

Czechoslovak Mathematical Journal

Peter Dénes

Über die Diophantische Gleichung $x^{np} + y^{np} = p^m \cdot z^{np}$

Czechoslovak Mathematical Journal, Vol. 1 (1951), No. 3, 179–185

Persistent URL: <http://dml.cz/dmlcz/100026>

Terms of use:

© Institute of Mathematics AS CR, 1951

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

ÜBER DIE DIOPHANTISCHE GLEICHUNG $x^{np} + y^{np} = p^m \cdot z^{np}$.

PETER DÉNES, Budapest.

(Eingegangen den 13. Jänner 1951.)

Es sei p eine Primzahl, $n > 0$ ganz, $0 < m \neq 3$ ganz; dann hat (1) keine Lösung in ganzen x, y, z , wenn p eine irreguläre Primzahl ist, die den unten angeführten Bedingungen I, II genügt.

In einer früherer Arbeit habe ich bewiesen,¹⁾ daß die Gleichung

$$x^{np} + y^{np} = p^m \cdot z^{np}, \quad xyz \neq 0, \tag{1}$$

in rationalen ganzen Zahlen x, y, z unlösbar ist, falls $p > 3$ eine reguläre Primzahl, m eine natürliche Zahl und n eine positive ganze Zahl ist. Auch gab ich meiner Vermutung Ausdruck, daß die Gleichung

$$x^t + y^t = t^m \cdot z^t, \quad xyz \neq 0, \tag{2}$$

wo t und m natürliche Zahlen sind, $t > 3$, wahrscheinlich keine ganzzahlige Lösung x, y, z besitzt.

In der vorliegenden Arbeit werden wir die Unlösbarkeit der Gleichung (1) in rationalen ganzen, nicht verschwindenden Zahlen für gewisse irreguläre Primzahlen beweisen.

p bezeichnet eine irreguläre Primzahl, $\zeta = e^{2\pi i/p}$, $k(\zeta)$ den Körper der p -ten Einheitswurzel, $k(\zeta + \zeta^{-1})$ den reellen Unterkörper von $k(\zeta)$. $\lambda = 1 - \zeta$, $\mathfrak{l} = [\lambda]$, $\mathfrak{A} = (1 - \zeta)(1 - \zeta^{-1})$, $\mathfrak{A} = [\mathfrak{A}]$. Die Primzahl p erfüllt die folgende Bedingungen:

I. Der zweite Faktor der Klassenzahl von $k(\zeta)$ ist prim zu p ;

II. Keine der Bernoullischen Zahlen B_{rp} $\left(r = 1, 2, \dots, \frac{p-3}{2}\right)$ ist durch p^3 teilbar.

Es gilt der folgende Satz:

Satz I. *Ist p eine irreguläre Primzahl, welche den Bedingungen I—II genügt und s eine natürliche Zahl, $s \geq \frac{3p-1}{2}$, so ist eine Gleichung*

$$\xi^p + \eta^p = E_0 \mathfrak{A}^s \psi^p \tag{3}$$

¹⁾ P. Dénes: Monatshefte f. Math. 54 (1950), 175—182.

wo E_0 eine Einheit, ξ, η, ψ nicht verschwindende, zu \mathfrak{k} prime Zahlen in $k(\zeta + \zeta^{-1})$ sind, unmöglich.

Beweis. Die Gleichung (3) kann bekanntlich in p Faktoren zerlegt werden:

$$\left. \begin{aligned} \xi + \eta &= \mathfrak{I}^{2s-p+1} \mathfrak{I} \mathfrak{I}_0^p \\ \xi + \eta \zeta^i &= \mathfrak{I} \mathfrak{I}_i^p \quad (i = 1, 2, \dots, p-1), \end{aligned} \right\} \quad (4)$$

wo \mathfrak{I} den größten gemeinsamen Idealteiler der Zahlen ξ, η , bedeutet und $\mathfrak{I}_0, \mathfrak{I}_1, \dots, \mathfrak{I}_{p-1}$ gewisse zu \mathfrak{I} prime Ideale in $k(\zeta)$ sind. Wegen (4) bestehen also die Kongruenzen

$$\frac{\xi + \eta \zeta^i}{1 - \zeta^i} \equiv -\eta \pmod{\mathfrak{I}^p} \quad (i = 1, 2, \dots, p-1). \quad (5)$$

Bedeutet i und k zwei Zahlen aus der Serie $1, 2, \dots, p-1$ und a eine natürliche Zahl, $a \leq p$, so ist

$$\left(\frac{\xi + \eta \zeta^i}{1 - \zeta^i} \right)^a \left(\frac{\xi + \eta \zeta^k}{1 - \zeta^k} \right)^{p-a} \equiv -\eta^p \equiv C \pmod{\mathfrak{I}^p}, \quad (6)$$

wo C eine rationale ganze Zahl ist. Aus (4) und (6) folgt, daß das Hauptideal

$$\mathfrak{I}_i^a \mathfrak{I}_k^{p-a} \mathfrak{I}^p \quad (i, k = 1, 2, \dots, p-1)$$

einer primären Zahl in $k(\zeta)$ gleich ist. Nach VANDIVER²⁾ ist ein Ideal von $k(\zeta)$, dessen p -te Potenz eine primäre Zahl ist, ein Hauptideal, falls der zweite Faktor der Klassenzahl von $k(\zeta)$ prim zu p ist (unsere Voraussetzung 1):

$$\mathfrak{I}_i^a \mathfrak{I}_k^{p-a} \mathfrak{I} \sim 1 \quad (i, k = 1, 2, \dots, p-1). \quad (7)$$

Laut den Gleichungen (4) gelten ausserdem

$$\mathfrak{I}_k^{p-1} \mathfrak{I} \sim \mathfrak{I}_k^{-1} \quad (k = 1, 2, \dots, p-1) \quad (8)$$

und wenn wir in (7) $a = 1$ setzen, wird aus (7) und (8)

$$\mathfrak{I}_i \sim \mathfrak{I}_k \quad (i, k = 1, 2, \dots, p-1). \quad (9)$$

Weiter ist

$$[\psi] = \mathfrak{I} \prod_{i=0}^{p-1} \mathfrak{I}_i \sim 1,$$

woraus wegen (9)

$$\mathfrak{I} \mathfrak{I}_0 \mathfrak{I}_k^{p-1} \sim 1$$

folgt, also ist wegen (8)

$$\mathfrak{I}_0 \sim \mathfrak{I}_k \quad (k = 1, 2, \dots, p-1). \quad (10)$$

²⁾ H. S. Vandiver: Transactions Amer. Math. Soc. **31** (1929), 613–642, Lemma 1.

Wird nun k von 0 , i und $p - i$ verschieden gewählt, so sind die Ideale

$$\frac{j_0}{j_k}, \frac{j_i}{j_k}, \frac{j_{p-i}}{j_k}.$$

Hauptideale und können durch Zahlen

$$\frac{\varrho_0}{\varrho_k}, \frac{\varrho_i}{\varrho_k}, \frac{\varrho_{p-i}}{\varrho_k}$$

des Körpers $k(\zeta)$ repräsentiert werden. Wir können aus (4) die folgenden Gleichungen

$$\frac{\xi + \eta}{\xi + \eta\zeta^k} = \beta_0 \lambda^{2s-p} \frac{\varrho_0^p}{\varrho_k^p}$$

$$\frac{\xi + \eta\zeta^i}{\xi + \eta\zeta^k} = \beta_i \frac{\varrho_i^p}{\varrho_k^p}$$

$$\frac{\xi + \eta\zeta^{-i}}{\xi + \eta\zeta^k} = \beta_{p-i} \frac{\varrho_{p-i}^p}{\varrho_k^p}$$

bilden, wo $\beta_0, \beta_i, \beta_{p-i}$ Einheiten in $k(\zeta)$ sind und aus welchen wir die Gleichung

$$\varrho_i^p - \vartheta_i \varrho_{p-i}^p = \vartheta_0 \lambda^{2s-p} \varrho_0^p \quad (11)$$

gewinnen können. Hier bezeichnen ϑ_0, ϑ_i reelle Einheiten in $k(\zeta)$ und aus der ersten Gleichung von (4) können wir auch folgern, daß ϱ_0 reell ist.

Wir bilden durch die Substitution $s = \zeta : \zeta^{-1}$ die konjugierte Gleichung von (11):

$$\vartheta_i \varrho_i^p - \varrho_{p-i}^p = \vartheta_0 \lambda^{2s-p} \varrho_0^p. \quad (12)$$

Dann ist es ersichtlich, daß nur $\vartheta_i = 1$ sein kann; es ist also:

$$\varrho_i^p - \varrho_{p-i}^p = \varepsilon_i' \lambda^{2s-p} \varrho_0^p \left(i = 1, 2, \dots, \frac{p-1}{2} \right), \quad (13)$$

in welchen ε_i' Einheiten von $k(\zeta)$ bedeuten.

Aus

$$\frac{j_i}{j_k} = \left[\frac{\varrho_i}{\varrho_k} \right] \quad (i, k = 0, 1, \dots, p-1)$$

folgt

$$[Q_i] = t j_i \quad (i = 0, 1, \dots, p-1), \quad (14)$$

wo t ein Ideal in $k(\zeta)$ ist. Wird in (14) $i = 0$ gesetzt, so ist es ersichtlich, daß t reell ist, weil ϱ_0 und j_0 ebenfalls reell sind. Die Gleichung (13) kann in die folgenden Faktoren zerlegt werden:

$$\left. \begin{aligned} \varrho_i - \varrho_{p-i} &= j^{2s-2p+1} \mathfrak{g}_{i0}^p \\ \varrho_i - \varrho_{p-i} \zeta^k &= \text{f. t. } \mathfrak{g}_{ik}^p \quad (k = 1, 2, \dots, p-1), \end{aligned} \right\} \quad (15)$$

in welchen $\mathfrak{g}_{i0}, \dots, \mathfrak{g}_{i,p-1}$ zu \mathfrak{f} prime Ideale in $k(\zeta)$ sind.

Das Hauptideal $[\varrho_i - \varrho_{p-i} \zeta^k]$ ($k = 0, 1, \dots, p-1$) bleibt bei der Anwendung der Substitution $s = \zeta : \zeta^{-1}$ unverändert, also gehören die Ideale $\mathfrak{g}_{i0}, \dots, \mathfrak{g}_{i,p-1}$ zum reellen Unterkörper $k(\zeta + \zeta^{-1})$. Aus (15) folgt ferner

$$\varrho_i - \varrho_{p-i} \equiv 0 \pmod{\mathfrak{f}^{2s-2p+1}} \quad \left(i = 1, 2, \dots, \frac{p-1}{2} \right) \quad (16)$$

und

$$\frac{\varrho_i - \varrho_{p-i} \zeta^k}{\varrho_j - \varrho_{p-j} \zeta^k} = \frac{\mathfrak{g}_{ik}^p}{\mathfrak{g}_{jk}^p} \quad \left(i, j = 1, 2, \dots, \frac{p-1}{2}, i \neq j \right).$$

Da das Ideal $\frac{\mathfrak{g}_{ik}}{\mathfrak{g}_{jk}}$ reell und seine p -te Potenz Hauptideal ist, ist es wegen der Voraussetzung I. auch selbst ein Hauptideal:

$$\frac{\mathfrak{g}_{ik}}{\mathfrak{g}_{jk}} = \left[\frac{\gamma_{ik}}{\gamma_{jk}} \right] \quad \left(k = 1, 2, \dots, p-1 \right)$$

$$\left(i, j = 1, 2, \dots, \frac{p-1}{2}, i \neq j \right).$$

Hiedurch wird für $k = 1$

$$\frac{\varrho_i - \varrho_{p-i} \zeta}{\varrho_j - \varrho_{p-j} \zeta} = \delta_{ij} \frac{\gamma_i^p}{\gamma_j^p},$$

δ_{ij} eine Einheit in $k(\zeta)$, woraus wegen (16)

$$\frac{\varrho_i}{\varrho_j} \equiv \frac{\varrho_{p-i}}{\varrho_{p-j}} \equiv \delta_{ij} \frac{\gamma_i^p}{\gamma_j^p} \pmod{\mathfrak{f}^{2s-2p}},$$

beziehungsweise

$$\frac{\sigma_i}{\sigma_j} = \frac{\varrho_i \varrho_{p-i}}{\varrho_j \varrho_{p-j}} \equiv \frac{\delta_i^* \gamma_i^{2p}}{\delta_j^* \gamma_j^{2p}} \pmod{\mathfrak{f}^{2s-2p}} \quad \left(i, j = 1, 2, \dots, \frac{p-1}{2}, i \neq j \right) \quad (17)$$

folgt, wo δ_i^*, δ_j^* Einheiten des Körpers $k(\zeta)$ sind.

Es sollen nun aus den Gleichungen (4) die folgenden reellen Gleichungen gebildet werden:

$$\left. \begin{aligned} (\xi + \eta)^2 &= \mathfrak{f}^{2s-p+1} \mathfrak{f}_0^{2p} \\ (\xi + \eta \zeta^i) (\xi + \eta \zeta^{-i}) &= \mathfrak{f} \mathfrak{f}_i^{2p} \mathfrak{f}_{p-i}^{2p} \quad \left(i = 1, 2, \dots, \frac{p-1}{2} \right). \end{aligned} \right\} \quad (18)$$

Wird k von 0, i und $p - i$ verschieden gewählt, so sind laut (9) und (10) die Ideale

$$\frac{\mathfrak{I}_0^2}{\mathfrak{I}_1 \mathfrak{I}_{p-k}}, \frac{\mathfrak{I}_i \mathfrak{I}_{p-i}}{\mathfrak{I}_k \mathfrak{I}_{p-k}}, \left(i = 1, 2, \dots, \frac{p-1}{2} \right) i \neq k,$$

Hauptideale und können der Bezeichnung (17) nach durch die Zahlen

$$\left[\frac{\varrho_0^2}{\sigma_k} \right], \left[\frac{\sigma_i}{\sigma_k} \right] \left(i = 1, 2, \dots, \frac{p-1}{2} \right) i \neq k$$

ersetzt werden. Damit erhalten wir aus (18)

$$\left. \begin{aligned} \frac{\xi^2 + 2\xi\eta + \eta^2}{\xi^2 + \xi\eta(\zeta^k + \zeta^{-k}) + \eta^2} &= H_0 A^{2s-p} \frac{\sigma_0^2}{\sigma_k^2} \\ \frac{\xi^2 + \xi\eta(\zeta^i + \zeta^{-i}) + \eta^2}{\xi^2 + \xi\eta(\zeta^k + \zeta^{-k}) + \eta^2} &= H_i \frac{\sigma_i^2}{\sigma_k^2} \left(i = 1, 2, \dots, \frac{p-1}{2} \right) i \neq k, \end{aligned} \right\} \quad (19)$$

wo $H_0, H_1, \dots, H_{\frac{p-1}{2}}$ Einheiten in $k(\zeta + \zeta^{-1})$ sind. Eliminieren wir die Zahlen $\xi^2 + \eta^2$ und $\xi\eta$ aus den ersten drei Gleichungen der Schar (19), so bekommen wir

$$\sigma_1^2 + e_2 \sigma_2^2 = e_0 A^{s'} \sigma_0^2. \quad (20)$$

In (20) sind e_0, e_2 Einheiten, $\sigma_0, \sigma_1, \sigma_2$ Zahlen des Körpers $k(\zeta + \zeta^{-1})$ und

$$\begin{aligned} \sigma_0 &= \varrho_0^2, \\ s' &= 2s - p > 2p. \end{aligned} \quad (21)$$

Nach (20) und (21) ist

$$e_2 \equiv - \frac{\sigma_1^2}{\sigma_2^2} \pmod{\mathfrak{I}^{2s-p}}.$$

Andererseits gilt zufolge (17)

$$\frac{\sigma_1^2}{\sigma_2^2} \equiv \frac{\delta_1^{*p}}{\delta_2^{*p}} \cdot \frac{\gamma_1^{2p^2}}{\gamma_2^{2p^2}} \pmod{\mathfrak{I}^{2s-p+1}},$$

woraus sich wegen unserer Voraussetzung $p \geq \frac{3p-1}{2}$

$$e_2 \equiv - \frac{\delta_1^{*p}}{\delta_2^{*p}} \cdot C^p \pmod{\mathfrak{I}^{2p-2}}$$

ergibt, wo C eine rationale ganze Zahl ist. Die Einheit

$$e_2 \frac{\delta_2^{*p}}{\delta_1^{*p}}$$

ist also nach einem Satze von VANDIVER³⁾ die p -te Potenz einer Einheit in $k(\zeta)$, und so ist e_2 selbst eine volle p -te Potenz in $k(\zeta)$. Hierdurch wird (20)

$$\sigma_1^p + \sigma_2'^p = e_0 A^{s'} \sigma_0^p, \quad (22)$$

welcher Ausdruck dieselbe Form hat, wie die Gleichung (3). Wegen (21) erfüllt auch die Zahl s' die Voraussetzung $s' > \frac{3p-1}{2}$. Die Zahlen $\sigma_0, \sigma_1, \sigma_2$ sind numerische Faktoren der Zahl ψ und dementsprechend sind ihre Normen kleiner als $N(\psi)$. Die Fortsetzung der angewendeten Methode muss also entweder zu einem Widerspruch, oder zu einer Gleichung

$$\omega_1^p + \omega_2^p = \Theta A^t \omega_0^p \quad (23)$$

führen, $t > \frac{3p-1}{2}$, in welcher $\Theta, \omega_0, \omega_1, \omega_2$ alle Einheiten des Körpers $k(\zeta + \zeta^{-1})$ sind. In diesem Falle ist

$$\omega_1 + \omega_2 \zeta = \lambda \zeta^b \Theta_1,$$

wo Θ_1 eine Einheit in $k(\zeta + \zeta^{-1})$ und b eine rationale ganze Zahl ist. Die durch die Substitution $s = \zeta : \zeta^{-1}$ entspringende konjugierte Gleichung lautet:

$$\omega_1 + \omega_2 \zeta^{-1} = -\lambda \zeta^{-b-1} \Theta_1.$$

Aus diesen beiden Gleichungen erhält man

$$(\omega_1 + \omega_2)(1 + \zeta) = \lambda(\zeta^b - \zeta^{-b}) \Theta_1,$$

woraus, da

$$\omega_1 + \omega_2 \equiv 0 \pmod{f^p}$$

ist, sich

$$\zeta^b - \zeta^{-b} \equiv 0 \pmod{f^p}$$

ergibt, was aber unmöglich ist. Damit ist Satz 1 bewisen.

Satz 2. Sind p eine irreguläre Primzahl, welche den Bedingungen I–II genügt, n eine positive ganze Zahl, m eine natürliche Zahl, $m \neq 3$, so ist die Gleichung

$$x^{np} + y^{np} = p^m \cdot z^{np}, \quad xyz \neq 0 \quad (1)$$

in rationalen ganzen Zahlen x, y, z unlösbar.

Beweis. Die Gleichung (1) kann auf die Form

$$X^p + Y^p = p^m \cdot Z^p \quad (24)$$

gebracht werden. Ist $m = 0$, so bedeutet (24) den ersten Fall des letzten

³⁾ H. S. Vandiver, loc. cit., Lemma 2. Vandiver wendet in der Kongruenz des Lemmas den Modul f^{2p} an; im Beweise des Lemmas (s. Gleichung 3a) ist aber nur die Erfüllung der Kongruenz nach dem Modul f^{2p-2} erforderlich.

Fermatschen Satzes, welchen für Primzahlen p , die die Voraussetzung I. erfüllen, VANDIVER⁴⁾ bewies.

Ist $m = 1$, so lautet die Gleichung (3)

$$\xi^p + \eta^p = E_0 A^{\frac{p-1}{2}} \psi^p,$$

welche jedoch offensichtlich unmöglich ist, da ξ, η reelle Zahlen bedeuten, also

$$\xi^p \equiv a \pmod{\mathfrak{k}^{\frac{p+1}{2}}}$$

$$\eta^p \equiv b \pmod{\mathfrak{k}^{\frac{p+1}{2}}}$$

gelten, wo a, b rationale ganze Zahlen sind. Besteht also

$$\xi^p + \eta^p \equiv 0 \pmod{\mathfrak{k}^{\frac{p-1}{2}}},$$

so muss auch

$$\xi^p + \eta^p \equiv 0 \pmod{\mathfrak{k}^{\frac{p+1}{2}}}$$

erfüllt sein.

Wenn $m = 2$ ist, dann hat die Gleichung (13) die Form

$$\varrho_i^p - \varrho_{p-i}^p = \varepsilon'_i \lambda^{p-2} \varrho_0^p. \quad (25)$$

Auch diese Gleichung ist unmöglich, da ϱ_i und ϱ_{p-i} durch Multiplikation mit einer Einheitswurzel semiprimär gemacht werden können und deswegen

$$\varrho_i^p - \varrho_{p-i}^p \equiv 0 \pmod{\mathfrak{p}}$$

ist. (25) könnte also nur bestehen, wenn ϱ_0 gegen Annahme durch \mathfrak{f} teilbar wäre.

Ist endlich $m > 3$, so folgt der Beweis unmittelbar aus Satz 1.

⁴⁾ H. S. Vandiver: Bull. Amer. Math. Soc. **40** (1934), 118—126.