LOGIQUE MATHEMATIQUE CLASSIQUE, ARITHMETIQUE ET FERMAT
Démonstration directe du « grand théorème de Fermat »
par Ahmed IDRISSI BOUYAHYAOUI

LOGIQUE MATHEMATIQUE CLASSIQUE, ARITHMETIQUE ET FERMAT
Notation :
les connecteurs :
$\wedge, \vee, \neg, \Rightarrow, \Leftrightarrow$
opérateurs logiques : conjonction, disjonction, négation, implication .
les quantificateurs : $\forall$(pour tout …) , $\exists$(il existe au moins …)
négation de $\forall$, $\exists$: $\neg\forall = \exists$, $\neg\exists = \forall$
valeurs logiques : P(a^n)=V : proposition vraie, P(a^n)=F : proposition fausse ;
a, n $\in$N+ : a et n sont des entiers positifs .
< X,Y > =1 : X et Y sont premiers entre eux (p.g.c.d (X,Y)=1).
$\underset{m}{\pm}$: + ou bien - (signes opératoires) .
$\prod_{i=1}$: produit de m facteurs d'indice i .
$x \equiv y \ (mod\ m)$: x et y sont congrus modulo m .
$x \neq y \ (mod\ m)$: x et y ne sont pas congrus modulo m .
Tous les nombres considérés sont des entiers naturels positifs (N+).

LOGIQUE MATHEMATIQUE CLASSIQUE, ARITHMETIQUE ET FERMAT :
RESUME

Chapitre 1 :
Propriété P :
$$P(a^n) = V \Leftrightarrow (\exists\, y, x \in N + | a^n = y^n \pm x^n, a, n \in N+)$$
Cette propriété P est héréditaire, certains facteurs premiers (ou tous ?) de la puissance a^n possèdent cette propriété induite.
Etablissement d'une **règle de réduction d'une puissance donnée** à un de ses facteurs premiers (méthode de «descente finie») :
$$(Z^n = Y^n + X^n, Z, Y, X, n \in N+) \Rightarrow$$
$$(P(Z^n) = V \Rightarrow (Z^n = a^n b^n, P(a^n) = V \vee P(b^n) = V))$$
$$(a, b \in N+, < a, b >= 1)$$

Théorème F (F, en hommage à Fermat) :
$$[P(Z^n = (\prod_{i=1}^{m} {p_i}^{\alpha_i})^n) = V \Rightarrow$$
$$(\exists\, {p_i}^{\alpha_i} \in E = \{({p_1}^{\alpha_1}), ({p_2}^{\alpha_2}), ..., ({p_m}^{\alpha_m})\})(P(({p_i}^{\alpha_i})^n) = V)] = V$$

Chapitre 2 : **Démonstration probable de Fermat de son « grand théorème » :**
Généralisation du théorème F :
$$[P(Z^n = (\prod_{i=1}^{m} {p_i}^{\alpha_i})^n) = V \Rightarrow$$

$$(\forall {p_i}^{\alpha_i} \in E = \{({p_1}^{\alpha_1}), ({p_2}^{\alpha_2}), ..., ({p_m}^{\alpha_m})\})(P(({p_i}^{\alpha_i})^n) = V)] = V$$

vrai pour n=1, n=2, hypothèse de Fermat : vrai pour tout n .
D'où :
$[(Z^n = Y^n + X^n, Z, Y, X, n \in N+) \Rightarrow P(Z^n) = P(Y^n) = P(X^n) = V,$
$(2^\alpha)^n$ facteur premier de $ZYX] \Rightarrow$

$$[P((ZYX)^n) = (\prod_{i=1}^{s} p_i^{\alpha_i})^n) = V \Rightarrow$$

$$(P((2^\alpha)^n) = V), \alpha \in E = \{\alpha_i, i = 1, ...s\} \Rightarrow$$
$$[(\exists u, v \in N + |(2^\alpha)^n = u^n \pm v^n) \Rightarrow$$
$$[(\forall u, v, n, \alpha \in N+, (2^\alpha)^n \neq u^n \pm v^n, n > 2) \Rightarrow$$
$$(\forall Z, Y, X, n \in N+, Z^n \neq Y^n + X^n, n > 2)]$$

Chapitre 3 :
Démonstration du grand théorème de Fermat
ou démonstration élémentaire du théorème de Fermat-Wiles :
Théorème A (A, en hommage à Abel) :

$[^\forall p$ premier (pair ou impair) ,
$$y, x, n, \alpha \in N+, n > 2 : (p^\alpha)^n \neq y^n \pm x^n, P((p^\alpha)^n) = F] = V \Rightarrow$$

Théorème de Fermat-Wiles :
$$[\forall\ Z, Y, X, n \in N+, n > 2 : Z^n \neq Y^n + X^n, P(Z^n) = F] = V$$

Démonstration du théorème A :
Suites et séries numériques .

Chapitre 4 :
Démonstration du théorème A :
Caractères de divisibilité des nombres et, suites et séries numériques.

LOGIQUE MATHEMATIQUE CLASSIQUE, ARITHMETIQUE ET FERMAT :
Chapitre 1 :
Utilisation de la **logique mathématique bivalente** pour établir une 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 :
Enoncé de la propriété P :
P(a^n) : « La puissance a^n est égale à la somme ou à la différence de deux puissances de même degré $n, a, n \in N+$ »
Dans la logique bivalente (tiers exclu) : $P(a^n) \vee \neg Pa^n)$= V ,
la proposition P(a^n) est vraie : P(a^n) = V , ou fausse : P(a^n) = F .
Etablissement de la **propriété héritée :**
$$(Z^n = Y^n + X^n, Z, Y, X, n \in N+) \Rightarrow$$
$$(P(Z^n) = V \Rightarrow (Z^n = a^n b^n, P(a^n) = V \vee P(b^n) = V))$$
$$(a, b \in N+, < a, b >= 1)$$

C’est une règle de réduction ou méthode de «descente finie».

Propositions logiques :

(1) - :

$$[(\forall\ a, b, n \in N+, Z = ab)$$
$$((P(a^n) = F) \wedge (P(b^n) = F) \Rightarrow P(Z^n = a^n b^n) = F)] = V$$

de contraposée :

$$[(\forall\ a, b, n \in N+, Z = ab)$$
$$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))]$$

Remarque :

$$[((P(a^n) = F) \wedge (P(b^n) = F) \Rightarrow P(Z^n = a^n b^n) = F)] = V$$

est une restriction de :

$$(P(a^n) = F) \vee (P(b^n) = F) \Rightarrow P(Z^n = a^n b^n) = F$$

contraposée de :

$$P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \wedge (P(b^n) = V)$$

Preuve :

Supposons :

(2) - :

$$(\exists\ a, b, n \in N+, Z = ab)$$
$$((P(a^n) = F) \wedge (P(b^n) = F) \Rightarrow P(Z^n = a^n b^n) = V)$$

Cette proposition (2), contradictoire de (1), a pour contraposée :

(3) - :

$$(\exists\ a, b, n \in N+, Z = ab)$$
$$(P(Z^n = a^n b^n) = F \Rightarrow (P(a^n) = V) \vee (P(< b^n)) = V))$$

[négation de (1)] en contradiction avec la proposition affirmée vraie :

$$[(P(a^n) = V) \vee (P(b^n)) = V)) \Rightarrow (P(Z^n = a^n b^n) = V] = V$$

(La multiplication étant distributive par rapport à l’addition et la soustraction, et associative.)

La proposition (3) [négation de (1)], contraposée de la contradictoire de (1), mène à une contradiction, la proposition (1) est donc vraie.

La proposition (1) étant vraie, sa contraposée, proposition équivalente, est vraie aussi :

$$[(\forall\ a, b, n \in N+, Z = ab)$$
$$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))] = V$$

Autre formulation de preuve équivalente :

On a la proposition vraie par définition : $[(\forall\ a, b, n \in N+, Z = ab)$
$(P(a^n) = V) \vee (P(b^n) = V) \Rightarrow (P(Z^n = a^n b^n) = V)] = V$

de réciproque : $[(\forall\ a, b, n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))]$

qui a pour contradictoire : $[(\exists\ a, b, n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = F) \wedge (P(b^n) = F))]$

qui a pour contraposée : $[(\exists\ a, b, n \in N+, Z = ab)$
$(P(a^n) = V) \vee (P(b^n) = V) \Rightarrow (P(Z^n = a^n b^n) = F)] = F$

[négation de la réciproque]
Proposition en contradiction avec la proposition vraie par définition, elle est donc fausse et l'on a : $[(\forall\ a,b,n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))] = V$

A - :
A1 - :
$[(\forall\ a,b,n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))] = V$
A2 - :
$[(\forall\ a,b,n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))] = V$
$\Rightarrow [(P(Z^n = a^n b^n) = V) \wedge (P(a^n) = F) \Rightarrow (P(b^n) = V)]$

Cette proposition (A) donne une **règle opératoire** qui, par itérations successives, constitue une **règle de réduction ou de « descente finie»** relevant du principe d'induction finie.
Ainsi la proposition (A1) implique la proposition de réduction :
B - :
$Z = \prod_{i=1}^{m} {p_i}^{\alpha_i}$, Z décomposé en un produit de facteurs premiers, $\alpha_i \in N+$
$[(P(Z^n = (\prod_{i=1}^{m} {p_i}^{\alpha_i})^n = V \Rightarrow$
$(P(({p_1}^{\alpha_1})^n = V) \vee (P(({p_2}^{\alpha_2})^n) = V)) \vee .... \vee (P(({p_m}^{\alpha_m})^n) = V))] = V$
de proposition équivalente :
C - :
Théorème F :
$[P(Z^n = (\prod_{i=1}^{m} {p_i}^{\alpha_i})^n) = V \Rightarrow$

$(\exists\ {p_i}^{\alpha_i} \in E = \{({p_1}^{\alpha_1}), ({p_2}^{\alpha_2}), ..., ({p_m}^{\alpha_m})\})(P(({p_i}^{\alpha_i})^n) = V)] = V$

Application :
Démonstration du grand théorème de Fermat
ou démonstration élémentaire du théorème de Fermat-Wiles :
Soit $Z = \prod_{i=1}^{m} {p_i}^{\alpha_i}$, Z décomposé en un produit de facteurs premiers, $\alpha_i \in N+$

H : $[\forall\ Z,Y,X,n \in N+, n > 2 | Z^n = Y^n + X^n] \Rightarrow$
C : $[\exists\ y,x,n \in N+, n > 2 | ({p_j}_j^{\alpha})^n = y^n \pm x^n, {p_j}^{\alpha_j}$ facteur premier de Z, p_j : pair ou impair , $\alpha_j \in N+]$

D'après le théorème F établi ci-dessus (chapitre 1) :

$$[P(Z^n = (\prod_{i=1}^{m} {p_i}^{\alpha_i})^n) = V \Rightarrow$$

$$(\exists\, {p_i}^{\alpha_i} \in E = \{({p_1}^{\alpha_1}), ({p_2}^{\alpha_2}), ..., ({p_m}^{\alpha_m})\})(P(({p_i}^{\alpha_i})^n) = V)] = V$$

Mais,

Théorème A :

$$[^{\forall}\, p \text{ premier (pair ou impair)}$$

$$\forall y, x, n, \alpha \in N+, n > 2 : (p^{\alpha})^n \neq y^n \pm x^n, P((p^{\alpha})^n) = F] = V \Rightarrow$$

Théorème de Fermat-Wiles :

$$[^{\forall}\, Z, Y, X, n \in N+, n > 2 : Z^n \neq Y^n + X^n, P(Z^n) = F] = V$$

Remarques :

Je crois que c'est le schéma de démonstration annoncée par Pierre de Fermat (1601-1665).

La démonstration du théorème A :

$[^{\forall}\, p$ premier (pair ou impair) ,

$\forall y, x, n, \alpha \in N+, n > 2 : (p^{\alpha})^n \neq y^n \pm x^n, P((p^{\alpha})^n) = F] = V$,

comporte en fait deux démonstrations (arithmétiques, Ch3, Ch4) dont la plus courte est évidente ou immédiate.

Je crois aussi qu'Abel (1802-1829) s'était engagé (conjoncture d'Abel, 1823) à emprunter le chemin du schéma de démonstration annoncée par Fermat, mais la vie ne lui a pas laissé le temps nécessaire pour trouver une bonne direction.

Quant à moi, cela fait plus de 45 ans que je suis, de temps en temps, à la recherche de méthodes mathématiques dont les outils étaient connus de Fermat pour résoudre « l'énigme de Fermat ». J'ai essayé, sans succès, plusieurs méthodes (analyse, géométrie, arithmétique) ne faisant pas appel à la logique mathématique. C'est en reprenant l'étude des formes quadratiques binaires et des triplets pythagoriciens, surtout la généralisation des triplets pythagoriciens primitifs et la conjoncture d'Abel, que la logique mathématique bivalente m'est apparue être un outil salvateur.

Ahmed IDRISSI BOUYAHYAOUI

Chapitre 2

Démonstration probable de Fermat (1601 - 1665) :

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 $Z, Y, X, n \in N+$ et $n > 2$.»

De l'étude des formes quadratiques et ayant observé que si $z^2 = y^2 + x^2$, tout facteur premier ${p_j}^{\alpha_j}$ de zyx au carré est somme ou différence de deux puissances carrées :

$({p_j}^{\alpha_j})^2 = u^2 \pm v^2$, Fermat aurait déduit en généralisant la règle de réduction (méthode de « descente finie ») :

$$(P(Z^n) = V, n \in N+) \Rightarrow (Z^n = a^n b^n \Rightarrow (P(a^n) = V) \wedge (P(b^n) = V))$$

$(a, b \in N+, < a, b >= 1)$

Si $Z^n = Y^n + X^n$ alors, 2^α étant un facteur premier de ZYX, $(2^\alpha)^n = U^n \pm V^n$, égalité impossible pour n>2 , il en est de même de l'hypothèse $Z^n = Y^n + X^n, n > 2$.

Pour la forme quadratique simple $y^2 + x^2$, si $z^2 = y^2 + x^2$ alors tout facteur premier $({p_j}^{\alpha_j})^2$ de z^2 est de cette forme car :

- tout diviseur de $y^2 + x^2$ est de cette forme ;
- tout nombre impair est égal à la différence de deux carrés ;
- le nombre 2^β, pour $\beta > 2$, est égal à la différence de deux carrés .

D'où :

$(z^2 = y^2 + x^2; {p_j}^{\alpha_j} \mid zyx;\ p_j$premier ,

$x, y, z, \alpha_j \in N+) \Rightarrow (p_j{}^{\alpha_j})^2 = u^2 \pm v^2; u, v \in N+)$

Dans une lettre adressée à Mersenne en 1638, Fermat souhaite trouver deux cubes dont la somme est égale à un cube, deux bicarrés dont la somme est égale à un bicarré. Le même problème fut proposé à Frénicle en 1640 et à Wallis en 1657.

Une autre généralisation :
Fermat croyait tous premiers les nombres :

$F_n = 2^{2^n} + 1$(nombres de Fermat) .

Dans une lettre adressée à Frénicle en 1640, comme dans une autre adressée à Pascal en 1654, Fermat indique qu'il ne possède pas la démonstration assurée de son assertion.
Mais, Euler (1707-1783) constata que 641 divise exactement F_5.

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

Chapitre 3 :
Démonstration du grand théorème de Fermat
ou démonstration élémentaire du théorème de Fermat-Wiles:
Démonstration du théorème A :
Théorème A

$[\forall p$ premier (pair ou impair),
$\forall y, x, n, \alpha \in N+, n > 2 :$
$(p^\alpha)^n \neq y^n \pm x^n, P((p^\alpha)^n) = F] = V \Rightarrow$

Théorème de Fermat-Wiles :

$[\forall Z, Y, X, n \in N+, n > 2 : Z^n \neq Y^n + X^n, P(Z^n) = F] = V$

Démonstration :
Théorème F (chapitre 1) :

$[P(Z^n = (\prod_{i=1}^{m} {p_i}^{\alpha_i})^n) = V \Rightarrow$

$(\exists\, {p_i}^{\alpha_i} \in E = \{{p_1}^{\alpha_1}, {p_2}^{\alpha_2}, ..., {p_m}^{\alpha_m}\})(P(({p_i}^{\alpha_i})^n) = V)] = V$
Ce théorème indique une dérivation terminale de la règle de réduction :
$P(Z^n) = V \Rightarrow (Z^n = a^n b^n \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))$
$(a, b \in N+, < a, b >= 1)$

Soit ${p_j}^{\alpha_j}$ tel que $P(({p_j}^{\alpha_j})^n) = V$ et $({p_j}^{\alpha_j})^n = y^n \pm x^n,\ <\ p_j,\ y,\ x >= 1$.
Posons $q_0 = p_j$ et $\beta_0 = \alpha_j, q_0$ nombre premier (pair ou impair) .
Soit $({q_0}^{\beta_0})^n = {y_0}^n \pm {x_0}^n, q_0 = p_j, y_0 = y, x_0 = x, n > 2,$ la nouvelle hypothèse .
Posons $({q_k}^{\beta_k})^n = y_k^n \pm x_k^n, <\ q_k,\ y_k,\ x_k\ >= 1,\ q_k$ nombre premier, k=0,1,2,..

Un **résultat important**
qui permet une démonstration immédiate du grand théorème de Fermat :
Lucas a démontré en 1891 : si $x^n + y^n = z^n$, 0 < x < y < z, alors z, y ont au moins 2 facteurs premiers).
Markoff (1895), Sauer (1905), Mileikowsky (1932) contribuèrent à une démonstration affirmée. (in « 13 lectures on Fermat's Last Theorem », par Paulo Ribenboim, 1979).
Ce résultat , compte tenu de la règle de réduction établie plus haut, permet de construire une série numérique alternée divergente et de conclure à une impossibilité, la limite assignée étant finie .
On a $({q_k}^{\beta_k})^n = {y_k}^n - {x_k}^n, < q_k, y_k, x_k >= 1, q_k$ premier pair ou impair, avec la condition nécessaire $y_k - x_k = 1,$ d'où $q_k < x_k < y_k,$ et, puisque
$P({x_k}^n) = V, {x_k}^n = {a_k}^n({q_{k+1}}^{\beta_{k+1}})^n$ tel que $P(({q_{k+1}}^{\beta_{k+1}})^n) = V,$
d'où :
$({q_k}^{\beta_k})^n = {y_k}^n - {a_k}^n({q_{k+1}}^{\beta_{k+1}})^n, k = 0, 1, 2, ...$
et la **suite** engendrée :
$({q_0}^{\beta_0})^n = {y_0}^n - {a_0}^n({q_1}^{\beta_1})^n$
$({q_1}^{\beta_1})^n = {y_1}^n - {a_1}^n({q_2}^{\beta_2})^n$
…….
$({q_k}^{\beta_k})^n = {y_k}^n - {a_k}^n({q_{k+1}}^{\beta_{k+1}})^n$
……
A partir de cette suite on obtient, après développement, la **série numérique alternée** :
$({q_0}^{\beta_0})^n = {y_0}^n - {a_0}^n{y_1}^n + {a_0}^n{a_1}^n{y_2}^n - {a_0}^n{a_1}^n{a_2}^n{y_3}^n + \ldots\ldots\ldots\ldots\ldots$
$\ldots(-1)^{k+1}{a_0}^n{a_1}^n\ldots{a_k}^n{y_{k+1}}^n$
……
Comme $a_k \geq 2$ et $y_k \geq 2,$ la valeur absolue du terme général de la série est :
${a_0}^n{a_1}^n\ldots{a_k}^n{y_{k+1}}^n > \lim_{k\to\infty} 2^{n(k+1)} \to \infty$. Cette série numérique alternée est donc **divergente** et, par conséquence, l'égalité
$({q_0}^{\beta_0})^n = {y_0}^n - {x_0}^n, q_0, y_0, x_0, \beta_0, n \in N^+, n > 2,$ est impossible .
D'où le théorème de Fermat-Wiles :
$[\forall\ Z, Y, X, n \in N+, n > 2 : Z^n \neq Y^n + X^n, P(Z^n) = F] = V$

Comme le résultat obtenu par Lucas n'était pas connu de Fermat, je continue mon exposé dans le sens du cas général conforme à la définition donnée de la propriété P (chapitre 1) :
$(q_k{}^{\beta_k})^n = y_k{}^n \pm x_k{}^n$
.

Nombre de facteurs premiers dans x_k :
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.

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

Pour **n = 4 :**
1 - : $(2^{\beta_k})^4 = y_k^4 + x_k^4, 0 \equiv 2(mod4)$, 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 ($y_k^2 + x_k^2 \equiv 2\ (mod4)$).
Donc, l'égalité $(2^{\beta_k})^n = y_k^n \pm x_k^n, y_k, x_k, n, \beta_k \in N+$ et n>2, est impossible et, par suite, q_k est nécessairement impair et un des deux nombres x_k ou y_k est pair et a, nécessairement, au moins deux facteurs premiers.
Dans l'égalité $(q_k{}^{\beta_k})^n = y_k{}^n \pm x_k{}^n$, 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 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 :
$(q_k{}^{\beta_k})^n = \pm y_k^n \pm (2^{\alpha_k})^n a_k{}^n (q_{k+1}{}^{\beta_{k+1}})^n$, y_k et a_k sont des nombres impairs,
$a_k \geq 1$, k=0, 1, 2, … .
D'où la **suite** ($\pm$: + ou bien -, signes opératoires) :
$(q_0{}^{\beta_0})^n = \pm y_0^n \pm x_0^n = \pm y_0^n \pm (2^{\alpha_0})^n a_0{}^n (q_1{}^{\beta_1})^n$
$(q_1{}^{\beta_1})^n = \pm y_1{}^n \pm x_1^n = \pm y_1{}^n \pm (2^{\alpha_1})^n a_1{}^n (q_2{}^{\beta_2})^n$
...
$(q_k{}^{\beta_k})^n = \pm y_k^n \pm x_k^n = \pm y_k^n \pm (2^{\alpha_k})^n a_k{}^n (q_{k+1}{}^{\beta_{k+1}})^n$
....
Le terme général $(q_k{}^{\beta_k})^n$ de la suite $\{(q_k{}^{\beta_k})^n\}$, q_k nombre premier impair, est tel que $(q_k{}^{\beta_k})^n \geq 3^n$.

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 :

$(q_0{}^{\beta_0})^n = \pm y_0{}^n \pm (2^{\alpha_0})^n a_0{}^n y_1{}^n \pm (2^{\alpha_0})^n (2^{\alpha_1})^n a_0{}^n a_1{}^n y_2{}^n$
$\pm (2^{\alpha_0})^n (2^{\alpha_1})(2^{\alpha_2})^n a_0{}^n a_1{}^n a_2{}^n y_3{}^n \pm ... \pm 2^{\alpha_0})^n (2^{\alpha_1})^n (2^{\alpha_2})^n$
$...(2^{\alpha_k})^n a_0{}^n a_1{}^n ... a_k{}^n y_{k+1}{}^n \pm ....$

Pour simplifier l'écriture, posons :

$c_k = \alpha_0 + \alpha_1 + \alpha_2 + ... + \alpha_k,\ \alpha_k \geq 1$, k=0, 1, 2, … .

$c_k \geq k + 1$

$b_k = a_0 a_1 a_2 ... a_k,\ ;\ ;\ ;\ ; b_k$ 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

$R_k = \pm 2^{nc_k} (b_k{}^n y_{k+1}{}^n \pm 2^{n\alpha_{k+1}} b_{k+1}{}^n y_{k+2}{}^n \pm$... est de valeur absolue :

$|R_k| \geq 2^{n(k+1)}$ et $\lim_{k\to\infty} |R_k| \to \infty$, ce qui conduit à une **égalité impossible** puisque le nombre $(q_0{}^{\beta_0})^n$ est fini.

Donc l'égalité , $(q_0{}^{\beta_0})^n = y_0{}^n \pm x_0{}^n$ est impossible .

Autre formulation :

Le terme général de la série a une valeur absolue égale à : $2^{nc_k} b_k{}^n y_{k+1}{}^n$.

Comme $\lim_{k\to\infty} 2^{nc_{k+1}} \to \infty$, **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 $(q_0{}^{\beta_0})^n = y_0{}^n \pm x_0{}^n$ est impossible .

Les hypothèses,

$(p_j{}^{\alpha_j})^n = y^n \pm x^n, (q_k{}^{\beta_k})^n = y_k{}^n \pm x_k{}^n, q_0{}^{\beta_0} = p_j^{\alpha_j}, (k = 0, 1, 2, ...)$, (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 .

Ahmed IDRISSI BOUYAHYAOUI

Chapitre 4 :

Démonstration du théorème A :

Autre démonstration utilisant le caractère de divisibilité des nombres et le développement en suites et séries numériques :

Par hypothèse $Z^n = Y^n + X^n$ et

$P(Z^n) = P(Y^n) = P(X^n) = P((ZYX)^n) = V, < Z,\ Y,\ X\ >= 1$, donc nécessairement, au moins trois facteurs premiers distincts vérifient la propriété $P(a^n)$.

Soit q^{β} , un facteur premier impair de ZYX tel que $P((q^{\beta})^n) = V$ et soit 2^{α} , le facteur premier pair de ZYX tel que, supposons, $P((2^{\alpha})^n) = V$.

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.

Soit $(2^{\alpha})^n = y^n \pm x^n, < 2, y, x >= 1, n > 2 : n$**impair :**
L'égalité : $(2^{\alpha})^n = y^n \pm x^n = (y \pm x)[(y^n \pm x^n)/(y \pm x)]$est impossible, le premier membre est une puissance de 2 et dans le produit du second membre, le facteur $[(y^n \pm x^n)/(y \pm x)]$est impair .
n pair : n = 4
1 - : $(2^{\alpha})^4 = y^4 + x^4, 0 \equiv 2\ (mod\ 4)$, égalité impossible, ($y^4 + x^4$, supérieur à 4, n'est pas une puissance de 2) .
2 - : $(2^{\alpha})^4 = y^4 - x^4 = (y^2 - x^2)(y^2 + x^2)$, égalité impossible, le facteur $(y^2 + x^2)$, supérieur à 4, n'est pas une puissance de 2, $((y^2 + x^2) \equiv 2\ (mod\ 4))$.
Donc, l'égalité $(2^{\alpha})^n = y^n \pm x^n, y, x, n, \alpha \in N+$et n>2, est impossible.

Soit $(q^{\beta})^n = y^n \pm x^n, < q, y, x >= 1, q$**nombre premier impair :**
n = 4 : $(q^{\beta})^4 = y^4 \pm x^4$,
1 - : $(q^{\beta})^4 = y^4 - x^4 = (y^2 - x^2)(y^2 + x^2)$,
les deux facteurs (impairs) du produit du second membre étant premiers entre eux et leur produit étant égal à une puissance d'un nombre premier, cette égalité est donc impossible.
2 - : $(q^{\beta})^4 = y^4 + x^4$,
Posons
$(q_k{}^{\beta_k})^4 = y_k{}^4 + x_k{}^4, k = 0, 1, 2, ..., q_0 = q,\ \beta_0 = \beta,\ y_0 = y,\ x_0 = x, < q_k, y_k, x_k >= 1.$

D'où
$y_k{}^4 = ((q_k{}^{\beta_k})^2 - x_k{}^2)((q_k{}^{\beta_k})^2 + x_k{}^2), < br/ > x_k{}^4 = ((q_k{}^{\beta_k})^2 - y_k{}^2)((q_k{}^{\beta_k})^2 + y_k{}^2)$

et les nombres y_k et x_k ont chacun au moins deux facteurs premiers.
Comme $P(y_k{}^4 = (q_k{}^{\beta_k})^4 - x_k{}^4) = P(x_k{}^4 = (q_k{}^{\beta_k})^4 - y_k{}^4) = V$, on en déduit $x_k = a_k q_{k+1}{}^{\beta_{k+1}}$ tel que $P(q_{k+1}{}^{\beta_{k+1}})^n) = V, a_k \in N+, a_k \geq 2$ et l'on a
$(q_k{}^{\beta_k})^4 = y_k{}^4 + a_k{}^4 (q_{k+1}\beta_{k+1})^4$, k= 0, 1, 2, ….. .
D'où la **suite :**
$(q_0{}^{\beta_0})^4 = y_0{}^4 + x_0{}^4 = y_0{}^4 + a_0{}^4 (q_1{}^{\beta_1})^4$
$(q_1{}^{\beta_1})^4 = y_1{}^4 + x_1{}^4 = y_1{}^4 + a_1{}^4 (q_2{}^{\beta_2})^4$
……..
$(q_k{}^{\beta_k})^4 = y_k{}^4 + x_k{}^4 = y_k{}^4 + a_k{}^4 (q_{k+1}\beta_{k+1})^4$
……..

Comme $(q_0{}^{\beta_0})^4 > (q_1{}^{\beta_1})^4 > (q_2{}^{\beta_2})^4 > ... > (q_k{}^{\beta_k})^4 > \cdots$, la suite $\{(q_k{}^{\beta_k})^4\}$est décroissante indéfiniment. Cette « descente infinie » est impossible, les nombres premiers

impairs $q_k$étant supérieurs à 2 . L'égalité $(q_0{}^{\beta_0})^4 = y_0{}^4 + x_0{}^4$ est impossible .
Donc, l'égalité $(q^{\beta})^4 = y^4 + x^4$ est impossible .

Soit $(q^{\beta})^n = y^n + x^n$, $< q,y,x > = 1, n > 2$ et impair :
(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 :
$[(y^n + x^n) / (y + x)] = [[(y + x) - x]^n + x^n] / (y + x)$
$= [(y + x)^n - n(y + x)^{(n-1)}x + ... + n(y + x)x^{(p-1)}] / (y + x)$
$= (y + x)Q(y,x) + nx^{(p-1)}$ 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 p.g.c.d 1 ou p .
Si p.g.c.d = 1, les deux facteurs du second membre, $(y + x)$ et $[(yp + xp) / (y + x)]$, 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 p.g.c.d = p , alors p=q , et l'on a : $(q^{\beta})^q = (y + x)[(y + x)Q(y,x) + qx^{(p-1)}]$.
Les deux facteurs du second membre, $(y + x)$ *et* $[(y + x)Q(y,x) + qx^{(p-1)}]$, 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 $[(y + x)Q(y,x) + qx^{(p-1)}]$ 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 impossible .
Ainsi, l'égalité $(q^{\beta})^n = y^n + x^n$ est impossible .
Soit $(q^{\beta})^n = y^n - x^n, < q, y, x >= 1, q$ **premier impair, n impair > 2 :**
Posons
$(q_k{}^{\beta_k})^n = y_k{}^n - x_k{}^n, k = 0, 1, 2, ..., q_0 = q, \beta_0 = \beta, y_0 = y, x_0 = x.$
L'égalité $(q_k{}^{\beta_k})^n = y_k{}^n - x_k{}^n = (y - x)[(y^n - x^n)/(y - x)]$ implique nécessairement $y_k - x_k = 1$ et l'on a $y_k > x_k > q_k{}^{\beta_k}, y_k{}^n = x_k{}^n + (q_k{}^{\beta_k})^n$.
Le nombre x_k a au moins deux facteurs premiers sinon on aurait la contradiction :
$y_k - x_k = 1$ et $y_k{}^n = x_k{}^n + (q_k{}^{\beta_k})^n$ impliquant $y_k - q_k{}^{\beta_k} = 1$ et $x_k = q_k{}^{\beta_k}$, ce qui est impossible puisque $< q_k,y_k,x_k >=1$.
Posons $x_k = a_k q_{k+1}{}^{\beta_{k+1}}$ tel que $P((q_{k+1}{}^{\beta_{k+1}})n) = V, a_k \in N+, a_k \geq 2$, et $(q_k{}^{\beta_k})^n = y_k{}^n - a_k{}^n (q_{k+1}{}^{\beta_{k+1}})^n, q_k{}^{\beta_k}$ premier impair, k= 0, 1, 2, … .
D'où la **suite :**
$(q_0{}^{\beta_0})^n = y_0{}^n - x_0{}^n = y_0{}^n - a_0{}^n (q_1{}^{\beta_1})^n$
$(q_1{}^{\beta_1})^n = y_1{}^n - x_1{}^n = y_1{}^n - a_1{}^n (q_2{}^{\beta_2})^n$
……..
$(q_k{}^{\beta_k})^n = y_k{}^n - x_k{}^n = y_k{}^n - a_k{}^n (q_{k+1}{}^{\beta_{k+1}})^n$
……..

Le terme général $(q_k{}^{\beta_k})^n$ de la suite $\{(q_k{}^{\beta_k})^n\}$ est tel que $(q_k{}^{\beta_k})^n \geq 3^n$.

Développement en **série numérique alternée :**

La suite d'égalités ci-dessus permet d'associer à $(q_0^{\beta_0})^n$ une série numérique :

$(q_0^{\beta_0})^n = y_0^n - a_0^n(y_1^n - a_1^n(y_2^n$
$-a_2^n(y_3^n - ... - a_k^n(y_{k+1}^n - x_{k+1}^n)...))))$

D'où le développement en série alternée :

$(q_0^{\beta_0})^n = y_0^n - a_0^n y_1^n + a_0^n a_1^n y_2^n - a_0^n a_1^n a_2^n y_3^n + ... + (-1)^{k+1} a_0^n a_1^n ... a_k^n y_{k+1}^n ...$

Pour simplifier l'écriture, posons : $b_k = a_0 a_1 a_2 ... a_k, a_k \geq 2, k = 0, 1, ...$

$(q_0^{\beta_0})^n = y_0^n - b_0^n y_1^n + b_1^n y_2^n - b_2^n y_3^n + ... + (-1)^{k+1} b_k^n y_{k+1}^n ....$

Le terme général de la série a pour valeur absolue : $b_k^n y_{k+1}^n > 2^{n(k+1)}$.

Comme $\lim_{k \to \infty} 2^{n(k+1)} \to \infty$, la série est **divergente**.

La condition nécessaire de convergence (Cauchy) 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, $(q_0^{\beta_0})^n = y_0^n - x_0^n$ est impossible .

Les hypothèses, $(p_j^{\alpha_j})^n = y^n \pm x^n, (q_k^{\beta_k})^n = y_k^n \pm x_k^n, q_0^{\beta_0} = p_j^{\alpha_j}$, (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 .

Ahmed IDRISSI BOUYAHYAOUI

A ma mère, à mon épouse, à mes instituteurs, à mes professeurs, à mon père, à ma belle-mère, à mon beau-père, à mes enfants, à mes petits-enfants, au pays qui me porte, à l'amitié, aux sciences et à la culture.

Ahmed Idrissi Bouyahyaoui

Ce document provient de « http://fr.wikipedia.org/wiki/LOGIQUE_MATHEMATIQUE_CLASSIQUE,_ARITHMETIQUE_ET_FERMAT ».