Les nombres premiers

(Spécialité Maths)
Terminale S

Dernière mise à jour : Mercredi 23 Avril 2008

Vincent OBATON, Enseignant au lycée Stendhal de Grenoble (Année 2007-2008)

J'aimais et j'aime encore les mathématiques pour elles-mêmes comme n'admettant pas l'hypocrisie et le vague, mes deux bêtes d'aversion.

Stendhal

Table des matières

1 Définition **4**

2 Décomposition des entiers en produits de facteurs premiers **5**

3 Petit théorème de Fermat **6**

4 Applications **7**
4.1 Le codage RSA 7

1 Définition

Définition 1 :

> On dit qu'un nombre entier naturel st premier s'il admet exactement deux diviseurs entiers naturels distincts : 1 et lui même.

Notation :
Dans la suite de ce cours, on note P l'ensemble des nombres premiers.

Théorème 1 :

> Tout entier naturel n distinct de 1 admet au moins un diviseur premier.

Démonstration :

- Si $n = 0$ alors le théorème est vrai car 2 divise 0.
- On note n un entier naturel ≥ 2 et $D_n = \{p \in \mathbb{N}, p \neq 1 \text{ tel que } p|n\}$
  $n \in \mathbb{D}_n$ donc D_n n'est pas vide.
  D_n admet un plus petit élément que l'on note p_1.
  Démontrons que p_1 est premier.
  On note d un diviseur entier naturel $\neq 1$ de p_1. Il en existe au moins un p_1 lui même.
  On a donc $d|p_1$ et $p_1|n$ donc $d|n$ or p_1 est le plus petit diviseur de n donc $\boxed{d \geq p_1}$
  De plus comme $d|p_1$ alors $\boxed{d \leq p_1}$
  D'après les deux remarques précédentes, $d = p_1$.
  p_1 admet donc d et 1 comme seul diviseur donc $p_1 \in P$

Théorème 2 :

> L'ensemble P est un ensemble infini.

Démonstration :
Démontrons ce théorème par l'absurde.
On suppose que P est un ensemble fini et on note $P = \{p_1, p_2, p_3, \ldots, p_n\}$.
Soit $d = \prod_{i=1}^{n} p_i + 1$
d n'est pas premier car il est plus grand que tous les p_i pour $i \in [|1, .., n|]$
Il a donc un diviseur premier m d'après le théorème précédent. m est dans l'ensemble $P = \{p_1, p_2, p_3, \ldots, p_n\}$.
Comme $m \in \{p_1, p_2, p_3, \ldots, p_n\}$ alors m divise d et m divise $\prod_{i=1}^{n} p_i$ donc m divise 1. Ce qui est absurde.
Donc l'ensemble des nombres premiers est infini.

2 Décomposition des entiers en produits de facteurs premiers

Théorème 3 :

Tout entier naturel non nul m distincts de 1 se décompose de façon uniqe sous la forme :
$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n} \qquad (1)$$
avec p_i des nombres premiers tels que $0 < p_1 < p_2 < \ldots < p_n$ et $\alpha_i \in \mathbb{N}^*$

Démonstration :
▷ Existence de la décomposition :
Récurrence sur $m \geq 2$:
On note $\mathcal{P}_m$ la propriété : Tout entier naturel k ($2 \leq k \leq m$) admet une décomposition de la forme (1).
Initialisation :
$\mathcal{P}_2$ est vraie car $2 = 2^1$.
Hérédité :
On suppose que $\mathcal{P}_m$ est vraie :

1. Si $m+1 \in P$ alors $m+1 = (m+1)^1$ donc $\mathcal{P}_{m+1}$ est vraie.
2. Si $m+1 \notin P$:
   D'après le théorème 1 $m+1$ admet un diviseur premier p et $m+1 = pq$ avec $q \in \mathbb{N}$ et $2 \leq q \leq m$
   On a $q \neq 0$ car $m+1 \neq 0$ et $q \neq 1$ car $m+1 \notin P$.
   On applique alors l'hypothèse de récurrence sur q et donc $\mathcal{P}_{m+1}$ est vraie.

Conclusion :
Tout entier naturel non nul m distincts de 1 se décompose sous la forme :
$$m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n}$$
avec p_i des nombres premiers tels que $0 < p_1 < p_2 < \ldots < p_n$ et $\alpha_i \in \mathbb{N}^*$
▷ Démontrons maintenant l'unicité d'une telle décomposition :
Les seuls nombres premiers divisant m d'après le théorème de Gauss, sont p_1, $_2$ …, p_n.
Pour tout $i \in [|1; n|]$, $p_i^{\alpha_i}$ divise m mais $p_i^{\alpha_i+1}$ ne divise pas m.
En effet, si $p_i^{\alpha_i+1}$ divise m alors il existe $q \in \mathbb{N}$ tel que $m = p_i^{\alpha_i+1} \times q$
et en simplifiant on aurait :
$p_1^{\alpha_1} \times p_2^{\alpha_2} \times p_2^{\alpha_i} \ldots \times p_2^{\alpha_i+2} \times p_n^{\alpha_n} = p_i^1 \times q$ et donc $p_i = p_1$ ou $p_i = p_2 \ldots$ ou $p_i = p_n$ ce qui n'est pas le cas.
Donc les α_i sont les exposants des plus grande puissances de p_i, divisant m.
Donc la décomposition est unique car nous n'avons pas le choix des p_i et des α_i.

Proposition 1 :

On note m un entier dont la décomposition en facteurs premiers est $m = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n}$
Les diviseurs (positifs)de m sont les entiers de la forme :
$$p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times \mathrm{p}_n^{\beta_n}$$
avec pour tout $i \in [|1; n|]$, $0 \leq \beta_i \leq \alpha_i$

Théorème 4 :

> Tout entier naturel $n \geq 2$ non premier admet au moins un diviseur premier p tel que $p \leq \sqrt{n}$

Démonstration :

On note n un entier naturel ≥ 2 et $n \notin P$.
On note p_1 le plus petit des diviseurs premiers de n.
alors il existe $k \in \mathbb{N}$ tel que $n = p_1 \times k$ avec $k \leq p_1$
On a donc $n = p_1 \times k \geq p_1^2$
Or la fonction $x \mapsto \sqrt{x}$ est strictement croissante sur $\mathbb{R}^+$
donc $\sqrt{n} \leq p_1$.

3 Petit théorème de Fermat

Théorème 5 :

> Soit p un nombre premier et a un entier non divisible par p.
> Alors $a^{p-1} - 1$ est divisible par p
> $a^{p-1} \equiv 1\ [p]$

Démonstration :

1. Expliquez pourquoi p ne divise aucun de la suite a, $2a$, ..., $(p-1)a$.
2. Démontrer par l'absurde, que le reste des divisions de a, $2a$, ..., $(p-1)a$ par p sont tous différents.
3. En déduire les restes possibles de la division de a, $2a$, ..., $(p-1)a$ par p.
4. En déduire que $a^{p-1} \times 1 \times 2 \times 3 \ldots (p-1) \equiv 1 \times 2 \times 3 \ldots (p-1)\ [p]$
5. En déduire que $a^{p-1} \equiv 1\ [p]$

Corollaire :

> Si p est un nombre premier et a un entier quelconque
> Alors $a^p - a$ est divisible par p
> $a^p \equiv a\ [p]$

Démonstration :
A faire ...

Propriété 1 :

> Si p est un nombre premier et a un entier, alors
> p divise a
> ou
> p et a sont premiers entre eux

Démonstration :
A faire ...

Propriété 2 :

Si p est un nombre premier et a et b deux entiers, alors
Si p divise ab
Alors p divise a ou p divise b.

Démonstration :
A faire ...

4 Applications

4.1 Le codage RSA

Voir prochain DM