Nombres premiers

Table des matières

I Activités 1 et 3 page 39 1

II Définitions et exemples : 1

III Théorème fondamental de l'arithmétique 3

IV Liste des nombres premiers inférieurs à 1000 : 5

I Activités 1 et 3 page 39

II Définitions et exemples :

Définition

On dit qu'un entier naturel n est premier s'il admet exactement deux diviseurs entiers naturels distincts : 1 et n.

Remarque : les premiers entiers naturels premiers sont : 2, 3, 5, 7, 11...

Remarque

Ne pas confondre entiers premiers et entiers premiers entre eux

Exemple : 14 et 15 sont premiers entre eux (aucun diviseur commun), mais aucun des deux n'est premier.

Théorème :

1. Tout entier naturel $n \geqslant 2$ admet au moins un diviseur premier.
2. Tout naturel non premier autre que 1 admet un diviseur premier a tel que $a \leq \sqrt{n}$
3. L'ensemble $\mathbb{P}$ des nombres premiers est infini.

Démonstration :

1. Supposons $n \geq 2$.

- Si n est premier, comme n est un diviseur de lui-même, c'est clair.
- Supposons n non premier.
  On considère l'ensemble des diviseurs de n.
  On rappelle que toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
  L'ensemble des diviseurs de n distincts de n est non vide (il contient au moins un diviseur propre ($\neq n$) de n), donc admet un plus petit élément p.
  Soit d un diviseur de p, différent de 1. (d existe, par exemple p).
  $d \leq p$, d divise p et p divise n, donc d divise n, donc $d \geq p$ (définition de p).
  On en déduit que $d = p$, donc que p est premier.

2. Soit $n > 1$, n non premier. n admet donc un diviseur d autre que 1 et n.
   Il existe d' entier non nul tel que $n = dd'$.
   $d \geq 2$ et $d' \geq 2$.
   Supposons $d \leq d'$. $d \leq d' \Rightarrow d^2 \leq dd' = n \Rightarrow d \leq \sqrt{n}$.
3. On effectue une **démonstration par l'absurde**.
   On suppose que l'ensemble $\mathbb{P}$ est fini ; avec n éléments $p_1, p_2, \ldots p_n$.
   On pose $\boxed{k = p_1 p_2 \times p_n + 1}$.
   On a deux cas possibles :
   - k est premier. Or k est plus grand que chacun des nombres $p_1, p_2, \ldots, p_n$. on a donc un nouveau nombre premier, qui n'est pas dans la liste supposée complète des nombres premiers. On a une contradiction.
   - k n'est pas premier.
     p_1 ne divise pas k. En effet, si p_1 divisait k, comme p_1 divise le produit $p_1 p_2 \ldots p_n$, alors p_1 diviserait la différence $k - p_1 p_2 \ldots p_n$, c'est-à-dire 1. On obtiendrait $p_1 = 1$, ce qui est impossible, puisque p_1 est premier.
     De même avec les autres nombres $p_2, p_3, \ldots, p_n$.
     On en déduit que k n'admet aucun diviseur premier, ce qui contredit la première partie du théorème (tout entier autre que 1 admet au moins un diviseur premier)

Remarque

On ne connaît pas la liste de tous les nombres premiers. On n'a pas de formule permettant de les trouver tous.
Étant donné un grand nombre, il est difficile (long) avec un ordinateur de savoir si ce nombre est premier ou pas. Nous verrons que c'est sur cette difficulté à savoir si un grand nombre est premier ou pas que reposent la plupart des codes secrets utilisés en cryptographie.

Test de primalité :
Soit n un entier naturel ≥ 2. Si n n'est divisible par aucun nombre premier dont le carré est inférieur ou égal à n, alors n est premier.

Moyens de trouver les premiers nombres premiers :

1. **Crible d'Erathosthène :**
   On dresse par exemple la liste des nombres entre 1 et 100 dans un tableau. On barre la case contenant 1, puis celles contenant les multiples de 2 (sauf 2), les multiples de 3 (sauf 3) et ainsi de suite.

2. Trouver un algorithme programmable sur une calculatrice.
   Pour tester si un nombre est premier, on le divise par 2, puis par 3, puis par tous les entiers a à partir de a en allant de 2 en 2, tant que $a^2 \leq n$.
   Remarque : k divise n si $E\left(\frac{n}{k}\right) = \frac{n}{k}$.

Exercice :

1. Développer $(a^2+8)^2$, puis factoriser a^4+64.
2. Montrer que a^4+64 n'est pas premier, quel que soit a entier au moins égal à 1.

Solution :

1. $(a^4+8)^2 = a^4+16a^2+64$, donc $a^4+64 = (a^4+8)^2 - 16a^2 = (a^2+8-4a)(a^2+8+4a)$.
2. $a^2+8-4a = (a-2)^2+4 \geq 4$.
   $a^2+8+4a = (a+2)^2+4 \geq 4$
   Ainsi, $a^4+64 = m \times n$ avec m et n entiers strictement supérieurs à 1, donc ce nombre n'est pas premier.

III Théorème fondamental de l'arithmétique

Théorème fondamental de l'arithmétique

Tout naturel strictement supérieur à 1 se décompose en produit de facteurs premiers et cette décomposition est unique à l'ordre des facteurs près.

Démonstration de l'existence :

Soit $n \geq 2$.
Si n est premier, n se décompose en un seul facteur premier, lui-même.
Si n n'est pas premier, il admet au moins un diviseur premier p et $n = p \times d_1$, avec $1 < p < n$ et $1 < d_1 < n$.
Si d_1 est premier, on a décomposé n en produit de deux facteurs premiers.
Si d_1 n'est pas premier, on utilise le résultat précédent pour écrire $d_1 = p' \times d_2$ avec p' premier, $1 < p' < d_1$ et $1 < d_2 < d_1$.
On a alors $n = p \times p' \times d_2$.
On continue...
Les entiers $d_1, d_2, \ldots, d_n$ forment une suite strictement décroissante de naturels : on continue jusqu'à ce qu'on arrive à 1.
On a alors la décomposition.

On admet l'unicité. (on la démontrera plus tard, dans un autre chapitre)

Exemple : donner la décomposition de 5544.
On effectue des divisions successives par les facteurs premiers pris dans l'ordre croissant.
On peut aussi programmer la calculatrice.

Propriété

Un naturel d divise un naturel n si, et seulement si, les facteurs premiers de la décomposition en facteurs premiers de d se trouvent dans celle de n avec des exposants au moins égaux à ceux avec lesquels ils figurent dans celle de d.

Démonstration :
Supposons que d divise n. Soit p un facteur premier de la décomposition de d et α l'exposant de p dans cette décomposition.
Alors $n = d \times q = (p^\alpha a)q$, avec a et q entiers.
On a $n = p^\alpha(aq)$. Soit β l'exposant de p dans la décomposition en facteurs premiers de aq et γ l'exposant de p dans celle de n.
On a : $\gamma = \alpha + \beta$, donc on a bien $\alpha \leq \gamma$.

Réciproquement : soit $n = p_1^a p_2^b \dots p_r^l$ et $d = p_1^{a'} p_2^{b'} \dots p_r^{l'}$ avec $0 \leq a' \leq a, \dots, 0 \leq l' \leq l$.
Alors $n = p_1^{a-a'} p_2^{b-b'} \dots p_r^{l-l'} \times d$ et d divise n.

Exemple :
Cherchons les diviseurs de 648. $648 = 2^3 \times 3^4$. Ses diviseurs sont de la forme $2^a \times 3^b$ avec a et b entiers tels que $0 \leq a \leq 3$ et $0 \leq b \leq 4$.
Pour les trouver tous, il suffit de faire un arbre.
On remarque que le nombre de ces diviseurs est le nombre total de sous-branches de l'arbre, qui est $4 \times 5 = 20$.
La liste des diviseurs de 648 est : {1 ; 2 ; 4 ; 8 ; 3 ; 6 ; 12 ; 24 ; 9 ; 18 ; 36 ; 72 ; 27 ; 54 ; 108 ; 216 ; 81 ; 162 ; 324 ; 648}

Propriété

Si $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, le nombre de diviseurs est $(\alpha_1 + 1) \times \cdots (\alpha_k + 1)$

IV Liste des nombres premiers inférieurs à 1000 :

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997		