DEMONSTRATION DIRECTE DU GRAND THEOREME DE FERMAT
par Ahmed Idrissi Bouyahyaoui

Résumé :
Une propriété P ou nonP est attachée à toute puissance a^n , $P(a^n)$ 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. »

Théorème F (F : en hommage à Fermat) **:**
$(Z^n = Y^n+X^n,\ P(Z^n = \prod_{i=1}^{m} (p_i^{\alpha_i})^n)) \Longrightarrow$
$[(\exists\ p_i^{\alpha_i} \in E = \{ p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots , p_m^{\alpha_m}\}) \mid (P((p_i^{\alpha_i})^n), (p_i^{\alpha_i})^n = y^n \pm x^n)]$
pour Y, X, y, x, n, $\alpha_i \in N^+$ et $p_1, p_2, \ldots , p_m$ sont des nombres premiers.

Or le **théorème A** contredit la conclusion du théorème F.
Cette conclusion est fausse pour n>2 et ainsi $Z^n \neq Y^n+X^n$.

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

----ooo----

DEMONSTRATION DIRECTE DU GRAND THEOREME 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 sa copie de l'édition de Bachet de l'Arithmética de Diophante.

Expression algébrique :
« L'égalité $Z^n = Y^n + X^n$ est impossible pour Z, Y, X, n $\in N^+$ et 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 toute puissance a^n , $P(a^n)$ ou $\neg P(a^n)$:

P(a^n) =« la puissance a^n est somme ou différence de deux puissances de même degré n. »
¬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 , ¬P(2^4)=V ; 4^2 , 2^4 : nombres de la forme a^n .

Application des règles 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 :
$(Z^n = Y^n + X^n \ , \ Z, Y, X, n \in N^+ , <Z, Y, X> =1) \Longrightarrow$
$[P(Z^n) \Longrightarrow (\forall a, b \in N^+ , <a, b> = 1) (P(Z^n = a^n b^n) \Longrightarrow P(a^n) \vee P(b^n))]$

$P(Z^n = a^n b^n) \Longrightarrow P(a^n) \vee P(b^n)$
est une **règle de réduction** ou une **méthode de** «**descente finie**» dont la démonstration est donnée ci-après par une preuve directe et une preuve par l'absurde.

Preuve directe de la règle de réduction :
Comme pour tout y, x, n $\in N^+$, $2^n \neq y^n + x^n$, $< 2, y, x> = 1$ et $n>2$, $3^n \neq y^n + x^n$, $2^n 3^n \neq y^n + x^n$, $< 2,3, y, x> = 1$ et $n>1$,
on peut affirmer que les propositions suivantes sont possibles :
$\neg P(a^n) \wedge \neg P(b^n)$, **$\neg P(a^n b^n)$** et **$\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow \neg P(a^n b^n)$,** a, b, n $\in N^+$, et n>2.
Donc on peut écrire la proposition vraie :
$[(\forall a, b, n \in N^+, <a, b> = 1, n > 2) (\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow \neg P(a^n b^n) \vee P(a^n b^n))] \Longrightarrow$
Avec la distibutivité de $\Longrightarrow$ par rapport à $\vee$ on peut écrire :
$(\forall a, b, n \in N^+, <a, b> = 1, n > 2)$
$[(\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow \neg P(a^n b^n)) \vee (\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow P(a^n b^n))]$.
Evaluons les deux propositions contradictoires suivantes de mêmes prémisses vraies :
(**1**) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2) (\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow \neg P(a^n b^n))$
(2) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2) (\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow P(a^n b^n))$
La propositionde (2) a pour contraposée :
(3) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2) (\neg P(a^n b^n) \Longrightarrow P(a^n) \vee P(b^n))$
qui est fausse, de contenu contradictoire :
elle est en contradiction avec la **proposition formellement vraie** :
(**4**) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2) (P(a^n) \vee P(b^n) \Longrightarrow P(a^n b^n))$
Preuve : la multiplication est distributive par rapport à l'addition et la soustraction, et associative.
Donc la proposition (2) est fausse et l'on a :
$(\forall a, b, n \in N^+, <a, b> = 1, n > 2)$
$[[(\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow \neg P(a^n b^n)) \vee (\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow P(a^n b^n))] \wedge \neg(\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow P(a^n b^n))]$
$\Longrightarrow$
$(\forall a, b, n \in N^+, <a, b> = 1, n > 2) (\neg P(a^n) \wedge \neg P(b^n) \Longrightarrow \neg P(a^n b^n))$.
Donc la proposition (**1**) est vraie et de contraposée la **règle de réduction** :

(**5**) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2)\ (P(a^n b^n) \Longrightarrow P(a^n) \vee P(b^n))$

Preuve de la règle de réduction par l'absurde :

Supposons : $\mathbf{P(Z^n = a^n b^n)}$, $a, b, n \in N^+$, $<a, b> = 1, n>2$.

Dans cette hypothèse, on a la proposition vraie :

$(\forall a, b, n \in N^+, <a, b> = 1, n > 2)\ (P(Z^n = a^n b^n) \Longrightarrow (P(a^n) \vee P(b^n)) \vee (\neg P(a^n) \wedge \neg P(b^n)))$

Avec la distibutivité de $\Longrightarrow$ par rapport à $\vee$ on peut écrire :

$(\forall a, b, n \in N^+, <a, b> = 1, n > 2)$

$[(P(Z^n = a^n b^n) \Longrightarrow P(a^n) \vee P(b^n)) \vee (P(Z^n = a^n b^n) \Longrightarrow (\neg P(a^n) \wedge \neg P(b^n))]$.

Evaluons les deux propositions contradictoires suivantes de mêmes prémisses vraies par hypothèse :

(6) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2)\ (P(Z^n = a^n b^n) \Longrightarrow P(a^n) \vee P(b^n))$

(7) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2)\ (P(Z^n = a^n b^n) \Longrightarrow \neg P(a^n) \wedge \neg P(b^n))$

La propositionde (7) a pour contraposée :

(8) $(\forall a, b, n \in N^+, <a, b> = 1, n > 2)\ (P(a^n) \vee P(b^n) \Longrightarrow \neg P(a^n b^n))$

qui est fausse, de contenu contradictoire :

elle est en contradiction avec la **proposition formellement vraie** :

(**9**) $(\forall a, b, n \in N^+, n > 2, <a, b> = 1)\ (P(a^n) \vee P(b^n) \Longrightarrow P(a^n b^n))$

Preuve : la multiplication est distributive par rapport à l'addition et la soustraction, et associative.

Donc la proposition (7) est fausse et l'on a :

$(\forall a, b, n \in N^+, <a, b> = 1, n > 2)$

$[[(P(a^n b^n) \Longrightarrow P(a^n) \vee P(b^n)) \vee (P(a^n b^n) \Longrightarrow \neg P(a^n) \wedge \neg P(b^n))] \wedge \neg (P(a^n b^n) \Longrightarrow \neg P(a^n) \wedge \neg P(b^n))]$

$\Longrightarrow$

$(\forall a, b, n \in N^+, <a, b> = 1, n > 2)\ (P(Z^n = a^n b^n) \Longrightarrow P(a^n) \vee P(b^n))$.

Donc la proposition (6) est vraie (hypothèse initiale: $P(Z^n)$) et de contraposée la **règle de réduction** :

$(\forall a, b, n \in N^+, <a, b> = 1, n > 2)\ (P(Z^n = a^n b^n) \Longrightarrow P(a^n) \vee P(b^n))$

qui, par réductions successives suivant des déductions logiquement vraies (inférences), permet d'aboutir à la **réduction terminale** : le théorème F.

Théorème F (F : en hommage à Fermat) **:**

$(Z^n = Y^n + X^n,\ P(Z^n = \prod_{i=1}^{m} (p_i^{\alpha_i})^n)) \Longrightarrow$

$[(\exists\ p_i^{\alpha_i} \in E = \{ p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots\ldots, p_m^{\alpha_m}\}) \mid (P((p_i^{\alpha_i})^n), (p_i^{\alpha_i})^n = y^n \pm x^n)]$

où $Y, X, y, x, n, \alpha_i \in N^+$ et $p_1, p_2, \ldots\ldots, p_m$ sont des nombres premiers.

Or le **théorème A** contredit la conclusion du théorème F.

Cette conclusion est fausse pour n>2 et ainsi $Z^n \neq Y^n + X^n$.

Théorème A (A : en hommage à Abel) **:**

$[(\forall$ p premier (pair ou impair), y, x, n, $\alpha \in N^+, n>2)\ (\neg P((p^{\alpha})^n), (p^{\alpha})^n \neq y^n \pm x^n)] \Longrightarrow$

$[(\forall Z, Y, X, n \in N^+, n>2)\ (\neg P(Z^n = \prod_{i=1}^{m} (p_i^{\alpha_i})^n) = \neg P(Z^n),\ Z^n \neq Y^n + X^n)]$

Conjecture d'Abel (1802-1829) :

$(\forall z, y, x, n \in N^+, n>2)\ (<z, y, x>=1, z^n = y^n + x^n) \Longrightarrow$

aucun z, y, x ne peut être une puissance d'un nombre premier.

Démonstration du théorème A :
Par hypothèse (théorème F) :
$(Z^n = Y^n+X^n,\ P(Z^n = \prod_{i=1}^{m} (p_i^{\alpha_i})^n)) \Longrightarrow (\exists\ p_i^{\alpha}i \mid P((p_i^{\alpha_i})^n), (p_i^{\alpha_i})^n = y^n \pm x^n)$

Posons $q_0^{\beta_0} = p_i^{\alpha_i}$, $(q_0^{\beta_0})^n = (p_i^{\alpha_i})^n = y^n \pm x^n = y_0^n \pm x_0^n$ et soit $q_k^{\beta_k}$ tel que $P((q_k^{\beta_k})^n)$:
$(q_k^{\beta_k})^n = y_k^n \pm x_k^n$, q_k nombre premier (pair ou impair), β_k, $n \in N^+$, $n>2$, $k=0, 1, 2, \ldots$.
$<q_k, y_k, x_k >=1$.

Si $\mathbf{q_k = 2}$ alors on a : $(2^{\alpha_k})^n = y_k^n \pm x_k^n, < 2, y_k, x_k> = 1$, **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 $(2^{\alpha_k})^n = y_k^n \pm x_k^n = (y_k \pm x_k)((y_k^n \pm x_k^n)/(y_k \pm x_k))$ est impossible, le premier membre de l'égalité est une puissance de 2 et, dans le produit du second membre de l'égalité , le facteur $[(y_k^n \pm x_k^n)/(y_k \pm x_k)]$ est impair. $[y_k > x_k \geq 1 \Longrightarrow (y_k^n \pm x_k^n)/(y_k \pm x_k) > 1]$.

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

2 - : $(2^{\alpha_k})^4 = y_k^4 - x_k^4 = (y_k^2 - x_k^2)(y_k^2 + x_k^2)$, 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 $(2^{\alpha_k})^n = y_k^n \pm x_k^n$, $y_k, x_k, n, \alpha_k \in N^+$, 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 : (1*) $(q_k^{\beta_k})^n = \pm y_k^n \pm x_k^n$.
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 $P((q_{k+1})^{\beta_{k+1}})^n)$, q_{k+1} nombre premier impair, et l'égalité (1*) devient :
$(q_k^{\beta_k})^n = \pm y_k^n \pm (2^{\alpha_k} a_k q_{k+1}^{\beta_{k+1}})^n$,
y_k et a_k sont des nombres impairs, $a_k \geq 1$, $k=0, 1, 2, \ldots$.
D'où **la suite** ($\pm$: + 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 :
$(q_0^{\beta_0})^n = \pm y_0^n \pm (2^{\alpha}_0)^n a_0^n (y_1^n \pm (2^{\alpha}_1)^n a_1^n (y_2^n \pm \ldots \pm (2^{\alpha}_k)^n a_k^n (y_{k+1}^n \pm x_{k+1}^n)\ldots))$

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

Pour simplifier l'écriture, posons :
$c_k = \alpha_0 + \alpha_1 + \alpha_2 + \ldots + \alpha_k$, $\alpha_k \geq 1$, $k=0, 1, 2, \ldots .$ $c_k \geq k+1$
$b_k = a_0 a_1 a_1 \ldots a_K$, $a_K \geq 1$, $b_k \geq 1$, b_k est un nombre impair ,
d'où :
$(q_0^{\beta_0})^n = \pm y_0^n \pm 2^{nc_0} b_0^n y_1^n \pm 2^{nc_1} b_1^n y_2^n \pm 2^{nc_2} b_2^n y_3^n \pm \ldots \pm 2^{nc_k} b_k^n y_{k+1}^n \pm \ldots .$

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 $R_k = \pm 2^{nc_k} b_k^n y_{k+1}^n \pm 2^{nc_{k+1}} b_{k+1}^n y_{k+2}^n \pm \ldots$ est de valeur absolue :
$|R_k| \geq 2^{nc_k} \geq 2^{n(k+1)}$, d'où $\lim |R_k| \longrightarrow \infty$ $(k \longrightarrow \infty)$, 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 pour n>2.

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 $\lim 2^{n(k+1)} \longrightarrow \infty$ $(k \longrightarrow \infty)$, la série est divergente.
La condition nécessaire de convergence de 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 $(q_0^{\beta_0})^n = \pm y_0^n \pm x_0^n$ est impossible pour n>2.

L'hypothèse $(q_0^{\beta_0})^n = (p_j^{\alpha}{}_j)^n = y^n \pm x^n$, déduite avec le théorème F de l'hypothèse initiale $Z^n = Y^n + X^n$, étant fausse pour n>2, l'égalité $Z^n = Y^n + X^n$ est impossible pour Z, Y, X, $n \in N^+$ et $n > 2$.

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

Ahmed IDRISSI BOUYAHYAOUI