

BULLETIN DE LA S. M. F.

E. MAILLET

Sur l'équation indéterminée $a^m + b^m = c^m$ en nombres entiers différents de zéro, quand m est fractionnaire et sur une équation analogue plus générale

Bulletin de la S. M. F., tome 45 (1917), p. 26-36

http://www.numdam.org/item?id=BSMF_1917__45__26_1

© Bulletin de la S. M. F., 1917, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

**SUR L'ÉQUATION INDÉTERMINÉE $a^m + b^m = c^m$, EN NOMBRES
ENTIERS DIFFÉRENTS DE ZÉRO, QUAND m EST FRACTION-
NAIRE, ET SUR UNE ÉQUATION ANALOGUE PLUS GÉNÉRALE;**

PAR M. EDMOND MAILLET.

I. Nous nous occupons ici principalement de l'équation indéterminée

$$(1) \quad a^m + b^m = c^m$$

en nombres entiers ⁽¹⁾ tous $\neq 0$, dans le cas où $m = \frac{n}{p}$ est un nombre rationnel > 0 , n et p étant premiers entre eux, et $p > 1$. Cette équation a déjà été envisagée ⁽²⁾; mais il ne semble pas que des résultats un peu étendus aient été obtenus à son sujet pour $n > 2$; un Mémoire annoncé par M. Dutordoir n'a jamais été publié à notre connaissance. Lorsque n est égal à 1 ou 2, l'équation (1) admet les solutions évidentes connues

$$a = a_1^p, \quad b = b_1^p, \quad c = c_1^p,$$

où a_1, b_1, c_1 sont les systèmes d'entiers $\neq 0$ en nombre infini

⁽¹⁾ Sauf indication contraire, cette expression et celle de nombre rationnel s'appliqueront toujours à des nombres entiers ou rationnels ordinaires ou naturels.

⁽²⁾ Voir, par exemple, DUTORDOIR, *Annales de la Société scientifique de Bruxelles*, t. XVII, 1893, p. 81; CASHMORE, *Fermat's last theorem*, Londres, 1916.

satisfaisant à

$$(1 \text{ bis}) \quad a_1^n + b_1^n = c_1^n.$$

Le théorème que l'on peut considérer comme vraisemblable et que nous établirons, par exemple, pour $m > 1$ et dans d'autres cas, c'est que l'équation (1), n étant quelconque, équivaut à l'équation (1 bis), qui fait l'objet du dernier théorème de Fermat, pour chaque valeur de n , et présente, par suite, comme elle, de nombreux cas certains d'impossibilité pour $n > 2$.

Il y a un théorème analogue pour l'équation indéterminée $a^{m_1} + b^{m_2} = c^{m_3}$, où les $m_i (i = 1, 2, 3)$ sont des nombres rationnels > 0 , a, b, c étant des entiers premiers entre eux deux à deux : nous l'établissons, par exemple, quand un des m_i est > 1 . Enfin, il y en a un aussi pour l'équation analogue à (1) avec m rationnel négatif et égal à $-m_1$, équation qui équivaut à l'équation (1) pour $m = m_1$.

II. Envisageons l'ensemble des entiers et des racines $p^{\text{ièmes}}$ d'entiers. L'ensemble ou corps formé à l'aide de ces nombres par addition, soustraction ou multiplication est composé de nombres entiers algébriques; en effet, les entiers ordinaires et leurs racines $p^{\text{ièmes}}$ sont des entiers algébriques; de plus, la somme, la différence, le produit de deux entiers algébriques sont des entiers algébriques (1).

Rappelons encore que, si α, β, γ sont des entiers algébriques tels que γ divise α et β , γ divise aussi $\alpha + \beta$ et $\alpha - \beta$.

Pour déterminer les solutions de (1), on peut toujours supposer a, b, c premiers entre eux deux à deux.

Si, en effet, les entiers ordinaires a et b par exemple sont divisibles par le nombre premier ordinaire λ , on a

$$a = \lambda a', \quad b = \lambda b', \quad c^{\frac{n}{p}} = \lambda^{\frac{n}{p}} \left(a'^{\frac{n}{p}} + b'^{\frac{n}{p}} \right) = \lambda^{\frac{n}{p}} \delta,$$

où δ est un entier algébrique; λ divise c , car δ^p est un entier ordinaire. Le raisonnement est analogue quand on suppose que c et,

(1) DIRICHLET, *Vorlesungen über Zahlentheorie*, 3^e édition, 1879, p. 452 et suiv.

par exemple, a ont un diviseur premier commun λ_1 : celui-ci divise b . Si donc (1) a une solution en entiers a, b, c ayant le plus grand commun diviseur d , soit $a = a''d, b = b''d, c = c''d$; a'', b'', c'' sont premiers entre eux deux à deux et solutions de (1); inversement toute solution a'', b'', c'' de (1) en donne une solution a, b, c , quel que soit d .

III. Envisageons donc l'équation (1) avec $a, b, c \neq 0$ et premiers entre eux deux à deux. On a

$$(2) \quad c^n = (a^m + b^m)^p = a^n + b^n + C_p^1 a^m b^{n-m} + \dots + C_p^\alpha a^{m\alpha} b^{n-m\alpha} + \dots$$

Soient λ un nombre premier qui divise a , mais non p, λ^k la plus haute puissance de λ qui divise a ; on a

$$(3) \quad c^n - a^n - b^n = C_p^1 a^m b^{n-m} + \dots;$$

dans le deuxième membre, les termes non écrits sont tous divisibles par a^{2m} , par suite par λ^{2mk} ; le premier terme l'est (1) par λ^{mk} et non par $\lambda^{\frac{n_1}{p}}$ avec n_1 entier $> kn$.

Donc $c^n - a^n - b^n$ est divisible par λ^{km} et non par $\lambda^{km + \frac{1}{p}}$; il en résulte [note (1) précédente, 3°] $kn = hp$ et, puisque n est premier à $p, k = k'p$ (k' entier).

Ainsi, l'exposant de la plus haute puissance de tout diviseur premier de a , lorsque ce diviseur est premier à p , est multiple de p ; a est de la forme $a = a_1^p a_2$, où a_1 est premier à p , tandis que les diviseurs premiers de a_2 divisent tous p . On a, de même,

(1) Soient $A, B, C, \theta, \theta_1$ des entiers > 0 ; $\delta, \delta_1, \delta_2$ des entiers algébriques :

1° Si $A^{\frac{\theta_1}{p}} = B^{\frac{\theta}{p}} \cdot \delta, B^\theta$ divise A^θ , et réciproquement; on le voit de suite en remarquant que δ^p est un entier ordinaire; quand $\theta = \theta_1, B$ divise A .

2° Si $\delta_1 = A^{\theta_1} B^{\frac{\theta_1}{p}} C$, soit λ^k la plus haute puissance du nombre premier λ , premier à B et C , qui divise A : la plus haute puissance de $\lambda^{\frac{1}{p}}$ qui divise δ_1 est $\lambda^{k\theta_1}$; on le voit de suite en considérant δ_1^p .

3° Si $A = \lambda^{\theta_1} \delta_2$, où δ_2 n'est pas divisible par $\lambda^{\frac{1}{p}}$, on a $\theta n = hp$ (h entier). On le voit en envisageant δ_2^p , qui est un entier premier à λ .

$b = b_1^p b_2$, où les diviseurs premiers de b_2 divisent p , tandis que b_1 est premier à p .

D'autre part, d'après (1),

$$(4) \quad b^n = (c^m - a^m)^p = c^n + (-1)^p [\alpha^n - C_p^1 c^m \alpha^{n-m} + \dots];$$

en raisonnant sur c et cette formule comme on l'a fait sur a et la formule (2), on voit que $c = c_1^p c_2$, où les diviseurs premiers de c_2 divisent p , tandis que c_1 est premier à p . On obtient alors ce résultat :

THÉORÈME I. — *La résolution de l'équation (1) équivaut à celle de l'équation*

$$(5) \quad a_2^m a_1^n + b_2^m b_1^n = c_2^m c_1^n,$$

où a_1, b_1, c_1 , premiers deux à deux, sont premiers à p , tandis que a_2, b_2, c_2 , premiers aussi deux à deux, n'ont d'autres diviseurs premiers que ceux de p .

IV. Reprenons la formule (3), en désignant maintenant par λ un diviseur premier commun de p et de a , par suite de a_2 . Soient λ^k et λ^l les plus hautes puissances de λ qui divisent p et a .

Nous avons besoin, pour la suite, de savoir déterminer la plus haute puissance de λ qui divise

$$C_p^\alpha = \frac{p!}{\alpha! (p-\alpha)!}, \quad \alpha \leq \frac{p}{2},$$

au moins dans des cas étendus. Soit

$$\alpha = A_0 \lambda^i + A_1 \lambda^{i-1} + \dots + A_i, \quad A_0 > 0, \quad 0 \leq A_j < \lambda \quad (j = 0, 1, \dots, i),$$

le nombre α écrit dans le système de numération de base λ . On sait (1), ou l'on voit facilement, que la plus haute puissance de λ qui divise $\alpha!$ est λ^{e_α} , avec

$$(6) \quad e_\alpha = \frac{\alpha - (A_0 + A_1 + \dots + A_i)}{\lambda - 1}.$$

Soit λ^{f_α} la plus haute puissance de λ qui divise C_p^α ; proposons-

(1) *Encyclopédie des Sciences mathématiques* (J. Molk), t. I, vol. 3, fasc. 1, p. 4.

nous de trouver, dans la suite f_1, f_2, \dots , des f_α d'indices croissants, la suite S de ceux qui sont plus petits que les nombres analogues d'indice plus petit.

Admettons que α soit divisible par λ^s et non par λ^{s+1} ($s = 0, 1, 2, \dots$). On a, s_1 étant $\leq s$,

$$C_p^{\alpha+\lambda^s} = C_p^\alpha \frac{N}{D},$$

avec

$$N = (p - \alpha) \dots (p - \alpha - \lambda^{s_1} + 1), \quad D = (\alpha + 1) \dots (\alpha + \lambda^{s_1}).$$

N et D sont chacun le produit de λ^{s_1} nombres consécutifs; dans un pareil produit il y a un facteur φ_{s_1} divisible par λ^{s_1} et qui peut être divisible par une puissance de λ d'exposant supérieur à s_1 , $\lambda - 1$ autres facteurs divisibles par λ^{s_1-1} et non par λ^{s_1} , $\lambda^2 - \lambda$ autres facteurs divisibles par λ^{s_1-2} et non par λ^{s_1-1}, \dots . Soit

$$\sigma = s_1 + (\lambda - 1)(s_1 - 1) + (\lambda^2 - \lambda)(s_1 - 2) + \dots = \frac{\lambda^{s_1} - 1}{\lambda - 1}.$$

D, divisible par λ^σ ne pourra l'être par $\lambda^{\sigma+1}$ que si le facteur $\varphi_{s_1} = \alpha + \lambda^{s_1}$ de D l'est par λ^{s_1+1} , ce qui exige $s = s_1$; si donc $s > s_1$, ou si $\alpha + \lambda^s$, avec $s = s_1$, n'est pas divisible par λ^{s+1} , N étant divisible par λ^σ , on a

$$f_{\alpha+\lambda^s} \geq f_\alpha.$$

Faisant successivement $s = 0, 1, 2, \dots$, on voit que les valeurs de f_α appartenant à la suite S font partie des valeurs

$$g_s = f_{\lambda^s} \quad (s = 0, 1, 2, \dots);$$

car si le nombre $\nu = \nu_1 \lambda^s$, avec ν_1 premier à λ et > 1 , f_ν ne fait pas partie de S, puisque $f_\nu \geq f_{\nu-\lambda^s}$, que $\nu_1 - 1$ soit ou non divisible par λ . On a

$$g_s = e_p - e_\alpha - e_{p-\alpha} \quad (\alpha = \lambda^s),$$

$$e_\alpha = \frac{\alpha - 1}{\lambda - 1} = \frac{\lambda^s - 1}{\lambda - 1};$$

si le nombre p s'écrit

$$p = \lambda^{t_1}(B_0 \lambda^{t_1} + B_1 \lambda^{t_1-1} + \dots + B_{t_1}) \quad (B_0 > 0, B_{t_1} > 0),$$

dans le système de numération de base λ , on a

$$e_p = \frac{p - (B_0 + \dots + B_{t_1})}{\lambda - 1};$$

quant à $p - \alpha$, si $s \geq k_1$ et si le coefficient B_{k_1+t-s} de λ^s dans p est $\neq 0$, on a

$$(7) \quad e_{p-\alpha} = \frac{p - \lambda^s - (B_0 + \dots + B_{t-1})}{\lambda - 1};$$

dans les autres cas, posant $B_{t+1} = \dots = B_{t+k_1} = 0$, soit B_{k_1+t-u} le premier des coefficients

$$B_{k_1+t-s-1}, \quad B_{k_1+t-s-2}, \quad \dots,$$

qui soit $\neq 0$; $p - \alpha$ s'écrit dans le système de numération de base λ

$$p - \alpha = B_0 \lambda^{k_1+t} + \dots + (B_{k_1+t-u} - 1) \lambda^u + (\lambda - 1) \lambda^{u-1} + \dots \\ + (\lambda - 1) \lambda^s + B_{k_1+t-s+1} \lambda^{s-1} + \dots$$

et

$$(8) \quad e_{p-\alpha} = \frac{p - \lambda^s - (B_0 + \dots + B_{t-1}) - (\lambda - 1)(u - s)}{\lambda - 1}.$$

On a ainsi

$$(9) \quad \begin{cases} g_s = 0 & \text{avec la formule (7),} \\ g_s = u - s & \text{avec la formule (8).} \end{cases}$$

Par conséquent :

1° Quand $s < k_1$, la seconde formule (9) ayant lieu,

$$k_1 + t - u = t, \quad u = k_1, \quad g_s = k_1 - s;$$

2° Quand $s = k_1$,

$$g_s = 0, \quad \text{car} \quad B_t \neq 0;$$

3° Quand $s > k_1$,

$$g_s = 0 \quad \text{si} \quad B_{k_1+t-s} \neq 0$$

et

$$g_s = u - s \leq k_1 + t - s < t \quad \text{si} \quad B_{k_1+t-s} = 0.$$

V. Ceci posé, l'équation (3) a pour terme général dans le deuxième membre $C_p^\alpha a^{m\alpha} b^{n-m\alpha}$, lequel est divisible par λ^{d_α} et non par $\lambda^{d_\alpha + \frac{1}{p}}$, si

$$d_\alpha = f_\alpha + k m \alpha.$$

Cherchons la plus petite valeur d_{α_1} de d_α ; $k m \alpha$ croissant avec α , f_α sera plus petit que f_α quand $\alpha < \alpha_1$ et fera partie de la suite S;

d_{α_1} sera un des nombres

$$(10) \quad G_s = g_s + km\lambda^s.$$

Or $G_{k_1} = km\lambda^{k_1}$ est plus petit que G_s pour $s > k_1$ (au cas où l'on peut avoir $s > k_1$); α_1 correspond donc à un des nombres (10) avec $s \leq k_1$, pour lesquels

$$(11) \quad G_s = k_1 - s + km\lambda^s.$$

Considérons dans (11) G_s comme fonction continue de s ; on a

$$G'_s = km\lambda^s L\lambda - 1, \quad G''_s = km\lambda^s (L\lambda)^2 > 0.$$

Nous nous bornerons à conclure que G'_1 est positif et plus petit que G'_s , pour $s > 1$, si

$$(12) \quad km\lambda L\lambda \geq 1;$$

supposant cette condition remplie, d_{α_1} est l'un des nombres G_0, G_1 ; ce sera G_0 si

$$\begin{aligned} k_1 + km &< k_1 - 1 + km\lambda, \\ km(\lambda - 1) &> 1; \end{aligned}$$

cette condition et, *a fortiori*, la condition (12) seront remplies si

$$(13) \quad m > \frac{1}{\lambda - 1}.$$

Admettant que (13) ait lieu; dans le deuxième membre de (3), le premier terme est divisible par λ^{k_1+km} et non par $\lambda^{k_1+km+\frac{1}{p}}$ qui divise chacun des autres termes; donc $c^n - a^n - b^n = \lambda^{k_1+km}\delta$, où δ est un entier algébrique non divisible par $\lambda^{\frac{1}{p}}$. Il en résulte [n° III, note (1), 3°], par la considération de δ^p , que $k_1 + km$ est un entier, c'est-à-dire $k = k'p$, où k' est entier; la plus haute puissance de λ qui divise a est $\lambda^{k'p}$.

Un raisonnement identique s'applique à chacun des diviseurs premiers de p qui divisent a ou b , et même, avec quelques changements de signes, à ceux qui divisent c d'après (4), pourvu que chacun de ces diviseurs satisfasse à (13). Donc :

THÉORÈME II. — *L'équation (5) du théorème I peut se mettre*

sous la forme

$$(14) \quad a_2^m a_1^n + b_2^m b_1^n = c_2^m c_1^n,$$

où $a_1', b_1', c_1', a_2', b_2', c_2'$ sont premiers entre eux deux à deux, et a_2', b_2', c_2' n'ont d'autres facteurs premiers λ que ceux de p qui satisfont à

$$(15) \quad m \leq \frac{1}{\lambda - 1}.$$

En particulier :

COROLLAIRE. — Si, μ étant le plus petit facteur premier de p , on a

$$(16) \quad m > \frac{1}{\mu - 1},$$

l'équation (1) équivaut à une équation de la forme (1 bis).

Ce résultat comprend un de ceux annoncés au n° I.

VI. Nous pouvons encore établir le résultat suivant :

THÉORÈME III. — Si, dans l'équation (5) du théorème I, un des nombres ordinaires a_2, b_2, c_2 est une puissance $p^{\text{ième}}$ exacte d'un nombre ordinaire, cette équation équivaut encore à une équation de la forme (1 bis). Il en est ainsi en particulier quand p n'a pas plus de deux facteurs premiers distincts.

De même, (14) équivaut à (1 bis) si a_2', b_2' ou c_2' est une puissance $p^{\text{ième}}$ exacte.

En effet, soient, par exemple,

$$b_2 = \beta^p, \quad a_2 = \alpha^{\varpi_1 \theta_1}, \quad c_2 = \gamma^{\varpi_2 \theta_2}, \quad p = \varpi_1 p_1 = \varpi_2 p_2,$$

où α, γ ne sont puissances d'aucun autre nombre, où θ_1 est premier à p_1 , θ_2 à p_2 , tandis que ϖ_1 et ϖ_2 divisent p ; soit, par exemple $p_2 \leq p_1$. On a

$$(17) \quad x^{p_1} = \alpha^{\theta_1 n}, \quad z^{p_2} = \gamma^{\theta_2 n}, \quad [a_1^n x + (b_1 \beta)^n]^{p_2} = c_1^{p_2 n} \gamma^{\theta_2 n},$$

d'après (5).

Si $p_1 = 1$, on a $p_2 = 1$, a_2, b_2, c_2 sont des puissances $p^{\text{ièmes}}$ exactes et (5) peut se mettre sous la forme (1 bis). D'autre part on ne peut avoir $p_1 > 1$, sans quoi, θ, n étant premier à p_1 et $p_2 \leq p_1$, la première équation (17) ne serait pourtant pas irréductible, contrairement à ce qu'on sait (1), à cause de la dernière équation (17).

On peut raisonner de même, soit quand $p_1 \leq p_2$, soit quand c'est a_2 ou c_2 , et non b_2 , qui est une puissance $p^{\text{ième}}$ exacte.

L'extension à (14) est évidente.

c. q. f. d.

COROLLAIRE. — *Quand p a au moins trois facteurs premiers distincts, soient μ_1, μ_2, μ_3 avec $\mu_1 < \mu_2 < \mu_3$, les trois plus petits. Si l'on a*

$$m > \frac{1}{\mu_3 - 1},$$

l'équation (1) et l'équation (5) équivalent encore à une équation de la forme (1 bis).

En effet, dans ce cas, l'inégalité (15) ne peut avoir lieu que si λ est égal à μ_1 ou à μ_2 . Dans l'équation (14), a'_2, b'_2, c'_2 , premiers entre eux deux à deux, ne peuvent avoir d'autres facteurs premiers que μ_1 et μ_2 , c'est-à-dire que l'un d'eux se réduit à l'unité; le théorème III ci-dessus s'applique.

VII. Tous les raisonnements, calculs et résultats précédents s'étendent à l'équation indéterminée

$$(18) \quad a^{m_1} + b^{m_2} = c^{m_3},$$

où a, b, c sont des entiers ordinaires $\neq 0$ et premiers entre eux deux à deux (2), et où

$$m_1 = \frac{N_1}{P_1} = \frac{n_1}{p}, \quad m_2 = \frac{N_2}{P_2} = \frac{n_2}{p}, \quad m_3 = \frac{N_3}{P_3} = \frac{n_3}{p},$$

(1) TH. VAHLEN, *Acta mathematica*, t. XIX.

(2) On pourrait chercher à supprimer cette dernière restriction en essayant de ramener, comme au n° II, le cas où a, b, c sont des entiers quelconques au cas où a, b, c sont premiers entre eux deux à deux; mais des difficultés spéciales apparaissent. Toutefois on les surmonte assez facilement quand on suppose que deux des quantités n_1, n_2, n_3 sont égales entre elles et multiples de la troisième.

$\frac{N_i}{P_i}$ ($i = 1, 2, 3$) étant une fraction irréductible et p le plus petit commun multiple de P_1, P_2, P_3 . On opérera presque mot pour mot de la même manière.

Le théorème que l'on peut espérer établir, c'est que l'équation (18) équivaut à l'équation

$$(18 \text{ bis}) \quad a_1^{N_1} + b_1^{N_2} = c_1^{N_3}$$

en entiers $a_1, b_1, c_1 \neq 0$.

L'équation (5) est remplacée par

$$(19) \quad a_2^{m_1} a_1^{N_1} + b_2^{m_2} b_1^{N_2} = c_2^{m_3} c_1^{N_3},$$

où a_1, b_1, c_1 sont des entiers premiers deux à deux et à p , tandis que les entiers a_2, b_2, c_2 , aussi premiers deux à deux, n'ont d'autres diviseurs premiers que ceux de p .

Dans le cas où p est quelconque, l'équation (14) du théorème II devient

$$a_2^{m_1} a_1^{N_1} + b_2^{m_2} b_1^{N_2} = c_2^{m_3} c_1^{N_3},$$

où $a'_1, b'_1, c'_1, a'_2, b'_2, c'_2$ sont premiers entre eux deux à deux, et a'_2, b'_2, c'_2 n'ont d'autres facteurs premiers que ceux λ de p satisfaisant respectivement à

$$(20) \quad m_i \leq \frac{1}{\lambda - 1} \quad (i = 1, 2, 3).$$

Si l'un des entiers a'_2, b'_2, c'_2 est une puissance P_1, P_2 ou $P_3^{\text{ième}}$ exacte respectivement, par exemple si p n'a pas plus de deux facteurs premiers différents, on voit, en raisonnant comme au théorème III (1), que (18) équivaut à (18 bis). Cette même équivalence a lieu quand une des inégalités (20) est impossible, car alors un des nombres a'_2, b'_2, c'_2 est égal à 1; il en est ainsi quand une des quantités m_i est plus grande que $\frac{1}{\mu - 1}$, μ étant le plus petit diviseur premier de p , ou quand les m_i sont toutes plus

(1) Si $b_2 = \beta^{P_2}$, on pose

$$a_2 = \alpha^{\sigma_1 \theta_1}, \quad c_2 = \gamma^{\sigma_3 \theta_3}, \quad P_1 = \sigma_1 p_1, \quad P_3 = \sigma_3 p_3,$$

où θ_1 est premier à p_1 , θ_3 à p_3 .

grandes que $\frac{1}{\mu_3 - 1}$, d'après la définition de μ_3 (n° VI, Corollaire).

VIII. L'équation (1), où m est négatif, équivaut à une équation de même forme où m est positif.

Soit, en effet, l'équation

$$(21) \quad \frac{1}{a^m} + \frac{1}{b^m} = \frac{1}{c^m} \quad \text{ou} \quad b^m c^m + c^m a^m = a^m b^m \quad (m > 0);$$

c divise ab [n° III, note (1), 1°], et si $ab = Cc$,

$$a^m + b^m = C^m.$$

Soit d le plus grand commun diviseur de a et b , $a = \alpha d$, $b = \beta d$, où α , β sont premiers entre eux; d divise C , et $C = \gamma d$,

$$(22) \quad \alpha^m + \beta^m = \gamma^m;$$

α , β , étant premiers entre eux, le sont aussi chacun à γ , car un diviseur commun à α et γ , par exemple, diviserait β (n° II). L'équation (22) est de la forme (1). On a

$$ab = \alpha\beta d^2 = Cc = \gamma dc, \quad \alpha\beta d = \gamma c,$$

et γ divise d .

Inversement, soit α , β , γ une solution de (22) en entiers $\neq 0$ et d un multiple quelconque de γ ; posons $\alpha\beta d = \gamma c$; on a

$$(\gamma dc)^m = (\alpha dc)^m + (\beta dc)^m;$$

soient

$$a = \alpha d, \quad b = \beta d, \quad \gamma dc = \alpha\beta d^2 = ab, \\ (ab)^m = (ac)^m + (bc)^m,$$

et l'on obtient une solution de (21). Les équations (21) et (22) sont entièrement équivalentes; cette conclusion ne suppose pas $p > 1$.