

1. Preuve directe du théorème de Fermat-Wiles :

2. « $\forall z, \forall y, \forall x, \forall n \in \mathbb{N}^*, n > 2 : z^n \neq y^n + x^n$. »

3. Résumé :

4. Définitions :

5. $a, b, n \in \mathbb{N}^*$.

6. Une propriété $P(a,n)$ ou $\neg P(a,n)$ est attachée à toute puissance a^n :

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

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

8. $(a, b)=1$: a et b sont premiers entre eux ($\text{pgcd}(a,b)=1$).

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

10. 1 – Règle d'exclusion : $\neg P(a,n) \wedge \neg P(b,n) \rightarrow \neg P(axb,n)$

i. i.e. : $(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^n b^n \neq y^n + x^n$

– D'où le **Théorème F** :

11. $(Z = \prod_{i=1}^m p_i^{\alpha_i}) \wedge (\forall i : \neg P(p_i^{\alpha_i}, n)) \rightarrow (\neg P(\prod_{i=1}^m p_i^{\alpha_i}, n)) \rightarrow (\forall Y, \forall X \in \mathbb{N}^* : Z^n \neq Y^n + X^n)$

12. où $n, \alpha_i, m \in \mathbb{N}^*, i=1,2, \dots, m$, et p_1, p_2, \dots, p_m des nombres premiers.

13. 2 – Règle de réduction : $P(axb,n) \rightarrow P(a,n) \vee P(b,n)$

i. i.e. : $a^n b^n = y^n + x^n \rightarrow (a^n = r^n + s^n) \vee (b^n = u^n + v^n)$

– D'où le **Théorème F bis** :

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

15. $(\exists p_i^{\alpha_i} \in E = \{ p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_m^{\alpha_m} \} \text{ tel que } (P(p_i^{\alpha_i}, n), (p_i^{\alpha_i})^n = y^n + x^n)$

16. où $Y, X, y, x, n, \alpha_i, m \in \mathbb{N}^+$, et p_1, p_2, \dots, p_m des nombres premiers

17. 3 – Théorème A :

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

19. \rightarrow le théorème de Fermat-Wiles :

20. $(\forall Z, \forall Y, \forall X, \forall n \in \mathbb{N}^*) \wedge (n > 2) \wedge (Z = \prod_{i=1}^m p_i^{\alpha_i}) :$

21. $\prod_{i=1}^m \neg P(p_i^{\alpha_i}, n) \rightarrow \neg P(\prod_{i=1}^m p_i^{\alpha_i}, n) \rightarrow Z^n \neq Y^n + X^n$.

22. Chapitre 1 :

23. Preuve directe de la règle d'exclusion :

(1) Comme

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

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

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

27. les prémisses qui sont composées des propositions négatives :

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

29. Les propositions existentielles (particulières) contenant exclusivement ces prémisses

30. doivent être des inférences immédiates vraies (Aristote) et elles sont donc vraies si et

31. seulement si leurs conclusions sont vraies.

32. 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),

33. les prémisses qui comportent des propositions affirmatives :

34. $P(a,n)$, $P(b,n)$ ou $P(a \times b, n)$, sont vraies ou fausses.

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

Exemple : la proposition logiquement vraie (formellement vraie) :

35. $(\forall (a, b, n) \in \mathbb{N}^{*3}) \wedge ((a, b) = 1) : P(a, n) \vee P(b, n) \rightarrow P(a \times b, n)$,

36. i.e. : $(a^n = r^n + s^n) \vee (b^n = u^n + v^n) \rightarrow a^n b^n = a^n (u^n + v^n) + b^n (r^n + s^n)$

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

38. Principe du tiers exclu :

39. $\forall (a, b, n) \in \mathbb{N}^{*3} : (\neg P(a, n) \wedge \neg P(b, n)) \vee (P(a, n) \vee P(b, n)) = \text{Vrai}$.

40. Principe de la non-contradiction :

41. $\forall (a, b, n) \in \mathbb{N}^{*3} : (\neg P(a, n) \wedge \neg P(b, n)) \wedge (P(a, n) \vee P(b, n)) = \text{Faux}$.

42. On peut écrire les propositions suivantes :

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

44. **1** - Etant donnée la proposition, déduite de (1), de prémisses et conclusion vraies :

45. **(11)** $(\exists (a, b, r, s, u, v, y, x, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) :$

a. $(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^n b^n \neq y^n + x^n$

b. de subcontraire :

46. **(12)** $(\exists (a, b, r, s, u, v, y, x, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) :$

a. $(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^n b^n = y^n + x^n$

b. fautive, puisque sa contraposée :

47. **(13)** $(\exists (a, b, r, s, u, v, y, x, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) :$

a. $a^n b^n \neq y^n + x^n \rightarrow (a^n = r^n + s^n) \vee (b^n = u^n + v^n)$ ($\neg P(a \times b, n) \wedge P(a \times b, n) = \text{Faux}$)

b. est fautive, la prémisses vraie est en contradiction avec la conclusion puisque :

i. $(a^n = r^n + s^n) \vee (b^n = u^n + v^n)$

ii. $\rightarrow a^n b^n = (r^n + s^n) b^n$ ou $a^n (u^n + v^n) = ((br)^n + (bs)^n)$ ou $((au)^n + (av)^n)$

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

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

49. **(14)** $(\forall (a, b, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) : \neg P(a, n) \wedge \neg P(b, n) \rightarrow \neg P(a \times b, n)$

50. **2** - La proposition :

51. **(21)** $(\forall (a, b, r, s, u, v, y, x, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) :$

a. $(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^n b^n \neq y^n + x^n$

b. est vraie car sa contradictoire :

52. **(22)** $(\exists (a, b, r, s, u, v, y, x, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) :$

a. $(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^n b^n = y^n + x^n$

- b. est fausse puisque sa contraposée :
53. (23) $(\exists (a, b, r, s, u, v, y, x, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1)$:
- a. $a^n b^n \neq y^n + x^n \rightarrow (a^n = r^n + s^n) \vee (b^n = u^n + v^n)$ $(\neg P(a \times b, n) \wedge P(a \times b, n) = \text{Faux})$
- b. est fausse, la prémisse vraie est en contradiction avec la conclusion puisque :
- i. $(a^n = r^n + s^n) \vee (b^n = u^n + v^n)$
- ii. $\rightarrow a^n b^n = (r^n + s^n) b^n$ ou $a^n (u^n + v^n) = ((br)^n + (bs)^n)$ ou $((au)^n + (av)^n)$
- c. l'implication (23) est fausse et, par équivalence, sa contraposée (22) l'est aussi.

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

55. (24) $(\forall (a, b, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) : \neg P(a, n) \wedge \neg P(b, n) \rightarrow \neg P(a \times b, n)$
1. i.e. : $(a^n \neq r^n + s^n) \wedge (b^n \neq u^n + v^n) \rightarrow a^n b^n \neq y^n + x^n$

56. 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 .

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

58. $(Z = \prod_{i=1}^m p_i^{\alpha_i}) \wedge (\forall i : \neg P(p_i^{\alpha_i}, n)) \rightarrow (\neg P(\prod_{i=1}^m p_i^{\alpha_i}, n)) \rightarrow (\forall Y, \forall X \in \mathbb{N}^* : Z^n \neq Y^n + X^n)$
59. où $n, \alpha_i, m \in \mathbb{N}^*$, $i=1, 2, \dots, m$, et p_1, p_2, \dots, p_m des nombres premiers.

60. La **règle d'exclusion**, proposition de prémisse et conclusion vraies,, a pour contraposée la **règle de réduction**, proposition logiquement vraie (formellement vraie) :

61. (25) $(\forall (a, b, n) \in \mathbb{N}^{*3}) \wedge (n > 1) \wedge ((a, b) = 1) : P(a \times b, n) \rightarrow P(a, n) \vee P(b, n)$
1. i.e. : $a^n b^n = y^n + x^n \rightarrow (a^n = r^n + s^n) \vee (b^n = u^n + v^n)$

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

63. **Théorème F-bis** :

64. $(Z^n = Y^n + X^n, Z = \prod_{i=1}^m p_i^{\alpha_i}, P(\prod_{i=1}^m p_i^{\alpha_i}, n)) \rightarrow$
65. $[\exists p_i^{\alpha_i} \in E = \{p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_m^{\alpha_m}\} \text{ tel que } (P(p_i^{\alpha_i}, n), (p_i^{\alpha_i})^n = y^n + x^n)]$
66. où $Y, X, y, x, n, \alpha_i, m \in \mathbb{N}^+$, et p_1, p_2, \dots, p_m des nombres premiers.

67. Or le **théorème A** contredit la conclusion du théorème F-bis .

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

69. **Théorème A** :

70. $(\forall p \text{ premier pair ou impair } \forall y, \forall x, \forall n, \forall \alpha \in \mathbb{N}^*) \wedge (n > 2) : \neg P(p^\alpha, n), (p^\alpha)^n \neq y^n + x^n .$
71. \rightarrow le théorème de Fermat-Wiles :
72. $(\forall Z, \forall Y, \forall X, \forall n \in \mathbb{N}^*) \wedge (n > 2) \wedge (Z = \prod_{i=1}^m p_i^{\alpha_i}) :$
73. $\prod_{i=1}^m \neg P(p_i^{\alpha_i}, n) \rightarrow \neg P(\prod_{i=1}^m p_i^{\alpha_i}, n) \rightarrow Z^n \neq Y^n + X^n .$

74. Chapitre 2 :

75. Démonstration du théorème A :

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

77. 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.

78. Soit q^α un facteur premier :

79. Pour $q=2$:

80. Pour n impair > 2 :

81. 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. [$y > x \geq 1 \rightarrow (y^n + x^n)/(y+x) > 1$].

82. Pour $n = 4$:

83. $(2^\alpha)^4 = y^4 + x^4$, $0 \equiv 2 \pmod{4}$, égalité impossible.

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

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

86. Pour $n = 4$:

87. $(q^\beta)^4 = y^4 + x^4$,
supposons y impair,

88. d'où :

$y^4 = ((q^\beta)^2 - x^2)((q^\beta)^2 + x^2)$, où les deux facteurs du second membre sont

89. premiers entre eux et, leur produit étant un carré, ils sont chacun un carré :

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

91. Pour n impair :

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

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

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

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

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

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

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

94. 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 .

95. Si p.g.c.d = 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 p.g.c.d = 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

96. $[(y + x)Q(y,x) + qx^{(q-1)}]$ 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 .

97. D'où le **Théorème A** (A: en hommage à Abel) :

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

99. → le théorème de Fermat-Wiles :

100. $(\forall Z, \forall Y, \forall X, \forall n \in \mathbb{N}^*) \wedge (n > 2) \wedge (Z = \prod_{i=1}^m p_i^{\alpha_i}) :$

101. $\prod_{i=1}^m \neg P(p_i^{\alpha_i}, n) \rightarrow \neg P(\prod_{i=1}^m p_i^{\alpha_i}, n) \rightarrow Z^n \neq Y^n + X^n,$

102. où $n, \alpha_i, m \in \mathbb{N}^*, i=1,2, \dots, m$, et p_1, p_2, \dots, p_m des nombres premiers.

Ahmed Idrissi Bouyahyaoui

© INPI – Paris