Arithmétique

SOMMAIRE

Quelques programmes pour tester les notions

Introduction

a) **Un petit aperçu**

L'arithmétique est l'étude des nombres et plus particulièrement celle des entiers naturels.
Les entiers naturels permettent de dénombrer des collections d'objets, de les comparer (caractère cardinal et ordinal).
On comprend aussi, qu'à partir d'un entier naturel donné, on peut en trouver un autre plus grand en lui ajoutant 1, qui est son successeur.
Dernière ces objets simples à comprendre, qui semblent naturels par leur utilisation pratique, se cachent bien des propriétés surprenantes et des mystères cachés.

Ils rentrent aussi dans des théories mathématiques importantes, comme les structures algébriques d'anneaux et de corps ou encore la logique mathématique qui permet de construire de manière rigoureuse l'ensemble des entiers, soit de manière axiomatique, en rajoutant 5 axiomes qui définissent $\mathbb{N}$ à ceux qui définissent la théorie des ensembles (ZFC) (Paeno ≈1880), soit directement à partir de ces derniers (Von Neumann ≈1940)

b) **Des mystères cachés**

Bien des questions se posent encore sur ces nombres, et il est probable que de nouvelles théories verront le jour pour y répondre :

1) Conjecture de Goldbach

Un ami d'Euler, Christian Goldbach, a proposé en 1742 la conjecture que tout entier pair est somme de deux nombres premiers et tout entier impair somme de trois nombres premiers.
Aucune de ces deux conjectures n'est encore complètement démontrée, mais Vinogradov a pu établir en 1937 que tout nombre impair assez grand est somme de trois nombres premiers.

2) Hypothèse de Riemann

Elle porte sur les zéros de la fonction zéta à variable complexe:
$z(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$ où s est un nombre complexe.
L'hypothèse est que les zéros seraient tous de partie réelle égale à ½
C'est l'un des problèmes de Hilbert non résolu (1900) et qui est un des problèmes du millénaire (2000)
Les nombres premiers et cette fonction sont liés par le fait que la démonstration de cette

conjecture permettrait de mieux connaître la répartition des nombres premiers.

Euler (18ième siècle) a démontré que :
$z(s) = \prod_{p \in P} \frac{1}{1-p^{-s}}$ $avec\ Re(s) > 1$ où *P* est l'ensemble des nombres premiers
et z(2) = $\frac{\pi^2}{6}$
La première formule est le produit eulérien qui permet de démontrer cet équivalent :
$p_n \approx nln(n)$ où p_n désigne le n ième nombre premier

3) Nombres de Fermat
Ce sont les nombres de la forme $2^{2^n} + 1$ $noté\ F_n$ où n est un entier naturel
On ne sait pas encore si F_{33} est premier ou pas
On ne sait pas s'il y a une infinité de nombres de Fermat premiers ni une infinité de nombres de Fermat non premiers

4) Nombres parfaits
Ce sont les entiers naturels qui sont égaux à la somme de leurs diviseurs propres positifs ;
On ne sait pas s'il y en a une infinité.

c) **Quelques citations**
« Tout est nombre » Pour l'école Pythagoricienne (vers 550 avant J.C.)
« Le seul objet naturel de la pensée mathématique, c'est le nombre entier » Henri Poincaré 1854-1912
« Dieu fit les nombres naturels ; tout autre est l'œuvre de l'homme » Léopold Kronecker au 19ième siècle

Retour au sommaire

Cours

Divisibilité

a) Définition
Soient a et b deux entiers, b≠0
On dit que b divise a et on note b|a, lorsqu'il existe un entier k tel que a=bk
On dit aussi que a est divisible par b ou a est un multiple de b ou b est un diviseur de a.

b) Division euclidienne
Théorème
Soient a et b deux entiers, b non nul.
Il existe un et un seul couple (q,r) d'entiers vérifiant

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

Démonstration
Existence
Si a est un multiple de b, c'est-à-dire a=kb où k est un entier,
alors le couple (k,0) convient
Sinon, en prenant le plus grand multiple de b inférieur à a qui est de la forme kb où k est un entier.
Notons r=a-kb
alors le couple (k,r) convient.
Unicité
Notons (q,r) et (q',r') deux couples vérifiant

$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$ et $\begin{cases} a = bq' + r' \\ 0 \leq r' < |b| \end{cases}$

Démontrons que ces deux couples sont égaux.

On a donc r-r'=b(q'-q), et donc r-r' est un multiple de b.

Mais on a aussi -|b|<r-r'<|b|, or le seul multiple de b strictement compris entre -|b| et |b| est 0, donc r-r'=0 et donc r=r'.

On en déduit aisément que bq=bq' et comme b≠0, q=q'

c) Propriétés

D1) Soient a et b deux entiers, b≠0

$\boxed{b|a \iff le\ reste\ de\ la\ division\ euclidienne\ de\ a\ par\ b\ est\ nul}$

Démonstration :

⇒

Par hypothèse, il existe k entier tel que a=bk=bk+0 et par unicité du couple (q,r) dans la division euclidienne de a par b, on a (q,r)=(k,0) et donc r=0

⇐ (Réciproquement)

si r=0 alors a=qb et donc b divise a

D2) Soient a, b et c trois entiers, b≠0 et c≠0

$\boxed{Si\ c|b\ et\ b|a\ alors\ c|a}$

Démonstration :

Par hypothèse, il existe deux entiers n et m tels que b=cn et a=bm

Donc a=cnm et comme nm est un entier, c|a

D3) Soient a, b et c trois entiers, c≠0

$\boxed{Si\ c|b\ et\ c|a\ alors\ c\ divise\ toute\ combinaison\ à\ coefficients\ entiers\ de\ a\ et\ b}$

Démonstration :

Soient x et y deux entiers quelconques, considérons la combinaison ax+by

Par hypothèse il existe deux entiers m et n tels que a=cm et b=cn

Donc ax+by=c(mx+ny) et comme mx+ny est un entier on a donc c|(ax+by)

En particulier c|(a+b) et c|(a-b)

D4) Soient a et b deux entiers non nuls

$\boxed{Si\ a|b\ et\ b|a\ alors\ a = b\ ou\ a = -b}$

Démonstration :

Par hypothèse il existe deux entiers m et n tels que a=bm et b=an donc a=mna et comme a est non nul, on a mn=1 ;

Mais m et n sont deux entiers, donc m=n=1 ou m=n=-1, c'est-à-dire a=b ou a=-b

Remarques :

L'ensemble des diviseurs d'un entier a strictement positif est de la forme : $\{-a, \dots, -1, 1, \dots a\}$

$\mathbb{Z}^*$ est l'ensemble des diviseurs de 0

Retour au sommaire

Congruences

a) Définition

Soient a et b deux entiers, et p un entier naturel non nul
On dit que a est congru à b modulo p et on note a ≡ b (p) ou a ≡ b modulo p, lorsque a et b ont le même reste dans la division euclidienne par p

b) Propriétés

Par la suite a, b, c et d désignent des entiers et p un entier strictement positif

C1) $\boxed{a \equiv b(p) \Leftrightarrow p|(a-b)}$

Démonstration :

⇒

Par hypothèse, a et b ont le même reste dans la division euclidienne par p et si on le note r, on a $a=q_1p+r$ et $b=q_2p+r$ où q_1 et q_2 sont deux entiers
donc $a-b=p(q_1-q_2)$ et donc p|(a-b)

⇐ (Réciproquement)
Par hypothèse, il existe un entier k tel que a-b=kp
On a par ailleurs $a=q_1p+r_1$ et $b=q_2p+r_2$ par la division euclidienne de a par p et b par p
Donc $a-b=p(q_1-q_2)+r_1-r_2$ et comme a-b=kp, on obtient $r_1-r_2 = p(k-q_1+q_2)$ qui est un multiple de p.
Mais $0 \leq r_1 < p$ et $0 \leq r_2 < p$ donc $-p < r_1 - r_2 < p$ et donc $r_1-r_2=0$ car le seul multiple de p strictement entre –p et p est 0
Donc $r_1=r_2$ c'est-à-dire a ≡ b (p)

Conséquences :
1) Si r est le reste de la division euclidienne de a par p alors a ≡ r (p)
2) a ≡ 0 (p) ⇔ p|a

C2) $\boxed{si\ a \equiv b\ (p)\ et\ c \equiv d\ (p)\ alors\ a+c \equiv b+d\ (p)}$

Démonstration :
Par hypothèse, et avec C1) p|(a-b) et p|(c-d) et d'après D3) p|(a-b)+(c-d) soit p|((a+c)-(b+d)) et avec C1) on obtient a+c ≡ b+d (p)

C3) $\boxed{si\ a \equiv b\ (p)\ et\ c \equiv d\ (p)\ alors\ ac \equiv bd\ (p)}$

Démonstration :
Par hypothèse, et avec C1) p|(a-b) et p|(c-d) et d'après D3) p|(a-b)c+(c-d)b ou encore p|(ac-bd) et avec C1) on a ac ≡ bd (p)
En particulier en prenant c=d et comme c ≡ c (p), on a alors ac ≡ bc (p)

C4) Soit n un entier naturel non nul quelconque

$\boxed{Si\ a \equiv b(p)\ alors\ a^n \equiv b^n(p)}$

Démonstration par récurrence
Notons P(n) la proposition « $a^n \equiv b^n$ (p) »
Elle est vraie au rang initial 1 : c'est l'hypothèse
Soit n un entier strictement positif, supposons P(n) vraie : $a^n \equiv b^n$ (p) (HR), et démontrons qu'alors P(n+1) est vraie : $a^{n+1} \equiv b^{n+1}$ (p)
Mais a ≡ b (p), et par hypothèse de récurrence, $a^n \equiv b^n$ (p), on en déduit donc d'après C3), que $a^{n+1} \equiv b^{n+1}$ (p)
La proposition P(n) est vraie au rang initial 1 et est héréditaire, elle est donc vraie pour tout entier n supérieur ou égal à 1

Un exemple d'utilisation des congruences dans le calcul d'un reste :
Quel est le reste de la division euclidienne de a=2222222222 par 97 ?
On décompose a ainsi : $a=22 + 22x100 + 22x100^2 + 22x100^3 + 22x100^4$

$100 \equiv 3(97)$ donc, avec C4) $100^2 \equiv 3^2(97)$ d'où $100^2 \equiv 9(97)$

$100^3 \equiv 3^3(97)$ d'où $100^3 \equiv 27(97)$

$100^4 \equiv 3^4(97)$ d'où $100^4 \equiv 81(97)$

avec C3) $22 \times 100 \equiv 22 \times 3(97)$ d'où $22 \times 100 \equiv 66(97)$

$22 \times 100^2 \equiv 22 \times 9(97)$ d'où $22 \times 100^2 \equiv 198(97)$

$22 \times 100^3 \equiv 22 \times 27(97)$ d'où $22 \times 100^3 \equiv 594(97)$

$22 \times 100^4 \equiv 22 \times 81(97)$ d'où $22 \times 100^4 \equiv 1782(97)$

et avec C2) $a \equiv 22+66+198+594+1782(97)$ d'où $a \equiv 2662(97)$

Et on recommence : $2662 = 26 \times 100 + 62 \equiv 26 \times 3 + 62(97)$ donc $2662 \equiv 140(97)$

$140 = 100 + 40 \equiv 3 + 40(97)$ et donc $a \equiv 43(97)$: 43 est le reste demandé

Retour au sommaire

Nombres premiers

a) Définition

Soit p un entier strictement supérieur à 1, nous savons déjà que p admet au moins 2 diviseurs positifs : 1 et lui-même.

p est dit premier lorsqu' il n'a pas d'autres diviseurs positifs que 1 et lui-même, c'est-à-dire lorsqu'il a exactement 2 diviseurs positifs : 1 et lui-même.

L'ensemble des nombres premiers commence par 2, 3, 5, 7, 11, 13, 17, 19 etc...

1 n'est pas premier.

b) Propriétés

P1)

$\boxed{\textit{Un entier naturel } n \textit{ strictement supérieur à } 1, \textit{qui n'est pas premier, admet au moins un diviseur premier}}$

Démonstration

Notons p le plus petit diviseur positif de n autre que 1 et n.

p existe car n n'est pas premier.

Supposons p non premier : il aurait un diviseur positif d tel que $1<d<p$

Mais $d|p$ et $p|n$ donc $d|n$, de plus $1<d<n$ car $1<d<p$ et $p<n$, on aurait alors $d \geq p$ car p est le plus petit diviseur positif de n autre que 1 et n ; ce qui est en contradiction avec $d<p$.

Donc on a démontré par l'absurde que p est premier.

Remarque

$p|n \Rightarrow n=pq$ où q est un entier et comme $1<p<n$ alors $1<q<n$.

De plus, comme $q|n$ on en déduit que $p \leq q$ car p est le plus petit diviseur positif de n autre que 1 et n.

en multipliant les 2 membres par p, on obtient $p^2 \leq n$ soit $p \leq \sqrt{n}$.

On a donc démontré que si n est un entier naturel non premier alors n admet au moins un diviseur premier qui est inférieur ou égal à $\sqrt{n}$ (P1 bis)

P2) $\boxed{\textit{Il y a une infinité de nombres premiers}}$

Démonstration par l'absurde

Supposons qu'il y en ait un nombre fini N:

$p_1, p_2, p_3, \ldots, p_N$ classés dans l'ordre croissant.

Soit $a=p_1p_2p_3\ldots p_N+1$, a n'est pas premier car $a>p_N$, donc a admet un diviseur premier, d'après P1) qui est l'un des N nombres premiers de la liste, disons p_i.

$p_i|a$ et $p_i|p_1p_2p_3\ldots p_N$ car p_i est l'un des facteurs de ce produit, donc $p_i|a-p_1p_2p_3\ldots p_N$, c'est-à-dire $p_i|1$ et donc $p_i=1$, ce qui est impossible car p_i est premier.

P3) $\boxed{Critère\ de\ primalité}$

Ecrivons exactement la contraposée de (P1 bis) :

Si un entier naturel n n'est divisible par aucun des nombres premiers inférieurs ou égaux à $\sqrt{n}$ *alors n est premier.*

P4*)* $\boxed{Décomposition\ en\ facteurs\ premiers}$

Algorithme :
variables n,q entiers et une liste
n saisi par l'utilisateur, n strictement supérieur à 1
q=n
liste vide
traitement
tant que q n'est pas premier
ajouter p le plus diviseur positif de q dans la liste
affecter à q la valeur q/p
ajouter q à la liste
sortie
afficher la liste

En python, par exemple :

```
n=int(input("donner un entier strictement supérieur à 1"))
p=2
t=[]
q=n
while q!=1:
  while q%p!=0:
     p=p+1
  t.append(p)
  q=q//p
print(t)
```

ou pour un meilleur affichage

```
n=int(input("donner un entier strictement supérieur à 1"))
p=2
t=[]
q=n
while q!=1:
  while q%p!=0:
     p=p+1
  t.append(p)
  q=q//p
print(n," = ",end="")
for i in range(len(t)):
   if i<len(t)-1:
      print(t[i],"x",end="")
   else:
       print(t[i])
```

print(t)

En entrant 1250, on obtient 1250 = 2 x5 x5 x5 x5

L'algorithme se termine bien car la variable q est un entier strictement supérieur à 1 qui diminue strictement après chaque boucle.
La liste ainsi obtenue est une décomposition en facteurs premiers de n.
Les nombres premiers qui interviennent sont dans l'ordre croissant, c'est une conséquence de P1).

On admet l'unicité d'une telle décomposition dans un premier temps, elle est démontrée dans le chapitre sur le théorème de Bezout.
L'unicité est importante ; elle permet de démontrer, par exemple, qu'il n'y a pas d'autres nombres premiers que ceux qui interviennent dans cette décomposition d'un entier n, qui divisent n.
En effet, s'il existait un tel autre nombre premier p qui diviserait n, alors on aurait n=pq où q est un entier, et en décomposant q par l'algorithme précédent, on obtiendrait une autre décomposition en facteurs premiers de n.
Par conséquent, tout diviseur positif de n autre que 1, ne peut avoir dans sa décomposition en facteurs premiers, que des nombres premiers qui interviennent déjà dans celle de n.
De la même manière, on pourrait démontrer que l'exposant d'un nombre premier dans la décomposition d'un diviseur de n ne peut pas être strictement supérieur à celui qui intervient dans la décomposition de n.
Autrement dit, cette décomposition permet d'obtenir exactement tous les diviseurs positifs de n.

En prenant l'exemple de $1250=2^1x5^4$, tout diviseur positif de 1250 est de la forme 2^ix5^j où i est dans {0, 1} et j dans {0, 1, 2, 3, 4}.
Ce qui donne en tout 2x5=10 diviseurs positifs :
$2^05^0=1$
$2^05^1=5$
$2^05^2=25$
$2^05^3=125$
$2^05^4=625$
$2^15^0=2$
$2^15^1=10$
$2^15^2=50$
$2^15^3=250$
$2^15^4=1250$

Retour au sommaire

PGCD et nombres premiers entre eux
a) Définitions
Soient a et b 2 entiers.
si a=b=0, alors l'ensemble des diviseurs communs (qui divisent à la fois a et b) est $\mathbb{Z}^*$
sinon l'ensemble des diviseurs communs est fini donc admet un plus grand élément noté PGCD(a,b) et appelé plus grand diviseur commun de a et b.
Ce PGCD est donc supérieur ou égal à 1.
Remarques
R1) PGCD(0,a)=|a| si a est entier non nul
R2) si b>0, on a PGCD(a,b)=b ⇔ b|a (les deux implications sont simples à démontrer)

Lorsque PGCD(a,b)=1, on dit que a et b sont premiers entre eux ou a premier avec b.

b) Algorithme d'Euclide et conséquences
Il repose sur la propriété suivante :

Lemme d'Euclide :

Si a, b, c, d sont 4 entiers, b non nul, vérifiant a=bc+d
alors L'ensemble des diviseurs communs de a et b est le même que l'ensemble des diviseurs communs de b et d
En particulier PGCD(a,b)=PGCD(b,d)

Démonstration
si n|a et n|b alors n|a-bc or a-bc=d donc n|b et n|d
Réciproquement, si n|b et n|d alors n|bc+d or bc+d=a donc n|b et n|a

On utilise cette propriété dans la division euclidienne de a par b :
a=bq+r implique PGCD(a,b)=PGCD(b,r)

algorithme :
En python

```
a=int(input("donner un entier a"))
b=int(input("donner un entier b"))
x=a
y=b
r=x%y
while r!=0:
  print(x,"=",y,"x",x//y,"+",r)
  x=y
  y=r
  r=x%y
print(x,"=",y,"x",x//y)
print("")
print("PGCD(",a,",",b,") =",y)
```

En prenant a=420 et b=540, ce programme affiche
420 = 540 x 0 + 420
540 = 420 x 1 + 120
420 = 120 x 3 + 60
120 = 60 x 2

PGCD(420 , 540) = 60

On peut faire une version avec moins d'affichage :

```
a=int(input("donner un entier a"))
b=int(input("donner un entier b"))
x=a
y=b
r=x%y
while r!=0:
```

```
    x=y
    y=r
    r=x%y
print(y)
```

L'algorithme se termine car la variable r diminue strictement, en effet, elle contient à la fin de la boucle, le reste de la division euclidienne par la valeur de r au début de la boucle.
Si on note r_i et r_{i+1} les valeurs de r avant et après la boucle i on a r_{i+1} reste d'une division euclidienne par r_i , donc $0 \leq r_{i+1} < r_i$
De plus, d'après le lemme d'Euclide, PGCD(x,y) ne change pas, il est constant.
On a donc **PGCD(a,b)=PGCD(y,0) =y où y est le dernier reste non nul** (dernière valeur de y).
On a aussi le fait que les diviseurs communs de a et b sont exactement ceux de y et 0, c'est-à-dire de y.
Autrement dit :
E1) *conséquence 1*

$\boxed{\textit{les diviseurs communs de } a \textit{ et } b \textit{ sont exactement les diviseurs de leur } PGCD}$

En multipliant a et b par un *entier strictement positif k*
x=ka
y=kb
et en remarquant que x%y=k(a%b) car a=bq+r et $0 \leq r < |b| \Leftrightarrow ka = kbq + kr$ et $0 \leq kr < k|b|$
On obtient :
E2) *conséquence 2*

$\boxed{PGCD(ka, kb) = kPGCD(a, b)}$

E3) *conséquence 3*

Si d=PGCD(a,b) et si on note a' et b' les entiers vérifiant a=da' et b= db'
Alors a' et b' sont premiers entre eux

Démonstration
d=PGCD(a,b)=PGCD(da',db')=d.PGCD(a',b') d'après E2), et en simplifiant par d>0, on obtient PGCD(a',b')=1 et donc a' et b' sont premiers entre eux.

c) Propriétés

PP1) *Si p et p' sont deux nombres premiers distincts*
Alors p et p' sont premiers entre eux

Démonstration
Les diviseurs positifs de p sont 1 et p, et ceux ce p' sont 1 et p', comme $p \neq p'$ alors seul 1 est commun.

PP2*) Soient n un entier et p un nombre premier*
p premier avec n $\Leftrightarrow$ p ne divise pas n

Démonstration
Les seuls diviseurs positifs de p sont 1 et p, donc
soit PGCD(n,p)=1 ce qui équivaut à dire que n et p sont premiers entre eux
soit PGCD(n,p)=p ce qui équivaut à p|n d'après R2)

PP3) *Soient a, b deux entiers non nuls*
a est premier avec b ⇔ Il n'y a pas de nombres premiers qui se trouvent à la fois dans la décomposition de a et dans celle de b

En effet, un diviseur commun de a et de b ne peut avoir dans sa décomposition en facteurs premiers, que des nombres premiers qui sont à la fois dans celle de a et celle de b (voir le chapitre concernant la décomposition en facteurs premiers et l'unicité de cette décomposition)

Retour au sommaire

Théorème de Bezout et ses conséquences

a) Théorème de Bezout

Soient a et b deux entiers
a et b sont premiers entre eux⇔ il existe au moins un couple (u,v) d'entiers tel que au+bv=1

Démonstration

⇒

Comme a et b sont premiers entre eux, au moins des 2 est non nul.
Notons E, l'ensemble des entiers strictement positifs de la forme ax+by où x et y sont des entiers
Cet ensemble est un sous ensemble de $\mathbb{N}^*$ non vide car contient par exemple a^2+b^2, donc il admet un plus petit élément, noté d, qui est de la forme au+bv par définition de E.
Si on démontre que d=1, on aura démontré l'implication.
Pour démontrer que d=1, nous allons démontrer que d divise a et divise b, car alors d sera un diviseur commun de a et b et donc un diviseur de leur PGCD qui vaut 1 par hypothèse et donc d=1

Notons (q,r) le couple de la division euclidienne de a par d :
a=qd+r et 0≤**r<d**
r=a-qd=a-q(au+bv)=(1-qu)a+(-qv)b
Comme r est un reste, r≥0
si r>0, alors r∈ E, par définition de E et donc r≥d car d est le plus petit élément de E, mais cela est impossible car **r<d**, donc r=0 ce qui signifie que d|a
Et de la même manière, on démontre que d|b

⇐ (réciproque)

Soit d=PGCD(a,b), par hypothèse au+bv=1 pour un certain couple (u,v) d'entiers, mais d|a et d|b donc d|(au+bv) c'est-à-dire d|1 , et donc d=1, ce qui démontre l'implication réciproque.

b) Théorème de Gauss

Soient a, b et c trois entiers
Si a|bc et a premier avec b
Alors a|c

Démonstration
Par hypothèses, il existe un entier k tel que bc=ka, et d'après le théorème de Bezout, il existe un couple d'entiers (u,v) tel que au+bv=1
Cette dernière égalité, en multipliant les deux membres par c donne :
acu+bcv=c, et comme bc=ka, on a acu+akv=c et donc a(cu+kv)=c et comme cu+kv est un entier, on en déduit que a|c

c)Autres propriétés

P1) *Soient a, b et c trois entiers*
Si a est premier avec b et est premier avec c

Alors a est premier avec bc

Démonstration

Par hypothése et d'après le théorème de Bezout, il existe deux couples d'entiers (u,v) et (u',v') tels que au+bv=1 et au'+cv'=1

En multipliant ces deux égalités membres à membres, on obtient :

a(auu'+bvu'+cuv')+bcvv'=1 et d'après la réciproque de Bezout, on en déduit que a et bc sont premiers entre eux.

P2) *Soient a, b et c trois entiers*
Si a et b divisent c et a premier avec b
Alors ab divise c

Démonstration

Par hypothèse, il existe deux entiers k et k' tels que c=ka et c=k'b, donc ka=k'b.
a divise donc k'b et comme a est premier avec b, d'après le théorème de Gauss, a divise k'.
Il existe donc un entier k'' tel que k'=ak''.
On obtient donc c=k'b=abk'' et donc ab divise c.

P3) *Soient a, b, c et n quatre entiers, n strictement positif*
Si ac≡bc(n) et c premier avec n
Alors a≡b(n)

Démonstration

Par hypothèse, il existe un entier k tel que ac-bc=kn ou encore c(a-b)=kn.
Donc n|c(a-b), et comme c et n sont premiers entre eux, d'après le théorème de Gauss, on en déduit que n|a-b, c'est-à-dire a≡b(n).

P4) *La décomposition en facteurs premiers d'un entier est unique*

Démonstration par l'absurde

Supposons qu'un entier naturel ait deux décompositions en facteurs premiers différentes, on aurait une égalité entre deux produits de nombres premiers, qui, après simplification, donnerait $p_1p_2..p_N=q_1q_2..q_M$ où tous les facteurs sont des nombres premiers et ceux qui sont dans un membre ne se retrouvent pas dans l'autre membre.
$p_1|q_1q_2..q_M$, mais p_1 premier avec q_1 car p_1 et q_1 sont deux nombres premiers distincts, donc d'après le théorème de Gauss, $p_1|q_2..q_M$
Ainsi de suite, jusqu'à $p_1|q_M$, ce qui est absurde car p_1 et q_M sont deux nombres premiers distincts.

d) <u>Petit Théorème de Fermat</u>

Si a est premier avec p
Alors $a^{p-1}\equiv 1(p)$

Démonstration

Soit i ∈ {1,2,.., p-1} alors i est premier avec p car p est premier et p ne divise pas i (PP2)
et **donc S=1x2x..x(p-1) est premier avec p** d'après (P1)
Notons r_i le reste de la division euclidienne de ia par p où i ∈ {1,2,.., p-1}

$a\equiv r_1(p)$
$2a\equiv r_2(p)$
…
$(p-1)a\equiv r_{p-1}(p)$

D'où, en multipliant membres à membres ces p-1 congruences (C3), on obtient

$(1x2x3x…x(p-1))a^{p-1}\equiv r_1r_2…r_{p-1}(p)$
C'est-à-dire
$Sxa^{p-1}\equiv r_1r_2…r_{p-1}(p)$
Démontrons que $r_1r_2…r_{p-1}=S$, on pourra alors en déduire que $a^{p-1}\equiv 1(p)$ en appliquant (P3) **car S est premier avec p.**
Pour cela on va démontrer que les deux ensembles {1,2,…, p-1} et $\{r_1, r_2, …,r_{p-1}\}$ sont égaux.
Comme, pour tout $i \in \{1,2,.., p-1\}$, $r_i \in \{0, 1,2,.., p-1\}$, il suffit de démontrer que
1) pour tout $i \in \{1,2,.., p-1\}$, $r_i \neq 0$ et
2) pour tous i et j distincts dans {1,2,.., p-1}, $r_i \neq r_j$

Pour 1) Par l'absurde :
S'il existe $i \in \{1,2,.., p-1\}$ tel que $r_i=0$, on aurait $ia\equiv 0(p)$, et comme a est premier avec p, alors $i\equiv 0(p)$ avec (P3), c'est-à-dire p|i, ce qui est absurde car $i \in \{1,2,.., p-1\}$,

Pour 2) Par l'absurde :
S'il existe i et j distincts dans {1,2,.., p-1} tels que $r_i = r_j$, on aurait $ia\equiv ja(p)$, et comme a est premier avec p, alors, d'après P3), $i\equiv j(p)$ c'est-à-dire p|(i-j)
ce qui est absurde car $i-j \in \{-(p-1),..,-2,-1,1,2,.., p-1\}$, $(i-j\neq 0$

Retour au sommaire

PPCM

a) Définition

Soient a et b deux entiers non nuls ; si on note E l'ensemble des multiples communs de a et b, strictement positifs, cet ensemble est une partie non vide de $\mathbb{N}$, car contient par exemple |a|x|b|, donc admet un plus petit élément appelé le plus petit multiple commun de a et b et noté PPCM(a,b)

b) Propriétés

M1) *Soient a et b deux entiers strictement positifs et soit d=PGCD(a,b)*
Alors PPCM(a,b)=da'b' où a' et b' sont définis par a=da' et b=db'

(On sait déjà que a' et b' sont premiers entre eux d'après E3))
Remarque : dans le cas général, il faut prendre les valeurs absolues de a' et de b'
Démonstration
Notons E l'ensemble des multiples de da'b' et F l'ensemble des multiples communs de a et b.
Démontrons que E=F, on en déduira que PPCM(a,b)=da'b'
et aussi que les multiples communs de a et b sont exactement les multiples de leur PPCM

Soit $n \in E$, il existe k entier tel que n=kda'b', donc n=kb'a=ka'b et donc n est un multiple de a et de b, c'est-à-dire $n \in F$.

Réciproquement
Soit $n \in F$, il existe deux entiers k et k' tels que
n=ka=k'b donc kda'=k'db' et donc ka'=k'b'
On en déduit que a' divise k'b', et comme a' est premier avec b', d'après le théorème de gauss, a' divise k' et donc il existe un entier k'' tel que k'=a'k''.
On obtient alors n=k'db'=k''da'b' et donc n est un multiple de da'b', c'est-à-dire $n \in E$.

M2) *Soient a et b deux entiers*
|ab|= PGCD(a,b) PPCM(a,b)

Démonstration

Reprenons les notations de M1)

|ab|=d|a'|d|b'|=d(d|a'||b'|)=PGCD(a,b)xPPCM(a,b) d'après M1)

M3) *Soient a et b deux entiers et k un entier strictement positif*
PPCM(ka,kb)=kPPCM(a,b)

Démonstration

On a PPCM(ka,kb)xPGCD(ka,kb)=k|a|k|b|=k x PGCD(a,b) x k x PPCM(a,b) d'après M2)
=PGCD(ka,kb) x k x PPCM(a,b) d'après E2)

Donc en simplifiant par PGCD(ka,kb) qui est non nul, on obtient :
PPCM(ka,kb)=kPPCM(a,b)

M4) *Décomposition du PPCM en facteurs premiers*

De la décomposition en facteurs premiers de a et de b, on en déduit celle de leur PGCD puis celle du PPCM, en utilisant M2)

Exemple :

$a=2^3x5^2x7$

$b=2^2x3^4x7$

$PGCD(a,b)=2^2x7$ car dans la décomposition d'un diviseur commun il ne peut y avoir que 2 ou 7 comme nombres premiers, et donc le PGCD, qui est le plus grand des diviseurs communs, aura exactement 2 et 7 comme nombres premiers dans sa décomposition avec le plus grand exposant possible.

$PPCM(a,b)=2^3x3^4x5^2x7$ car en le multipliant par le PGCD, on doit retrouver $ab=2^5x3^4x5^2x7^2$

On remarque que $a'=2x5^2$ et $b'=3^4$ qui sont bien premiers entre eux car ils n'ont pas de nombres premiers communs dans leur décomposition.

Retour au sommaire

RSA

a) Principe

L'idée est de coder un message (par exemple un nombre) en un autre message (un autre nombre).
Pour cela on dispose de 2 clés publiques dont une est n.
Tout le monde peut alors coder.
Mais personne peut décoder, c'est à dire retrouver le message d'origine à partir du message codé.
Cela vient du fait que n est le produit de 2 grands nombres premiers p et q distincts.
n est donné mais pas p ni q.
Pour décoder il faudrait connaître p et q or pour de très grands nombres on ne sait pas en un temps raisonnable décomposer n en pq même avec des machines puissantes.
Par exemple en prenant n constitué de 1024 chiffres binaires soit à peu près 308 chiffres décimaux, c'est impossible actuellement.
On a pu factoriser un entier de 768 bits en 2 ans et demi avec des ressources informatiques importantes.
Maintenant reste le problème de la création de ces clés donc de génération de grands nombres premiers.
C'est là qu'interviennent les pseudo premiers ou plus exactement des nombres dont il est fort probable qu'ils soient premiers et qui sont générés rapidement.

b) Démonstration

Principe du fonctionnement du cryptage RSA.

Des nombres remarquables

1) Nombres de Fermat

Ce sont les nombres de la forme $2^{2^n}+1$, notés F_n, où n est un entier naturel.
Ils ne sont pas tous premiers, d'ailleurs on ne sait pas s'il y en a une infinité de premiers ni une infinité de non premiers.
de F_0 à F_4 premiers
de F_5 à F_{32} non premiers
F_{33} on ne sait pas encore

Si $n \neq n'$ Alors F_n *et* F_n, sont premiers entre eux (théorème de Goldbach)

La conjecture de Goldbach, pas encore démontrée et énoncé en 1742 est :
« Tout nombre entier pair supérieur à 3 peut s'écrire comme la somme de 2 nombres premiers »

Soit k entier naturel $x=2^k+1$ premier ⇒ $k=2^n$ où n est un entier naturel (réciproque fausse !)
⇒x est nombre de Fermat

Retour au sommaire

2) Nombre de Mersenne

Ce sont les nombres premiers de la forme 2^p-1 où p est premier.
On note M_k le k-ième nombre de Mersenne.
Si note $A_p=2^p-1$ alors
$M_1=A_2=3$
$M_2=A_3=7$
$M_3=A_5=31$
$M_4=A_7=127$
mais $M_5 \neq A_{11}$ car $A_{11}=2047=23x89$ donc non premier

On a aussi la propriété suivante :
2^n-1 premier⇒ n premier
Autrement dit, parmi les nombres de la forme 2^n-1 où n est un entier naturel, il y a 3 catégories :
n non premier et alors 2^n-1 n'est pas premier
n est premier et $2^n-1 = A_n$ n'est pas premier
n est premier et $2^n-1 = A_n$ est un nombre de Mersenne c'est à dire premier

Retour au sommaire

3) Nombres parfaits

Ce sont les entiers naturels qui sont égaux à la somme de leurs diviseurs propres positifs
Par exemple 6 est parfait car 6=1+2+3
où encore 2 305 843 008 139 952 128 (découvert par Leonhard Euler)

Voilà une méthode pour générer des nombres parfaits :

"Lorsque la somme d'une suite de nombres doubles les uns des autres est un nombre premier, il suffit de multiplier ce nombre par le dernier terme de cette somme pour obtenir un nombre parfait."

1+2=3 qui est premier donc 2x3=6 est parfait.
1+2+4=7 qui est premier donc 4x7=28 est parfait.
1+2+4+8=15 n'est pas premier.
1+2+4+8+16=31 est premier donc 16x31=496 est parfait.

En découle une formule qui porte aujourd'hui le nom de **Formule d'Euclide** :
$2^{p-1}(2^p - 1)$ est parfait si p et (2p - 1) sont premiers.
Actuellement, 40 nombres parfaits sont connus. Le plus grands possède 12 640 858 chiffres et est égal à :
$2^{20\,996\,010}(2^{20\,996\,011}-1)$.
Et on ne sait pas s'il y en a une infinité

Retour au sommaire

4) Nombres pseudo premiers

Un petit rappel sur le petit théorème de Fermat :
Soit p un nombre premier et a un entier premier avec p alors $a^{p-1} \equiv 1(p)$
ou encore p divise $a^{p-1}-1$
a est premier avec p quand a n'est pas un multiple de p, en particulier quand a est dans {2,3,.., p-1}

Mais attention, la réciproque est fausse !
(C'est bien dommage car sinon nous aurions eu un critère pour reconnaître si un nombre est premier.)
Les nombres qui contredisent la réciproque du petit théorème de Fermat sont les nombres de Carmichaël.
C'est-à-dire des nombres p non premiers tels que, pour tout a dans {2,3,.., p-1},
p divise $a^{p-1}-1$.
Le plus petit est 561=3x11x17.
Remarquez que la vérification risque d'être fastidieuse à cause des puissances à calculer.
Ils sont cependant rares, plus rares que les nombres premiers mais cependant il y en a une infinité (Théorème de Granville en 1994).
Il y a 245 nombres de Carmichael pour 78494 nombres premiers inférieurs à 10^6 (proportion de 3 pour 1000)

Maintenant changeons un peu la définition :
Considérons un nombre p non premier tel que p divise $a^{p-1}-1$ pour une valeur particulière de a dans {2,3,.., p-1}
(On a changé « pour tout a » par « un a particulier »
Ces nombres sont les nombres de Poulet ou a-pseudo premiers ou pseudo premiers de base a.
Par exemple 341 est le plus petit pseudo-premier de base 2.
Les nombres de Carmichaël et les nombres de Poulet sont les nombres pseudo premiers, c'est-à-dire des nombres qui ne sont pas premiers et qui « contredisent en partie » la réciproque du théorème de Fermat.
Un nombre de Carmichael est donc un pseudo premier de base a pour tout a
dans {2,3,.., p-1}.

Mais pourquoi les appelle-t-on pseudo premier ?
Prenons le problème à l'envers, c'est-à-dire considérons un entier p dont on ne sait pas s'il est premier ou pas.
Effectuons les calculs a^{p-1} -1 pour a dans {2,3,.., p-1}.

si, pour une valeur de a, p ne divise pas a^{p-1} -1 alors p n'est pas premier (c'est la contraposée du théorème de Fermat)

sinon , pour tout a dans {2,3,.., p-1}., p divise a^{p-1} -1 alors soit p est premier soit p est un nombre de Carmichaël et comme la proportion de nombres de Carmichaël par rapport aux nombres premiers est très faible, il est fort probable qu'il soit premier (99,9..% de chance)

Bien sûr il y a trop de calculs à effectuer et on pourrait alors se contenter de prendre a=2 mais dans ce cas la probabilité diminue car la proportion de nombres pseudo premiers de base 2 par rapport aux nombres premiers est plus importante.

D'où l'idée d'un compromis entre précision et calcul en prenant 4 valeurs de a ou 4 témoins:
2, 3, 5,7 (Test de Fermat)
Ce test consiste à choisir un nombre p et à effectuer les 4 calculs : 2^{p-1}-1, 3^{p-1}-1 ,5^{p-1}-1 ,7^{p-1}-1
Si p divise ces 4 nombres il y aura une forte probabilité que p soit premier. Mais ce n'est pas certain !

Les nombres de Chernik sont des nombres de la forme (6n+1)(12n+1)(18n+1) dont les 3 facteurs 6n+1 , 12n+1 , 18n+1 sont premiers .
Ce sont des nombres de Carmichaël !

Retour au sommaire

5) Nombres premiers

Il y a des livres entiers consacrés aux nombres premiers et ce n'est pas quelques paragraphes qui pourront les résumer.
Les nombres premiers bien connus : 2, 3, 5, 7,11... sont essentiels.

Du point de vue théorique :
Ce sont les briques, les atomes qui permettent de reconstituer tous les autres entiers.
En effet un nombre premier n'est pas décomposable en produit de 2 entiers autres que 1 et lui-même.
Tout entier est soit premier soit décomposable en produit d'au moins 2 nombres premiers et cette décomposition est unique (nombre composé)
Par exemple 12=2x2x3
Autrement dit tout entier est soit premier soit composé (de nombres premiers).
On comprend l'importance de ces nombres.
Il y en a une infinité et le fait qu'ils ne soient pas décomposables leur confère tout un tas de propriétés intéressantes :
Deux nombres premiers distincts sont premiers entre eux.
Un nombre premier p est premier avec tout entier qui n'est pas un multiple de p.
Un nombre premier p divise a^{p-1}-1 ($a^{p-1}\equiv 1(p)$) pour tout a dans {2,3,.., p-1}.
L'ensemble des restes modulo p muni de + et x est un corps, en particulier,
soit a dans {1,2,3,.., p-1} il existe b dans {1,2,3,.., p-1} tel que $ab\equiv 1(p)$

(Remarque : les nombres premiers entre eux interviennent dans les théorèmes
de Gauss « si a divise bc et a premier avec b alors a divise c »
et de Bezout « a et b sont premiers entre eux si et seulement si il existe au moins un couple d'entiers (u,v) tel que au+bv=1 »)

On a une assez bonne idée de la répartition des nombres premiers.
En notant $\pi(x)$, le nombre de nombres premiers inférieurs ou égaux à x on a :
$\pi(x) \sim x/\ln(x)$, quand $x \to +\infty$
Par exemple pour x=100 000 000 il y a à peu près 5 428 681 nombres premiers inférieurs à x en utilisant cette formule (il y en a en fait 5 761 455)

On a aussi ce résultat par Felgner en 1990 : $0{,}91\, n \ln(n) < p_n < 1{,}7\, n \ln(n)$ où p_n désigne le n-ième nombre premier.

Retour au sommaire

Applications

a) **Cryptage ou chiffrement**

Quand on utilise sa carte bancaire ou internet, des données sont transmises de façon sécurisée, c'est-à-dire qu'elles sont chiffrées ou cryptées.
Les protocoles utilisés finissent par un « s » de « sécurisé » comme https ou ftps.
La méthode pour sécuriser le transfert de ces données utilise, entre autres, le cryptage RSA (Rivest, Shamir, Adleman).
Des clefs publiques (n,e) sont données et connues pour crypter, mais pour décrypter il en faut une autre.
Le petit théorème de Fermat est central dans la démonstration de ce cryptage.

D'autres cryptages (affine, exponentiel, chiffrement de Hill) sont aussi des problèmes d'arithmétique.
En cryptographie, les nombres premiers sont essentiels.

b) **Contrôle d'erreur**

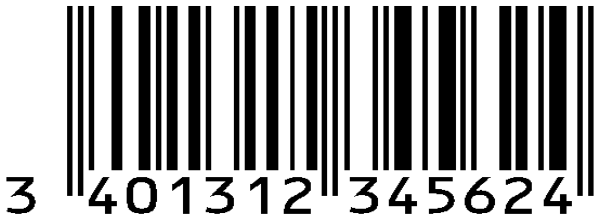
1) Clef de contrôle numéro INSEE
2) Clef RIB
3) Code barre
4) Flash code
5) Détection et correction d'erreur en informatique : CRC, code de Hamming, LRE, bit de parité

Il y a plusieurs situations où il semble judicieux de détecter, voire de corriger, des erreurs :
Lors de la saisie d'un numéro (INSEE ou compte bancaire), lors de la lecture d'un code barre ou d'un flash code, lors de la transmission de données sur un support physique.

1) et 2) Prenons par exemple un numéro de sécurité sociale qui est constitué de 13 chiffres plus 2 autres chiffres qui constituent la clef de contrôle.
Si on note A le nombre constitué des 13 premiers chiffres, et K constitué des 2 derniers chiffres (K est la clef)
K=97-r où r est le reste de la division euclidienne de A par 97.
On montre aisément que 97 divise A+K.
Si on fait une erreur de saisie, par exemple l'un des 15 chiffres est faux ou 2 chiffres consécutifs

sont permutés, alors A+K n'est plus divisible par 97.
Autrement dit, une fois les 15 chiffres saisis, la machine teste si 97 divise A+K et dans la négative un message d'erreur apparait.

3) et 4) Penons un code barre constitué d'espaces blancs et noirs avec 13 chiffres en dessous.
Les espaces blancs et noirs représentent des chiffres binaires (0 et 1).
Cette suite de chiffres binaires est le codage, selon une norme précise, de 12 chiffres décimaux qui sont écrits dessous le code barre.
Le premier chiffre se calcule autrement.
Sur ces 13 chiffres, un est une clef de contrôle calculée modulo 10.
Si on note c1c2...c13 ces 13 chiffres, c13 est la clef de contrôle et on doit avoir:
(c1+c3+...+c13) + 3(c2+c4+...+c12) divisible par 10



Ici on a un code barre EAN13 car avec 13 chiffres.
Un espace blanc (noir) correspond à un certain nombre de 0 (1).
Les grands traits donnent la largeur de l'unité.
Chaque chiffre est codé par 7 chiffres binaires avec 3 normes possibles A, B ou C.
Le premier chiffre indique la norme utilisée pour les 12 chiffres qui suivent.
Ici 3, et dans ce cas 4 est codé avec la norme A par 1132, c'est-à-dire 0100011 en binaire, ce qui correspond bien aux 4 premiers espaces (blanc noir blanc noir) après les premiers grands traits.
Le lecteur optique, doit traduire les espaces en une suite de chiffres binaires, les convertir en une donnée numérique et contrôler les erreurs.
Le premier chiffre est déterminé par le type de séquence des 6 chiffres qui suivent :
par exemple AABBBA correspond à 3.
Le lecteur reconnaît la norme utilisée donc peut trouver le premier chiffre.
Une erreur sur un chiffre peut être due à une usure ou une déformation du code barre, d'où l'intérêt du chiffre qui la détecte.
Dans ce cas, le lecteur optique ne donne aucun résultat et il faut saisir les 13 chiffres.

Le flash code est, en quelque sorte, un code barre en 2 dimensions.

Si l'on peut mémoriser un nombre de 13 chiffres dans le premier cas, ce qui parait suffisant pour une liste d'articles vendus en magasin, avec un flash code on peut mémoriser 7089 chiffres, soit beaucoup plus d'informations possibles.

5) Dans les ordinateurs et à travers les câbles qui définissent un réseau local ou internet, seuls les chiffres binaires 0 ou 1 sont utilisés ou reconnus.
Sauf que cela n'existe pas physiquement.

Chaque 0 ou 1 doit donc être transformé, par exemple en signal électromagnétique, ce signal peut être altéré et donc, à la réception des chiffres binaires peuvent être faux.
Par exemple sur le câble Ethernet, seules des trames sont véhiculées, qui contiennent en partie des données mais aussi une partie qui servira à contrôler des erreurs de transmission.
C'est le CRC, qui est calculé à partir d'une division euclidienne d'un polynôme dont les coefficients sont les chiffres binaires qui correspondent à la donnée transmise par un polynôme particulier.

C'est de l'arithmétique sur un anneau euclidien autre que $\mathbb{Z}$.
En cas d'erreur détectée, il sera alors possible, par exemple, de demander le ré-envoi de la trame.

Les autres méthodes utilisent de l'arithmétique modulo 2.
Voir ce document fait par des élèves sur les problèmes de détection et correction d'erreurs.

Comme on peut le constater sur ces premiers exemples, bien des technologies utilisées quotidiennement reposent sur nos connaissances en arithmétique.

d) Les problèmes suivants utilisent la notion de PGCD et le théorème de Bezout :

Problème chinois

Voilà un exemple classique :

« Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ? »

L'inconnue x doit vérifier:

$x \equiv 3(17)$

$x \equiv 4(11)$

$x \equiv 5(6)$

et il y a plusieurs solutions.

Le problème se généralise.

Problèmes de calendrier

On cherche le jour de la semaine d'une date donnée.

On compte le nombre de jours qui séparent cette date et une autre dont on connait le jour de la semaine et on en calcule le reste de la division euclidienne par 7.

Problèmes de coïncidence

En astronomie par exemple, on observe à des dates différentes deux astres dont on connait la période de révolution.

A quelle date pourra-t-on les observer en même temps ?

Ce problème peut se traduire par une équation de Bezout dont la résolution est classique.

On sait quand il y a des solutions ou pas et quand il y en a, on sait les trouver toutes.

Problèmes de pavage

On veut recouvrir une surface rectangulaire par des dalles carrées les plus grandes possibles.

C'est une simple utilisation du PGCD

Retour au sommaire