Nombres de Mersenne et de Fermat
Notes et solutions

1 Introduction

Démonstration du théorème 1. On admet que tout entier naturel strictement supérieur à 1 a un diviseur premier. Soit n un entier non premier, et p son plus petit diviseur premier ($1 \leqslant p \leqslant n$). On note q l'entier tel que $n = pq$.

Si $p > \sqrt{n}$ alors $q < \sqrt{n} \leqslant p$. L'entier q a un diviseur premier strictement inférieur à p, donc n a un diviseur premier strictement inférieur à p, ce qui est impossible.

On a donc $p \leqslant \sqrt{n}$. □

Exemple 1

1. L'entier 37901 n'est pas premier car $37901 = 151 \times 251$.
   Il faut 36 divisions pour trouver le facteur 151.
2. L'entier 37907 est premier : il n'est divisible par aucun des 44 nombres premiers plus petits que sa racine carrée.

2 Nombres de Mersenne

2.1 Introduction

Démonstration du théorème 2. Plusieurs approches sont possibles :

- Congruence : $a \equiv 1 \pmod{(a-1)}$ donc $a^n \equiv 1 \pmod{(a-1)}$.
- Récurrence : on utilise l'égalité $a^{n+1} - 1 = a \times (a^n - 1) + a - 1$.
- Suites géométriques : $1 + a + a^2 + \cdots + a^{n-1} = \dfrac{a^n - 1}{a - 1}$.

□

Exemple 2

1. L'entier $20^{13} - 1$ n'est pas premier car il est divisible par $20 - 1 = 19$.
2. L'entiers $2^{35} - 1$ n'est pas premier car $2^{35} - 1 = \left(2^5\right)^7 - 1$ donc il est divisible par $2^5 - 1 = 31$ (et aussi par $2^7 - 1 = 127$ car $2^{35} - 1 = \left(2^7\right)^5 - 1$).

Démonstration du corollaire 1. On a $a^n - 1$ divisible par $a - 1$

Si on a $a > 2$ (et toujours $n \geqslant 2$), alors $1 < a - 1 < a^n - 1$ donc $a^n - 1$ n'est pas premier. □

Démonstration du corollaire 2. Si $n = pq$ alors $2^n - 1 = (2^p)^q - 1$ est divisible par $2^p - 1$.

Si n n'est pas premier alors il existe un entier p tel que $n = pq$ et $1 < p < n$.

On a alors $1 < 2^p - 1 < 2^n - 1$ donc $2^n - 1$ n'est pas premier. □

Exemple 3

- Les entiers 4, 6, 8, 9, 10, 12, 14, 15 et 16 ne sont pas premiers donc les nombres de Mersenne correspondants ne sont pas premiers.
- Parmi les nombres de Mersenne restant, $M_2 = 3$ est premier, $M_3 = 7$ est premier, $M_5 = 31$ est premier, $M_7 = 127$ est premier.
- $M_{11} = 2047 = 23 \times 89$ n'est pas premier (9 divisions pour trouver le facteur 23).
- $M_{13} = 8191$ est premier car il n'est divisible par aucun des 24 nombres premiers inférieurs à sa racine carrée.

2.2 Les diviseurs premiers des nombres de Mersenne

Exemple 4 On peut remarquer que le théorème de Fermat seul ne permet pas de démontrer la primalité. Par exemple pour l'entier 341, on calcule $2^{340} \pmod{341}$ en utilisant l'*exponentiation rapide* :

$$\begin{aligned}
2^2 &\equiv 4 && \pmod{341}\\
2^4 &\equiv 16 && \pmod{341}\\
2^8 &\equiv 256 && \pmod{341}\\
2^{16} &\equiv 64 && \pmod{341}\\
2^{32} &\equiv 4 && \pmod{341}\\
2^{64} &\equiv 16 && \pmod{341}\\
2^{128} &\equiv 256 && \pmod{341}\\
2^{256} &\equiv 64 && \pmod{341}
\end{aligned}$$

On a $340 = 256 + 64 + 16 + 4$ donc $2^{340} \equiv 64 \times 16 \times 64 \times 16 \equiv 1 \pmod{341}$.
On a donc $2^{340} \equiv 1 \pmod{340}$ mais 341 n'est pas premier !

Démonstration du théorème 4. Soit k_0 le plus petit entier naturel non nul tel que $a^{k_0} \equiv 1 \pmod{p}$.
On écrit la division euclidienne de k par k_0 : $k = q \times k_0 + r$ avec $0 \leqslant r < k_0$.
On a $a^k \equiv a^{q \times k_0 + r} \equiv \left(a^{k_0}\right)^q \times a^r \equiv a^r$.
Si $a^k \equiv 1 \pmod{p}$ alors $a^r \equiv 1 \pmod{p}$ avec $0 \leqslant r < k_0$. Or k_0 est le plus petit entier naturel non nul vérifiant cette équivalence. Donc $r = 0$ et k est un multiple de k_0. □

Démonstration du corollaire 3. Soit p et q deux nombres premiers. Si q divise M_p alors $2^p \equiv 1 \pmod{q}$.
L'ordre de 2 modulo q est donc un diviseur de p. Or p est premier donc l'ordre de 2 est p.
D'autre part, q est un nombre premier et $q \neq 2$ donc d'après le théorème de Fermat, $2^{q-1} \equiv 1 \pmod{q}$.
L'entier $q - 1$ est donc un multiple de p, l'ordre de 2 modulo q.
De plus, $q - 1$ est pair donc il existe un entier k tel que $q - 1 = 2kp$, c'est-à-dire $q = 2kp + 1$. □

Exemple 5 On peut déjà remarquer que pour M_{11}, les facteurs 23 et 89 sont bien de la forme $2k \times 11 + 1$.

- L'entier $M_{17} = 131\,071$ est premier car il n'est divisible par aucun des 4 nombres premiers de la forme $2k \times 17 + 1$ inférieurs à sa racine carrée (103, 137, 239 et 307).
- L'entier $M_{19} = 524\,287$ est premier car il n'est divisible par aucun des 7 nombres premiers de la forme $2k \times 17 + 1$ inférieurs à sa racine carrée (191, 229, 419, 457, 533, 571 et 647).
- L'entier M_{23} n'est pas premier car il est divisible par $47 = 2 \times 23 + 1$ (une seule division pour trouver le facteur).
- L'entier M_{29} n'est pas premier car il est divisible par $233 = 8 \times 29 + 1$ (deux divisions pour trouver le facteur).

Pour montrer que M_{31} est premier, il faudrait effectuer 157 divisions.
Euler démontre que si q divise M_{31} alors q est de la forme $248k + 1$ ou $248k + 63$, ce qui réduit le nombre de divisions à effectuer à 84. Il prouve ainsi en 1772 que M_{31} est premier.

3 Nombres de Fermat

3.1 Introduction

Démonstration du théorème 5. Plusieurs approches sont possibles :

- Congruence : $a \equiv -1 \pmod{(a+1)}$ donc $a^n \equiv -1 \pmod{(a+1)}$ si n est impair.
- Suites géométriques : $1 - a + a^2 + \cdots - a^{n-1} = \dfrac{1-(-a)^n}{1+a} = \dfrac{a^n+1}{a+1}$ si n est impair.

□

Exemple 6

1. L'entier $6^3 + 1$ n'est pas premier car il est divisible par $6 + 1 = 7$.
2. L'entiers $2^{12} + 1$ n'est pas premier car $2^{12} + 1 = \left(2^4\right)^3 + 1$ donc il est divisible par $2^4 + 1 = 17$.

Démonstration du corollaire 4. On suppose que $m = pq$, avec $p > 1$ impair. On a donc $q < m$.

Or $a^m + 1 = (a^q)^p + 1$ est divisible par $a^q + 1$ avec $1 < a^q + 1 < a^m + 1$, donc $a^m + 1$ n'est pas un nombre premier.

□

Exemple 7 Les nombres de Fermat $F_0 = 3$, $F_1 = 5$, $F_2 = 17$ et $F_3 = 257$ sont tous premiers.

3.2 Les diviseurs premiers des nombres de Fermat

Démonstration du théorème 6. Soit p un nombre premier.

Si p divise F_n alors $2^{2^n} \equiv -1 \pmod{p}$ et $2^{2^{n+1}} \equiv 1 \pmod{p}$.

L'ordre de 2 modulo p est donc un diviseur de 2^{n+1}.

Or les diviseurs de 2^{n+1} sont de la forme 2^k, avec $0 \leqslant k \leqslant n+1$.

Si l'ordre était 2^k avec $0 \leqslant k \leqslant n$, alors on aurait $2^{2^n} \equiv 1 \pmod{p}$, ce qui est impossible.

Donc l'ordre de 2 modulo p est 2^{n+1}.

D'autre part, d'après le théorème de Fermat, $2^{p-1} \equiv 1 \pmod{p}$.

Donc $p - 1$ est un multiple de 2^{n+1}. Il existe un entier k tel que $p = k \times 2^{n+1} + 1$. □

Exemple 8

1. Le nombre $F_4 = 65\,537$ est premier car il n'est divisible par aucun des 2 nombres premiers de la forme $k \times 2^5 + 1$ inférieurs à sa racine carrée (97 et 193).
2. Les facteurs premiers éventuels de F_5 sont de la forme $k \times 2^6 + 1 = 64k + 1$.
   Cinq divisions (193, 257, 449, 577, 641) suffisent pour trouver le premier facteur 641 :

$$F_5 = 4\,294\,967\,297 = 641 \times 6\,700\,417$$

   Euler trouve ce facteur en 1732, en utilisant cette méthode, ce qui démontre que la conjecture que Fermat avait faite — tous les F_n sont premiers — est fausse.

   Il aurait pu montrer que 6 700 417 est premier car il n'est divisible par aucun des 7 autres nombres premiers de la forme $64k + 1$ inférieurs à sa racine carrée (641, 769, 1153, 1217, 1409, 1601 et 2113).

   Il aurait alors obtenu un nombre premier de 7 chiffres, le plus grand connu à cette date, avec seulement 12 divisions et une table de nombres premiers jusqu'à 2500.

4 Pour aller plus loin

4.1 Nombres de Mersenne

Diviseurs des nombres de Mersenne

En 1772, Euler démontre que si q premier divise M_p, avec p premier, alors $q \equiv \pm 1 \pmod 8$.
Cela réduit d'environ un facteur 2 le nombre de diviseurs premiers à tester pour un nombre de Mersenne.

Résultats ultérieurs

- Cette méthode permet de trouver la factorisation complète de M_{37}, M_{41}, M_{43}, M_{47} et M_{53} qui ont des facteurs de taille accessible.
- En 1867, Landry trouve le facteur $3050 \times 59 + 1 = 179951$ de M_{59} en effectuant 143 divisions.
  Un peu plus de 1000 divisions supplémentaires lui sont nécessaires pour montrer que $M_{59}/179951$ est premier, ce qui sera le plus grand nombre premier connu pendant 9 ans.
- Il faudrait effectuer plus de six cents mille divisions pour prouver par cette méthode que M_{61} est premier.

4.2 Nombres de Fermat

Diviseurs des nombres de Fermat

On peut améliorer le théorème 6 en utilisant les deux ingrédients suivants :
- Les nombres de Fermat sont premiers entre eux. En effet, on a $F_{n+1} - 2 = F_n \times (F_n - 2)$ et donc :

$$F_{n+1} - 2 = F_n \times F_{n-1} \times \cdots \times F_1 \times F_0$$

- Si p premier divise F_n, avec $n \geqslant 2$ alors il existe un entier k tel que $p = k \times 2^{n+2} + 1$.
  Ce théroème, dû à Lucas en 1878, peut se démontrer comme le théorème 6 en montrant d'abord que F_{n-1} a pour ordre 2^{n+2} modulo p.

On conclut que les diviseurs propre premiers de F_n ($n \geqslant 2$) sont de la forme $k \times 2^{n+2} + 1$, où k est un entier ayant au moins un facteur premier impair.

Résultats ultérieurs

Environ quatre mille divisions seraient nécessaires pour trouver la factorisation complète de F_6 :

$$F_6 = 274\,177 \times 67\,280\,421\,310\,721$$

Cette factorisation sera trouvée en 1855 par Clausen (dans une lettre à Gauss non publiée) puis retrouvée en 1880 par Landry (à 82 ans).

Si Clausen avait prouvé en 1855 que le plus grand facteur est premier (ce qu'il n'a pas fait), ce facteur aurait alors été le plus grand nombre premier connu.