

demi-tangente un des demi-axes x_1 . Il existe des hypersurfaces régulières à k dimensions: $S^k, S_-^k, S_+^k, k=1, 2, \dots, n$ (S^n, S_+^n, S_-^n étant des domaines de E_n) telles que

$$1^0 \quad \Theta \in S^1 \subset S^2 \subset \dots \subset S^n;$$

$$2^0 \quad S^{k-1} \text{ coupe } S^k \text{ en } S_-^k \text{ et } S_+^k; \quad S^k = S_-^k + S^{k-1} + S_+^k, \quad k=2, 3, \dots, n, \text{ et } S^1 = S_-^1 + \{\Theta\} + S_+^1;$$

3^0 L'hypersurface S^k est tangente à l'hyperplan $x_{k+1} = \dots = x_n = 0$ dans Θ , $k=1, 2, \dots, n-1$;

4^0 il existe une classification de la famille \mathcal{R}^n de toutes les demi-caractéristiques tendant vers Θ en sous-familles $\mathcal{R}_+^k, \mathcal{R}^k, \mathcal{R}_-^k$, telle que

$$a) \quad \mathcal{R}^1 = \mathcal{R}_-^1 + \mathcal{R}_+^1, \quad \mathcal{R}^k = \mathcal{R}_-^k + \mathcal{R}^{k-1} + \mathcal{R}_+^k, \quad k=2, 3, \dots, n,$$

b) la famille \mathcal{R}^k , ou \mathcal{R}_-^k , ou \mathcal{R}_+^k engendre $S^k - \{\Theta\}$, ou S_-^k , ou S_+^k ;

toute demi-caractéristique de \mathcal{R}_-^k , ou \mathcal{R}_+^k , tend vers Θ en ayant pour demi-tangente le demi-axe négatif, ou positif (la famille \mathcal{R}^1 , ou \mathcal{R}_+^1 , ne contient qu'une seule demi-caractéristique et S_-^1 , ou S_+^1 , est une restriction à gauche de cette demi-caractéristique).

Travaux cités

- [1] H. Dulac, *Points singuliers des équations différentielles*, Mem. Sc. Math., 41 (1934).
 [2] E. Kamke, *Differentialgleichungen reeller Funktionen*, Leipzig 1930.
 [3] — *Differentialgleichungen, Lösungsmethoden und Lösungen I*, Leipzig 1943.
 [4] S. Lefschetz, *Lectures on differential equations*, Princeton 1948.
 [5] O. Perron, *Über die Gestalt der Integralkurven einer Differentialgleichung erster Ordnung in der Umgebung eines singulären Punktes*, Math. Zeitschr. 15 (1922), p. 121-146.
 [6] — *Über die Gestalt der Integralkurven einer Differentialgleichung erster Ordnung in der Umgebung eines singulären Punktes*, Zweiter Teil, *ibid.* 16 (1923), p. 273-295.
 [7] T. Ważewski, *Sur la coïncidence asymptotique des intégrales de deux systèmes d'équations différentielles*, Bull. Acad. Sc. et Lettr., Sér. A, 1940, p. 147-150.
 [8] — *Sur certaines conditions de coïncidence asymptotique des intégrales des deux systèmes d'équations différentielles*, Comptes-rendus des séances de la Classe III: Sciences mathem. et phys. de la Société des Sciences et des Lettres de Varsovie 42 (1949), p. 198-203.
 [9] — *Sur un principe topologique d'examen de l'allure asymptotique des intégrales des équations différentielles ordinaires*, Ann. Soc. Polon. Math. 20 (1947), p. 279-313.

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK
 INSTITUT MATHÉMATIQUE DE L'ACADÉMIE POLONAISE DES SCIENCES

Über die Gleichung $x^m + 1 = y^n$

von R. OBLÁTH (Budapest)

Die Frage ob es zwei aufeinander folgende Zahlen (ausser $-1, 0; 0, 1; 8, 9$) gibt, welche beide volle Potenzen sind, wurde zwar schon im Mittelalter gestellt¹⁾, ist aber auch heute noch nicht vollständig gelöst. Es handelt sich also um die diophantische Gleichung

$$(I) \quad x^m + 1 = y^n.$$

¹⁾ Levi ben Gerson (1288-1344) — einer der bedeutendsten Mathematiker des Mittelalters — hat bewiesen, dass

$$3^{m+1} \pm 1$$

für $m > 1$ keine Potenz der Zahl 2 ist (vgl. S. L. E. Dickson, *History of the Theory of Numbers*, vol. II. *The Diophantine Analysis*, New York 1934, p. 731).

Die Geschichte und Literatur des Problems habe ich in früheren Publikationen — besonders in der ungarischen — ausführlich dargestellt. (*Über die Zahl $x^2 - 1$* , Mathematica B. (holländische) VIII (1939-1940), p. 161-172; *Az $x^2 - 1$ számokról*, Mat. és Fiz. Lapok 47 (1940), p. 58-77; *Sobre ecuaciones imposibles de la forma $x^m + 1 = y^n$* , Revista Mat. Hisp.-Americana I (1941), p. 122-140). Nach dem Erscheinen dieser Arbeiten wurde ein wichtiger Fund gemacht. Die bis dahin als verschollen geltende *Solutio duorum problematum* etc. von Frénicle aus dem Jahre 1657 wurde aufgefunden und von J. E. Hofmann ausführlich bekannt gemacht (J. E. Hofmann, *Neues über Fermats zahlentheoretische Herausforderungen* von 1657, Abhandl. d. Preuss. Akad. d. Wiss. 9 (1943), p. 1-52).

Theorema 10 der *Solutio* behandelt die Gleichung (II) (siehe J. E. Hofmann, l. c., p. 24). Der Satz behauptet die Unmöglichkeit der unbestimmten Gleichung

$$p^n + 1 = x^2$$

(p ungerade Primzahl, $n \geq 2$). Ich erzähle Frénicle's geistreichen Beweis in modernen Bezeichnungen. Der Satz ist für gerade n selbstverständlich. Wäre nun $p^n + 1 = x^2$ für ein ungerades n erfüllbar, so liesse sich $p^n = (x+1)(x-1)$ in zwei Teiler mit der Differenz 2 zerlegen. Die Teiler von p^n sind $1, p, \dots, p^{n-1}$. Die kleinstmögliche Differenz zweier Teiler ist $p(p-1)$ und tritt für $n=3$ auf. Sie ist aber stets grösser als 2, da $p \geq 3$ ist. Der Satz gilt auch für $p=2$, wenn $n \geq 4$ ist; $n=3$ ist eine Ausnahme, $2^3 + 1 = 3^2$.

In einer noch nicht publizierten Arbeit hat R. Hampel den folgenden Satz bewiesen:

SATZ 1. *Unter der Bedingung*

$$(1) \quad |x-y|=1$$

ist die diophantische Gleichung (I) — von den Ausnahmen $-1, 0; 0, 1; 2, 3$ abgesehen — in ganzen Zahlen unmöglich.

In den nachfolgenden Zeilen gebe ich für diesen Satz einen anderen, sehr einfachen Beweis, der hauptsächlich einige Ergebnisse von T. Nagell benützt.

In der Gleichung (I) kann m keine gerade Zahl sein, denn infolge eines Satzes von V. A. Lebosgue [1]²⁾ hat die Gleichung

$$x^2+1=y^n$$

keine ganzzahlige Lösungen mit $x \neq 0$; m ist daher ungerade. Zwei Fälle sind zu unterscheiden:

$$\begin{aligned} \text{A.} \quad & x=y+1, \\ & (y+1)^m+1=y^n \quad (n > m), \\ & y^n - y^m - \dots - my - 2 = 0. \end{aligned}$$

Die zulässigen Werte für y sind daher bloss $y = \pm 1, \pm 2$ und für x die Werte $x = 2, 0, 3, -1$, was die triviale Lösung $x = 0, y = -1, n$ gerade ergibt.

$$\begin{aligned} \text{B.} \quad & x=y-1, \\ & (y-1)^m+1=y^n \quad (m > n), \\ & y^m - y^n + \dots + my = 0. \end{aligned}$$

Nach Ausschliessung der trivialen Lösung $y = 0, (x = -1)$ ist sofort sichtbar, dass y ein Teiler des Exponenten m sein muss:

$$y = \pm d, \quad d > 0, \quad d | m.$$

Im Falle $y = d$ hat man

$$(2) \quad (d-1)^m+1=d^m$$

und

$$(3) \quad (d-1)^{m-1} = \frac{d^m-1}{d-1} = d^{m-1} + \dots + d + 1.$$

²⁾ S. auch T. Nagell [2].

Da m ungerade ist, muss es auch d sein. Mithin ist das erste Glied von (3) eine gerade Zahl, also auch das dritte. Nun besteht aber dieses aus n ungeraden Summanden, daher ist n gerade.

Im Falle $y = -d$ wird dasselbe ganz analog gezeigt, dann steht es aber in Widerspruch mit der Gleichung

$$-(d+1)^m+1 = (-d)^n,$$

aus welcher sich n als ungerade ergibt, so dass man weiter nur den Fall $y = d$ zu betrachten hat.

Wird $n = 2r$ gesetzt, so lässt sich (2) in der Form

$$(d-1)^m+1 = (d^r)^2,$$

also in der Form

$$(4) \quad \xi^m+1 = \eta^2$$

schreiben. Es wurde jedoch von Nagell [3] bewiesen, dass (4), von den trivialen Fällen abgesehen, nur dann bestehen kann, wenn jeder Primteiler des Exponenten m — also auch ihr Aggregat d — die Form $8a+1$ hat. Das erste Glied von (3) ist daher durch eine hohe Potenz der Zahl 2 teilbar (mindestens durch 8), folglich auch das dritte, in diesem ist aber jeder Summand $\equiv 1 \pmod{8}$, weswegen der Exponent n durch 8 teilbar ist; $n = 4r$, und (I) erhält die Form

$$x^m+1 = (y^r)^4 = z^4.$$

Diese Gleichung ist nun infolge eines zuerst von S. Selberg [5]³⁾ bewiesenen Satzes des Nagell unmöglich, w. z. b. w.

Hampel hat auch über die Abweichung der beiden Potenzen im Falle (I) einen genaueren Satz aufgestellt, der sich ähnlich beweisen lässt.

SATZ 2. *Unter der Bedingung (1) ist*

$$|x^m - y^n| = k \geq \max(5, y+1),$$

ausgeschlossen natürlich die trivialen Lösungen der Gleichung (I) und die ebenfalls trivialen Fälle $x = \pm 2, y = \pm 1, n = 2; x = \pm 1, y = \pm 2, m = 2$.

$k > 1$ folgt aus Satz 1. Die Bedingung (1) zeigt, dass x und y ungleicher Parität sind, k kann demnach keine gerade Zahl sein. Wenn nun in

$$(5) \quad (y \pm 1)^m - y^n = k,$$

$$(5') \quad y^n \pm \dots \pm my - (k \pm 1) = y^n$$

³⁾ S. auch T. Nagell [4].

$k=3$ gesetzt wird, dann kann y bloss $\pm 1, \pm 2$ oder ± 4 sein; die zugehörigen x -Werte sind $2, 3, 5; 0, 1, 3; -2, 3, -5; 0, -1, -3$. Nach Ausschliessung der trivialen Ausnahmen bleiben die Werte

- (a) $y = \pm 2, \quad x = \pm 3;$
 (b) $y = \pm 4, \quad x = \pm 3;$
 (c) $y = \pm 4, \quad x = \pm 5.$

Die Gruppierung (a) und (b) ist unmöglich mod 3, die Gruppierung (c) mod 5.

(5) ist aber auch mit $k=y$ oder $y \pm 1$ unmöglich, denn dann wären beide Seiten teilerfremd. Es sei nun

$$(6) \quad k \leq y - 2, \quad k + 1 \leq y - 1.$$

Aus (5') folgt, dass y ein Teiler des absoluten Gliedes sein muss, was durch (6) ausgeschlossen ist, denn y kann kein Teiler einer Zahl $\leq y - 1$ sein.

Zum Schluss will ich noch einen Satz über die Gleichung (I) mitteilen.

Satz 3. Die diophantische Gleichung (*n* Primzahl)

$$(II) \quad x^2 - 1 = y^n$$

ist — von den trivialen Lösungen $0, -1; 1, 0; 3, 2$ abgesehen — für jeden Exponenten $n < 25\,000$ unmöglich.

Beweis. In meiner unter¹⁾ zitierten (spanischen) Arbeit habe ich bewiesen, dass das Bestehen der Gleichung (II) (*n* Primzahl)

$$(7) \quad 2^{n-1} \equiv 1 \pmod{n^2}$$

nach sich zieht. D. H. Lehmer⁴⁾ hat aber jüngst gezeigt, dass die Kongruenz (7) ausser den bekannten Lösungen $n=1093$ und $n=3511$ unter 25 000 keine anderen hat. In meinen zitierten Arbeiten habe ich jedoch den Satz auch für diese Werte bewiesen, so, dass er also im vollen angegebenen Umfange gilt.

Zitate

[1] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$* , Nouv. Ann. de Math. 9 (1850), p. 178-181.

[2] T. Nagell, *Analyse indéterminée de degré supérieur*, Mémorial des Sciences Mathématiques 39 (1929), p. 58.

[3] — *Sur une équation diophantienne à deux indéterminées*, Det kongelige Norsk Videnskabers Selskab Forhandling VII, 38 (1934), p. 136-139.

[4] — Norsk. Mat. Tidskr. 1 (1919).

[5] S. Selberg, ebenda, 14 (1932), p. 79-80.

[6] N. G. W. H. Beeger, *On even numbers m dividing $2^m - 2$* , Amer. Math. Monthly 58 (1951), p. 553-555.

⁴⁾ Siehe N. Beeger [6].

Über den letzten Fermatschen Satz in relativ-zyklischen Zahlkörpern

von P. DÉNES (Budapest)

Fermat hat seine berühmte Behauptung die Gleichung

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

$n > 2$, sei in ganzen, nicht verschwindenden Zahlen x, y, z unlösbar, nur für rationale Zahlen ausgesprochen. Die Zerlegung der linken Seite der Gleichung in Faktoren führt ins Gebiet der Kreiskörper, und die Behandlung des Problems erfolgte seit den Kummerschen Arbeiten fast ausschliesslich in Kreiskörpern. Natürlich sind unendlich viele algebraische Zahlkörper vorhanden, in welchen die Fermatsche Gleichung lösbar ist; z. B. im Körper $k(\sqrt[n]{2})$ gilt die Lösung $1, 1, \sqrt[n]{2}$. Aber auch in solchen Zahlkörpern ist folgende Frage von grossem Interesse: gibt es nur singuläre Lösungen, oder existieren auch unendlich viele Lösungsstellen.

Unter den wenigen Arbeiten, die das Fermatsche Problem in Nicht-Kreiskörpern untersuchen, seien die Arbeiten von Fueter [1], der die Unlösbarkeit der Gleichung $x^3 + y^3 = z^3$ in gewissen quadratischen Zahlkörpern zeigte, und die von Burnside [2], der unendlich viele quadratische Zahlkörper aufzeigte in welchen $x^3 + y^3 = z^3$ lösbar ist, erwähnt.

In der vorliegenden Arbeit werden wir das Problem in einer Serie von relativ-zyklischen Zahlkörpern untersuchen.

Diese Zahlkörper-Serie wird auf Grund einer früheren Arbeit [3] folgendermassen erzeugt: l bezeichne eine reguläre Primzahl, $\zeta = e^{2\pi i/l}$, k_0 den Zahlkörper der l^{ten} Einheitswurzel, $\lambda = 1 - \zeta$, $l = (\lambda)$, und E_0 sei eine Einheit in k_0 , die nicht die l^{te} Potenz einer Einheit aus k_0 ist. Wir bilden den Kummerschen Körper $k_1 = k(\sqrt[l]{E_0}, \zeta)$. Es sei ferner E_1 eine Einheit aus k_1 , welche nicht die l^{te} Potenz einer Einheit aus k_1 ist; durch Adjunktion der l^{ten} Wurzel der Einheit E_1 zum Körper k_1 erhält man den Körper $k_2 = k(\sqrt[l]{E_1}, k_1)$. Man kann in dieser Weise fortfahren, und das allgemeine Glied dieser Serie ist $k_i = k(\sqrt[l]{E_{i-1}}, k_{i-1})$, wobei E_{i-1} eine Einheit des Körpers k_{i-1} bezeichnet, die nicht die l^{te} Potenz einer Einheit in k_{i-1} ist.