18 | Arithmétique dans $\mathbb{Z}$

J'ai découvert une preuve vraiment remarquable de ce théorème, que cette marge est trop petite pour contenir.

Pierre de Fermat (1607-1655) sur ce qui deviendra, plus de 300 ans plus tard, le dernier théorème de Fermat (ou théorème de Fermat-Wiles).

I – Divisibilité dans les entiers naturels

1 – Diviseurs et multiples

Définition 18.1 – Soient a et $b \in \mathbb{Z}$, on dit que a est un **diviseur** de b, ou que a divise b ou encore que b est un multiple de a, s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Notation 18.2 – Si d est un diviseur de a, on note $d \mid a$.
Pour tout $a \in \mathbb{Z}$, l'ensemble des multiples de a n'est autre que l'ensemble $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$.

Exemple 18.3 –

- 1 divise tous les entiers relatifs mais n'est divisible que par 1 et -1.
- 0 est un multiple de tout entier relatif mais n'est le diviseur que de lui-même.
- L'ensemble des diviseurs de 6 est $\{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Remarque 18.4 – La relation « divise » est réflexive sur $\mathbb{Z}$ car pour tout entier relatif a, on a $a \mid a$.
Elle est également transitive sur $\mathbb{Z}$ car si $a \mid b$ et $b \mid c$ alors $a \mid c$.
En ajoutant la proposition suivante (antisymétrie), c'est une relation d'ordre SUR $\mathbb{N}$.

Proposition 18.5 – Antisymétrie de la divisibilité sur $\mathbb{N}$

Soient $a, b \in \mathbb{N}$. On a $\quad (a \mid b \text{ et } b \mid a) \iff a = b.$

Démonstration.
$\boxed{\Longrightarrow}$ On suppose que $a \mid b$ et $b \mid a$. Il existe deux entiers naturels k et k' tels que $b = ka$ et $a = k'b$ ce qui donne $a = kk'a$. Si $a \neq 0$, alors $kk' = 1$. Comme k et k' sont des entiers naturels, on a nécessairement $k = k' = 1$ ce qui montre que $a = b$. Si $a = 0$, alors $b = k \times 0 = 0$ donc $a = b = 0$.
$\boxed{\Longleftarrow}$ Si $a = b$ alors le résultat est évident. □

Proposition 18.6 – Propriétés de la divisibilité

Soient $a, b, c, d \in \mathbb{Z}$. On a :

- **Combinaisons linéaires :** Si $d \mid a$ et $d \mid b$, alors $d \mid (au + bv)$ pour tous $u, v \in \mathbb{Z}$.
- **Produit :** Si $a \mid b$ et $c \mid d$, alors $ac \mid bd$, et en particulier $a^k \mid b^k$ pour tout $k \in \mathbb{N}$.

Démonstration.

- Soient $u, v \in \mathbb{Z}$. Supposons que $d \mid a$ et $d \mid b$. Alors il existe deux entiers relatifs k et k' tels que $a = dk$ et $b = dk'$. Avec deux tels entiers naturels k et k', on a donc $au + bv = dku + dk'v = d(ku + k'v)$. Puisque $ku + k'v$ est un entier relatif, on obtient que $d \mid (au + bv)$
- Par hypothèse $b = ak$ et $d = cl$ pour certains $k, l \in \mathbb{Z}$, donc $bd = (ac)(kl)$ avec $kl \in \mathbb{Z}$, donc $ac \mid bd$.

□

Proposition 18.7

Soient a, b deux entiers **naturels non nuls**. Si b divise a alors $b \leqslant a$.

Démonstration. Si b divise a, alors $a = bk$ où k est un entier naturel. Puisque $a \neq 0$, $k \neq 0$, donc $k \geqslant 1$ donc $bk \geqslant b$ donc $b \leqslant a$. □

2 – Relation de congruence modulo un entier

Définition 18.8 – Soient $a, b, n \in \mathbb{Z}$. On dit que a est **congru à b modulo n** si $n \mid (b-a)$, i.e. s'il existe un entier $k \in \mathbb{Z}$ pour lequel $a = b + kn$. Cette relation se note $a \equiv b[n]$.

Équivalence fondamentale dans les deux sens : $\boxed{n \mid a \iff a \equiv 0[n]}$.

Cette équivalence nous permettra de passer du vocabulaire de la divisibilité à celui des congruences et réciproquement.

Théorème 18.9 – Propriétés de la relation de congruence modulo un entier

Soient $a, a', b, b', m, n \in \mathbb{Z}$.

1. **Relation d'équivalence :** La relation $\equiv [n]$ est une relation d'équivalence sur $\mathbb{Z}$.
2. **Somme :** Si $a \equiv b[n]$ et $a' \equiv b'[n]$, alors $a + a' \equiv b + b'[n]$.
3. **Produit :** Si $a \equiv b[n]$ et $a' \equiv b'[n]$, alors $aa' \equiv bb'[n]$, et en particulier $a^k \equiv b^k[n]$ pour tout $k \in \mathbb{N}$.
4. **Multiplication/division par un entier non nul :** Si m est non nul : $a \equiv b[n] \iff ma \equiv mb[mn]$.

Démonstration.

1. • Réflexivité : Pour tout $a \in \mathbb{Z}$: $a = a + 0 \times n$ et $0 \in \mathbb{Z}$, donc $a \equiv a[n]$.
   • Transitivité : Soient $a, b, c \in \mathbb{Z}$. Si $a \equiv b[n]$ et $b \equiv c[n]$: $a = b + kn$ et $b = c + ln$ pour certains $k, l \in \mathbb{Z}$, donc : $a = b + kn = (c + ln) + kn = c + (k + l)n$ avec $k + l \in \mathbb{Z}$, donc $a \equiv c[n]$.
   • Symétrie : Soient $a, b \in \mathbb{Z}$. Si $a \equiv b[n]$: $a = b + kn$ pour un certain $k \in \mathbb{Z}$, donc $b = a + (-k)n$ avec $-k \in \mathbb{Z}$, donc $b \equiv a[n]$.
2. n divise $b - a$ et $b' - a'$, donc aussi $(b + b') - (a + a')$ par somme, donc $a + a' \equiv b + b'[n]$.
3. n divise $b - a$ et $b' - a'$, donc aussi $b(b' - a') + a'(b - a) = bb' - aa'$ par combinaison linéaire, donc $aa' \equiv bb'[n]$.
4. $a \equiv b[n] \iff n|(b-a) \overset{m\neq 0}{\iff} mn|m(b-a) \iff ma \equiv mb[mn]$.

□

Exemple 18.10 – $2^{345} + 5^{432}$ est divisible par 3.

Démonstration. $2^{345} + 5^{432} \equiv (-1)^{345} + (-1)^{432} \equiv -1 + 1 \equiv 0\ [3]$. □

Exemple 18.11 – Pour tout $n \in \mathbb{Z}$ impair : $n^2 \equiv 1[8]$.

Démonstration. Pour un certain $k \in \mathbb{Z}$: $n = 2k + 1$, donc : $n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1$. Cela dit, k ou $k + 1$ est pair car ces deux entiers sont consécutifs, donc $k(k+1)$ est pair aussi : $k(k+1) \equiv 0[2]$. A fortiori : $4k(k+1) \equiv 0[8]$, donc $n^2 = 4k(k+1) + 1 \equiv 1[8]$. □

3 – Division euclidienne dans les entiers naturels

Théorème 18.12 – Division euclidienne dans $\mathbb{N}$

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

q est appelé **quotient de la division euclidienne de a par b.**
r est appelé **reste de la division euclidienne de a par b.**
Par ailleurs, $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r \equiv a[b]$.

Exemple 18.13 – Division euclidienne de 27 par 7. On a $27 = 3\times 7+6$ et $0 \leqslant 6 < 7$. Le nombre 27 est appelé le dividende de cette division euclidienne, 7 le diviseur, 3 est le quotient et 6 le reste.

Démonstration.

• Unicité de (q,r). Soient (q,r) et (q',r') deux couples d'entiers naturels vérifiant

$$a = qb+r, \quad 0 \leqslant r < b \qquad \text{et} \qquad a = q'b+r', \quad 0 \leqslant r' < b.$$

Montrons que $q = q'$ et que $r = r'$.

$a = bq+r = bq'+r$, donc $b(q-q') = r-r'$. Donc $|r-r'|$ est un multiple de b

Comme $-b < -r' \leqslant 0$, on a $-b < r-r' < b$ c'est-à-dire $|r-r'| < b$. Donc $r-r' = 0$ et $b(q-q') = 0$, donc $q = q'$ car $b \neq 0$.

• Existence du couple (q,r).

L'ensemble $A = \{n \in \mathbb{N}, nb \leqslant a\}$ est une partie non vide de $\mathbb{N}$ puisque $0 \in A$. De plus A est majoré par a car si $n \in A$ alors $nb \leqslant a$ et donc $n \leqslant a$ car $b \geqslant 1$. L'ensemble A possède donc un plus grand élément que l'on note q et qui vérifie

$$qb \leqslant a \ \ (\text{car } q \in A) \qquad \text{et} \qquad (q+1)b > a \ \ (\text{car } q+1 \notin A).$$

En posant $r = a-qb$, on a $a = qb+r$ et $0 \leqslant r < (q+1)b - qb = b$. □

On s'intéresse dans l'exemple qui suit à la première équation diophantienne de ce chapitre. On appelle ainsi toute équation à inconnues entières construite à partir des seules opérations d'addition et de multiplication - par exemple, les équations $2x+3y = 5$ ou $x^3+2 = y^4$ d'inconnue $(x,y) \in \mathbb{Z}^2$.

Exemple 18.14 – Soient $x,y,z \in \mathbb{Z}$ trois entiers solutions de l'équation de Fermat $x^3+y^3 = z^3$. Alors l'un des entiers x,y ou z est divisible par 3 .

Démonstration.

Supposons par l'absurde que ni x ni y ni z n'est divisible par 3 . Le reste de la division euclidienne de x par 9 est alors l'un des entiers $1,2,4,5,7,8-$ on peut rejeter les cas 0,3 et 6 . Le tableau ci-contre montre que $x^3 \equiv \pm 1$ [9], et bien sûr de même $y^3 \equiv \pm 1$ [9] et $z^3 \equiv \pm 1$ [9].

Or par hypothèse : $x^3+y^3 \equiv z^3$[9]. À gauche, x^3+y^3 est congru modulo 9 à : $1+1 = 2$ ou $1-1 = 0$ ou $-1+1 = 0$ ou $-1-1 = -2$, alors qu'à droite $z^3 \equiv \pm 1$[9] - contradiction!

x[9]	x^2[9]	x^3[9]
1	1	1
2	4	$8 \equiv -1$
4	$16 \equiv -2$	$-8 \equiv 1$
$5 \equiv -4$	$16 \equiv -2$	$8 \equiv -1$
$7 \equiv -2$	4	$-8 \equiv 1$
$8 \equiv -1$	1	-1

□

Exemple 18.15 – Le reste de la division euclidienne de 2^{65362} par 7 est 2 .

Démonstration. Il n'est évidemment pas question de poser la division euclidienne de 2^{65362} par 7 : l'entier 2^{65362} possède près de 20000 décimales! Heureusement $2^3 \equiv 8 \equiv 1$ [7]. C'est l'idée-phare de cet exemple - dénicher, si elle existe, la première puissance de 2 congrue à 1 modulo 7 . Une fois qu'on en a trouvé une, c'est facile, on peut « raisonner modulo 3 dans l'exposant » car pour tout $k, r \in \mathbb{N}$: $2^{3k+r} \equiv 1^k \times 2^r \equiv 2^r$ [7].

En l'occurrence, ici : $65362 \equiv 1$[3], donc $2^{65362} \equiv 2^1 \equiv 2$[7]. □

Proposition 18.16 – Lien entre division euclidienne et divisibilité

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. On note r le reste de la division euclidienne de a par b. On a

$$b \mid a \iff r = 0.$$

Démonstration. Notons q et r respectivement le quotient et le reste de la division euclidienne de a par b. $\boxed{\Leftarrow}$ Si $r = 0$ alors on a $a = bq$ donc $b|a$. $\boxed{\Rightarrow}$ Supposons que $b|a$. Alors il existe $k \in \mathbb{N}$ tel que $a = bk+0$. Considérons un tel k. Comme $0 \leqslant 0 < b$, par unicité du quotient et du reste dans la division euclidienne de a par b, $k = q$ et $r = 0$. □

II – PGCD, PPCM

1 – Plus Grand Commun Diviseur (PGCD)

Soient a et b deux entiers naturels non tous les deux nuls. Supposons que $a \neq 0$. Si un entier naturel n divise a alors $n \leqslant a$. Ainsi, l'ensemble des nombres entiers naturels qui divisent à la fois a et b est un ensemble fini de nombres (car il est inclus dans $[\![1, a]\!]$) et cet ensemble est non vide (car il contient 1). Cet ensemble possède donc un plus grand élément.

Définition 18.17 – Soient a et b deux entiers naturels. Si $(a, b) \neq (0, 0)$, on appelle **Plus Grand Commun Diviseur** (ou PGCD) le plus grand entier naturel qui divise a et b. On le note $a \wedge b$.

Remarque 18.18 – Si a et b sont non nuls, $1 \leqslant a \wedge b \leqslant \min(a, b)$.
Pour tout entier naturel $a > 0$, $a \wedge 0 = a$.
Par convention, on pose $0 \wedge 0 = 0$.

Exemple 18.19 – Les diviseurs de 15 sont 1, 3, 5, 15 et ceux de 12 sont 1, 2, 3, 4, 6, 12 donc $15 \wedge 12 = 3$.

Proposition 18.20 – Division euclidienne et PGCD

Soient a et b deux entiers naturels non nuls. On note r le reste de division euclidienne de a par b. On a

$$a \wedge b = b \wedge r.$$

Démonstration. Notons q le quotient de cette division euclidienne.

- ▷ Par définition, $a \wedge b$ divise a et b et comme $r = a - bq$, $a \wedge b$ divise r. Ainsi $a \wedge b$ divise b et r donc par définition de $b \wedge r$, on a $a \wedge b \leqslant b \wedge r$.
- ▷ Par définition, $b \wedge r$ divise b et r et comme $a = bq + r$, $b \wedge r$ divise a. Ainsi $b \wedge r$ divise a et b donc par définition de $a \wedge b$, on a $b \wedge r \leqslant a \wedge b$.

Finalement $b \wedge r = a \wedge b$. □

Remarque 18.21 – Le résultat de cette dernière proposition donne une justification à l'algorithme d'Euclide utilisé pour déterminer le PGCD de deux nombres entiers strictement positifs.

Algorithme d'Euclide : Pour calculer le PGCD de deux entiers naturels non nuls a et b. On effectue une suite de divisions euclidiennes en commençant par celles de a par b. À chaque étape, le couple (diviseur, reste) de la division euclidienne effectuée devient le couple (dividende, diviseur) de la division euclidienne suivante. Lorsqu'on aboutit à un reste nul, le dernier diviseur est le PGCD de a et b. C'est aussi le dernier reste non nul.

Exemple 18.22 –

- ▷ Effectuer la division euclidienne de a par b : $a = bq + r$.
- ▷ Si $r = 0$, alors $a \wedge b = b$.
- ▷ $Sr \neq 0$, alors $a \wedge b = b \wedge r$, donc on recommence en remplaçant a et b par b et r.

Calculons par exemple $210 \wedge 154$.
$210 = 154 \times 1 + 56$, donc $210 \wedge 154 = 154 \wedge 56$.
$154 = 56 \times 2 + 42$, donc $154 \wedge 56 = 56 \wedge 42$.
$56 = 42 \times 1 + 14$, donc $56 \wedge 42 = 42 \wedge 14$.
$42 = 14 \times 3 + 0$, donc $42 \wedge 14 = 14$.
Finalement, $210 \wedge 154 = 14$.

```
1 def PGCD_Euclide(a:int,b:int)->int:
2     """ Calcule le PGCD des deux entiers passés en entrée."""
3     dividende,diviseur = a,b
4     while diviseur != 0:
5         dividende,diviseur = diviseur,dividende%diviseur
6     return dividende
```

Définition 18.23 – Soient a et b deux entiers relatifs. On appelle **Plus Grand Commun Diviseur** (ou PGCD) de a et b, que l'on note $a \wedge b$, l'entier naturel défini par $a \wedge b = |a| \wedge |b|$.

2 – Relations de Bézout

Théorème 18.24 – Relations de Bézout, cas de deux entiers

Soient $a, b \in \mathbb{Z}$. Il existe des entiers $u, v \in \mathbb{Z}$ pour lesquels $a \wedge b = au + bv$.
Une telle relation est appelée UNE **relation de Bézout** de a et b.

ATTENTION ! Les entiers u et v ne sont pas du tout uniques.
Par exemple : $4 \wedge 6 = 2$, mais on a à la fois : $2 = (-1) \times 4 + 1 \times 6$ et $2 = 2 \times 4 + (-1) \times 6$.

Démonstration. On peut supposer sans perte de généralité que $0 \leqslant b \leqslant a$. Reprenons les restes successifs de l'algorithme d'Euclide en posant $r_0 = a$ et $r_1 = b$ et en notant pour $k \in \mathbb{N}$, tant que $r_{k+1} > 0$, r_{k+2} le reste de la division euclidienne de r_k par r_{k+1}. Le quotient de cette division euclidienne sera quant à lui noté q_{k+2} : $r_{k+2} = r_k - q_{k+2} r_{k+1}$. La suite ainsi construite est finie de rang final N pour lequel $r_N = 0$.

On définit alors deux nouvelles familles $(u_k)_{0 \leqslant k \leqslant N}$ et $(v_k)_{0 \leqslant k \leqslant N}$ par : $(u_0, v_0) = (1, 0)$, $(u_1, v_1) = (0, 1)$ et $(u_{k+2}, v_{k+2}) = \big(u_k - q_{k+2} u_{k+1}, v_k - q_{k+2} v_{k+1}\big)$ pour tout $k \in [\![0, N-2]\!]$. Montrons par récurrence double que $r_k = au_k + bv_k$ pour tout $k \in [\![0, N]\!]$.
Initialisation : $r_0 = a = a \times 1 + b \times 0 = au_0 + bv_0$ et $r_1 = b = a \times 0 + b \times 1 = au_1 + bv_1$.
Hérédité : Soit $k \in [\![0, N-2]\!]$. Si $r_k = au_k + bv_k$ et $r_{k+1} = au_{k+1} + bv_{k+1}$:

$$r_{k+2} = r_k - q_{k+2} r_{k+1} \overset{\text{HDR}}{=} (au_k + bv_k) - q_{k+2}(au_{k+1} + bv_{k+1}) = a\big(u_k - q_{k+2} u_{k+1}\big) + b\big(v_k - q_{k+2} v_{k+1}\big) = au_{k+2} + bv_{k+2}.$$

Il découle de cette récurrence, en particulier, que $a \wedge b = r_{N-1} = au_{N-1} + bv_{N-1}$. □

Le procédé de construction des entiers u et v de la démonstration qui précède s'appelle l'algorithme d'Euclide étendu. En résumé, alors que l'algorithme d'Euclide ne s'intéresse qu'aux restes des divisions euclidiennes successives effectuées, l'algorithme d'Euclide étendu va plus loin en tenant compte aussi des quotients successifs obtenus.

Exemple 18.25 – $3080 \wedge 525 = 35 = 7 \times 3080 + (-41) \times 525$

Démonstration. On calcule d'abord les restes successifs associés aux entiers 3080 et 525 :

$$3080 = 5 \times 525 + 455, \quad 525 = 1 \times 455 + 70, \quad 455 = 6 \times 70 + 35, \quad 70 = 2 \times 35 + 0.$$

Le dernier reste non nul vaut 35, c'est notre PGCD. Pour calculer un jeu de coefficients de Bézout associé, on remonte la chaîne des divisions euclidiennes successives en partant du PGCD 35 :

$$\begin{aligned} 35 &= 455 - 6 \times 70 && \text{(On a éliminé 35.)} \\ &= 455 - 6 \times (525 - 1 \times 455) = (-6) \times 525 + 7 \times 455 && \text{(On a éliminé 70.)} \\ &= (-6) \times 525 + 7 \times (3080 - 5 \times 525) = 7 \times 3080 + (-41) \times 525. && \text{(On a éliminé 455.)} \end{aligned}$$

□

On peut généraliser les résultats et notions ci-dessus à un nombre quelconque d'entiers.

Définition 18.26 – Soient $a_1, \dots, a_r \in \mathbb{Z}$. On appelle **plus grand commun diviseur** de $a_1, \dots, a_r$ le plus grand entier naturel qui divise $|a_1|, \dots, |a_r|$. On le note $a_1 \wedge \cdots \wedge a_r$.

Théorème 18.27 – Relations de Bézout, cas général

Soient $a_1, \dots, a_r \in \mathbb{Z}$. Il existe des entiers $u_1, \dots, u_r \in \mathbb{Z}$ pour lesquels $a_1 \wedge \cdots \wedge a_r = a_1 u_1 + \cdots + a_r u_r$. Une telle relation est appelée UNE **relation de Bézout** de $a_1, \dots, a_r$.

Exemple 18.28 – $10 \wedge 15 \wedge 24 = 1 = (-5) \times 10 + 5 \times 15 + (-1) \times 24$

Démonstration. $\begin{cases} \text{Première relation de Bézout :} & 10 \wedge 15 = 5 = (-1) \times \underline{10} + 1 \times \underline{15}. \\ \text{Deuxième relation de Bézout :} & 5 \wedge 24 = 1 = 5 \times \underline{5} + (-1) \times \underline{24}. \end{cases}$

On emboîte : $\begin{aligned} 10 \wedge 15 \wedge 24 = 5 \wedge 24 = 5 \times \underline{5} + (-1) \times \underline{24} &= 5 \times ((-1) \times \underline{10} + 1 \times \underline{15}) + (-1) \times \underline{24} \\ &= (-5) \times \underline{10} + 5 \times \underline{15} + (-1) \times \underline{24}. \end{aligned}$ □

3 – Plus Petit Commun Multiple (PPCM)

Soient a et b deux entiers naturels non nuls. L'ensemble des entiers naturels non nuls qui sont à la fois multiples de a et de b est un sous-ensemble non vide (car il contient ab) de $\mathbb{N}$ donc il possède un plus petit élément.

Définition 18.29 – Soient a et b deux entiers naturels non nuls. On appelle **Plus Petit Commun Multiple** (ou PPCM) le plus petit entier naturel non nul qui soit un multiple de a et de b. On le note $a \vee b$.

Remarque 18.30 –

- $\max(a,b) \leqslant a \vee b \leqslant ab$
- Encore une fois, pour deux entiers relatifs a et b, on définit le PPCM de a et b, noté $a \vee b$, par $a \vee b = |a| \vee |b|$.

Exemple 18.31 – Les multiples strictement positifs de 6 sont 6, 12, 18, 24, 30… et ceux de 8 sont 8, 16, 24, 32… donc $6 \vee 8 = 24$.

Proposition 18.32

Soit $(a,b) \in (\mathbb{N}^*)^2$. Si $b \mid a$ alors $a \wedge b = b$ et $a \vee b = a$.

Démonstration. On suppose que $b|a$. Alors $b \leqslant a$ donc $\max(a,b) = a$ et $\min(a,b) = b$. On sait donc que $a \wedge b \leqslant b$. Or b est un diviseur de a et de b donc $a \wedge b = b$. De même, on sait que $a \leqslant a \vee b$ or a est multiple de a et de b donc $a \vee b = a$. □

Proposition 18.33 – PPCM des diviseurs d'un entier

Soit $(a,b) \in (\mathbb{N}^*)^2$ et n un entier naturel. Si $a \mid n$ et $b \mid n$, alors $a \vee b \mid n$.

Démonstration. On suppose que $a \mid n$ et $b \mid n$. On écrit la division euclidienne de n par $a \vee b$: on considère l'unique couple (q,r) d'entiers naturels tels que

$$n = a \vee b \times q + r \qquad \text{et} \qquad 0 \leqslant r < a \vee b.$$

Comme $r = n - a \vee b \times q$, on peut affirmer que r est un multiple de a et de b. Or $r < a \vee b$ donc $r = 0$. Ceci démontre que $a \vee b \mid n$. □

4 – Entiers premiers entre eux

Définition 18.34 – Soient a et b deux entiers naturels non nuls. On dit que a et b sont **premiers entre eux** lorsque $a \wedge b = 1$.

Exemple 18.35 – $15 \wedge 34 = 1$ donc 15 et 34 sont premiers entre eux.

ATTENTION ! Ne confondez pas $a \nmid b$ et $a \wedge b = 1$, ça n'a rien à voir ! Par exemple, $6 \nmid 15$ mais $6 \wedge 15 = 3 \neq 1$

Dire que $a \wedge b = 1$, c'est dire que a et b n'ont **AUCUN** diviseur commun hormis ± 1. La relation $a \nmid b$ n'empêche pas quant à elle a et b de partager de nombreux diviseurs communs, elle empêche seulement a d'être intégralement « présent » dans b.

Proposition 18.36

Pour tous $a, b \in \mathbb{Z}$ de PGCD d : $a = da'$ et $b = db'$ pour certains entiers $a', b' \in \mathbb{Z}$ **PREMIERS ENTRE EUX** .

Démonstration. Tout simplement, si $(a,b) \neq (0,0)$: $\quad d = a \wedge b = (da') \wedge (db') = d(a' \wedge b'), \quad$ donc $a' \wedge b' = 1$. □

Exemple 18.37 – L'équation $x^2 = y^2 + (x \wedge y) + 2$ d'inconnue $(x,y) \in \mathbb{N}^2$ admet $(2,1)$ et $(2,0)$ pour seules solutions.

Démonstration.

- **Analyse :** Soit $(x,y) \in \mathbb{N}^2$. On suppose que $x^2 = y^2 + (x \wedge y) + 2$ et on pose $d = x \wedge y$. Clairement $(x,y) \neq (0,0)$, donc $d \neq 0$. En outre $x = dx'$ et $y = dy'$ pour certains $x', y' \in \mathbb{N}$ premiers entre eux.
  L'équation devient $d^2x'^2 = d^2y'^2 + d + 2$, donc d divise 2, i.e. $d = 1$ ou $d = 2$.
  — Cas où $d = 1$: $\quad (x'+y')(x'-y') = 3, \quad$ or 3 est premier et $x'-y' \leqslant x'+y'$, donc $x'+y' = 3$ et $x'-y' = 1$. Aussitôt $(x',y') = (2,1)$, et enfin $(x,y) = (2,1)$.
  — Cas où $d = 2$: $\quad (x'+y')(x'-y') = 1, \quad$ donc $x'+y' = x'-y' = 1$, i.e. $(x',y') = (1,0)$, et enfin $(x,y) = (2,0)$.
- **Synthèse :** Les couples $(2,1)$ et $(2,0)$ sont bel et bien solutions de l'équation étudiée.

□

Définition 18.38 – Soient $a_1, \dots, a_r \in \mathbb{Z}$.

- On dit que $a_1, \dots, a_r$ sont **premiers entre eux dans leur ensemble** si leurs seuls diviseurs communs sont ± 1, i.e si $a_1 \wedge \cdots \wedge a_r = 1$.
- On dit que $a_1, \dots, a_r$ sont **premiers entre eux deux à deux** si $a_i \wedge a_j = 1$ pour tous $i, j \in [\![1, r]\!]$ distincts.

Remarque 18.39 – Premiers entre eux **DEUX À DEUX** $\implies$ Premiers entre deux **DANS LEUR ENSEMBLE**
mais **LA RÉCIPROQUE EST FAUSSE!** Par exemple, 6, 10 et 15 sont premiers entre eux dans leur ensemble, mais pourtant :

$$6 \wedge 10 = 2 \neq 1, \qquad 6 \wedge 15 = 3 \neq 1, \qquad 10 \wedge 15 = 5 \neq 1$$

Théorème 18.40 – Théorème de Bézout

Soient $a, b \in \mathbb{Z}$. Les assertions suivantes sont équivalentes :

1. a et b sont premiers entre eux.
2. Il existe deux entiers $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Démonstration. L'implication **1.** $\implies$ **2.** est une simple relation de Bézout - déjà prouvée. Pour la réciproque **2.** $\implies$ **1.**, supposons l'existence de deux entiers $u, v \in \mathbb{Z}$ pour lesquels $au + bv = 1$ et fixons d un diviseur commun positif de a et b. Alors d divise $au + bv = 1$, donc $d = 1$. Comme voulu $a \wedge b = 1$. □

Lemme 18.41 – Lemme de Gauss

Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ avec $a \wedge b = 1$, alors $a \mid c$.

Démonstration. Par hypothèse, $bc = ak$ pour un certain $k \in \mathbb{Z}$ et $au + bv = 1$ pour certains $u, v \in \mathbb{Z}$ - relation de Bézout. Multiplions par c : $\quad acu + bcv = c$, puis remplaçons bc par ak : $\quad a(cu + kv) = c$. Ainsi $a \mid c$. □

Théorème 18.42 – Conséquences directes du Lemme de Gauss

Soient $a, b, m, n, a_1, \dots, a_r \in \mathbb{Z}$.

1. **Lemme d'Euclide :** Pour tout **NOMBRE PREMIER** p : $\quad p \mid ab \iff p \mid a$ ou $p \mid b$.
2. **Division dans une congruence :** Si $am \equiv bm\,[n]$ avec $m \wedge n = 1$, alors $a \equiv b\,[n]$.
3. **Produits d'entiers :**
   - Si chacun des entiers $a_1, \dots, a_r$ est premier avec n, leur produit $a_1 \dots a_r$ l'est aussi.
   - Si les entiers $a_1, \dots, a_r$ divisent n et sont premiers entre eux **DEUX À DEUX**, leur produit $a_1 \dots a_r$ divise n.

Démonstration.

1. Si p divise a ou b, p divise ab. Réciproquement, si p divise ab et si p ne divise pas a, alors $p \wedge a = 1$ car p est premier, donc $p \mid b$ d'après le théorème de Gauss. Bref, si p divise ab : $\quad p \mid a$ ou $p \mid b$.

2. $n \mid (a-b)m$ et $m \wedge n = 1$, donc $n \mid (b-a)$ d'après le lemme de Gauss, i.e. $a \equiv b[n]$.
3. Montrons le résultat dans le cas de deux entiers $a, b \in \mathbb{Z}$.
   - Si $a \wedge n = b \wedge n = 1$, alors $au + nv = bu' + nv' = 1$ pour certains $u, v, u', v' \in \mathbb{Z}$ d'après le théorème de Bézout, donc par produit : $1 = (au+nv)(bu'+nv') = (ab)(uu') + n(auv' + vbu' + nvv')$, donc $(ab) \wedge n = 1$ de nouveau d'après le théorème de Bézout.
   - Faisons l'hypothèse que : $a|n$, $b|n$ et $a \wedge b = 1$. Ainsi $n = ak$ pour un certain $k \in \mathbb{Z}$, donc b divise $n = ak$, or $a \wedge b = 1$, donc $b \mid k$ d'après le théorème de Gauss. A fortiori, ab divise $ak = n$.

□

ATTENTION !

1. La primalité de p est indispensable au lemme d'Euclide. Par exemple $4 \mid 2 \times 2$ mais $4 \nmid 2$.
2. On ne peut pas toujours « simplifier par m » dans une congruence, encore faut-il que m et n n'aient rien de commun à part ± 1, i.e. qu'ils soient premiers entre eux. Par exemple $2 \times 3 \equiv 2 \times 0[6]$, mais $3 \not\equiv 0[6]$.
3. En général : $a \mid n$ et $b|n \not\Rightarrow ab|n$. Par exemple, 12 est divisible par 4 et 6 , mais pas par 24. Ensuite, il est impératif de supposer $a_1, \dots, a_r$ premiers entre eux **DEUX À DEUX** dans la deuxième partie de l'assertion **3**. Par exemple, pour : $n = 30, a_1 = 6, a_2 = 10$ et $a_3 = 15$, les entiers a_1, a_2 et a_3 divisent n mais sont seulement premiers entre eux **DANS LEUR ENSEMBLE** , et clairement leur produit $a_1 a_2 a_3 = 900$ ne divise pas n.

Théorème 18.43 – Forme irréductible d'un rationnel

Tout rationnel peut être écrit d'une et une seule manière, appelée sa **forme irréductible**, sous la forme $\frac{p}{q}$ où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ avec p et q premiers entre eux.

Démonstration.

- **Unicité :** Soient $(p,q), (p',q') \in \mathbb{Z} \times \mathbb{N}^*$. On suppose que $r = \frac{p}{q} = \frac{p'}{q'}$ avec $p \wedge q = 1$ et $p' \wedge q' = 1$. Aussitôt $pq' = p'q$, donc $q \mid pq'$. Cela dit $p \wedge q = 1$, donc $q \mid q'$ d'après le lemme de Gauss, puis $q' \mid q$ par symétrie des rôles de q et q'. Conclusion : $|q| = |q'|$, et comme q et q' sont positifs : $q = q'$. Divisons enfin l'égalité $pq' = p'q$ par $q = q'$. Comme voulu $p = p'$.
- **Existence :** Par définition $r = \frac{a}{b}$ pour certains $a, b \in \mathbb{Z}$ avec $b \neq 0$, et même $b > 0$ sans perte de généralité. En notant d le PGCD de a et b : $a = dp$ et $b = dq$ pour certains $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux, et donc $r = \frac{a}{b} = \frac{dp}{dq} = \frac{p}{q}$.

□

Remarque 18.44 – En choisissant p dans $\mathbb{Z}$ et q dans $\mathbb{N}^*$, on impose que le signe de la fraction soit porté par son numérateur. Sans cela, il n'y aurait pas unicité de la forme irréductible.

III – Nombres premiers

1 – Généralités

Définition 18.45 – On appelle **nombre premier** tout entier naturel non nul admettant exactement 2 diviseurs entiers naturels distincts : 1 et lui-même.
L'ensemble des nombres premiers est souvent noté $\mathbb{P}$.

Exemple 18.46 – Les premiers nombres premiers sont 2,3,5,7,11...

ATTENTION ! 1 et 0 ne sont **PAS** premiers. Non non, vraiment, ils ne **SONT PAS** premiers.

Remarque 18.47 – Deux nombres premiers distincts sont premiers entre eux.

Proposition 18.48 – Existence d'un diviseur premier

Tout nombre entier supérieur ou égal à 2 est divisible par un nombre premier

Démonstration. Pour tout $n \in \mathbb{N}\setminus\{0,1\}$, on note $\mathcal{P}_n$ la propriété $\mathcal{P}_n$: « n admet un diviseur premier ».

La propriété est vraie pour $n = 2$ car 2 admet un diviseur premier : lui-même.

Soit $n \in \mathbb{N}\setminus\{0,1\}$. On suppose que pour tout $k \in [\![2,n]\!]$, $\mathcal{P}_k$ est vraie. Si $n+1$ est premier, alors il a un diviseur premier : lui-même. Si $n+1$ n'est pas premier, alors il existe $k \in [\![2,n]\!]$ tel que $k \mid (n+1)$. Par hypothèse de récurrence, k possède un diviseur premier qui est *a fortiori* un diviseur premier de $n+1$ et donc $\mathcal{P}_{n+1}$ est vraie. □

Théorème 18.49 – Théorème d'Euclide

Il existe une infinité de nombres premiers.

Démonstration. Montrons ce résultat par l'absurde.

Supposons qu'il existe un nombre fini $n \geqslant 2$ de nombres premiers. Notons les $p_1, p_2, \dots, p_n$ et supposons que $p_1 < p_2 < \cdots < p_n$. Considérons le nombre $N = p_1 p_2 \dots p_n + 1$. Alors $N \geqslant 2$.

D'après la proposition **??**, N admet un diviseur premier. Or aucun des nombres premiers $p_1,\dots,p_n$ ne divise N puisque le reste de la division euclidienne de N par l'un des ces nombres vaut 1 (en effet N s'écrit $p_i.q+1$ avec $q \in \mathbb{N}$ pour tout $i \in [\![1,n]\!]$). Contradiction! □

Crible d'Eratosthène :

Pour déterminer les nombres premiers inférieurs à une entier n fixé, on peut réaliser un **crible d'Ératosthène**. Le principe est le suivant :

1. on écrit tous les nombres de 2 à n ;
2. on conserve le nombre premier 2 et on raye tous les multiples de 2 (qui ne sont donc pas premiers) ;
3. pour chaque nombre suivant p non rayé, on conserve p et on raye les multiples de p ;
4. lorsque l'algorithme s'arrête (on est arrivé à n), tous les nombres non rayés sont les nombres premiers inférieurs à n.

Voici une implémentation en Python :

```
1  def eratosthene(N: int) -> list:
2      """
3      Renvoie la liste des nombres premiers inférieurs à N.
4      """
5      # dictionnaire indiquant pour chaque nombre s'il est premier ou pas.
6      est_premier = { i: True for i in range(2,N+1)}
7      for k in range(2, int(N**(1/2))+1):
8          if est_premier[k]:
9          # Si k est premier, on barre les multiples de k
10             for m in range(2*k, N+1, k):
11                 est_premier[m] = False
12     # on ne renvoie que les premiers
13     return [k for k in est_premier if est_premier[k]]
```

Application pour trouver les nombres premiers inférieurs à 100 :

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2 – Valuation p-adique et décomposition en produit de facteurs premiers

Théorème 18.50 – Décomposition d'un nombre en produit de nombres premiers

$\forall n \in \mathbb{N}$, si $n \geqslant 2$, alors n admet une décomposition en facteurs premiers de la forme $n = q_1 q_2 \dots q_k$ où $q_1, \dots, q_k$ sont des nombres premiers. Cette décomposition est unique à l'ordre près des facteurs.

On peut également écrire cette décomposition sous la forme

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où $p_1, \dots, p_r$ sont des nombres premiers distincts deux à deux et $\alpha_1, \dots, \alpha_r$ des entiers naturels non nuls.

Démonstration.

• Existence : On procède par récurrence forte. Pour tout $n \geqslant 2$, on pose P_n « $\forall k \in [\![2, n]\!]$, k admet une décomposition en facteurs premiers. »

Initialisation : 2 est premier.

Hérédité : Soit $n \geqslant 2$ entier. On suppose P_n vraie.

Si $n+1$ est premier, il se décompose en lui-même.

Si $n+1$ n'est pas premier, il est divisible par p premier avec $p < n$. Donc $n+1 = p \times q$ avec $q \in \mathbb{N}$. Alors $q \in [\![2, n]\!]$, donc d'après l'hypothèse de récurrence, q est décomposable en $q_1 \times \dots \times q_r$ où les q_i sont premiers.

Donc $n+1 = p \times q_1 \times \dots \times q_r$. Donc P_{n+1} est vraie.

D'où l'existence par récurrence.

• Unicité : On procède par récurrence forte. Pour tout $n \geqslant 2$, on pose P_n « $\forall k \in [\![2, n]\!]$, k admet une unique décomposition en facteurs premiers. »

Initialisation : Si $2 = q_1 \times \dots \times q_r$ où les q_i sont premiers, $r \in \mathbb{N}^*$, alors pour tout $i \in [\![1, r]\!]$, $q_i \geqslant 2$, donc $2 \geqslant 2^r$. Donc $r = 1$ et $q_1 = 2$. La décomposition de 2 est bien unique.

Hérédité : Soit $a \geqslant 2$ entier fixé. On suppose que P_a est vraie.

Soient $p_1 \times \dots \times p_r$ et $q_1 \times \dots \times q_n$ deux décomposition de $a+1$ en facteurs premiers.

Alors $p_1 \mid q_1 \dots q_n$, donc il existe i tel que $p_1 \mid q_i$. Quitte à renuméroter, on suppose que $p_1 \mid q_1$. Or q_1 est premier, donc $p_1 = q_1$.

Donc $p_2 \times \dots \times p_r$ et $q_2 \times \dots \times q_n$ sont deux décomposition de $\dfrac{a+1}{p_1}$ en facteurs premiers. Par hypothèse de récurrence, ce sont les mêmes à l'ordre près. Donc les deux décompositions de $a+1$ sont les mêmes à l'ordre près. Donc P_{a+1} est vraie.

D'où l'unicité par récurrence. □

Remarque 18.51 – Ce théorème est parfois appelé « théorème fondamental de l'arithmétique. »

Exemples de recherche de la décomposition d'un nombre en produits de nombres premiers

$$360 = 2 \times 180 = 2^2 \times 90 = 2^3 \times 45 = 2^3 \times 3 \times 15 = 2^3 \times 3^2 \times 5.$$

$$343 = 7 \times 49 = 7^3.$$

$$9295 = 5 \times 1859 = 5 \times 11 \times 169 = 5 \times 11 \times 13^2.$$

$$5152 = 2 \times 2576 = 2^2 \times 1288 = 2^3 \times 644 = 2^4 \times 322 = 2^5 \times 161 = 2^5 \times 7 \times 23.$$

Définition 18.52 – Soit $n \in \mathbb{Z}^*$ et $p \in \mathbb{P}$. On appelle **valuation p-adique de n**, que l'on note $v_p(n)$ l'exposant de p dans la décomposition en facteur premier de $|n|$.

Exemple 18.53 – La décomposition en produit de facteurs premiers de 60 est $60 = 2^2 \times 3 \times 5$ donc :

$$v_2(60) = 2, \quad v_3(60) = 1, \quad v_5(60) = 1 \text{ et } \forall p \in \mathbb{P} \setminus \{2, 3, 5\}, \quad v_p(60) = 0$$

Remarque 18.54 –

- On peut également définir la valuation p-adique de n comme le plus grand élément (il existe !) de $\{k \in \mathbb{N} \,;\, p^k \mid n\}$.

- Pour tout $n \in \mathbb{Z} \setminus \{0\}$, le théorème **??** permet d'écrire :

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

étant entendu qu'une infinité de termes dans le produit ci-dessus valent 1, et qu'on peut donc assimiler ce produit à un produit fini.

Théorème 18.55 – Additivité des valuations p-adiques

Pour tous $p \in \mathbb{P}$ et $a, b \in \mathbb{Z}\setminus\{0\}$: $\quad v_p(ab) = v_p(a) + v_p(b)$.

Démonstration. Par définition des valuations p-adiques : $a = p^{v_p(a)}a'$ et $b = p^{v_p(b)}b'$ pour certains $a', b' \in \mathbb{Z}\setminus\{0\}$ non divisibles par p. Ainsi, p étant premier : $\quad p \wedge a' = p \wedge b' = 1, \quad$ donc $p \wedge (a'b') = 1$, donc $p \nmid a'b'$. L'égalité $ab = p^{v_p(a)+v_p(b)}a'b'$ montre ainsi que $v_p(ab) = v_p(a) + v_p(b)$. □

Exemple 18.56 – Pour tous $p, q \in \mathbb{P}$ et $k \in \mathbb{N}$: $\quad v_p\left(q^k\right) = kv_p(q) = \begin{cases} k & \text{si } q = p \\ 0 & \text{sinon.} \end{cases}$

Exemple 18.57 – $\sqrt[5]{\dfrac{4}{3}}$ est irrationnel.

Démonstration. Par l'absurde, supposons $\sqrt[5]{\dfrac{4}{3}}$ rationnel, disons $\sqrt[5]{\dfrac{4}{3}} = \dfrac{a}{b}$ pour certains $a, b \in \mathbb{N}^*$. Aussitôt $3a^5 = 4b^5$, donc en particulier $v_3\left(3a^5\right) = v_3\left(4b^5\right)$, ce qui s'écrit aussi : $5v_3(a) + 1 = 5v_3(b)$, et modulo 5 : $1 \equiv 0[5]$ - contradiction! □

Théorème 18.58

Soient $a, b \in \mathbb{Z} \setminus \{0\}$.

1. a divise b si et seulement si pour tout $p \in \mathbb{P}$: $\quad v_p(a) \leqslant v_p(b)$.
2. $\quad a \wedge b = \displaystyle\prod_{p \in \mathbb{P}} p^{\min\{v_p(a), v_p(b)\}} \quad$ et $\quad a \vee b = \displaystyle\prod_{p \in \mathbb{P}} p^{\max\{v_p(a), v_p(b)\}}$.

Démonstration.

1. Si $a \mid b$, alors $b = ak$ pour un certain $k \in \mathbb{Z}\setminus\{0\}$, donc $v_p(b) = v_p(a) + v_p(k) \geqslant v_p(a)$ pour tout $p \in \mathbb{P}$. Inversement, si $v_p(a) \leqslant v_p(b)$ pour tout $p \in \mathbb{P}$, $p^{v_p(a)}$ divise $p^{v_p(b)}$, donc $\displaystyle\prod_{p \in \mathbb{P}} p^{v_p(a)} = a$ divise $\displaystyle\prod_{p \in \mathbb{P}} p^{v_p(b)} = b$.
2. Pour le PGCD, posons $d = \displaystyle\prod_{p \in \mathbb{P}} p^{\min\{v_p(a), v_p(b)\}}$. D'après **1.**, d divise à la fois a et b. Pour montrer que $d = a \wedge b$, nous allons prouver que $\dfrac{a}{d} \wedge \dfrac{b}{d} = 1$.
   Soit $p \in \mathbb{P}$. Si $v_p(a) \leqslant v_p(b)$, alors $v_p(d) = v_p(a)$, donc $v_p\left(\dfrac{a}{d}\right) = v_p(a) - v_p(d) = 0$, donc p ne divise pas $\dfrac{a}{d}$. Si au contraire $v_p(a) > v_p(b)$, p ne divise pas $\dfrac{b}{d}$. Dans les deux cas, p ne divise pas à la fois $\dfrac{a}{d}$ et $\dfrac{b}{d}$. En résumé, $\dfrac{a}{d}$ et $\dfrac{b}{d}$ n'ont aucun diviseur commun premier, donc sont premiers entre eux.
   Pour le PPCM, la démarche est la même. On pose $m = \displaystyle\prod_{p \in \mathbb{P}} p^{\max\{v_p(a), v_p(b)\}}$. Alors $a \mid m$ et $b \mid m$. On montre alors que $\dfrac{m}{a}$ et $\dfrac{m}{b}$ sont premiers entre eux.

□

Exemple 18.59 – $360 = 2^3 \times 3^2 \times 5$ et $336 = 2^4 \times 3 \times 7$ donc

$$360 \wedge 336 = 2^3 \times 3 = 24 \qquad \text{et} \qquad 360 \vee 336 = 2^4 \times 3^2 \times 5^1 \times 7^1 = 5040$$

Exemple 18.60 – Pour soustraire les fractions $\frac{11}{360}$ et $\frac{5}{336}$ on prendra pour dénominateur commun $360 \vee 336$.

$$\frac{11}{360} - \frac{5}{336} = \frac{11}{2^3 \times 3^2 \times 5} - \frac{5}{2^4 \times 3 \times 7} = \frac{11 \times 2 \times 7}{2^4 \times 3^2 \times 5 \times 7} - \frac{5^2 \times 3}{2^4 \times 3^2 \times 5 \times 7} = \frac{154 - 75}{2^4 \times 3^2 \times 5 \times 7} = \frac{79}{2^4 \times 3^2 \times 5 \times 7}$$

Corollaire 18.61 – Relation PGCD-PPCM

Soit $(a, b) \in (\mathbb{Z}^*)^2$. $\quad (a \wedge b) \times (a \vee b) = ab.$

Démonstration. Avec les mêmes notations que précédemment,

$$\begin{aligned} a \wedge b \times a \vee b &= \prod_{p \in \mathbb{P}} p^{\min\left(v_p(a), v_p(b)\right)} \times \prod_{p \in \mathbb{P}} p^{\max\left(v_p(a), v_p(b)\right)} \\ &= \prod_{p \in \mathbb{P}} p^{\min\left(v_p(a), v_p(b)\right) + \max\left(v_p(a), v_p(b)\right)} \\ &= \prod_{p \in \mathbb{P}} p^{v_p(a) + v_p(b)} \\ &= \prod_{p \in \mathbb{P}} p^{v_p(a)} \times \prod_{p \in \mathbb{P}} p^{v_p(b)} \\ &= a \times b \end{aligned}$$

□

3 – Petit théorème de Fermat

Théorème 18.62 – Petit théorème de Fermat

Pour tous $p \in \mathbb{P}$ et $a \in \mathbb{Z}$: $\quad a^p \equiv a[p]$, et si $p \wedge a = 1$, i.e. si $p \nmid a$: $\quad a^{p-1} \equiv 1[p]$.

Démonstration.

- Pour tout $k \in [\![1, p-1]\!]$: $\quad k\binom{p}{k} = p\binom{p-1}{k-1}$, $\quad$ donc p divise $k\binom{p}{k}$. Or p est premier et $k \in [\![1, p-1]\!]$, donc p est premier avec k, donc divise $\binom{p}{k}$ d'après le lemme de Gauss, i.e. : $\binom{p}{k} \equiv 0[p]$ $\quad \star$.
- Montrons à présent par récurrence que $a^p \equiv a[p]$ pour tout $a \in [\![0, p-1]\!]$ - comme on raisonne modulo p, ce sera alors vrai aussi pour tout $a \in \mathbb{Z}$.

  Initialisation : $\quad 0^p = 0 \equiv 0[p]$.

  Hérédité : Soit $a \in [\![0, p-2]\!]$. Si $a^p \equiv a[p]$, alors $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \overset{\star}{\equiv} \underbrace{a^p}_{k=p} + \underbrace{1}_{k=0} \overset{\text{HDR}}{\equiv} a + 1[p]$.
- Enfin, si a n'est pas divisible par p : $\quad p \wedge a = 1 \quad$ car p est premier. Or p divise $a^p - a = a\left(a^{p-1} - 1\right)$, donc d'après le théorème de Gauss, p divise $a^{p-1} - 1$, i.e. $a^{p-1} \equiv 1[p]$.

□

Exemple 18.63 – Pour tout $n \in \mathbb{Z}$, tout diviseur premier impair de $n^2 + 1$ est congru à 1 modulo 4 .

Démonstration. Soient $n \in \mathbb{Z}$ et $p \in \mathbb{P} \setminus \{2\}$. On suppose que p divise $n^2 + 1$. Aussitôt $n^2 \equiv -1[p]$ et n n'est pas divisible par p. En outre, p étant impair, $\frac{p-1}{2}$ est un entier, donc d'après le petit théorème de Fermat : $1 \equiv n^{p-1} \equiv \left(n^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}[p]$. $\quad$ Or $(-1)^{\frac{p-1}{2}} \in \{\pm 1\}$ et $p \geqslant 3$, donc cette congruence est en fait une égalité, autrement dit $(-1)^{\frac{p-1}{2}} = 1$. Comme voulu, $\frac{p-1}{2}$ est pair, i.e. $p \equiv 1\ [4]$. □

Exemple 18.64 – Il existe une infinité de nombres premiers congrus à 1 modulo 4 .

Démonstration. Supposons par l'absurde qu'il n'existe qu'un nombre fini de nombres premiers congrus à 1 modulo 4 , notons $p_1, \dots, p_r$ leur liste complète et posons $N = (2p_1 \dots p_r)^2 + 1$. Supérieur ou égal à 2 et impair, N possède un diviseur premier p impair, et comme $p_1, \dots, p_r$ ne divisent pas N, p n'est aucun d'entre eux. Pourtant, d'après l'exemple précédent, p est lui-même congru à 1 modulo 4 - contradiction. □

Remarque 18.65 – Plus généralement, le **TRÈS DIFFICILE** *théorème de la progression arithmétique de Dirichlet*, démontré vers 1840, affirme que pour tous $a, b \in \mathbb{N}^*$ premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo b.

Exemple 18.66 – L'équation $y^2 = x^3 - 3$ d'inconnue $(x, y) \in \mathbb{Z}^2$ n'a pas de solution.

Démonstration. Supposons par l'absurde qu'elle en possède une (x, y). Si x est pair : $y^2 = x^3 - 3 \equiv -3 \equiv 5[8]$, or il n'est pas dur de vérifier que a^2 est congru à 0,1 ou 4 modulo 8 pour tout $a \in \mathbb{Z}$. Conclusion : x est impair. Un simple calcul montre alors que y^2 est pair donc y lui-même est pair, disons $y = 2y'$ pour un certain $y' \in \mathbb{Z}$.
Remarquons alors que : $(x+1)(x^2 - x + 1) = x^3 + 1 = y^2 + 4 = 4(y'^2 + 1)$ ⋆. Or $x^2 - x + 1 = x(x-1) + 1$ est impair, et de plus positif car $x^2 - x + 1 = \left(x - \frac{1}{2}\right)^2 + \frac{3}{4}$. Tout diviseur premier éventuel de $x^2 - x + 1$ se trouve ainsi être impair, donc divise $y'^2 + 1$ d'après ⋆, donc est congru à 1 modulo 4 d'après un exemple précédent. En retour, $x^2 - x + 1$ étant un produit de puissances de ces nombres premiers : $x^2 - x + 1 \equiv 1[4]$, donc $x(x-1)$ est divisible par 4. Comme x est impair, il en découle que $x \equiv 1[4]$, donc enfin que $(x+1)(x^2 - x + 1) \equiv 2[4]$, ce qui contredit la relation ⋆. □

IV – Culture : Quelques questions de recherche actuelles en arithmétique

1 – Conjecture de Syracuse

Définition 18.67 – Soit $a \in \mathbb{N}^*$. La **suite de Syracuse** de a est définie par récurrence :

$$u_0 = a, \qquad \forall n \in \mathbb{N},\ u_{n+1} = \begin{cases} \dfrac{u_n}{2} & \text{si } u_n \text{ est pair} \\ 3u_n + 1 & \text{si } u_n \text{ est impair} \end{cases}$$

Exemple 18.68 – Les premiers termes de la suite associée à 5 :

$$5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \dots$$

Les premiers termes de la suite associée à 15 :

$$15, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \dots$$

Les premiers termes de la suite associée à 18 :

$$9, 28, 14, 7, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \dots$$

Conjecture 18.69 – Conjecture de Syracuse, Collatz 1937

Pour tout $a \in \mathbb{N}$, il existe un rang pour lequel la suite de Syracuse de a vaut 1.

Résultats actuels : La conjecture a été vérifiée jusqu'à 2^{68}. (2020)

Quelle que soit la fonction f vérifiant $\lim_{+\infty} f = +\infty$, la suite de Syracuse partant de presque n'importe quel x finit par descendre sous $f(x)$. (Tao, 2019)

2 – Nombres premiers jumeaux

Définition 18.70 – Soient a et $b \in \mathbb{N}$. On dit que (a,b) est un **couple de nombres premiers jumeaux** si a et b sont premiers tous les deux et $b-a=2$.

Exemple 18.71 – $(3,5)$, $(5,7)$, $(11,13)$, $(59,61)$, ...

Conjecture 18.72

Il existe une infinité de couples de nombres premiers jumeaux.

Résultats actuels : La plus grande paire de nopmbre premiers jumeaux connue est constituée des nombres $2996863034895 \times 2^{1290000} - 1$ et $2996863034895 \times 2^{1290000} + 1$ (Greer, 2016).

Il existe une infinité de couples (a,b) de nombres premiers tels que $|b-a| \leqslant 246$. (Maynard/Tao, 2014).

3 – Conjecture de Goldbach

Conjecture 18.73 – Conjecture de Golbach,1742

Tout nombre entier pair supérieur ou égal à 4 est la somme de deux nombres premiers.

Exemple 18.74 –

$4 = 2+2$

$6 = 3+3$

$12 = 5+7$

$28 = 11+17$

$100 = 11+89 = 17+83$

Résultats actuels : La conjecture est vérifiée au moins jusqu'à 4×10^{18} (Tomás Oliveira e Silva, Siegfried Herzog et Silvio Pardi, 2014).

Tout nombre pair supérieur ou égal à 4 est la somme d'un nombre premier et d'un autre ayant au plus 2 facteurs premiers. (Jingrun, 1966)

Tout entier impair > 5 est la somme de trois nombres premiers. (Helfgott, 2013)

4 – Nombres parfaits

Définition 18.75 – Soit $n \in \mathbb{N}^*$. n est dit **parfait** si il est égal à la somme de ses diviseurs autres que lui-même.

Exemple 18.76 – Les diviseurs de 6 sont 1, 2, 3 et 6. $1+2+3=6$, donc 6 est parfait.
28 et 496 sont également parfaits.

Question 18.77

Les nombres parfaits sont-ils en quantité finie ou infinie?

Résultats actuels : On connait une cinquantaine de nombres parfaits. Le dixième est :

$$19156194260823610729479337808430363813099732154816921 6.$$

Le 47ème (il est prouvé que c'est le 47ème par ordre croissant) a 12 millions de chiffres.

Question 18.78

Existe-t-il un nombre parfait impair?

Résultats actuels : Si un tel nombre existe, il doit être plus grand que 10^{1500}. (Pascal Ochem et Michaël Rao, 2012).

Les spécialistes penchent plutôt vers l'inexistence d'un tel nombre.