Nombres premiers : de Euclide à Fermat

Hervé Stève

herve.steve@hotmail.fr

Kafemath du 24/05/2012

PLAN

1. Nombres
2. Euclide et le Théorème fondamental
3. Infinité
4. Crible d'Eratosthène
5. Quelques propriétés
6. Petit théorème de Fermat

Les nombres

- nombres entiers naturels : 1, 2, …,n ,n+1, …
- objet physique → objet mathématique
  - objet « chaise » défini :

    la chaise
  - objet « chaise » indéfini :

    une chaise → 1 est le nombre de chaises
  - plusieurs objets « chaises » → n chaises
  - comptage « à l'œil nu » : n = 2 , 3 , 4
  - comptage avec une méthode de calcul : n > 4
    - 1 par 1 avec un doigt ou les doigts
    - 5 par 5 avec des tas, des bâtons …

Les diviseurs

- entiers qui divisent un nombre entier n
- diviseurs de 12 ?

  Réponse : {1, 2, 3, 4, 6, 12} 6 diviseurs

  12 = 3 x 4 = 2 x 6 = 2 x 2 x 3 = 1 x 12
- diviseurs de 13 = {1, 13} 2 diviseurs

  13 = 1 x 13
- diviseurs de 1 = {1} 1 diviseur

  1 = 1 x 1 = 1 x 1 x 1 = 1 x 1 x … x 1
- diviseurs de 0 = {0,1, …} infinité de diviseurs

  0 = n x 0

Nombres premiers : définition

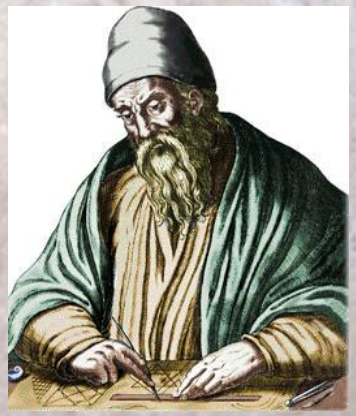
Un entier p > 1 est premier s'il n'est divisible seulement par 1 et par lui-même

- Donc p a 2 diviseurs = {1, p}
- 1 n'est pas premier : il n'a qu'un diviseur !
- 2 est le seul nombre premier pair
- 2, 3, 5, 7, 11, 13, 17, 19, … début de la liste des nombre premiers
- Nombres premiers entre eux :

  a et b premiers si 1 est le seul diviseur commun

  ex) 10 = 1 x 2 x 5 premier avec 21= 1 x 3 x 7

Euclide (vers 325 – 265 a.j.c.)



- Grec, auteur des Eléments
- Disciple d'Aristote ?
- Enseigne en Egypte (Ptolémée Ier)
- Les Eléments : treize livres (compilation)
  - Les livres 1 à 4 : géométrie plane
  - les livres 5 à 6 : théorie des rapports
  - Les livres 7 à 9 : arithmétique
  - le livre 10 : théorie des nombres irrationnels
  - livres 11 à 13 : géométrie des solides, avec l'étude des propriétés des cinq polyèdres réguliers et une démonstration de leur existence

Les *Éléments* sont remarquables par la clarté avec laquelle les théorèmes sont énoncés et démontrés.

Fondation de la Géométrie Euclidienne

Théorème fondamental (Euclide)

Tout nombre entier > 1 se décompose en un produit unique de facteurs premiers :

$$n = 2^{e_1} \times 3^{e_2} \times \ldots \times p_k^{e_k}$$

ex) $12 = (2 \times 2) \times 3 = \mathbf{2}^2 \times \mathbf{3}$

2 et 3 sont les « atomes » de 12 → premiers

Preuve : existence + unicité (Lemme d'Euclide)

Existence du produit

- Par l'absurde : soit **n** le plus petit nombre qui ne peut être décomposé en facteurs premiers (**n** > 1)
- **n** n'est pas premier (car un nombre premier se décompose en lui-même !)
- Donc **n** = a x b avec a < **n** et b < **n**
- Donc a et b décomposables en nombres premiers => **n** aussi : IMPOSSIBLE

Division euclidienne

Théorème :

À deux entiers naturels ***a*** et ***b***, avec ***b*** non nul, la division euclidienne associe un quotient ***q*** et un reste $0 \leq r < 1$, tous deux entiers naturels, vérifiant : $a = b \times q + r$.

Le couple (q,r) est unique

Lemme d'Euclide

(lemme = résultat intermédiaire)

si un nombre premier ***p*** divise le produit de deux nombres entiers ***b*** et ***c***, alors ***p*** divise ***b*** ou ***c***.

Preuve : la division euclidienne dit que

b =p q + r avec r<p et c = p s + t avec t<p

- Alors le produit bc :

bc=(pq+r)(ps+t)=p(pqs+rs+qt)+rt

- Comme p divise bc alors rt=0 donc

r=0 ou s=0 CQFD

Unicité du produit

- Supposons que **n** a deux décompositions en facteurs premiers :

$n = 2^{e_1} \times 3^{e_2} \times \ldots \times p_k^{e_k} = 2^{f_1} \times 3^{f_2} \times \ldots \times q_l^{f_l}$

- Soit p nombre premier de la première décomposition
- Alors p divise la seconde décomposition et donc l'un de ses facteurs q (Lemme d'Euclide)
- q est premier donc q = p
- On divise n par p, puis on recommence avec un facteur … jusqu'à obtenir 1

Infinité des nombres premiers (Euclide)

Preuve par l'absurde :

soit L = liste finie des k nombres premiers jusqu'à p_k

$L = \{2, 3, 5, \ldots, p_k\}$

soit n(*) = $2 \times 3 \times 5 \times \ldots \times p_k + 1$: n n'est pas divisible par 2, 3, 5, … p_k car le reste de n par p_k est 1

$\rightarrow$ donc n divisible par p premier > p_k

$\rightarrow$ donc la liste n'est pas finie

(*) n = 3, 7, 31, 211, 2311 premiers

mais n = 30031 = 59 x 509

Test si premier

- Très difficile si nombre n très grand
- Astuce :

test de divisibilité jusqu'à p_k plus proche > $\sqrt{n}$

ex) n=101 : test sur 2,3,5,7 et 11

sur 2 ? non car n impair

sur 3 ? non car il suffit de tester sur s=1+0+1=2

Sur 5 ? non car unité différent de 0 et 5

sur 7 ? non 7 x 14 = 98 et 7 x 15 = 105

sur 11 ? non 11 x 9 = 99 et 11 x 10 = 110

donc n est premier

Eratosthène (vers 276-194 av J.C.)

- Grec, né à Cyrène (Libye actuelle)
- Bibliothèque d'Alexandrie (vers -245 sous Ptolémée III)
- Maths : crible, duplication du cube ($C^3=2c^3$)
- Astronomie : calcul de la circonférence de la terre 39 375 km (proche de 40 075,02 km), Inclinaison de l'écliptique sur l'équateur, …
- Géographie, géométrie

Crible d'Eratosthène

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

soit 26 nombres premiers jusqu'à 100

Intervalles sans nombres premiers

- Notation factorielle : n! = 2 x 3 x 4 x … x n

  2!=2 ; 3!=6 ; 4!=24 ; … ; 10!=3 628 800

- Pour tout entier n > 2, pas de nombre premiers entre n!+2 et n!+n

en effet : n!+k divisible par k, pour k=2,…,n

Exemple : entre 3 628 802 et 3 628 810

Donc il existe une suite de 1000 entiers consécutifs non premiers !

jumeaux

- Jumeaux : $\{p_i , p_i+2\}$

{2, 3} seul couple premiers consécutifs

ex) {3,5}, {5,7}, {11,13}, …, {881,883}, …

un seul triplé {3, 5, 7}

le plus grand connu > 100000 chiffres (août 1979)

Infinité de jumeaux ?

Pierre de Fermat (1607-1665)

- Français, né à Beaumont-de-Lomagne (Montauban)
- Avocat à Bordeaux => conseiller à la Cour
- Lien avec le milieu scientifique
- Optique : principe de Fermat

« La lumière se propage d'un point à un autre sur des trajectoires telles que la durée du parcours soit extrémale »

- Maths : ne donne pas les démonstrations !
  - Méthodes des tangentes
  - Petit théorème : test de primalité (voir plus loin)
  - Méthode de la descente infinie
  - Le dernier théorème … démontré en 1995 !

Petit Théorème de Fermat

(Démontré par Euler en 1736)

$a^p - a$ divisible par p premier

- Formule du binôme de Newton :

$$(a+1) = a+1$$

$$(a+1)^2 = a^2 + 2a + 1$$

$$(a+1)^3 = a^3 + 3a^2 + 3a + 1$$

$$\vdots$$

$$(a+1)^p = a^p + C_p^1 a^{p-1} + C_p^2 a^{p-2} + \ldots + C_p^{p-1} a + 1$$

$$\text{avec } C_p^k = \frac{p(p-1)(p-2)\ldots(p-k+1)}{k!}$$

Petit théorème

- Preuve petit théorème :

Par récurrence : supposons vrai pour a, démontrons le pour a+1. Ainsi :

$$(a+1)^p-(a+1)=\underbrace{a^p-a}_{\text{divise } p}+\underbrace{[(a+1)^p-a^p-1]}_{\text{divise } p \text{ en effet}}$$

d'après la formule du binôme on a :

$$(a+1)^p-a^p-1=C_p^1a^{p-1}+C_p^2a^{p-2}+\ldots+C_p^{p-1}a$$

avec p divise les coefficients C_p^k pour k=1,…,p-1

Nombres premiers suite …

- Mersenne, Euler, Goldbach
- John Napier : les logarithmes et densité
- Gauss : arithmétique modulaire
- Riemann, Poincaré : nombres complexes et fonctions analytiques
- Hardy/Littlewood/Ramanujan
- Récemment : cryptographie (1975)

Factorisation des nombres premiers

Bibliographie

- « les nombres premiers » Enrique Gracian chez RBA (2011)
- « dans la jungle des nombres premiers » John Derbyshire chez Dunod (2007)
- « les Nombres premiers, entre l'ordre et la chaos » Gérald Tennenbaum, Michel Mendès France chez Dunod (2011 réédition)
- « merveilleux nombres premiers » [Broché] Jean-Paul Delahaye chez Belin
- « Le petit livre des grands nombres » John Gribbin, Mary Gribbin Collection: Hors collection, Dunod
- « La Symphonie des nombres premiers » [POINTS – Science Poche] Marcus Du Sautoy (Auteur), Raymond Clarinard (Traduction)
- « Comment faire du calcul un jeu d'enfant : Sommes, différences, produits, quotients, multiples et diviseurs, nombres premiers pour pratiquer le calcul mental... et se jouer du calcul » de APMEP et Nicolas Dahan (Broché – 2007)
- « La nature et les nombres » de Ian Stewart, Paris Hachette 2000 Editeur espagnol