]\!]\ p_i \text{ nombre premier} \\ \forall i \in [\![1, r-1]\!]\ p_i < p_{i+1} \\ \forall i \in [\![1, r]\!]\ \alpha_i \geq 1 \\ n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \end{cases}$$

En notant $(P_i)_{i \in \mathbb{N}^*} = (P_1, P_2, \dots) = (2,3,5, \dots)$ la suite croissante des naturels premiers,

$$\forall n \in \mathbb{N}^* |\ n \geq 2\ \ \exists! s \in \mathbb{N}\ \exists! v_1, \dots, v_s \in \mathbb{N}\ \begin{cases} s \geq 1 \\ v_s \geq 1 \\ n = P_1^{v_1} P_2^{v_2} \dots P_s^{v_s} = 2^{v_1} 3^{v_2} \dots \end{cases}$$

Dans ce cas v_i n'est autre que la valuation de P_i dans n.
Un entier $n \geq 2$ peut s'écrire $n = \prod_{k=1}^{\infty} P_k^{v_{P_k}(n)} = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ puisque à partir d'un certain rang les valuations sont nulles.

Conséquences.

Le nombre de diviseurs positifs d'un entier naturel $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} \geq 2$ est $|D^+(n)| = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$
Pour $a = P_1^{v_1} P_2^{v_2} \dots P_s^{v_s} \geq 2$ et $b = P_1^{v'_1} P_2^{v'_2} \dots P_{s'}^{v'_{s'}}$ on peut calculer PGCD et PPCM.
$a \wedge b = P_1^{\min(v_1, v'_1)} P_2^{\min(v_2, v'_2)} \dots P_{\min(s,s')}^{\min(v_s, v'_s)}$
$a \vee b = P_1^{\max(v_1, v'_1)} P_2^{\max(v_2, v'_2)} \dots P_{\max(s,s')}^{\max(v_s, v'_s)}$

Théorème d'Euler. $\forall n \geq 2\ \forall a \in \mathbb{Z}\ a^{\phi(n)} \equiv 1 \bmod n$

$\forall n \geq 2\ \forall a \in \mathbb{Z}|\ a \wedge n = 1$, alors $a^{n!} \equiv 1 \bmod n$

Petit théorème de Fermat.

$\forall p$ premier $\forall a \in \mathbb{Z}$ Si p ne divise pas a alors $a^{p-1} \equiv 1 \bmod p$

$\forall p$ premier $\forall a \in \mathbb{Z}\ a^p \equiv a \bmod p$

Théorème des restes chinois

Dans Z. Si $n_1, \dots, n_k \in \mathbb{Z}$ sont 2 a 2 premiers entre eux et $n = n_1 \dots n_k$ alors

l'application $\frac{Z}{nZ} \to \frac{Z}{n_1 Z} \times \dots \frac{Z}{n_k Z} : x \mapsto \left(\overline{x}^1, \dots, \overline{x}^k\right)$ est un isomorphisme d'anneaux.

Wilson. Un entier $p \geq 2$ est premier ssi $(p-1)! \equiv 1 \bmod p$

Exercices.

Un **nombre de Mersenne** est un nombre de la forme $\boldsymbol{M_p} = 2^p - 1$ avec p premier.

Un **nombre de Fermat** est un nombre premier de la forme $2^n - 1$ avec $n \in \mathbb{N}$.

Pour un nombre de Fermat $2^n - 1$, on a $n = 2^k$. On ne sait pas s'il y a un nombre de Fermat pour $k \geq 5$.

Les nombres de Fermat sont premiers entre eux 2 à 2. Il y a une infinité de nombre premiers.

Une racine rationnelle d'un polynôme de $\mathbb{Z}[X]$ est nécessairement entière.

La racine n-ieme d'un entier est soit entière soit irrationnelle.

Il y a une infinité de nombres premiers de la forme $6k - 1$, $k \in \mathbb{N}^*$.

Pour $a, b \in \mathbb{N}^*, a \wedge b = 1$, il existe une infinite de nombre premiers de la forme $ak + b, k \in \mathbb{N}$.

Il n'y pas de $P \in \mathbb{Z}[X]$ tel que $\forall n \in \mathbb{N}\ P(n)$ premier.

En notant $\pi(x)$ le nombre de premiers inferieurs a x, alors $\pi(x) \sim_{x \to \infty} \frac{x}{\ln x}$

Pour $n \in \mathbb{N}^*$ on note $\boldsymbol{\sigma(n)} = \sum_{d \in D^+(n)} d$ la somme des diviseurs positifs de n.

Un **entier $\boldsymbol{n} \in \mathbb{N}^*$ est parfait** s'il est la somme de ses diviseurs stricts, ssi $\sigma(n) = 2n$

Pour $n, m \in \mathbb{N}^*, n \wedge m = 1$, alors $\sigma(nm) = \sigma(n)\sigma(m)$

Si $2^k - 1$ est premier, alors $2^{k-1}\left(2^k - 1\right)$ est parfait. Si n est parfait pair, alors $n = 2^{k-1}\left(2^k - 1\right)$

Un nombre parfait impair s'il existe doit être de la forme $n = p^{1+4\alpha}Q^2$ avec p premier, $p \equiv 1 \bmod 4$, $\alpha \in \mathbb{N}$, $Q \in \mathbb{N}^*$ avec $p \wedge Q = 1$. Un parfait impair a au moins 3 facteurs premiers distincts.

On ne connait pas de parfait impair, on ne sait pas s'il y en a.

Théorème de Liouville. Pour un entier $p \geq 6$, et $m \in \mathbb{N}^*$, $(p-1)! + 1 = p^m$ n'a pas de solution.

Si p premier, $p = 4k + 3$, $(k \in \mathbb{N}^*)$, $2p + 1$ premier, alors M_p n'est pas premier.

L'équation $x^2 + y^2 = z^2, (x, y, z) \in \mathbb{N}^{*3}$, (x, y) ou $(y, x) = \left(2kmn, k(m^2 - n^2)\right), z = k(m^2 + n^2), k \in \mathbb{N}^*, (m, n) \in \mathbb{N}^2, m > n$