Divisibilité

Guesmi.B

Définition 1 *On dit qu'un entier a est un multiple d'un entier b, ou que b est un diviseur de a lorsqu'il existe un entier k tel que a=kb.*

Définition 2 *On dit qu'un entier $p \geq 2$ est premier lorsqu'il possède pour seuls diviseurs positifs 1 et lui-même.*

Division Euclidienne

Il s'agit de formaliser avec précision la bonne vieille division euclidienne, celle que vous connaissez depuis l'école primaire.

Théorème *Soit a un entier (relatif) et $b \geq 1$ un entier strictement positif. Alors il existe un couple (q ;r) unique (d'entiers) vérifiant la double condition :*

$$a = bq + r \ \ et \ 0 \leq r < b$$

Démonstration : On va prouver successivement l'existence et l'unicité de (q,r).

Existence de (q,r) : la démonstration se prête bien à discuter selon le signe de a. Le cas où $a \geq 0$ est le cas contenant l'essentiel de la démonstration ; lorsque a<0, on ne peut utiliser mot à mot la même preuve, mais on se ramène alors sans mal au cas intéressant déjà traité.

Premier cas (le cas significatif) : si $a \geq 0$.

L'idée de la démonstration est de dire que le quotient de a par b est le plus grand entier q tel que bq soit encore plus petit que a.

Introduisons donc l'ensemble $A = \{c \in IN \ tel \ que \ bc \leq a\}$. L'ensemble A est un ensemble d'entiers naturels ; il est non vide, car il contient0. Il est fini : en effet soit d un entier tel que $d \geq a + 1$; on a alors $bd \geq b(a+1) > a$, donc d n'appartient pas à A et ainsi A ne contient que des entiers inférieurs ou égaux à a.

L'ensemble A possède donc un plus grand élément q. Posons r=a-bq. La première condition sur (q,r) est alors évidemment vérifiée, c'est la seconde qui nécessite une vérification.

Comme $q \in A$, par définition de A, on a $bq \leq a$. Donc r=a-bq≥ 0.

Comme q est maximal parmi les éléments de A, q+1 n'est pas un element de A. Donc b(q+1)>a, donc r<b.

L'existence est démontrée dans ce cas.

Second cas (preuve sans imagination) : si a<0.

Posons a’=a(1-b). Comme a<0 et 1-b<0, on obtient $a' \geq 0$.

On peut donc, en appliquant le premier cas, faire la division euclidienne de a’ par b ; notons (q’,r) le couple ainsi obtenu : on a alors a’=bq’+r, avec en outre $0 \leq r < b$. En réinjectant la définition de a’, on écrit alors

a-ab=bq’+r, donc a=(a+q’)b+r. Si on pose q=a+q’, on constate qu'on a réussi la division euclidienne de a par b.

Unicité de (q,r) : soit (q_1 ;r_1) et (q_2,r_2) des couples vérifiant les deux conditions exigées dans l'énoncé du théorème.

On déduit de a=$bq_1+r_1=bq_2+r_2$ que $b(q_1-q_2)=r_1-r_2$. Ainsi, r_1-r_2 est un multiple de b.

Des conditions $r_1 \geq 0$ et $r_2<b$, on déduit que $-b<r_1-r_2$.

Des conditions $r_1<b$ et $r_2 \geq 0$, on déduit que $r_1-r_2<b$.

Ainsi r_1-r_2 est un multiple de b compris strictement entre -b et b. La seule possibilité est que r_1-r_2 soit nul. On en déduit $r_1=r_2$, puis, en allant reprendre l'égalité $b(q_1-q_2)=r_1-r_2$, que $q_1=q_2$

PGCD et PPCM

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

c divise a *et* b *si et seulement si* c *divise* d.

Demonstration

Existence de d

On note m le ppcm de a et b et on pose $d = \frac{ab}{m}$. Remarquons que ce nombre d est bien un entier : en effet, ab étant un multiple commun évident de a et b, c'est un multiple de leur ppcm. Reste à prouver qu'il convient.

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

Preuve de l'implication directe : supposons que n est un diviseur commun de a et b. On peut donc introduire deux entiers k et l tels que a=kn et b=ln. Pour travailler sur ce sur quoi nous avons des informations, à savoir les multiples de a et b, introduisons le nombre $n' = \frac{ab}{n}$. Ce nombre n' vaut aussi $\frac{a}{n}b = kb$ et $\frac{b}{n}a = la$. C'est donc un entier, et même un multiple commun de aet b. C'est donc un multiple de m. Il existe donc un entier c tel que n'=cm, soit $\frac{ab}{n} = c\frac{ab}{d}$, donc d=cn. On a bien prouvé que n divise d.

Preuve de l'implication réciproque : puisque $a = d\frac{m}{b}$ où $\frac{m}{b}$ est un entier, d divise a ; symétriquement puisque$b = d\frac{m}{a}$, d divise b. Supposons maintenant que n divise d. On voit alors aussitôt que n divise a et b.

Unicité de d

C'est exactement le même principe que pour le ppcm, on laisse donc cette partie de la démonstration en exercice (très) facile.

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.

Cette démonstration est la plus élémentaire ; elle 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 (partie significative) puis son unicité (partie très facile).

Existence de m

Introduisons l'ensemble $\mathcal{A}$ formé des entiers strictement positifs simultanément multiples de a et de b. L'ensemble $\mathcal{A}$ n'est pas vide, puisqu'il contient l'entier ab. 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 méthodiquement 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. C'est réglé.

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.

Lemme (de Gauss) *Soit a, b et c trois entiers strictement positifs. Si a divise le produit bc et si a est premier avec c, alors a divise b.*

Démonstration : Puisque a est premier avec c, le pgcd(a,c)=1 donc il existe des entiers relatifs s et t tels que sa+tc=1(identite de Bezout).(seulement 4èmaths) Multiplions cette identité par b : on obtient bsa+btc=b. Mais dans cette écriture, abs est évidemment multiple de a tandis que tbc l'est parce que bc est multiple de a. On en déduit que b, somme des deux multiples de a que sont asb et tbc, est lui-même un multiple de a.

Théorème **(énoncé approximatif)** *Tout entier $n \geq 2$ peut être écrit de façon unique comme produit de facteurs premiers*

Définition *On dit que deux entiers $a \geq 1$ et $b \geq 1$ sont premiers entre eux lorsque leur seul diviseur commun positif est 1*

Calcul du pgcd(141 , 24)

Voici les divisions euclidiennes successives et leurs conséquences en termes de pgcd.

(1) $141 = 5 \times 24 + 21$ $\qquad$ $\mathrm{pgcd}(141, 24) = \mathrm{pgcd}(24, 21)$

(2) $24 = 1 \times 21 + 3$ $\qquad$ $\mathrm{pgcd}(24, 21) = \mathrm{pgcd}(21, 3)$

(3) $21 = 7 \times 3 + 0$ $\qquad$ $\mathrm{pgcd}(21, 3) = \mathrm{pgcd}(3, 0) = 3$

(dernier reste non nul)

LES NOMBRES DE FERMAT

Fermat croyait qu'en ajoutant 1à ces puissances de 2,
on obtenait toujours des nombres premiers
Or, seuls les cinq du début sont premiers (a ce moment)

Nombre de Fermat $F_n = 2^{2^n} + 1 = D_n + 1 \; avec \; D_n = 2^{2^n}$
$D_n^2 = 2^{2^n} . 2^{2^n}$
$= 2^{2^n + 2^n}$
$= 2^{2.2^n}$
$= 2^{2^{n+1}}$
$= D_{n+1}$
D'où
$F_{n+1} = D_{n+1} + 1$
$= D_n^2 + 1$
Or $D_n = F_n - 1$
donc $F_{n+1} = (F_n - 1)^2 + 1$ (1)

exercice
montrer que $\forall n \geq 2 \, , F_n \; se \; termine \; par \; 7$
Exercice
Montrer que $F_0 . F_1 . F_2 \dots \dots . F_{n-1} = F_n - 2$
Exercice corrige
on a montrer que (1) $F_n = (F_{n-1} - 1)^2 + 1$
donc $F_n = F_{n-1}^2 - 2F_{n-1} + 2$
$= F_{n-1}^2 - 2(F_{n-2} - 1)^2$
Et donc par itération
$F_n = F_0 . F_1 . F_2 \dots \dots \dots . F_{n-1} + 2$
$= F_{n-1} + 2^{n-1} F_0 . F_1 \dots \dots . F_{n-2}$
remarque
F_5 n'est pas premier
F_5=4294967297 est divisible par 641

Nombres de Mersene
Sont les nombres de la forme $M_p=2^p-1$
Propriete

Soit a un entier naturel.

Soit n un entier strictement supérieur à 1.

On a alors :

a^n - 1 premier $\Rightarrow$ (a = 2 et n est premier)

demonstration

Soit a un entier naturel.

Soit n un entier strictement supérieur à 1.

On a a^n - 1 premier.

Nous allons tout d'abord montrer qu'il vient alors forcément a = 2, puis nous démontrerons que si 2n - 1 est premier, alors n est premier.

On voit tout d'abord que a ≠ 0 et a ≠ 1 car -1 et 0 ne sont pas premiers.

Comme a ≠ 1, en appliquant la formule sur la somme partielle d'une série géométrique, il vient :

$a^n - 1$ =(a-1)$(a^0 + a^1 + a^2 + \cdots \ldots\ldots + a^{n-1})$

Comme a^n - 1 est premier par hypothèse, l'un des deux facteurs vaut 1 ou -1.

Examinons chaque possibilité :

$(a^0 + a^1 + \cdots \ldots\ldots + a^{n-1} = -1 \Rightarrow$ a < 0, ce qui est absurde.

$(a^0 + a^1 + \cdots \ldots\ldots + a^{n-1}$ = 1 $\Rightarrow$ a = 0, ce qui est absurde.

(a - 1) = -1 $\Rightarrow$ a = 0, ce qui est absurde.

(a - 1) = 1 $\Rightarrow$ a = 2.

Il vient donc, comme unique solution, a = 2.

On a donc $2^n - 1$ qui est premier; montrons qu'alors n est premier.

Supposons que n soit un nombre composé; il vient alors

$\exists$ (k,h) $\in$ (IN-{1})² / n = k.h

On peut, ici encore, appliquer la formule sur la somme partielle d'une série géométrique :

$2^n - 1 = 2^{k^h} - 1 = (2^k - 1)((2^{k^0} + (2^k)^1 + (2^k)^2 + \cdots \ldots\ldots\ldots + (2^k)^{h-1})$

Comme $2^n - 1$ est premier, l'un des deux facteurs vaut 1 ou -1.

Le cas -1 étant éliminé car les deux facteurs sont positifs, il reste

Soit $(2^k$ - 1) = 1 et alors k = 1, ce qui est absurde par hypothèse.

Soit $((2^k)^0 + (2^k)^1 + \cdots \ldots\ldots + (2^k)^{h-1}$=1 et alors h = 1, ce qui est aussi absurde.

On aboutit à une absurdité dans tous les cas, donc le nombre n ne peut être composé

NOMBRES PARFAITS

definition

nϵIN ,on dit que n est parfait si n est égale à la somme de ses propres diviseurs

EXEMPLES :
6 ;28 ;496 ;8128 ;33550336 ;8589869056 ;137438691328 ;2305843008139952128 ;…….

On remarque que tous ces nombres se terminent par 6 ou 8

Propriete

Soit $M_k = 2^k - 1$ et N=$2^{k-1}M_k$;$k \geq 2$

Si M_k *est premier alors N est parfait*

Demonstation

Les diviseur de N sont ceux de 2^{k-1} et de M_k
D_N=les diviseurs de 2^{k-1}+les memes diviseurs x M_k (car M_k est premier)
Posons $\sigma(n)$ =la somme des diviseurs de N
Donc $\sigma(n) = n + n = 2n$
Soit n=$2^{k-1}M_k$ alors 2n=2^kM_k
Les diviseur de sont les diviseurs de 2^{k-1} et de M_k(premier)
Alors les diviseurs de n sont 2^0 ;2^1 ;2^2 ;…… ;2^{k-1} ;1xM_k ;2xM_k ;2^2xM_k ;…… ;2^{k-1}xM_k
Donc $\sigma(n) = (1 + 2 + 2^2 + \cdots \ldots \ldots + 2^{k-1})(1 + M_k)$
$= \sigma(2^{k-1}).\sigma(M_k)$
Calculons $\sigma(2^{k-1}) = 1 + 2 + 2^2 + \cdots \ldots \ldots + 2^{k-1}$
$\frac{2^k-1}{2-1} = 2^k - 1$
$\sigma(M_k) = 1 + M_k$
=1+2^k-1

=2^k

Alors $\sigma(n) = 2^k(2^k - 1)$

$= 22^{k-1}(2^k - 1)$
=2n D'où n est parfait

Les nombres premiers

Définitions

1. Un **nombre premier** n'a que deux facteurs : 1 et lui-même.
2. Un **nombre composé** a plus de deux facteurs.
3. **Le nombre 1** n'est ni un nombre premier, ni un nombre composé

Théorème : Il existe une infinité de nombre premiers

Démonstration :
Supposons le contraire, c'est à dire qu'il existe un nombre fini de nombre premiers disons p1, p2,...., pk.

Alors considérons le nombre N = ($p_1 \times p_2 \times ... \times p_k$) + 1.
Si N est premier, alors on a trouvé un nombre premier plus grand que pk, ce qui contredit l'affirmation.

Sinon, N est composé, alors N est divisible par un nombre premier p qui est forcement un des nombres $p_1, p_2, ..., p_k$ (puisque ce sont les seuls).
De ce fait, il existe un premier noté pi tel que pi divise N = ($p_1 \times p_2 \times ... \times p_k$) + 1.
Or cela implique que pi divise 1, et donc que $p_i = 1$ ce qui est impossible.

Remarque : Pour être précis, le fait que pi divise N et le produit ($p_1 \times p_2 \times ... \times p_k$) implique que :
N= p1 × a et que (p1 × p2 × ... × pk) = p1 × b et donc que p1 × (a - b) = 1 soit p1 divise 1

EXERCICES

EXERCICE1

Trouver les couples (a , b) d'entiers naturels tels que $0 < a < b$ dont le PGCD d et le PPCM m vérifient
$2m + 3d = 78$ et tels que a ne soit pas un diviseur de b.
Correction

On peut commencer par remarquer que d est $\leq$ m et sont tous deux >0.
Donc, s'ils vérifie $2m + 3d = 78$ alors on doit avoir $d < 27$.
Si on pose a' et b' définis par : $a = a'.d$ et $b = b'.d$, on sait que,d étant le PGCD de a et b alors a' et b' sont premiers entre eux.
Comme PGCD(a,b).PPCM(a,b) = $a.b$, on en déduit que :
$m = a'.b'.d$
L'équation peut alors s'écrire: $d(2a'.b' + 3) = 78$.
Comme $(2a'.b' +3)$ est impair, d est pair et doit être un diviseur de 78 inférieur à 27.
Donc, d = 2 ou 6.

Si $d = 2$ alors $(2a'.b' + 3) = 39$ et $a'.b' = 18$.
Comme a' et b' sont premiers entre eux, on a:
(a' = 1 et b' = 18) ou (a' = 2 et b' = 9).
D'où (a = 2 et b = 36) ou (a' = 4 et b' = 18) (on a $a < b$).
Comme a ne doit pas diviser b, la première solution n'est pas envisageable.
Si $d = 6$ alors $(2a'.b' + 3) = 13$ et $a'.b' = 5$.
D'où a = 6 et b = 30. Mais a ne doit pas diviser b donc cette solution n'est pas acceptable.

Seule solution {(4 , 18)}

EXERCICE2

Déterminer les paires d'entiers naturels {a,b} vérifiant: $m - 18d = 791$
où m est le PPCM et d le PGCD des nombres a et b

Correction

a' et b' sont définis par : $a = a'.d$ et $b = b'.d$
On peut toujours supposer que $a \leq b$.

On sait que *a'* et *b'* sont premiers entre eux.
On sait aussi que $m = d.a'.b'$
Alors, $d(a'.b' - 18) = 791$.
d est donc un diviseur de 791. La décomposition de 791 en facteurs premiers est : 791 = 7x133. D'où 4 cas possibles:

- $d = 1$: alors $a'b' = 809$. Comme 809 est premier, on a
  $a' = 1$ et $b' = 809$ d'où une solution : $\{a,b\} = \{1 , 809\}$
- $d = 7$: alors $a'b' = 131$. Ce nombre est aussi premier, on a donc: $a' = 1$ et $b' = 131$ d'où la solution $\{7 , 917\}$
- $d = 113$: alors $a'b' = 25$.
  Comme *a'* et *b'* sont premiers entre eux, on a:
  $a' = 1$ et $b' = 25$ d'où la solution $\{113 , 2828\}$
- $d = 791$: alors $a'b' = 19$. Nombre premier donc
  $a' = 1$ et $b' = 19$ d'où la solution $\{791 , 15029\}$

Conclusion:
Les paires $\{a,b\}$ solutions sont :
$\{1 , 809\}$, $\{7 , 917\}$, $\{113 , 2828\}$, $\{791 , 15029\}$

Exercice3

Déterminer tous les couples (a,b) d'entiers naturels tels que
$\text{PGCD}(a,b) + \text{PPCM}(a,b) = b + 9$

Correction

Posons $d = \text{PGCD}(a,b)$ et $m = \text{PPCM}(a,b)$.
On sait alors que $d.m = a.b$
Comme *d* est un diviseur de *b* et de *m*, la relation : $d + m = b + 9$ implique que *d* doit être aussi un diviseur de 9.
Les valeurs possibles de *d* sont donc : 1 ou 3 ou 9.

- **Si *d* = 1.**
  Dans ce cas, *a* et *b* sont premiers entre eux.
  La relation s'écrit : $1 + a.b = b + 9$ ou encore : $b(a - 1) = 8$.
  On obtient alors :
  $b = 1$ et $a - 1 = 8$ donc $a = 9$. Le couple (9,1) est solution
  OU
  $b = 2$ et $a - 1 = 4$ donc $a = 5$. Le couple (5,2) est solution.
  OU
  $b = 4$ et $a - 1 = 2$ donc $a = 3$. Le couple (3,4) est solution.
  OU
  $b = 8$ et $a - 1 = 1$ donc $a = 2$. Non solution car non-premiers entre eux.
- **Si *d* = 3.**
  Dans ce cas la relation s'écrit, comme $m = (ab / d)$:
  $9 + a.b = 3b + 27$ ou encore $b(a - 3) = 18$.
  Comme *b* doit être un multiple de $d = 3$, les valeurs possibles de *b* sont alors: 3 ou 6 ou 9 ou 18. D'où les cas:
  $b = 3$ et $a - 3 = 6$ donc $a = 9$. Le couple (9,3) est solution.
  $b = 6$ et $a - 3 = 3$ donc $a = 6$. Non solution car leur PGCD n'est pas 3.
  $b = 9$ et $a - 3 = 2$ donc $a = 5$. Non solution car leur PGCD n'est pas 3.
  $b = 18$ et $a - 3 = 1$ donc $a = 4$. Non solution car leur PGCD n'est pas 3.
- **Si *d* = 9.**
  Dans ce cas, comme $m = ab / d$, la relation s'écrit :

$81 + ab = 9b + 81$ ou encore $ab = 9b$.
Si b est non nul, alors $a = 9$.
Les solutions obtenues sont alors de la forme $(9 , 9k)$ k est un entier naturel nul quelconque (car b est divisible par 9).
Si $b = 0$ alors a est quelconque.
Mais comme PGCD(a, 0) = a et PPCM(a , 0) = 0, la relation s'écrit dans ce cas : $a + 0 = 0 + 9$ **donc $a = 9$ et le coule (9 , 0) est solution.**

Conclusion:
L'ensemble des couples d'entiers naturels (a , b) vérifiant :

PGCD(a , b) + PPCM(a , b) = b + 9

est formé des éléments :
(9 , 1) , (5 , 2) , (3 , 4) , (9 , 3) , (9 , 9k) où k est un entier naturel

Exercice4

Trouver les couples d'entiers naturels (a,b) vérifiant le système:

$$\begin{cases} a+b=651 \\ ppcm(a,b)=108pgcd(a,b) \end{cases}$$

Correction

On cherche tous les couples d'entiers (a , b) vérifiant :

a + b = 651 et PPCM(a , b) = 108.PGCD(a , b).

Posons, comme d'habitude, m = PPCM(a , b) et d = PGCD(a , b).
On sait que $a.b = m.d$.

Première remarque:
Comme $a + b = 651$ et que d est un diviseur de a et b, d est aussi un diviseur de 651. Or , la décomposition de 651 en facteurs premiers est :651 = 3 * 7 * 31 .
Les diviseurs de 651 sont donc : 1 - 3 - 7 - 31 - 21 - 93 - 217 - 651.

Deuxième remarque:
En multipliant par d dans la relation : PPCM(a , b) = 108.PGCD(a , b) , on peut alors écrire que le couple (a , b) doit vérifier :

$$a + b = 651 = S \quad \text{et} \quad a.b = 108.d^2 = P \quad .$$

a et b doivent donc être les solutions de l'équation du second degré :

$$X^2 - S.X + P = 0 \quad \text{ou encore} \quad X^2 - 651.X + 108.d^2 = 0$$

Le discriminant de cette équation est : $\Delta = 651^2 - 432.d^2$.
En fonction de d les valeurs possibles de a et b sont alors, en utlisant l'expression des racines d'une équation du second degré en fonction du discriminant:

$$a = \frac{651 - \sqrt{651^2 - 432d^2}}{2} \quad et \quad b = \frac{651 + \sqrt{651^2 - 432d^2}}{2}$$

Mais comme d doit être un diviseur de 651 et que l'existence de ces racines suppose que le discriminant soit positif, les seuls cas à étudier sont :

d = 1 ou 3 ou 7 ou 21 ou 31.

- Pour d = 1 ou 3 ou 7 , les valeurs a et b obtenues ne sont pas entières.
- Pour d = 21, on obtient a = 84 et b = 567.

- Pour $d = 31$, on obtient $a = 279$ et $b = 372$.

Il ne reste plus qu'à tester ces éventuelles solutions:

- **Pour *a* = 84 et *b* = 567** , on a :
  PGCD(84 , 567) = 21 et PPCM(84 , 567) = 2268 = 108 x 21.
  Donc (84 , 567) est une solution, et par symétrie, on a aussi (567 , 84).

- **Pour *a* = 279 et *b* = 567** , on a :
  PGCD(279 , 372) = 93 (et non 31 comme prévu!!!) et
  PPCM(279 , 372) = 1116 qui n'est pas égal à 108x93.
  Ce n'est pas une solution.

Conclusion:
Les seuls couples vérifiant a + b = 651 et PPCM(a , b) = 108.PGCD(a , b) sont (84 , 567) et (567 , 84)

Exercice5

Déterminer tous les couples d'entiers naturels (a,b) tels que PGCD(a,b) = 10 et PPCM(a,b) = 100

EXERCICES