Über die diophantische Gleichung $x^p + y^p = cz^p$

Von KÁLMÁN GYŐRY (Debrecen)

1. Für den Fall einer regulären Primzahl p haben E. MAILLET [1], H. S. VANDIVER [2], P. DÉNES [3] und andere Resultate bezüglich der diophantishe Gleichung

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

erhalten, wo x, y, z von Null verschiedene und c gewisse Bedingungen erfüllende ganze rationale Zahlen sind.

Wenn $c = 1$ ist, ist insbesondere (1) die Fermatsche Gleichung.

Im Weiteren seien $p > 3$ eine beliebige Primzahl, und c eine ganze rationale Zahl, für welche $(\varphi(c), p) = 1$ gilt, wo $\varphi(c)$ die Eulersche Funktion ist. Wir können gleichzeitig voraussetzen, daß in (1) x, y und z paarweise relativ prim sind.

Bei der Untersuchung der Gleichung (1) werden wir die folgenden drei Fälle unterscheiden:

I. Fall: x, y und z sind zu p relativ prim,

II. Fall: x oder y ist durch p teilbar,

III. Fall: z ist durch p teilbar.

Wir werden jetzt kurz die bisherigen, sich auf die Fälle I. und II. beziehenden Resultate zusammenfassen. Aus den Ergebnissen von S. LUBELSKI erhalten wir mittels entsprechender Modifizierung der Bezeichnungen die folgenden Sätze ([4] Satz 1. und Satz 2., oder [5]).

Satz A. *Es seien $p > 3$ eine beliebige Primzahl, und c eine ganze Zahl, für welche $(\varphi(c), p) = 1$ gilt. Wenn die Gleichung* (1) *eine ganzzahlige Lösung besitzt, und $p \nmid xz$ ist, dann gilt für eine beliebige ganze Zahl $r \mid x$*

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

Satz B. *Es sei c eine ganze Zahl, für welche $(\varphi(c), p) = 1$ und $c^{p-1} \not\equiv 2^{p-1} \pmod{p^2}$ gilt. Wenn die Gleichung* (1) *eine ganzzahlige Lösung hat und $p \nmid z$ ist, dann gilt für eine beliebige ganze Zahl $r \mid (x - y)$*

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

Der folgende Satz stammt auch von S. LUBELSKI ([4], Satz 6.):

Satz C. *Es sei c eine ganze Zahl, für welche $(\varphi(c), p)=1$ und $c^{p-1}\not\equiv 2^{p-1} \pmod{p^2}$ gilt. Wenn die Gleichung* (1) *eine ganzzahlige Lösung hat und $p\nmid z$ ist, dann gilt*

$$c^{p-1}\equiv 1 \pmod{p^2}.$$

Im Zusammenhang mit den Sätzen A. und B. haben T. MORISHIMA und T. MIYOSHI Folgendes gezeigt [5]:

Satz D. *Es sei c eine ganze Zahl, für welche $(\varphi(c), p)=1$ und $c^{p-1}\not\equiv 2^{p-1} \pmod{p^2}$ gilt. Wenn die Gleichung* (1) *eine ganzzahlige Lösung besitzt, und $p\nmid xyz$ ist, dann gilt für eine beliebige ganze Zahl $r\mid(x+y)$*

$$r^{p-1}\equiv 1 \pmod{p^2}.$$

Wir bemerken schließlich, daß S. LUBELSKI ([4], Sätze 3. und 8.), T. MORISHIMA und T. MIYOSHI [5] das folgende Resultat erhalten haben:

Satz E. *Es sei c eine ganze Zahl, für welche $(\varphi(c), p)=1$ und $c^{p-1}\not\equiv 2^{p-1} \pmod{p^2}$ gilt. Wenn die Gleichung* (1) *eine durch p nicht teilbare, ganzzahlige Lösung besitzt, dann gilt*

$$2^{p-1}\equiv 1 \quad \text{und} \quad 3^{p-1}\equiv 1 \pmod{p^2}.$$

2. Es sei $p>3$ eine beliebige Primzahl. Wir setzen voraus, daß die Gleichung

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

eine paarweise relativ prime, ganze rationale Lösung x, y, z hat, wo c eine ganze rationale Zahl ist, welche nicht die p-te Potenz einer ganzen rationalen Zahl ist, und welche nicht durch eine Primzahl der Form $pt+1$ teilbar ist, d. h. $(\varphi(c), p)=1$.

Wir zeigen, daß Satz D. auch im Falle II. gilt, und damit geben wir eine Verallgemeinerung des Satzes C. Andererseits werden wir beweisen, daß der Satz A. auch im Falle III. gilt.

Der Kreisteilungskörper $K(\zeta)$ sei durch $\zeta=e^{\frac{2\pi i}{p}}$ definiert, und es sei $\lambda=1-\zeta$. Wir betrachten den durch die Gleichungen

$$\left(\frac{\alpha}{\mathfrak{t}}\right)=\zeta^k, \quad \alpha^{\frac{N(\mathfrak{t})-1}{p}}\equiv\left(\frac{\alpha}{\mathfrak{t}}\right) \pmod{\mathfrak{t}}$$

definierten p-ten Potenzcharakter, wo α eine ganze Zahl, $\mathfrak{t}$ ein Primideal in $K(\zeta)$, $(\mathfrak{t}, \alpha p)=1$, und $N(\mathfrak{t})=t^f$ der Norm von $\mathfrak{t}$ ist. Ferner sei, wenn die kanonische Form des Ideals $\mathfrak{a}$ $\mathfrak{a}=\prod_{\mathfrak{t}}\mathfrak{t}$ ist, wo $\mathfrak{a}$ zu p und zu α relativ prim ist, die folgende Gleichung gültig:

$$\left(\frac{\alpha}{\mathfrak{a}}\right)=\prod_{\mathfrak{t}}\left(\frac{\alpha}{\mathfrak{t}}\right).$$

Wie üblich, werden wir die ganze Zahl $\alpha\in K(\zeta)$ primär nennen, wenn $\lambda\nmid\alpha$ und $\alpha\equiv a \pmod{\lambda^2}$ ist, wo a eine ganze rationale Zahl ist. Ist nun $r\neq p$ eine Primzahl, α primär und zu r relativ prim, so gilt nach dem Reziprozitätssatz von Eisenstein [6] die Gleichung

$$\left(\frac{\alpha}{r}\right)\left(\frac{r}{\alpha}\right)^{-1}=1.$$

Mit Hilfe dieser Ergebnisse werden wir den folgenden Satz beweisen:

Satz 1. *Es sei $p>3$ eine beliebige Primzahl, und c eine ganze rationale Zahl, für welche $(\varphi(c), p)=1$ und $c^{p-1} \not\equiv 2^{p-1} \pmod{p^2}$ gilt. Dann hat die Gleichung*

$$x^p + y^p = cz^p;\ p \nmid z \tag{1''}$$

nur dann eine paarweise relativ prime ganze rationale Lösung, wenn für eine beliebige ganze Zahl $r|c$

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

gilt.

Zuerst werden wir das folgende Lemma beweisen:

Lemma. *Sind $p>3$ und $r \neq p$ beliebige Primzahlen, und x, y und z ganze rationale Zahlen, für welche*

$$\frac{x^p+y^p}{x+y} = z^p, \quad (x, y) = 1, \quad (x^2-y^2, p) = 1 \quad \text{und} \quad r|(x+y) \tag{2}$$

ist, dann gilt

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

Beweis. Wir können $(r, z)=1$ voraussetzen. Sonst ist nämlich

$$z^p = \frac{x^p+y^p}{x+y} = \frac{[(x+y)-y]^p+y^p}{x+y} = (x+y)^{p-1} - p(x+y)^{p-2}y + \ldots + py^{p-1}$$

und wegen $(x, y)=1$ folgt $r|p$, was nicht möglich ist. Andererseits ist offenbar $p \nmid z$. Dann kann man aber (2) in folgender Form schreiben:

$$\prod_{m=1}^{p-1} (x+\zeta^m y) = z^p$$

wo die Ideale $[x+\zeta^m y]$ $(m=1, 2, \ldots, p-1)$ paarweise relativ prim und p-te Potenzen von Idealen in $K(\zeta)$ sind. Ähnliches können wir vom Ideal $[\zeta^y x+\zeta^{-x} y]$ sagen, wo $\zeta^y x+\zeta^{-x} y$ primär ist. Somit gilt, nach dem Reziprozitätssatz von Eisenstein

$$1 = \left(\frac{\zeta^y x+\zeta^{-x} y}{r}\right) = \left(\frac{\zeta^y x-\zeta^{-x} x}{r}\right) = \left(\frac{\zeta^y-\zeta^{-x}}{r}\right) = \left(\frac{\zeta}{r}\right)^{-x}\left(\frac{1-\zeta^{x+y}}{r}\right).$$

Durch Quadrieren beider Seiten erhalten wir:

$$1 = \left(\frac{\zeta}{r}\right)^{-2x}\left(\frac{1-2\zeta^{x+y}+\zeta^{2(x+y)}}{r}\right) = \left(\frac{\zeta}{r}\right)^{-2x}\left(\frac{\zeta}{r}\right)^{x+y}\left(\frac{\zeta^{-(x+y)}-2+\zeta^{x+y}}{r}\right) = \left(\frac{\zeta}{r}\right)^{y-x},$$

weil $\zeta^{-(x+y)}-2+\zeta^{x+y}$ reell ist. Daraus folgt $\left(\frac{\zeta}{r}\right)=1$, also ist tatsächlich

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

BEWEIS DES SATZES 1. Da laut Voraussetzung c durch p nicht teilbar ist und keine Teiler der Form $pt+1$ hat, folgen aus (1″) die Gleichungen

$$x+y = cu^p, \quad \frac{x^p+y^p}{x+y} = v^p.$$

Weiterhin ist wegen $c^{p-1} \not\equiv 2^{p-1} \pmod{p^2}$ und $p \nmid z$, $(x^2-y^2, p)=1$. Wenn also $r|c$ ist, dann gilt auch $r|(x+y)$, und damit haben wir nach dem Lemma unsere Behauptung bewiesen.

Bemerkung. Damit haben wir den Satz D. von T. Morishima und T. Miyoshi auch im Falle II. bewiesen, und gleichzeitig haben wir den Satz C, welcher von *S.* Lubelski stammt, verallgemeinert.

Schließlich werden wir zeigen, daß der Satz A. auch im Falle III. gilt.

Satz 2. *Es sei $p>3$ eine beliebige Primzahl, und c eine ganze rationale Zahl, welche keinen Primteiler der Form $pt+1$ hat. Wenn die Gleichung* (1′) *eine paarweise relativ prime ganze rationale Lösung hat, und $p \nmid x$ ist, dann gilt für eine beliebige ganze Zahl $r|x$*

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

Lemma. *Ist $p>3$ eine Primzahl, sind ferner x, y, z und r ganze rationale Zahlen, und gilt*

$$\frac{x^p+y^p}{x+y} = pz^p, \quad (x, y) = 1 \quad \textit{und} \quad r|x, \tag{3}$$

dann ist

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

BEWEIS. Aus (3) folgt $p^2 \nmid \frac{x^p+y^p}{x+y}$, d. h. $p \nmid z$. Dann ergibt sich aber aus (3)

$$[x+\zeta^m y] = [\lambda]\mathfrak{a}_m^p \qquad (m=1, 2, \ldots, p-1), \tag{4}$$

wo $\mathfrak{a}_m^p$ ein Ideal in $K(\zeta)$ ist. Aus (3) folgt auch $p|(x+y)$, und so erhalten wir mit den Bezeichnungen $x+y=pu$ und

$$p = (1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{p-1}) = \lambda^{p-1}\varepsilon$$

wo ε eine Einheit ist, im Falle $m=2$ die Beziehung

$$x+\zeta^2 y = \zeta^2(x+y)+x(1-\zeta^2) = \zeta^2\lambda^{p-1}\varepsilon u + x(1-\zeta^2) =$$

$$= \lambda\left(\zeta^2\lambda^{p-2}\varepsilon u + x(1+\zeta)\right).$$

Aus (4) folgt somit

$$[\zeta^2\lambda^{p-2}\varepsilon u + x(1+\zeta)] = \mathfrak{a}_2^p,$$

d. h.

$$[\zeta^{\frac{p+3}{2}}\lambda^{p-2}\varepsilon u + x(\zeta^{\frac{p-1}{2}} + \zeta^{\frac{p+1}{2}})] = \mathfrak{a}_2^p,$$

wo im Falle $p>3$

$$\alpha = \zeta^{\frac{p+3}{2}} \lambda^{p-2} \varepsilon u + x(\zeta^{\frac{p-1}{2}} + \zeta^{\frac{p+1}{2}})$$

primär ist. Deshalb ist für eine beliebige Primzahl $r \neq p$ und $r \nmid z$, $\left(\frac{\alpha}{r}\right) = 1$. Es gilt also

$$\left(\frac{x+\zeta^2 y}{r}\right) = \left(\frac{\zeta^2 \lambda^{p-1} \varepsilon u + x(1-\zeta^2)}{r}\right) = \left(\frac{\lambda}{r}\right)\left(\frac{\zeta}{r}\right)^{\frac{p+1}{2}}\left(\frac{\alpha}{r}\right) =$$

$$= \left(\frac{\lambda}{r}\right)\left(\frac{\zeta}{r}\right)^{\frac{p+1}{2}} = \left(\frac{\zeta}{r}\right).$$

Wenn nun $r|x$ gilt, dann ist $\left(\frac{\zeta}{r}\right) = 1$, d. h. es folgt in der Tat

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

Beweis des Satzes 2. Nach Satz 1. dürfen wir uns auf den Fall beschränken, wo $p|z$, oder $p|c$ gilt. Da c keinen Primteiler der Form $pt+1$ hat, erhalten wir aus der Gleichung (1′) die Gleichungen

$$x+y = c' p^k u^p, \quad \frac{x^p+y^p}{x+y} = pv^p,$$

wo $c'|c$ gilt. Unsere Behauptung folgt nun auf Grund des Lemmas.

Literatur

[1] E. Maillet, Sur les équations indéterminées de la forme $x^\lambda+y^\lambda = cz^\lambda$, *Acta Math.* **24** (1901), 247—256.

[2] H. S. Vandiver, On trinomial diophantine equations connected with the Fermat relation, *Monatsh. Math. Phys.* **43** (1936), 317—320.

[3] P. Dénes, Über die diophantische Gleichung $x^l+y^l = cz^l$, *Acta Math.* **88** (1952), 241—251.

[4] S. Lubelski, Studien über den großen Fermatschen Satz, *Prace Matematyczne-Fiz.* **42** (1935), 11—44.

[5] T. Morishima—T. Miyoshi, On the diophantine equation $x^p+y^p = cz^p$, *Proc. Amer. Math. Soc.* **16** (1965), 833—836.

[6] E. Landau, Vorlesungen über Zahlentheorie, *Leipzig*, 1927. Band 3. 277—311.

(Eingegangen am 11. Dezember 1965.)