Le théorème de Fermat

1. Remarques et rappels

Si p est **un nombre premier** et si $k \in \mathbb{N}$ et $1 \leqslant k \leqslant p-1$ alors $\mathscr{P}\text{gcd}(p;k)=1$.

Démonstration:

Soit d un diviseur commun de p et k.

$1 \leqslant d \leqslant k < p$ et $d \in D_p = \{1 ; p\}$ donc $d = 1$

Le seul diviseur commun de p et k est 1 donc p et k sont premiers entre eux soit $\mathscr{P}\text{gcd}(p;k)=1$.

a ; b et p sont des entiers naturels non nuls. Si p est premier avec a et si p est premier avec b alors p est premier avec ab , c'est à dire:

Si $\mathscr{P}\text{gcd}(p;a)=1$ et si $\mathscr{P}\text{gcd}(p;b)=1$ alors $\mathscr{P}\text{gcd}(p;ab)=1$

Démonstration:
On utilise le théorème de Bezout.
$\mathscr{P}\text{gcd}(p;a)=1$ donc il existe deux entiers relatifs u et v tels que $up+va=1$
$\mathscr{P}\text{gcd}(p;b)=1$ donc il existe deux entiers relatifs u' et v' tels que $u'p+v'b=1$
On a donc:

$va = 1-up$

$v'b = 1-u'p$

On multiplie membre à membre les deux égalités

$vv'ab = (1-up)(1-u'p)$

$vv'ab = 1-u'p-up+uu'p^2$

$(u+u'-uu'p)p+vv'ab = 1$

On pose $U = u+u'-uu'p$ et $V = vv'$

Donc $Up+Vab = 1$

D'après le théorème de Bezout, p et ab sont premiers entre eux: $\mathscr{P}\text{gcd}(p;ab)=1$

$n \in \mathbb{N}$ et $n \geqslant 2$. $p ; a_1 ; a_2 ; \ldots ; a_n$ sont des entiers naturels non nuls.

Si p est **premier** avec les n nombres $a_1 ; a_2 ; \ldots ; a_n$ alors p est **premier** avec $a_1 \times a_2 \times \ldots \times a_n$

Démonstration:
On peut effectuer un raisonnement par récurrence

Conséquence:

p entier naturel non nul.
Si p est **un nombre premier** avec p est **premier** avec $(p-1)!$

Démonstration:

p est premier donc p est premier avec les nombres: 1; 2; 3; …; (p-1) donc p est premier avec leur produit:

$1\times 2\times 3\times \ldots \times (p-1)=(p-1)!$

2. Le théorème de Fermat

Soit p un nombre premier.

Pour tout entier naturel a premier avec p , on a: $\boxed{a^{p-1}\equiv 1\,(p)}$.

Démonstration:

p est premier avec a donc $a\neq 0$

On considère les $(p-1)$ nombres: $a\,;2a\,;\ldots\,;(p-1)a.$

On effectue la division euclidienne de ces nombres par p , on note $r_1;r_2;\ldots;r_{p-1}$ les $p-1$ restes.

Si $k\in\mathbb{N}$ et $1\leqslant k\leqslant p-1$, alors k est premier avec p , comme a est premier avec p alors ka est premier avec p .
Donc le reste r_k de la division euclidienne de ka par p est non nul et $1\leqslant r_k\leqslant p-1$.

On suppose qu'il existe k et k' tels que $1\leqslant k\leqslant p-1$ et $1\leqslant k'\leqslant p-1$ et $k'<k$ et $r_{k'}=r_k$.

On a $1\leqslant k'<k\leqslant p-1$

$1\leqslant k-k'\leqslant p-1$ (p est premier avec $k-k'$)

$ka=qp+r_k$

$k'a=q'p+r_{k'}$

Donc, $(k-k')a=(q-q')p$

p divise $(k-k')a$

p est premier avec a

D'après le théorème de Gauss, p divise $k-k'$. Or p est premier avec $k-k'$ donc il n'existe pas $k\neq k'$ tel que $r_{k'}=r_k$.

Conséquence:

Les $(p-1)$ restes sont non nuls et distincts 2 à2 donc: $r_1\times r_2\times\ldots\times r_{p-1}=(p-1)!$

Or, on a: $a\times(2a)\times(3a)\times\ldots\times(p-1)a=(p-1)!a^{p-1}$

$a\equiv r_1\,(p)$ $2a\equiv r_2\,(p)$ … $(p-1)a\equiv r_{p-1}\,(p)$

Donc:

$a\times(2a)\times(3a)\times\ldots\times(p-1)a\equiv r_1\times r_2\times\ldots\times r_{p-1}\,(p)$

$(p-1)!a^{p-1}\equiv(p-1)!\,(p)$

$(p-1)![a^{p-1}-1]\equiv 0\,(p)$

p divise $(p-1)![a^{p-1}-1]$

p est premier avec $(p-1)$!

D'après le théorème de Gauss, p divise $(a^{p-1}-1)$ soit $a^{p-1}\equiv 1(p)$

3. Corollaire

Pour tout entier naturel a et tout nombre premier p : $\boxed{a^p\equiv a(p)}$

Démonstration:

$a^p-a=a(a^{p-1}-1)$

Si p divise a le résultat est immédiat.

Si p ne divise pas a alors p et a sont premiers entre eux et donc $a^{p-1}\equiv 1(p)$. Par suite, $a(a^{p-1}-1)\equiv a(p)$.

Donc $a^p\equiv a(p)$.

4. Test de primalité de Fermat

4.1. Nombres pseudos premiers de base 2 (ou nombres de Poulet)

a) Réciproque du théorème de Fermat

$p=341=11\times 31$ (p n'est pas un nombre premier)

$2^{11}=2048$

$2048=6\times 341+2$

Donc, $2^{11}\equiv 2(341)$

Par suite, $2^{341}\equiv(2^{11})^{31}(341)$

Donc, $2^{341}\equiv 2^{31}(341)$

Or, $2^{31}\equiv(2^{11})^2\times 2^9(341)$

$2^{31}\equiv 2^2\times 2^9(341)$

$2^{31}\equiv 2(341)$

Conclusion : $\boxed{2^{341}\equiv 2(341)}$

Et, **la réciproque du théorème de Fermat est fausse**.

b) Définition

On nomme **nombre pseudo premier de base 2** (ou nombre de Poulet) tout entier naturel p supérieur ou égal à 2, non premier tel que $\boxed{2^p\equiv 2(p)}$

(Paul Poulet mathématicien : 1888-1946)

c) Remarques

- Les nombres de Poulet sont :
  341 ; 561 ; 645 ; 1105 ; 1387 ; 1729 ; 1905 ; 2047 ; 2465 ; ...

- On vérifie que 561 est un nombre de Poulet en utilisant le tableur d'OpenOffice.
  $561=3\times11\times17$
  561 n'est pas un nombre premier.
  On veut vérifier que $2^{561}\equiv2(561)$

  A1 : 1 B1 : 2 C1 : =MOD(B1,561)
  A2 : =A1+1 B2 : =C1*B$1 C2 : =MOD(B2,561)
  On étire jusque A561 ; B561 ; C561
  On obtient :
  A561 : 561 B561 : 2 C561 : 2
  Si $2\leqslant p\leqslant561$ alors C*p* est le reste de la division euclidienne de 2*C*$p-1$ par 561.
  On a donc :
  $2^p\equiv2*Cp-1(561)$
  Et, $2^p\equiv Cp(561)$
  Conclusion : $\boxed{2^{561}\equiv2(561)}$
  On peut aussi utiliser le logiciel Xcas et l'instruction $irem(2\wedge561,561)$ qui donne le reste de la division de 2^{561} par 561.
  On obtient $irem(2\wedge561,561)=2$ donc $2^{561}\equiv2(561)$

- Derrick Henry-Lehmer (1905-1991) démontra que le plus petit nombre de Poulet pair était 161038

- Il y a une infinité de nombres de Poulet

4.2. Nombres de Carmichaël

a) Exemples

- On reprend le tableur d'OpenOffice
  On remplace dans B1 2 par 3, on obtient : $3^{561}\equiv3(561)$.
  Ou en utilisant le logiciel Xcas : $irem(3\wedge561,561)=3$
  Donc, 561 est un nombre pseudo premier de base 3.

- De même, on remplace dans B1 2 par 4, et on obtient : $4^{561}\equiv4(561)$
  Ou en utilisant le logiciel Xcas : $irem(4\wedge561,561)=4$
  Donc, 561 est un nombre pseudo premier de base 4.

- On peut vérifier pour tout entier naturel a compris entre 1 et 560 que : $a^{561}\equiv a(561)$
  Donc, 561 est un nombre pseudo premier de base a (avec $1\leqslant a\leqslant560$)
  Avec Xcas, on écrit facilement un algorithme qui permet de vérifier que pour tout entier naturel a compris entre 1 et 560, on a $irem(a\wedge561,561)=a$

b) Définition

On nomme **nombre de Carmickaël** tout entier naturel n supérieur ou égal à 2, non premier tel que pour tout entier naturel a, vérifiant $1 \leqslant a \leqslant n-1$ et premier avec n, on ait $a^n \equiv a(n)$.

c) Remarques

- Tous les nombres de Carmichaël sont des nombres de Poulet.
- Les premiers nombres de Carmichaël sont :
  561 ; 1105 ; 1729 ; 2465 ; 2821 ; 6601 ; 6911 ; 10585 ; 29341 ; 41041 ; 46657 ; 52633 ; ...
- Tous les nombres de Carmichaël sont impairs.
- Tout nombre de Carmichaël est le produit d'au moins trois facteurs.
- Il existe une infinité de nombre de Carmichaël.
- Les nombres de Carmichaël sont « rares ». Il y en a 105 212 inférieurs à 10^{15}, donc si on choisit au hasard un entier naturel non nul inférieur à 10^{15} alors la probabilité d'obtenir un nombre de Carmichaël est inférieure à 10^{-9}.

4.3. Test de primalité de Fermat

p est un entier naturel « assez grand ». On étudie l'hypothèse : p est un nombre premier.
On choisit au hasard un nombre a tel que $1 < a \leqslant p-1$.

- Si a^p n'est pas congru à $a(p)$, alors p **n'est pas un nombre premier**.
- Si $a^p \equiv a(p)$, il est possible que p soit **un nombre premier** ou que p soit **un nombre pseudo premier** de base a (on peut alors choisir une autre valeur de a)
  (on peut avoir un nombre de Carmichaël mais on conclut que p est « probablement premier », c'est à dire que la probabilité qu'il ne soit pas premier est « faible »).

4.4. Nombre de Mersenne

a) Définition

$n \in \mathbb{N}^*$ .On nomme **nombre de Mersenne** tout entier naturel : $M_n = 2^n - 1$

b) Remarques

Si $n \geqslant 2$ et n non premier alors M_n **n'est pas un nombre premier**.

Démonstration :
$n = pq$ avec $1 < p < n$ et $1 < q < n$
$2^n = 2^{pq} = (2^p)^q$
$M_n = 2^n - 1 = (2^p)^q - 1$
$2^p - 1 \equiv 0(2^p - 1)$
Donc, $2^p \equiv 1(2^p - 1)$

Et, $(2^p)^q \equiv 1^q (2^p - 1)$
Donc, $2^n \equiv 1 (2^p - 1)$
Et, $2^n - 1 \equiv 0 (2^p - 1)$

$2^p - 1$ est un diviseur de $M_n = 2^n - 1$ et $1 < 2^p - 1 < 2^n - 1$
Donc, M_n n'est pas un nombre premier.

Si $M_n = 2^n - 1$ est **premier** alors n est **un nombre premier**.

La réciproque est fausse.
Exemple : $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ n'est pas premier, pourtant 11 est un nombre premier.

Depuis le seizième siècle, on étudia la primalité des nombres de Mersenne. Finalement, c'est en 1947 que la liste des nombres de Mersenne premiers, pour n inférieur à 258, fut établie :
n=2 ; 3 ; 5 ; 7 ; 13 ; 17 ; 19 ; 31 ; 61 ; 89 ; 107 et 127.
Maintenant, l'utilisation des ordinateurs permet de déterminer des nombres de Mersenne premiers de plus en plus grands (ceux sont les nombres premiers les plus connus).
Exemple : M_n avec n=42643801 est premier.

4.5. Nombres de Fermat

a) Définition

$n \in \mathbb{N}$ .On nomme **nombre de Fermat** tout entier naturel de la forme : $F_n = 2^{2^n} + 1$

b)

$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3$ premier
$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 5$ premier
$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 17$ premier
$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 257$ premier
$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65537$ premier
$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 * 6700417$ non premier
$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 3$ non premier

c)
Les nombres de Fermat premiers interviennent dans un théorème de Gauss précisant le nombre de côtés des polygones réguliers constructibles à la règle et au compas.
Énoncé du théorème :
Soit p un nombre premier supérieur ou égal à 3, α un entier naturel, al;ors le polygone régulier à p^α côtés est constructible à la règle et au compas si et seulement si $\alpha = 1$ et p est un nombre de Fermat.
On démontre aussi que :
Le polygone régulier à n ($n \geqslant 3$)côtés est constructible à la règle et au compas si et seulement si $n = 2^m \times F_a \times F_b \times \ldots \times F_r$ où les F_i sont des nombres de Fermat premiers distincts deux à deux et m un entier naturel.