LOGIQUE MATHEMATIQUE CLASSIQUE, ARITHMETIQUE ET FERMAT

Certaines lignes sont numérotées pour permettre de cibler les remarques éventuelles concernant les erreurs de formalisation et les erreurs de raisonnement .

Le grand théorème de Fermat :
1 **-** « 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. »
2 **-** Cette assertion a été écrite vers 1637 par Fermat sur une marge de son Diophante.

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

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

5 **–** Le présent article (chapitre 1) décrit avec précision une résolution de « l'énigme de Fermat » utilisant des outils mathématiques connus de Fermat .

6 **–** De l'énoncé littérale *1-* , comme de l'énoncé algébrique *3-*, on déduit **la propriété P :**
7 **-** P(a^n) : « La puissance a^n est égale à la somme ou à la différence de deux puissances de même degré $n, a, n \in N+$ »
Comme dans la logique bivalente (tiers exclu) : $P(a^n) \vee \neg Pa^n)$ = V ,
8 **-** la proposition P(a^n) est vraie et c'est noté P(a^n) = V
ou la proposition P(a^n) est fausse et c'est noté P(a^n) = F .

9 **-** 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 :

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

Propositions logiques :
12 **-** (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 :
$[(\forall\ a, b, n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))]$
(règle de réduction ou méthode de «descente finie»)
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 :
13 **-** (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) L12, a pour contraposée, proposition équivalente :
14 **-** (3) - :
$(\exists\, a, b, n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = F \Rightarrow (P(a^n) = V) \vee (P(< b^n)) = V))$
or 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.)
on a :

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

Ce qui est contradictoire (en logique bivalente (tiers exclu) on a : $P(a^n) \vee \neg P a^n) =$ V) .
La proposition (3) L14, contraposée de (2) L13, la contradictoire de (1) L12, mène à une contradiction, la proposition (1) L12 est donc vraie.
15 **-** La proposition (1) L12 étant vraie, sa contraposée, proposition équivalente, est vraie aussi :
$[(\forall\, a, b, n \in N+, Z = ab)$
$(P(Z^n = a^n b^n) = V \Rightarrow (P(a^n) = V) \vee (P(b^n) = V))] = V$
(règle de réduction ou méthode de «descente finie»)

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

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

16 **-** Cette règle de réduction ou méthode de «descente finie» permet, par réductions (dérivations) successives suivant des productions vraies, d'aboutir à la production terminale :

17 **-** Théorème F :

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

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

Formalisation :

18 **-** $P(a^n)$ est une proposition « concrète » déduite des énoncés 1- (ou 3-) , et où l'objet a^n, avec a et n des nombres entiers positifs, se définit par lui-même : une puissance de degré n .

19 **-** 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 .

20 **-** Par contre P(a, n) est un prédicat binaire où a et n peuvent être des variables quantifiées (liées) ou non (libres) et où l'objet (a, n) est une liste qu'il faut préciser être un couple (et non une paire) et qu'il faut ensuite identifier comme étant une puissance de facteur a et de degré n .

Exemples : $4^2 = 5^2 - 3^2$, $P(4,2) = V$, $P(2,4) = F$; couples (a,n) interprétés a^n .

21 **-** Bien sûr $P(a^n)$ et P(a, n) ont même définition mais l'objet a^n est plus concis, moins de quantité d'information et plus de sens .

Ainsi on a avec le prédicat P(Z, n) :

22 **-** Théorème F :

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

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

où la notion de puissance de degré n n'est pas mise en évidence .