LES NOMBRES DE FERMAT

Notions réinvesties : congruences, tout entier admet au moins un diviseur premier, petit théorème de Fermat, théorème de Gauss

En 1640, dans une lettre adressée à Bernard Frénicle de Bessy, Pierre de Fermat énonce son petit théorème et explique que tous les nombres de la forme $2^{2^n}+1$ sont premiers.
En effet, en notant F_n ces nombres : $F_0=3$ (premier)
$F_1=5$ (premier) $F_2=17$ (premier) $F_3=257$ (premier) $F_4=65\,537$ (premier) …

… Il s'agira de la seule conjecture erronée de Fermat.

On rappelle la liste des nombres premiers inférieurs à $1\,000$:

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

A. Une condition nécessaire

Soit $k \in \mathbb{N}$, $k \geqslant 2$.
Démontrons le théorème suivant :

> Si 2^k+1 est premier, alors k est une puissance de 2.

Supposons que 2^k+1 est premier, puis supposons par l'absurde que k n'est pas une puissance de 2.

1. Justifier que k admet un diviseur impair, noté q, tel que $q \geqslant 3$.

2. a) On note donc $k=qk'$.
En utilisant la formule de factorisation ci-dessous[1], démontrer que $2^{k'}+1$ est un diviseur de 2^k+1.

b) En déduire que 2^k+1 n'est pas premier et conclure.

DIFFÉRENCE DE PUISSANCES

$$a^n-b^n=(a-b)\left(\sum_{i=0}^{n-1} a^{n-1-i}b^i\right) \quad i.e. \quad a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\ldots+ab^{n-2}+b^{n-1})$$

Remarque : Fermat avait donc conjecturé que la réciproque est vraie.

1 Facilement démontré par récurrence

B. Est-ce suffisant ?

1. Vérifier que F_4 est bien premier.

2. Calculer F_5. En utilisant un logiciel de calcul formel, pouvez-vous déterminer si ce nombre est premier ou composé ?

C. Quelques propriétés des nombres de Fermat

LE DERNIER CHIFFRE

1. Émettre une conjecture sur le dernier chiffre de F_n.

2. Démontrer que pour tout entier naturel n : $F_{n+1}=(F_n-1)^2+1$.

3. En déduire une démonstration de votre conjecture.

LE THÉORÈME DE GOLBACH

1. Démontrer que pour tout entier naturel n : $F_{n+1}-2=F_n(F_n-2)$.

2. En déduire que pour tout entier naturel non nul : $F_n=\left(\prod_{i=0}^{n-1} F_i\right)+2$.

Le théorème de Golbach affirme :

> **THÉORÈME DE GOLBACH**
> Deux nombres de Fermat distincts sont premiers entre eux.

3. Démontrer ce théorème.

LE THÉORÈME D'EULER et LA FACTORISATION HISTORIQUE DE F_5

En 1729, Christian Golbach signale la conjecture de Fermat au jeune Leonhard Euler.
En 1732, Euler a 25 ans et démontre que F_5 est composé !
Il ne dévoilera la construction de sa preuve que quinze ans plus tard. En voici les principales étapes.

Admettons[2] le théorème démontré par Euler :

> **THÉORÈME D'EULER**
> Tout facteur premier d'un nombre de Fermat F_n est de la forme $k\,2^{n+1}+1$
> où k est un entier admettant un diviseur impair supérieur ou égal à 3.

On rappelle que $F_5=2^{32}+1$.

1. Démontrer qu'un diviseur premier de F_5 est nécessairement de la forme $64k+1$.

2. En utilisant le théorème d'Euler, tester les différentes valeurs de k possibles entre 3 et 10.
En déduire que F_5 est composé.

3. En 1880, T. Clausen et F. Landry ont démontré que F_6 est divisible par $1071\times 2^8+1$, c'est-à-dire 274 177. Avec la méthode utilisée par Euler pour trouver 641, cela correspond à quelle valeur de k ?

2 Démonstration accessible ici, elle utilise le petit théorème de Fermat ainsi que le théorème de Gauss.

Ce que l'on sait (ou ne sait pas) en mars 2017

• De nos jours, les seuls nombres de Fermat premiers sont F_0, F_1, F_2, F_3 et F_4.
Il est probable que les seuls nombres premiers de cette forme soient 3, 5, 17, 257 et 65 537, car Boklan et Conway[3] ont pré-publié en mai 2016 une analyse très fine[4] estimant la probabilité d'un autre nombre premier à moins d'un sur un milliard !

• Conjectures non démontrées : - il n'existe aucun autre nombre de Fermat premiers.
- il existe une infinité de nombres de Fermat composés.

• On connaît toutes les factorisations de F_5 à F_{11}.

• On connaît 292 nombres de Fermat composés et 336 facteurs premiers.

• La dernière découverte date du 28 janvier 2017 : $3\,370\,842\,847\times 2^{3\,058}+1$ divise $F_{3\,056}$.

Sur F_{11}

F_{11} est le plus grand nombre de Fermat dont on connaît la factorisation complète.
Cette factorisation a utilisé environ 360 millions de multiplications modulaires…
$F_{11}=319\,489\times 974\,849\times 167\,988\,556\,341\,760\,475\,137\times 3\,560\,841\,906\,445\,833\,920\,513\times p_{564}$
où $p_{564}=173\,462\,447\,179\,147\,555\,430\ \ldots\ 382\,441\,723\,306\,598\,834\,177$ est un nombre à 564 chiffres.

Sur F_{12}

F_{12} est composé mais on ne connaît pas sa factorisation complète :
$F_{12}=114\,689\times 26\,017\,793\times 63\,766\,529\times 190\,274\,191\,361\times 1\,256\,132\,134\,125\,569\times C_{1187}$
avec $C_{1187}=568\,630\,647\,535\,356\,955\,169\,033\,410\,940\,867\,804\,839\,360\,742\,060\,818\,433\times C_{1133}$
où C_{1133} est un nombre non connu de 1133 chiffres.
Depuis le 27 mars 2010, on connaît donc 6 des diviseurs premiers de F_{12}, mais toujours pas sa factorisation complète.
Pour vous donner une idée de l'évolution des recherches sur F_{12}, les facteurs connus ont été découverts en 1877, 1903, 1903, 1974, 1986 et 2010.

Sur F_{20}

F_{20} est le plus petit nombre de Fermat dont on sait qu'il est composé mais dont on ne connaît aucun diviseur premier !
Avant 2010, le plus petit tel nombre était F_{14} : le 3 février 2010, un diviseur à 54 chiffres de F_{14} a été découvert par Tapio Rajala de l'université de Jyväskylä en Finlande.

3 Je vous invite à voir l'excellente vidéo de Eljj qui explique ce qu'est la « suite de Conway », dont parle Bernard Werber dans son best-seller « Le jour des fourmis » : https://youtu.be/IsKBRj6_VSs
La conclusion est géniale, et vous la comprendrez en visualisant la vidéo :
« le théorème cosmologique explique finalement que dans un univers régit uniquement par la suite audioactive, n'importe quelle graine finit par engendrer la création de l'Univers tout entier. Ça a quand même plus de gueule qu'une théorie des Bogdanov ! »

4 https://arxiv.org/pdf/1605.01371v2.pdf

Les informations connues sur les nombres de Fermat F_i pour i entre 5 et 100

n	F_n composé	Nb de facteurs premiers connus	Factorisation complète	Année de découverte des facteurs
5	X	2	X	1732 | 1732
6	X	2	X	1855 | 1855
7	X	2	X	1970 | 1970
8	X	2	X	1980 | 1980
9	X	3	X	1903 | 1990 | 1990
10	X	4	X	1953 | 1962 | 1995 | 1995
11	X	5	X	1899 | 1899 | 1988 | 1988 | 1988
12	X	6		1877 | 1903 | 1903 | 1974 | 1986 | 2010
13	X	4		1974 | 1991 | 1991 | 1995
14	X	1		2010
15	X	3		1925 | 1987 | 1997
16	X	2		1953 | 1996
17	X	2		1978 | 2011
18	X	2		1903 | 1999
19	X	3		1962 | 1963 | 2009
20	X	0		
21	X	1		1963
22	X	1		2010
23	X	1		1878
24	X	0		
25	X	3		1963 | 1985 | 1987
26	X	1		1963
27	X	2		1963 | 1985
28	X	1		1997
29	X	1		1980
30	X	2		1963 | 1963
31	X	1		2001
32	X	1		1963
33				
34				
35				
36	X	2		1886 | 1981
37	X	1		1991
38	X	2		1903 | 1963
39	X	2		1956 | 2012
40				
41				
42	X	2		1963 | 2011
43	X	1		2000
44				
45				
46				
47				
48	X	1		2001

n	F_n composé	Nb de facteurs premiers connus	Factorisation complète	Année de découverte des facteurs
49				
50				
51				
52	X	3		1963 | 1982 | 2010
53				
54				
55	X	1		1956
56				
57				
58	X	1		1957
59				
60				
61	X	1		1986
62	X	1		1977
63	X	1		1956
64	X	1		1986
65	X	1		2013
66	X	1		1977
67				
68				
69				
70				
71	X	1		1977
72	X	1		1986
73	X	1		1906
74				
75	X	1		1982
76				
77	X	2		1957 | 1998
78				
79				
80				
81	X	1		1957
82				
83	X	1		2005
84				
85				
86	X	1		2012
87				
88	X	1		2001
89				
90	X	1		2001
91	X	1		1977
92				
93	X	1		1979
94	X	1		2001

n	F_n composé	Nb de facteurs premiers connus	Factorisation complète	Année de découverte des facteurs
95				
96	X	1		2008
97				
98				
99	X	1		1979
100				

Pour des informations et des mises à jour sur les découvertes liées aux nombres de Fermat :

http://www.prothsearch.com/fermat.html
http://www.fermatsearch.org/news.html
http://villemin.gerard.free.fr/Wwwgvmm/Decompos/Fermatva.htm