LOGIQUE MATHEMATIQUE CLASSIQUE, ARITHMETIQUE ET FERMAT

(Formulation explicite de la preuve de l'établissement de la règle de réduction ou méthode de « descente finie »)

Démonstrations directes du grand théorème de Fermat (chapitre 1).

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, $n \in N^+$ et n>2. »

Le présent article décrit avec précision 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 cette propriété P attachée à une puissance donnée : $P(a^n)$.
Soit la proposition **$P(a^n)$ =** « **la puissance a^n est somme ou différence de deux puissances de même degré n** » .
Pour a et n entiers positifs donnés, la proposition $P(a^n)$ est vraie ($P(a^n)=V$) ou fausse ($P(a^n)=F$).

Cette notation est conforme à l'esprit et la lettre de l'énoncé du grand théorème de Fermat.
Exemples : $4^2 = 5^2 – 3^2$, $P(4^2) = V$, $P(2^4) = F$; nombres de la forme a^n .

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 :

Etablissement de la **propriété héritée :**
$(Z^n = Y^n + X^n$, Z, Y, X, $n \in N^+$, <Z, Y, X> =1) ==>
$(P(Z^n) = V$ == > $(Z^n = a^n b^n$, $(P(a^n) = V) \vee (P(b^n) = V)))$
(a, b € N^+ , <a, b> = 1)
C'est une **règle de réduction** ou **méthode de** «**descente finie**».

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 trois propositions dont au moins une est vraie :
1 - : $P(Z^n = a^n b^n) =V$ ==> $(P(a^n) = V) \wedge (P(b^n) = V)$ ou

2 - : $P(Z^n = a^n b^n) = V \implies (P(a^n) = V) \vee (P(b^n) = V)$ ou
3 - : $P(Z^n = a^n b^n) = V \implies (P(a^n) = F) \wedge (P(b^n) = F)$
Cette dernière proposition (3) est fausse.
Sa contraposée :
4 - : $[(P(a^n) = V) \vee (P(b^n) = V) \implies P(Z^n = a^n b^n) = F] = F$
est fausse puisque par hypothèse $P(Z^n = a^n b^n) = V$ et la multiplication étant distributive par rapport à l'addition et la soustraction, et associative, on doit avoir :
5 - : $[(P(a^n) = V) \vee (P(b^n) = V) \implies P(Z^n = a^n b^n) = V] = V$.
(les deux propositions (4) et (5) sont contradictoires et en vertu du principe du tiers exclu, la propositions (4) est à exclure)

Les règles de réduction ou méthodes de «descente finie» retenues sont donc :
6 - : $P(Z^n = a^n b^n) = V \implies (P(a^n) = V) \wedge (P(b^n) = V)$ ou
7 - : $[P(Z^n = a^n b^n) = V \implies (P(a^n) = V) \vee (P(b^n) = V)] = V$
où la règle (7) est nécessairement vraie.

La règle (6) : $P(Z^n = a^n b^n) = V \implies (P(a^n) = V) \wedge (P(b^n) = V)$, **règle probable de Fermat**, permet de déduire :
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 $Z^n = Y^n + X^n$, $n > 2$.

La règle de réduction ou méthode de «descente finie» (7) nécessairement vraie :
$[P(Z^n = a^n b^n) = V \implies (P(a^n) = V) \vee (P(b^n) = V)] = V$
permet, par réductions successives suivant des déductions (inférences) vraies, d'aboutir à la réduction terminale :

Théorème F :

$[P(Z^n = (\prod_{i=1}^{m} p_i^{\alpha i})^n) = V \implies$
$(\exists\, p_i^{\alpha i} \in E = \{ (p_1^{\alpha 1}), (p_2^{\alpha 2}), \ldots\ldots , (p_m^{\alpha m})\}) \mid (P((p_i^{\alpha i})) = V)] = V$
où $p_1, p_2, \ldots\ldots , p_m$ sont des nombres premiers.

Théorème A (chapitres 3 et 4) **:**

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

===>

Théorème de Fermat-Wiles :

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

Ahmed Idrissi Bouyahyaoui