Chapitre 2

Notions d'Arithmétique

Introduction

Quand vous avez appris l'addition et la multiplication, vous avez commencé par additionner et multiplier des entiers, puis des nombres décimaux, des nombres réels... et vous avez sans doute eu la sensation que cela revenait au même : En tant qu'opérations, l'addition des entiers ou des réels, la multiplication des entiers ou des réels se manipulent quasiment de la même manière. Et pourtant, les entiers et les réels sont deux objets mathématiques très différents. L'arithmétique, qui est l'étude des nombres entiers, est un chapitre à part et réputé difficile des mathématiques, où certains problèmes d'apparence anodine peuvent rester des siècles sans solution.

Il est donc fondamental, quand des nombres apparaissent dans un problème, de bien voir s'il s'agit de nombres entiers ou de nombres réels, en sachant que les méthodes de résolution n'ont rien à voir et la difficulté est tout autre. Sauf lorsque cela sera précisé, les nombres qui interviennent dans ce chapitre sont des entiers relatifs (positifs, négatifs ou nuls), éléments de $\mathbb{Z}$.

2.1 Divisibilité

Une notion joue un rôle essentiel dans l'étude des nombres entiers, et elle est dénuée de tout intérêt dans l'étude des nombres réels : la divisibilité.

Défintion : Un entier a est dit divisible par un entier b s'il existe un entier q tel que $a = bq$.

On dit également que b divise a, ou que b est un diviseur de a, et on note $b|a$.

Signalons tout de suite quelques propriétés immédiates de la divisibilité :

Propriétés :

1) tout entier $a \in \mathbb{Z}$ divise 0 et est divisible par 1 et a ,

2) si $a|b$ et $b|c$, alors $a|c$,

3) soit m un entier non nul, alors $a|b$ si et seulement si $ma|mb$,

4) si $a|b$ et $a|c$, alors $a|bx + cy$ pour tous entiers x et y , en particulier $a|b - c$ et $a|b + c$.

5) il n'existe pas d'entier strictement compris entre 0 et 1. cette proporiété est fondamentale

Comme aplication par exemple, si b divise a et $|b| > |a|$, alors $a = 0$, sinon, en écrivant $a = bq$, le quotient $|q| = |a|/|b|$ serait un entier strictement compris entre 0 et 1.

2.2 Division euclidienne

Les principales propriétés de la divisibilité des entiers découlent de la division euclidienne

Théorème : (Division euclidienne)

Soit b un entier strictement positif. Tout entier $a \in \mathbb{Z}$ s'écrit, de manière unique, sous la forme $a = bq + r$ avec $\quad q \in \mathbb{Z}$ et $0 \leq r < b$.

Le reste r de la division euclidienne joue un rôle plus important que le quotient q, et le fait que r soit strictement inférieur à b est essentiel.

Preuve : Pour prouver l'existence des entiers q et r, on considère la progression arithmétique $.., a + 2b, a + b, a, a - b, a - 2b, ...$ et on appelle $r = a - qb$ le plus petit terme positif ou nul de la progression.

Si r était supérieur ou égal à b, $r - b = a - (q + 1)b$ serait un terme positif ou nul de la progression, strictement inférieur à r, ce qui contredit l'hypothèse.

Quant à l'unicité, si $a = bq + r = bq' + r'$, la différence $r - r' = b(q' - q)$ est divisible par b.

Or $|r - r'| < b$. Donc $r - r' = 0$, i.e $r = r'$ et $q = q'$.

2.3 Numération

Depuis bien longtemps, nous écrivons les entiers en base 10 : il y a 10 symboles $(0, 1, 2, ..., 9)$ et chaque nombre s'écrit avec un chiffre des unités, un chiffre des dizaines, des centaines, etc.

Nous allons étudier cette façon d'écrire les entiers et la généraliser à d'autres bases.

La base 2 est utilisée au coeur des ordinateurs : il y a alors 2 symboles 0 et 1, correspondant à deux états électriques possibles : tension nulle / non-nulle aux bornes d'un composant.

Proposition : Soit b un entier supérieur ou égal à 2. Pour tout entier naturel n, il existe un entier $k > 0$ et des entiers $c_0, ..., c_k \in \{0, ..., b - 1\}$ tels que l'on ait :

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0.$$

On peut en outre imposer les conditions $k = 0$ si $n = 0$, et $c_k \neq 0$ si $n \neq 0$.

Ce qui détermine les entiers k et $c_0, ..., c_k$ de manière unique.

Par exemple, si $b = 10$, on a $1729 = 1 \cdot 10^3 + 7 \cdot 10^2 + 2 \cdot 10 + 9$.

Si la base est autre que 10, on écrit $n = c_k c_{k-1} ... c_0$, voire $\overline{n = c_k c_{k-1} ... c_0}^{(b)}$ si l'on veut préciser la base.

En pratique, on représente chaque entier entre 0 et $b - 1$ par un symbole.

Si $b \leq 10$, le choix $0, ..., b - 1$ s'impose.

Pour les bases supérieures à 10, il est courant d'employer les lettres majuscules (c'est ce qu'utilisent les informaticiens pour l'hexadécimal ,la base 16), ou les lettres grecques.

On écrira par exemple $\overline{A6B}^{(16)}$ pour $10 \times \ 16^2 + 6 \times \ 16 + 11 = 2560 + 96 + 11 = 2667$.

Démontrons la proposition :

On démontre l'existence par récurrence sur n.

Pour $n = 0$, on peut écrire $n = 0$, avec $k = 0$ et $c_0 = 0$.

Supposons qu'on puisse écrire de la sorte tout entier strictement inférieur à n.

Soit alors q et r le quotient et le reste de la division euclidienne de n par b. On a bien $0 \leq r \leq b-1$.

Comme $q \leq n/b < n$, l'entier q s'écrit sous la forme $d_m b^m + d_{m-1}b^{m-1}+\cdots+d_0$, où les d_i sont des entiers compris entre 0 et $b-1$, avec $m = 0$ si $q = 0$, et $c_m \neq 0$ si $q \neq 0$.

On a

$n = bq + r = b(d_m b^m + d_{m-1}b^{m-1}+\cdots+d_0) + r = c_k b^k+\cdots+c_1 b + c_0$,

en posant $c_0 = r, k = m+1$, et $c_i = d_{i-1}$ si $1 \leq i \leq m+1$.

ce qui montre l'existence d'une écriture de l'entier n en base b.

Démontrons maintenant l'unicité, toujours par récurrence sur n.

Elle est vraie si $n = 0$, et même si $n < b$.

Supposons qu'il y ait unicité pour tout entier strictement inférieur à n et supposons qu'un entier n supérieur ou égal à b s'écrive à la fois $c_k b^k+\cdots+c_0$ et $d_m b^m+\cdots+d_0$.

Comme on a supposé $n > b$, on a $k > 1$ et $m > 1$.

Alors, l'écriture $n = b(c_k b^{k-1}+\cdots+c_1) + c_0 = b(d_m b^{m-1}+\cdots+d_1) + d_0$

montre que le reste de la division euclidienne de n par b est égal à c_0 et à d_0.

On a donc $c_0 = d_0$,

et alors $\frac{n-c_0}{b} = c_k b^{k-1}+\cdots+c_1 = d_m b^{m-1}+\cdots+d_1$.

Ce sont deux écritures en base b de l'entier $(n-c_0)/b$, qui est inférieur à n , elles coïncident donc,

ce qui entraîne $k-1 = m-1$, d'où $k = m$, et $c_i = d_i$ pour $1 \leq i \leq k$. C.Q.F.D.

Dans la démonstration, les chiffres du développement en base b sont déterminés de la droite vers la gauche, par des divisions euclidiennes par b.

C'est ainsi qu'on procède en pratique.

Écrivons par exemple 1729 en base 7.

La division euclidienne de 1729 par 7 s'écrit $1729 = 7\times247+0$, puis on a $247 = 7\times35+2$, puis $35 = 7\times5$. Ainsi, $1729 = 7\times247+0 = 7\times(7\times35+2)+0 = 7^3\times5+7\times2+0$,

donc 1729 s'écrit $\overline{5020}^{(7)}$ en base 7.

Pour convertir, par exemple, l'entier $\overline{6353}^{(8)}$, de la base 8 à la base 10, on peut procéder de deux manières.

La première est la plus lourde et consiste à écrire :

$\overline{6353}^{(8)} = 6\times8^3+3\times8^2+5\times8+3 = 6\times512+3\times64+5\times8+3 = 3072+192+40+3 = 3307$

puisque $8^2 = 64$ et $8^3 = 8\times64 = 512$.

Il est cependant plus facile et moins coûteux d'écrire

$\overline{6353}^{(8)} = 3+8(5+8(3+8\times6)) = 3+8(5+8(51)) = 3+8(413) = 3+3304 = 3307$.

Cela revient à écrire

$c_k b_k+\cdots+c_0 = c_0 + b(c_1 + b(c_2 + b(c_3+\cdots+b\times c_k)))$,

Cette méthode est parfois appelée méthode de HÖRNER.

2.4 Algorithme d'Euclide

Etant donnés deux nombres entiers a et b, nous pouvons nous demander quels sont les nombres qui sont diviseurs de a et de b. On les appelle les diviseurs communs de a et b.

Par exemple, si l'on prend $a = 24$ et $b = 18$, on constate que les diviseurs communs sont $2, 3$ et 6.

Le plus grand des diviseurs communs joue un rôle important :

Définition : Soient a et b des entiers . L'entier naturel d est appelé le plus grand commun diviseur (pgcd) de a et b s'il satisfait les deux propriétés suivantes :

(i) $d|a$ et $d|b$,

(ii) si $d'|a$ et $d'|b$ alors $d' \leq d$ pour tout $d' \in \mathbb{N}$

Le pgcd de a et b est noté $\text{pgcd}(a, b)$, ou tout simplement (a, b).

Dans l'exemple ci-dessus, on a $(18, 24) = 6$.

On peut définir de la même manière le pgcd de n nombres $a_1, a_2, ..., a_n$ qui sera noté $(a_1, a_2, ..., a_n)$.

Par exemple, on a $(15, 18, 24) = 3$.

Définition : On dit que deux nombres entiers a et b sont premiers entre eux si leur pgcd est 1, autrement dit si $(a, b) = 1$.

On dira que les nombres $a_1, a_2, ..., a_n$ sont premiers deux à deux si $(a_i, a_j) = 1$ pour $i \neq j$.

Remarquons que si les nombres $a_1, a_2..., a_n$ sont premiers deux à deux, alors on a $(a_1, a_2, ...an) = 1$. Mais la réciproque n'est pas vraie. En effet :

On a $(15, 3, 5) = 1$ mais 3 et 15 ne sont pas premiers entre eux car $(3, 15) = 3$.

Nous allons donner maintenant un algorithme (L'algorithme d'Euclide) qui permet de calculer le pgcd de deux nombres entiers.

Il repose sur les deux lemmes suivants :

Lemme1 : Si $a = bq + r, (a, b) = (b, r)$.

Démonstration :

Soit d un diviseur commun de a et de b : d est aussi un diviseur de $a - bq = r$. d est donc un diviseur commun de b et de r.

Réciproquement, si d est un diviseur commun de b et de r, alors d divise également $a = bq + r$: c'est donc un diviseur commun de a et de b.

Les diviseurs communs de a et de b sont donc les mêmes entiers que les diviseurs communs de b et de r, d'où l'égalité : $(a, b) = (b, r)$.

lemme2 : Si b divise a, $(a, b) = b$.

Démonstration :

Si b divise a, b est un diviseur commun de a et de b. donc $(a, b) = b$, car aucun nombre plus grand que b ne peut diviser b.

On peut remarquer que la réciproque est exacte, c'est-à-dire que $(a, b) = b$ entraîne que b divise a.

L'algorithme d'Euclide [1] consiste alors à effectuer la division euclidienne de a par b :

1. EUCLIDE (vers 325 av JC - vers 265 av JC [Alexandrie])
Son nom reste attaché à la mathématique "grecque" d'Alexandrie, au IIIe siècle av. J.C. et à un ouvrage :

on obtient un reste r_1. On divise ensuite b par r_1 : on obtient un reste r_2. On continue ...
On a donc :

Algorithme d'Euclide : Soient a et b deux nombres entiers naturels. On suppose que $b \leq a$

On calcule alors (a, b) en faisant des divisions euclidiennes successives comme suit :

$$\begin{array}{lll} a & = b \times\ q_1 + r_1 & 0 \leq r_1 < b \\ b & = r_1 \times\ q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = r_1 \times\ q_2 + r_2 & 0 \leq r_3 < r_2 \\ ... & ... & ... \\ r_{n-4} & = r_{n-3} \times\ q_{n-2} + r_{n-2} & 0 \leq r_{n-2} < r_{n-3} \\ r_{n-3} & = r_{n-2} \times\ q_{n-1} + r_{n-1} & 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} & = r_{n-1} \times\ q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = r_n \times\ q_{n+1} + 0 & \end{array}$$

L'algorithme s'arrête lorsque le reste vaut 0 et le dernier reste non nul (dans l'algorithme ci-dessus : r_n) est le pgcd de a et b.

Preuve :

Tout d'abord l'algorithme s'arrête bien car les restes successifs verifient : $0 \geq r_1 > r_2 > r_3 > ... > r_{n-2} > r_{n-1} > r_n$

Donc c'est une suite strictement décroissante d'entiers naturels et donc on arrive bien après un nombre fini de divisions à un reste égal à 0.

D'autre part, d'après le lemme 1, on a :

$$(a, b) = (b, r_1) = (r_1, r_2) = ... = (r_{n-1}, r_n)$$

et d'après le lemme 2, on a :

$$(r_{n-1}, r_n) = r_n.$$

Le PGCD de a et de b est donc r_n c'est-à-dire le dernier reste non nul obtenu.

Plus précisément on a même montré que les diviseurs (positifs) communs de a et b sont les diviseurs de r_n, c'est-à-dire de leur PGCD.

Remarque : Puisque l'algorithme a pour objet le calcul d'un PGCD, il est possible de se restreindre aux entiers positifs, un PGCD de deux entiers relatifs étant égal au PGCD de leurs valeurs absolues.

Exemple : Calculer le $PGCD$ de 48 et 27

$48 = 27 \times\ 1 + 21$

$27 = 21 \times\ 1 + 6$

$21 = 6 \times\ 3 + 3$

$6 = 3 \times\ 2 + 0$

Donc $(48, 27) = 3$

Les Éléments (13 livres prodigieux dont trois consacrés à l'Arithmétique : les livres VII, VIII et IX). Cet ouvrage est considéré comme l'un des textes fondateurs des mathématiques modernes

2.4.1 Identité de Bézout

Si d est le plus grand diviseur commun de deux entiers a et b ($d = (a, b)$), alors il existe deux entiers u et v tels que :

$$au + bv = d$$

Démonstration

Supposons a et b strictement positifs.

Reprenons l'algorithme d'Euclide pour la détermination du PGCD :

$$\begin{array}{lll} a & = b \times\ q_1 + r_1 & 0 \leq r_1 < b \\ b & = r_1 \times\ q_2 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = r_1 \times\ q_2 + r_2 & 0 \leq r_3 < r_2 \\ ... & ... & ... \\ r_{n-4} & = r_{n-3} \times\ q_{n-2} + r_{n-2} & 0 \leq r_{n-2} < r_{n-3} \\ r_{n-3} & = r_{n-2} \times\ q_{n-1} + r_{n-1} & 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} & = r_{n-1} \times\ q_n + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} & = r_n \times\ q_{n+1} + 0 & \end{array}$$

On va montrer par récurrence que tous les restes $r_1, r_2, r_3, \ldots$ s'écrivent sous la forme $r_i = au_i + bv_i$.

Cela est vrai pour r_1 : $r_1 = 1.a - q_1.b$

et pour r_2 : $r_2 = b - (1.a - q_1.b)q_2 = -q_2.a + (1 + q_1q_2)b$.

Supposons que cela soit vrai pour un reste r_i : $r_i = au_i + bv_i$ et aussi pour le reste précédent r_{i-1} : $r_{i-1} = au_{i-1} + bv_{i-1}$.

On a alors

$r_{i+1} = r_{i-1} - r_i.q_{i+1} = (au_{i-1} + bv_{i-1}) - (au_i + bv_i)q_{i+1}$

$= (u_{i-1} - u_iq_{i+1})a + (v_{i-1} - v_iq_{i+1})b$.

Par récurrence le résultat est prouvé pour tous les restes r_i et en particulier pour le reste r_n qui est le PGCD de a et b.

On peut vérifier que le résultat reste valable même si a et b ne sont pas strictement positifs.

Théorème de Bézout

Soient a et b deux entiers naturels non nuls. Alors a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que

$$au + bv = 1.$$

Démonstration : L'identité de Bézout montre que si le PGCD de a et b est 1, alors il existe deux entiers relatifs u et v tels que $au + bv = 1$.

Réciproquement, si $au + bv = 1$, et si d était un diviseur positif commun de a et de b, ce serait aussi un diviseur de 1, c'est-à-dire que $d = 1$. a et b sont donc premiers entre eux.

Remarque : u et v ne sont pas uniques : En effet, pour tout q, on a encore $d = a(u - bq) + b(v + aq)$.

Mais u et v sont premiers entre eux : s'ils avaient un diviseur positif commun d', dd' diviserait au et bv donc diveserait $d = au + bv$, ce qui n'est possible que si $d' = 1$.

En choisissant, parmi les $(u - bq)$, le reste de la division de u par b, on peut imposer $0 \leq u < b$.

Pour calculer des identités de Bezout on peut utiliser les différentes équations obtenues dans l'algorithme d'Euclide, en commencant par l'avant dernière.

$$\begin{aligned}
(a,b) &= r_n && \text{étape } 0\\
&= r_{n-2} - r_{n-1}q_n && \text{étape } 1\\
&= r_{n-4} - r_{n-3}q_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n && \text{étape } 2\\
&.. \\
&= \text{en fonction de } r_{n-k}, ...r_{n-2k} && \text{étape } k\\
&= au + bv && \text{étape } n
\end{aligned}$$

Exemple : On reprend l' exemple avec 48 et 27

$48 = 27 \times\ 1 + 21$
$27 = 21 \times\ 1 + 6$
$21 = 6 \times\ 3 + 3$
$6 = 3 \times\ 2 + 0$

Donc

$$\begin{aligned}
3 &= -3 \times\ 6 + 21\\
&= -3 \times\ (27 - 21) + (48 - 27)\\
&= -3 \times\ (2 \times\ 27 - 48) + 48 - 27\\
&= -7 \times\ 27 + 4 \times\ 48
\end{aligned}$$

$\Rightarrow 27 \times\ (-7) + 48 \times\ 4 = 3 = (27, 48)$

De ce théorème de Bézout découle en particulier le théorème de Gauss :

2.4.2 Théorème de Gauss

Théorème de Gauss : Si $a|bc$ et si a est premier avec b, alors $a|c$.

Preuve : Puisque a et b sont premiers entre eux, il existe u et v tels que $au + bv = 1$.

Comme a divise bc, il divise $a(uc) + (bc)v = (au + bv)c = c$.

Corollaire : si a est premier avec b et avec c, alors il est premier avec le produit bc.

En effet, tout diviseur d de a est premier avec b (si d et b avaient un diviseur commun, celui-ci serait diviseur commun de a et b).

Si a et bc avaient un diviseur commun d, celui-ci, premier avec b, donc d'après le théorème de Gauss devrait diviser c, ce qui n'est pas possible car a et c sont premiers entre eux.

Nous avons là une propriété forte de la divisibilité dans $\mathbb{Z}$, il existe d'autres ensembles de nombres où la divisibilité ne vérifie pas le théorème de Gauss.

Munis de ce théorème de Gauss, nous sommes maintenant bien armés pour étudier la décomposition d'un entier en facteurs premiers.

Mais avant cela, quelques mots sur la notion de ppcm (plus petit commun multiple), qui complète utilement celle de pgcd.

2.4.3 PPCM

Définition et Théorème : Soit $a \geq 1$ et $b \geq 1$ deux entiers. Alors il existe un unique entier $m \geq 1$ tel que pour tout entier $c \geq 1$,

c est un multiple de a et de b si et seulement si c est un multiple de m.

m est donc Le plus petit multiple (strictement positif) commun de a et b,

Il s'appelle le PPCM (Plus Petit Commun Multiple) de a et de b et se note PPCM$(a; b)$.

Démonstration :

La démonstration consiste à choisir pour m le multiple commun de a et b le plus petit au sens de la relation habituelle $\leq$, puis à vérifier qu'il marche.

La preuve est en deux parties : d'abord l'existence de m puis son unicité .

Existence de m :

Introduisons l'ensemble A formé des entiers strictement positifs simultanément multiples de a et de b . L'ensemble A n'est pas vide, puisqu'il contient l'entier ab, et est inclus dans $\mathbb{N}$,Il admet donc un plus petit élément m . On va vérifier que cet entier m convient.

Pour faire cette vérification, soit un entier $n \geq 1$; nous avons désormais à montrer une équivalence, distinguons les deux sens.

Preuve de l'implication directe : Supposons donc que n est un multiple commun de a et b , et montrons que n est un multiple de m .

Pour ce faire, effectuons la division euclidienne de n par m , soit $n = mq + r$, avec $0 \leq r < m$.

Comme n et m sont des multiples de a , $r = n - mq$ aussi ; de même avec b.

Ainsi r est un multiple commun de a et b .

Si r était un entier strictement positif, vu l'inégalité $r < m$ il contredirait la minimalité de m .

C'est donc que $r = 0$ et donc que n est un multiple de m .

Preuve de l'implication réciproque : Supposons ici que n est un multiple de m . Comme m est lui-même multiple de a , n est à son tour multiple de a ; de même avec b .

Unicité de m :

Soit m et m' vérifiant les hypothèses du théorème. Comme m est un multiple de m , c'est un multiple commun de a et b , donc un multiple de m'. De même, m' est un multiple de m . Cela implique que m et m' sont forcément égaux au signe près. Comme ils sont tous deux strictement positifs, ils sont égaux. Fin de la démonstration.

Remarquons au passage que si a et b sont premiers entre eux, leur ppcm est égal à leur produit, et tout multiple commun de a et b est multiple du produit ab.

Plus généralement, si $a_1, a_2, ..., a_k$ sont k entiers deux à deux premiers entre eux, tout multiple commun de $a_1, a_2, ..., a_k$ est divisible par le produit $a_1a_2...a_k$. Cela se démontre de proche en proche , par récurrence sur k.

Exemple : Les multiples strictement positifs de 24 sont $24, 48, 72, 96, 120, 144, 168, 192, 216, 240,$ ... Ceux de 36 sont: $36, 72, 108, 144, 180, 216, 252,$. .

Donc PPCM$(24; 36) = 72$.

2.5 Nombres premiers

Définition : Un nombre premier est un entier supérieur ou égal à 2 qui n'est divisible que par 1 et lui-même. Un entier qui n'est pas premier est dit composé.

Propriétés :

- 1 n'est pas premier, tous les nombres premiers sauf 2 sont impairs.

- Si n est un entier et p un nombre premier, soit p divise n, soit p est premier avec n.

En particulier, p est premier avec tous les entiers naturels strictement inférieurs à p.

- Le plus petit diviseur naturel $p > 1$ d'un entier n est obligatoirement premier : En effet,

s'il admettait un diviseur strictement compris entre 1 et p, celui-ci diviserait n et p et ne serait pas le plus petit diviseur de n.

2.5.1 Crible d'Eratosthène

LEMME : Soit n un entier ≥ 2. Si n n'est pas premier, il existe un nombre premier $p \leq \sqrt{n}$ qui divise n.

Montrons ceci par récurrence sur n.

C'est vrai pour $n = 2, n = 3$ qui sont premiers, et aussi pour $n = 4$ qui n'est pas premier.

Supposons que le résultat soit vrai pour tout entier $< n$.

Si n est premier, le résultat est vrai. Sinon, n a un diviseur m, avec $1 < m < n$.

On peut écrire $n = km$. Si $m \leq k$, on a $m^2 \leq km = n$, d'où $m \leq \sqrt{n}$. En particulier, $m < n$.

Dans l'autre cas, $k \leq m$, on raisonne de même en échangeant les rôles de k et m.

Par récurrence, ou bien m est premier, ou bien m a un diviseur premier inférieur ou égal à sa racine carrée.

En particulier, m a un diviseur premier p et $p \leq m \leq \sqrt{n}$.

Crible d'Eratosthène [2]

Pour déterminer les entiers jusqu'à une certaine borne qui sont des nombres premiers, Eratosthène a inventé le procédé suivant, qu'on appelle crible d'Ératosthène.

On commence par écrire tous les entiers de 2 à, disons 30 :

$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30.$

Le premier d'entre eux est premier, on le garde et on raye tous ses multiples. On trouve alors

$2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29.$

Le suivant non rayé, 3, n'est multiple d'aucun entier plus petit que lui, donc est premier. On le garde et on élimine les multiples de 3. Il nous reste alors

$2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29..$

Ensuite, il y a 5, on fait la même chose qu'avec le 3. Il nous reste :

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$

Le suivant est 7, et est supérieur à la racine carrée de 30.

2. Eratosthène (IIIe av. JC) Astronome, géographe et mathématicien, nommé à la tête de la bibliothèque d'Alexandrie, il est resté célèbre pour son crible et pour avoir le premier mesuré le méridien terrestre.

Par suite, et en vertu du lemme précédent, tous les entiers qui restent sont des nombres premiers et la liste des nombres premiers inférieurs ou égaux à 30 est :

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

2.5.2 Théorème de décomposition en facteurs premiers

Théorème : Tout entier naturel n se décompose d'une et d'une seule manière en un produit de facteurs premiers abstraction faite de l'ordre des facteurs.

Ce théorème fondamental se démontre en deux temps : existence de la décomposition d'une part, unicité d'autre part.

L'existence est assez simple :

On procède par l'absurde, supposons qu'il existe des entiers naturels qui n'admettent pas de décomposition, et soit n le plus petit d'entre eux.

Soit n n'admet pas de diviseur strictement compris entre 1 et n, et n est premier par définition.

Soit il admet un diviseur d, donc $n = dq$. Les entiers d et q sont tous deux compris entre 1 et n donc tous deux admettent une décomposition en facteurs premiers (puisque n est le plus petit n'admettant pas de décomposition). Le produit de ces deux décompositions est une décomposition de n. Contradiction.

L'unicité nécessite le théorème de Gauss. Il est clair que deux nombres premiers distincts sont premiers entre eux. Supposons que n admette deux décompositions distinctes et classons les nombres premiers par ordre croissant :

$$n = p_1 p_2 ... p_k = p_1^{'} p_2^{'} ... p_k^{'}$$

avec $p_1 \leq p_2 ... \leq p_k$ et $p_1^{'} \leq p_2^{'} .. \leq .p_k^{'}$. Soit i le plus petit indice tel que $p_i \neq p_i^{'}$.

Le nombre $n^{'} = p_i p_{i+1} ... p_k = p_i^{'} p_{i+1}^{'} ... p_k^{'}$ est divisible par p_i et par $p_i^{'}$.

Or si $p_i < p_i^{'}$, p_i est strictement inférieur à tous les facteurs premiers $p_j^{'}$de la seconde décomposition de $n^{'}$ (puisque $p_i^{'} \leq p_j^{'}$ pour $i \leq j$),

il est donc premier avec chacun de ces nombres premiers, et d'après le théorème de Gauss, il est premier avec leur produit $n^{'}$,

ce qui contredit le fait que p_i est, dans la première décomposition, un facteur premier de $n^{'}$.

Il en va de même si $p_i^{'} < p_i$.

Deux exercices classiques pour mettre en application le théorème de Gauss et les nombres premiers :

Exercice : Si p est un nombre premier, Alors pour tout k strictement compris entre 0 et p, le coeficient binomial $C_p^k = \frac{p!}{k!(p-k)!}$ est divisible par p.

Preuve :

Rappelons que $p! = 1 \times \ 2 \times \ ... \times \ p$, avec $0! = 1! = 1$. Les C_p^k forment le triangle de Pascal et la relation $C_{p+1}^k = C_p^k + C_p^{k-1}$ permet de prouver qu'ils sont tous des entiers.

L'important est que si p est premier, il apparaît au numérateur et pas au dénominateur, donc on ne peut pas simplifier par p. Autrement dit : $p! = C_p^k.k!(p-k)!$

Or p divise $p!$ et est premier avec tous les entiers $1, ..., k$ (car $k < p$), ainsi qu'avec $1, ..., p-k$ (car $k > 0$), donc avec leur produit $k!(p-k)!$. Donc p divise C_p^k.

Théorème d'Euclide : Il existe une infinité de nombre premiers.

Preuve : Par l'absurde, supposons qu'il existe un nombre fini de nombres premiers $p_1, p_2, ..., p_k$.

Le nombre $n = p_1p_2...p_k + 1$ est premier avec chacun des nombres premiers $p_1, p_2, ..., p_k$:

Si p_i divisait n, comme p_i divise $n - 1 = p_1p_2...p_k$, donc p_i diviserait la différence qui est 1.

Or n admet au moins un facteur premier, qui n'appartient pas à $\{p_1, ..., p_k\}$.

Ce qui prouve que cet ensemble ne contient pas tous les nombres premiers.

Calcul du PGCD et du PPCM à partir de la décomposition en facteurs premiers :

Théorème : Soit deux entiers naturels $a = p_1^{n_1}p_2^{n_2}...p_k^{n_k}$ et $b = p_1^{m_1}p_2^{m_2}...p_k^{m_k}$ décomposés en utilisant les mêmes nombres premiers (quitte à compléter avec des exposants nuls).

Le PGCD de a et b est l'entier $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ où $\alpha_i = \min(\ n_i, m_i)\ \ 1 \leq i \leq k$

Le PPCM de a et b est l'entier $p_1^{\beta_1}p_2^{\beta_2}...p_k^{\beta_k}$ où $\beta_i = \max(\ n_i, m_i)\ \ 1 \leq i \leq k$

Démonstration : Evidente

Exemple : $12936 = 2^3 \times\ 3^1 \times\ 7^2 \times\ 11^1 \times\ 13^0$ et $3276 = 2^2 \times\ 3^2 \times\ 7^1 \times\ 11^0 \times\ 13^1$.

Le PGCD de 12936 et 3276 est donc $84 = 2^2 \times\ 3^1 \times\ 7^1 \times\ 11^0 \times\ 13^0$.

Le PPCM de 12936 et 3276 est donc $504504 = 2^3 \times\ 3^2 \times\ 7^2 \times\ 11^1 \times\ 13^1$.

Propriété : PGCD$(a, b)\times$ PPCM$(a, b) = ab$.

Démonstration :

Dans le produit $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k} \times\ p_1^{\beta_1}p_2^{\beta_2}...p_k^{\beta_k}$ on retrouve exactement, bien que dans le désordre, tous les facteurs premiers des décompositions de a et de b.

On peut donc aussi calculer le PGCD avec l'algorithme d'Euclide, puis en déduire le PPCM par la formule ci-dessus.

2.6 Équations Diophantiennes

Il s'agit des équations de la forme : $ax + by = c$ avec $(a, b, c) \in \mathbb{Z}^* \times \mathbb{Z}^* \times \mathbb{Z}$

a) On va donner une condition nécessaire et suffisante pour que l'équation admette au moins une solution.

b) Dans ce cas, on va déterminer l'ensemble de toutes les solutions.

a) Posons $d = (a, b)$.

Soient a' et b' tels que : $a = da'$ et $b = db'$

D'après l'homogénéité du *pgcd*, on a alors : $a' \wedge b' = 1$

L'équation s'écrit : $d(a'x + b'y) = c$

Distinguons deux cas :

· Si d ne divise pas c, alors l'équation n'a pas de solutions.

· Si d divise c, alors on pose $c = dc^{'}$. Notre équation s'écrit alors : $a^{'}x + b^{'}y = c^{'}$

Par ailleurs, comme $a' \wedge b^{'} = 1$, le théorème de Bézout assure l'existence d'un couple (u, v) tel que : $a^{'}u + b^{'}v = 1$

En multipliant par $c^{'}$, on a alors : $a^{'}c'u + b^{'}c^{'}v = c^{'}$

Le couple $(c^{'}u, c^{'}v)$ est donc une solution particulière de l'équation Diophantienne $ax + by = c$.

Une condition nécessaire et suffisante d'existence de solution est donc que le *pgcd* de a et b divise c.

b) On suppose désormais que le *pgcd* de a et b divise c.

Nous connaissons maintenant une solution particulière $(c^{'}u, c^{'}v)$.

On peut en déduire l'ensemble des solutions.

Soit (x, y) une solution quelconque de l'équation $ax + by = c$.

On a alors :

$$\begin{cases} a^{'}x + b^{'}y = c^{'} \\ a^{'}c^{'}u + b^{'}c^{'}v = c^{'} \end{cases}$$

Par différence, il vient : $a^{'}(x - c^{'}u) + b^{'}(y - c^{'}v) = 0$

En conséquence : $a^{'}|b^{'}(y - c^{'}v)$

Et comme $a^{'} \wedge b^{'} = 1$, on a, d'après le théorème de Gauss : $a^{'}|(y - c'v)$

Donc : $\exists k \in \mathbb{Z}, y = ka^{'} + c^{'}v$

En remplaçant on a : $a^{'}(x - c^{'}u) + b^{'}ka^{'} = 0$

Et comme $a^{'} \neq 0 : x = -b^{'}k + c^{'}u$

Réciproquement, on vérifie que, pour tout $k \in \mathbb{Z}$, le couple $(-b^{'}k + c^{'}u, ka^{'} + c^{'}v)$ est bien solution de l'équation Diophantienne.

Conclusion : les couples (x, y) solutions de l'équation $ax + by = c$ (lorsque (a, b) divise c) sont de la forme :

$$(x, y) = (-b^{'}k + c^{'}u, ka^{'} + c^{'}v), \quad k \in \mathbb{Z}$$

Application : En multipliant mon jour de naissance par 12 et mon mois de naissance par 31, j'obtiens 442.

Quelle est ma date de naissance ? (On ne demande pas l'année)

Notons J et M mon jour et mon mois de naissance respectivement.

On a donc : $12J + 31M = 442$

Comme $12 \wedge 31 = 1$, l'équation admet des solutions. (Donc je suis bien né !)

On recherche une solution particulière en appliquant l'algorithme d'Euclide-Bézout :

$31 = 2 * 12 + 7$

$12 = 1 * 7 + 5$

$7 = 1 * 5 + 2$

$5 = 2 * 2 + 1$

$2 = 2 * 1 + 0$

Puis, on exprime le *pgcd* en fonction des restes précédents :

$1 = 5 - 2 * 2$

$1 = 5 - 2 * (7 - 5) = -2 * 7 + 3 * 5$
$1 = -2 * 7 + 3 * (12 - 7) = 3 * 12 - 5 * 7$
$1 = 3 * 12 - 5 * (31 - 2 * 12) = -5 * 31 + 13 * 12$
Finalement, un couple (u, v) possible est $(-5, 13)$.
On a donc : $-5 * 31 + 13 * 12 = 1$
En multipliant par 442 : $-2210 * 31 + 5746 * 12 = 442$
Donc le couple $(J_0, M_0) = (5742, -2210)$ est une solution particulière de l'équation $12J + 31M = 442$.

On recherche maintenant l'ensemble de toutes les solutions. Soit (J, M) une solution quelconque.

$$\begin{cases} 12J + 31M = 442 \\ 5746 * 12 - 2210 * 31 = 442 \end{cases}$$

Par différence, il vient : $12(J - 5746) + 31(M + 2210) = 0$
En conséquence : $31|12(J - 5746)$
Et comme $12 \wedge 31 = 1$, on a, d'après le théorème de Gauss :
$31|J - 5746$
Donc : $\exists$k $\in \mathbb{Z}$, $J = 31k + 5746$
Or, évidemment $J \in [1, 31]$: $1 \leq 31k + 5746 \leq 31$
$-5745 \leq 31k \leq -5715$
$k = -185$
$J = 11$
On en déduit : $M = 10$
Je suis donc né un 11 octobre.

2.7 Congruences

Tout comme on distingue nombres pairs et nombres impairs , multiples de 3, nombres de la forme $3k + 1$, nombres de la forme $3k + 2$, plus généralement, on peut classer les entiers en n classes modulo n, à savoir :

2.7.1 Définition et proporiétés des congruences

Définition : Soient $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $n \in \mathbb{N}$ et $n > 1$ a est dit congru à b modulo n si et seulement si $a - b$ est divisible par n, ce qui s'écrit :

$$a \equiv b \ (mod\ n) \ \Leftrightarrow n|(a - b)$$

Il s'agit bien là d'une relation d'équivalence : En effet on a vu dans le chapitre précédent que :

- $a \equiv a \ (mod\ n)$,
- si $a \equiv b \ (mod\ n)$, alors $b \equiv a \ (mod\ n)$,
- si $a \equiv b \ (mod\ n)$ et $b \equiv c \ (mod\ n)$, alors $a \equiv c \ (mod\ n)$.

et que :

$$\dot{x} = \{x,\, x + kn, k \in \mathbb{Z}\ \},$$

L'ensemble quotient (ensemble de toutes les classes d'équivalence) est noté $\mathbb{Z}/n\mathbb{Z}$

Exemple :

1. $13 \equiv 8\ (mod\ 5)$ car, $13 - 8 = 1 \times 5$
2. $115 \equiv 11\ (mod\ 13)$ car, $115 - 11 = 104 = 8 \times 13$
3. $967 \equiv 16420\ (mod\ 17)$ car $967 - 16420 = -(909) \times 17$
4. $35 \equiv -3 \equiv 11\ (mod\ 2)$.

Remarque : $a \equiv b\ (mod\ n)$ s'écrit aussi $a \equiv b\ [n]$

Proposition : Soient $x \in \mathbb{Z}$, $y \in \mathbb{Z}$, $n \in N$ et $n > 1$

$$x \equiv y\ (mod\ n) \Leftrightarrow x \text{ et } y \text{ ont le même reste dans la division euclidienne par } n$$

Preuve :

1. Supposons que $x \equiv y\ (mod\ n)$ alors $x - y = kn$ où $k \in \mathbb{Z}$

La division par n donne : $x = an + r$ et $y = bn + r'$ où r et r' sont tels que $0 \leq r \leq n-1$ et $0 \leq r' \leq n-1$

Donc, $x - y = (a-b)n + (r - r')$, où on aura $-(n-1) \leq r - r' \leq (n-1)$,

$x - y$ étant un multiple de n, la seule possibilité pour $r - r'$ est d'être nul , donc : $r = r'$

2. Supposons que x et y ont même reste dans la division par n

Alors, $x = an + r$, et $y = bn + r$, avec $0 \leq r \leq n-1$ donc, $x - y = (an + r) - (bn + r) = n(a-b)$,

ce qui montre que $x \equiv y\ (mod\ n)$.

Corrollaire : . Soit n un entier > 1. Alors tout nombre entier a est congru modulo n à un et un seul entier r de l'ensemble $\{0, 1, 2, ..., n-1\}$.

De plus, cet entier r est exactement le reste de la division de a par n.

En d'autres termes, si $0 \leq r < n$, alors

$$a \equiv r\ (mod\ n) \Leftrightarrow a = qn + r \quad \text{où } q \text{ est le quotient de } a \text{ par } n \text{ et } r \text{ le reste.}$$

Démonstration : C'est une conséquence immédiate de la proposition précédente.

Proposition : On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalence, alors, $\mathbb{Z}/n\mathbb{Z}$ est un ensemble de n classes qui sont, en fait, tous les restes dans la division euclidienne par n.

$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, ..., \dot{n-1}\right\} = \{k\mathbb{Z}, 1 + k\mathbb{Z}, ..., (k-1) + k\mathbb{Z}\}$

Démonstration :

D'après le corrollaire précedent, tout $x \in \mathbb{Z}$ est congru, modulo n à un reste dans la division par n.

Comme il y a n restes, qui sont $0, 1, 2, ..., n-1$. Il y a donc n classes et on a :

$\mathbb{Z}/n\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, ..., \dot{n-1}\right\} = \{k\mathbb{Z}, 1 + k\mathbb{Z}, ..., (k-1) + k\mathbb{Z}\}$

Exemple :

$\mathbb{Z}/5\mathbb{Z} = \left\{\dot{0}, \dot{1}, \dot{2}, \dot{3}, \dot{.4}\right\} = \{k\mathbb{Z}, 1 + k\mathbb{Z}, 2 + k\mathbb{Z}, 3 + k\mathbb{Z}, 4 + k\mathbb{Z}\}$.

Proposition : La relation de congruence est compatible avec l'addition et la multiplication c'est à dire :

1. si $a \equiv b\ (mod\ n)$ et $a^{'} \equiv b^{'}\ (mod\ n)$, alors $a + a^{'} \equiv b + b^{'}(mod\ n)$. et
2. si $a \equiv b\ (mod\ n)$ et $a^{'} \equiv b^{'}\ (mod\ n)$, alors $aa^{'} \equiv bb^{'}\ (mod\ n)$,

Démonstration :

1. si $a \equiv b\ (mod\ n)$ et $a^{'} \equiv b^{'}\ (mod\ n)$, alors $a + a^{'} \equiv b + b^{'}(mod\ n)$.

En effet, si n divise $a - b$ et $a^{'} - b^{'}$, n divise $(a + a^{'}) - (b + b^{'}) = (a - b) + (a^{'} - b^{'})$,

2. De même, si $a \equiv b\ (mod\ n)$ et $a^{'} \equiv b^{'}\ (mod\ n)$, alors $aa^{'} \equiv bb^{'}\ (mod\ n)$,

car si n divise $a - b$ et $a^{'} - b^{'}$, n divise $aa^{'} - bb^{'} = a^{'}(a - b) + b(a^{'} - b^{'})$.

En particulier, si $a \equiv b\ (mod\ n)$, $a^2 \equiv b^2\ (mod\ n)$: on rappelle que $a^2 - b^2 = (a-b)(a+b)$.

Plus généralement pour tout $k > 0$, $a^k \equiv b^k\ (mod\ n)$:

$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + ... + ab^{k-2} + b^{k-1})$ ce qu'on démontre en développant :

$$a(a^{k-1} + a^{k-2}b + ... + b^{k-1}) = a^k + a^{k-1}b + ... + ab^{k-1}$$

et

$$-b(a^{k-1} + ... + ab^{k-2} + b^{k-1}) = -a^{k-1}b - ... - ab^{k-1} - b^k.$$

La relation $\equiv$ se comporte sur de nombreux points comme la relation d'égalité $=$.Néanmoins, une propriété de la relation d'égalité n'est plus vraie pour celle de congruence, à savoir la simplification :

si $ab \equiv ac\ (mod\ n)$, on n'a pas nécessairement $b \equiv c\ (mod\ n)$. Par exemple $2.1 \equiv 2.3\ (mod\ 4)$ mais $1 \neq 3\ (\text{mod } 4)$.

Mais on a : :

si $ma \equiv mb\ (mod\ n)$ et **si** m **est premier avec** n, alors $a \equiv b\ (mod\ n)$.

Ceci veut dire qu'il est possible de simplifier modulo n à la condition que le nombre par lequel on simplifie soit premier avec n.

En effet, si n divise $ma - mb = m(a - b)$, en étant premier avec m, n divise $a - b$, donc $a \equiv b\ (mod\ n)$.

Changement de modulus :

Jusqu'ici, nous avons vu des propriétés des congruences faisant intervenir un seul modulus. Nous allons maintenant étudier le comportement de la relation de congruence lors d'un changement de modulus.

Théorème :

(i) Si $a \equiv b\ (mod\ n)$ et d divise n, alors $a \equiv b\ (mod\ d)$.

(ii) Si $a \equiv b\ (mod\ r)$ et $a \equiv b\ (mod\ s)$ alors $a \equiv b\ (mod\ m)$. où m est le ppcm de r et de s.

Démonstration :

Le point (i) est évident.

Pour (ii). Par hypothèse, $b - a$ est un multiple de r et de s. Donc, $b - a$ est un multiple du ppcm de r et s ce qui démontre (ii).

Définition Un ensemble $X = \{x_1, x_2, ..., x_n\}$ de n entiers est dit système complet de résidus modulo n si pour tout entier $x \in \mathbb{Z}$, il existe un et un seul x_k tel que $x \equiv x_k(mod\ n)$. Autrement dit si X contient un et un seul élément de chaque classe d'équivalence modulo n.

Cette définition sert essentiellement à énoncer le lemme suivant :

Lemme

Si $X = \{x_1, x_2, ..., x_n\}$ est un système complet de résidus modulo n et si a est un entier premier avec n, alors $aX = \{ax_1, ax_2, ..., ax_n\}$est un système complet de résidus modulo n.

En effet, si deux éléments de aX appartenaient à la même classe, c'est-à-dire si $ax_i \equiv ax_j$ $(mod\ n)$, n diviserait $a(x_i - x_j)$.

Or n est premier avec a donc (théorème de Gauss) n diviserait $x_i - x_j$: ce qui voudrait dire que x_i et x_j appartiendraient à la même classe $(x_i \equiv x_j(mod\ n))$, ce qui est contraire à l'hypothèse.

Comme il existe exactement n classes modulo n et n éléments de aX appartenant tous à des classes distinctes, aX contient un élément dans chaque classe modulo n.

Le principal théorème résultant de ce lemme et le (petit) théorème de Fermat :

2.7.2 Théorème du Fermat

Théorème : Soit p un nombre premier et a un entier premier avec p (ou : non divisible par p). Alors $a^{p-1} \equiv 1(mod\ p)$.

Il en résulte que $a^p \equiv a\ (mod\ p)$, ce dernier résultat étant vrai même si a est divisible par p (donc pour tout $a \in \mathbb{Z}$).

Preuve :

L'ensemble $X = \{0, 1, 2, ..., p-1\}$ est un système complet de résidus modulo p. Donc $aX = \{0, a, 2a, ..., a(p-1)\}$est un système complet de résidus modulo p puisque a est premier avec p.

Donc chaque $i \in \{1, ..., p-1\}$ est congru modulo p, à un $k_i a$ et un seul pour $k_i \in \{1, ..., p-1\}$.

Le produit : $1 \times\ 2 \times\ ... \times\ (p-1)$ est donc congru modulo p à $a \times\ 2a \times\ ... \times\ (p-1)a = a^{p-1}(1 \times\ 2 \times\ ... \times\ (p-1))$

Or $1 \times 2 \times ... \times (p-1)$ est premier avec p, car p est premier donc premier avec $1, 2, ..., p-1$.

Il en résulte après simplification que 1 est congru à a^{p-1}.

2.7.3 Théorème chinois

Peut-on trouver un nombre impair, qui soit congru à 2 modulo 7 et à 17 modulo 33 ?

Ce résultat est connu de longue date des Chinois (d'où son nom), et peut s'énoncer ainsi de manière très générale :

Théorème :

Soient $a_1, a_2, ..., a_k$ k entiers positifs deux à deux premiers entre eux, et $b_1, b_2, ..., b_k$ k entiers quelconques. Posons $A = a_1 a_2 ... a_k$.

Alors Il existe un et un seul entier B vérifiant : $0 \leq B < A$ tel que le système d'équation :

$$\begin{cases} x \equiv b_1\ (mod\ a_1) \\ x \equiv b_2\ (mod\ a_2) \\ \qquad ... \\ x \equiv b_k\ (mod\ a_k) \end{cases}$$

est équivalent à $x \equiv B \ (mod\ A)$.

Mais comment démontre-t-on ce théorème, et comment trouve-t-on B?

Démonstration : Pour tout i, posons $A = a_i q_i$ (q_i est le produit de tous les a_j autres que a_i).

a_i étant premier avec chaque a_j, par hypothèse, il est donc premier avec leur produit q_i, donc, d'après Bézout, il existe u_i et v_i tels que $u_i a_i + v_i q_i = 1$, ce qui entraîne $v_i q_i \equiv 1 \ (mod\ a_i)$.

Par ailleurs, $v_i q_i \equiv 0 \ (mod\ a_j)$ pour tout a_j autre que a_i.

De sorte que l'entier $B^{'} = b_1 v_1 q_1 + b_2 v_2 q_2 + ... + b_k v_k q_k$ est bien solution du système d'équations.

Et il en va de même de tout entier $x \equiv B^{'}(mod\ A)$, dont un et un seul, B, vérifie $0 \leq B < A$.

Réciproquement, si x et $x^{'}$ sont deux solutions du système d'équations, pour tout i on $x \equiv x^{'}(mod\ a_i)$. Il en découle que $x - x^{'}$ est divisible par chacun des a_i, donc par leur ppcm, en l'occurrence leur produit A (puisqu'ils sont deux à deux premiers entre eux).

Exemple: le système d'équation :

$$\begin{cases} x \equiv 1(mod\ 2) \\ x \equiv 2(mod\ 7) \\ x \equiv 17(mod\ 33) \end{cases}$$

est équivalent à $x \equiv 149(mod\ 462)$.

En effet, on a :

$A = 2 \times\ 7 \times\ 33 = 462$

$a_1 = 2 \qquad q_1 = 231 \qquad 116 \times 2 - 1 \times\ 231 = 1$

$a_2 = 7 \qquad q_2 = 66 \qquad 19 \times 7 - 2 \times\ 66 = 1$

$a_3 = 33 \qquad q_3 = 14 \qquad 3 \times\ 33 - 7 \times\ 14 = 1$

donc :

$$\begin{aligned} B^{'} &= 1 \times (-1 \times\ 231) + 2 \times (-2 \times\ 66) + 17 \times (-7 \times\ 14) \\ &= -2161 \\ &= (-10 \times\ 231) + 149 \end{aligned}$$

ce qui entraîne $B = 149$.

Exercice : Montrer que quel que soit l'entier n strictement positif, (aussi grand que soit n), on peut trouver n entiers strictement positifs consécutifs dont aucun n'est premier.

Solution :

cet exercice prouve que la distance de deux nombres premiers consécutifs peut être aussi grande que l'on veut.

Cette distance de deux nombres premiers consécutifs p_k et p_{k+1} pose d'ailleurs bien des problèmes fort diffciles : il est vraisemblable qu'il existe une infinité de nombres premiers p_k tels que $p_{k+1} - p_k = 2$ (nombres premiers jumeaux), et dans l'autre sens, il est vraisemblable que cette différence $p_{k+1} - p_k$ est majorée.

Toujours est-il que $p_{k+1} - p_k$ n'est pas majoré par une constante, c'est l'objet du présent exercice :

Grâce au théorème chinois, c'est simple à prouver.

Comme il existe une infinité de nombres premiers, choisissons en n : $p_1, p_2, ..., p_n$ distincts, donc deux à deux premiers entre eux.

Le système d'équations :

$x \equiv -1 \ (mod \ p_1)$

$x \equiv -2 \ (mod \ p_2)$

...

$x \equiv -n \ (mod \ p_n)$

est équivalent à $x \equiv B(mod \ A)$, avec $A = p_1 p_2 ... p_n$ et $0 < B < A$.

Pour tout i, $A + B + i$ est divisible par p_i, et il n'est pas égal à p_i, car il est strictement supérieur à $A = p_1 p_2 ... p_n$. Donc $A + B + i$ n'est pas premier.

$A+B+1$, $A+B+2$, ..., $A+B+n$ sont donc bien n entiers strictement positifs consécutifs dont aucun n'est premier.

2.8 Indicatrice d'Euler

Définition : L'indicatrice d'Euler [3] φ est la fonction de l'ensemble des entiers strictement positifs dans lui-même, qui à n associe le nombre d'entiers positifs inférieurs à n et premiers avec n.

Exemple :. On a : $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$

$\varphi(1) = 1$

$\varphi(2) = 1$

$\varphi(3) = 2$

$\varphi(4) = 2$

$\varphi(5) = 4$

$\varphi(6) = 2$

$\varphi(7) = 6$

$\varphi(8) = 4$

---

3. EULER Leonhard, suisse, $1707 - 1783$

Né à Bâle, il fut l'élève de Jean Bernoulli.

Introduits par les Bernoulli, il s'installa à Saint-Pétersbourg (1730) auprès de Pierre Ier le Grand et remplaça Daniel Bernoulli (1733) à l'Académie des sciences pour la physique et les mathématiques.

Appelé à Berlin (1741) par Frédéric II, roi de Prusse, il présida l'Académie des sciences jusqu'en 1766 (c'est Lagrange qui lui succédera).

Il fut nommé membre associé de l'Académie des sciences de Paris (1755). Vers la fin de sa vie, alors aveugle, il revint à Saint-Pétersbourg invité par Catherine II. Il est sans doute un des plus grands mathématiciens de tous les temps.

Euler intervint dans les trois domaines fondamentaux de la science de son époque : l'astronomie (orbites planétaires, trajectoires des comètes), les sciences physiques (champs magnétiques, hydrodynamique, optique, nature ondulatoire de la lumière, mécanique des solides...), et les mathématiques, dans toutes ses branches, de l'arithmétique à la géométrie différentielle en passant par l'analyse numérique et fonctionnelle, le calcul des variations, les courbes et les surfaces algébriques, le calcul des probabilités et les premiers aspects de la théorie des graphes et de la topologie.

Ses fils Jean-Albert ($1734 - 1800$), Charles ($1740 - 1790$) et Christophe ($1743 - 1812$) furent aussi des mathématiciens renommés à Saint-Pétersbourg.

...
$\varphi(p) = p - 1$ pour tout nombre premier p.

Théorème :. Soient m, n $\in \mathbb{N}$ premiers entre eux. Alors

$$\varphi(mn) = \varphi(m).\varphi(n) :$$

Nous démontrerons ce théorème dans le chapitre suivant.

Théorème : Soit p un nombre premier. Alors

$$\varphi(p^k) = (p - 1).\ p^{k\text{-}1} \text{ pour tout entier } k \in \mathbb{N}.$$

Démonstration : Par définition, $\varphi(p^k)$ est le nombre d'entiers n satisfaisant $1 \leq n < p^k$ et qui sont premiers avec p^k.

Comptons d'abord le nombre d'entiers naturels $m < p^k$ qui ne sont pas premiers avec p^k.

Comme p est un premier, il faut que de tels m soient multiples de p.

Les entiers $p, 2p, 3p, 4p, ..., (p^{k-1} - 1)p$ sont donc les seuls entiers naturels $< p^k$ qui ne sont pas premiers avac p^k. Il y en a exactement $p^{k-1} - 1$.

Il y a donc

$$p^k - 1 - (p^{k-1} - 1) = p^k - p^{k-1} = (p - 1)p^{k-1}$$

entiers naturels $< p^k$ qui sont premiers avec p^k d'où la valeur de $\varphi(p^k)$.

Les deux théorèmes précédents permettent de calculer $\varphi(n)$ pour n'importe quel entier n en le factorisant en produit de facteurs premiers. Si

$$n = p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$$

avec $n_i \geq 1$ pour tout i, alors

$$\varphi(n) = (p_1 - 1)p^{n_1 - 1} ... (p_k - 1)p^{n_k - 1}$$

Exemple : On a :
$\varphi(12) = \varphi(2^2) \times \varphi(3) = 2 \times 2 = 4$
$\varphi(60) = \varphi(5) \times \varphi(12) = 4 \times 4 = 16$
$\varphi(128) = \varphi(2^7) = 2^6 = 64$
$\varphi(81) = \varphi(3^4) = 2 \times 3^3 = 54$
$\varphi(1000) = \varphi(23) \times \varphi(53) = 2^2 \times 4 \times 5^2 = 400$

Combien y a-t-il de nombres premiers ?

Cela fait près de 2500 ans que les hommes s'intéressent aux nombres premiers , qui a toujours été et qui reste un bel exemple de la beauté, de la richesse et de la vie des mathématiques. Et ces nombres fascinants n'ont pas encore fini de nous révéler leurs mystères.

A partir d'une notion très simple : " un nombre est premier s'il n'admet que 2 diviseurs distincts : 1 et lui-même.

Les questions les plus simples mais aux réponses très compliquées se sont multipliées. Euclide, 400 ans avant JC, avait posé et résolu le premier problème : " Y a-t-il une infinité de nombres premiers ? ".

La démonstration ci dessus qu'il en a fait est non seulement un des premiers exemples de " preuve mathématique ", mais aussi une belle démonstration par sa simplicité.

Deux siècles après Euclide, Eratosthène s'attaque au délicat problème de construction d'une liste de nombres premiers (voir ci-dessus). L'observation d'une liste de nombres premiers est riche en questionnements,.

La raréfaction des nombres premiers est quant à elle mieux comprise aujourd'hui. Dès 1798, en examinant les tables étendues obtenues par lui même et par d'autres, Gauss avait émis l'hypothèse que la fonction $\varphi(n)$, la fonction d'Euler, est, pour les grandes valeurs de n, approximativement égale à $n/ln(n)$.

Plus précisement :

$$\lim_{n\to+\infty} \varphi(n)\frac{\log(n)}{n} = 1$$

Au siècle suivant, de nombreux mathématiciens ont essayé de démontrer la conjecture de Gauss, dont la démonstration fut établie la même année 1896 à quelques mois d'intervalle par Charles-Jean de la Vallée Poussin et Jacques Hadamard, et connu sous le nom du théorème de raréfaction des nombres premiers.

Il reste cependant dans l'univers de la répartition des nombres premiers beaucoup d'incertitudes et de questionnements. Si on a établi une loi de comportement asymptotique de cette répartition, on ignore encore toute la logique de la répartition des nombres premiers.

Enfin, si l'étude mathématique des nombres premiers est aussi importante, c'est aussi car les applications de cette théorie sont extrêmement riches dans d'autres domaines scientifiques, en particulier dans le domaine de l'informatique où les critères de primalité d'un nombre, les algorithmes de factorisation sont très largement utilisés dans le domaine de la cryptographie en particulier.

Que peut bien avoir d'intéressant le nombre $2^{20996011} - 1$?

C'est le plus grand nombre premier connu jusqu'en 2003 : il est fait de 6320430 chiffres et il a été découvert le 17 novembre 2003. Il aura fallu 25000 années de temps calcul partagé sur les ordinateurs de 211000 volontaires répartis sur la planète. Il faut croire que la recherche de nombres premiers a quelque chose de très fascinant.

Les deux derniers nombres premiers connus ont eté découverts en 2009 sont :
$2^{43112609} - 1$ et $2^{37156667} - 1$

Le premier, un mammouth ne compte pas moins de 12978189 chiffres et le second, un petit garçon à coté, avec "seulement" 11185272 chiffres.

A titre de comparaison, le précédent, découvert l'année passée, possédait 9808358 chiffres.