Exposé 12

Nbr premiers ; existence et unicité de la décomposition d'un nbr en facteurs premiers. Incertitude de l'ensemble des nbr premiers. Exposé peut faire appel à la calculatrice. Exemple(s) d'algorithme(s) de recherche de nb premiers.

0- Pré-Requis :

- multiples - diviseurs.
- division euclidienne dans $\mathbb{N}$
- PGCD et PPCM de a et b, $a, b \in \mathbb{N}^*$
- Nbr premiers entre eux, Thm de Gauss.
- Raisonnement par récurrence.

I Nombres premiers :

1) Définition

Déf: Un entier naturel n est premier ssi $n > 1$ et s'il n'admet que 1 et lui même comme diviseurs de $\mathbb{N}$.

Rq:
- Si $z \in \mathbb{Z}$, z est premier ssi $|z|$ est premier.
- 0 et 1 ne sont pas premiers.
- 2 est le seul nb pair premier.
- 3, 4, 7, 5 et des nbr premiers.

2) Propriétés :

Prop: $\forall n \in \mathbb{N}$, $n > 1$ admet au moins un diviseur premier.

Prop: Tout nbr premier est premier avec tous les entiers qu'il ne divise pas.

Prop: 2 nombres premiers distincts sont premiers entre eux.

Prop: Tout nombre premier p est premier avec tout entier de 1 à $(p-1)$

Exo: Mq si p premier, p divise C_p^k $\forall k$ tq $0 < k < p$

3) L'ensemble des nombres premiers $\mathbb{P}$

Prop: $\mathbb{P}$ est infini

[[On suppose que $\mathbb{P}$ est fini ie $\exists N \in \mathbb{N}$ tq $\mathbb{P} = \{p_1, \dots, p_N\}$

On considère l'entier $P = p_1 \times p_2 \times \dots \times p_N$

$P+1 \in \mathbb{N}$, donc d'après prop précédente, $\exists q$ premier tq $q \mid P+1$

q premier donc $\exists i \in [\![1, N]\!]$ tq $q = p_i$

On a donc $\left.\begin{array}{l} q = p_i \mid P \\ q = p_i \mid P+1 \end{array}\right\} \Rightarrow q = p_i \mid p+1-p = 1$ Absurde (car $q = p_i$ premier > 1)

Donc q premier, $q \notin \mathbb{P}$ absurde.]]

Rq: $\mathbb{P}$ est infini, par contre la répartition de nbrs premiers est irrégulière

En effet on peut trouver une suite n entiers consécutifs non premiers,

Exo: La suite de terme général : $u_n = (n+1)! + (n+1)$ (u_n divisible par $n+1$, $\forall n \in \mathbb{N}$)

Rq : On a donc montré qu'il y avait une infinité de nbr premier mais que ceux ci ot repartis de manière irrégulière.
=) Problème : comment trouver des nbr premiers ?.

II Algorithme de Recherche de Nombres premiers :

Prop : Un entier $n > 1$ non premier admet au moins un diviseur premier dont le carré est inférieur à n.

1) 1ère algorithme (Conséquence de la proposition)

Pour savoir si $n \in \mathbb{N} \setminus \{0,1\}$ est premier, on va diviser successivement par tous les entiers $d \geq 2$ et tq $d^2 \leq n$.
Si le reste d'une division est 0, le nbr n'est pas premier, sinon n est premier.

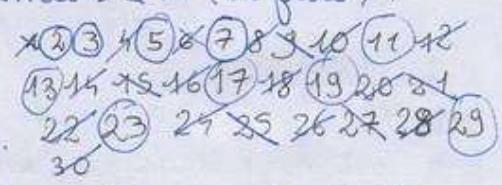
Exemple : 47 ? $2 \nmid 47$ et $2^2 \leq 47$, $3 \nmid 47$ et $3^2 \leq 47$, ..., $6 \nmid 47$ et $6^2 \leq 36$, $7 \nmid 47$ et $7^2 = 49 > 47$ donc 47 est premier.
(car sinon il aurait un div premier p tq $p^2 \leq 47$!)

Rq : On peut améliorer cet algorithme.

2) Crible d'Eratosthène :

Il permet d'établir la liste des nbr premiers $\leq n$ (n fixé).

- Choisir n
- Ecrire la liste des nbr de 2 à n
- Entourer 2
- Supprimer tous les multiples de 2 de cette liste.
- Entourer le premier nombre non barré de la liste suivant 2, soit 3. Ce nbr ne possède pas de diviseur premier strict inférieur à lui, donc sera premier.
- Supprimer tous les multiples de 3 de la liste ...



- S'arrêter dès que le dernier nombre entouré élevé au carré dépasse n.

Tous les nombres premiers de la liste et alors entourés.

III Décomposition en facteurs premiers :

Thm : Si un nb premier divise un produit de facteurs non nuls alors il divise l'un des facteurs.

Cor Thm : Si un nb premier divise un produit de facteurs premiers alors il est égal à l'un d'eux.

Thm Fondamental de l'arithmétique :

Thm : Tout $n \in \mathbb{N}$ ($n > 1$) s'écrit de manière unique comme produit de facteurs premiers p_i, $i \in [\![1, m]\!]$ $p_1 \leq \dots \leq p_m$, $m \geq 1$

Soit $n \in \mathbb{N}$, $n \geq 2$

I Existence : - si $n \in \mathbb{P}$, la décomposition est faite.

- si $n \notin \mathbb{P}$ alors n admet au moins un div premier p_1 (prop du I)

$n = p_1 n_1$

- si $n_1 \in \mathbb{P}$ ...
- si $n_1 \notin \mathbb{P}$ ... On construit ainsi une suite strict décroissante ... d'où l'existence de la décomposition.

Unicité : (Recurrence)

P_n : K tq $2 \in K \in n$ se décompose de manière unique en produit de facteurs premiers."

- $n = 2$ OK
- Hq $P_n \Rightarrow P_{n+1}$

On pose $n+1 = \underbrace{p_1 \times \dots \times p_k = q_1 \times \dots \times q_p}$ (ie 2 décomp en facteur premier.

ie $p_1 \mid q_1 \dots q_p$ et p_1 premier, q_i premier $\forall i$ $\Big\}$ $\overset{\text{Gauss}}{\Rightarrow} \exists i \in [\![1, p]\!]$ tq $p_1 = q_i$

de $\frac{n+1}{p_1} = p_2 \times \dots \times p_k = q_1 \times \dots q_{i-1} \times q_{i+1} \times \dots \times q_p$ or $\frac{n+1}{p_1} < n+1$ car $p_1 > 1$.

Donc hypothèse de récurrence $\frac{n+1}{p_1}$ admet une décomposition unique et donc $n+1$ admet une décomposition unique //

Rq : Dans la décomposition précédente, certains facteurs premiers peuvent être égaux.

Corollaire : Tout $n \in \mathbb{N}$, $(n > 1)$ se décompose de manière unique de la forme : $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, p_i premiers, $p_1 < \dots < p_k$, $\alpha_i \in \mathbb{N}^*$

IV Applications :

1) Expressions du PGCD et PPCM de deux entiers.

Si les décompositions de a et b s'écrivent :

$a = \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{n} p_i^{\beta_i}$ avec $(\alpha_i, \beta_i) \in \mathbb{N}^2$

$\text{pgcd}(a,b) = \prod_{i=1}^{n} p_i^{\min(\alpha_i, \beta_i)}$ et $\text{ppcm}(a,b) = \prod_{i=1}^{n} p_i^{\max(\alpha_i, \beta_i)}$

Démonstrations

Propriétés

i) Soit $n \in \mathbb{N}$, $n > 1$

$D = \{ d \in \mathbb{N},\ d > 1,\ d \mid n \}$

$D \neq \emptyset$ car $n \in D$ et $D \subset \mathbb{N}$

D partie non vide et minorée (par 1) de $\mathbb{N}$ donc D admet un plus petit élément.

Soit d_0 ce plus petit élément.

- Si d_0 est un nombre premier alors la propriété vraie.
- sinon $\exists K \in \mathbb{N}$, diviseur de d_0 tq $2 \leq K < d_0$.

  K est donc un diviseur de n inférieur à d_0 absurde

ii) [[évident]]

iii) Soit $p, q \in \mathbb{P}$, $p \neq q$

pgcd(p,q) divise p or p premier $\Rightarrow$ pgcd(p,q) = 1 ou p

q = q $\Rightarrow$ pgcd(p,q) = 1 ou q

$p \neq q \Rightarrow$ **pgcd(p,q) = 1**

iv) évident

II Proposition :

[[Soit $n \in \mathbb{N}$, $n > 1$, $n \notin \mathbb{P}$, d'après une prop ou précédemment, n admet un plus petit diviseurs, d_0, $d_0 > 1$ et que d_0 est un nombre premier.

de $\exists k \in \mathbb{N}$ tq $n = k d_0$ or d_0 plus petit diviseur donc $k \geq d_0$

et **$n = k d_0 \geq d_0^2$**]]

Exo de la partie I

[[p premier, p divise C_p^k $\forall k$ tq $0 < k < p$

soit $0 < K < p$

$$C_p^K = \frac{p \cdot (p-1) \times \cdots \times 1}{K!(p-K)!} = \frac{p \times \cdots \times (p-K+1)}{K!}$$

de $K!\, C_p^K = p \times \cdots \times (p-K+1) \Rightarrow$ p divise $K! C_p^K$ et $p \wedge K! = 1$ car $0 < K < p$

Gauss

$p \mid C_p^K$]]

III Thm :

[[Récurrence sur k le nb de facteurs que divise n ($n \in \mathbb{P}$

- si $k = 2$ $n \mid p_1 p_2$ si n ne divise pas p_1 alors pgcd$(n, p_1) = 1$ (car $D_n = \{1, n\}$)

$\Rightarrow$ GAUSS $n \mid p_2$

- ...]]