

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 –

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 $(a \mid b \text{ et } b \mid a) \iff a = b$.

Démonstration.

□

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.

□

Proposition 18.7

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

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

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 : $n \mid a \iff a \equiv 0[n]$.

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.

□

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

Démonstration.

□

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

Démonstration.

□

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

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

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 –

Démonstration.

□

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.

□

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

Démonstration.

□

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.

□

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 $n \leq a$. 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 $\llbracket 1, a \rrbracket$) 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, $1 \leq a \wedge b \leq \min(a, b)$.

Pour tout entier naturel $a > 0$, $a \wedge 0 = a$.

Par convention, on pose $0 \wedge 0 = 0$.

Exemple 18.19 –

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.

□

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 $a \wedge b = b$.
- ▷ Si $r \neq 0$, alors $a \wedge b = b \wedge r$, donc on recommence en remplaçant a et b par b et r .

Calculons par exemple $210 \wedge 154$.

```

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 $0 \leq b \leq a$. 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 $(u_k)_{0 \leq k \leq N}$ et $(v_k)_{0 \leq k \leq N}$ par : $(u_0, v_0) = (1, 0)$, $(u_1, v_1) = (0, 1)$ et $(u_{k+2}, v_{k+2}) = (u_k - q_{k+2}u_{k+1}, v_k - q_{k+2}v_{k+1})$ pour tout $k \in \llbracket 0, N-2 \rrbracket$. Montrons par récurrence double que $r_k = au_k + bv_k$ pour tout $k \in \llbracket 0, N \rrbracket$.

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 $k \in \llbracket 0, N-2 \rrbracket$. Si $r_k = au_k + bv_k$ et $r_{k+1} = au_{k+1} + bv_{k+1}$:

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

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

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.

$\square$

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 $a_1 \wedge \dots \wedge a_r$.

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 $a_1 \wedge \dots \wedge a_r = a_1 u_1 + \dots + a_r u_r$. 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.

$\square$

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 –

- $\max(a, b) \leq a \vee b \leq ab$
- 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 –**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.

□

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.

□

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 –

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.

□

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.

□

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 $a_1 \wedge \dots \wedge a_r = 1$.
- On dit que $a_1, \dots, a_r$ sont **premiers entre eux deux à deux** si $a_i \wedge a_j = 1$ pour tous $i, j \in \llbracket 1, r \rrbracket$ 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 :

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

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.

□

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.

□

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 : $p \mid ab \iff p \mid a$ 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.

□

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 $b \mid n \not\Rightarrow ab \mid n$. 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.

□

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.

□

Théorème 18.49 – Théorème d'Euclide

Il existe une infinité de nombres premiers.

Démonstration.

□

Crible d'Eratosthène :

Pour déterminer les nombres premiers inférieurs à un entier n fixé, on peut réaliser un **crible d'Eratosthène**. 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 $n \geq 2$, 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.

□

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

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 donc :

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 18.50 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 $a, b \in \mathbb{Z} \setminus \{0\}$: $v_p(ab) = v_p(a) + v_p(b)$.

Démonstration.

□

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

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

Démonstration.

□

Théorème 18.58

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

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

Démonstration.

□

Exemple 18.59 – $360 =$ et $336 =$ donc

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

Corollaire 18.61 – Relation PGCD-PPCM

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

Démonstration.

□

3 – Petit théorème de Fermat

Théorème 18.62 – Petit théorème de Fermat

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

Démonstration.

□

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

Démonstration.

□

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

Démonstration.

□

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.

□

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 :

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

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 :

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

Les premiers termes de la suite associée à 18 :

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

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 – $(3, 5), (5, 7), (11, 13), (59, 61), \dots$

Conjecture 18.72

Il existe une infinité de couples de nombres premiers jumeaux.

Résultats actuels : La plus grande paire de nombres 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 $|b - a| \leq 246$. (Maynard/Tao, 2014).

3 – Conjecture de Goldbach

Conjecture 18.73 – Conjecture de Goldbach, 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 connaît une cinquantaine de nombres parfaits. Le dixième est :

$$191561942608236107294793378084303638130997321548169216.$$

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.