Preuve directe du grand théorème de Fermat :

«$(\forall (z, y, x, n) \in N^{*4}) \wedge (n>2)\ \ z^n \neq y^n + x^n$.»

Par Ahmed Idrissi Bouyahyaoui

Résumé :

Définitions :

$a, b, n \in N^*$.

Une propriété P(a,n) ou ¬P(a,n) est attachée à toute puissance a^n :

$P(a,n) = \exists (y, x) \in N^{*2}\ \ a^n = y^n + x^n$,

$\neg P(a,n) = \forall (y, x) \in N^{*2}\ \ a^n \neq y^n + x^n$,

(a, b)=1 : a et b sont premiers entre eux (pgcd(a,b)=1).

« Inférence : raisonnement consistant à admettre une proposition du fait de sa liaison avec d'autres propositions antérieurement admises. »

1 – Règle d'exclusion : $(\forall (a, b, n) \in N^{*3}) \wedge (n>1) \wedge ((a,b)=1)$ **[**$\neg P(a,n) \wedge \neg P(b,n) \rightarrow \neg P(a_x b,n)$]

[i.e. : $\forall (r,s,u,v,x,y) \in N^{*6}\ \ [(a^n \neq r^n+s^n) \wedge (b \neq u^n+v^n) \rightarrow\ a^n b^n \neq y^n+x^n]$]

– D'où le **Théorème F :**

$(Z=\Pi_{i=1}^{m} p_i^{\alpha} i) \rightarrow [[(\forall i\ \neg P(p_i^{\alpha} i,n)) \rightarrow (\neg P(\Pi_{i=1}^{m} p_i^{\alpha} i,n))] \rightarrow (\forall (Y, X) \in N^{*2}\ \ Z^n \neq Y^n+X^n)]$

où n, α_i , $m \in N^*$, i=1,2, … m, et $p_1, p_2, \ldots, p_m$ des nombres premiers.

2 – Règle de réduction : $(\forall (a, b, n) \in N^{*3}) \wedge (n>1) \wedge ((a,b)=1)$ **[**$P(a_x b,n) \rightarrow P(a,n) \vee P(b,n)$]

(contraposée de **1** -)

[i.e. : $(\exists (y, x) \in N^{*2}\ \ a^n b^n = y^n+x^n) \rightarrow (\exists (r,s,u,v,) \in N^{*4}\ \ (a^n = r^n+s^n) \vee (b^n = u^n+v^n))$]

– D'où le **Théorème F**-bis :

$(Z^n = Y^n+X^n, Z=\Pi_{i=1}^{m} p_i^{\alpha} i , P(\Pi_{i=1}^{m} p_i^{\alpha} i,n)) \rightarrow$

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

où Y, X, y, x, n, α_i , $m \in N^*$, et $p_1, p_2, \ldots, p_m$ des nombres premiers.

Le **théorème A** contredit la conclusion du théorème F-bis.

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

3 – Théorème A :

$(\forall$ p premier pair ou impair $(\forall (y, x, n, \alpha) \in N^{*4}) \wedge (n>2)\ \ \neg P(p^{\alpha},n), (p^{\alpha})^n \neq y^n + x^n$.

→ le grand théorème de Fermat :

$(\forall (Z, Y, X, n) \in N^{*4}) \wedge (n>2)$

$[(Z= \Pi_{i=1}^{m} p_i^{\alpha} i) \rightarrow [[\Pi_{i=1}^{m} \neg P(p_i^{\alpha} i,n) \rightarrow \neg P(\Pi_{i=1}^{m} p_i^{\alpha} i,n)] \rightarrow Z^n \neq Y^n+X^n]]$.

où α_i , $m \in N^*$, i=1,2, … m, et $p_1, p_2, \ldots, p_m$ des nombres premiers.

Chapitre 1 :

Preuve directe de la règle d'exclusion :

(1) Comme

$(\forall(y, x, n)\in N^{*3})\wedge(n>1)\ \ (2^n \neq y^n + x^n)$,

$(\forall(y, x, n)\in N^{*3})\wedge(n>1)\ \ (3^n \neq y^n + x^n)$,

$(\forall(y, x, n)\in N^{*3})\wedge(n>1)\ \ (2^n3^n \neq y^n + x^n)$,

les prémisses qui sont composées des propositions négatives :

$\neg P(a,n)$, $\neg P(b,n)$ ou $\neg P(a_xb,n)$, peuvent être supposées vraies .

Les propositions existentielles (particulières) contenant exclusivement ces prémisses doivent être des inférences immédiates vraies (Aristote) et elles sont donc vraies si et seulement si leurs conclusions sont vraies.

Les propositions sont affirmatives.

Comme $3^1=2^1+1^1$, $5^1=3^1+2^1$, $3^1*5^1=8^1+7^1$, $5^2=4^2+3^2$, $3^2*5^2=12^2+9^2$ et (1) ,

les prémisses qui comportent des propositions affirmatives :

$P(a,n)$, $P(b,n)$ ou $P(a_xb,n)$, sont vraies ou fausses.

Les propositions contenant ces prémisses, si elles sont vraies, elles peuvent l'être seulement logiquement (formellement).

Les propositions sont conditionnelles.

Exemple : la proposition logiquement vraie (formellement vraie) :

$(\forall(a, b, n)\in N^{*3})\wedge((a, b)=1)\ \ [P(a,n) \vee P(b,n) \rightarrow P(a_xb,n)]$,

[i.e. : $(\exists (r,s,u,v,)\in N^{*4}\ \ (a^n=r^n + s^n)\vee(b^n=u^n + v^n) \rightarrow (\exists (y, x)\in N^{*2}\ \ a^nb^n = y^n + x^n$,

$a^nb^n=a^n(u^n + v^n)\vee b^n(r^n + s^n)=((au)^n+(av)^n)\vee((br)^n+(bs)^n))$]

(la multiplication est distributive par rapport à l'addition et associative).

Principe du tiers exclu : $\forall(a, b, n)\in N^{*3}\ \ \neg P(a_xb,n) \vee P(a_xb,n)$ = Vrai .

Principe de la non-contradiction : $\forall(a, b, n)\in N^{*3}\ \ \neg P(a_xb,n) \wedge P(a_xb,n)$ = Faux .

On peut écrire les propositions suivantes :

La **subcontraire** et la **contradictoire** du « **carré logique d'Aristote** » sont utilisées pour établir deux preuves équivalentes :

1 - Etant donnée la proposition, déduite de (1), de prémisse et conclusion vraies :

(11) $(\exists(a, b)\in N^{*2})\wedge(\forall n\in N^*)\wedge(n>1)\wedge((a,b)=1)\ \ [\neg P(a,n) \wedge \neg P(b,n) \rightarrow \neg P(a_xb,n)]$,

[i. e. : $\forall(r, s, u, v, y, x)\in N^{*6}\ \ [(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^nb^n \neq y^n + x^n]$],

de subcontraire :

(12) $(\exists(a, b)\in N^{*2})\wedge(\forall n\in N^*)\wedge(n>1)\wedge((a,b)=1)\ \ [\neg P(a,n) \wedge \neg P(b,n) \rightarrow P(a_xb,n)]$,

[i. e. : $(\forall(r,s,u,v)\in N^{*4}\ \ (a^n \neq r^n + s^n)\wedge(b^n \neq u^n + v^n)) \rightarrow (\exists(y, x)\in N^{*2}\ \ a^nb^n = y^n+x^n)$],

fausse, puisque sa contraposée :

(13) $(\exists(a, b)\in N^{*2})\wedge(\forall n\in N^*)\wedge(n>1)\wedge((a,b)=1)\ \ [\neg P(a_xb,n) \rightarrow P(a,n) \vee P(b,n)]$,

[i. e. : $(\forall(y,x)\in N^{*2}\ \ a^nb^n \neq y^n + x^n) \rightarrow (\exists (r,s,u,v)\in N^{*4}\ \ (a^n = r^n+s^n)\vee(b^n = u^n+v^n))$]

$(\neg P(a_xb,n)\wedge P(a_xb,n)$ = Faux)

est fausse, la prémisse vraie est en contradiction avec la conclusion puisque :

$(\forall (a, b, n)\in N^{*3})\wedge((a, b)=1)$ $[P(a,n) \vee P(b,n) \rightarrow P(a_xb,n)]$,

[i.e. : $(\exists (r,s,u,v,)\in N^{*4}$ $(a^n=r^n + s^n)\vee(b^n=u^n + v^n) \rightarrow (\exists (y, x)\in N^{*2}$ $a^nb^n =y^n+x^n$,

$a^nb^n=a^n(u^n + v^n)\vee b^n(r^n + s^n)=((au)^n+(av)^n)\vee((br)^n+(bs)^n))$]

est une proposition logiquement (formellement) vraie.

L'implication (13) est fausse et, par équivalence, sa contraposée (12) l'est aussi.

Donc, la proposition (11) est **universelle** et donne **la règle d'exclusion** :

(14) $(\forall (a, b, n)\in N^{*3})\wedge(n>1)\wedge((a,b)=1)$ **[**$\neg P(a,n) \wedge \neg P(b,n) \rightarrow \neg P(a_xb,n)]$

[i. e. : $\forall (r, s, u, v, y, x)\in N^{*6}$ $[(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^nb^n \neq y^n + x^n]$]

2 - La proposition :

(21) $(\forall (a, b, n)\in N^{*3})\wedge(n>1)\wedge((a,b)=1)$ **[**$\neg P(a,n) \wedge \neg P(b,n) \rightarrow \neg P(a_xb,n)]$

[i. e. : $\forall (r, s, u, v, y, x)\in N^{*6}$ $[(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^nb^n \neq y^n + x^n]$]

est vraie car sa contradictoire :

(22) $(\exists (a, b, n)\in N^{*3})\wedge(n>1)\wedge((a,b)=1)$ $[\neg P(a,n) \wedge \neg P(b,n) \rightarrow P(a_xb,n)]$,

[i. e. : $(\forall (r,s,u,v)\in N^{*4}$ $(a^n \neq r^n + s^n)\wedge(b^n \neq u^n + v^n))$ $\rightarrow$ $(\exists (y, x)\in N^{*2}$ $a^nb^n = y^n+x^n)$],

est fausse puisque sa contraposée :

(23) $(\exists (a, b, n)\in N^{*3})\wedge(n>1)\wedge((a,b)=1)$ $[\neg P(a_xb,n) \rightarrow P(a,n) \vee P(b,n)]$

[i. e. : $(\forall (y,x)\in N^{*2}$ $a^nb^n \neq y^n + x^n)$ $\rightarrow (\exists (r,s,u,v)\in N^{*4}$ $(a^n = r^n+s^n)\vee(b^n = u^n+v^n))$]

$(\neg P(a_xb,n)\wedge P(a_xb,n) = Faux)$

est fausse, la prémisse vraie est en contradiction avec la conclusion puisque :

$(\forall (a, b, n)\in N^{*3})\wedge((a, b)=1)$ $[P(a,n) \vee P(b,n) \rightarrow P(a_xb,n)]$,

[i.e. : $(\exists (r,s,u,v,)\in N^{*4}$ $(a^n=r^n + s^n)\vee(b^n=u^n + v^n) \rightarrow (\exists (y, x)\in N^{*2}$ $a^nb^n =y^n+x^n$,

$a^nb^n=a^n(u^n + v^n)\vee b^n(r^n + s^n)=((au)^n+(av)^n)\vee((br)^n+(bs)^n))$]

est une proposition logiquement (formellement) vraie.

L'implication (23) est fausse et, par équivalence, sa contraposée (22) l'est aussi.

Donc, la proposition (21) est **la règle d'exclusion** :

(24) $(\forall (a, b, n)\in N^{*3})\wedge(n>1)\wedge((a,b)=1)$ $[\mathbf{\neg P(a,n) \wedge \neg P(b,n) \rightarrow \neg P(a_xb,n)}]$

[i. e. : $\forall (r, s, u, v, y, x)\in N^{*6}$ $[(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^nb^n \neq y^n + x^n]$]

La **règle d'exclusion** montre que si aucun de deux facteurs, premiers entre eux et de puissance n, n'est une somme de deux puissances de même degré n, leur produit n'est pas non plus une somme de deux puissances de même degré n .

D'où le **Théorème F** (F: en hommage à Fermat) **:**

$(Z=\Pi_{i=1}^{m} p_i^{\alpha}i) \rightarrow [[(\forall i$ $\neg P(p_i^{\alpha}i,n)) \rightarrow (\neg P(\Pi_{i=1}^{m} p_i^{\alpha}i,n))] \rightarrow (\forall (Y, X) \in N^{*2}$ $Z^n \neq Y^n+X^n)]$

où $n, \alpha_i , m \in N^*$, i=1,2, … m, et $p_1, p_2, ….. , p_m$ des nombres premiers.

La contraposée de la **règle d'exclusion** (proposition vraie) est la **règle de réduction,** proposition logiquement vraie (formellement vraie) **:**

(25) $(\forall (a, b, n) \in N^{*3}) \wedge (n>1) \wedge ((a,b)=1)$ [**$P(a_x b,n) \rightarrow P(a,n) \vee P(b,n)$**]

[i.e. : $(\exists (y, x) \in N^{*2}\ \ a^n b^n = y^n + x^n) \rightarrow (\exists (r,s,u,v,) \in N^{*4}\ \ (a^n = r^n + s^n) \vee (b^n = u^n + v^n))$]

La règle de réduction, par réductions successives suivant des déductions logiquement vraies (inférences), permet d'aboutir à la **réduction terminale** :

Théorème F-bis :
$(Z^n = Y^n + X^n, Z = \Pi_{i=1}^{m} p_i^{\alpha} i , P(\Pi_{i=1}^{m} p_i^{\alpha} i, n)) \rightarrow$
$[(\exists\, p_i^{\alpha} i \in E = \{ p_1^{\alpha}{}_1, p_2^{\alpha}{}_2, \ldots\ldots , p_m^{\alpha}{}_m\})\ \ (P(p_i^{\alpha} i, n), (p_i^{\alpha} i)^n = y^n + x^n)]$
où Y, X, y, x, n, α_i , m $\in$ N+, et p_1, p_2, ….. , p_m des nombres premiers.

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

Théorème A :
$(\forall$ p premier pair ou impair $(\forall (y, x, n, \alpha) \in N^{*4}) \wedge (n>2)\ \ \neg P(p^{\alpha}, n), (p^{\alpha})^n \neq y^n + x^n$.
$\rightarrow$ le grand théorème de Fermat :
$(\forall (Z, Y, X, n) \in N^{*4}) \wedge (n>2)$
$[(Z = \Pi_{i=1}^{m} p_i^{\alpha} i) \rightarrow [[\Pi_{i=1}^{m} \neg P(p_i^{\alpha} i, n) \rightarrow \neg P(\Pi_{i=1}^{m} p_i^{\alpha} i, n)] \rightarrow Z^n \neq Y^n + X^n]]$.
où α_i , m $\in N^*$, i=1,2, … m, et p_1, p_2, ….. , p_m des nombres premiers.

Chapitre 2 :

Démonstration du théorème A :

Pour n>2, tout facteur premier de puissance n n'est pas somme de deux puissances de même degré n.

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

Soit q^{α} un facteur premier :

Pour q=2 :

Pour n impair > 2 :

L'égalité $(2^{\alpha})^n = y^n + x^n = (y + x)((y^n + x^n)/(y + x))$ 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 $[(y^n + x^n)/(y + x)]$ est impair. $[y> x \geq 1 \rightarrow (y^n + x^n)/(y + x) > 1]$.

Pour n = 4 :

$(2^{\alpha})^4 = y^4 + x^4$, $0 \equiv 2 \pmod 4$, égalité impossible.

Donc, **l'égalité $(2^{\alpha})^n = y^n + x^n$, y, x, n, $\alpha \in N^*$, n>2, est impossible** et, par suite, **q est nécessairement impair.**

Soit $(q^{\beta})^n = y^n + x^n$, où y, x, n $\in N^*$, (q, y, x)=1 et n>2 , q nombre premier impair :

Pour n = 4 :

$(q^{\beta})^4 = y^4 + x^4$,

supposons y impair,

d'où :

$y^4 = ((q^{\beta})^2 - x^2) ((q^{\beta})^2 + x^2)$, où les deux facteurs du second membre sont premiers entre eux et, leur produit étant un carré, ils sont chacun un carré :

$(q^{\beta})^2 - x^2 = u^2$ et $(q^{\beta})^2 + x^2 = v^2$, ce qui est impossible (Fermat).

Pour n impair :

Soit $(q^{\beta})^n = y^n + x^n$, (q, y, x)=1 et n>2 :

(Abel, in « Analyse indéterminée », par Robert D. Carmichael, 1929)

$(q^{\beta})^n = y^n + x^n = (y + x)[(y^n + x^n) / (y + x)]$

où le facteur $[(y^n + x^n)/(y+x)]$ peut s'écrire sous la forme :

$[(y^n + x^n) / (y + x)] = [[(y + x) - x]^n + x^n] / (y + x)$

$= [(y + x)^n - n(y + x)^{(n-1)}x + ... + n(y + x)x^{(n-1)}] / (y + x)$

$= (y + x)Q(y,x) + nx^{(n-1)}$ où Q(y,x) est un polynôme en y et x à coefficients entiers .

Posons n=p, p premier impair .

Comme y et x sont premiers entre eux, les deux facteurs :

$(y + x)$ et $[(y + x)Q(y,x) + px^{(p-1)}]$ ont pour pgcd = 1 ou p .

Si pgcd = 1, les deux facteurs du second membre, $(y + x)$ et $[(y^p + x^p) / (y + x)]$, sont premiers entre eux et leur produit admettant une décomposition en un seul facteur premier, l'égalité $(q^{\beta})^p = y^p + x^p$ est impossible .

Si pgcd = p , alors p=q , et l'on a : $(q^{\beta})^q = (y + x)[(y + x)Q(y,x) + qx^{(q-1)}]$.
Les deux facteurs du second membre, $(y + x)$ et $[(y + x)Q(y,x) + qx^{(q-1)}]$, doivent être des puissances de q . Le terme $(y + x)Q(y,x)$ étant divisible par q^2 et (q,y,x) =1, le facteur $[(y + x)Q(y,x) + qx^{(q-1)}]$ n'est pas divisible par q^2 et donc n'est pas une puissance de q contrairement à l'hypothèse. L'égalité $(q^{\beta})^q = y^q + x^q$ est donc impossible .

Ainsi, l'égalité $(q^{\beta})^n = y^n + x^n$ est impossible pour n>2.

D'où le **Théorème A** (A: en hommage à Abel) **:**
$(\forall$ p premier pair ou impair $(\forall (y, x, n, \alpha) \in N^{*4}) \wedge (n>2)$ $\neg P(p^{\alpha},n), (p^{\alpha})^n \neq y^n + x^n$.
→ le grand théorème de Fermat :
$(\forall (Z, Y, X, n) \in N^{*4}) \wedge (n>2)$
$[(Z= \Pi_{i=1}^{m} p_i^{\alpha}i) \rightarrow [[\Pi_{i=1}^{m} \neg P(p_i^{\alpha}i,n) \rightarrow \neg P(\Pi_{i=1}^{m} p_i^{\alpha}i,n)] \rightarrow Z^n \neq Y^n+X^n]]$.
où α_i , $m \in N^*$, i=1,2, … m, et p_1, p_2, ….. , p_m des nombres premiers.

Ahmed Idrissi Bouyahyaoui