ÜBER DIE DIOPHANTISCHE GLEICHUNG $x^l + y^l = cz^l$.

Von

PETER DÉNES

in Budapest.

Mit dem Problem der Lösbarkeit der unbestimmten Gleichung

$$x^l + y^l = cz^l \tag{1}$$

in rationalen ganzen, nicht verschwindenden Zahlen x, y, z beschäftigen sich eine Anzahl von Arbeiten[1], welche die Unlösbarkeit der Gleichung (1) für gewisse Primzahlexponenten und spezielle rationale ganze Zahlen c bewiesen. Unter den Werten von c ist besonders $c = 2$ von grossem Interesse, weil eine Anzahl von Diophantischen Problemen auf diese Gleichung zurückgeführt werden kann[2]; die Unlösbarkeit der Gleichung

$$x^n + y^n = 2z^n, \quad xyz \neq 0, 1 \tag{2}$$

in rationalen ganzen Zahlen x, y, z ist bis jetzt jedoch nur für die Exponenten $n = 3, 4, 5$ und deren Mehrfache bestätigt.[3] Es ist jedoch sehr wahrscheinlich, dass die Gleichung (2), wenn $n > 2$, keine rationale ganze Lösung hat.

Das Ziel der vorliegenden Arbeit ist, weitere Untersuchungen bezüglich der Lösbarkeit der Gleichung (1) zu unternehmen und für die Zahl c solche Bedingungen zu

---

[1] U. a.: 1 a) E. MAILLET: Acta Math., Bd. 24, 1901, S. 247—256. 1 b) ——: Ann. di Mat. pura ed appl., Ser. III, Bd. 12, 1906, S. 145—178. 1 c) S. LUBELSKI: Prace Matematyczne-Fizyczne, Bd. 42, 1935, S. 11—44. 1 d) H. S. VANDIVER: Monatshefte f. Math. u. Phys., Bd. 43, 1936, S. 317—320.

[2] Siehe diesbezüglich u. a.: R. OBLÁTH: Tohoku Math. Journ., Bd. 38, 1933, S. 73—92. ——: Matematikai és Fizikai Lapok, Bd. 47, 1940, S. 58—77. ——: Revista Matematica Hispano-Americana, Serie 4^{O}, Bd. I, 1941, S. 122—143. ——: Journ. of the London Math. Soc., Bd. 23, 1948, S. 252—253. ——: Matematikai Lapok, Bd. I, 1950, S. 138—139. P. ERDÖS: Journ. of the London Math. Soc., Bd. 14, 1939, S. 245—249. P. Erdös informierte mich ferner über seine neue, im Bd. 26, 1951. des Journ. of the London Math. Soc. erscheinende Arbeit: $\binom{n}{k}$ ist keine m-te Potenz, falls $m > 1$, $k > 3$, $n \geq 2k$, und gab seiner Vermutung Ausdruck, dass der Satz wahrscheinlich auch für $k = 2$ und $k = 3$ gültig bleibt, wenn $m > 2$ ist. Die Vermutung wird durch die Sätze 7 bis 9 für eine Reihe von Primexponenten bestätigt.

[3] EULER: Algebra II, § 247. LEGENDRE: Essai sur la théorie des nombres, An. VI, S. 409. LEJEUNE DIRICHLET: Crelle's Journal, Bd. 3, 1828, S. 354—376.

finden, welche auch für $c=2$ gültig sind und dadurch die bisherigen spärlichen Resultate über die unbestimmte Gleichung (2) zu erweitern.

Es bezeichne l eine reguläre Primzahl, $\zeta=e^{2\pi i/l}$, $k(\zeta)$ den Kreiskörper der l-ten Einheitswurzeln, $\lambda=1-\zeta$, $\mathfrak{l}=(\lambda)$. Es gilt der folgende Satz:

Satz 1. l sei eine reguläre Primzahl, $l>3$, $k(\zeta)$ der zugehörige Kreisteilungskörper, ξ, η seien reelle Zahlen, $\mathfrak{a}$, $\mathfrak{z}$ reelle Ideale des Körpers $k(\zeta)$. Weiter seien ξ, η, $\mathfrak{a}\,\mathfrak{z}$ teilerfremd und prim zu $\mathfrak{l}$, ferner sei $\mathfrak{a}$ höchstens durch $\frac{l-3}{2}$ verschiedene und nur durch reelle Primideale des Körpers $k(\zeta)$ teilbar. Dann ist die Diophantische Gleichung

$$\xi^l+\eta^l=\mathfrak{a}\,\mathfrak{z}^l,\ (\xi)(\eta)\,\mathfrak{z}\neq 1 \tag{3}$$

unmöglich.

Beweis. Die linke Seite der Gleichung (3) kann in l verschiedene Faktoren zerlegt werden, welche bekanntlich, da ξ, η teilerfremd und $\mathfrak{a}$, $\mathfrak{z}$ nicht durch $\mathfrak{l}$ teilbar sind, sämtlich zueinander relativ prim sind:

$$\xi+\eta\zeta^i=\mathfrak{a}_i\,\mathfrak{i}_i^l \quad (i=0,\,1,\,\ldots,\,l-1). \tag{4}$$

Die Ideale $\mathfrak{a}_1,\,\mathfrak{a}_2,\,\ldots,\,\mathfrak{a}_{l-1}$ können nur Einheitsideale sein. Wäre nämlich etwa $\mathfrak{a}_j\neq 1$, also

$$\xi+\eta\zeta^j\equiv 0 \pmod{\mathfrak{a}_j},$$

so ergibt die durch die Substitution $\zeta:\zeta^{-1}$ entspringende Kongruenz, dass auch

$$\xi+\eta\zeta^{-j}\equiv 0 \pmod{\mathfrak{a}_j}$$

ist, was der Tatsache, dass die Faktoren (4) teilerfremd sind, widerspricht. Es lautet also die Zerlegung von (3):

$$\xi+\eta=\mathfrak{a}\,\mathfrak{i}_0^l, \tag{5}$$

$$\xi+\eta\zeta^i=\mathfrak{i}_i^l \quad (i=1,\,2,\,\ldots,\,l-1). \tag{6}$$

Da l eine reguläre Primzahl ist, erhalten wir in bekannter Weise aus (6):

$$\xi+\eta\zeta^i=\zeta^{u_i}\varepsilon_i\,\varrho_i^l \quad (i=1,\,2,\,\ldots,\,l-1), \tag{7}$$

wo ε_i reelle Einheiten, ϱ_i zu $\mathfrak{l}$ prime Zahlen des Körpers $k(\zeta)$ sind. Ferner gilt

$$u_i\equiv i\cdot\frac{t}{s+t} \pmod{l} \quad (i=1,\,2,\,\ldots,\,l-1),$$

wobei die Zahlen s, t durch die Kongruenzen $\xi\equiv s \pmod{\mathfrak{l}^2}$ und $\eta\equiv t \pmod{\mathfrak{l}^2}$ bestimmt sind. Werden die aus den Gleichungen (7) erzeugbaren Kongruenzen

$$\xi(1-\zeta^{2u_i}) \equiv \eta(\zeta^{2u_i-i} - \zeta^i) \pmod{\mathfrak{l}^l},$$

welche für die Werte $i = 0, 1, \ldots, l-1$ gültig sind, addiert, so ergeben sich die Beziehungen

$$u_i \equiv \frac{i}{2} \pmod{l} \quad (i = 1, 2, \ldots, l-1)$$

und

$$\xi \equiv \eta \pmod{\mathfrak{l}^{l-1}}.$$

Damit wird aus (7):

$$\xi\zeta^{-i/2} + \eta\zeta^{i/2} = \varepsilon_i \varrho_i^l \quad (i = 1, 2, \ldots, l-1). \tag{8}$$

Aus (5) und (8) gewinnen wir die folgende Gleichung

$$\varrho_1^l + \varrho_{l-1}^l = \mathfrak{a}\mathfrak{i}_0^l, \tag{9}$$

in der die Zahlen ϱ_1 und ϱ_{l-1} einander nach der Substitution $\zeta : \zeta^{-1}$ konjugiert sind. Die Gleichung (9) zerfällt in die folgenden Faktoren:

$$\varrho_1 + \varrho_{l-1}\zeta^k = \mathfrak{b}_k \mathfrak{g}_k^l \quad (k = 0, 1, \ldots, l-1),$$

welche sämtlich zueinander relativ prim sind. Unter den $l-1$ Werten von $k = 1, 2, \ldots, l-1$ gibt es gewiss ein Paar: m und $l-m$, so, dass $\mathfrak{b}_m = \mathfrak{b}_{l-m} = 1$ ist, da $\mathfrak{a}$ höchstens $\frac{l-3}{2}$ verschiedene Primidealteiler besitzt. Wir haben also 3 Gleichungen:

$$\left.\begin{aligned} \varrho_1 + \varrho_{l-1} &= \mathfrak{b}_0 \mathfrak{g}_0^l, \\ \varrho_1\zeta^{-m/2} + \varrho_{l-1}\zeta^{m/2} &= \vartheta_m \tau_m^l, \\ \varrho_1\zeta^{m/2} + \varrho_{l-1}\zeta^{-m/2} &= \vartheta_{l-m}\tau_{l-m}^l, \end{aligned}\right\} \tag{10}$$

in welchen ϑ_m, ϑ_{l-m} reelle Einheiten, τ_m, τ_{l-m} reelle Zahlen des Körpers $k(\zeta)$ sind, da die Gleichungen (10) bei Anwendung der Substitution $\zeta : \zeta^{-1}$ unverändert bleiben. Aus den Gleichungen (10) gewinnt man

$$\tau_m^l + \frac{\vartheta_{l-m}}{\vartheta_m}\tau_{l-m}^l = \mathfrak{b}_0 \mathfrak{g}_0^l. \tag{11}$$

Wir untersuchen jetzt die Einheit

$$\gamma_m = \frac{\vartheta_{l-m}}{\vartheta_m}.$$

Aus (8) können wir die folgenden Gleichungen bilden:

$$\frac{\xi\zeta^{-i/2} + \eta\zeta^{i/2}}{\xi\zeta^{i/2} + \eta\zeta^{-i/2}} = \left(\frac{\varrho_i}{\varrho_{l-i}}\right)^l \quad \left(i = 1, 2, \ldots, \frac{l-1}{2}\right),$$

woraus sich für ein beliebiges Primideal $\mathfrak{q}$ des Körpers $k(\zeta)$ die Potenzcharaktere ergeben:

$$\left\{\frac{\xi\zeta^{-i/2}+\eta\zeta^{i/2}}{\xi\zeta^{i/2}+\eta\zeta^{-i/2}}{\mathfrak{q}}\right\}=1 \quad \left(i=1, 2, \ldots, \frac{l-1}{2}\right). \tag{12}$$

Wird $\mathfrak{q}=\mathfrak{p}$ als ein Teiler der Zahl $\xi+\eta\zeta$ gewählt, so gestaltet sich (12) wegen

$$\xi\zeta^{-i/2}+\eta\zeta^{i/2}\equiv\eta(\zeta^{i/2}-\zeta^{-i/2+1}) \pmod{\mathfrak{p}},$$

wie folgt:

$$\left\{\frac{\Theta_i}{\mathfrak{p}}\right\}=1 \quad \left(i=1, 2, \ldots, \frac{l-3}{2}\right) \tag{13}$$

mit

$$\Theta_i=\frac{\zeta^{i/2}-\zeta^{-i/2}}{\zeta^{(i+2)/2}-\zeta^{-(i+2)/2}} \quad \left(i=1, 2, \ldots, \frac{l-3}{2}\right).$$

Wir zeigen, dass $\Theta_1, \Theta_2, \ldots, \Theta_{\frac{l-3}{2}}$ ein solches unabhängiges Einheitssystem des Körpers $k(\zeta)$ bilden, dass eine beliebige Einheit H des Körpers $k(\zeta)$ durch eine Gleichung

$$H^d=\prod_{i=1}^{\frac{l-3}{2}}\Theta_i^{d_i} \tag{14}$$

ausgedrückt werden kann, wobei die Zahl d, falls $d, d_1, \ldots, d_{\frac{l-3}{3}}$ keinen gemeinsamen Faktor haben, zu l prim ist.

Betrachten wir nämlich die sogenannten Kreiseinheiten

$$e_k=\frac{\zeta^{r^{k/2}}-\zeta^{-r^{k/2}}}{\zeta^{r^{k-1/2}}-\zeta^{-r^{k-1/2}}} \quad \left(k=1, 2, \ldots, \frac{l-1}{2}\right),$$

wobei r eine primitive Wurzel nach l bezeichnet, so kann bekanntlich die Einheit H in der Form

$$H^f=\prod_{k=1}^{\frac{l-3}{2}}e_k^{f_k} \tag{15}$$

ausgedrückt werden. Dabei ist f, falls $f, f_1, \ldots, f_{\frac{l-3}{2}}$ keinen gemeinsamen Faktor haben und l eine reguläre Primzahl ist, nicht durch l teilbar. Aus den Gleichungen (14) und (15) ergibt sich für die Exponenten ein lineares Gleichungssystem, mit dem aus den Exponenten $f_1, \ldots, f_{\frac{l-3}{2}}$ die Exponenten $d_1, \ldots, d_{\frac{l-3}{2}}$ eindeutig bestimmt werden können und woraus auch $d=f$ folgt. Aus (13) und (14) können wir also schliessen, dass der Potenzcharakter

$$\left\{\frac{H}{\mathfrak{p}}\right\} = 1$$

ist. Hieraus folgt auch

$$\left\{\frac{H}{\varrho_i}\right\} = 1 \quad \left(i = 1, 2, \ldots, \frac{l-1}{2}\right) \tag{16}$$

für eine jede reelle Einheit H des Körpers $k(\zeta)$. Wählt man für die Einheit H in (16) die Einheiten

$$E_n = \prod_{k=1}^{\frac{l-3}{2}} e_k^{r^{-2kn}} \quad \left(n = 1, 2, \ldots, \frac{l-3}{2}\right), \tag{17}$$

so bestätigte Vandiver[1], dass aus (16) und (17) die Kongruenzen

$$\varrho_i \equiv \varrho_{l-i} \pmod{\mathfrak{l}^{l-1}} \quad \left(i = 1, 2, \ldots, \frac{l-1}{2}\right) \tag{18}$$

folgen. Aus den beiden letzten Gleichungen von (10) haben wir sodann

$$\frac{\vartheta_{l-m}\,\tau_{l-m}^l}{\vartheta_m\,\tau_m^l} \equiv \frac{\varrho_1\,\zeta^{m/2} + \varrho_{l-1}\,\zeta^{-m/2}}{\varrho_1\,\zeta^{-m/2} + \varrho_{l-1}\,\zeta^{m/2}} \equiv 1 \pmod{\mathfrak{l}^{l-1}}.$$

Es ist also die Einheit γ_m nach dem Modul l einer rationalen ganzen Zahl kongruent, woraus folgt, dass γ_m in $k(\zeta)$ eine volle l-te Potenz ist. Die Gleichung (11) wird hierdurch

$$\tau_m^l + \tau_{l-m}'^l = \mathfrak{b}_0\,\mathfrak{g}_0^l. \tag{19}$$

Sie hat die gleiche Form wie Gleichung (3), und das Ideal $\mathfrak{b}_0$ enthält nur reelle und höchstens $\frac{l-3}{2}$ verschiedene Primidealteiler. Die Norm des Ideals $\mathfrak{g}_0$ ist kleiner als die Norm des Ideals $\mathfrak{z}$. Unterwirft man die Gleichung (19) derselben Umformung wie die Gleichung (3), so gelangt man zu einer der Gleichung (19) ähnlichen Gleichung:

$$\tau_m^{*l} + \tau_{l-m}^{*l} = \mathfrak{b}_0^*\,\mathfrak{g}_0^{*l}, \tag{20}$$

in welcher die Norm des Ideals $\mathfrak{g}_0^*$ kleiner ist, als die Norm des Ideals $\mathfrak{g}_0$. Die Methode fortsetzend, stösst man schliesslich entweder auf einen Widerspruch, oder es entsteht eine Gleichung von der Form (19), in welcher $\mathfrak{g}_0$ das Einheitsideal ist. In diesem Falle hat man die zwei konjugierten Gleichungen

$$\tau_m + \tau_{l-m}'\,\zeta = \zeta^{1/2}\,\varepsilon',$$
$$\tau_m + \tau_{l-m}'\,\zeta^{-1} = \zeta^{-1/2}\,\varepsilon',$$

[1] H. S. Vandiver: Proc. Nat. Acad. Sci., Bd. 17, 1931, S. 661—673.

in welchen ε' eine reelle Einheit in $k(\zeta)$ ist. Wie leicht einzusehen, haben diese Gleichungen die einzige Lösung

$$\tau_m = \tau'_{l-m} = \varepsilon'', \quad \mathfrak{b}_0 = (2), \tag{21}$$

wobei ε'' eine reelle Einheit des Körpers $k(\zeta)$ bezeichnet. Aus (21) folgt

$$\vartheta_m \tau^l_m = \vartheta_{l-m} \tau^l_{l-m} = \varepsilon''',$$

wobei ε''' eine reelle Einheit in $k(\zeta)$ ist. Hierdurch gehen die beiden letzten Gleichungen von (10) in die Form über:

$$\varrho_1 + \varrho_{l-1} \zeta^m = \zeta^{m/2} \varepsilon''',$$
$$\varrho_1 + \varrho_{l-1} \zeta^{-m} = \zeta^{-m/2} \varepsilon'''.$$

Die einzige Lösung ist

$$\varrho_1 = \varrho_{l-1} = \varepsilon^*, \quad \mathfrak{a} = (2)$$

wobei ε^* eine reelle Einheit des Körpers $k(\zeta)$ ist. In gleicher Weise können wir aus den Gleichungen (8) schliessen, dass auch

$$\xi = \eta = \varepsilon^{**},$$

gilt, wobei ε^{**} eine reelle Einheit des Körpers $k(\zeta)$ bezeichnet. Wird also diejenige Gleichung (19), in welcher $\mathfrak{g}_0 = 1$ ist, in einer umgekehrten Kette bis zur Ausgangsgleichung (3) zurückgeführt, so sehen wir, dass in diesem Falle die Zahlen ξ, η Einheiten sind und $\mathfrak{z}$ das Einheitsideal des Körpers $k(\zeta)$ darstellt. Hierdurch sind wir mit unserer Voraussetzung

$$(\xi)(\eta)\mathfrak{z} \neq 1 \tag{22}$$

in Widerspruch geraten. Daraus ist aber ersichtlich, dass man mit der Voraussetzung (22) zu keiner Gleichung (19) gelangen kann, in welcher $\mathfrak{g}_0 = 1$ ist. Die herangezogene descente infinie muss also schliesslich zu einem Widerspruch führen. Damit ist Satz 1 bewiesen.

Satz 2. l sei eine reguläre Primzahl, $l > 3$, $k(\zeta)$ der zugehörige Kreisteilungskörper, ξ, η seien reelle Zahlen, $\mathfrak{a}$, $\mathfrak{z}$ reelle Ideale des Körpers $k(\zeta)$. Weiter seien ξ, η, $\mathfrak{a}\mathfrak{z}$ teilerfremd und prim zu $\mathfrak{l}$, und $\mathfrak{a}$ zerfalle in zwei Primideale, bzw. in zwei Primidealpotenzen, welche zueinander nach der Substitution $\zeta : \zeta^{-1}$ konjugiert sind. Dann ist die Diophantische Gleichung

$$\xi^l + \eta^l = \mathfrak{a}\mathfrak{z}^l, \quad (\xi)(\eta)\mathfrak{z} \neq 1 \tag{23}$$

unmöglich.

Beweis. Bei der Zerlegung der Gleichung (23) in Faktoren ähnlich zu (4) tritt das Ideal $\mathfrak{a}$ entweder in der Gleichung $i = 0$ auf, oder es kommen seine konjugierten Faktoren in den konjugierten Gleichungspaaren $i = m$, $l - m$ vor. Im ersten Falle führt die Methode des Satzes 1 zu einer, der Gleichung (19) ähnlichen Gleichung, welche die gleiche Struktur hat wie (23). Im zweiten Falle haben wir, da $l > 3$ ist, wenigstens die folgenden 5 Gleichungen

$$\begin{aligned} \xi + \eta &= \varepsilon_0 \varrho_0^l \\ \xi \zeta^{-n/2} + \eta \zeta^{n/2} &= \varepsilon_n \varrho_n^l \\ \xi \zeta^{n/2} + \eta \zeta^{-n/2} &= \varepsilon_n \varrho_{l-n}^l \\ \xi + \eta \zeta^m &= \mathfrak{a}_m \mathfrak{i}_m^l \\ \xi + \eta \zeta^{-m} &= \mathfrak{a}_{l-m} \mathfrak{i}_{l-m}, \end{aligned}$$

wobei $\mathfrak{a} = \mathfrak{a}_m \mathfrak{a}_{l-m}$ ist. Die ersten drei Gleichungen ergeben

$$\varrho_n^l + \varrho_{l-n}^l = \varepsilon_0 \varrho_0^l,$$

wobei ε_0 die l-te Potenz einer Einheit in $k(\zeta)$ ist, da l eine reguläre Primzahl ist. Diese descente führt also entweder zu einem Widerspruch, wie im Satz 1, oder zu der Fermatschen Gleichung, welche für reguläre Primexponenten unmöglich ist.

Satz 3. l sei eine reguläre Primzahl, $k(\zeta)$ der zugehörige Kreisteilungskörper, ξ, η seien reelle Zahlen, $\mathfrak{a}, \mathfrak{z}$ reelle Ideale des Körpers $k(\zeta)$. Weiter seien $\xi, \eta, \mathfrak{a}\mathfrak{z}$ teilerfremd, und es sei von den Zahlen ξ, η etwa η durch $\mathfrak{l}$ teilbar. $\mathfrak{a}$ enthält nur reelle Primidealteiler. Dann besteht eine notwendige Bedingung für die Lösbarkeit der Diophantischen Beziehung

$$\xi^l + \eta^l = \mathfrak{a}\mathfrak{z}^l \tag{24}$$

in der Gleichung

$$\left\{\frac{\zeta}{\mathfrak{q}}\right\} = 1,$$

wobei $\mathfrak{q}$ ein Primidealteiler von $\mathfrak{a}$ ist.

Beweis. Die Gleichung (24) zerfällt in die Faktoren

$$\xi + \eta = \mathfrak{a}\mathfrak{i}_0^l$$

und

$$\xi + \eta \zeta^i = \varepsilon_i \varrho_i^l \quad (i = 1, 2, \ldots, l-1),$$

in welchen ε_i reelle Einheiten und $\mathfrak{i}_0$ ein reelles Ideal in $k(\zeta)$ sind. Aus diesen Gleichungen gewinnt man

$$\varrho_1^l + \zeta \varrho_{l-1}^l = \mathfrak{a}\mathfrak{i}_0^l. \tag{25}$$

Ist $\mathfrak{q}$ ein Primidealteiler von $\mathfrak{a}$, so liefert (25) die Kongruenz:

$$\zeta \equiv -\left(\frac{\varrho_1}{\varrho_{l-1}}\right)^l \pmod{\mathfrak{q}},$$

und dies den Potenzcharakter

$$\left\{\frac{\zeta}{\mathfrak{q}}\right\} = 1.$$

Satz 4. l sei eine reguläre Primzahl, $l>3$, $k(\zeta)$ der zugehörige Kreisteilungskörper, ξ, η seien reelle Zahlen, $\mathfrak{a}, \mathfrak{z}$ reelle Ideale des Körpers $k(\zeta)$. Weiter seien $\xi, \eta, \mathfrak{a}\mathfrak{z}$ teilerfremd, und das Ideal $\mathfrak{a}$ sei prim zu $\mathfrak{l}$ und enthalte höchstens $\frac{l-3}{2}$ verschiedene und nur reelle Primidealfaktoren, unter welchen für wenigstens einen Primidealfaktor $\mathfrak{q}$ der Potenzcharakter

$$\left\{\frac{\zeta}{\mathfrak{q}}\right\} \neq 1$$

gilt. Dann ist die Diophantische Gleichung

$$\xi^l + \eta^l = \mathfrak{a}\mathfrak{z}^l, \quad (\xi)(\eta)\mathfrak{z} \neq 1 \tag{26}$$

unmöglich.

Im Beweise unterscheiden wir drei Fälle.

Im Falle a) sind $\xi, \eta, \mathfrak{z}$ prim zu $\mathfrak{l}$, und der Beweis folgt aus Satz 1.

Im Falle b) ist eine der Zahlen ξ, η durch $\mathfrak{l}$ teilbar, und der Beweis folgt aus Satz 3.

Im Falle c) sei $\mathfrak{z}$ durch $\mathfrak{l}$ teilbar. Dann folgt der Beweis unmittelbar aus dem Lemma der unter [1a)] zitierten Arbeit von Maillet.

Satz 5. l sei eine reguläre Primzahl, $l>3$, $k(\zeta)$ der zugehörige Kreisteilungskörper, ξ, η seien reelle Zahlen, $\mathfrak{a}, \mathfrak{z}$ reelle Ideale des Körpers $k(\zeta)$. Weiter seien $\xi, \eta, \mathfrak{a}\mathfrak{z}$ teilerfremd, und das Ideal $\mathfrak{a}$ sei prim zu $\mathfrak{l}$ und zerfalle in zwei Primidealpotenzen, welche zueinander nach der Substitution $\zeta : \zeta^{-1}$ konjugiert sind und welche dem Potenzcharakter

$$\left\{\frac{\zeta}{\mathfrak{q}}\right\} \neq 1$$

genügen. Dann ist die Diophantische Gleichung (26) unmöglich.

Im Beweise werden dieselben 3 Fälle unterschieden, wie im Satz 4. Der Fall a) folgt aus Satz 2, Fall b) aus Satz 3 und der Fall c) aus dem Mailletschen Lemma.

In den weiteren Ausführungen beschränken wir uns auf ganze rationale Veränderliche.

Satz 6. l sei eine reguläre Primzahl, x, y, z, c seien rationale ganze Zahlen, x, y, cz seien teilerfremd, und unter den Zahlen x, y sei etwa y durch l teilbar. c besitze keinen Primteiler von der Form $kl+1$. Dann besteht eine notwendige Bedingung für die Lösbarkeit der Diophantischen Gleichung

$$x^l + y^l = cz^l \tag{27}$$

in der Beziehung

$$q^{l-1} \equiv 1 \pmod{l^2}, \tag{28}$$

wobei q ein Teiler von c ist.

Beweis. Da laut Voraussetzung c keinen Primidealteiler vom ersten Grade hat, lautet die Zerlegung von (27):

$$x + y = c a^l$$
$$x + y\zeta^i = \varepsilon_i \varrho_i^l \quad (i = 1, 2, \ldots, l-1),$$

wobei ε_i reelle Einheiten in $k(\zeta)$ sind. Aus diesen Gleichungen erhalten wir ähnlich wie im Satz 3 die Bedingung

$$\left\{\frac{\zeta}{\mathfrak{q}}\right\} = 1,$$

wobei $\mathfrak{q}$ ein Primidealteiler von c ist. Ist die Norm des Ideals $\mathfrak{q}$ gleich q^f, so entspricht dieser Potenzcharakter bekanntlich der Kongruenz (28).

Satz 7. l sei eine reguläre Primzahl, $l > 3$, c eine zu l prime rationale ganze Zahl von der Form

$$c = p_1^{u_1} \cdots p_s^{u_s},$$

wobei $p_1, \ldots, p_s$ Primzahlen sind, welche nach l zu den Exponenten $f_1, \ldots, f_s$ gehören. Sind $f_1, \ldots, f_s$ sämtlich gerade und

$$\sum_{i=1}^{s} \frac{1}{f_i} \leqq \frac{l-3}{2(l-1)}, \tag{29}$$

ist ferner für wenigstens einen Wert j unter den Zahlen $1, \ldots, s$

$$p_j^{l-1} \not\equiv 1 \pmod{l^2},$$

so ist die Diophantische Gleichung

$$x^l + y^l = cz^l; \quad xyz \neq 0, 1 \tag{30}$$

unlösbar in ganzen rationalen Zahlen x, y, z.

Der Beweis folgt aus dem Satz 4, dessen Voraussetzungen die obigen enthalten. Da die Exponenten $f_1, \ldots, f_s$ gerade sind, enthält c nur reelle Primidealfaktoren des

Körpers $k(\zeta)$. Die Primzahl p_i enthält $\frac{l-1}{f_i}$ verschiedene Primidealfaktoren in $k(\zeta)$[1]; c enthält also insgesamt

$$(l-1)\sum_{i=1}^{s}\frac{1}{f_i}$$

Primidealfaktoren, woraus ersichtlich ist, dass die Voraussetzungen der Sätze 4 und 7 gleichbedeutend sind.

Satz 8. l sei eine reguläre Primzahl, $l>3$, c sei eine Potenz der zu l primen rationalen Primzahl p, welche nach l zum Exponent $\frac{l-1}{2}$ gehört. Ist ferner

$$p^{l-1}\not\equiv 1 \pmod{l^2},$$

so ist die unbestimmte Gleichung (30) in ganzen rationalen Zahlen x, y, z unlösbar.

Der Beweis folgt aus Satz 5.

Nun gehen wir auf den speziellen Fall $c=2$ über und fassen die Ergebnisse der Sätze 7 und 8 für diesen Fall im folgenden Satz zusammen:

Satz 9. l sei eine reguläre Primzahl, und 2 gehöre nach l entweder zu einem geraden Exponenten oder zum Exponenten $\frac{l-1}{2}$. Ist ferner

$$2^{l-1}\not\equiv 1 \pmod{l^2},$$

so ist die Diophantische Gleichung

$$x^l+y^l=2z^l, \quad xyz\neq 0, 1 \tag{31}$$

in ganzen rationalen Zahlen x, y, z unlösbar.

Wir werden jetzt untersuchen, für welche Exponenten unter 619 der Satz 9 gilt. Nach Vandiver[2] kommen bis 619 die folgenden irregulären Primzalen vor:

37, 59, 67, 101, 103, 131, 149, 157, 233, 257, 263, 271, 283, 293, 307, 311, 347, 353, 379, 401, 409, 421, 433, 461, 463, 467, 491, 523, 541, 547, 557, 577, 587, 593, 607, 617.

Wir stellen in einer Tabelle die regulären Primzahlen bis 619 und die Exponenten, zu welchen 2 nach dem Modul l gehört, zusammen.

$l=$	7	11	13	17	19	23	29	31	41	43	47	53
$f_2=$	3	10	12	8	18	11	28	5	20	14	23	52

[1] E. Kummer: Journ. de Liouville, Bd. 16, 1851, S. 431 ff.

[2] H. S. Vandiver: American Math. Monthly, Bd. LIII, 1946, S. 571.

$l =$	61	71	73	79	83	89	97	107	109	113	127
$f_2 =$	60	35	9	39	82	11	48	106	36	28	7

$l =$	137	139	151	163	167	173	179	181	191	193
$f_2 =$	68	138	15	162	83	172	178	180	95	96

$l =$	197	199	211	223	227	229	239	241	251	269
$f_2 =$	196	99	210	37	226	76	119	24	50	268

$l =$	277	281	313	317	331	337	349	359	367	373
$f_2 =$	92	35	156	316	30	21	348	179	183	372

$l =$	383	389	397	419	431	439	443	449	457
$f_2 =$	191	388	44	418	43	73	442	224	76

$l =$	479	487	499	503	509	521	563	569	571
$f_2 =$	239	243	166	251	508	260	281	284	114

$l =$	599	601	613
$f_2 =$	299	25	612

Aus dieser Tabelle können wir entnehmen, dass unter den regulären Primzahlen kleiner als 619 der Satz 9 für die folgenden nicht gültig ist:

$$31,\quad 73,\quad 89,\quad 127,\quad 151,\quad 223,\quad 281,$$

da die zweite Voraussetzung des Satzes 9:

$$2^{p-1} \not\equiv 1 \pmod{p^2}$$

für alle Primzahlen p mit $p < 1093$ erfüllt ist.[1]

[1] N. G. W. H. Beeger: Nieuw Archief voor Wiskunde, 2, Bd. 20, 1939, S. 51—54.