Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 42 (1996)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LA CONJECTURE abc
Autor: Nitaj, Abderrahmane
Kapitel: 3. Applications de la conjecture abc
DOI: https://doi.org/10.5169/seals-87869

3. APPLICATIONS DE LA CONJECTURE *abc*

Dans cette partie, nous décrivons la plupart des conséquences de la conjecture *abc* montrant ainsi son importance en théorie des nombres.

3.1. LES CONJECTURES DE SZPIRO

Les conjectures de Szpiro sont antérieures (1983) à la conjecture *abc* et certaines d'entre elles ont les mêmes conséquences. Nous donnons deux de ces conjectures. La conjecture suivante est une conséquence de la conjecture *abc* et a été très étudiée ([13], [15], [17], [31]).

CONJECTURE 3.1.1. (Szpiro, forme forte). *Pour tout* $\varepsilon > 0$, *il existe une constante* $c(\varepsilon) > 0$ *telle que pour toute courbe elliptique semi-stable* E *sur* $\mathbf{Q}$, *de discriminant minimal* Δ_E *et de conducteur* N_E *on ait:*

$$|\Delta_E| \leqslant c(\varepsilon) N_E^{6+\varepsilon} .$$

Le conducteur d'une courbe elliptique semi-stable est le radical de son discriminant minimal. Pour une définition exacte du conducteur, on peut consulter [27].

La conjecture suivante est connue aussi sous le nom de conjecture de Lang-Szpiro.

CONJECTURE 3.1.2. *Pour tout* $\varepsilon > 0$ *et pour tout couple* (A, B) *d'entiers premiers entre eux, il existe une constante* $c(\varepsilon, A, B) > 0$ *telle que pour tous les entiers* u, v, k *vérifiant* $(Au, Bv) = 1$ *et* $k = Au^3 + Bv^2$, *on ait:*

$$|u| \leqslant c(\varepsilon, A, B) r(k)^{2+\varepsilon} \quad \text{et} \quad |v| \leqslant c(\varepsilon, A, B) r(k)^{3+\varepsilon} .$$

PROPOSITION 3.1.3. *La conjecture abc est équivalente à la conjecture 3.1.2.*

Preuve. Admettons d'abord la conjecture *abc*. Soient A, B, u, v et k des entiers tels que $(Au, Bv) = 1$ et $k = Au^3 + Bv^2$. La conjecture *abc* donne:

$$|v|^2 \leqslant \frac{c_1(\varepsilon)}{|B|} (r(ABuvk))^{1+\varepsilon} \leqslant c_2(\varepsilon, A, B) |uv|^{1+\varepsilon} (r(k))^{1+\varepsilon} .$$

Supposons que $|Au^3| \leqslant |Bv^2|$ (le cas inverse se fait de la même manière), alors $|u| \leqslant c_3(A, B)|v|^{2/3}$. En reportant cette majoration dans l'inégalité ci-dessus, on obtient:

$$|v|^2 \leqslant c_4(\varepsilon, A, B)|v|^{5(1+\varepsilon)/3}(r(k))^{1+\varepsilon},$$

et par suite:

$$|v|^{(1-5\varepsilon)/3} \leqslant c_4(\varepsilon, A, B)\, r(k)^{1+\varepsilon}.$$

Prenons ε tel que $1 - 5\varepsilon > 0$ et posons $\varepsilon' = 18\varepsilon/(1 - 5\varepsilon)$, alors:

$$|v| \leqslant c_5(\varepsilon, A, B)\ (r(k))^{3(1+\varepsilon)/(1-5\varepsilon)} \leqslant c_6(\varepsilon', A, B)\ (r(k))^{3+\varepsilon'}.$$

On obtient alors pour $|u|$:

$$|u| \leqslant c_6^{2/3}(\varepsilon', A, B)\, c_3(A, B)\, r(k)^{2(3+\varepsilon')/3} \leqslant c_7(\varepsilon', A, B)\ (r(k))^{2+\varepsilon'}.$$

Ceci prouve la conjecture 3.1.2.

Inversement, admettons la conjecture 3.1.2. Soient a, b et c des entiers positifs vérifiant $a < b$, $a + b = c$ et $(a, b) = 1$. Alors:

$$(a^2 + ab + b^2)^3 - ((b - a)\ (a + 2b)\ (2a + b)/2)^2 = 3^3(ab(a + b)/2)^2.$$

Cette relation peut être éventuellement simplifiée par 3^3 si $a \equiv b \pmod 3$. En appliquant la conjecture 3.1.2, on obtient:

$$a^2 \leqslant b^2 \leqslant a^2 + ab + b^2 \leqslant c_1(\varepsilon)(r(abc))^{2+\varepsilon},$$

et donc:

$$a \leqslant b \leqslant (c_1(\varepsilon))^{1/2}(r(abc))^{1+\varepsilon/2},$$

et finalement:

$$c \leqslant c(\varepsilon')\ (r(abc))^{1+\varepsilon'}.$$

Ceci prouve la conjecture *abc*. $\square$

3.2. Conséquences sur les triplets d'entiers

Les propositions suivantes montrent l'influence de la conjecture *abc* sur l'architecture des triplets d'entiers.

PROPOSITION 3.2.1. *Si la conjecture abc est vraie, alors pour tout* $\varepsilon > 0$, *il existe une constante* $c(\varepsilon)$ *telle que pour tout triplet*

(x_1, x_2, x_3) *d'entiers positifs, vérifiant* $x_1 + x_2 = x_3$ *et* $(x_1, x_2) = 1$, *un des* $x_i, i \in \{1, 2, 3\}$, *vérifie:*

$$x_i \leqslant c(\varepsilon)\,(r(x_i))^{3+\varepsilon}\,.$$

Cette proposition fait apparaître un lien entre la conjecture abc et le théorème de Fermat. Nous avons aussi le résultat suivant:

THÉORÈME 3.2.2. *Si la conjecture* abc *est vraie, alors pour tout* $\varepsilon > 0$ *et tout entier* $a \geqslant 1$, *il existe une constante* $c_1(\varepsilon, a) > 0$ *telle que pour tout entier* $n \geqslant 2$ *et tout entier* $x \geqslant 2$ *vérifiant* $(a, x) = 1$ *on ait:*

$$x^{n-1} \leqslant c_1(\varepsilon, a)\,(r(x^n - a^n))^{1+\varepsilon}\,.$$

Preuve. Soit ε fixé tel que $0 < \varepsilon < 1/2$. Appliquons la conjecture abc à la relation $(x^n - a^n) + a^n = x^n$ avec $(a, x) = 1$. On obtient:

$$x^n \leqslant c(\varepsilon, a)\,(r(x^n - a^n))^{1+\varepsilon} x^{1+\varepsilon}\,,$$

Alors:

$$x^{n-1} \leqslant (c(\varepsilon, a))^{(n-1)/(n-1-\varepsilon)}(r(x^n - a^n))^{(n-1)(1+\varepsilon)/(n-1-\varepsilon)}\,.$$

Si ε est assez petit et si $n \geqslant 2$, on a d'une part $(n-1)/(n-1-\varepsilon) < 2$ et d'autre part:

$$\frac{(n-1)\,(1+\varepsilon)}{n-1-\varepsilon} \leqslant \frac{1+\varepsilon}{1-\varepsilon} = 1 + \varepsilon'\,,$$

avec $\varepsilon' = 2\varepsilon/(1-\varepsilon)$. On obtient finalement la conclusion du théorème. □

3.3. LES NOMBRES DE WIEFERICH

Un nombre premier p vérifiant la congruence

$$a^{p-1} \equiv 1 \pmod{p^2}$$

avec $a = 2$ est appelé nombre de Wieferich. En 1909, celui-ci a montré que si un nombre premier p ne vérifie pas la congruence ci-dessus, alors il n'existe pas d'entiers $x > 0$, $y > 0$ et $z > 0$, premiers entre eux, tels que $xyz \not\equiv 0 \pmod{p}$ et $x^p + y^p = z^p$ (premier cas du théorème de Fermat). En 1910, Mirimanoff a prouvé la même chose avec $a = 3$. Les nombres premiers vérifiant cette congruence sont très rares. Par exemple, les seuls nombres premiers p vérifiant cette congruence avec $a = 2$ et $p \leqslant 3 \times 10^{10}$ sont 1093 et 3511. De même, les seuls vérifiant cette congruence avec $a = 3$ et $p \leqslant 2^{30}$ sont 11 et 1006003 (voir [14] ou [22]). Un problème encore ouvert est la conjecture suivante:

CONJECTURE 3.3.1. *Soit* $a \geqslant 2$. *Il existe une infinité de nombres premiers* p *tels que* $a^{p-1} \not\equiv 1 \pmod{p^2}$.

J. H. Silverman [28] a montré que cette conjecture est une conséquence de la conjecture *abc*.

3.4. LA CONJECTURE DE MORDELL

Une des conséquences les plus étonnantes de la conjecture *abc* est le fait que celle-ci implique tout simplement la conjecture de Mordell, devenue théorème de Faltings:

Toute courbe de genre $g \geqslant 2$ *définie sur* $\mathbf{Q}$ *n'admet qu'un nombre fini de points rationnels.*

Cette conjecture a été redémontrée par la suite par P. Vojta [34] et E. Bombieri [1]. En 1991, N. D. Elkies a déterminé son lien avec la conjecture *abc* (voir [4]).

THÉORÈME 3.4.1. (Elkies). *La conjecture* *abc* *implique la conjecture de Mordell.*

A la fin de son article, Elkies donne le corollaire suivant:

COROLLAIRE 3.4.2. (Elkies). *La conjecture* *abc* *implique que pour tout* $\varepsilon > 0$ *et tout polynôme* $P \in \mathbf{Z}[X, Y]$, *homogène, de degré* d *et sans facteurs carrés, il existe une constante* $c(\varepsilon, P)$ *telle que pour tout couple* (a, b) *d'entiers premiers entre eux, vérifiant* $P(a, b) \neq 0$ *on ait:*

$$\sup(|a|, |b|)^{d-2} \leqslant c(\varepsilon, P)\, r(P(a, b))^{1+\varepsilon} .$$

3.5. LA CONJECTURE D'ERDŐS-WOODS

La conjecture suivante a été formulée par P. Erdős, puis par Woods en 1981.

CONJECTURE 3.5.1. (Erdős-Woods). *Il existe une constante* $k > 0$ *telle que pour tous les entiers positifs* x *et* y, *si* $r(x+i) = r(y+i)$ *pour tout* i, $i = 1, 2, \ldots, k$, *alors* $x = y$.

Cette conjecture est fausse pour $k = 2$ ($x = 2^n - 3$, $y = 2^{2n} - 2^{n+1} - 1$ conviennent). Par contre pour $k \geqslant 3$, aucun exemple d'entiers différents vérifiant les égalités de la conjecture d'Erdős-Woods n'est connu. M. Langevin a montré le résultat suivant (voir [11, 12]).

PROPOSITION 3.5.2. (Langevin). *La conjecture abc implique que la conjecture d'Erdős-Woods est vraie avec $k = 3$, sauf peut-être pour un nombre fini d'exceptions pour x et y.*

3.6. LA CONJECTURE DE HALL

En 1971, M. Hall Jr. a énoncé la conjecture suivante [7]:

CONJECTURE 3.6.1. (Hall). *Il existe une constante $c > 0$ telle que pour tous entiers $x > 1$ et $y > 0$ vérifiant $x^3 \neq y^2$ on ait:*

$$|x^3 - y^2| \geqslant c \max(x^3, y^2)^{1/6}.$$

On sait par exemple depuis 1738 (Euler), que les seules solutions non triviales de l'équation $|x^3 - y^2| = 1$ sont $(x, y) = (2, \pm 3)$. La relation $28187351^3 - 149651610621^2 = -1090$, montre que dans la conjecture de Hall, la constante c vérifie $c \leqslant 0{,}205305$. La conjecture abc n'admet pour conséquence que la forme faible suivante de la conjecture de Hall (voir [17], [25]).

CONJECTURE 3.6.2. *Pour tout $\varepsilon > 0$, il existe une constante $c(\varepsilon) > 0$ telle que pour tous les entiers $x > 1$ et $y > 0$ on ait:*

$$|x^3 - y^2| \geqslant c(\varepsilon) \max(x^3, y^2)^{1/6 - \varepsilon}.$$

3.7. L'ÉQUATION DE FERMAT GÉNÉRALISÉE

La conjecture abc s'applique particulièrement aux équations diophantiennes à trois termes, dont l'équation de Fermat généralisée.

THÉORÈME 3.7.1. *Si la conjecture abc est vraie et si A, B, C sont des entiers strictement positifs, alors l'équation:*

$$Ax^l + By^m = Cz^n$$

n'admet qu'un nombre fini de solutions en entiers positifs x, y, z, l, m, n vérifiant $l^{-1} + m^{-1} + n^{-1} < 1$ et $(x, y, z) = 1$.

Preuve. Si $z = 1$, alors le théorème est clair, même sans admettre la conjecture abc. Supposons donc que $z \geqslant 2$ et que $(x, y, z) = 1$. Soit $d = (Ax^l, By^m, Cz^n)$. Alors d est borné. En appliquant la conjecture abc au triplet $(Ax^l/d, By^m/d, Cz^n/d)$, on obtient:

$$Cz^n/d \leqslant c_1(\varepsilon) \left(r(ABCx^l y^m z^n/d^3)\right)^{1+\varepsilon},$$

d'où l'on tire:

$$z^n \leqslant c_2(\varepsilon, C) \left(dr \left(\frac{ABCx^l y^m z^n}{d^3} \right) \right)^{1+\varepsilon} \leqslant c_3(\varepsilon, A, B, C)\, (xyz)^{1+\varepsilon}.$$

Puisque $Ax^l < Cz^n$ et $By^m < Cz^n$, alors $x < c_4(A, C) z^{n/l}$ et $y < c_5(B, C) z^{n/m}$. Ainsi

$$z^n \leqslant c_6(\varepsilon, A, B, C)\, (z^n)^{(1+\varepsilon)(l^{-1}+m^{-1}+n^{-1})},$$

ce qui donne:

$$(z^n)^{1-(1+\varepsilon)(l^{-1}+m^{-1}+n^{-1})} \leqslant c_6(\varepsilon, A, B, C).$$

Si $l^{-1} + m^{-1} + n^{-1} < 1$ et si ε est assez petit, alors $1 - (1+\varepsilon)(l^{-1} + m^{-1} + n^{-1}) > 0$ et donc z^n est borné. Ainsi z, x, y, l, m, n sont bornés. □

REMARQUE 3.7.2. On peut trouver d'autres démonstrations de cette proposition dans [25] et [33]. Dans le cas $A = B = C = 1$, seules 10 solutions sont connues avec $l^{-1} + m^{-1} + n^{-1} < 1$:

$$1 + 2^3 = 3^2, \quad 13^2 + 7^3 = 2^9, \quad 17^3 + 2^7 = 71^2,$$
$$2^5 + 7^2 = 3^4, \quad 3^5 + 11^4 = 2^2 . 61^2,$$

ainsi que les solutions suivantes, découvertes par Beukers et Zagier (voir [3]):

$$17^7 + 76271^3 = 21063928^2, \quad 1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2,$$
$$33^8 + 1549034^2 = 15613^3.$$

3.8. QUELQUES CONJECTURES SUR LES NOMBRES PUISSANTS

DÉFINITION 3.8.1. *Un entier n est un nombre puissant s'il possède la propriété suivante: si p divise n et si p est premier, alors p^2 divise n.*

Si n est un nombre puissant, alors il s'écrit de façon unique sous la forme $n = a^2 b^3$, où b est sans facteurs carrés et son radical $r(n)$ vérifie donc $r(n) \leqslant n^{1/2}$.

Les conjectures citées dans cette partie proviennent de [22] et de [6] (B16).

CONJECTURE 3.8.2. (Erdős-Mollin-Walsh). *Il n'y a aucun triplet de nombres puissants consécutifs.*

Cette conjecture est vérifiée pour tous les triplets d'entiers inférieurs à 2^{60} [18] et implique en particulier qu'il existe une infinité de nombres premiers p tels que

Ceci fait apparaître un lien avec le premier cas du théorème de Fermat (voir [22]).

La conjecture abc ne permet pas de répondre totalement à la conjecture 3.8.2, mais permet d'avoir ceci (voir [17]):

PROPOSITION 3.8.3. *La conjecture abc implique qu'il n'y a qu'un nombre fini de triplets de nombres puissants consécutifs.*

Les conjectures suivantes concernent les nombres de Fermat et de Mersenne et il est facile de montrer qu'elles sont des conséquences de la conjecture abc ([17]).

CONJECTURE 3.8.4. *Pour tout entier $k \geqslant 2$, soit n_k le nombre puissant le plus proche de 2^k avec $n_k \neq 2^k$. Alors $\lim_{k \to \infty} |2^k - n_k| = +\infty$.*

CONJECTURE 3.8.5. *Il existe une infinité de nombres de Fermat et de Mersenne qui ne sont pas des nombres puissants.*

Pour terminer cette partie, citons la conjecture suivante sur les nombres *4-puissants,* qui sont des entiers n tels que $r(n)^4 \mid n$ (voir problème B16 de [6], édition 1981). Cette conjecture est aussi une conséquence de la conjecture abc.

CONJECTURE 3.8.6. (Erdős). *L'équation $x + y = z$ n'admet qu'un nombre fini de solutions en entiers positifs 4-puissants, premiers entre eux.*

3.9. LA CONJECTURE DE RICHARD

La conjecture suivante est tirée de [23]:

CONJECTURE 3.9.1. (Richard). *Si deux entiers x et y vérifient pour tout entier $n \geqslant 0$:*

$$r(x^{2^n} - 1) = r(y^{2^n} - 1) ,$$

alors ils sont égaux.

A. Schinzel a montré de façon élégante que cette conjecture est une conséquence de la conjecture abc (voir [17], [23]).

3.10. LE PROBLÈME DE CROFT

Le problème de savoir dans quelle mesure la différence $|n! - 2^m|$ peut être petite par rapport à 2^m s'appelle le problème de Croft (voir [6], F23). Des résultats expérimentaux nous ont motivé pour proposer la conjecture suivante (voir [17]).

CONJECTURE 3.10.1. *Il existe une constante* $c > 0$ *telle que pour tous les entiers* m *et* n *avec* $(m, n) \neq (0, 0), (1, 0), (2, 1)$ *on ait:*

$$n \leqslant c(r(|n! - 2^m|))^{1/n}\,.$$

La conjecture *abc* implique cependant une forme faible de cette conjecture (voir [17]).

PROPOSITION 3.10.2. *La conjecture* *abc* *implique que pour tout* $\varepsilon > 0$, *il existe une constante* $c(\varepsilon) > 0$ *telle que pour tous les entiers* m *et* n *avec* $(m, n) \neq (0, 0), (1, 0), (2, 1)$, *on ait:*

$$n \leqslant c(\varepsilon)\,(r(|n! - 2^m|))^{(1+\varepsilon)/n}\,.$$

3.11. AUTRES CONSÉQUENCES

Nous regroupons dans cette partie plusieurs conséquences de la conjecture *abc*. Cela concerne en particulier des équations diophantiennes liées à des problèmes ouverts.

PROPOSITION 3.11.1. *Soient* $A > 0, B > 0$ *et* k *des entiers. La conjecture* *abc* *implique que l'équation*

$$Ax^m - By^n = k$$

n'a qu'un nombre fini de solutions en entiers $x > 1, y > 1, m > 1, n > 1$ *avec* $mn > 4$.

Cette proposition est liée à une conjecture de Pillai. Lorsque $A = 1, B = 1$ et $k = 1$, cette conjecture porte le nom de conjecture de Catalan, qui affirme en plus que $(x, y, m, n) = (3, 2, 2, 3)$ est l'unique solution. En 1976, R. Tijdeman [32] a montré que l'équation de Catalan n'admet qu'un nombre fini de solutions.

PROPOSITION 3.11.2. *La conjecture* *abc* *implique que l'équation*

$$\left(\frac{x}{v}\right)^m - \left(\frac{y}{w}\right)^n = 1$$

n'admet qu'un nombre fini de solutions en entiers positifs $v, w, x, y, m > 1$ *et* $n > 1$ *vérifiant* $(x, v) = 1, (y, w) = 1$ *et* $mn > 4$.

Cette proposition est liée à une conjecture de Shorey et Tijdeman (voir [26], p. 202). Cette conjecture est vraie en particulier si l'une des variables v, w, x ou y est composée de nombres premiers fixés.

PROPOSITION 3.11.3. *La conjecture abc implique que l'équation*

$$(x!)^n + 1 = y^m$$

n'admet qu'un nombre fini de solutions en entiers $x > 0$, $y > 0$, $n \geqslant 1$ *et* $m \geqslant 2$.

Cette proposition est liée à un problème de Brocard (voir [6], D25) et sa démonstration (voir [17] et [21]) est basée sur l'utilisation des inégalités suivantes, déduites des formules de Stirling et de Chebyshev (voir [19], p. 374), valables pour $x \geqslant 2$:

$$\begin{cases} (x/e)^x < x!\,, \\ \prod_{p \leqslant x} p < 4^x, \ p \text{ premier}\,. \end{cases} \tag{3.11.4}$$

PROPOSITION 3.11.5. *La conjecture abc implique que l'équation*

$$n! + 1 = p_k^a p_{k+1}^b$$

n'admet qu'un nombre fini de solutions en entiers $n \geqslant 1$, $a \geqslant 0$, $b \geqslant 0$ *et* $p_{k-1} \leqslant n < p_k$ *où* $(p_i), i \geqslant 1$ *est la suite des nombres premiers.*

Cette proposition est liée à une conjecture d'Erdős-Stewart (voir [6], A2). Sa démonstration est basée aussi sur les inégalités (3.11.4).

PROPOSITION 3.11.6. *La conjecture abc implique que l'équation*

$$x^n + y^n = n!z^n$$

n'a qu'un nombre fini de solutions en entiers $x > 0$, $y > 0$, $z > 0$ *et* $n \geqslant 4$.

Cette proposition est liée à un problème ouvert sur les équations diophantiennes (voir [6], D2).

PROPOSITION 3.11.7. *La conjecture abc implique que pour tout entier* $a \geqslant 1$, *l'équation*

$$\frac{x^n - y^n}{x - y} = az^m$$

n'a qu'un nombre fini de solutions en entiers $x > y > 0$, $z > 0$, $n > 3$, $m > 1$ *avec* $(x, y) = 1, 3n^{-1} + m^{-1} < 1$.

Cette proposition est une réponse générale à un problème de H. Edgar ([6], D10) et de Shorey-Tijdeman ([26], pp. 202, 203).

PROPOSITION 3.11.8. *La conjecture abc implique que l'équation*

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}$$

n'a qu'un nombre fini de solutions en entiers $x > y > 1$ et $m > n > 3$.

La recherche de solutions pour l'équation ci-dessus est appelée problème de Goormaghtigh (voir [6], B25). Avec $n = 3, (x, y, m, n) = (2, 5, 5, 3)$, $(2, 90, 13, 3)$ sont les seules solutions connues.

PROPOSITION 3.11.9. *La conjecture abc implique que pour tout entier $d \geqslant 1$, l'équation*

$$x(x + d) \dots (x + kd) = y^n$$

n'a qu'un nombre fini de solutions en entiers $x > 0$, $k \geqslant 2$, $y > 0$ et $n \geqslant 2$.

Cette proposition montre le lien entre la conjecture abc et les progressions arithmétiques. P. Erdős et J.L. Selfridge ont montré en 1975 que l'équation ci-dessus n'a pas de solution dans le cas particulier $d = 1$ (voir [33] pour plus de détails).

4. A LA RECHERCHE DE FORMES EFFECTIVES

Soient a, b et c trois entiers positifs, premiers entre eux et vérifiant $a + b = c$. Soit $r = r(abc)$, le radical de abc. On définit le rapport de Oesterlé-Masser pour le triplet (a, b, c) par:

$$\alpha = \alpha(a, b, c) = \frac{\log c}{\log r} .$$

On définit de même le rapport de Szpiro pour le même triplet par:

$$\rho = \rho(a, b, c) = \frac{\log abc}{\log r} .$$

Ce dernier rapport est lié à la conjecture de Szpiro (voir conjecture 3.1.1) par les courbes elliptiques $E_{a,b,c}$ que Y. Hellegouarch [9] a mis au point en 1972 pour étudier le théorème de Fermat. C'est en utilisant ces mêmes courbes que K. Ribet a établit le lien entre la conjecture de Shimura-Taniyama-Weil et le théorème de Fermat. Pour un triplet (a, b, c) d'entiers positifs vérifiant $a + b = c$ et $(a, b) = 1$, la courbe $E_{a,b,c}$ est définie par:

$$E_{a,b,c}\colon y^2 = x(x - a)(x + b) .$$