M. Bonneton

M. Maciol

Eléments d'arithmétique

1. La division euclidienne

« *Eléments* », le plus vieux traité d'arithmétique connu, est dû à Euclide (environ - 300 avant J.C) qui y introduit notamment la division qui porte aujourd'hui son nom.
N désigne l'ensemble des entiers naturels. **Z** désigne l'ensemble des entiers (relatifs).

(**Z**, +, ×) est un anneau commutatif et unitaire (et euclidien !). On sous-entend parfois l'existence de l'addition et de la multiplication (internes) dans **Z** en écrivant que **Z** est un anneau.

$\mathbf{N}^*$ (resp. $\mathbf{Z}^*$) désigne l'ensemble des entiers naturels (resp. des entiers) non nuls.

1.1 Définitions

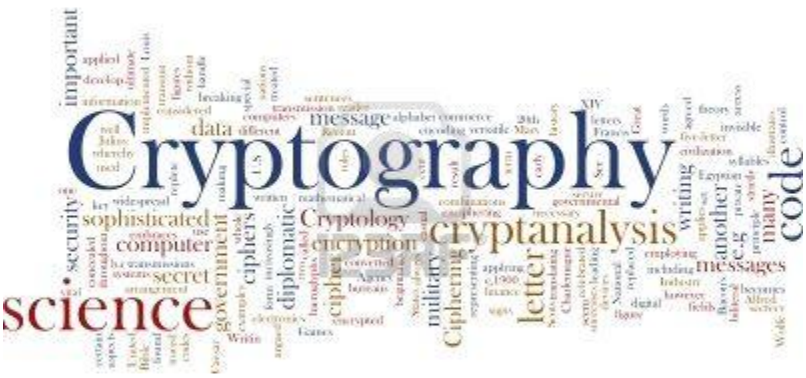
Soient $a \in \mathbf{Z}$ et $n \in \mathbf{Z}$.

a est dit multiple de n lorsqu'il existe q, $q \in \mathbf{Z}$, tel que $a = nq$.

Lorsque $a \in \mathbf{Z}^*$ et $n \in \mathbf{Z}^*$ et a multiple de n, on dit que n divise a, ce que l'on note $n \mid a$, ou que n est un diviseur de a.

L'ensemble des multiples de n est noté n**Z**. On a donc $n \mid a \Leftrightarrow a \in n\mathbf{Z}$.

<u>Exemples</u> : $0\mathbf{Z} = \{0\}$, $1\mathbf{Z} = \mathbf{Z}$, $2\mathbf{Z} = -2\mathbf{Z}$
$= \{\ldots,-6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$ etc.



1.2 Divisibilité dans $\mathbf{N}^*$

Proposition 1

La relation de divisibilité dont le symbole est $|$ est une relation d'ordre partiel dans $\mathbf{N}^*$.

1.3 La division euclidienne

1.3.1 Théorème 1 (premier théorème d'Euclide)

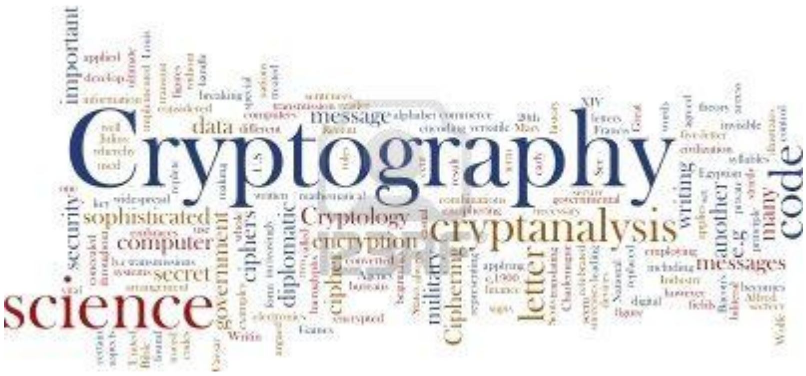
Soient $a \in \mathbf{Z}$ et $n \in \mathbf{N}^*$.

$\exists\, !\, q \in \mathbf{Z}$, $\exists\, !\, r \in \mathbf{N}$, tels que $a = nq + r$, avec $0 \leq r < n$.

1.3.2 Définition

Effectuer la division euclidienne de a par n, c'est trouver q et r tels que $a = nq + r$, avec $0 \leq r < n$.

a, n, q, r sont appelés dividende, diviseur (ou module), quotient et reste, respectivement.



2. Congruence modulo n

Carl Friedrich Gauss (1777-1855) « crée » la théorie des congruences en 1801 (dans *Disquisitiones arithmeticae*). En fait, il semble que les astronomes babyloniens et chinois (voir « théorème chinois ») utilisaient déjà cette notion. La célèbre notation ≡, symbole de la (relation de) congruence est cependant due à Gauss, ainsi que d'importants résultats d'arithmétique portant sur les nombres premiers.

Soit $n \in \mathbf{N}^*$, $n > 1$.

2.1 Relation de congruence modulo n, dans Z

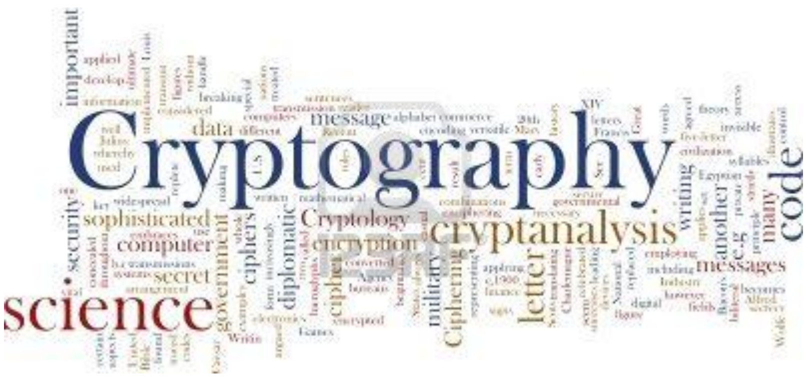
2.1.1 Définition

Soient $a \in \mathbf{Z}$ et $b \in \mathbf{Z}$.

a et b sont dits congrus modulo n lorsqu'ils ont le même reste dans la division euclidienne par n. On écrit alors $a \equiv b \pmod{n}$ ou plus simplement $a \equiv b$ (n).
En particulier, puisqu'il existe $q \in \mathbf{Z}$ et $r \in \mathbf{N}$ tels que $a = nq + r$ avec $0 \leq r < n$, on a toujours $a \equiv r$ (n). De plus, $n \mid a \Leftrightarrow a \equiv 0$ (n).

2.1.2 Applications numériques

Vérifier que $57 \equiv 0$ (3) ; $19 \equiv 1$ (9) ; $10109 \equiv 0$ (11) ; $1000 \equiv 1$ (9) ; $65 \equiv 13$ (26).



2.1.3 Proposition 2

$a \equiv b\ (n) \Leftrightarrow n \mid a - b \Leftrightarrow a - b \in n\mathbf{Z}$.

2.1.4 Proposition 3

La relation de congruence modulo n est une relation d'équivalence dans **Z**.

2.1.5 Proposition 4

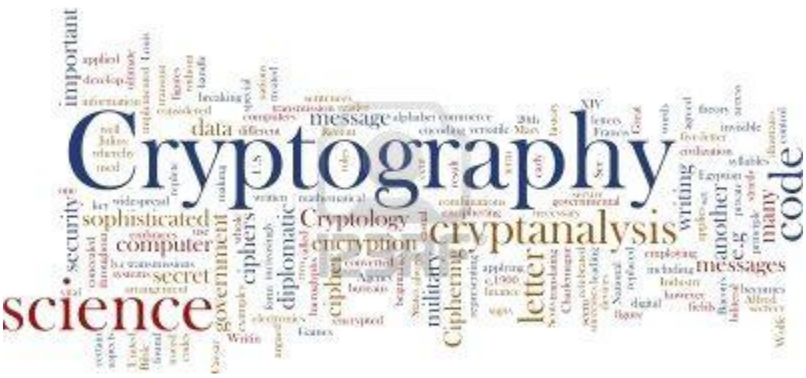
La congruence est compatible avec l'addition et la multiplication dans **Z**.

On en déduit facilement les résultats suivants :

Si $a \equiv b\ (n)$, alors :

1) $\forall c \in \mathbf{Z}$, $a + c \equiv b + c\ (n)$ et $ac \equiv bc\ (n)$
2) $-a \equiv -b\ (n)$
3) $\forall k \in \mathbf{N}$, $a^k \equiv b^k\ (n)$.

2.1.6 Exercices



a) Montrer que :

1) $\forall k \in \mathbf{N}$, $10^k \equiv 1$ (9). En déduire le critère de divisibilité par 9 : tout entier est congru à la somme de ses chiffres modulo 9.

2) $\forall k \in \mathbf{N}$, $10^{2k} \equiv 1$ (11) et $10^{2k+1} \equiv -1$ (11). En déduire un critère de divisibilité par 11.

b) Calculer l'entier naturel x tel que $0 \leq x \leq 10$ et $4\,813\,986\,705\,432^{15} \equiv x$ (11).

c) Quels sont les deux derniers chiffres de $7^{9^{9^9}}$? (Tout nombre est congru à ses deux derniers chiffres modulo 100…)

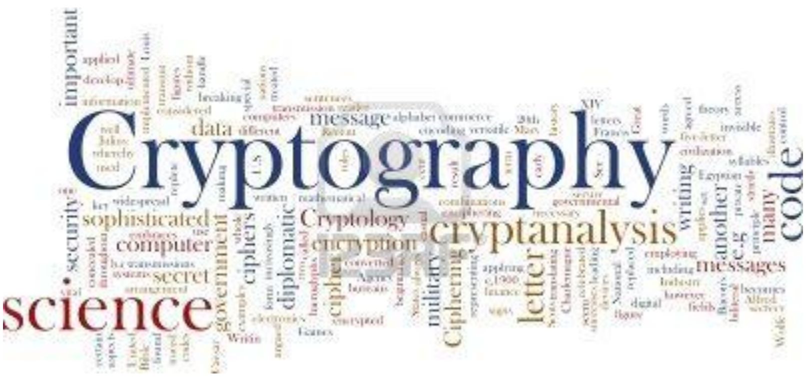
3. L'anneau $(\mathbf{Z}_n, +, \times)$

3.1 Les entiers modulo n

Soit $n \in \mathbf{N}^*$, $n > 1$.

3.1.1 Définition

Soit $a \in \mathbf{Z}$. On appelle classe de congruence (modulo n) de a



l'ensemble, noté $\bar{a}$, des entiers congrus à a modulo n : $\bar{a} = \{ b \in \mathbf{Z}, a \equiv b\ (n) \}$. Le nombre a est appelé représentant de la classe $\bar{a}$ (à laquelle il appartient).

Le représentant d'une classe peut être choisi arbitrairement car $a \equiv r\ (n) \Leftrightarrow \bar{a} = \bar{r}$.

Généralement, on choisit comme représentant de la classe $\bar{a}$ le reste r de la division euclidienne de a par n.

3.1.2 Exemple Dans la congruence modulo 3, on a :

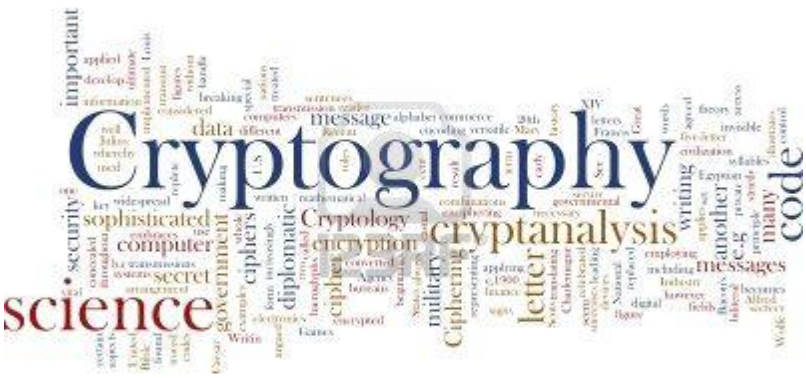
$\bar{0} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}, \bar{1} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ et $\bar{2} = \{\ldots, -4, -1, 2, \ldots\}$

3.1.3 Proposition 5 et définition

L'ensemble $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$ est une partition de **Z**. Il est appelé ensemble des « entiers modulo n » et est noté **Z**/n**Z** ou encore $\mathbf{Z}_n$.

3.2 L'addition dans $\mathbf{Z}_n$

3.2.1 Définition



On définit dans Z_n une addition interne (signe +) de la façon suivante :

$$\forall \bar{a}, \forall \bar{b}, \bar{a} + \bar{b} = \overline{a+b}$$

3.2.2 Exemples

Dans Z_9, $\bar{4} + \bar{5} = \bar{0}$ et $\bar{6} + \bar{8} = \bar{5}$. Dans Z_{31}, $\overline{27} + \overline{30} = \overline{26}$.

3.2.3 Propriétés de l'addition dans Z_n

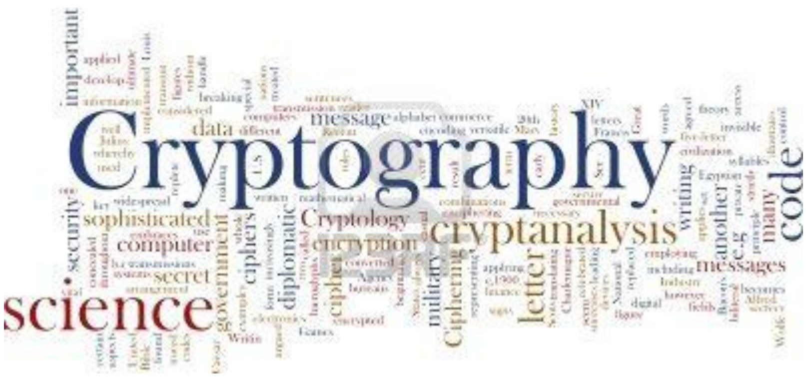
L'addition est associative et commutative. $\bar{0}$ est élément neutre et tout entier modulo n possède un opposé dans Z_n. Par exemple, $\bar{4}$ et $\bar{5}$ sont opposés dans Z_9 (voir exemple ci-dessus).

(Z_n , +) est donc un groupe commutatif.

3.2.4 Exercice

Construire la table de l'addition dans Z_6.

3.3 La multiplication dans Z_n



3.3.1 Définition

On définit dans $\mathbf{Z}_n$ une multiplication interne de la façon suivante :

$\forall \bar{a}, \forall \bar{b}, \bar{a} \times \bar{b} = \overline{ab}$.

3.3.2 Exemples

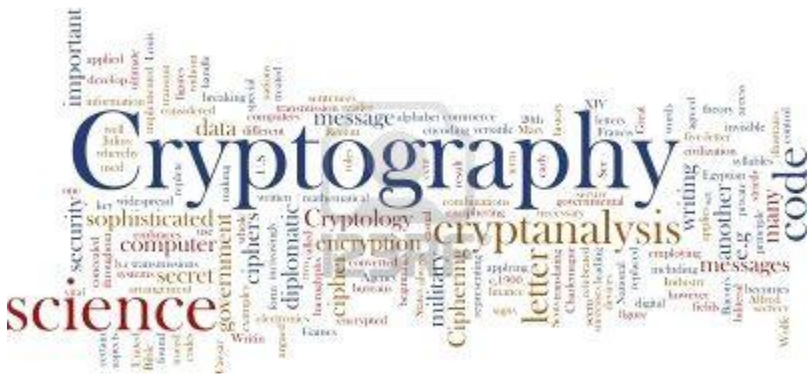
Dans $\mathbf{Z}_{11}$, $\bar{3} \times \bar{4} = \bar{1}$ et $\bar{8} \times \bar{9} = \bar{6}$. Dans $\mathbf{Z}_{26}$, $\bar{2} \times \overline{13} = \bar{0}$ et $\bar{3} \times \bar{9} = \bar{1}$.

3.3.3 Propriétés de la multiplication dans $\mathbf{Z}_n$

La multiplication dans $\mathbf{Z}_n$ est associative, commutative et distributive sur l'addition. $\bar{1}$ est élément neutre.

3.3.4 Définition

Soient $\bar{a} \neq \bar{0}$ et $\bar{b} \neq \bar{0}$. Les entiers modulo n $\bar{a}$ et $\bar{b}$ sont dits diviseurs de $\bar{0}$ modulo n lorsque $\bar{a} \times \bar{b} = \bar{0}$ dans $\mathbf{Z}_n$.



Par exemple, $\overline{2}$ et $\overline{3}$ sont diviseurs de $\overline{0}$ modulo 6, mais ne le sont pas modulo 7.

3.3.5 Définition ; notion d'inverse

$\overline{a}$ est dit inversible modulo n s'il existe $\overline{b}$ tel que $\overline{a} \times \overline{b} = \overline{1}$. On dit alors que les entiers (modulo n) $\overline{a}$ et $\overline{b}$ sont inverses l'un de l'autre, modulo n.

Par exemple, $\overline{6}$ et $\overline{4}$ sont inverses l'un de l'autre modulo 23.

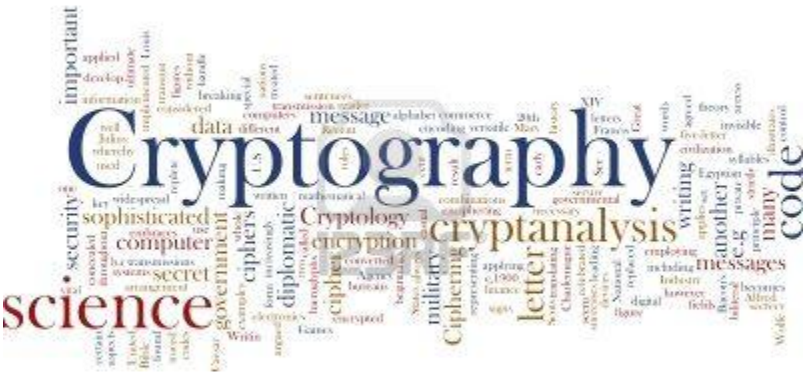
3.3.6 Exercice

Construire les tables de la multiplication dans Z_6 et dans Z_7. Commentaires.

3.4 L'anneau des entiers modulo n

3.4.1 Notations

La structure (Z_n , +, $\times$) est appelée anneau des entiers modulo n. Cet anneau est unitaire et commutatif. Pour plus de commodité, l'entier modulo n $\overline{a}$ sera dorénavant noté a.



On note $\mathbf{Z}_n^*$ l'ensemble des entiers modulo n inversibles.

3.4.2 Exercices

a) Déterminer $\mathbf{Z}_{10}^*$

b) Résoudre dans $\mathbf{Z}_9$ les équations suivantes (d'inconnue x):

$7x + 1 = 5$; $3x = 1$; $3x = 0$; $2x^2 = 5$.

c) Calculer 247^{349} dans $\mathbf{Z}_7$.

4. Nombres premiers ; pgcd et ppcm de deux entiers naturels ; algorithmes d'Euclide

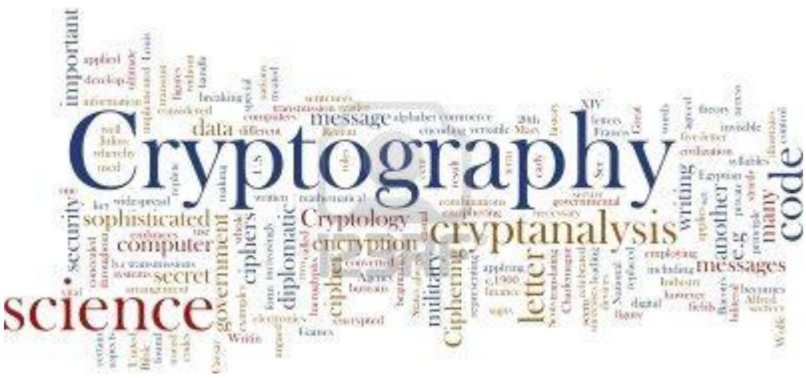
4.1 Les nombres premiers

4.1.1 Définition

Soit $p \in \mathbf{N}^*$, $p > 1$. L'entier (naturel) p est dit premier si ses seuls diviseurs (distincts) sont 1 et lui-même. L'entier 1 n'est donc pas premier. Un entier non premier est dit composé.

4.1.2 Résultats importants

a) Théorème 2 (dû à Euclide)



L'ensemble des nombres premiers est infini.

b) Proposition 6

Soit $n \in \mathbf{N}^*$, $n > 1$. L'entier n possède au moins un diviseur premier et se décompose de façon unique en produit de facteurs premiers.

c) Proposition 7

Soit $n \in \mathbf{N}^*$, $n > 1$.

Si n est composé, alors il existe p premier tel que $p \mid n$ et $p^2 \leq n$.

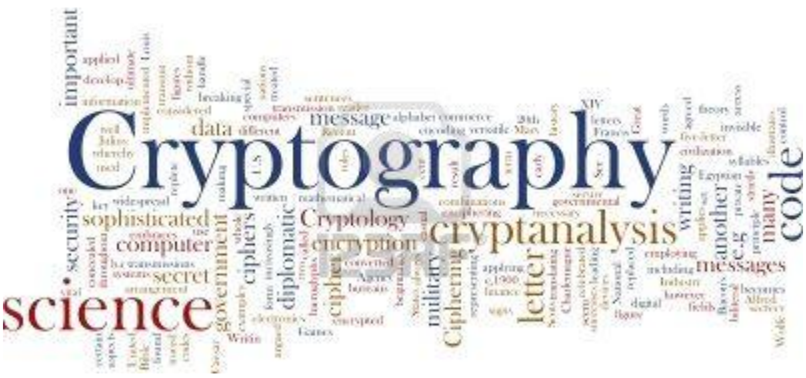
On en déduit un critère de primalité :

Si n n'est divisible par aucun nombre premier dont le carré lui est inférieur, alors n est premier.

4.1.3 Crible d'Eratosthène

Eratosthène est né à Cyrène vers –284. Il fut « bibliothécaire » à la très fameuse Bibliothèque d'Alexandrie où il mourut vers –192. Il fut le premier à donner une mesure relativement exacte de la circonférence de la terre.

0) Dresser la liste finie L_0 = { 2, 3, 4, …, n }.



1) 2 est premier, donc on garde 2 et on efface dans L_0 tous les nombres pairs supérieurs à 2. On obtient ainsi une liste L_1. Le plus petit entier non effacé est 3 donc :
2) 3 est premier, donc on garde 3 et on efface tous les multiples de 3 de L_1 qui sont supérieurs à 3. On obtient ainsi L_2. Le plus petit entier de L_2 non effacé est 5 donc :

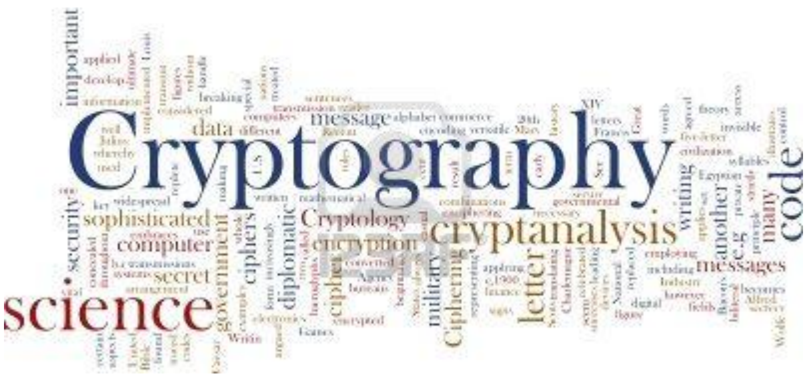
…

Lorsqu'on ne peut plus effacer de nombre, la liste L_r obtenue est la liste des nombres premiers appartenant à L_0.

4.1.4 Exercices

1) Etablir la liste des nombres premiers inférieurs à 500 à l'aide du crible d'Eratosthène.
2) Décomposer 1 179 750 en un produit de facteurs premiers.
3) 1517 et 2309 sont-ils premiers ?
4) Les nombres de Mersenne (1644)

   Pierre Marin de Mersenne, né dans le Maine en 1588, mourut à Paris en 1648. Religieux de l'Ordre des Minimes et scientifique il échangea une importante correspondance avec Descartes, Pascal et Fermat notamment.



On rappelle que $\forall a\in\mathbf{N}$, $\forall n\in\mathbf{N}^*$, $a^n-1 = (a-1)(a^{n-1} + a^{n-2} +\ldots+ a^2 + a + 1)$.

Soit $n\in\mathbf{N}^*$, $n > 1$ et soit $a\in\mathbf{N}^*$.

a) Montrer que si $a^n -1$ est premier, alors $a = 2$.
b) Soit $(p, q)\in\mathbf{N}^2$. Montrer que si $p\neq 0$, alors $2^p - 1 \mid 2^{pq} - 1$.
c) En déduire que si 2^n-1 est premier, alors n est premier. Réciproque ?

Les nombres 2^p-1, notés M_p, où p est premier, sont appelés nombres de Mersenne. Ils ne sont pas tous premiers. Par exemple, $M_{11} = 2047 = 23\times 89$. F.Cole a factorisé M_{67} en 1903 : $2^{67}-1 = 193\,707\,721\times 761\,838\,257\,287$.

En août 2008 on a trouvé le 45ème nombre de Mersenne premier : $2^{43112609} - 1$ qui occupe 12978189 bits…Le 46ème a été trouvé en septembre 2008 mais il est plus « petit » : $2^{37156667} - 1$ n'occupant que 11185272 bits…

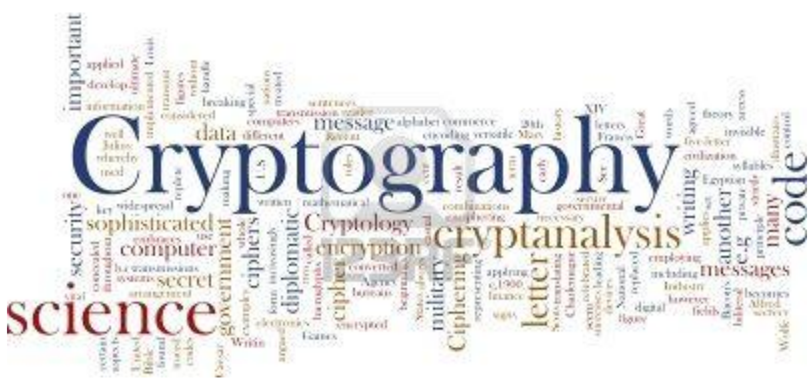
Pour en savoir plus : http://www.mersenne.org/

d) Calculer M_2, M_3, M_5 et M_7. Sont-ils premiers ?

5) Les nombres de Fermat

Pierre de Fermat (1601-1665) fut conseiller au Parlement de Toulouse. Concernant l'arithmétique, il est auteur de nombreuses conjectures célèbres mais n'a pas toujours pris le temps d'en fournir la preuve !

Leonhard Euler (1707-1783) fut le plus grand mathématicien du milieu du XVIIIe siècle. Ses contributions, notamment à la théorie des nombres, sont très nombreuses.



Pour n $\in\mathbf{N}$, le nombre $F_n = 2^{2^n} + 1$ est appelé nombre de Fermat.

Fermat conjecturait en 1640 que ce nombre est premier, $\forall n\in\mathbf{N}$. C'est faux : Euler a factorisé F_5 en 1732 : F_5 = 4 294 967 297 = 641×6 700 417.

Calculer F_0, F_1, F_2, F_3 et F_4. Sont-ils premiers ?

On sait aujourd'hui que F_n est composé pour $5 \leq n \leq 21$ et on conjecture que F_n est composé à partir d'un certain rang.

6) <u>La conjecture de Goldbach</u>

Christian Goldbach (1690-1764), dans une lettre à Euler datant de 1742, livre sa célèbre conjecture (non encore totalement démontrée à ce jour…) :

« Tout entier pair supérieur à 2 est somme de deux nombres premiers »

Trouver deux nombres premiers dont la somme vaut 5 000.

4.1.5 Théorèmes

<u>Théorème 3 : théorème des nombres premiers (tnp)</u>

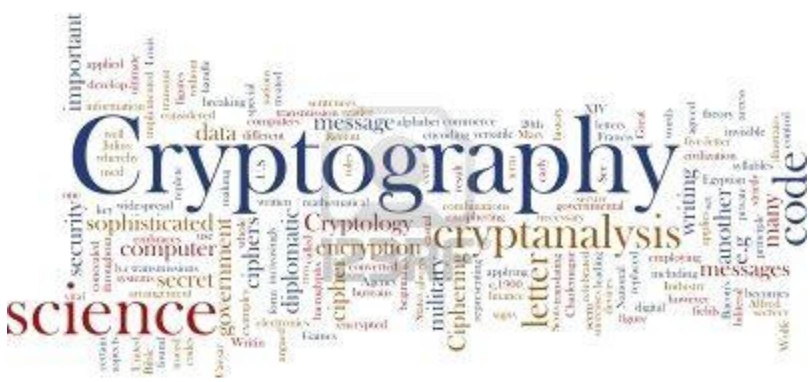
Adrien-Marie Legendre (1752-1833), auteur d'un *Essai sur la théorie des nombres*, apporte notamment une preuve du « grand » *théorème* de Fermat pour n = 5.

Jacques Hadamard (1865-1963) apporte le premier une preuve du « théorème des nombres premiers ».

Charles de La Vallée Poussin (1866-1962), auteur de travaux sur la théorie des nombres.

Bernhard Riemann (1826-1866) s'est illustré dans de nombreuses branches des mathématiques et a fourni une contribution majeure à la théorie analytique des nombres grâce à sa fameuse fonction ζ.

Conjecturé par Gauss en 1792, puis Legendre en 1798 puis 1808, démontré en 1896



par Hadamard et en 1898 par La Vallée Poussin, s'appuyant sur les travaux de Riemann sur la fonction ζ (1859), le théorème des nombres premiers donne un ordre de grandeur de $\pi(x)$.

On note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x pour $x \in \mathbf{R}$.

$$\text{tnp : Pour } x \text{ suffisamment « grand », } \pi(x) \sim \frac{x}{\ln x}.$$

Théorème 4 : (postulat de Bertrand) Théorème de Tchébychev (1854)

Joseph Bertrand (1822-1900) postule en1845 que si $n > 3$, il existe au moins un nombre premier compris entre n et $2n - 2$.
Pafnouti Lvovitch Tchebychev (1821-1894), grand mathématicien russe, démontre ce postulat en 1854.

On a montré depuis qu'il existe toujours un nombre premier entre x et $\frac{9}{8}x$ pour $x \geq 48$ (Breusch, 1931) et entre x^3 et $(x + 1)^3$ pour x assez grand (Ingham, 1932).

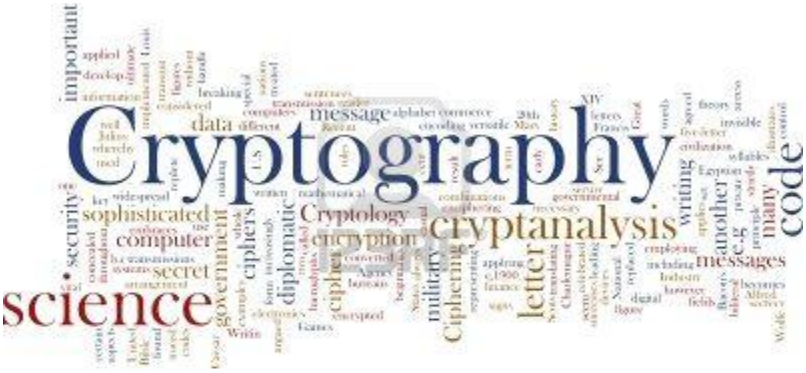
4.2 Pgcd de deux entiers naturels

Soient $a \in \mathbf{N}^*$ et $b \in \mathbf{N}^*$.

4.2.1 Définitions

1) On appelle pgcd(a, b) le plus grand diviseur commun à a et b. Pgcd(a, b) peut être noté $a \wedge b$.
2) a et b sont dits étrangers (ou premiers entre eux) lorsque $a \wedge b = 1$.

4.2.2 Remarques ; exemples



Deux nombres premiers sont nécessairement étrangers. La réciproque est fausse. Par exemple, $7 \wedge 9 = 1$, $8 \wedge 9 = 1$.

6 et 8 ne sont pas étrangers car $6 \wedge 8 = 2$.

4.2.3 Propriétés

1) $\wedge$ est une loi de composition (interne) dans $\mathbf{N}^*$, commutative et associative.
2) $a \wedge a = a$
3) La multiplication est distributive par rapport à $\wedge$
4) $a \wedge b = d \Leftrightarrow$ il existe a' et b' tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$.
5) $k \wedge a \wedge b = 1 \Rightarrow k \wedge (ab) = (k \wedge a)(k \wedge b)$

4.3 Ppcm de deux entiers naturels

Soient $a \in \mathbf{N}^*$ et $b \in \mathbf{N}^*$.

4.3.1 Définition

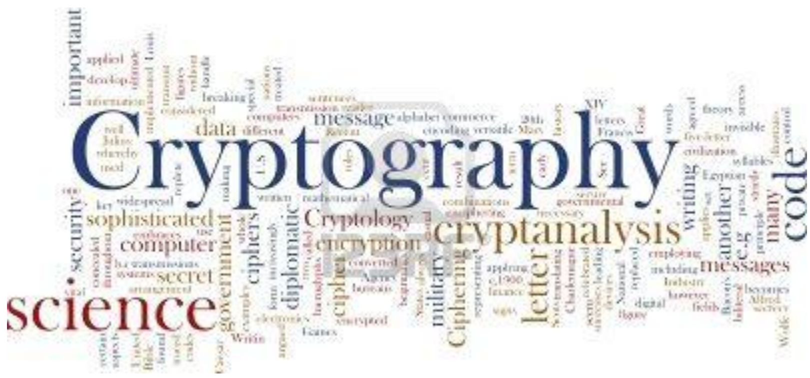
On appelle ppcm(a, b) le plus petit multiple commun à a et b. Ppcm(a, b) peut être noté $a \vee b$.

4.3.2 Exemples

$2 \vee 3 = 6$; $2 \vee 4 = 4$; $4 \vee 6 = 12$

4.3.3 Propriétés

1) $\vee$ est une loi de composition (interne) dans $\mathbf{N}^*$, commutative, associative et ayant 1 pour élément neutre.
2) $a \vee a = a$
3) La multiplication est distributive par rapport à $\vee$



4) $(a \wedge b)(a \vee b) = ab$. En particulier, si $a \wedge b = 1$, alors $a \vee b = ab$.

4.4 Algorithme d'Euclide (recherche du pgcd)

4.4.1 Principe de l'algorithme

Soient $a \in \mathbf{N}^*$, $b \in \mathbf{N}^*$ et $b < a$.

On opère les divisions euclidiennes suivantes :

1) $a = bq_1 + r_1$ avec $0 \le r_1 < b$

2) $b = r_1q_2 + r_2$ avec $0 \le r_2 < r_1$

3) $r_1 = r_2q_3 + r_3$ avec $0 \le r_3 < r_2$

…

n) $r_{n-2} = r_{n-1}q_n + r_n$ avec $0 \le r_n < r_{n-1}$

n+1) $r_{n-1} = r_nq_{n+1}$.

On a alors $a \wedge b = r_n$.

Application numérique : déterminer $1800 \wedge 1296$.

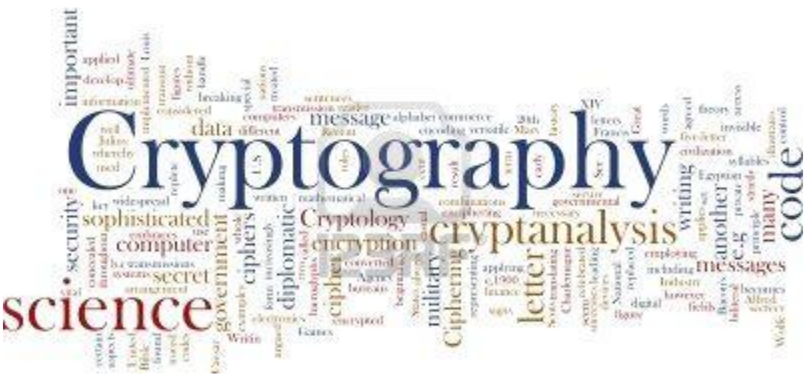
4.4.2 Théorème 5 : théorème de Lamé (1845)

Gabriel Lamé (1795-1870) s'intéressa notamment à l'algorithme d'Euclide.

Le nombre d de divisions nécessaires à la terminaison de l'algorithme d'Euclide appliqué à a et b, où b < a, vérifie $d \le \log a$ où $\alpha = \dfrac{1+\sqrt{5}}{2}$.

N.B α est appelé Nombre d'Or…

Application numérique : quel est le nombre maximal de « boucles » nécessaires à la détermination du pgcd de 41 871 597 et de n'importe quel nombre qui lui est



inférieur en utilisant l'algorithme d'Euclide ?

4.5 Algorithme d'Euclide étendu ; théorème de Bachet ; conséquences

L'algorithme d'Euclide étendu permet d'établir une relation entre a, b et $a \wedge b$ très riche de conséquences. Cette relation, dont la paternité fut attribuée à tort à Etienne Bézout (1730-1783), auteur d'une relation analogue dans l'anneau des polynômes, est en fait due à Claude Gaspard Bachet de Méziriac (1581-1638).

4.5.1 Algorithme d'Euclide étendu

Les égalités euclidiennes 1), 2), …n) de l'algorithme d'Euclide permettent d'écrire :

1') $a - bq_1 = r_1$ (1). D'où $aq_2 - bq_1q_2 = r_1q_2$. Ceci, ôté de 2), fournit :

2') $-aq_2 + b(1 + q_1q_2) = r_2$, de la forme $au_2 + bv_2 = r_2$ (2). On opère de même en multipliant (2) par q_3 pour obtenir, après l'avoir ôté de 3) :

3') $a(1 + q_2q_3) + b(-q_1 - q_3 - q_1q_2q_3) = r_3$, de la forme $au_3 + bv_3 = r_3$.

…

On obtient ainsi, de proche en proche, une relation de la forme :

$$au_n + bv_n = r_n = a \wedge b.$$

4.5.2 Exemple

Avec a = 1800 et b = 1296, on a trouvé en 4.4.1 : $1296 \wedge 1800 = 72$ avec :

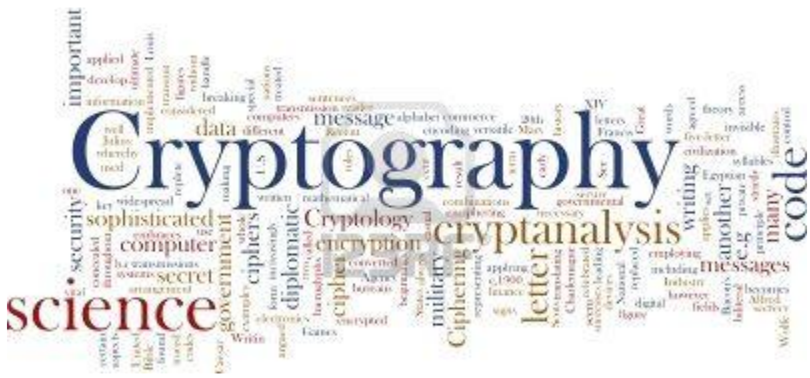
$1800 = 1296 \times 1 + 504$; $1296 = 504 \times 2 + 288$; $504 = 288 \times 1 + 216$;

$288 = 216 \times 1 + 72$ et enfin $216 = 72 \times 3$.

On a donc :

$$72 = 288 - 216 = 288 - (504 - 288) = 2 \times 288 - 504 = 2 \times (1296 - 2 \times 504) - 504$$
$$= 2 \times 1296 - 5 \times 504 = 2 \times 1296 - 5(1800 - 1296) \text{ d'où :}$$

$72 = 7 \times 1296 - 5 \times 1800$.



4.5.3 Théorème 6 : théorème de Bachet (Formule de Bézout)

Soient $a \in \mathbf{N}^*$, $b \in \mathbf{N}^*$.

Il existe $u \in \mathbf{Z}$, il existe $v \in \mathbf{Z}$, tels que $au + bv = a \wedge b$.

En particulier, si $a \wedge b = 1$, il existe des entiers relatifs u et v tels que $au + bv = 1$. C'est cette dernière relation qui est souvent appelée identité de Bézout. On en déduit immédiatement que si $a \wedge b = 1$ et $a < b$, alors a est inversible modulo b car $au \equiv 1\ (b)$.

Voilà pourquoi $\mathbf{Z}_{10}{}^*$ contient aussi peu d'éléments (voir 3.4.2 a). En effet, seuls 1, 3, 7 et 9 sont étrangers à 10.

4.5.4 Conséquences du théorème de Bachet

Diophante (environ – 410 ; environ – 325) s'intéressa notamment aux équations du type $ax + by = c$ où a,b et c sont des entiers donnés et où x et y sont des entiers inconnus. Ces équations sont appelées aujourd'hui équations diophantiennes.

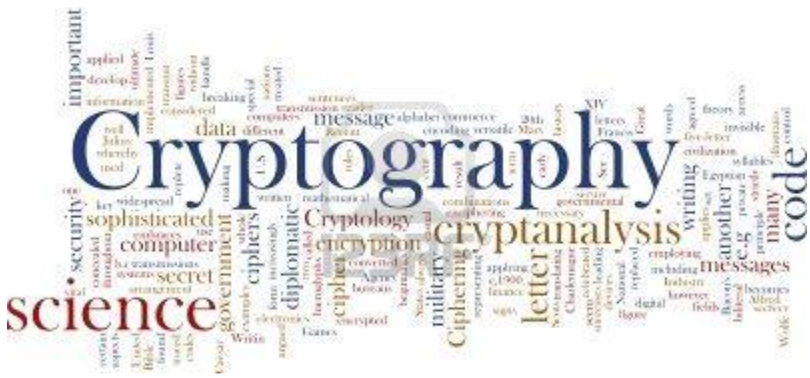
Proposition 8

$a \wedge b = 1 \Leftrightarrow \forall z \in \mathbf{Z}$, l'équation diophantienne $ax + by = z$ possède au moins une solution $(x, y) \in \mathbf{Z}^2$.

Proposition 9

p premier $\Leftrightarrow (\mathbf{Z}_p, +, \times)$ est un corps (commutatif). Ce corps peut être noté $\mathbf{F}_p$.

N.B Ce dernier résultat est particulièrement important : il signifie que tous les entiers



non nuls modulo p sont inversibles. L'inverse de a (p) sera noté a^{-1} (p).

On a $\mathbf{F}_p^* = \{ 1, 2, 3, \ldots, p-1 \}$. **F** signifie "field" en anglais.

4.5.5 Exercice : construction de l'algorithme d'Euclide étendu

Soient k et n tels que $0 < k < n$ avec $d = k \wedge n$. Il s'agit de calculer efficacement u et v tels que $un + vk = d$. Si, de plus, on a $d = 1$, alors $k^{-1} = v$ (n).

On pose $u_0 = 1$, $u_1 = 0$, $v_0 = 0$, $v_1 = 1$;

On pose aussi $u_{i+2} = -q_i u_{i+1} + u_i$ et $v_{i+2} = -q_i v_{i+1} + v_i$ où q_i est défini par la suite des divisions euclidiennes :

$n = kq_0 + r_0$

$k = r_0 q_1 + r_1$

$r_0 = r_1 q_2 + r_2$

…

$r_{i-2} = r_{i-1} q_i + r_i$

…

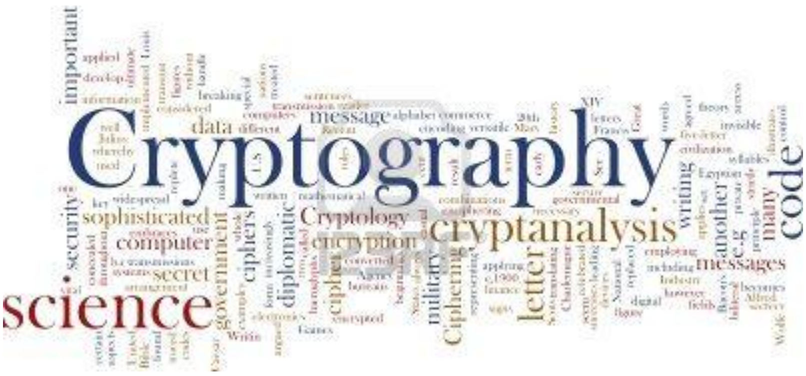
On montre alors (par récurrence) que pour tout i, $u_{i+2}n + v_{i+2}k = r_i$. La suite des r_i étant strictement décroissante et minorée par 0, on arrive ainsi nécessairement à la relation $u_{m+2}n + v_{m+2}k = r_m = d = k \wedge n$. d'où $u = u_{m+2}$ et $v = v_{m+2}$. On montre par ailleurs que u et v vérifient $|u| \le k$ et $|v| \le n$.

On montre enfin que l'algorithme d'Euclide étendu, vu sous la forme ci-dessus, est « rapide », même pour de grandes valeurs de k et de n.

4.6 Théorème de Gauss et conséquences

4.6.1 Théorème 7 : théorème de Gauss

(il serait dû en fait à Jean Prestet (1648-1690)…)



$a \wedge b = 1 \Leftrightarrow (\ \forall c \in \mathbf{Z}$, si $a \mid bc$, alors $a \mid c)$

ou encore :

$a \wedge b = 1 \Leftrightarrow (\forall c \in \mathbf{Z},\ bc \equiv 0\ (a) \Rightarrow c \equiv 0\ (a)\ )$.

4.6.2 Conséquences

1) $(\ a \wedge b = 1$ et $a \wedge c = 1\ ) \Rightarrow a \wedge (bc) = 1$
2) $a \wedge b = 1 \Rightarrow (\ \forall n > 1,\ a \wedge b^n = 1)$
3) (p premier et $p \mid ab) \Rightarrow (\ p \mid a$ ou $p \mid b\ )$
4) $\forall n \geq 1$,(p premier et $p \mid a^n\ ) \Rightarrow p \mid a$

5. Indicateur d'Euler ; « grands » théorèmes

5.1 Définition de l'indicateur d'Euler

$\forall n \in \mathbf{N}^*$, $n>1$, on note $\varphi(n)$ le nombre d'éléments de $\mathbf{Z}_n^*$. C'est donc le nombre d'éléments inversibles de $\mathbf{Z}_n$. C'est donc aussi le nombre d'entiers naturels strictement positifs, inférieurs ou égaux à n et premiers avec n. On admet par ailleurs que $\varphi(1) = 1$. $\varphi(n)$ est appelé indicateur d'Euler. La notation $\varphi(n)$ a été introduite par Gauss.

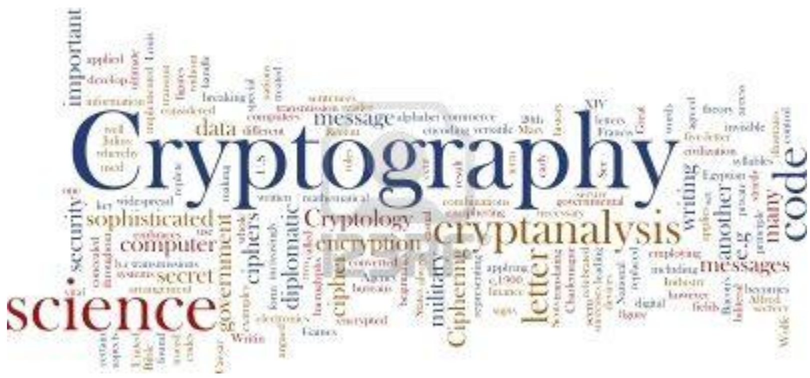
5.2 Exemple

Calculer $\varphi(n)$ pour tout n compris entre 1 et 10.

5.3 Théorème 8 (dû à Euler)

$n = \sum_{d} \varphi(d)$ où les valeurs de d sont les diviseurs de n.

Application numérique Vérifier que $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$



5.4 Corollaire

p premier $\Leftrightarrow \varphi(p) = p - 1$.

5.5 Théorème 9 : théorème d'Euler (1760)

Si $a \wedge n = 1$, alors $a^{\varphi(n)} \equiv 1\ (n)$

Cet important théorème généralise une conjecture due à Fermat, son « petit » *théorème*, qui devient ainsi un corollaire du théorème d'Euler.

5.6 Corollaire : « petit » *théorème* de Fermat (1640 environ)

Si p est premier, alors pour tout a tel que $1 \leq a \leq p - 1$, $a^{p-1} \equiv 1\ (p)$.

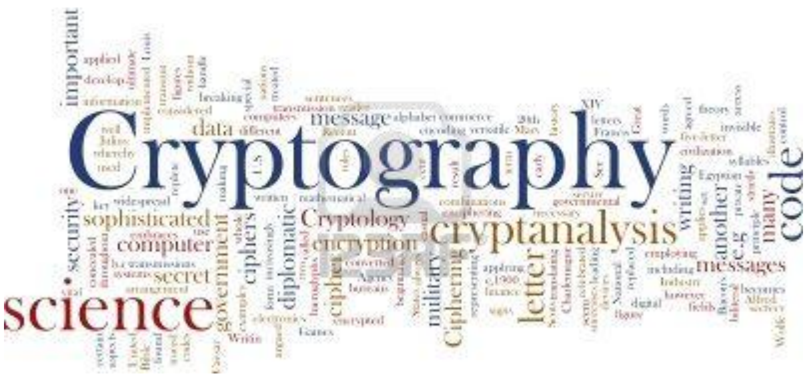
La réciproque est fausse, donc ce théorème ne caractérise pas les nombres premiers. Un nombre n non premier tel que, pour tout a étranger à n et inférieur à n, on a quand même $a^{n-1} \equiv 1\ (n)$ est appelé nombre de Carmichaël (Robert D. Carmichaël (1879-1967), professeur à l'Université de l'Illinois). Les trois premiers nombres de Carmichaël sont 561, 1105 et 1729. On a montré (en 1992, Alford, Granville et Pomerance) qu'il existe une infinité de nombres de Carmichaël.

5.7 Théorème10 : « théorème chinois »

Si $p \wedge q = 1$, alors les anneaux $\mathbf{Z}_{pq}$ et $\mathbf{Z}_p \times \mathbf{Z}_q$ sont isomorphes.

Ce résultat peut être étendu à un nombre fini d'entiers naturels premiers entre eux deux à deux.

Cet important théorème (établi et démontré en 1734 par Euler) est en



fait la forme la plus aboutie d'un résultat utilisé depuis l'antiquité par les (astronomes ?) chinois mais aussi vraisemblablement par les (astronomes ?) babyloniens (voir corollaire 1).

5.7.1 Corollaire 1 : « lemme chinois » ou « théorème des restes chinois »

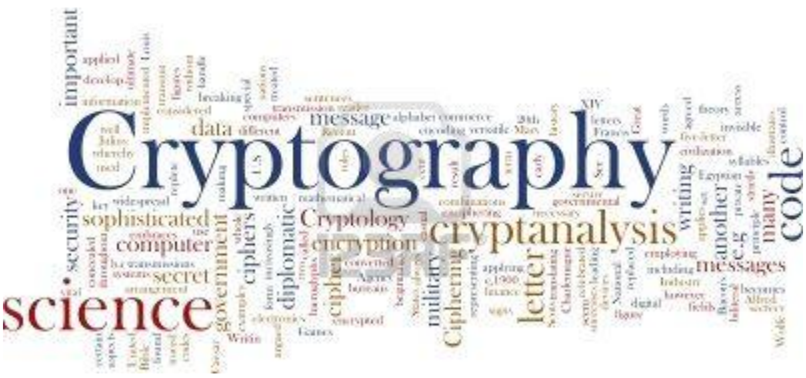
Lorsque $p \wedge q = 1$, le système $\begin{cases} x \equiv a \ (p) \\ x \equiv b \ (q) \end{cases}$ où a et b sont des entiers naturels donnés, possède une unique solution x dans $\mathbf{Z}_{pq}$.

On montre que la solution est $x = upb + vqa \ (pq)$ où u et v vérifient le théorème de Bachet : $up + vq = 1$. On trouve u et v grâce à l'algorithme d'Euclide étendu.

Ce corollaire traduit le fait que la projection naturelle $\mathbf{Z}_{pq} \to \mathbf{Z}_p \times \mathbf{Z}_q$ est bijective.

Remarque Lorsque $p_1, p_2, .., p_k$ sont premiers entre eux deux à deux, le système $\begin{cases} x \equiv a_1 (p_1) \\ x \equiv a_2 (p_2) \\ \ldots \\ x \equiv a_k (p_k) \end{cases}$ se résout de proche en proche en trouvant d'abord x_{12} (p_1p_2), puis x_{123} $(p_1p_2p_3)$, jusqu'à trouver enfin x $\left(\prod_{i=1}^{k} p_i\right)$.

On peut aussi procéder de la façon suivante : en posant n =

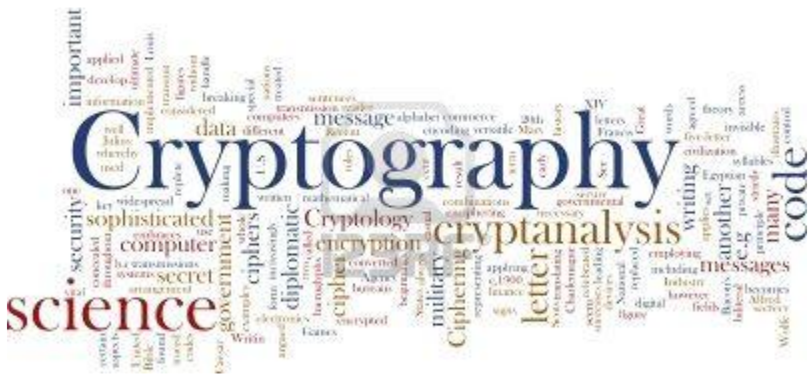


$\prod_{i=1}^{k} p_i$, puis $m_i = \frac{n}{p_i}$, on calcule $m_i^{-1}(p_i)$ grâce à l'algorithme d'Euclide étendu puis $c_i = m_i(m_i^{-1}(p_i))$. On a alors $x \equiv \sum_{i=1}^{k} a_i c_i \ (n)$.

On attribue au mathématicien chinois Sun-Tsu (environ 100 après J.C) la résolution du problème consistant à trouver les entiers x dont la division par 3, 5 et 7 a pour reste 2, 3 et 2 respectivement. La solution est 23 modulo 105. Le même cas particulier fut donné par le mathématicien grec Nichomachus autour de 100 après J.C. Il fut généralisé par un certain Chin Chiu-Shao en 1247.

5.7.2 Exercices

1) Une fleuriste possède encore en fin de journée un certain nombre de roses qu'elle assemble en bouquets. Si elle les regroupe par 5, il lui en restera 4 alors qu'il ne lui en restera que 2 si elle en fait des bouquets de 9. Combien lui reste-t-il de roses sachant qu'elle en avait reçu 70 en début de journée ?
2) On cherche à ranger environ 700 bouteilles par caisses de 5, de 6 ou de 13. Dans le premier cas, il en reste 4, dans le deuxième 3 et dans le dernier 10. Quel est le nombre total exact de bouteilles ?
3) (Trouvé sur le Web, proposé par Ahmed Zahidi en l'an 2000)
   Une comète A est apparue dans le ciel de la côte d'Azur il y a un an. Cette comète A n'apparaît que tous les 3 ans. Une comète B est apparue dans le ciel de la côte d'Azur il y a cinq ans. Cette comète B n'apparaît que tous les 7 ans. Une comète C est apparue dans le ciel de la côte d'Azur il y a huit ans. Cette comète C n'apparaît que tous les 17 ans.



En quelle année au plus tôt verra-t-on sur le ciel de la côte d'Azur filer les trois comètes A, B et C ?

5.7.3 Corollaire 2

$p \wedge q = 1 \Rightarrow \varphi(pq) = \varphi(p)\varphi(q)$

En particulier, si p et q sont premiers et $p \neq q$, alors $\varphi(pq) = (p-1)(q-1)$.

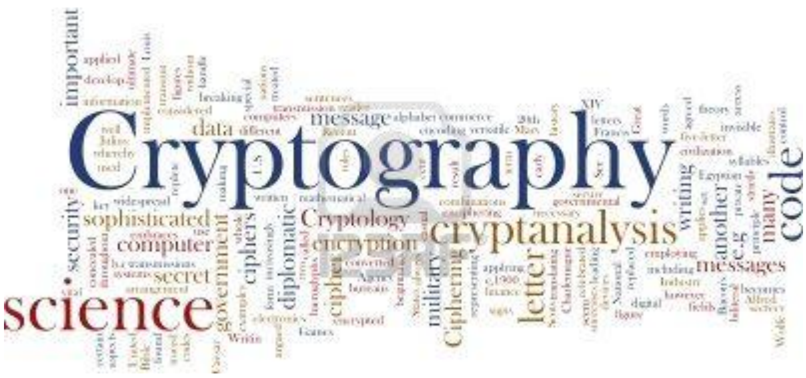
Ce dernier résultat est l'un des outils essentiels du cryptosystème RSA.

5.7.4 Corollaire 3

Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ est la décomposition de n en facteurs premiers, alors

$\varphi(n) = n\prod_{i=1}^{k}(1-p_i^{-1})$.

Ce résultat permet de calculer $\varphi(n)$ dès lors qu'on sait factoriser n. C'est cette factorisation de n (pour n grand !) qui reste de nos jours



encore très difficile…et fonde la validité du système RSA.

Remarque

La décomposition fournie par le corollaire 3 prouve que $\varphi(n)$ est pair pour $n > 2$, donc dans ce cas, on aura toujours $2 \wedge \varphi(n) \neq 1$.