Séminaire de philosophie et mathématiques

P. Ribenboin

Les idées de Kummer sur le théorème de Fermat

Séminaire de Philosophie et Mathématiques, 1979, fascicule 3
« Les idées de Kummer sur le théorème de Fermat », , p. 1-11

<http://www.numdam.org/item?id=SPHM_1979___3_A1_0>

LES IDEES DE KUMMER SUR LE THEOREME DE FERMAT.

par P. RIBENBOIN

Conférence au Séminaire "Philosophie et Mathématique" de Dieudonné-Loi-Thom, à l'Ecole Normale Supérieure, Paris. Le 5 mars, 1979.

Je passe en revue quelques unes des principales idées de Kummer sur ce qu'on appelle le "dernier théorème de Fermat". Il s'agit de l'affirmation (pas encore démontrée dans toute sa généralité) :

(DTF) si $n \geqslant 3$ il n'existe pas des nombres naturels non nuls x, y, z tels que

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

Par contre, pour $n = 2$, il existe de tels entiers, comme par exemple, 3, 4, 5 : $3^2 + 4^2 = 5^2$.

Pour démontrer le DTF pour toute valeur de l'exposant n, il suffit de le faire pour $n = 4$ et pour les exposants n qui sont des nombres premiers p, car si $n = \ell m$, $\ell, m \geqslant 2$, et si $x, y, z \neq 0$ satisfont $x^{\ell m} + y^{\ell m} = z^{\ell m}$ alors x^ℓ, y^ℓ, z^ℓ satisfont $(x^\ell)^m + (y^\ell)^m = (z^\ell)^m$.

Fermat a laissé une démonstration pour $n = 4$, où il introduisit la méthode de la descente infinie : en supposant qu'il existe une solution (x, y, z) de l'équation de Fermat, on fabrique une nouvelle solution (x', y', z'), avec $0 < x' < x$, et on répète cet argument. Le procédé doit nécessairement s'arrêter, car $x, x', \ldots$ sont des entiers positifs. Cela mène donc à une contradiction.

Euler a démontré le théorème pour $n = 3$. Une autre démonstration pour $n = 3$, due à Gauss, a été trouvée parmi ses papiers à sa mort et a été publiée en 1876. Gauss a même réussi à montrer qu'il n'existe pas de solution non nulle dans le corps d'Eisenstein $\underline{\underline{O}}(\sqrt{-3})$, engendré par les racines cubiques de l'unité.

Legendre a reproduit la démonstration d'Euler dans son livre "Théorie des Nombres". Indépendamment, et simultanément, Legendre et Dirichlet ont démontré le DTF pour $n = 5$ (1825/8). En 1832, Dirichlet a montré le théorème pour $n = 14$, sensiblement plus facile à traiter que l'exposant $n = 7$. Pour ce dernier, la démonstration a été fournie par Lamé (1939), et simplifiée aussitôt par Lebesgue (1840).

A ce moment, il y avait à Paris un intérêt très considérable pour le DTF. Il faut noter, outre les mathématiciens déjà cités (en incluant Dirichlet qui a séjourné à Paris), que Cauchy avait produit des travaux substantiels en théorie des nombres, plus précisément sur la décomposition des polynômes radicaux, ce qui, en langage moderne, se traduirait par l'étude de l'arithmétique des corps cyclotomiques.

En 1847, Lamé a présenté à l'Académie des Sciences de Paris une démonstration du DTF pour un exposant quelconque, et les détails de ce travail retentissant ont été publiés au Journal le Liouville. Néanmoins, Liouville a observé que la démonstration n'était pas correcte, car Lamé faisait usage de la décomposition unique de certaines expressions en polynômes des racines de l'unité, en facteurs irréductibles. Or ceci n'était nullement évident, peut être même pas vrai. Après quelques essais, Lamé s'est rendu compte de la difficulté essentielle qu'il restait à vaincre.

Tout ceci situe le cadre où Kummer a commencé ses travaux remarquables sur le DTF.

Déjà en 1837, Kummer avait publié son premier travail, écrit en latin, sur l'équation de Fermat, avec exposant pair. Il a montré :

Si $n > 1$ est impair, s'il existe des entiers x, y, z (non nuls) tels que p. g. c. d $(n, x\,y\,z) = 1$ et $x^{2n} + y^{2n} = z^{2n}$ alors $n \equiv 1 \pmod 8$.

La démonstration était très simple et a été retrouvée à maintes reprises, même très récemment. Plusieurs auteurs ont travaillé sur les exposants pairs, en obtenant des résultats d'un certain intérêt. Ainsi, en 1960 Long a montré :

Si n est un entier dont le dernier chiffre (en représentation décimale) est 4 ou 6, si x, y, z sont des entiers non nuls tels que $x^n + y^n = z^n$ alors p. g. c. d $(n, x\,y\,z) > 2$.

Dans cette lignée, en décembre 1977, Terjanian a publié le meilleur résultat possible, à savoir :

Si $p \geq 3$ est premier, s'il existe des entiers naturels non nuls x, y, z tels que $x^{2p} + y^{2p} = z^{2p}$ alors $2p$ divise x ou y.

Il est remarquable de constater que la démonstration de Terjanian est entièrement élémentaire et classique, n'utilisant que des propriétés de divisibilité d'expressions du type $\frac{z^p \pm y^p}{z \pm y}$ ainsi que du symbole de Jacobi.

Cela peut suggérer la possibilité de trouver aussi une démonstration élémentaire, lorsque l'exposant est un premier p, de ce qu'on a convenu d'appeler le

(Premier Cas du DTF) S'il existe des entiers non nuls x, y, z tels que $x^p + y^p = z^p$ alors nécessairement p divise $x\,y\,z$.

Toutefois, je ne le crois pas, car on ne pourrait plus travailler avec la réciprocité quadratique et il faudrait nécessairement faire usage d'une loi de réciprocité pour des restes de puissances p, ce qui est nettement plus difficile.

Le premier travail important de Kummer sur le théorème de Fermat a été conçu en 1844, année où il avait déjà reconnu que le théorème de factorisation unique n'est pas vrai pour les corps cyclotomiques en général, par exemple, lorsque $p = 23$. En 1847, dans une lettre à Liouville, qui accompagne son travail, Kummer explique qu'il a été conduit à considérer une nouvelle classe de nombres complexes, qu'il appelait des nombres complexes idéaux, dans le but de garantir pour ces nombres la décomposition unique. Ailleurs, Kummer explique les nombres idéaux au moyen d'une analogie avec la chimie. A son époque, on connaissait l'existence de certaines substances contenant des radicaux avec du fluor, toutefois on n'avait pas réussi à isoler le fluor lui-même. Celui-ci étant, d'après Kummer, l'analogue de ses nombres idéaux, tandis que les radicaux, qui apparaissaient dans la nature, étaient comme les vrais (= "wirklich") nombres complexes. La définition même de nombre idéal donnée par Kummer s'exprime en termes de divisibilité ; aujourd'hui, cela correspond au concept de "diviseur", qui s'est présenté naturellement dans la théorie des fonctions algébriques. L'interprétation des idéaux comme certains sous-ensembles est due à Dedekind, lorsqu'il a cherché à comprendre ces idées de Kummer. S'il est bien vrai que la notion ensembliste d'idéal

a une grande valeur, celle de Kummer était certainement plus appropriée pour l'étude de la divisibilité - ce point de vue étant d'ailleurs partagé par Hasse, Weyl et beaucoup d'auteurs modernes.

Je passerai en silence l'histoire courante à propos d'une démonstration de Kummer, envoyée à Dirichlet, pas plus tard que 1844, où précisément Kummer aurait commis l'erreur commune de supposer la factorisation unique. Cette histoire, propagée par Hensel, est analysée par Edwards (1975), lors de la récente découverte d'une lettre de Liouville à Dirichlet.

Ce que Kummer a montré en 1947 est le résultat suivant :

LE DTF est vrai en supposant que l'exposant p satisfait les deux conditions suivantes (en langage moderne) :

1) Si un idéal I est tel que I^p soit un idéal principal, alors I est lui-même un idéal principal.

2) Si ω est une unité du corps cyclotomique des racines p-ièmes de l'unité, s'il existe un entier m tel que $\omega \equiv m \pmod{p}$ alors ω est la p-ième puissance d'une unité.

En quelque sorte, ce sont deux hypothèses de travail, qui faisaient marcher le raisonnement que Kummer avait envisagé, le problème devenant donc celui de savoir pour quelles valeurs de p ces deux hypothèses étaient satisfaites.

D'abord Kummer a eu l'espoir que ces hypothèses étaient toujours vérifiées. En essayant de les démontrer, il a été conduit à faire une étude approfondie de l'artithmétique des corps cyclotomiques. Il a écrit une série d'articles très importants de 1847 à 1851, dont un, traduit en français, est paru au Journal de Liouville (1851). Dans ces articles, Kummer a introduit les notions, aujourd'hui fondamentales, de classes d'idéaux, nombre de classes, il a fait les premiers calculs du nombre de classes. Il a aussi étudié les unités des corps cyclotomiques et, parmi d'autres choses, il a montré que la condition (1) est équivalente à la suivante.

1') p ne divise pas le nombre de classes h_p du corps cyclotomique

$$\underset{\approx}{\mathbb{Q}}(\zeta_p) \quad , \quad \zeta_p = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p} .$$

En outre, la condition (1) entraîne (2) - ceci constitue le "lemme des unités" de Kummer, dont la démonstration est très délicate et requiert des méthodes transcendantes, plus précisément λ-adiques (λ étant le premier cyclotomique qui divise p).

Tout premier p satisfaisant la condition (1') s'appelle un premier <u>régulier</u>. En d'autres termes, Kummer a démontré :

Si p est un premier régulier, le DTF est vrai pour l'exposant p.

Et même, il n'y a pas d'éléments non-nuls $\alpha, \beta, \gamma \in \underset{\approx}{Q}(\zeta_p))$ tels que $\alpha^p + \beta^p = \gamma^p$. Soit dit en passant, la démonstration de Kummer était erronée pour le cas général, comme l'a observé Hilbert, mais le théorème reste vrai au moyen d'une modification appropriée de la démonstration.

Il n'est peut être pas inutile d'esquisser cette démonstration pour montrer comment l'idée de Kummer était naturelle.

On part de l'existence d'entiers non nuls x, y, z tel que $x^p = z^p - y^p$: on peut les supposer deux à deux premiers. On veut arriver à une contracdiction. Il est plus que naturel d'exprimer la différence $z^p - y^p$ comme un produit ; cela se fait en utilisant $\zeta = \zeta_p$:

$$x^p = z^p - y^p = \prod_{j=o}^{p-1} (z - \zeta^j y).$$

Le premier cas à considérer est celui où p ne divise pas $x\ y\ z$. Je ne dirai rien sur l'autre cas, car l'idée est la même, quoique il y ait des complications supplémentaires.

On aimerait pouvoir dire que les facteurs $z - \zeta^j y$ sont deux à deux premiers, et de ce fait, chacun serait une puissance p-ième d'un entier cyclotomique bien déterminé. Ceci est défendu, car faux. Ce qu'on peut faire c'est de travailler avec des idéaux, pour lesquels il y a décomposition unique en idéaux premiers. En mettant de côté l'idéal I, p. g. c. d. des idéaux principaux $(z - \zeta^j y)$ (pour $j = 0, 1, \ldots, p-1$), ceux qui restent sont des idéaux deux à deux premiers, c'est-à-dire

$$(x - \zeta^j y) = J_j^p . I \quad (j = 0, 1, \ldots., p-1).$$

D'ailleurs, puisqu'on est dans le premier cas, l'idéal premier $\lambda = (1 - \zeta)$

ne divise aucun J_j. Donc, chacun des idéaux fractionnaires quotients

$$\left(\frac{J_j}{J_{p-1}}\right)^p = \frac{J_j^p\, I}{J_{p-1}^p\, I} = \frac{(z - \zeta^j y)}{(z - \zeta^{p-1} y)}$$

est principal $(j = 0, 1, \ldots, p-2)$. Puisque p satisfait la condition (1') alors chaque idéal $\frac{J_j}{J_{p-1}}$ est lui-même principal, engendré, disons, par γ_j. Ceci s'écrit alors sous la forme

$$\alpha - \zeta^j \beta = \omega_j\, \gamma_j^p ,$$

ω_j étant une unité. D'après Kummer, $\omega_j = \varepsilon_j\, \zeta^{c_j}$, ε_j étant une unité réelle et $0 \leqslant c_j \leqslant p-1$.

La démonstration se poursuit de la façon suivante : si on prend des congruences, on peut remplacer γ_j par des entiers naturels m_j :

$\gamma_j \equiv m_j \pmod{\lambda}$, donc $\gamma_j^p \equiv m_j^p \pmod{\lambda^p}$, car $(p) = (\lambda^{p-1})$.

Ainsi

$$\alpha - \zeta^j \beta \equiv \varepsilon_j\, \zeta^{c_j}\, m_j^p \pmod{\lambda^p} ,$$ et en prenant le complexe conjugué

$$\bar{\alpha} - \zeta^{-j}\, \bar{\beta} \equiv \varepsilon_j\, \zeta^{-c}\, m_j^p \pmod{\lambda^p}$$

d'où

$$\alpha - \zeta^j \beta \equiv \zeta^{2c}\, (\bar{\alpha} - \zeta^{-j} \bar{\beta}) \pmod{\lambda^p} \quad \text{pour} \quad j = 0, 1, \ldots, p-2.$$

Ensuite, Kummer arrive à montrer que $c_j \equiv jb \pmod{p}$ pour un entier rationnel b approprié). Ceci permet d'écrire un système d'équations (où les ρ_j sont des entiers cyclotomiques)

$$\begin{cases} \alpha - \beta - \bar{\alpha} + \bar{\beta} = \rho_0\, \lambda^p \\ \alpha - \zeta\beta - \zeta^{2b}\, \bar{\alpha} + \zeta^{2b-1}\, \bar{\beta} = \rho_1\, \lambda^p \\ \alpha - \zeta^2\beta - \zeta^{4b}\, \bar{\alpha} + \zeta^{4b-2}\, \bar{\beta} = \rho_2\, \lambda^p \\ \alpha - \zeta^3\beta - \zeta^{6b}\, \bar{\alpha} + \zeta^{6b-3}\, \bar{\beta} = \rho_3\, \lambda^p \end{cases}$$

et la règle de Cramer implique que

$$(1 - \zeta)\, (1 - \zeta^{2b})\, (1 - \zeta^{2b-1})\, (\zeta - \zeta^{2b})\, (\zeta - \zeta^{2b-1})\, (\zeta^{2b} - \zeta^{2b-1}) \equiv 0 \pmod{\lambda^p}.$$

On discute les valeurs possibles de b, arrivant dans chaque cas à une contradiction. Ceci démontre le théorème dans le cas où p ne divise pas x y z.

Pour démontrer son théorème principal, Kummer a eu donc besoin d'étudier à fond l'arithmétqque des corps cyclotomiques, en créant la théorie des nombres algébriques, comme branche indépendante de la théorie des nombres.

Toutes les notions fondamentales y sont déjà : idéaux premiers, détermination explicite de générateurs d'idéaux premiers, formules pour le nombre de classes, structure du groupe des unités, régulateur. Il faut dire que certains de ces concepts avaient été considérés aussi par Dirichlet, ce qui n'enlève de mérite ni à l'un ni à l'autre. Il est vrai aussi que Kummer s'est restreint spécifiquement au cas de corps cyclotomiques. L'extension aux corps de nombres algébriques généraux a été faite surtout par Dedekind.

Et après ce théorème principal, où se sont orientées les recherches de Kummer concernant le DTF ?

Ce qu'il fallait faire était :

1°) Caractériser les nombres premiers réguliers.

2°) Savoir s'il y en avait beaucoup, une infinité au moins.

3°) Etendre le théorème principal à des exposants premiers irréguliers, ou, au moins satisfaisant des conditions additionnelles.

Pour savoir si p divise le nombre de classes h_p du corps cyclotomique $\underset{\sim}{Q}(\zeta_p)$, il suffit de calculer h_p. Or Kummer a bien trouvé les formules suivantes, basé sur des travaux de Dirichlet, et qui sont les meilleures connues à ce jour :

$$h_p = h_p^- \cdot h_p^+$$

où h_p^- et h_p^+ sont des entiers positifs, appelés le nombre de classes relatif (ou premier facteur) et le nombre de classes réel (ou deuxième facteur), qui sont donnés par

$$h_p^- = \frac{1}{(2p)^{\frac{p-3}{2}}} \left| G(\eta)\ G(\eta^3) \ldots\ G(\eta^{p-2}) \right|$$

$$h_p^+ = \frac{2^{\frac{p-3}{2}}}{R} \prod_{k=1}^{\frac{p-3}{2}} \left| \sum_{j=o}^{\frac{p-3}{2}} \eta^{2kj} \log \left| 1 - \zeta^{g^j} \right| \right|$$

où g est une racine primitive modulo p,

$1 \leqslant g_j \leqslant p-1$ et $g_j \equiv g^j$ (modulo p) pour tout $j \geqslant 0$,

$$G(X) = \sum_{j=o}^{p-2} g_j X^j$$

η est une racine $(p-1)$-ième de l'unité

R est le régulateur du corps cyclotomique, à savoir,

$R = 2^{\frac{p-3}{2}} \det(L)$, L étant la matrice suivante

$$L = \begin{pmatrix} \log|\varepsilon_1^{(1)}| \ldots\ldots\ldots\ldots\ldots \log|\varepsilon_1^{(r)}| \\ \\ \log|\varepsilon_r^{(1)}| \ldots\ldots\ldots\ldots\ldots \log|\varepsilon_r^{(r)}| \end{pmatrix}$$

avec :

r_1 = nombre d'immersions réelles de $\underset{\approx}{Q}(\zeta_p)$

$2r_2$ = nombre des autres immersions de $\underset{\approx}{Q}(\zeta_p)$ dans le corps des complexes

$r = r_1 + r_2 - 1$,

$\{\varepsilon_1, \ldots, \varepsilon_r\}$ est un système fondamental d'unités du corps $\underset{\approx}{Q}(\zeta_p)$ et pour tout $\alpha \in \underset{\approx}{Q}(\zeta_p)$, on désigne par

$\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(r_1)}$ les images de α dans $\underset{\approx}{R}$,

$\alpha^{(r_1+1)}, \alpha^{(r_1+2)}, \ldots, \alpha^{(r_1+2r_2)}$ les autres images de α dans $\underset{\approx}{C}$,

de sorte que $\alpha^{(r_1+r_2+j)}$ soit le complexe conjugué de $\alpha^{(r_1+r_2)}$ (pour $j = 1, \ldots, r_2$).

En somme, c'est une formule difficile à expliquer, encore plus difficile à obtenir et visiblement bien réfractaire à être appliquée à des calculs explicites. Et, en quelque sorte, miraculeuse, si on tient compte du fait que h_p^+ est forcément un entier, bien qu'il soit donné par un produit de sommes de produits de logarithmes et d'expressions trigonométriques

$$\eta^{2kj} = \cos\frac{4kj\pi}{p-1} + i \sin\frac{4kj\pi}{p-1} .$$

Déjà pour des petites valeurs de p les calculs sont très laborieux.

Remarquons toutefois que ce qui comptait, c'était de savoir si p divise h_p, et non pas de calculer h_p exactement. Kummer a montré :

Si p divise h_p^+ alors p divise h_p^-.

Donc p divise h_p si et seulement si p divise h_p^-, ce qui est, en tout cas, une avance considérable, compte tenu du fait que le facteur h_p^+ ne peut pas se traiter sans des méthodes très puissantes.

Pour la divisibilité de h_p^- par p, Kummer a donné le critère de régularité suivant :

p divise $h_p^- \iff$ il existe un entier $2k$, $2 \leqslant 2k \leqslant p-3$,

tel que p^2 divise la somme $\sum_{j=1}^{p-1} j^{2k}$.

Or, ces sommes s'expriment, comme Euler avait montré, au moyen des nombres de Bernoulli, considérés d'abord en théorie des probabilités. Le critère devient alors :

p divise $h_p^- \iff p$ divise un des nombres $B_2, B_4, \ldots, B_{p-3}$,

où B_n représente le n-ième nombre de Bernoulli. Ce sont des nombres rationnels, définis récursivement par la relation symbolique

$$(B + 1)^{n+1} - B^{n+1} = 0 ,$$

ou explicitement (en remplaçant B^k par B_k) :

$$\binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \ldots + \binom{n+1}{n} B_1 + 1 = 0 .$$

Dire que p divise B_{2k}, signifie qu'il divise son numérateur, lorsque B_{2k} s'écrit comme fraction irréductible.

Ce dernier critère est assez pratique, car les nombres de Bernoulli peuvent, au moins en théorie, se déterminer inductivement les uns après les autres, il est vrai par une récursion de longueur croissante. Il y a même des formules, de nature plus technique, qui permettent de simplifier le travail considérablement. Le seul problème c'est que les nombres qui apparaissent ont des numérateurs qui grandissent vertigineusement, et la question même d'écriture devient

un problème pour le moins agaçant. Pensez que le numérateur de B_{210} a autour de 250 chiffres.

Tous ces résultats ne permettent toutefois pas de prévoir si un nombre premier donné sera régulier (à moins d'effectuer les calculs correspondants), ni même de prévoir la distribution des nombres premiers réguliers.

Sur ces points, sans vouloir m'étendre, je veux signaler que Kummer a calculé, à la main, c'est-à-dire, sans le secours de machine, le nombre de classes relatif jusqu'à $p = 163$ et il a ainsi déterminé les premiers premiers irréguliers 37, 59, 67, 101, 103, 131, 149, 157. Il a conjecturé, sans une base apparemment très forte, qu'il y avait à peu près autant de premiers réguliers que d'irréguliers.

Notons à ce propos, sans rentrer dans aucun détail, que Jensen a démontré en 1915 qu'il existe une infinité de premiers irréguliers (même congrus à 3 modulo 4), qu'on n'a jamais démontré qu'il existe une infinité de premiers réguliers (cela semble très difficile) ; néanmoins, avec des raisonnements heuristiques, Siegel a indiqué en 1964 que

$$\lim_{N \to \infty} \frac{\text{nombre de premiers irréguliers } p \leqslant N}{\text{nombre de premiers } p \leqslant N} = 1 - \frac{1}{\sqrt{e}} \cong 0.39\ldots$$

ce qui est confirmé par les calculs les plus récents (Wagstaff, $N = 125000$).

Kummer a aussi montré le DTF pour des classes d'exposants irréguliers, toutefois définis au moyen de conditions de vérification difficile. Il s'agit là de considérations très techniques où Kummer a d'ailleurs commis des erreurs (comme l'a signalé, et en partie corrigé, Vandiver, dès 1919).

Par contre, ses efforts pour le premier cas du théorème de Fermat ont été plus réussis. Se fondant sur des congruences, qui faisaient intervenir les nombres de Bernoulli, et dont la démonstration est un joyau typiquement kummérien, Kummer a montré que, si le premier cas du théorème de Fermat est faux pour l'exposant p, alors p divise en fait les nombres de Bernoulli B_{p-3}, B_{p-5}. D'ailleurs, le fait que p divise B_{p-3} avait été découvert par Cauchy et Genocchi, bien auparavant. Mirimanoff a ensuite étendu ceci jusqu'à B_{p-7}, B_{p-9}. Plus récemment, Morishima a montré que p diviserait aussi B_{p-11}, B_{p-13}. Or, si on examine les tables les plus étendues de Wagstaff, on se rend compte que ce phénomène est extrêmement rare. En effet,

il est très rare que p divise un grand nombre de nombres de Bernoulli (avec indice au plus $p-3$), et il n'arrive pratiquement jamais que p divise des nombres de Bernoulli successifs. Tout ceci est en rapport avec la structure profonde du groupe des classes, et peut un peu se comprendre à travers les travaux de Hecke, Scholz, Eichler et Ribet.

Que dire alors du résultat frappant de Krasner (1934) ? Il a en effet montré :

Soit $n_o = (45\,!)^{88}$. Si p est un nombre premier, $p > n_o$, si $k(p) = [\sqrt[3]{\log p}]$ et si le premier cas du DTF est faux pour p alors p divise les $k(p)$ nombres de Bernoulli $B_{p-3}, B_{p-5}, \ldots, B_{p-k(p)-1}$. (Le nombre n_o n'a rien d'absolu, et peut être réduit avec un peu de soin, mais reste tout de même trop grand pour des fins pratiques).

Ce théorème, qui met Krasner parmi les héritiers de Kummer, indique la plausibilité du premier cas du DTF.

Il serait injuste, vis à vis de Kummer, de ne pas mentionner que, même en théorie des nombres, il a eu d'autres contributions et idées de toute première grandeur - peut être encore plus importantes. C'est la théorie de la loi de réciprocité pour le symbole de restes de puissances, précurseur de la théorie des corps de classes, et il faut le dire, liée, en quelque sorte, au théorème de Fermat, comme allaient le montrer Furtwängler, dès 1912, et Hasse vers 1926.

L'oeuvre de Kummer a été continuée et amplifiée par les nombreux mathématiciens qui se sont occupés (et qui s'occuperont) du DTF. Il y a certainement de quoi apprendre et comprendre, et la publication de ses oeuvres en 1975, annotées par A. Weil permettra aux mathématiciens un examen attentif de ses riches idées.

=-=-=-=-=-=-=-=-=-=-=-=-=