Démonstrations de primalité
Nombres de Mersenne et de Fermat

1 Introduction

Le tableau suivant montre l'évolution du record du plus grand nombre premier connu, avant l'avénement de l'ordinateur :

1588	$2^{17}-1=131071$	6 chiffres	Cataldi
1588	$2^{19}-1=524287$	6 chiffres	Cataldi
1772	$2^{31}-1$	10 chiffres	Euler
1867	$\left(2^{59}-1\right)/179951$	13 chiffres	Landry
1876	$2^{127}-1$	39 chiffres	Lucas

Dans cet exposé, nous montrerons comment retrouver en Terminale S les résultats de Cataldi et d'Euler en utilisant le théorème de Fermat. Nous montrerons ensuite comment, par une méthode similaire, Euler aurait pu trouver un nombre premier de 7 chiffres dès 1732.

Le premier test de primalité non trivial est basé sur le théorème suivant.

Théorème 1. *Tout entier non premier plus grand que 2 a un diviseur premier inférieur ou égal à sa racine carrée.*

Application Si un entier plus grand que 2 n'a pas de diviseur premier inférieur ou égal à sa racine carrée, alors il est premier.

Exemple 1 L'entier 37901 est-il premier ? Et l'entier 37907 ?

2 Nombres de Mersenne

2.1 Introduction

On cherche des nombres premiers de la forme a^n-1, avec a et n entiers supérieurs ou égaux à 2.
Le théorème suivant permet d'éliminer beaucoup de possibilités.

Théorème 2. *Pour tous entiers a et n supérieurs ou égaux à 2, a^n-1 est divisible par $a-1$.*

On peut aborder ce théorème à différents niveaux :
- en terminale S ou L : à l'aide des congruences,
- en première : en utilisant le calcul de la somme $1+a+a^2+\cdots+a^{n-1}$,
- dans les classes antérieures : en développant le produit $(1+a+a^2+\cdots+a^{n-1})(a-1)$, éventuellement sur un exemple, ou bien en montrant que 10^n-1 est divisible par 9.

Exemple 2 Les entiers $20^{13}-1$ et $2^{35}-1$ ne sont pas premiers.

Plus généralement

Corollaire 1. *Si $a>2$ alors a^n-1 n'est pas un nombre premier.*

Définition 1. *Les entiers de la forme $M_n=2^n-1$ sont appelés nombres de Mersenne.*

Du théorème, on peut également déduire le corollaire

Corollaire 2. *Si n n'est pas premier alors 2^n-1 n'est pas un nombre premier.*

Exemple 3 Parmi les nombres de Mersenne M_2, M_3, M_4,...M_{16}, quels sont ceux qui sont premiers ?

2.2 Les diviseurs premiers des nombres de Mersenne

Pour montrer que M_{17} est premier, il faudrait tester tous les diviseurs premiers jusqu'à 362.
Pour montrer que M_{19} est premier, il faudrait tester tous les diviseurs premiers jusqu'à 724.
On peut accélerer le processus en utilisant le théorème de Fermat

Théorème 3. *Soit n un entier naturel. Si n est un nombre premier, alors pour tout entier a premier avec n, on a $a^{n-1} \equiv 1 \pmod{n}$ (c'est-à-dire n divise $a^{n-1} - 1$).*

Remarque Le théorème de Fermat peut être utilisé pour montrer qu'un entier *n'est pas premier* : si il existe un entier a premier avec n tel que $a^{n-1} \not\equiv 1 \pmod{n}$ alors n n'est pas premier.

Exemple 4 L'entier 37901 est-il premier ?
On calcule $2^{37900} \pmod{379001}$ en utilisant l'*exponentiation rapide* :

$$\begin{aligned}
2^2 &\equiv 4 && \pmod{37901}\\
2^4 &\equiv 16 && \pmod{37901}\\
2^8 &\equiv 256 && \pmod{37901}\\
2^{16} &\equiv 27635 && \pmod{37901}\\
2^{32} &\equiv 25976 && \pmod{37901}\\
2^{64} &\equiv 1073 && \pmod{37901}\\
2^{128} &\equiv 14299 && \pmod{37901}\\
2^{256} &\equiv 23407 && \pmod{37901}\\
2^{512} &\equiv 28694 && \pmod{37901}\\
2^{1024} &\equiv 22213 && \pmod{37901}\\
2^{2048} &\equiv 22151 && \pmod{37901}\\
2^{4096} &\equiv 455 && \pmod{37901}\\
2^{8192} &\equiv 17520 && \pmod{37901}\\
2^{16384} &\equiv 28102 && \pmod{37901}\\
2^{32768} &\equiv 17168 && \pmod{37901}
\end{aligned}$$

On a $37900 = 32768 + 4096 + 1024 + 8 + 4$ donc

$$2^{37900} \equiv 17168 \times 455 \times 22213 \times 256 \times 16 \equiv 12802 \pmod{37901}$$

donc 37901 n'est pas un nombre premier.
Malheureusement, le théorème de Fermat ne permet pas de montrer directement qu'un entier est premier.

Théorème 4. *Soit a et p deux entiers supérieurs ou égaux à 2. On suppose qu'il existe un entier naturel non nul k tel que $a^k \equiv 1 \pmod{p}$.*
Soit k_0 le plus petit entier naturel non nul tel que $a^{k_0} \equiv 1 \pmod{p}$.
L'entier k est alors un multiple de k_0. On dit que k_0 est l'ordre de a modulo p.

Corollaire 3. *Soit p et q deux nombres premiers. Si q divise M_p alors il existe un entier k tel que $q = 2kp+1$.*
Autrement dit, si p est premier alors les diviseurs premiers de M_p sont de la forme $2kp + 1$.

Exemple 5 Parmi les nombres de Mersenne M_{17}, M_{18}, $\ldots M_{30}$, quels sont ceux qui sont premiers ?

En 1772, Euler démontre que M_{31} est premier en utilisant un raffinement de cette méthode.

3 Nombres de Fermat

3.1 Introduction

On cherche des nombres premiers de la forme $a^m + 1$, avec $a \geqslant 2$ pair et $m \geqslant 1$.
Le théorème suivant permet d'éliminer beaucoup de possibilités.

Théorème 5. *Pour tous entiers a et m supérieurs ou égaux à 2,*
si m est impair alors $a^m + 1$ est divisible par $a + 1$.

Ce résultat est plus difficile à aborder avant la première...

Exemple 6 Les entiers $6^3 + 1$ et $2^{12} + 1$ ne sont pas premiers.

Plus généralement

Corollaire 4. *Si m est divisible par un nombre impair strictement plus grand que 1 alors $a^m + 1$ n'est pas un nombre premier.*

On en déduit en particulier que si $2^m + 1$ est premier alors m est une puissance de 2.

Définition 2. *Les entiers de la forme $F_n = 2^{2^n} + 1$ sont appelés nombres de Fermat.*

Exemple 7 Parmi les nombres de Fermat F_0, F_1, F_2 et F_3, quels sont ceux qui sont premiers ?

3.2 Les diviseurs premiers des nombres de Fermat

Théorème 6. *Soit p un nombre premier. Si p divise F_n alors il existe un entier k tel que $p = k \times 2^{n+1} + 1$.*
Autrement dit, les diviseurs premiers de F_n sont de la forme $k \times 2^{n+1} + 1$.

Exemple 8

1. Montrer que F_4 est un nombre premier.
2. Décomposer F_5 en facteurs premiers.

Table de nombres premiers

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	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617