NOMBRES PREMIERS

Remarque : lorsqu'on parlera de *diviseurs*, il sera sous-entendu qu'il s'agit de diviseurs *positifs*

I Définition et propriétés

Définition : Un nombre entier est dit premier s'il admet exactement deux diviseurs distincts : 1 et lui-même.

Le nombre 1 n'est donc pas un nombre premier.

Un nombre distinct de 1 et non premier est dit composé.

Ex : le début de la liste des nombres premiers est 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41…

Propriété : Tout nombre entier a strictement supérieur à 1 admet un diviseur premier.

Preuve : si a est premier alors le diviseur premier cherché est a.

Sinon, a admet un diviseur autre que 1 et a.

Notons $\mathcal{D}(a)$ l'ensemble des diviseurs de a.

$\mathcal{D}(a) = \{1 ; d_1 ; d_2 ; \dots ; a\}$ avec $1 < d_1 < d_2 < \dots < a$.

Si d_1 n'est pas premier, alors il admet un diviseur d tel que $1 < d < d_1$.

$d | d_1$ et $d_1 | a$ donc $d | a$. De plus, $d < d_1$.

Absurde car d_1 est le plus petit diviseur de a.

Donc d_1 est premier.

Propriété : Tout nombre composé a admet un diviseur premier inférieur ou égal à $\sqrt{a}$.

Preuve : a est composé donc il admet au moins un diviseur premier d tel que $1 < d < a$.

On peut donc écrire $a = d \times d'$ avec $1 < d \leq d' < a$ *(en prenant pour d le plus petit diviseur comme dans la preuve précédente)*

Ainsi, $d^2 \leq dd'$ c'est-à-dire $d^2 \leq a$ et donc $d \leq \sqrt{a}$.

Conséquence : Si aucun des entiers entre 2 et $\sqrt{n}$ ne divise n, alors n est premier.

⇨ *C'est ce qu'on appelle un « test de primalité ».*

Ex : 127 est-il un nombre premier ?

On a $\sqrt{127} \approx 11{,}3$. Or, 127 n'est pas divisible par 2, par 3, 5, 7 et 11.

Donc 127 est un nombre premier.

Propriété : Soit p un nombre premier.
1. Si p divise le produit ab de deux entiers, alors p divise a ou b.

2. Si p divise le produit ab de deux nombres premiers, alors $p = a$ ou $p = b$.

Preuve : 1. Si $p|a$, alors c'est fini.

Si $p \nmid a$, alors p et a sont premiers entre eux.

En effet, p est premier et donc ses seuls diviseurs sont 1 et p.

Par conséquent, le seul diviseur commun de a et p est 1

Donc p et a sont premiers entre eux.

Et puisque $p|ab$, alors $p|b$ d'après Gauss.

2. D'après 1., $p|a$ ou $p|b$.

Or, a et b n'admettent comme diviseurs que 1 et eux-mêmes.

Et puisque p est différent de 1, alors $p = a$ ou $p = b$.

Ex : Soient a et b deux nombres entiers supérieurs ou égaux à 2. Démontrer que si $a + b$ est un nombre premier, alors a et b sont premiers entre eux.

Supposons a et b non premiers entre eux.

Autrement dit, si on note $d = \text{PGCD}\ (a\ ;\ b)$ alors $d \geq 2$.

On a également $d \leq a < a + b$.

Or $d|a + b$ et $2 \leq d < a + b$.

$a + b$ possède donc un diviseur autre que 1 et que lui-même : absurde car $a + b$ est premier.

Donc a et b sont premiers entre eux.

Propriété : Il existe une infinité de nombres premiers.

Preuve : Supposons qu'il n'existe qu'un nombre fini de nombres premiers.

Soit p le plus grand de tous les nombres premiers. On pose $N = 2 \times 3 \times 5 \times \ldots \times p + 1$.

$N > 1$ donc N admet un diviseur premier d.

Nécessairement, d est donc l'un des nombres 2, 3, 5, … ou p.

d divise donc $2 \times 3 \times 5 \times \ldots \times p$ et puisque $d|$ N, alors $d|N - 2 \times 3 \times 5 \times \ldots \times p$.

Autrement dit, $d|1$. Absurde car d est un nombre premier !

Il existe donc bien une infinité de nombres premiers.

II Décomposition en produit de facteurs premiers

Théorème : Un nombre entier naturel supérieur ou égal à 2 est premier ou se décompose de manière unique (à l'ordre près) en produit de nombres premiers.

Preuve : L'unicité est admise *(faisable toutefois)*
Démontrons l'existence : soit n un entier naturel non premier.

n n'étant pas premier, il admet un diviseur premier p_1 différent de 1 et de n.

On peut donc écrire $n = p_1 \times q_1$ où q_1 est un diviseur de n différent de 1 et de n.

Si q_1 est premier, c'est terminé.

Sinon, q_1 admet un diviseur premier p_2.

On a alors $q_1 = p_2 \times q_2$ où q_2 est un diviseur de q_1 différent de 1 et de q_1.

Et ainsi, $q_2 < q_1 < n$ et $n = p_1 \times p_2 \times q_2$

Si q_2 est premier, c'est terminé. Et sinon, on recommence…

La suite (q_i) ainsi obtenue est telle que $1 \leq q_i < q_{i-1} < \cdots < q_2 < q_1 < n$.

Autrement dit, c'est une suite d'entiers naturels strictement décroissante.

Cette suite finit donc par s'arrêter, et donc, à un certain moment, on a forcément q_k qui est un diviseur premier. Et à ce moment-là, $n = p_1 \times p_2 \times \ldots \times p_k \times q_k$

Ex : Via la décomposition en facteurs premiers de $a = 540$ et $b = 168$, déterminer PGCD$(a\,;b)$.

$540 = 54 \times 10$
$= 9 \times 6 \times 2 \times 5$
$= 3 \times 3 \times 2 \times 3 \times 2 \times 5$
$= 2^2 \times 3^3 \times 5$

$168 = 2 \times 84$
$= 2 \times 2 \times 42$
$= 2 \times 2 \times 7 \times 2 \times 3$
$= 2^3 \times 3 \times 7$

Donc PGCD$(a\,;b) = 2^2 \times 3 = 12$ en prenant les plus petits exposants.

Ex : Quel est le plus petit carré multiple de 14 850 ?

⇨ $14\,850^2 = 220\,522\,500$ est un carré multiple de 14 850 mais …

⇨ $7\,425 \times 2\,112 = 15\,681\,600 = 3\,960^2$ est mieux…

Pour qu'un nombre soit un carré parfait, il faut que la puissance de chacun des facteurs de sa décomposition en facteurs premiers soit paire.

$$14\,850 = 50 \times 297$$
$$= 5^2 \times 2 \times 3 \times 99$$
$$= 2 \times 3^3 \times 5^2 \times 11$$

On prend donc $2^2 \times 3^4 \times 5^2 \times 11^2 = (2 \times 3^2 \times 5 \times 11)^2$

$$= 990^2$$
$$= 980\,100$$
$$= 14\,850 \times 66$$

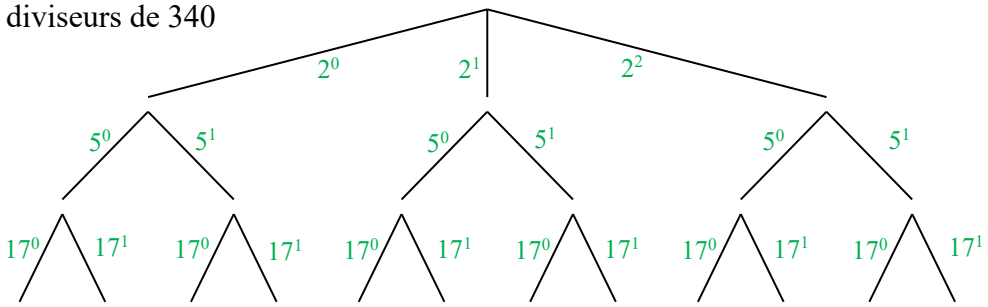
Le plus petit carré multiple de 14 850 est donc 980 100.

Propriété : Soit n un entier naturel non premier dont la décomposition en produit de facteurs premiers est $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.
Les diviseurs de n sont tous les nombres s'écrivant sous la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ où $0 \leq \beta_i \leq \alpha_i$ pour tout i compris entre 1 et k.

⇒ le nombre de diviseurs de n est $\prod_{i=1}^{k} (\alpha_i + 1) = (\alpha_1 + 1)(\alpha_2 + 1)\dots(\alpha_k + 1)$

Ex : déterminer la liste des diviseurs de 340

$340 = 2 \times 170$
$= 2 \times 2 \times 85$
$= 2^2 \times 5 \times 17$



A l'aide d'un arbre par exemple, les diviseurs de 340 sont :

1 / 2 / 4 / 5 / 10 / 17 / 20 / 34 / 68 / 85 / 170 / 340

III Le petit théorème de Fermat

Théorème : Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} \equiv 1 \ [p]$.

Autrement dit, $a^{p-1} - 1$ est un multiple de p.

⇨ Ce théorème donne une garantie de tomber sur « 1 » lors du cycle des puissances modulo p.

Corollaire : Si p est un nombre premier et si a est un entier, alors $a^p \equiv a \ [p]$.

Autrement dit, $a^p - a$ est un multiple de p.

Ex 1 : Démontrer que pour tout entier naturel n, 11 divise $7^{10n} - 1$.

11 est un nombre premier et 7 est premier avec 11.

Donc, d'après le petit théorème de Fermat, $7^{11-1} \equiv 1 \ [11]$.

$$7^{10} \equiv 1 \ [11]$$

$$(7^{10})^n \equiv 1^n \ [11]$$

$$7^{10n} \equiv 1 \ [11]$$

$$7^{10n} - 1 \equiv 0 \ [1]$$

Autrement dit, $11|7^{10n} - 1$.

Remarque : on pouvait le faire de manière classique, avec les congruences…

$7^2 = 49 \equiv 5 \ [11]$

$7^4 = (7^2)^2 \equiv 5^2 \ [11]$

$\equiv 3 \ [11]$

$7^{10} = (7^4)^2 \times 7^2 \equiv 3^2 \times 5 \ [11]$

$\equiv 45 \ [11]$

$\equiv 1 \ [11]$ puis la fin est la même…

Ex 2 : Montrer que pour tout $n \in \mathbb{N}^*$, $n^{13} - n$ est divisible par 26.

Il suffit en fait de montrer que $n^{13} - n$ est divisible par 2 et par 13.

On a donc $n^2 \equiv n \ [2]$ d'après le petit théorème de Fermat avec $p = 2$.

$n^4 \equiv n^2 \ [2] \equiv n \ [2]$

$(n^4)^3 \times n \equiv n^3 \times n \ [2]$

$n^{13} \equiv n^4 \ [2] \equiv n \ [2]$

De même, on a $n^{13} \equiv n \ [13]$ d'après le petit théorème de Fermat avec $p = 13$.

Donc $2|n^{13} - n$ et $13|n^{13} - n$.

Et puisque 2 et 13 sont premiers entre eux, $n^{13} - n$ est divisible par 26.

⇨ il existe un « grand » théorème de Fermat, connu sous le nom de théorème de Fermat *(tout court)*.

« Il n'existe pas d'entiers strictement positifs x, y et z tels que $x^n + y^n = z^n$ si n est un entier supérieur ou égal à 3. »

COMPLÉMENT

La preuve du petit théorème de Fermat est entre autres basée sur la formule du binôme de Newton :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Et avec $a = 1$:

$$(a+1)^n = \sum_{k=0}^{n} \binom{n}{k} a^k$$

Commençons par démontrer le corollaire : « *Si p est premier et si a est un entier, alors* $a^p \equiv a \ \ [p]$. »

Initialisation : $a = 0$

$0^p = 0 \equiv 0 \ \ [p]$ donc la propriété est vérifiée pour $a = 0$.

Hérédité : supposons que $a^p \equiv a \ \ [p]$ pour un certain $a \geq 1$.

Montrons que $(a+1)^p \equiv a+1 \ \ [p]$.

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

Or, $\binom{p}{k} = \dfrac{p!}{(p-k)!\,k!} = \dfrac{p(p-1)\ldots(p-k+1)}{k!}$ si $k \neq 0$.

Autrement dit, $k!\binom{p}{k} = p(p-1)\ldots(p-k+1)$.

Donc, si $k \neq 0$, p divise $k!\binom{p}{k}$.

De plus, si $k < p$, sachant que p est premier alors p est premier avec $k!$.

Donc p divise $\binom{p}{k}$ pour tout $1 \leq k \leq p-1$ d'après Gauss.

Ainsi, $(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a^1 + 1$

$$\equiv a^p + 0 \times a^{p-1} + 0 \times a^{p-2} + \cdots + 0 \times a^1 + 1 \ \ [p]$$

$$\equiv a^p + 1 \ \ [p]$$

$$\equiv a + 1 \ \ [p] \ \text{ par HR}$$

Par récurrence, on a donc $a^p \equiv a \ \ [p], \forall a \in \mathbb{N}$

A partir de là, $a^p = a + k \times p$ et donc $a^p - a = k \times p$

$$a(a^{p-1} - 1) = k \times p$$

Ainsi, si a n'est pas divisible par p alors p divise $a^{p-1} - 1$.