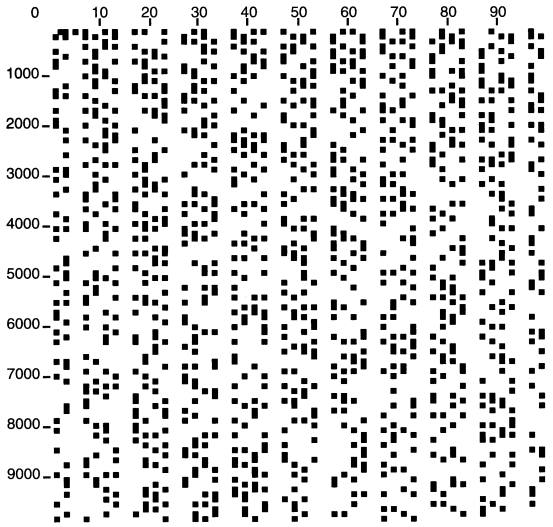
Les nombres premiers



Le crible d'Ératosthène appliqué aux 10 000 premiers entiers, disposés en un pavé de 100×100. On observe l'alternance d'une colonne vide sur deux, correspondant aux nombres pairs, et trouées de trois colonnes vides pour chaque dizaine (multiples de 2 et de 5).

Information [a]

«Les mathématiciens ont tenté, en vain jusqu'à ce jour, de découvrir une régularité dans la suite des nombres premiers, et nous avons de bonnes raisons de croire qu'il y a là un mystère que l'esprit humain ne pénétrera jamais. Il suffit d'ailleurs, pour s'en convaincre, de jeter un regard sur une table de nombres premiers (que certains ont pris la peine de calculer jusqu'à plusieurs centaines de milliers) ; on est alors instantanément convaincu qu'il ne règne ni ordre ni règle.»

Leonard Euler *(1707-1783)*

«Le problème de la distinction entre nombres premiers et nombres composés, et celui de la décomposition d'un nombre en produit de facteurs premiers sont les plus importants et les plus utiles de toute l'arithmétique. [...] L'honneur de la science semble exiger qu'on cultive avec zèle tout progrès dans la solution de ces légantes et célèbres questions.»

Carl Friedrich Gauss *(1777-1855)*

a. D'après l'ouvrage «Merveilleux nombres premiers» de Jean-Paul Delahaye.

Définition 1

Un nombre entier supérieur à 1 dont les seuls diviseurs sont 1 et lui-même est dit **premier** [a].

a. Par convention, 0 et 1 ne sont pas premiers. Un nombre premier ne possède que deux diviseurs.

Construction de la liste des nombres premiers par la méthode du crible d'Erathostène

Cette méthode permet d'établir la liste de nombres premiers inférieurs à un nombre entier n donné. Son principe est très simple. On écrit la liste de tous les nombres entiers de 1 jusqu'à n, on barre 1 qui n'est pas premier, on garde 2 qui est premier et on barre tous les nombres multiples de 2, on garde 3 et on barre tous ses multiples, puis on recherche à partir de 3 le premier nombre non barré, on le garde et on élimine, en les barrant, tous les multiples de ce nombre, et on continue ainsi jusqu'à épuiser toute la liste. Les nombres non barrés constituent la liste des nombres premiers inférieurs ou égaux à n. Avant d'écrire plus précisément cet algorithme, il nous faut choisir une représentation informatique qui traduit le fait qu'un nombre soit barré ou non. Pour cela on peut utiliser un tableau de n éléments indexés de 1 jusqu'à n. Les composantes de ce tableau pouvant avoir pour valeur soit 0 soit 1. Ainsi la valeur de la composante de rang k nous indiquera si le nombre k est premier ou non : la valeur 1 signifie oui, la valeur 0 signifiant non.

Exercice 1

Utiliser cette méthode pour dresser la liste des nombres premiers inférieurs à 100 avec la grille ci-contre.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

```
Variables : n, k, l (nombres entiers), tab (listes)
Entrée : n
début
    Pour k variant de 1 à n
        tab[k]←1
    FinPour
    tab[1]←0
    Pour k variant de 2 à n
        //On barre les multiples de k
        Si tab[k] = 1 alors
            l←2
            Tant que l * k ⩽ n
                tab[l * k]←0
                l←l + 1
            FinTantque
        FinSi
    FinPour
    Pour k variant de 2 à n
        Si tab[k] = 1 alors
            //On affiche la liste des nombres premiers
            Afficher k
        FinSi
    FinPour
fin
```

Algorithme 1 : Crible d'Érathostène

Exercice 2

Programmer cet algorithme avec Algobox.

Remarque

On peut écrire à partir de cet algorithme une version un peu plus performante en tenant compte des remarques suivantes :

- On peut passer d'un multiple m de k au multiple suivant en ajoutant k, une addition est plus rapide qu'une multiplication.
- Il est inutile d'examiner les multiples m de k inférieurs à k^2, car ils ont été déjà barrés.
- Il est inutile de chercher à barrer des nombres plus grands que $\sqrt{n}$, car tous ceux qui ne sont pas premiers l'ont déjà été. En effet un nombre plus grand que $\sqrt{n}$ qui n'est pas premier a forcément un facteur premier plus petit que $\sqrt{n}$, donc il aura été barré lorsque les multiples de ce facteur l'ont été.

Exercice 3

Modifier votre programme en tenant compte des remarques ci-dessus.

Décomposition d'un entier n en produit de facteurs premiers

On admet (théorème fondamental de l'arithmétique) qu'un nombre entier se décompose de manière unique en un produit de facteurs premiers. Le principe de la décomposition est très simple. Il consiste à essayer de diviser n par les nombres premiers successifs. Lorsqu'un nombre premier p divise n, il faut continuer à diviser n par ce nombre tant que cela est possible afin de connaître l'exposant de p.

Exercice 4

Décomposer les nombres 450 et 1 176 en produit de facteurs premiers.

Voici l'algorithme, il retourne la liste des nombres premiers p_1, p_2, ... , p_r et de leur exposant respectif e_1, e_2, ... , e_r tel que n soit égal à $p_1^{e_1}$, $p_2^{e_2}$, ... , $p_r^{e_r}$.

Variables : n, k, l (nombres entiers), P, F, E (listes)
Entrée : n
début
  $P \leftarrow$la liste des nombres premiers inférieurs ou égaux à n;
  $F \leftarrow rien$; //On initialise la liste des facteurs F avec la liste vide
  $E \leftarrow rien$; //On initialise la liste des exposants E avec la liste vide
  $k \leftarrow 1$;
  Tant que $n \neq 1$
    Si $P[k]$ ne divise pas n **alors**
      $k \leftarrow k+1$;
    FinSi
    Sinon
      $l \leftarrow 0$;
      Tant que $P[k]$ divise n
        $n \leftarrow n/P[k]$;
        $l \leftarrow l+1$;
      FinTantque
      $F \leftarrow F, P[k]$; //$P[k]$ est un facteur premier on l'ajoute à la liste F
      $E \leftarrow E, l$; //On ajoute son exposant l à la liste E des exposants
    FinSi
  FinTantque
  retourner F E;
fin

Algorithme 2 : Décomposition d'un entier n en produit de facteurs premiers