

# Mathématiques discrètes. C4 - Théorie des nombres.

16 février 2011

Contrôle continu sur les graphes : le 23 mars, 1 seul document autorisé : memento-graphes.pdf sur <http://www.lacl.fr/~matran/maths/>  
Deuxième partie du cours : nombres premiers, PGCD, PPCM, congruence, cryptographie, série génératrice.

## 1 Nombres premiers

**Notation.** Soient  $n$ ,  $d$  et  $q$  trois nombres naturels t.q.  $n = d \times q$ . On dit que  $d$  divise  $n$ ,  $d$  est un diviseur de  $n$ ,  $n$  est un multiple de  $d$  et  $n$  est divisible par  $d$ . Et on note  $d|n$ .

**Définition.** Un nombre naturel  $n$  est **premier** s'il admet exactement deux diviseurs 1 et  $n$ . Sinon et si  $n > 1$ , il est dit **composé**.

Désignons par  $\mathcal{P}$  l'ensemble de tous nombres premiers :  $\mathcal{P} = \{2, 3, 5, 7, \dots\}$   
Remarquons que  $1 \notin \mathcal{P}$ . De plus, 0 et 1 ne sont ni premiers ni composés.

**Théorème.** Il existe une infinité de nombres premiers. (second théorème d'Euclide)

Démonstration en TD. Indication. On pourra raisonner par l'absurde.

**Proposition.** Pour tout entier  $n \geq 2$ , on a

1.  $n$  est composé ssi il admet un diviseur  $d$  vérifiant  $1 < d < n$ .
2. le nombre  $n! + m$  est un entier composé pour tout  $m$  vérifiant  $2 \leq m \leq n$ .
3. le plus petit diviseur de  $n$  strictement supérieur à 1 est un nombre premier.

**Preuve.** ...

**Corollaire.** Tout entier  $n > 1$  admet au moins un diviseur premier.

**Preuve.** Une conséquence directe de la proposition précédente.

**Lemme d'Euclide.** Soient  $p$  un nombre premier,  $a$  et  $b$  deux nombres naturels. Alors  $p$  divise  $ab$  ssi  $p$  divise  $a$  ou  $p$  divise  $b$ .

**Preuve.** On admet ce résultat sans démonstration.

## 2 Décomposition en facteurs premiers

### Existence d'une décomposition

**Proposition.** Pour tout entier naturel non nul  $n$ , il existe une suite  $(v_p)_{p \in \mathcal{P}}$  d'entiers naturels nuls sauf un nombre fini d'entre eux vérifiant

$$n = \prod_{p \in \mathcal{P}} p^{v_p} = 2^{v_2} \times 3^{v_3} \times 5^{v_5} \times \dots$$

Cette écriture s'appelle la **décomposition en facteurs premiers** de l'entier  $n$ . La suite  $\{v_p\}$  est encore notée  $\{v_p(n)\}$ .

**Exemple.** Décomposer 504 en facteurs premiers.

$$504 = 2^3 \times 3^2 \times 7.$$

On peut écrire :

$$504 = 2^3 \times 3^2 \times 5^0 \times 7^1 \times 11^0 \times \dots$$

Et on a

$$v_2(504) = 3, \quad v_3(504) = 2, \quad v_5(504) = 0, \quad v_7(504) = 1 \dots$$

En général, on peut décomposer  $n$  en facteurs premiers de la façon récursive :

Etape 1. Si  $n = 1$ , tous les exposants sont nuls - Fin. Sinon, trouver  $p$  le plus petit diviseur strictement supérieur à 1 de  $n$ . On sait que  $p$  est un nombre premier.

Etape 2. On écrit  $n = p \times n/p$  et on répète l'étape 1 pour décomposer le nombre  $n/p$  en facteurs premiers.

**Remarque.** On n'a pas défini la décomposition en facteurs premiers de 0. Par convention, on dit parfois que

$$v_p(0) = \infty \forall p.$$

### Unicité de la décomposition

**Proposition.** Pour tout entier naturel  $n$ , la décomposition en facteurs premiers est unique. **Preuve.** Exercice.

**Corollaire.** Pour tout entier naturel de la forme  $n = m^k$ , les exposants  $v_p$  dans sa décomposition en facteurs premiers sont des multiples de  $k$ . **Preuve.** Une conséquence de la proposition précédente.

## 3 PGCD et PPCM de deux entiers

### 3.1 Diviseurs d'un entier

**Théorème.** Pour tout couple  $(a, b)$  d'entiers naturels de décompositions en facteurs premiers

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \text{ et } b = \prod_{p \in \mathcal{P}} p^{\beta_p},$$

une CNS pour que  $b$  divise  $a$  est que chaque exposant  $\beta_p$  dans  $b$  soit inférieur ou égal à l'exposant correspondant  $\alpha_p$  dans  $a$ .

**Preuve.** CN et CS.

**Notation.** On note  $div(a)$  l'ensemble des diviseurs de  $a$ .

**Exemple.** On se donne la décomposition en facteurs premiers de 5120 :

$$5120 = 2^{10} \times 5$$

Trouver  $div(5120)$  l'ensemble des diviseurs de 5120 et la somme de ses éléments.

Il y en a  $(10+1)(1+1) = 22$  diviseurs :  $2^i 5^j$  où  $0 \leq i \leq 10$  et  $0 \leq j \leq 1$ . La somme de tous ces diviseurs est donnée par

$$\begin{aligned} S &= \sum_{i=0}^{10} \sum_{j=0}^1 2^i 5^j \\ &= \sum_{i=0}^{10} 2^i \sum_{j=0}^1 5^j \\ &= \frac{2^{11} - 1}{2 - 1} \times \frac{5^2 - 1}{5 - 1}. \end{aligned}$$

**Généralisation.** Soit  $n$  un entier strictement supérieur à 1, de décomposition en facteurs premiers

$$n = \prod_{p \in \mathcal{P}} p^{v_p}.$$

L'ensemble  $\text{div}(n)$  est donné par

$$\text{div}(n) = \left\{ \prod_{p \in \mathcal{P}} p^{v'_p} \mid 0 \leq v'_p \leq v_p \right\}$$

Le cardinal de cet ensemble est

$$N = \prod_{p \in \mathcal{P}} (v_p + 1)$$

et la somme de ses éléments est

$$S = \prod_{p \in \mathcal{P}} \frac{p^{v_p+1} - 1}{p - 1}$$

**Proposition.** Si  $n^k$  divise  $m^k$  alors  $n$  divise  $m$ .

**Preuve....**

### 3.2 Diviseurs communs et PGCD.

**Théorème.** Soient  $a$  et  $b$  deux entiers naturels dont les décompositions en facteurs premiers sont

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \text{ et } b = \prod_{p \in \mathcal{P}} p^{\beta_p}.$$

L'ensemble de leurs diviseurs communs est  $div(d)$  où

$$d = \prod p^{\delta_p} \text{ avec } \delta_p = \min(\alpha_p, \beta_p) \quad \forall p.$$

**Preuve.**  $c$  est un diviseur commun de  $a$  et  $b$  ssi...

**Terminologie et notation.** On appelle  $d$  le PGCD de  $a$  et  $b$ , et on note  $d = PGCD(a, b)$ .

Si  $PGCD(a, b) = 1$ , on dit que  $a$  et  $b$  sont premiers entre eux.

Remarquons que cet entier  $d$  est, au sens propre, le plus grand diviseur commun de  $a$  et de  $b$ .

Cette définition de PGCD ne s'applique que pour les entiers strictement positifs et ne s'applique pas pour 0 car 0 n'admet pas décomposition en facteurs premiers. On présente alors une extension pour 0.

**2eme définition de PGCD.** Soient  $a$  et  $b$  deux entiers naturels. Le  $PGCD(a, b)$  est le plus grand entier satisfaisant  $d|a$  et  $d|b$ .

Par convention,  $PGCD(0, 0) = \infty$ .

**Propriété.** Si  $d = PGCD(a, b)$ , on a

$$div(a) \cap div(b) = div(d).$$

**Preuve.**

**Théorème.** Soient  $a$  et  $b$  deux entiers naturels. On a

$$PGCD(a, b) = PGCD(b, a), \quad PGCD(a, a) = PGCD(a, 0) = a, \quad PGCD(a, 1) = 1$$

et

$$PGCD(a, b)|a, \quad PGCD(a, b)|b.$$

**Théorème.** Soient  $a > b$  deux entiers naturels. On a

$$PGCD(a - b, b) = PGCD(a, b).$$

**Preuve.** On m.q.  $d$  est un diviseur commun de  $a$  et  $b$  ssi il est un diviseur commun de  $a - b$  et  $b$ . Cela signifie que  $div(a - b) \cap div(b) = div(a) \cap div(b)$  et le résultat.

**Théorème.** Soient  $a$  et  $b$  deux entiers naturels, les relations suivantes sont équivalentes

1.  $a$  divise  $b$
2.  $\text{div}(a) \subset \text{div}(b)$
3.  $\text{PGCD}(a, b) = a$ .

**Preuve.**  $1- > 2- > 3- > 1$

**Corollaire.** Pour tout entier  $a$  et tout nombre premier  $p$ ,  $\text{PGCD}(a, p) = p$  ou 1, selon que  $p$  divise  $a$  ou non.

**Preuve.** ...

**Définition.** Soient  $a$  et  $b$  deux entiers naturels, on dit que  $a$  et  $b$  sont **premiers entre eux**, ou **étrangers**, si

$$\text{PGCD}(a, b) = 1.$$

**Propriété.** Soient

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \text{ et } b = \prod_{p \in \mathcal{P}} p^{\beta_p}.$$

Alors  $a$  et  $b$  sont premiers entre eux ssi  $\min(\alpha_p, \beta_p) = 0$  pour tout  $p \in \mathcal{P}$ .

**Preuve.** Définition du PGCD.

**Corollaire.** On a

1. Tout nombre premier  $p$  est premier avec tout entier qu'il ne divise pas.
2. Deux nombres premiers distincts sont premiers entre eux.
3. Pour  $(a, b, n, m)$  t.q.

$$\text{PGCD}(a, b) = 1, n \geq 0, m \geq 0,$$

$$\text{on a } \text{PGCD}(a^n, b^m) = 1.$$

**Preuve....**

**Proposition.** Soient  $a, b, n : \text{PGCD}(a, b) = 1$ . Si le produit  $ab$  est de la forme  $c^n$ , il existe deux entiers  $u$  et  $v$  premiers entre eux t.q.  $a = u^n$  et  $b = v^n$ .

**Preuve.** Considérons les décompositions en facteurs premiers de  $a, b, c, \dots$

**Théorème.** Soient  $a, b, d$  trois entiers naturels. Alors  $d = PGCD(a, b)$  ssi l'on peut écrire  $a$  et  $b$  sous la forme

$$\begin{cases} a = da' \\ b = db' \end{cases}$$

t.q.  $a'$  et  $b'$  soient premiers entre eux.

**Preuve.** Définition du PGCD.

**Corollaire.** Pour tous entiers naturels  $a, b, c$ , on a

$$PGCD(ac, bc) = c \times PGCD(a, b).$$

**Preuve.** Conséquence du théorème précédent.

### 3.2.1 Déterminer PGCD de deux nombres

**Proposition.** Soient  $a, b \in \mathbb{N}, a \geq b$ . On a

$$PGCD(a, b) = PGCD(b, a - b)$$

**Algorithme des différences.** L'égalité précédente ramène le calcul du PGCD du couple  $(a, b)$  à celui du couple  $(b, a - b)$ .

**Exemple.** Trouver  $PGCD(6, 21)$ .

$a$	$b$	$ a - b $
6	21	15
6	15	9
6	9	3
6	3	3
3	3	

**L'algorithme d'Euclide** est basé sur la proposition suivante.

**Proposition.** Soient  $a, b \in \mathbb{N}, 1 \leq b \leq a$ . Soient  $q$  et  $r$  respectivement le quotient et le reste dans la division euclidienne de  $a$  par  $b$  :  $a = bq + r$ ,  $0 \leq r \leq b - 1$ . Alors

$$PGCD(a, b) = PGCD(b, r).$$

**Exemple.** Trouver  $PGCD(21, 6)$ .

$a$	$b$	$q$	$r$
21	6	3	3
6	3	2	0
3	0		

## 4 Multiples communs et PPCM.

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

$a\mathbb{N}^* = \{a, 2a, 3a, \dots\}$  l'ensemble des multiples de  $a$ ,

$b\mathbb{N}^* = \{b, 2b, 3b, \dots\}$  l'ensemble des multiples de  $b$ ,

On s'intéresse à  $a\mathbb{N}^* \cap b\mathbb{N}^*$  l'ensemble des multiples communs de  $a$  et  $b$ .

**Proposition.** Soient

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p}$$

et

$$b = \prod_{p \in \mathcal{P}} p^{\beta_p}$$

.

1. L'ensemble  $a\mathbb{N}^*$  des multiples de  $a$  est l'ensemble des entiers  $c$  qui s'écrivent sous la forme

$$c = \prod_{p \in \mathcal{P}} p^{\gamma_p}$$

avec  $\gamma_p \geq \alpha_p$  pour tout  $p$ .

2. L'ensemble  $a\mathbb{N}^* \cap b\mathbb{N}^*$  des multiples communs de  $a$  et  $b$  est l'ensemble des entiers  $c$  qui s'écrivent sous la forme

$$c = \prod_{p \in \mathcal{P}} p^{\gamma_p}$$

avec  $\gamma_p \geq \max(\alpha_p, \beta_p)$  pour tout  $p$ .

**Définition.** On appelle le plus petit commun multiple de  $a$  et  $b$ , et l'on note  $PPCM(a, b)$  l'entier

$$m = \prod_{p \in \mathcal{P}} p^{\max(\alpha_p, \beta_p)}.$$



**Exemple.** Trouver  $PPCM(120, 56)$ .

$120 = 2^3 \times 3 \times 5$  et  $56 = 2^3 \times 7$ . Alors

$$PPCM(120, 56) = 2^3 \times 3 \times 5 \times 7 = 840.$$

**Théorème.** L'ensemble des multiples communs de  $a$  et  $b$  est l'ensemble des multiples de leur PPCM  $m$  :

$$a\mathbb{N}^* \cap b\mathbb{N}^* = m\mathbb{N}^*.$$

**Propriété.** Pour tous  $a, b \in \mathbb{N}^*$ , on a

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

**Preuve.** Considérons les décompositions en facteurs premiers.

**Corollaire.** Si  $a$  et  $b$  sont premiers entre eux,  $PPCM(a, b) = ab$ .

**Corollaire.** Soient  $a, b \in \mathbb{N}^*$ ,  $d$  et  $m$  respectivement leur PGCD et PPCM. Il existe  $a'$  et  $b'$  t.q.

$$\begin{cases} a = da' \\ b = db' \\ PGCD(a', b') = 1 \\ m = a'b'd. \end{cases}$$

**Proposition.** Pour tous  $a, b \in \mathbb{N}^*$ , on a

$$PPCM(a, b) = PPCM(b, a) \quad PPCM(a, a) = PPCM(a, 1) = a,$$

et

$$PPCM(a, b) | ab \quad a | PPCM(a, b) \quad b | PPCM(a, b).$$

**Théorème.** Soient  $a, b \in \mathbb{N}^*$ .  $a$  divise  $b$  ssi  $PPCM(a, b) = b$ .

**Proposition.** Pour tous  $a, p \in \mathbb{N}^*$  t.q.  $p$  est un nombre premier,  $PPCM(a, p)$  est égal à  $a$  ou à  $ap$ , selon que  $p$  divise  $a$  ou non.

**Proposition.** Pour tous  $a, b, c \in \mathbb{N}^*$ , on a

$$PPCM(ac, bc) = cPPCM(a, b).$$

**Proposition.** Pour tous  $a, b \in \mathbb{N}^*$  et  $M$  un multiple commun de  $a$  et  $b$ , on dispose de l'égalité

$$PGCD(\frac{M}{a}, \frac{M}{b}) = \frac{M}{PPCM(a, b)}.$$