LOGIQUE MATHEMATIQUE CLASSIQUE, ARITHMETIQUE ET FERMAT :
Démonstration directe du grand théorème de Fermat,
par Ahmed Idrissi Bouyahyaoui

En 1994, **Andrew Wiles** a démontré la conjecture de Taniyama-Shimura-Weil dont le grand théorème de Fermat en est un corollaire.

Le grand théorème de Fermat :
« Il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré ; j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir. »
Cette assertion a été écrite vers 1637 par Fermat sur une marge de son Diophante.

Expression algébrique :
« L'égalité $Z^n = Y^n + X^n$ est impossible pour Z, Y, X, $n \in N^+$, n>2. »

Le présent article décrit une **résolution de** « **l'énigme de Fermat** » utilisant des **outils mathématiques connus de Fermat**.

Fermat parle de carré (a^2), de cube (a^3), de bicarré (a^4), …, de puissance de degré n (a^n), … .
Ces puissances sont somme ou différence de deux puissances de même degré, ou ne le sont pas. D'où la propriété P ou nonP attachée à une puissance donnée, $P(a^n)$ ou $\neg P(a^n)$:
$P(a^n)$ =« la puissance a^n est somme ou différence de deux puissances de même degré n. »
$\neg P(a^n)$ =« la puissance a^n n'est pas somme ou différence de deux puissances de même degré n. »
Cette notation est conforme à l'esprit et à la lettre de l'énoncé du grand théorème de Fermat.
Exemples : $4^2 = 5^2 - 3^2$, $P(4^2)=V$, $\neg P(2^4)=V$; 4^2 , 2^4 : nombres de la forme a^n .

Utilisation de la **logique mathématique bivalente** pour établir la propriété héritée par des facteurs premiers entre eux d'une puissance de degré n égale à la somme ou à la différence de deux puissances de même degré n :

Etablissement de la propriété héritée :
$(Z^n = Y^n + X^n$, Z, Y, X, $n \in N^+$, $\langle Z, Y, X\rangle = 1) \Longrightarrow$
$(P(Z^n) \Longrightarrow (\forall a, b \in N^+, \langle a, b\rangle = 1)\ (P(Z^n = a^n b^n) \Longrightarrow P(a^n) \vee P(b^n))$.

C'est une **règle de réduction** ou une **méthode de** «**descente finie**» dont la démonstration est donnée ci-dessous par une preuve directe et une preuve par le raisonnement par l'absurde.

Preuve directe de la règle de réduction :
Le **Théorème A** (page 3) **:**
$[(\forall$ p premier (pair ou impair), y, x, n, $\alpha \in N^+$, n>2) $[(\neg P((p^\alpha)^n), (p^\alpha)^n \neq y^n \pm x^n) \Longrightarrow$
$(\neg P(Z^n), Z^n \neq Y^n \pm X^n)]] = V$,
permet d'écrire la proposition vraie :
$(\forall$ p nombre premier (pair ou impair), n, $\alpha, \beta \in N^+$, n>2)$([\neg P((p^\alpha)^n)] = V)$.

D'où la proposition vraie :
$[\neg P((p^{\alpha})^{n}) \wedge \neg P((q^{\beta})^{n})] = V$, où p et q sont deux nombres premiers distincts, et n>2.
Donc on peut écrire les deux propositions contradictoires suivantes de mêmes prémisses vraies (w : disjonction exclusive) :
(**1**) $(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (\neg P(a^{n}) \wedge \neg P(b^{n}) ===> \neg P(a^{n}b^{n}))$ w
(2) $(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (\neg P(a^{n}) \wedge \neg P(b^{n})) ===> P(a^{n}b^{n}))$
Cette proposition (2) a pour contraposée :
(3) $(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (\neg P(a^{n}b^{n})) ===> P(a^{n}) \vee P(b^{n}))$
qui est fausse.
Elle est en contradiction avec la **proposition affirmée vraie** :
(**4**) $[(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (P(a^{n}) \vee P(b^{n})) ===> P(a^{n}b^{n}))] = V$
D'une part, preuve suffisante, la multiplication est distributive par rapport à l'addition et la soustraction, et associative, et, d'autre part, on ne peut pas avoir à la fois $\neg P(a^{n}b^{n})$ et $P(a^{n}b^{n})$ dans le système de logique bivalente (tiers exclu).
Donc la proposition (**1**) est vraie et sa contraposée aussi (**règle de réduction**) :
(**5**) $[(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (P(a^{n}b^{n}) ===> P(a^{n}) \vee P(b^{n}))] = V$.

Preuve de la règle de réduction par le raisonnement par l'absurde :
Supposons : $[P(Z^{n} = a^{n}b^{n})] = V$, $a, b, n \in N^{+}, <a, b> = 1$.
Dans cette hypothèse, on a (w : disjonction exclusive) :
(6) - : $[P(Z^{n} = a^{n}b^{n}) ===> (P(a^{n}) \vee P(b^{n})) w (\neg P(a^{n}) \wedge \neg P(b^{n}))] = V$,
est l'union disjonctive des deux propositions contradictoires :
(7) - : $P(Z^{n} = a^{n}b^{n}) ===> P(a^{n}) \vee P(b^{n})$ w
(8) - : $P(Z^{n} = a^{n}b^{n}) ===> \neg P(a^{n}) \wedge \neg P(b^{n})$
qui a pour contraposée :
(9) $[(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (P(a^{n}) \vee P(b^{n})) ===> \neg P(a^{n}b^{n}))]$
qui est fausse.
Elle est en contradiction avec la **proposition affirmée vraie** :
(**10**) $[(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (P(a^{n}) \vee P(b^{n})) ===> P(a^{n}b^{n}))] = V$.
(preuve déjà donnée en (4))
D'une part, preuve suffisante, la multiplication est distributive par rapport à l'addition et la soustraction, et associative, et, d'autre part, on ne peut pas avoir à la fois $\neg P(a^{n}b^{n})$ et $P(a^{n}b^{n})$ dans le système de logique bivalente (tiers exclu).
La proposition (7) est donc vraie et l'on a la **règle de réduction** :
$[(\forall a, b, n \in N^{+}, n > 2, <a, b> = 1) (P(Z^{n} = a^{n}b^{n}) ===> P(a^{n}) \vee P(b^{n}))] = V$
qui, par réductions successives suivant des déductions (inférences) vraies, permet d'aboutir à la **réduction terminale** : le théorème F.

Théorème F (F : en hommage à Fermat) **:**
$[P(Z^{n} = (\prod_{i=1}^{m} p_i^{\alpha} i)^{n}) ===>$
$(\exists p_i^{\alpha} i \in E = \{ p_1^{\alpha} 1, p_2^{\alpha} 2, ... , p_m^{\alpha} m\}) \mid (P((p_i^{\alpha} i)^{n}))] = V$
où $p_1, p_2, ... , p_m$ sont des nombres premiers.

Condition de validité de l'inférence terminale : $\alpha_i \geq \beta_i \geq 1$ et $P((p_i^{\beta} i)^{n}) \wedge \neg P((p_i^{(\beta i - 1)})^{n})$, pour que l'implication terminale de la chaine de déductions soit vraie.

Or le **théorème A** montre que la conclusion du théorème F est fausse.

Théorème A (A : en hommage à Abel) **:**
[($\forall$ p premier (pair ou impair), y, x, n, $\alpha \in N^+$, n>2)
$(\neg P((p^{\alpha})^n), (p^{\alpha})^n \neq y^n \pm x^n$ ===> $\neg P(Z^n=(\prod_{i=1}^{m} p_i^{\alpha}i)^n))] = V$
===>
[($\forall$ Z, Y, X, n $\in N^+$, n>2) $(\neg P(Z^n), Z^n \neq Y^n+X^n)] = V$

Démonstration du théorème A :
Par hypothèse :
$Z^n = Y^n + X^n$, $< Z, Y, X > = 1$, d'où $P(Z^n) = P(Y^n) = P(X^n) = P(ZYX)^n = V$
Théorème F :
$[P(Z^n = (\prod_{i=1}^{m} p_i^{\alpha}i)^n)$ ===>
$(\exists\ p_i^{\alpha}i \in E = \{ p_1^{\alpha}1, p_2^{\alpha}2, \ldots\ldots , p_m^{\alpha}m\}) \mid (P((p_i^{\alpha}i)^n))] = V$
où p_1, p_2, ….. , p_m sont des nombres premiers.

Soit $q_k\beta_k$, un facteur premier (pair ou impair) de ZYX tel que $P((q_k\beta_k)^n)$, q_k, β_k, $n \in N^+$, n>2 .

Si $\mathbf{q_k = 2}$ alors on aura : $(2\beta_k)^n = y_k^n \pm x_k^n$, $< 2, y_k, x_k > = 1$, n>2 .

Comme tout entier n>2 est un multiple de 4 ou d'un nombre premier impair, il suffit de prouver le grand théorème de Fermat pour n=4 et pour chaque nombre premier impair.

Pour n impair :
L'égalité $(2\beta_k)^n = y_k^n \pm x_k^n = (y_k \pm x_k)((y_k^n \pm x_k^n)/(y_k \pm x_k))$ est impossible, le premier membre est une puissance de 2 et, dans le produit du second membre, le facteur $[(y_k^n \pm x_k^n)/(y_k \pm x_k)]$ est impair. $[y_k > x_k \geq 1$ ===> $(y_k^n \pm x_k^n)/(y_k \pm x_k) > 1]$.

Pour n = 4 :
1 - : $(2\beta_k)^4 = y_k^4 + x_k^4$, $0 \equiv 2 \pmod 4$, égalité impossible, $y_k^4 + x_k^4$, supérieur à 4, n'est pas une puissance de 2 .
2 - : $(2\beta_k)^4 = y_k^4 - x_k^4 = (y_k^2 - x_k^2)(y_k^2 + x_k^2)$, égalité impossible, le facteur $(y_k^2 + x_k^2)$, supérieur à 4, n'est pas une puissance de 2 $(y_k^2 + x_k^2 \equiv 2 \pmod 4)$.

Donc, **l'égalité $(2\beta_k)^n = y_k^n \pm x_k^n$, y_k, x_k, n, $\beta_k \in N^+$, n>2, est impossible** et, par suite, **q_k est nécessairement impair** et un des deux nombres y_k ou x_k est pair et a, nécessairement, au moins deux facteurs premiers.

Dans l'égalité $(q_k\beta_k)^n = y_k^n \pm x_k^n$, avec n>2, supposons que x_k est pair, si nécessaire après une opération d'échange de signes et de dénominations : $(q_k\beta_k)^n = \pm y_k^n \pm x_k^n$.
Donc, **x_k est pair et a au moins 2 facteurs premiers.**
Par application du théorème F à x_k^n, on a :
$x_k = 2^{\alpha}{}_k\, a_k\, q_{k+1}{}^{\beta}k+1$ et $P((q_{k+1})^{\beta}k+1)^n) = V$, q_{k+1} nombre premier impair, et l'on a :
$(q_k\beta_k)^n = \pm y_k^n \pm (2^{\alpha}{}_k\, a_k\, q_{k+1}{}^{\beta}k+1)^n$,
y_k et a_k sont des nombres impairs, $a_k \geq 1$, k=0, 1, 2, … .
D'où **la suite** (± : + ou bien -) :
$(q_0\beta_0)^n = \pm y_0^n \pm x_0^n = \pm y_0^n \pm (2^{\alpha}{}_0)^n a_0^n (q_1\beta_1)^n$

$(q_1\beta_1)^n = \pm\ y_1^n \pm\ x_1^n = \pm\ y_1^n \pm\ (2^{\alpha}_1)^n a_1^n (q_2\beta_2)^n$
....
$(q_k\beta_k)^n = \pm\ y_k^n \pm\ x_k^n = \pm\ y_k^n \pm\ (2^{\alpha}_k)^n a_k^n (q_{k+1}\beta_{k+1})^n$
....
Le terme général $(q_k\beta_k)^n$ de la suite $\{(q_k\beta_k)^n\}$, q_k nombre premier impair, est tel que $(q_k\beta_k)^n > 2^n$.

Développement en série numérique :
La suite d'égalités ci-dessus permet d'associer à $(q_0\beta_0)^n$ une série numérique :
$(q_0\beta_0)^n = \pm\ y_0^n \pm (2^{\alpha}_0)^n a_0^n (y_1^n \pm (2^{\alpha}_1)^n a_1^n (y_2^n \pm ... \pm (2^{\alpha}_k)^n a_k^n (y_{k+1}^n \pm x_{k+1}^n)...))$

D'où après développement suivant la suite donnée ci-dessus :
$(q_0\beta_0)^n = \pm\ y_0^n \pm (2^{\alpha}_0)^n a_0^n y_1^n \pm (2^{\alpha}_0)^n (2^{\alpha}_1)^n a_0^n a_1^n y_2^n \pm (2^{\alpha}_0)^n (2^{\alpha}_1)^n (2^{\alpha}_2)^n a_0^n a_1^n a_2^n y_3^n \pm$
$... \pm (2^{\alpha}_0)^n (2^{\alpha}_1)^n (2^{\alpha}_2)^n ... (2^{\alpha}_k)^n a_0^n a_1^n a_2^n ... a_k^n y_{k+1}^n \pm ... .$

Pour simplifier l'écriture, posons :
$c_k = \alpha_0 + \alpha_1 + \alpha_2 + ... + \alpha_k$, $\alpha_k \geq 1$, $k=0, 1, 2, \ldots .$ $c_k \geq k+1$
$b_k = a_0\, a_1\, a_1 ... a_K$, $a_K \geq 1$, $b_k \geq 1$, b_k est un nombre impair ,
d'où :
$(q_0\beta_0)^n = \pm\ y_0^n \pm\ 2^{nc}_0\, b_0^n y_1^n \pm\ 2^{nc}_1\, b_1^n y_2^n \pm\ 2^{nc}_2\, b_2^n y_3^n \pm ... \pm\ 2^{nc}_k\, b_k^n y_{k+1}^n \pm ....$

La somme de toute association d'un nombre quelconque des éléments $\pm\ 2^{nc}_k\, b_k^n y_{k+1}^n$, k=0, 1, 2, 3, .. , n'est jamais nulle, les coefficients 2^{nc}_k étant tous distincts et les nombres $b_k^n y_{k+1}^n$ étant impairs.
Ainsi le reste $R_k = \pm\ 2^{nc}_k\, b_k^n y_{k+1}^n \pm\ 2^{nc}_{k+1}\, b_{k+1}^n y_{k+2}^n \pm ...$ est de valeur absolue :
$|R_k| \geq 2^{nc}_k \geq 2^{n(k+1)}$, d'où $\lim |R_k| \dashrightarrow \infty$ $(k \dashrightarrow \infty)$, ce qui conduit à une égalité impossible puisque le nombre $(q_0\beta_0)^n$ est fini.
Donc l'égalité $(q_0\beta_0)^n = \pm\ y_0^n \pm\ x_0^n$ est impossible .

Autre formulation :
Le terme général de la série est de valeur absolue égale à : $2^{nc}_k\, b_k^n y_{k+1}^n \geq 2^{nc}_k \geq 2^{n(k+1)}$.
Comme $\lim 2^{n(k+1)} \dashrightarrow \infty$ $(k \dashrightarrow \infty)$, la série est divergente.
La condition nécessaire de convergence [Cauchy (1789-1857)] n'étant pas satisfaite, la sommation totale de la série ne peut être égale à la limite assignée $(q_0\beta_0)^n$.

Donc l'égalité $(q_0\beta_0)^n = \pm\ y_0^n \pm\ x_0^n$, avec n>2, est impossible .
Les hypothèses, $(p_j^{\alpha}{}_j)^n = y^n \pm\ x^n$, $(q_k\beta_k)^n = \pm\ y_k^n \pm\ x_k^n$, $q_0\beta_0 = p_j^{\alpha}{}_j$, (k=0, 1, 2, ...) , (où p_j et q_k sont des nombres premiers), déduites de l'hypothèse initiale $Z^n = Y^n + X^n$, $n > 2$.
, étant fausses, l'égalité $Z^n = Y^n + X^n$, Z, Y, X, $n \in N^+$ et $n > 2$, est impossible.

Je crois que **Fermat** a considéré que la règle de réduction :
$P(Z^n = a^n b^n) \Longrightarrow P(a^n) \wedge P(b^n)$, a, b, $n \in N^+$, $\langle a, b \rangle = 1$,
est vraie pour tout $n \geq 1$ et a conclu par déduction ou par induction : puisque $Z^n = Y^n + X^n$ et $P((ZYX)^n) = V$, 2^{α} étant un facteur premier de ZYX , on a $(2^{\alpha})^n = u^n \pm v^n$, égalité impossible pour $n > 2$, il en est de même de l'hypothèse $Z^n = Y^n + X^n$, $n > 2$.

Ahmed IDRISSI BOUYAHYAOUI