LES NOMBRES PREMIERS

Table des matières

1 Notion de nombres premiers

1.1 Définition

Un entier naturel n est dit premier s'il admet seulement deux diviseurs distincts qui sont 1 et n.

Exemple 1

- *1 n'est donc pas premier*
- *2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 47, 53, 59, 61, 67, 71, 73,79, 83, 89, 97 sont les nombres premiers inférieurs à 100.*
- *Un entier non premier est dit composé*

1.2 Théorème : diviseurs premiers ROC

Tout entier $n \geq 2$ admet un diviseur premier.

Démonstration 1

- *Si n est premier, n admet un diviseur premier qui est lui même*
- *Si n n'est pas premier envisageons l'ensemble les diviseurs de n rangés dans l'ordre croissant*

$$D(n) = \{1; d_1; d_2; d_3, ...; n\}.$$

Nécessairement d_1 est premier, sinon il existerait d un diviseur de d_1 et donc de n plus petit que d_1

Exemple 2

- *Le plus petit diviseur premier de 17 est 17.*
- *Le plus petit diviseur premier de 25 est 5.*

1.3 Théorème : ensemble des diviseurs premiers

Tout entier naturel n non premier admet un diviseur premier $p \leq \sqrt{n}$.

Démonstration 2

Soit p_1 le plus petit diviseur premier de n .

- $n = p_1 \times q$.
- $q \neq 1$ *car n n'est pas premier et donc* $q \geq 2$.
- *L'entier $q \geq 2$ admet au moins un diviseur premier p_2 qui est aussi diviseur de n.*
- *On a alors $q \geq p_2 \geq p_1$ le plus petit des diviseurs premiers de n .*
- *On a donc $q \geq p_1$, et donc $p_1 \times q \geq {p_1}^2$. Autrement dit $n \geq {p_1}^2$, ou $p_1 \leq \sqrt{n}$.*

1.4 Application : le crible d'Eratosthène et algorithme de test de primalité

Pour savoir si un nombre est premier ou non, il suffit de tester sa divisibilité par tous les nombres premiers inférieurs ou égaux à sa racine carrée.

Algorithme de test de primalité

Début

Lire N

p $\longleftarrow$ 2

Tant que $p \leqslant \sqrt{N}$ faire

$R \longleftarrow$ Reste (N/p)

Si $R = 0$ alors

Écrire "N n'est pas premiers"

p $\longleftarrow N$

Sinon $p \longleftarrow p + 1$

Fsi

Ftq

Si $p \neq N$ alors écrire "p est premier"

FIN

Remarque : On peut encore diviser par deux le travail en ne testant que les nombres impairs, une fois que la divisibilité par deux a échoué.

1.5 Théorème sur l'ensemble infini des nombres premiers ROC

Il existe une infinité de nombres premiers

Démonstration 3

On raisonne par l'absurde : on suppose qu'il existe un nombre fini de nombres premiers que l' on note $p_1; p_2; p_3; ....., p_n$.
Et on considère le nombre $N = p_1 \times p_2 \times p_3 \times ..... \times p_i \times ..... \times p_n + 1$

N *étant strictement supérieur 1 d'après le théorème précédent il admet un diviseur premier.*
Ce diviseur premier est un diviseur de la liste finie $p_1; p_2; p_3; ....., p_n$. *On note* p_i *ce diviseur.*

Sachant que p_i *divise* N *, il divise donc* $p_1 \times p_2 \times p_3 \times ..... \times p_i \times ..... \times p_n + 1$
mais aussi $p_1 \times p_2 \times p_3 \times ..... \times p_i \times ..... \times p_n$, *donc la différence qui est 1.*
Et donc $p_i = 1$ *ce qui est impossible*

L'hypothèse faîte au début aboutit à une contradiction donc elle est fausse.
Autrement dit l'ensemble des nombres premiers ne peut être fini, il y en a donc une infinité.

2 Décomposition en un produit de facteurs premiers

2.1 Théorème : décomposition primaire

Tout entier n supérieur ou égal à 2 est premier ou produit de nombres premiers.

On note en regroupant les facteurs communs : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times .....p_r^{\alpha_r}$ appelé décomposition primaire.

Démonstration 4

On admet l'unicité de la décomposition et on démontre seulement l'existence d'un telle décomposition.

On suppose n non premier (composé), sinon n est sa propre décomposition.

- *n admet donc un diviseur premier* p_1 *et donc* $n = p_1 \times q_1$ *avec* $1 < q_1 < n$.
- *Si* q_1 *est premier la décomposition primaire de n est finie. Sinon* q_1 *admet un diviseur premier* p_2 .
  Ce qui permet d'écrire $q_1 = p_2 \times q_2$ *avec* $1 < q_2 < q_1$.
- *D'où* $n = p_1 \times q_1 = p_1 \times p_2 \times q_2$, *avec* $1 < q_2 < q_1 < n$.
- *On répète le procédé tant que le quotient* q_i *est différent de 1.*
  La liste des quotients est strictement décroissante $(1 < .....q_i < .....q_3 < q_2 < q_1.... < n)$.
  Cette liste est formée d'entiers strictement positifs, elle est donc finie.
  Au bout d'un nombre fini de k opérations, $q_k = 1$. *On a alors* $n = p_1 \times p_2 \times p_3..... \times p_k$

Exemple 3

16758	2
8379	3
2793	3
931	7
133	7
19	19
1	

$16758 = 2 \times 3^2 \times 7^2 \times 19$

2.2 Théorème sur la décomposition primaire

Soit n un entier naturel dont la décomposition primaire est $p_1^{\alpha_1} \times p_2^{\alpha_2} \times .....p_r^{\alpha_r}$.
Les diviseurs positifs de n sont les entiers de la forme $p_1^{\beta_1} \times p_2^{\beta_2} \times .....p_r^{\beta_r}$ où $0 \leq \beta_i \leq \alpha_i$ pour $1 \leq i \leq r$.

2.3 Corollaire : nombre de diviseurs d'un entier à partir de sa décomposition primaire

n dont la décomposition primaire est $p_1^{\alpha_1} \times p_2^{\alpha_2} \times .....p_r^{\alpha_r}$ a $(\alpha_1 + 1)(\alpha_2 + 1).....(\alpha_r + 1)$ diviseurs positifs.
Ainsi $16758 = 2 \times 3^2 \times 7^2 \times 19$ aura $2 \times 3 \times 3 \times 2 = 36$ diviseurs positifs.

3 Applications

3.1 Déterminons les entiers naturels n admettant 5 diviseurs positifs

Soit $p_1^{\alpha_1} \times p_2^{\alpha_2} \times .....p_r^{\alpha_r}$ la décomposition primaire de n.
n admettant 5 diviseurs positifs nous pouvons écrire que $(\alpha_1 + 1)(\alpha_2 + 1).....(\alpha_r + 1) = 5$
Donc les facteurs $\alpha_i + 1$ sont des diviseurs positifs de 5.
D'où tous ces facteurs sont égaux 1 sauf un qui est gal 5.
Autrement dit tous les α_i sont égaux 0 sauf un qui est égal 4.
Conclusion n est la puissance quatrième d'un nombre premier.
Soit $n = 2^4$, ou $n = 3^4$, ou $n = 5^4$..... etc.

3.2 Trouvons un nombre N de quatre chiffres, terminé par 9, divisible par 147 et qui soit un carré parfait

- Si N est divisible par 147 alors il existe un entier q tel que $N = 147 \times q$.
- Si N est un nombre de quatre chiffres alors $1000 \leq N \leq 9999$.
- Si N se termine par 9 alors q se termine par 7.
- $147 = 3 \times 7^2$, $N = 3 \times 7^2 \times q$. Et donc si N est un carré parfait,le quotient de q par 3 est un carré.

Le problème se ramène à la détermination de q.

On a $1000 \leq 147 \times q \leq 9999$ et donc $7 \leq q \leq 68$.

q se terminant par 7, $q \in \{17; 27; 37; 47; 57; 67\}$.

q doit être divisible par 3, donc $q = 27$ ou $q = 57$.

Et le quotient de q par 3 doit être un carré. Donc $q = 27$.

Conclusion $N = 147 \times 27 = 3^{\times}7^2 \times 3^3 = 3^4 \times 7^2 = 3969$.

3.3 Déterminons un entier naturel n dont la décomposition primaire est $n = 2^\alpha \times 3^\beta$ et tel que le nombre de diviseurs de n^2 soit le triple du nombre de diviseurs de n.

Si $n = 2^\alpha \times 3^\beta$ alors $n^2 = 2^{2\alpha} \times 3^{2\beta}$

Le nombre de diviseurs de n est $(\alpha + 1)(\beta + 1)$ et celui de n^2 est $(2\alpha + 1)(2\beta + 1)$.

On doit donc avoir $3(\alpha + 1)(\beta + 1) = (2\alpha + 1)(2\beta + 1)$

En développant on obtient : $3\alpha\beta + 3\alpha + 3\beta + 3 = 4\alpha\beta + 2\alpha + 2\beta + 1$

Soit $\alpha\beta - \alpha - \beta - 2 = 0$, ou encore $\alpha(\beta - 1) - \beta - 2 = 0$, $\alpha(\beta - 1) - (\beta - 1) - 3 = 0$,

$(\beta - 1)(\alpha - 1) - 3 = 0$

Soit $(\beta - 1)(\alpha - 1) = 3$, ce qui donne $\left\{ \begin{array}{l} \alpha - 1 = 1 \\ \beta - 1 = 3 \end{array} \right.$ ou $\left\{ \begin{array}{l} \alpha - 1 = 3 \\ \beta - 1 = 1 \end{array} \right.$ Soit $\left\{ \begin{array}{l} \alpha = 2 \\ \beta = 4 \end{array} \right.$ ou $\left\{ \begin{array}{l} \alpha = 4 \\ \beta = 2 \end{array} \right.$

On obtient $n = 2^2 \times 3^4 = 324$ ou $n = 2^4 \times 3^2 = 144$

3.4 Soit p un nombre premier supérieur ou égal à 5. Montrons que p s'écrit sous l'une des formes $6k - 1$ ou $6k + 1$ puis déterminons le reste de la division de $p^2 - 1$ par 24.

Conjecture en utilisant la calculatrice

- **Casio :** Menu, Liste, $list\,1(5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 53)$,
  $option$, $list\,2 = list\,1^2 - 1$, $list\,3 = list\,2 - 24\,Intg\,(list\,2 \div 24)$
- **Texas :** STAT, EDIT, $L1(5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 53)$,
  $L2 = L1^2 - 1$, $L3 = L2 - 24\,int(L2 \div 24)$.

1. Tout nombre supérieur ou égal à 5 est de l'une des formes : $6k - 1,\ 6k,\ 6k + 1,\ 6k + 2,\ 6k + 3,\ 6k + 4$, $k \in \mathbb{N}^*$.

Or p tant premier il ne peut être de la forme $6k,\ 6k + 2,\ 6k + 4$.

Donc les seules formes pour p premier supérieur ou égal à 5 sont $6k - 1$ ou $6k + 1$.

2. – Si $p = 6k - 1$ alors $p^2 - 1 = (p + 1)(p - 1) = 6k(6k - 2) = 6k \times 2(3k - 1) = 12k(3k - 1)$.

– Si k est pair alors $12k$ est divisible par 24, et donc $p^2 - 1 = 12k(3k - 1)$ aussi.

- Si k est impair alors $3k$ aussi et $3k-1$ est pair. D'où $12(3k-1)$ est divisible par 24, et donc $p^2-1=12k(3k-1)$ aussi.

– Si $p=6k+1$ alors $p^2-1=(p-1)(p+1)=6k(6k+2)=6k\times 2(3k+1)=12k(3k+1)$.

- Si k est pair alors $12k$ est divisible par 24, et donc $p^2-1=12k(3k+1)$ aussi.
- Si k est impair alors $3k$ aussi et $3k-1$ est pair. D'où $12(3k+1)$ est divisible par 24, et donc $p^2-1=12k(3k+1)$ aussi.

On peut donc en conclure que si p est un nombre premier supérieur 5 alors p^2-1 est divisible par 24.

Remarque : si l'on s'intéresse la liste des entiers tels que p^2-1 soit divisible par 24, on trouve :

5,7,11,13,17,19,23,**25**,29,31,**35**,37,41,47,**49**,53,**55**,59,61.....Cette liste comporte tous les nombres premiers supérieurs ou égal à 5, mais également des composés.