Arithmétique dans $\mathbb{Z}$

Extrait du programme officiel :

L'objectif de ce chapitre est d'étudier les propriétés de la divisibilité des entiers et des congruences.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Divisibilité et division euclidienne	
Divisibilité dans $\mathbb{Z}$, diviseurs, multiples.	Caractérisation des couples d'entiers associés.
Théorème de la division euclidienne.	
b) PGCD et algorithme d'Euclide	
PGCD de deux entiers naturels dont l'un au moins est non nul.	Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans $\mathbb{N}$) de l'ensemble des diviseurs communs à a et b. Notation $a \wedge b$.
Algorithme d'Euclide.	L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $a \wedge b$. $a \wedge b$ est le plus grand élément (au sens de la divisibilité) de l'ensemble des diviseurs communs à a et b.
Extension au cas de deux entiers relatifs.	
Relation de Bézout.	L'algorithme d'Euclide fournit une relation de Bézout. $\leftrightarrows$ I : algorithme d'Euclide étendu. L'étude des idéaux de $\mathbb{Z}$ est hors programme.
PPCM.	Notation $a \vee b$. Lien avec le PGCD.
c) Entiers premiers entre eux	
Couple d'entiers premiers entre eux.	
Théorème de Bézout.	Forme irréductible d'un rationnel.
Lemme de Gauß.	
PGCD d'un nombre fini d'entiers, relation de Bézout. Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux.	
d) Nombres premiers	
Nombre premier.	$\leftrightarrows$ I : crible d'Eratosthène.
L'ensemble des nombres premiers est infini.	
Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers.	
Pour p premier, valuation p-adique.	Notation $v_p(n)$. Caractérisation de la divisibilité en termes de valuations p-adiques. Expressions du PGCD et du PPCM à l'aide des valuations p-adiques.

CONTENUS	CAPACITÉS & COMMENTAIRES
e) Congruences	
Relation de congruence modulo un entier sur $\mathbb{Z}$.	Notation $a \equiv b\ [n]$.
Opérations sur les congruences : somme, produit.	Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont hors programme.
Petit théorème de Fermat.	

TABLE DES MATIÈRES

I Divisibilité et division euclidienne **2**
1 Multiples et diviseurs . . . 2
2 Division euclidienne . . . 3

II Diviseurs communs **4**
1 Définition . . . 4
2 Algorithme d'Euclide . . . 4
3 Relation de Bézout . . . 5
4 Caractérisation du pgcd . . . 8
5 Extension aux entiers relatifs . . . 8
6 Extension à plus de deux entiers . . . 9

III Nombres premiers entre eux **10**
1 Definition . . . 10
2 Propriétés . . . 11
3 Lemme de Gaußet applications . . . 12
4 Généralisation à plus de deux entiers . . . 13

IV Multiples communs **14**
1 Définition et caractérisation du ppcm . . . 14
2 Lien avec le pgcd . . . 15
3 Extension aux entiers relatifs . . . 16

V Nombres premiers **16**
1 Définition . . . 16
2 Propriétés . . . 18
3 Décomposition primaire et valuations p-adiques . . . 19

VI Congruences **21**
1 Définition . . . 21
2 Propriétés . . . 21
3 Petit théorème de Fermat . . . 22

4 Critères de divisibilité 23

I DIVISIBILITÉ ET DIVISION EUCLIDIENNE

1 Multiples et diviseurs

Définition

Si $a, b \in \mathbb{Z}$, on dit que b **divise** a ou que a **est un multiple de** b, et on note $b|a$ lorsque l'on a $k \in \mathbb{Z}$ tel que $a = kb$.
L'ensemble des multiples de b est noté $b\mathbb{Z}$.
Si $a|b$ et $b|a$, a et b sont dit **associés**.

Remarques

R 1 – $b|a \iff a \in b\mathbb{Z} \iff a\mathbb{Z} \subset b\mathbb{Z}$.
R 2 – $b|a \iff |b|||a|$.
R 3 – Si $a \neq 0$, $b|a \implies |b| \leqslant |a|$

Exemple

Diviseurs de 6 : $\{\pm 1, \pm 2, \pm 3, \pm 6\}$. On s'intéresse souvent aux seuls diviseurs positifs.

Propriétés

Soient $a, b, c, d, k, \ell \in \mathbb{Z}$.

(i) La relation | est transitive et réflexive sur $\mathbb{Z}$.
(ii) a et b sont associés si et seulement si $|a| = |b|$ si et seulement si $a = \pm b$.
(iii) $b|a \implies b|ac$
(iv) $b|a$ et $b|c \implies b|(ka + \ell c)$
(v) $b|a$ et $d|c \implies bd|ac$
(vi) $b|a \implies \forall\, n \in \mathbb{N},\ b^n|a^n$

Remarque

Relation d'ordre sur $\mathbb{N}$.

2 Division euclidienne

Théorème : Division euclidienne dans $\mathbb{Z}$

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que

$$\begin{cases} a = bq + r \\ 0 \leqslant r < b \end{cases}$$

*q est le **quotient** et r est le **reste** de la division euclidienne de a par b.*

Démonstration

- **Existence** :
  - ⋆ Si $a \in \mathbb{N}$: par récurrence sur a.
    - si $a < b$, le couple $(0,a)$ convient.
    - si c'est vrai pour jusqu'à $a-1$, avec $a \geqslant b$, alors $a-b = bq'+r'$ avec $0 \leqslant r' < b$. Donc $a = b(q'+1)+r'$. Le couple $(q'+1, r')$ convient.
  - ⋆ Si $a < 0$, on a (q', r') tels que $-a = bq' + r'$ donc $a = b(-q') - r'$.
    - Si $r' = 0$, le couple $(-q', 0)$ convient.
    - Sinon, le couple $(-q'-1, b-r')$ convient.
- **Unicité** : si $a = bq + r = bq' + r'$ avec $0 \leqslant r, r' < b$, alors $b(q-q') = r' - r \in]-b, b[$ donc $q - q' = 0$ puis $r - r' = 0$. □

Remarque

$q = \left\lfloor \frac{a}{b} \right\rfloor = \max\{k \in \mathbb{Z} \mid kb \leqslant a\}$ (autre preuve possible).

Propriété

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. $b|a$ si et seulement si le reste de la division euclidienne de a par b est nul.

Exercice

Déterminer tous les sous-groupes de $(\mathbb{Z}, +)$.
Si $(G,+) < (\mathbb{Z},+)$ non réduit à zéro, considérer $a = \min(G \cap \mathbb{N}^*)$ et montrer que $G = a\mathbb{Z}$ par division euclidienne.

II DIVISEURS COMMUNS

1 Définition

Définition - Propriété

Soient $a, b \in \mathbb{N}$ dont l'un au moins est non nul. Alors l'ensemble des diviseurs positifs communs à a et b admet un plus grand élément, appelé pgcd(a,b) noté $a \wedge b$.

Démonstration

Si, par exemple, $a \neq 0$, c'est une partie non vide (contient 1) de $\mathbb{Z}$, majorée par a. □

Exemple

Si $a = 12$ et $b = 18$, les diviseurs positifs de 12 sont $1, 2, 3, 4, 6, 12$, ceux de 18 sont $1, 2, 3, 6, 9, 18$. Donc $12 \wedge 18 = 6$.

Remarques

R 1 – $a \wedge 0 = a$ car l'ensemble des diviseurs positifs de 0 est $\mathbb{N}$.

R 2 – $a \wedge b = b \wedge a$

2 Algorithme d'Euclide

Propriété

Si $(a, b) \in \mathbb{N}^2 \setminus \{(0,0)\}$, $q \in \mathbb{N}$, alors les diviseurs communs à a et b sont les diviseurs communs à $a - bq$ et b, et en particulier $a \wedge b = (a - bq) \wedge b$.

Propriété : Algorithme d'Euclide[1]

Soient $(a, b) \in \mathbb{N}^2 \setminus \{(0,0)\}$.
On effectue les divisions euclidiennes successives

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\dots \\ \forall\, k,\quad r_{k-1} &= r_k q_{k+1} + r_{k+1} \end{aligned}$$

(en notant $a = r_{-1}$ et $b = r_0$.)
Le procédé s'arrête et le dernier reste non nul vaut $a \wedge b$.

Démonstration

La suite (r_k) est une suite d'entiers strictement décroissante positive d'après la division euclidienne, donc finit par s'annuler.
Si r est le dernier reste non nul, d'après la propriété, $a \wedge b = r \wedge 0 = r$. □

Implémentations en Python :

1. 

Euclide d'Alexandrie (vers -325 - Alexandrie vers -265) est un mathématicien grec. Peu de choses sont connues sur la vie d'Euclide. Il est l'auteur des *Éléments*, traités de géométrie considérés comme l'un des textes fondateurs des mathématiques modernes. Les résultats y sont démontrés avec une rigueur remarquable. Euclide donne des postulats à la base de la géométrie dite euclidienne de nos jours dont le 5ème particulièrement célèbre : par un point passe une et une seule parralèle à une droite fixée. On a longtemps pensé que ce postulat était en fait une conséquence des autres axiomes, jusqu'à ce qu'on construise, au XIXème siècle, une géométrie ne vérifiant pas ce postulat.

```python
def pgcd_rec(a, b):
    "renvoie le pgcd des entiers naturels a et b"
    if b == 0:
        return a
    else:
        return pgcd_rec(b, a % b)
```

Algorithme récursif efficace (terminal) car par de retour nécessaire sur la pile d'évaluation !

```python
def pgcd(a, b):
    "renvoie le pgcd des entiers naturels a et b"
    while b != 0:
        a, b = b, a % b
    return b
```

À la fin de la k^e étape, `a` contient r_{k-1} et `b` contient r_k.

Exemple

$360 \wedge 84 = 12$.

3 Relation de Bézout

Propriété

Si $(a,b) \in \mathbb{N}^2 \setminus \{(0,0)\}$, on peut trouver $(u,v) \in \mathbb{Z}^2$ tels que $au+bv = a \wedge b$.

Démonstration

Par récurrence forte sur b : si $b = 0$, $a \times 1 + 0 \times 0 = a = a \wedge 0$.
Si c'est vrai pour tout entier $< b$, $a \wedge b = b \wedge r$ avec $a = bq + r$, $0 \leqslant r < b$. Par HR, on a $U, V \in \mathbb{Z}$ tels que $bU + rV = b \wedge r = a \wedge b$, soit $bU + (a-q)V = a \wedge b$ donc $aV + b(U - bqV) = a \wedge b$.
Recurrence établie. □

On peut donc tirer des cœfficients de Bezout[1] de l'algorithme d'euclide en en remontant les étapes pour obtenir à chaque fois $a \wedge b$ comme combinaison linéaire de r_k et r_{k-1}.

Si on a déjà $a \wedge b = r_k U + r_{k+1} V$, comme $r_{k-1} = r_k q + r_{k+1}$, on a alors $a \wedge b = r_{k-1} V + r_k (U - qV)$.

Algorithme d'Euclide étendu en Python : C'est facile en récursif :

```python
def euclide_rec(a, b):
    """renvoie (d, u, v) où d = pgcd(a, b) et au + bv = d"""
    if b == 0:
        return (a, 1, 0)
```

1. 

Étienne Bezout (Nemours 1730 - Avon 1783) Éminent mathématicien, adjoint mécanicien à l'Académie des sciences en mars 1758, il fut nommé en 1763 professeur et examinateur des gardes-marine et composa pour eux un Cours de mathématiques en 4 volumes. Membre de l'Académie de marine, il est l'auteur de nombreux ouvrages dont un Traité de navigation (1769) et une Théorie générale des équations algébriques (1779). Bézout contribua beaucoup à orienter dans un sens mathématique la formation des jeunes officiers pour les rendre aptes aux calculs astronomiques les plus savants. Un tel système, où la théorie l'emportait trop souvent sur la pratique, contrairement à ce qui se faisait en Angleterre, provoqua d'assez vives polémiques.

```
    else:
        (q, r) = divmod(a, b)
        (d, u, v) = euclide_rec(b, r)
        return (d, v, u - q * v)
```

Pour une version itérative, c'est plus compliqué.

- On peut garder en mémoire les quotients successifs puis les parcourir de nouveau pour les calculs successifs de u et v :

```
def euclide(a,b):
    """renvoie (d, u, v) où d = pgcd(a, b) et au + bv = d"""
    r, r1, quotients = a, b, []
    while r1 != 0: # Algorithme d'Euclide avec mém. des quot.
        quotients.append(r // r1)
        r, r1 = r1, r % r1
        # k_e tour : r = r[k-1], r1 = r[k], quotients = [q[0],...,q[k]]
    u, v = 1, 0
    while quotients != []: # Parcours de la liste des quotients
        q = quotients.pop()
        u, v = v, u - q * v
    return r, u, v
```

- On peut chercher à chaque étape u_k, v_k tels que $au_k + bv_k = r_k$:
  - ⋆ $r_{-1} = a$ donc $(u_{-1}, v_{-1}) = (1, 0)$,
  - ⋆ $r_0 = b$ donc $(u_0, v_0) = (0, 1)$,
  - ⋆ puis comme $r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$,

$$\begin{aligned} r_{k+1} &= r_{k-1} - q_{k+1} \cdot r_k \\ &= a \cdot (u_{k-1} - q_{k+1} \cdot u_k) + b \cdot (v_{k-1} - q_{k+1} \cdot v_k), \end{aligned}$$

donc

$$\begin{cases} u_{k+1} = u_{k-1} - q_{k+1} \cdot u_k \\ v_{k+1} = v_{k-1} - q_{k+1} \cdot v_k \end{cases}$$

```
def euclide2(a,b):
    """renvoie (d, u, v) où d = pgcd(a, b) et au + bv = d"""
    r, r1 = a, b
    u, v = 1, 0
    u1, v1 = 0, 1
    while r1 != 0:
        q = r // r1
        r, r1 = r1, r % r1
        u, u1 = u1, u - q * u1
        v, v1 = v1, v - q * v1
    return r, u, v
```

À la fin de la k^e étape, `r` contient r_{k-1} et `r1` contient r_k, et `u` et `v` sont tels que $a \cdot u + b \cdot v = r$ et $a \cdot u1 + b \cdot v1 = r1$.

Exemples

E1 – Avec 360 et 84 :

$$360 = 84 \times 4 + 24 \quad (1)$$

$$84 = 24 \times 3 + \boxed{12} \quad (2)$$

De (2) on tire $84-24\times 3=12$ puis de (1), $84-(360-84\times 4)\times 3=12$, soit $84\times 13-360\times 3=12$.
Plus rapidement, on remarque que (2) -3(1) permet d'éliminer les 24 et laisse 12 dans le membre de droite.

E 2 – Même question avec 302 et 112 :

$$\begin{aligned} 302&=112\times 2+78 && +23\times(1)\\ 112&=78\times 1+34 && -16\times(2)\\ 78&=34\times 2+10 && +7\times(3)\\ 34&=10\times 3+4 && -2\times(4)\\ 10&=4\times 2+\boxed{2} && (5)\end{aligned}$$

Soit on remonte les équations en éliminant les restes successifs :

$$(5)-\underbrace{2(4)}_{\text{élim. 4}}+\underbrace{7(3)}_{\text{élim. 10}}-\underbrace{16(2)}_{\text{élim. 34}}+\underbrace{23(1)}_{\text{élim. 78}}$$

donne $302\times 23-112\times 62=2$.
Par l'autre méthode, on remonte équations :

$$\begin{aligned} 2&=10-4\times 2 && && (5)\\ &=10-(34-10\times 3)\times 2 && =-34\times 2+10\times 7 && (4)\\ &=-34\times 2+(78-34\times 2)\times 7 && =78\times 7-34\times 16 && (3)\\ &=78\times 7-(112-78\times 1)\times 16 && =-112\times 16+78\times 23 && (2)\\ &=-112\times 16+(302-112\times 2)\times 23 && && (1)\\ &=302\times 23-112\times 62 && && \end{aligned}$$

Remarques

R 1 – Il n'y a pas unicité, toutes les solutions seront trouvées plus tard (équation diophantienne).

R 2 – La relation de Bézout nous permet d'écrire $a\wedge b\mathbb{Z}\subset a\mathbb{Z}+b\mathbb{Z}$.
Comme $a\wedge b$ divise a et b, on a aussi $a\mathbb{Z}+b\mathbb{Z}\subset a\wedge b\mathbb{Z}$.
Ainsi, $a\mathbb{Z}+b\mathbb{Z}=a\wedge b\mathbb{Z}$.
En fait, comme $a\mathbb{Z}+b\mathbb{Z}$ est un sous-groupe de $(\mathbb{Z},+)$, on sait qu'il s'écrit $d\mathbb{Z}$ avec $d\in\mathbb{N}$ unique. C'est une définition alternative du pgcd (qui redonne directement la relation de Bézout, donc.)

4 Caractérisation du pgcd

Propriété

Soient $(a,b)\in\mathbb{N}^2\setminus\{(0,0)\}$, $d\in\mathbb{Z}$.

$$d=a\wedge b\iff\begin{cases} d\in\mathbb{N}\\ d|a \text{ et } d|b\\ \forall\, d'\in\mathbb{Z},\quad d'|a \text{ et } d'|b\Longrightarrow d'|d\end{cases}$$

Ainsi, $a\wedge b$ est le plus grand diviseur commun au sens de l'ordre $|$ également.

Remarque

Il est alors cohérent de poser $0 \wedge 0 = 0$, avec $0 = \max \mathbb{N}$ pour $|$.

Démonstration

Si $d = a \wedge b$, alors par définition, $d|a$ et $d|b$.
De plus, si $d'|a$ et $d'|b$, alors on a u, v tels que $au + bv = d$, donc $d'|d$.
Réciproquement, si $d|a$ et $d|b$, $d|a \wedge b$, et si $d'|a$ et $d'|b \Longrightarrow d'|d$, alors $a \wedge b|d$. d et $a \wedge b$ sont associés et positifs, donc égaux.
Ou alors : d est un diviseur positif commun, plus grand que tous les autres car vérifiant $d'|d$. □

Corollaire

Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$.

Propriété

Soient $(a, b) \in \mathbb{N}^2 \setminus \{(0,0)\}$, $c \in \mathbb{N}^*$, alors $(ca) \wedge (cb) = c(a \wedge b)$.

Démonstration

$c(a \wedge b) \in \mathbb{N}^*$
$c(a \wedge b)$ divise ca et cb donc $c(a \wedge b) \mid (ca) \wedge (cb)$.
$c(a \wedge b) = cau + cbv$ est divisible par $(ca) \wedge (cb)$. □

5 Extension aux entiers relatifs

Définition

Si $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, alors on pose $a \wedge b = |a| \wedge |b|$.
Il s'agit du plus grand diviseur commun à a et à b.

Propriété

(i) Les diviseurs communs à a et b sont les diviseurs de $a \wedge b$.
(ii) Si $a = bq + r$ (pas necessairement une division euclidienne), $a \wedge b = b \wedge r$.
(iii) On a $u, v \in \mathbb{Z}$ tels que $au + bv = a \wedge b$.
(iv) Si $c \in \mathbb{Z}$, $(ca) \wedge (cb) = |c|(a \wedge b)$.

6 Extension à plus de deux entiers

Définition

Soient $(a_1,\dots,a_n)\in(\mathbb{Z}^*)^n$. On note $a_1\wedge a_2\wedge\cdots\wedge a_n=\bigwedge_{k=1}^{n}a_k$ le plus grand diviseur commun à $a_1,a_2,\dots,a_n$.

Propriété

Si $a,b,c\in\mathbb{Z}^*$, $a\wedge b\wedge c=(a\wedge b)\wedge c=a\wedge(b\wedge c)$.

Plus généralement, les diviseurs communs à $a_1,\dots,a_n$ sont les diviseurs de $\bigwedge_{k=1}^{n}a_k$ et $a_1\wedge a_2\wedge\cdots\wedge a_n=(a_1\wedge a_2\wedge\cdots\wedge a_{n-1})\wedge a_n$.

Démonstration

Les diviseurs communs à a et b sont les diviseurs de $a\wedge b$.
Les diviseurs communs à a,b et c sont donc les diviseurs communs à $a\wedge b$ et c, ou encore les diviseurs communs à a et $b\wedge c$.
On généralise par récurrence. □

Propriété

On a $u_1,\dots,u_n\in\mathbb{Z}$ tels que $a_1u_1+\cdots a_nu_n=\bigwedge_{k=1}^{n}a_k$.

Démonstration

Par récurrence. □

III NOMBRES PREMIERS ENTRE EUX

1 Definition

Définition : Nombres premiers entre eux

$(a,b)\in\mathbb{Z}^2\setminus\{(0,0)\}$ sont dits premiers entre eux lorsque $a\wedge b=1$, c'est-à-dire lorsque le seul diviseur positif commun à a et b est 1.

Exemple

12 et 35 sont premiers entre eux.

Remarque

Tout diviseur de a est alors premier avec tout diviseur de b.

2 Propriétés

Théorème : Théorème de Bézout

$$a \wedge b = 1 \iff \exists\, u, v \in \mathbb{Z},\ \ au + bv = 1$$

Remarque

Les sens $\Longleftarrow$ n'est pas valable pour un pgcd$\neq 1$.

Démonstration

($\Longrightarrow$) a été vu dans le cas général.
($\Longleftarrow$) : si $au + bv = 1$, alors les diviseurs positifs communs à a et b divisent 1, donc il y en a un seul : 1. □

Propriété

Si $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$,

$$d = a \wedge b \iff \begin{cases} d \in \mathbb{N} \\ a = da' \\ b = db' \\ a' \wedge b' = 1 \end{cases}$$

Démonstration

$d|a$ et $d|a'$, et on a $u, v \in \mathbb{Z}$ tels que $da'u + db'v = d$ donc $a'u + b'v = 1$ donc $a' \wedge b' = 1$.
ou alors $d = (da') \wedge (db') = d(a' \wedge b')$ donc $a' \wedge b' = 1$. □

Propriété

$a \wedge bc = 1 \iff a \wedge b = 1$ et $a \wedge c = 1$

Remarque

Se généralise à un produit d'un nombre quelconque d'entiers.

Démonstration

$\Longrightarrow$: Si $a \wedge bc = 1$, alors on a u, v tels que $au + bcv = 1$ donc $a \wedge b = 1$ et $a \wedge c = 1$.
$\Longleftarrow$: Si $a \wedge b = 1$ et $a \wedge c = 1$, alors on a u, v, u', v' tels que

$$(au + bv)(au' + cv') = 1 = a(auu' + bu'v + cuv') + bc(vv')$$

donc $a \wedge bc = 1$. □

3 Lemme de Gaußet applications

Théorème : Lemme de Gauß[1]

Si $a|bc$ et $a \wedge b = 1$, alors $a|c$.

Démonstration

On a $u, v, k \in \mathbb{Z}$ tels que $1 = au + bv$ et $bc = ak$.
Donc $c = acu + bcv = a(cu + kv)$ donc $a|c$. □

Corollaire

Si $a \wedge b = 1$ tels que $a|c$ et $b|c$, alors $ab|c$.

Remarque

C'est faux si $a \wedge b \neq 1$: $6|24$ et $8|24$ mais $6 \times 8 \not| 24$.

Démonstration

On a k, ℓ tels que $c = ak = b\ell$. Par lemme de Gauß, $a|\ell$ danc on a ℓ' tel que $c = ab\ell'$. □

Corollaire : Fractions irréductibles

Tout nombre rationnel $r \in \mathbb{Q}$ s'écrit de manière unique sous la forme $\frac{p}{q}$ avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$.

1. 

Carl Friedrich Gauss (Brunswick 1777 - Göttingen 1855) est un mathématicien, astronome et physicien allemand. Surnommé *le prince des mathématiciens*, il est considéré comme l'un des plus grands mathématiciens de tous les temps. Gauss était un génie particulièrement précoce : à 7 ans (ou 10 selon les sources), il donne la formule calculant $1 + 2 + \cdots + 100$. À 19 ans, il fut le premier à démontrer la loi de réciprocité quadratique. Parmi ses autres prouesses, on peut citer la démonstration du théorème fondamental de l'algèbre, dans sa thèse en 1799, l'invention de la théorie des congruences, la résolution de problèmes de construction à la règle et au compas… Il est considéré comme le fondateur de la géométrie différentielle.

Démonstration

Existence : Si $r = \frac{a}{b}$, alors $a = da'$, $b = db'$ avec $d = a \wedge b$ donne $r = \frac{a'}{b'}$ avec $a' \wedge b' = 1$, le signe pouvant être donné à a'.

Unicité : si $r = \frac{p}{q} = \frac{p'}{q'}$ sous forme irréductible, alors $pq' = p'q$ donc par lemme de Gauß, $q|q'$ et $q'|q$ donc $q = q'$ car positifs. Donc $p = p'$. □

Application : **résolution des équations diophantiennes** $ax + by = c$ où $a, b, c \in \mathbb{Z}^*$ sont fixés, on cherche les solutions entières.

On a facilement qu'il y a des solutions si et seulement si $d = a \wedge b | c$.

Lorsque c'est le cas, on peut trouver une solution particulière (x_0, y_0) avec l'algorithme d'Euclide par exemple.

Alors (x, y) solution si et seulement si $a(x - x_0) = b(y_0 - y)$ si et seulement si $a'(x - x_0) = b'(y_0 - y)$ avec $a' \wedge b' = 1$ en divisant par d.

Par lemme de Gauß, $x = x_0 + b'k$ puis en réinjectant $y = y_0 - a'k$, la réciproque étant vraie.

Ensemble des solutions : $\{(x_0 + b'k, y_0 - a'k) \mid k \in \mathbb{Z}\}$.

Exemple

$199x + 54y = 4$. Ici, par l'algorithme d'Euclide, on a

(1) $199 = 54 \times 3 + 37$ (2) $54 = 37 \times 1 + 17$ (3) $37 = 17 \times 2 + 3$ (4) $17 = 3 \times 5 + 2$ (5) $3 = 2 \times 1 + \mathbf{1}$

Donc $199 \wedge 54 = 1$ et $(5) - (4) + 6(3) - 13(2) + 19(1)$ donne $199 \times 19 - 54 \times 70 = 1$.

On a donc comme solution particulière $x_0 = 76$ et $y_0 = -280$.

Comme ci-dessus, on a ensuite (x, y) est solution de (E) si et seulement si $199(x - x_0) + 54(y - y_0) = 0$ si et seulement si $199(x - x_0) = 54(y_0 - y)$. Comme $199 \wedge 54 = 1$ et $199|54(y_0 - y)$, le théorème de Gaußdonne alors $k \in \mathbb{Z}$ tel que $y_0 - y = 199k$ soit $y = -280 - 199k$. Puis, en remplaçant dans l'équation, $x = x_0 + 54k = 76 + 54k$. On vérifie aisément que la réciproque est vraie.

L'ensemble des solutions est donc $\{(76 + 54k, -280 - 199k) \mid k \in \mathbb{Z}\}$.

4 Généralisation à plus de deux entiers

Définition

$a_1, \ldots, a_n$ sont dits premiers entre eux dans leur ensemble lorsque $\bigwedge_{k=1}^{n} a_k = 1$, c'est-à-dire que le seul diviseur positif commun à tous les a_k est 1.

$a_1, \ldots, a_n$ sont dits premiers entre eux deux à deux lorsque $\forall\, i \neq j,\ \ a_i \wedge a_j = 1$.

Exemple

12, 15 et 20 sont premiers entre eux dans leur ensemble, mais pas deux à deux.

Propriété

Premiers entre eux deux à deux $\Longrightarrow$ premiers entre eux dans leur ensemble, mais la réciproque est fausse pour plus de deux entiers.

Propriété : Théorème de Bézout

$a_1, \dots, a_n$ sont premiers entre eux dans leur ensemble si et seulement si on a $u_1, \dots, u_n$ tels que $a_1u_1 + \cdots + a_nu_n = 1$.

Démonstration

$\Longrightarrow$ a déjà été vu dans le cas général.
$\Longleftarrow$ Si $a_1u_1 + \cdots + a_nu_n = 1$, alors les seuls diviseurs communs à tous les a_k sont des diviseurs de 1 donc ± 1.
□

Propriété

Si $a_1, \dots, a_n$ sont premiers entre eux deux à deux et divisent c, alors $a_1 \cdots a_n | c$.

Remarque

Faux si seulement premiers entre eux dans leur ensemble : $6, 10, 15$ divisent tous trois 30, mais pas leur produit !

Démonstration

Récurrence □

IV MULTIPLES COMMUNS

1 Définition et caractérisation du ppcm

Définition - Propriété

Soient $a, b \in \mathbb{N}^*$. Alors l'ensemble des multiples strictement positifs communs à a et b admet un plus petit élément, appelé ppcm(a, b) noté $a \vee b$.
On pose, de plus, $a \vee 0 = 0 \vee b = 0$.

Démonstration

C'est une partie non vide (contient ab) de $\mathbb{N}$. □

Remarques

R 1 – $a \vee b = b \vee a$

R 2 – Utile pour mettre au même dénominateur !

R 3 – Cette fois, c'est l'ensemble des multiples communs de a et b, $a\mathbb{Z} \cap b\mathbb{Z}$ qui est un sous-groupe de $(\mathbb{Z}, +)$ donc $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ avec $m \in \mathbb{N}$ unique étant le ppcm de a et b.

Exemple

Multiples >0 de 6 : $0, 6, 12, 18, \ldots$
Multiples >0 de 9 : $0, 9, 18, \ldots$
Donc $6 \vee 9 = 18$.

Propriété : Caractérisation

Soient $(a,b) \in (\mathbb{N}^*)^2$, $m \in \mathbb{Z}$.

$$m = a \vee b \iff \begin{cases} m \in \mathbb{N}^* \\ a|m \text{ et } b|m \\ \forall\, m' \in \mathbb{Z},\ \ a|m' \text{ et } b|m' \Longrightarrow m|m' \end{cases}$$

Ainsi, $a \vee b$ est le plus plus petit multiple commun >0 au sens de l'ordre $|$ également.

Démonstration

Si $m = a \vee b$, alors $m \in \mathbb{N}^*$ et $a|m$ et $b|m$ par définition. Si de plus, $a|m'$ et $b|m'$, alors par division euclidienne, $m' = mq + r$ avec $0 \leqslant r < m$ et r multiple commun à a et b, donc $r = 0$ et $m|m'$.
Réciproquement, si les trois propriétés sont vérifiées, m est un multiple >0 commun à a et b tel que les autres multiples communs >0 sont divisibles, donc plus grands que m. Il s'agit bien du plus petit d'entre eux.
Ou alors : $a|m$ et $b|m$ donc $(a \vee b)|m$, et $a|(a \vee b)$ et $b|(a \vee b)$ donc $m|(a \vee b)$. □

Corollaire

Les multiples communs à a et b sont les multiples de $a \vee b$.

Propriété

Si $a, b, c \in \mathbb{N}^*$, $(ca) \vee (cb) = c(a \vee b)$.

Démonstration

- $c(a \vee b) \in \mathbb{N}^*$
- $c(a \vee b)$ est un multiple commun à ca et cb donc $(ca) \vee (cb) \,|\, c(a \vee b)$.
- Si $ca|m'$ et $cb|m'$ alors $c|m'$ donc $m' = ck$ avec $a|k$ et $b|k$ donc $a \vee b|k$ donc $c(a \vee b)|m'$.

Par caractérisation, $(ca) \vee (cb) = c(a \vee b)$ □

2 Lien avec le pgcd

Propriété

Si $a, b \in \mathbb{N}^*$, $(a \wedge b)(a \vee b) = ab$.
En particulier, si $a \wedge b = 1$, $a \vee b = ab$.

Démonstration

- Si $a \wedge b = 1$,
  - ⋆ $a|(a \vee b)$ et $b|(a \vee b)$ et $a \wedge b = 1$ donc $ab|(a \vee b)$.
  - ⋆ ab multiple commun à a et b donc $(a \vee b)|ab$.
  - ⋆ Tout est $\geqslant 0$: $a \vee b = ab$.
- Sinon, si $d = a \wedge b$, $a = da'$, $b = db'$ avec $a' \wedge b' = 1$.
  $(a \vee b)(a \wedge b) = d^2(a' \vee b') = d^2 a'b' = ab$. □

Exemple

$6 \wedge 9 = 3$ donc $6 \vee 9 = \dfrac{6 \times 9}{3} = 18$. Ou : $6 \wedge 9 = 3(2 \wedge 3) = 3 \times 6 = 18$.

3 Extension aux entiers relatifs

Définition

Si $(a, b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$, alors on pose $a \vee b = |a| \vee |b|$.
Il s'agit du plus petit multiple commun > 0 de a et b s'ils sont non nuls.

Propriété

(i) *Si* $c \in \mathbb{Z}^*$, $(ca) \vee (cb) = |c|(a \vee b)$.

(ii) $(a \wedge b)(a \vee b) = |ab|$.

V NOMBRES PREMIERS

1 Définition

Définition

Un **nombre premier** est un entier naturel $p \geqslant 2$ dont les seuls diviseurs positifs sont 1 et p.
On notera $\mathscr{P}$ l'ensemble des nombres premiers.

Remarques

R 1 – 1 n'est pas premier.

R 2 – 2 est le seul nombre premier pair.

R 3 – Un nombre premier possède exactement 4 diviseurs : ± 1 et $\pm p$.

R 4 – Pour qu'un nombre entier n soit premier, il faut et il suffit qu'il n'ait pas de diviseur entre 2 et $\sqrt{n}$. D'où le test basique de primalité :

```
def est_premier(n):
    """teste si n est un nombre premier."""
    if n < 2:
```

```
        return False
    k = 2
    premier = True
    while k ** 2 <= n and premier:
        premier = (n % k != 0) # passe à False si k | n
        k += 1
    return premier
```

R 5 – **Crible d'Eratosthène** : Pour déterminer les nombres premiers $\leqslant n$, il suffit de dessiner dans un tableau contenant tous les entiers de 2 à n, puis barrer successivement les multiples (stricts) de 2, puis de 3, etc. jusqu'à $\sqrt{n}$.

		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

Implémentation en Python :

```
def crible(N):
    """Liste des nombres premiers <= N"""
    estPremier = [False for _ in range(N + 1)]
    estPremier[0:2] = [False, False]
    # A la fin de l'algo., on veut que
    # k soit premier ssi estPremier[k] contient True
    k = 2
    while k ** 2 <= N:
        if estPremier[k]:  # Si k est un nombre premier
            m = k * k
            # premier multiple potentiellement non encore rencontré
            while m <= N:    # Suppression des multiples de k
                estPremier[m] = False
                m += k
        k += 1
    return [k for k in range(N + 1) if estPremier[k]]
```

2 Propriétés

Propriété

Tout entier $\notin \{0, \pm 1\}$ possède un diviseur premier.

Remarques

R 1 – Tout entier $n \in \mathbb{N}^* \setminus \{1\}$ composé possède un diviseur premier $\leqslant \sqrt{n}$ (car si $n = k\ell$ alors $k \leqslant \sqrt{n}$ ou $\ell \leqslant \sqrt{n}$.)

R 2 – Conséquence : a et b sont premiers entre eux si et seulement s'ils n'ont pas de diviseur premier en commun.

Démonstration

$E = \{d \in \mathbb{N} \mid d \geqslant 2 \text{ et } d|n\}$ est non vide car $|n| \in E$, partie de $\mathbb{N}$, donc admet un plus petit élément p.
Si p admet un diviseur $k \geqslant 2$, alors $k \in E$ donc $k \geqslant p$ donc $k = p$: p est premier. □

Propriété

L'ensemble des nombres premiers est infini.

Démonstration

Sinon, $\mathscr{P} = \{p_1, \dots, p_n\}$ et $N = p_1 \cdots p_n + 1 \geqslant 2$ n'aurait pas de diviseur premier. □

Propriété

Si $p \in \mathscr{P}$ et $n \in \mathbb{Z}$, soit $p|n$, soit $p \wedge n = 1$.

Démonstration

Si $d = p \wedge n | p$ donc $d \in \{1, p\}$. □

Propriété

Soient $p \in \mathscr{P}$ et $a_1, \dots, a_n \in \mathbb{Z}$.
$p|(a_1 \times \cdots \times a_n)$ si et seulement si p divise l'un des a_k.

Remarque

C'est faux si p n'est pas premier !

Démonstration

$\Longleftarrow$: ok
$\Longrightarrow$: par contraposée, si p ne divise aucun des a_k, il est premier avec chacun d'entre eux donc avec leur

produit, donc il ne le divise pas. □

3 Décomposition primaire et valuations p-adiques

Théorème : Décomposition primaire

Soit $n \in \mathbb{Z}^*$. On peut trouver $k \in \mathbb{N}$, $p_1, \dots, p_k$ premiers deux à deux distincts, $\alpha_1, \dots, \alpha_k \in \mathbb{N}^*$ tels que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

appelée décomposition primaire de n.
De plus, cette écriture est unique à l'ordre des facteurs près.
$p_1, \dots, p_k$ sont les diviseurs premiers de n.

Remarque

Cette décomposition peut aussi s'écrire $n = \pm \prod_{p \in \mathscr{P}} p^{\alpha_p}$ avec les α_p éventuellement nuls lorsque p n'est pas un diviseur de n. Les cœfficients α_p sont toujours uniques.

Démonstration

- **Existence** : Il suffit de le montrer pour $n \in \mathbb{N}^*$. Par récurrence forte.
  - ⋆ C'est vrai pour $n = 1$ avec $k = 0$ (produit vide) et pour $n = p \in \mathscr{P}$.
  - ⋆ Si c'est vrai jusqu'à $n-1$ pour un certain $n \in \mathbb{N}^*$, alors n a un diviseur premier p. Alors $n = pn'$ avec $n' < n$. en appliquant HR à n' et en multipliant par le nombre premier p, on obtient le résultat sur n.
- **Unicité** : $\pm$ est le signe de n, donc unique.
  Les p_k sont nécessairement les diviseurs premiers de n, donc uniques. Leur nombre l'est aussi d'où l'unicité de k.
  Puis nécessairement $\alpha_k = \max\{i \in \mathbb{N} \mid p_k^i | n\}$ donne l'unicité de α_k. □

Exemple

$7\,007 = 7^2 \times 11^1 \times 13^1$.

Définition

Soit $p \in \mathscr{P}$ et $n \in \mathbb{Z}^*$.
On appelle **valuation p-adique** de n l'entier

$$v_p(n) = \max\{i \in \mathbb{N} \mid p^i | n\}.$$

Exemple

$v_7(7007) = 2$, $v_{11}(7007) = v_{13}(7007) = 1$, sinon $v_p(7007) = 0$.

Remarque

La décomposition primaire se réécrit $n = \pm \prod_{p\in\mathscr{P},\ p|n} p^{v_p(n)} = \pm \prod_{p\in\mathscr{P}} p^{v_p(n)}$.

Propriété

Soient $n, m \in \mathbb{Z}^*$, $p \in \mathscr{P}$.

(i) $v_p(n) \neq 0 \iff p|n$

(ii) $v_p(n \times m) = v_p(n) + v_p(m)$

(iii) $n|m \iff \forall\, p \in \mathscr{P},\ \ v_p(n) \leqslant v_p(m)$

(iv) $v_p(n \wedge m) = \min(v_p(n), v_p(m))$ *et* $v_p(n \vee m) = \max(v_p(n), v_p(m))$

Démonstration

(i) évident.

(ii) $nm = \pm \prod_{p\in\mathscr{P}} p^{v_p(n)} \times p^{v_p(m)} = \prod_{p\in\mathscr{P}} p^{v_p(n)+v_p(m)}$ puis on conclut par unicité de la décomposition primaire.

(iii) $\Longleftarrow$: par décomposition primaire.
$\Longrightarrow$: si $n|m$, alors $n = km$ donc $\forall\, p \in \mathscr{P},\ \ v_p(n) = v_p(k) + v_p(m) \geqslant v_p(m)$.
ou bien $\{i \in \mathbb{N} \mid p^i | n\} \subset \{i \in \mathbb{N} \mid p^i | m\}$.

(iv) $n \wedge m$ est un diviseur commun, donc $v_p(n \wedge m) \leqslant \min(v_p(n), v_p(m))$.
$p^{\min(v_p(n),v_p(m))}$ est un diviseur commun à n et m, donc divise $n \wedge m$, donc $\min(v_p(n), v_p(m)) \leqslant v_p(n \wedge m)$.
Pour $n \vee m$, il suffit d'écrire que $(n \wedge m)(n \vee m) = |nm|$ ou de faire la même chose. □

Remarque

Si $a = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ et $b = \pm p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ avec des exposants éventuellement nuls, alors

$$a \wedge b = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}$$

et

$$a \vee b = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Exemple

$352 = 2^5 \times 11$ et $1452 = 2^2 \times 3 \times 11^2$.
Donc $352 \wedge 1452 = 2^2 \times 11 = 44$ et $352 \vee 1452 = 2^5 \times 3 \times 11^2 = 11616$.

Exercices

Ex 1 – Si p est premier, montrer que $\sqrt{p} \notin \mathbb{Q}$.
Si $\sqrt{p} = \frac{a}{b}$, alors $2v_p(a) = 2v_p(b) + 1$, contradiction.

Ex 2 – $\sqrt{n} \in \mathbb{Q}$ si et seulement si n est un carré parfait.
Si $\sqrt{n} = \frac{a}{b}$, alors $a^2 = n \times b^2$, $\forall\, p \in \mathscr{P},\ \ 2v_p(a) = v_p(n) + 2v_p(b)$ donc $\forall\, p \in \mathscr{P},\ \ v_p(n) \in 2\mathbb{N}$, donc n est un carré parfait.
Ou encore : si $\sqrt{n} = \frac{a}{b}$ sous forme irréductible, alors $a^2 = n \times b^2$ donc $b^2 | a^2$. Or $a \wedge b = 1$ donc $b^2 = a^2 \wedge b^2 = 1$

donc $n = a^2$.

Ex 3 – Démontrer que le nombre de diviseurs positifs de n est $\prod_{p\in\mathcal{P}, p|n} (v_p(n)+1)$.

VI CONGRUENCES

1 Définition

Définition

Soit $n \in \mathbb{N}^*$. On dit que $a, b \in \mathbb{Z}$ sont **congrus modulo** n et on note $a \equiv b \ [n]$ lorsque $n|(a-b)$ ie lorsqu'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

Remarque

On a déjà vu qu'il s'agit d'une relation d'équivalence, dont l'ensemble des classes noté $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \ldots, \overline{n-1}\}$ contient les entiers modulo n.

2 Propriétés

Propriété

$\forall\, a \in \mathbb{Z},\ \exists!\, r \in [\![0, n-1]\!] \mid a \equiv r \ [n]$.
r est le reste de la division euclidienne de k par n.
Il y a donc exactement n classes d'équivalences : $\bar{0}, \bar{1}, \ldots, \overline{n-1}$.

Propriété

$n|k \iff k \equiv 0 \ [n]$.

Propriété : Compatibilité de + et ×

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b \ [n]$ et $c \equiv d \ [n]$.
alors $a + c \equiv b + d \ [n]$ et $a \times c \equiv b \times d \ [n]$.
Plus généralement, si $m \in \mathbb{N}$, $a^m \equiv b^m \ [n]$.

Exemples

E 1 – Reste de la division euclidienne de 2^{10} par 3 ? $2 \equiv -1 \ [3]$ donc $2^{10} \equiv 1 \ [3]$.

E 2 – $\forall\, n \in \mathbb{N},\ 7|3^{2n+1} + 2^{n+2} : 9 \equiv 2 \ [7]$ donc $3^{2n+1} \equiv 3 \times 2^n \equiv -4 \times 2^n \equiv -2^{n+2} \ [7]$ d'où le résultat.

Remarques

R 1 – Pour effectuer des calculs modulaires, il est souvent intéressant de se ramener à un nombre le plus petit possible en valeurs absolue : entre $-\left\lfloor \frac{n}{2} \right\rfloor$ et $\left\lfloor \frac{n}{2} \right\rfloor$.

R 2 – Ces propriétés permettent de créer des lois + et × sur $\mathbb{Z}/n\mathbb{Z}$ (la somme et le produit de deux entiers modulo n ne dépendent pas des représentants choisis.)

Propriétés

Soit $c \neq 0$.

(i) $ac \equiv bc \ [nc] \Rightarrow a \equiv b \ [n]$.

(ii) Si $c \wedge n = 1$ *alors* $ac \equiv bc \ [n] \Rightarrow a \equiv b \ [n]$.

Remarque

Pour que $\bar{k}$ soit inversible dans $\mathbb{Z}/n\mathbb{Z}$, il faut trouver ℓ tel que $\bar{k} \times \bar{\ell} = \bar{1}$, c'est-à-dire $k\ell \equiv 1 \ [n]$ soit encore $k\ell + np = 1$ ce qui équivaut à $k \wedge n = 1$.
En particulier, $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

Exemple

$2 \equiv 12 \ [10]$ mais $1 \not\equiv 6 \ [10]$. Cependant, $1 \equiv 6 \ [5]$.

3 Petit théorème de Fermat

Lemme

Soit p un nombre premier et $k \in [\![1, p-1]\!]$. Alors $p \left| \binom{p}{k} \right.$.

Démonstration

Comme $k\binom{p}{k} = p\binom{p-1}{k-1}$, $p \left| k \times \binom{p}{k} \right.$ et comme $p \nmid k$ et p est premier, $p \left| \binom{p}{k} \right.$. □

Théorème : Petit théorème de Fermat[1]

Soit p un nombre premier et $a \in \mathbb{Z}$.

$$a^p \equiv a \ [p].$$

En particulier, si $p \nmid a$, alors $a^{p-1} \equiv 1 \ [p]$.

Démonstration

Par récurrence sur $a \in \mathbb{N}$:
- **Initialisation** : Comme $p > 0$, $0^p = 0 \equiv 0 \ [p]$.
- **Hérédité** : Si c'est vrai pour un $a \geqslant 0$, alors $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \equiv a+1 \ [p]$ par le lemme puis HR, ce qui établit la récurrence.

Si $a \in \mathbb{Z}^-$, $-a \in \mathbb{N}$ et $a^p = (-1)^p(-a)^p \equiv (-1)^p(-a) \ [p]$.
- Soit $p = 2$ et on obtient $a^p \equiv (-a) \equiv a \ [2]$ car $-1 \equiv 1 \ [2]$.
- Soit p est impair et $a^p \equiv -(-a) \equiv a \ [p]$. □

Remarque

Si $p|a$, $a^{p-1} \equiv 0 \ [p]$.

Exemple

Reste de la division euclidienne de 2713^{217} par 5 : $2713^{217} \equiv 3^{217} \ [5]$ or $3^4 \equiv 1 \ [5]$ d'après le petit théorème de Fermat, et $217 = 4 \times n + 1$, donc $2713^{217} \equiv 3 \ [5]$.

On peut aussi remarquer que $213 \equiv -2 \ [5]$ et $(-2)^2 \equiv -1 \ [5]$.

4 Critères de divisibilité

Si $a_0, \ldots, a_k$ sont les chiffres de n en base 10, $n = a_0 + a_1 \times 10 + \cdots + a_k \times 10^k$, $\forall\, i, \ \ a_i \in [\![0,9]\!]$.

Divisibilité par 2 : $10^i \equiv 0 \ [2]$ donc $2|n \iff 2|a_0 \iff a_0 \in \{0,2,4,6,8\}$

Divisibilité par 3 : $10^i \equiv 1 \ [3]$ donc $3|n \iff 3 \left| \sum_{i=0}^{k} a_i \right.$

Divisibilité par 4 : $10^i = 10^{i-2} \times 100 \equiv 10^{i-2} \times 0 \equiv 0 \ [4]$ si $i \geqslant 2$ donc $4|n \iff 4|\overline{a_1 a_0}^{10}$

Divisibilité par 5 : $10^i \equiv 0 \ [5]$ si $i \geqslant 1$ donc $5|n \iff 5|a_0 \iff a_0 \in \{0,5\}$

1. 

Pierre de Fermat (Beaumont-de-Lomagne, première décennie du XVIIe siècle - Castres, 1665) est un magistrat, polymathe et surtout mathématicien français, surnommé « le prince des amateurs ». Il est en même temps un habile latiniste et helléniste. Il s'est aussi intéressé aux sciences physiques ; on lui doit notamment le principe de Fermat en optique. Il a contribué avec Descartes à la création de la géométrie analytique (par sa méthode générale pour la détermination des tangentes à une courbe plane), à celle du calcul infinitésimal (avec Leibniz et Newton), et à celle du calcul des probabilités (avec Pascal). Une partie de sa notoriété est due au "Grand théorème de Fermat" : l'équation $x^n + y^n = z^n$ n'a pas de solution entière pour n différent de 2. « J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir », avait-il noté. Il a fallu attendre 1994 pour avoir une solution complète, et que cette conjecture prenne le nom de *Théorème de Fermat-Wiles*. La démonstration de A. Wiles repose sur des méthodes que Fermat ne pouvait pas avoir utilisées, s'il avait une "merveilleuse" démonstration complète, celle-ci n'a pas encore été retrouvée, malgré les travaux de nombreux mathématiciens depuis 350 ans, recherches qui sont pour une part à l'origine du développement de la théorie des nombres.

Divisibilité par 8 : $10^i = 10^{i-3} \times 1000 \equiv 10^{i-3} \times 0 \equiv 0$ [8] si $i \geqslant 3$ donc $8|n \iff 8|\overline{a_2 a_1 a_0}^{10}$

Divisibilité par 9 : $10^i \equiv 1$ [9] donc $9|n \iff 9\left|\sum_{i=0}^{k} a_i\right.$

Divisibilité par 11 : $10^i \equiv -1$ [11] donc $11|n \iff 11|(a_0 - a_1 + a_2 - \cdots)$

Exemples

E1 – Justifier que le calcul $1\,994\,996 \times 26\,399\,273 = 52\,666\,454\,037\,908$ est faux : preuve par 9 en réduisant modulo 9.

E2 – Soit $n = 4444^{4444}$. f : $k \mapsto$ somme des chiffres de k. Calculer $f \circ f \circ f(n)$.
$f(n) \equiv n$ [9]. Or $4444 = 9 \times 493 + 7$, donc $4444 \equiv 7$ [9] et $4444^{4444} \equiv 7^{4444}$ [9].
Mais $7^2 \equiv 4$ [9], $7^3 \equiv -2$ [9] et $7^3 \equiv 1$ [9]. D'où $7^{4444} = 7^{3k+1} \equiv 7$ [9] donc $f(n) \equiv 7$ [9]. Puis $f(f(f(n))) \equiv 7$ [9].
De plus, $n \leqslant 10000^{5000} = 10^{20000}$. Donc n possède au plus 20 000 chiffres et $f(n) \leqslant 9 \times 20000 = 180000$.
Puis $f(f(n)) \leqslant 1 + 8 + 4 \times 9 = 45$ et $f(f(n)) \equiv f(n) \equiv 7$ [9].
Donc $f(f(f(n))) < 4 + 9 = 13$ et $f(f(f(n))) \equiv 7$ [9]. Donc $f(f(f(n))) = 7$.