ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

334

ÜBER DIE LÖSBARKEIT EINIGER DIOPHANTISCHER GLEICHUNGEN

VON

K. INKERI

HELSINKI 1963
SUOMALAINEN TIEDEAKATEMIA

https://doi.org/10.5186/aasfm.1963.334

Vorgelegt am 10. März 1963.

KESKUSKIRJAPAINO
HELSINKI 1963

Über die Lösbarkeit einiger Diophantischer Gleichungen

1. In einer früheren Arbeit [3] haben wir einige notwendige Lösbarkeitsbedingungen für die diophantische Gleichung

$$x^{l^n} + y^{l^n} + z^{l^n} = 0 \tag{1}$$

bewiesen, wo l eine ungerade Primzahl und n eine natürliche Zahl ist. Insbesondere wurde in [3] gezeigt, dass (1) in ganzen zu l primen Zahlen unmöglich ist, wenn

$$n > \frac{\sqrt{l}}{\log l} \tag{1}'$$

ist. Im folgenden werden wir die allgemeineren Gleichungen

$$x^l + y^l = cz^{l^n} \tag{2}$$

und

$$c_1x^{l^n} + c_1y^{l^n} = c_2z^{l^n} \tag{3}$$

untersuchen und einige Ergebnisse von [3] für diese Fälle verallgemeinern und erweitern. Hier bedeuten c_1 und c_2 natürliche Zahlen und c eine rationale Zahl. Ohne Beschränkung der Allgemeinheit kann man annehmen, dass c_1 und c_2 teilerfremd sind.

Früher haben LUBELSKI [5], MAILLET [6], [7], VANDIVER [13] und DÉNES [1] die Gleichung (2) im Fall $n = 1$ untersucht. In den drei letztgenannten Arbeiten hat man sich auf die regulären Primzahlen l beschränkt. Die Mehrzahl der folgenden Ergebnisse betreffend (2) und (3) schliessen sich als Verallgemeinerungen und Erweiterungen nahe an einige Resultate der genannten Untersuchungen, namentlich [5]. Entsprechend dem zuerst erwähnten Ergebnis (vgl. (1)') erhalten wir, dass (3) mit $l \nmid z$ unmöglich in ganzen Zahlen x, y, z ist, falls

$$n > \frac{(l-1)\log c}{\log l} \quad (c = \max(c_1, c_2) > 1)$$

ist und der Fall $c_1 = 1, c_2 = 2$ ausgeschlossen wird.

Zum Schluss betrachten wir einige Anwendungen. Besonders wird ein neuer, kurzer Beweis für folgendes das bekannte Catalansche Problem betreffende Ergebnis von OBLÁTH [10] dargestellt:

Gibt es ganze rationale Zahlen x, y, die der Gleichung

$$x^2 - 1 = y^l \ (x > 3)$$

genügen, so ist

$$2^{l-1} \equiv 1 \ , \ 3^{l-1} \equiv 1 \ (\mathrm{mod}\ l^2).$$

2. Im folgenden bedeutet l eine ungerade Primzahl, n eine natürliche Zahl, r eine primitive Wurzel $(\mathrm{mod}\ l)$, ζ eine primitive l^{te} Einheitswurzel und $K(\zeta)$ den von ζ erzeugten Kreiskörper. Wir brauchen zwei Hilfssätze, die in [3], S. 12—13 bewiesen worden sind.

Hilfssatz 1. Ist α eine semiprimäre ganze Zahl von $K(\zeta)$ und ist

$$(\alpha) = \mathfrak{a}^{l^n},$$

wo die Primfaktoren des Ideals $\mathfrak{a}$ von $K(\zeta)$ Primideale ersten Grades sind, so ist

$$\alpha^{Q(S)} = \beta^{l^n} .$$

Hierin ist β eine Zahl von $K(\zeta)$ und der symbolische Exponent

$$Q(S) = (1 - S^{\frac{l-1}{2}}) \sum_{j=0}^{l-2} r_j S^j \ , \tag{4}$$

wo S die Substitution $(\zeta : \zeta^r)$ bedeutet und die ganzen rationalen Koeffizienten r_j durch die Bedingungen

$$r_j r^j \equiv 1 \ (\mathrm{mod}\ l) \ , \ 1 \leqq r_j \leqq l - 1 \ (j = 0 \ , 1 \ , \ldots \ , l - 2) \tag{5}$$

definiert sind.

Hilfssatz 2. Es sei p eine von l verschiedene Primzahl und δ eine ganze oder gebrochene (zu p prime) Zahl in $K(\zeta)$. Ist dann

$$\delta^{l^n} \equiv \zeta^t \ (\mathrm{mod}\ p) \ , \tag{6}$$

wo t eine zu l prime ganze Zahl bezeichnet, so gilt die Kongruenz

$$p^{l-1} \equiv 1 \ (\mathrm{mod}\ l^{n+1}) \ . \tag{7}$$

Es sei erwähnt, dass man hier ohne Beschränkung der Allgemeinheit die Zahl t gleich 1 annehmen kann.

3. Folgende zwei Sätze geben Kriterien, die Verallgemeinerungen der bekannten Furtwänglerschen Kriterien betreffend die Fermatsche Vermutung sind. Diese Sätze nebst den späteren Sätzen 3, 5 und 6 enthalten

als Spezialfälle einige Hauptresultate von Lubelski (vgl. [5], Einführung und Sätze 1, 2, 3).

Satz 1. *Befriedigen die ganzen rationalen Zahlen* u, v, w *die Bedingungen*

$$u^{l-1} - u^{l-2}v + \ldots + v^{l-1} = \frac{u^l + v^l}{u+v} = w^{l^n}, \quad (u, v) = 1, \tag{8}$$

so besteht für eine Primzahl p *die Kongruenz* (7) *in folgenden Fällen:*

a) p/u, $l \nmid u$;
b) $p/u^2 - v^2$, $l \nmid u - v$.

Beweis. Der Fall $u + v = 0$ (d.h. $u = -v = \pm 1$) kommt offenbar nicht in Frage. Weil bekanntlich $l^2 \nmid \dfrac{u^l + v^l}{u+v}$, sieht man unmittelbar, dass $l \nmid w$ und $l \nmid u + v$ bestehen. Wäre nämlich $l/u + v$, so wäre auch $l \mid \dfrac{u^l + v^l}{u+v}$ und dann l/w.

Die rationalen Primteiler des Ausdrucks der linken Seite der Gleichung (8) haben die Form $kl + 1$ und daher sind ihre Primteiler in $K(\zeta)$ ersten Grades. Die Ideale $v + \zeta^i u$ $(i = 1, 2, \ldots, l-1)$, die Teiler dieses Ausdrucks, sind paarweise teilerfremd. Bezeichnen wir

$$\alpha = \zeta^{-u(u+v)^{-1}}(v + \zeta u),$$

wo $(u+v)^{-1}$ eine Lösung der Kongruenz $(u+v)x \equiv 1 \pmod{l}$ bedeutet, so ist α eine semiprimäre ganze Zahl in $K(\zeta)$, und es gilt

$$(\alpha) = \mathfrak{a}^{l^n},$$

wo $\mathfrak{a}$ ein solches Ideal von $K(\zeta)$ ist, dessen Primidealteiler ersten Grades sind. Auf Grund von Hilfssatz 1 folgt aus dieser Gleichung, dass

$$\alpha^{Q(S)} = \beta^{l^n} \tag{9}$$

ist, wo β eine Zahl von $K(\zeta)$ ist und $Q(S)$ das symbolische Polynom (4) bedeutet.

Leicht sieht man, dass $\zeta^{Q(S)} = \zeta^{-2}$ ist. Aus (9) folgt nun die Bedingung

$$(v + \zeta u)^{Q(S)} \zeta^{2u(u+v)^{-1}} = \beta^{l^n}. \tag{10}$$

Ist p/u, ergibt sich hieraus die Kongruenz

$$\beta^{l^n} \equiv \zeta^{2u(u+v)^{-1}} \pmod{p}.$$

Weil der Exponent von der Zahl ζ im Falle a) zu l prim ist, erhalten wir unter Benutzung von Hilfssatz 2 aus dieser Kongruenz die Bedingung (7).

Aus Symmetriegründen ist

$$(10)' \qquad (u + \zeta v)^{Q(S)} \zeta^{2v(u+v)^{-1}} = \gamma^{l^n} .$$

Um den Satz im Falle b) zu beweisen, dividieren wir die Gleichungen (10) und (10)′ durcheinander und benutzen die Annahme $u \equiv \pm v \pmod{p}$. Dann ergibt sich die Kongruenz

$$\delta^{l^n} \equiv \zeta^{2(u-v)\,(u+v)^{-1}} \pmod{p} ,$$

wo die Zahl δ zum Körper $K(\zeta)$ gehört und der Exponent von ζ zu l prim ist. Unter Benutzung von Hilfssatz 2) folgt hieraus die Richtigkeit der Kongruenz (7). Damit ist unser Satz vollständig bewiesen.

Satz 2. *Ist* $l > 3$ *und erfüllen die ganzen rationalen Zahlen* u, v, w *die Bedingungen*

$$(8)' \qquad \frac{u^l + v^l}{u + v} = l w^{l^n} , \; (u , v) = 1 ,$$

so besteht für jeden Primteiler p *von* uv *die Kongruenz* (7). *Dieses gilt auch für* $l = 3$, *falls* $l^2/u + v$ *ist.*

Beweis. Wir setzen jetzt

$$\alpha_i = \frac{u + \zeta^i v}{1 - \zeta^i} \qquad (i = 1 , 2 , \ldots , l - 1)$$

Nach (8)′ schliessen wir, dass die Ideale (α_i) ganz und paarweise teilerfremd sind und dass sie nur Primteiler ersten Grades enthalten, weil die rationalen Primteiler des Ausdrucks auf der linken Seite von (8)′ mit Ausnahme von l die Form $kl + 1$ haben. Da λ^{l-1}/l $(\lambda = 1 - \zeta)$ und $l/u + v$ (für $l = 3$ sogar $l^2/u + v$) gelten, so ist $\lambda^3/u + v$ und mithin

$$x = \alpha_1 = \frac{u + v}{\lambda} - v \equiv - v \pmod{\lambda^2} .$$

Demnach ist x eine semiprimäre Zahl von $K(\zeta)$. Wie oben stellt man fest, dass (9) auch jetzt bestehen muss. Unter Brücksichtigung der Relationen

$$\lambda^{1-S^{\frac{l-1}{2}}} = - \zeta , \; \zeta^{Q(S)} = \zeta^{-2}$$

entnimmt man

$$(u + \zeta v)^{Q(S)} \zeta = \delta^{l^n} ,$$

wo δ eine Zahl von $K(\zeta)$ ist. Ist nun p/v, so kommen wir zur Kongruenz

$$\zeta \equiv \delta^{l^n} \pmod{p} .$$

Nach Hilfssatz 2 folgt auch diesmal die Bedingung (7). Aus Symmetriegründen erhält man im Falle p/u dasselbe Ergebnis. Somit ist Satz 2 bewiesen.

4. Als einfache Folgerungen erhalten wir aus den vorigen Sätzen einige Ergebnisse über die Gleichungen (2) und (3).

Satz 3. *Ist* $l > 3$, *erfüllen die ganzen rationalen Zahlen* x, y, z *die Bedingungen*

$$x^l + y^l = cz^{l^n}\,,\ (x\,,\ y) = 1 \tag{11}$$

und ist c *eine rationale Zahl, deren Zähler und Nenner keinen Primteiler von der Form* $kl + 1$ *enthalten, so besteht für eine Primzahl* p *die Kongruenz* (7) *in beiden folgenden Fällen:*

a) $p/x\,,\ l \nmid x$;
b) $p/x^2 - y^2\,,\ l \nmid x^2 - y^2$.

Beweis. Man kann $c = \dfrac{c_2}{c_1}$ setzen, wo c_1 und c_2 ganze teilerfremde Zahlen ohne Primteiler von der Form $kl + 1$ sind und c_1 nicht durch l^n teilbar ist. Die trivialen Fälle $xy = 0$ und $x + y = 0$ sind offenbar sowohl in a) als in b) ausgeschlossen. Bekanntlich ist $\left(x + y\,,\ \dfrac{x^l + y^l}{x + y}\right) = 1$ oder l. Weil ferner $x + y$ und $\dfrac{x^l + y^l}{x + y}$ nur gleichzeitig durch l teilbar sein können und $l^2 \nmid \dfrac{x^l + y^l}{x + y}$ ist und weil die von l verschiedenen Primteiler von $\dfrac{x^l + y^l}{x + y}$ die Form $kl + 1$ haben, erfüllen $u = x$ und $v = y$ entweder die Bedingungen (8) oder (8)′ je nachdem $l \nmid c_2 z$ oder $l/c_2 z$ ist.

Besteht nun a) für p, so folgt aufgrund der Sätze 1 und 2, dass (7) gültig ist. Besteht b), so folgt (2) aus Satz 1, weil $c_2 z$ diesmal wegen $l \nmid x + y$ zu l prim ist.

Man erkennt leicht, dass Satz 3 auch für $l = 3$ gilt, wenn c zu l prim ist.

Es sei c eine ganze Zahl, die keinen Primteiler von der Form $kl + 1$ hat. Gibt es dann ganze Zahlen x, y, z, die die Bedingungen (11) und $l \nmid x^2 - y^2$ erfüllen, so gilt für jeden Primteiler p von c die Kongruenz (7). Das folgt unmittelbar aus Satz 3, b). Dieses Ergebnis enthält als Spezialfall einen Satz von Dénes (vgl. [1], Satz 6), denn $l \nmid x^2 - y^2$ ist gültig, wenn l/x oder l/y ist.

Aus Satz 3, a) folgt unmittelbar

Satz 4. *Erfüllen x, y, z, l und c im vorigen Satz genannten Bedingungen, so bestehen die Kongruenzen*

$$x^l \equiv x \pmod{l^{n+1}} \quad \text{für} \quad l \nmid x , \tag{12}$$

$$y^l \equiv y \pmod{l^{n+1}} \quad \text{für} \quad l \nmid y , \tag{12}'$$

$$(x \pm y)^l \equiv x^l \pm y^l \pmod{l^{n+1}} \quad \text{für} \quad l \nmid xy(x^2 - y^2) . \tag{12}''$$

Ist nämlich $l \nmid x$, so folgt aus Satz 3, a), dass für jeden Primteiler p von x die Kongruenz

$$p^l \equiv p \pmod{l^{n+1}}$$

gilt. Daraus ergibt sich dann unmittelbar $x^l \equiv x \pmod{l^{n+1}}$. Im Fall $l \nmid x^2 - y^2$ enthält man unter Benutzung von Satz 3, b), dass

$$(x \pm y)^l \equiv x \pm y \pmod{l^{n+1}}$$

ist. Hieraus, aus (12) und aus (12)′ folgt die Gültigkeit von (12)″.

Für die Gleichung (3) erhalten wir

Satz 5. *Ist $l > 3$ und erfüllen die ganzen rationalen Zahlen x, y, z die Bedingungen*

$$c_1(x^{l^n} + y^{l^n}) = c_2 z^{l^n} , \quad (x , y) = 1 , \tag{13}$$

wo c_1 und c_2 ganze teilerfremde Zahlen ohne Primteiler von der Form $kl^n + 1$ sind, so besteht die Kongruenz (7) für eine Primzahl p in den Fällen

a) $p \mid x$, $l \nmid x$;

b) $p \mid x^{2l^{n-1}} - y^{2l^{n-1}}$, $l \nmid x^2 - y^2$.

Beweis. Offenbar kann man annehmen, dass $l^n \nmid c_1$ ist. Wir setzen jetzt $u = x^{l^{n-1}}$, $v = y^{l^{n-1}}$. Hat eine Primzahl q die Eigenschaften

$$x^{l^{n-1}} + y^{l^{n-1}} \not\equiv 0 , \; x^{l^n} + y^{l^n} \equiv \pmod{q} ,$$

so hat sie bekanntlich (vgl. z.B. [3], S. 27) die Form $kl^n + 1$. Mit Hilfe dieser Tatsache erkennen wir leicht, dass u und v im Falle $l \nmid c_2 z$ den Bedingungen (8) und im Falle $l \mid c_2 z$ den Bedingungen (8)′ genügen. Da

$$x^{2l^{n-1}} \equiv x^2 \pmod{l}$$

ist, so folgt aus $l \mid x^{2l^{n-1}} - y^{2l^{n-1}}$, dass auch $l \mid x^2 - y^2$ sein muss. Demnach können wir Satz 1 und Satz 2 anwenden und erhalten unmittelbar die Kongruenz (7).

Satz 6. *Es sei $l > 3$, $m = l^n$ und c eine zu l prime rationale Zahl, welche die folgenden Eigenschaften hat:*

1) *kein Primteiler des Zählers oder des Nenners von* c *hat die Form* $kl + 1$,

2) c *ist ein* m^{ter} *Potenzrest* $(\text{mod } l^{n+1})$ *oder* $\frac{c}{2}$ *ein* m^{ter} *Potenznichtrest* $(\text{mod } l^{n+1})$.

Ist dann (11) *in ganzen durch* l *nicht teilbaren Zahlen lösbar, so ist*

$$2^{l-1} \equiv 1 \ (\text{mod } l^{n+1}) \ . \tag{14}$$

Beweis. Ist x oder y gerade, so folgt (14) unmittelbar aus Satz 3, a), weil $2/xy$ und $l \nmid xy$ gelten. Sind x und y beide ungerade, wobei $2/x-y$ ist, so folgt (14) aus Satz 3, b), wenn man zeigt, dass $l \nmid x+y$ und $l \nmid x-y$ gültig sind. Die erstere Bedingung besteht, denn sonst wäre l/c. Es sei jetzt $l/x-y$. Nach Satz 4 ist

$$x^l - y^l \equiv x - y \ (\text{mod } l^{n+1}) \ .$$

Hieraus folgt sofort, dass $l^{n+1}/x-y$ ist, denn wäre $l^h/x-y$, $l^{h+1} \nmid x-y$ und $h < n+1$, so wäre $l^{h+1}/x^l - y^l$ wegen $h \geqq 1$ und nach (13) doch $l^{h+1}/x-y$. Aufgrund dieses Ergebnis erhalten wir aus (11)

$$2x^l \equiv cz^{l^n} \ (\text{mod } l^{n+2}) \quad \text{und} \quad 2x^m \equiv cz^m \ (\text{mod } l^{n+2}) \ , \tag{15}$$

denn aus $x^l \equiv x \ (\text{mod } l^{n+1})$ folgt sukzessiv

$$x^{l^2} \equiv x^l \ , \ x^{l^3} \equiv x^l \ , \ \ldots \ , \ x^{l^n} \equiv x^l \ (\text{mod } l^{n+2}) \ .$$

Da mithin $\frac{c}{2}$ ein m^{ter} Potenzrest $(\text{mod } l^{n+1})$ ist, muss c nach Annahme 2) ein m^{ter} Potenzrest $(\text{mod } l^{n+1})$ sein. Dann ergibt sich aus (15)

$$2x^m \equiv t^m \ (\text{mod } l^{n+1}) \ .$$

Unter Verwendung des Eulerschen Satzes erhält man hieraus schliesslich die Kongruenz (14), womit Satz 6 bewiesen ist.

5. Wir betrachten jetzt die Gleichung (3), wo man natürlich c_1 und c_2 als teilerfremd annehmen kann. Den Fall $c_1 = c_2 = 1$ können wir wegen des anfangs genannten Ergebnisses (1)′ ausschliessen. Auch den Fall $c_1 = 1, c_2 = 2$, wo (3) die Lösung $x = y = z = 1$ hat, schliessen wir im folgenden Satz aus.

Satz 7. *Sind* c_1 *und* c_2 *zwei teilerfremde natürliche Zahlen und* $c_2 > 2$, *wenn* $c_1 = 1$ *ist, so ist die Gleichung*

$$c_1(x^{l^n} + y^{l^n}) = c_2 z^{l^n} \tag{13}'$$

mit $l \nmid z$ *in ganzen Zahlen* x, y, z *unmöglich, falls*

$$n > \frac{(l-1)\log c}{\log l} - 1 \quad (c = \max(c_1, c_2)) \tag{16}$$

ist.

Beweis. Wir stellen anfangs fest, dass (16) äquivalent der Ungleichung

$$l^{n+1} > c^{l-1} \tag{16}'$$

ist. Angenommen, (13)′ habe eine ganzzahlige Lösung x, y, z mit $l \nmid z$. Ohne Beschränkung kann man auch voraussetzen, dass $z > 0$ ist und dass x, y, z eine minimale Lösung in dem Sinne bildet, das z möglichst klein ist. Dann ist $(x, y) = 1$, denn wäre q ein Primteiler von (x, y), so folgte aus (13)′ $q^{l^n} | c_2$, weil andernfalls $\frac{x}{q}, \frac{y}{q}, \frac{z}{q}$ eine Lösung von (13)′ ergäben, was jedoch der Minimaleigenschaft widerspricht. Nun erhalten wir aus $q^{l^n} | c_2$

$$c_2^{l-1} \geqq q^{(l-1)\,l^n} \geqq 2^{(l-1)l^n} = 1 + (l-1)l^n + \ldots + (l-1)l^n + 1 > l^{n+1},$$

was wegen (16) unmöglich ist. Somit ist $(x, y) = 1$.

Ferner sieht man leicht, dass $l \nmid xy$ ist. Wäre nämlich z.B. $l | y$, so folgte aus (13)′

$$c_1 x^{l^n} \equiv c_2 z^{l^n} \pmod{l^{n+1}},$$

weil $l^n > n + 1$ ist. Erhebt man diese Kongruenz in die Potenz $l - 1$, so erhält man unter Benutzung des Eulerschen Satzes

$$c_1^{l-1} \equiv c_2^{l-1} \pmod{l^{n+1}},$$

was wegen $c^{l-1} > |c_1^{l-1} - c_2^{l-1}| \geqq l^{n+1}$ unmöglich ist.

Jetzt zeigen wir, dass $l \nmid x \pm y$ ist. Sonst wäre

$$x^{l^n} \equiv \mp y^{l^n} \pmod{l^{n+1}}$$

und somit nach (13)′ entsprechend

$$c_2 z^{l^n} \equiv \begin{cases} 0 \\ 2c_1 x^{l^n} \end{cases} \pmod{l^{n+1}}.$$

Die erstere Bedingung sieht man sofort wegen (16) als unmöglich. Wie oben folgt aus der letzteren Kongruenz

$$c_2^{l-1} \equiv (2c_1)^{l-1} \pmod{l^{n+1}}$$

und daraus ferner

$$(2c_1)^k + c_2^k \geqq l^{n+1}, \tag{17}$$

wo $k = \frac{l-1}{2}$ ist. Dies ist unmöglich, denn für $c_1 = 2, c_2 = 1$ ist die linke Seite von (17) $(2c_1)^k + c_2^k = c^{l-1} + 1 = 2^{l-1} + 1$, also eine durch l nicht teilbare Zahl, weshalb $c^{l-1} + 1 \geqq l^{n+1} + 2$ oder $c^{l-1} > l^{n+1}$ ist, was (16) widerspricht. In allen andern Fällen erhält man:

$$c_1^{2k} - 2c_1^k - c_2^k > c_1^k(c_1 - 3) \geqq 0 \quad \text{für} \quad c = c_1 ,$$
$$c_2^{2k} - 2c_1^k - c_2^k > c_2^k(c_2 - 3) \geqq 0 \quad \text{für} \quad c = c_2 ,$$

denn in beiden Fällen ist $c \geqq 3$. Somit führt auch jetzt (17) zum Widerspruch mit (16)'.

Schliesslich sehen wir aus (16)', dass c_1 und c_2 keine Primteiler von der Form $hl^n + 1$ haben können.

Nun wenden wir den Satz 5 an. Eine der Zahlen $x, y, x - y$ ist gerade. Im Falle $l = 3$ ist die rechte Seite der Ungleichung (16)' $\geqq 4$ und daher $n > 1$. Mithin folgt, dass

$$2^{l-1} \equiv 1 \pmod{l^{n+1}}$$

sein muss, was wegen (16)' unmöglich ist. Hiermit ist Satz 7 bewiesen.

Satz 8. *Ist c eine zu l prime ganze Zahl, die keinen Primteiler der Form $kl^n + 1$ hat und die der Bedingung*

$$c^{l-1} \not\equiv 1 \quad \text{und} \quad 2^{l-1} \pmod{l^{n+1}} \tag{18}$$

genügt, so ist die Gleichung

$$x^{l^n} + y^{l^n} = cz^{l^n} \tag{19}$$

in ganzen Zahlen x, y, z, wobei z durch l nicht teilbar ist, nicht lösbar.

Beweis. Angenommen, es gebe ganze Zahlen x, y, z mit $l \nmid z$, die (19) erfüllen. Ohne Beschränkung kann man annehmen, dass c keinen Teiler der Form a^{l^n} enthält. Sonst kann man nämlich z durch az und c durch $c' = \frac{c}{a}$ ersetzen, denn c' erfüllt auch die Bedingung (18), da

$$a^{l^n(l-1)} \equiv 1 \pmod{l^{n+1}}$$

ist. Ferner können wir annehmen, dass $(x, y) = 1$ ist.

Es ist $l \nmid xy$. Denn wäre z.B. $l \mid x$, so folgte aus (19) $y^{l^n} \equiv cz^{l^n} \pmod{l^{n+1}}$, weil $l^n > n + 1$ ist, und hieraus weiter $c^{l-1} \equiv 1 \pmod{l^{n+1}}$, was gegen (18) ist. Unter Benutzung von Satz 5, a) sieht man, dass jeder Primteiler p von xy der Kongruenz (7) genügt. Hieraus folgt, dass die Kongruenzen

$$x^l \equiv x \, , \; y^l \equiv y \pmod{l^{n+1}} \tag{20}$$

bestehen.

Es ist $l \nmid x - y$. Sonst wäre nämlich $x^{l^n} \equiv y^{l^n} \pmod{l^{n+1}}$ und somit wegen (19)

$$2x^{l^n} \equiv cz^{l^n} \pmod{l^{n+1}}, \tag{21}$$

woraus $c^{l-1} \equiv 2^{l-1} \pmod{l^{n+1}}$ folgen würde, was gegen die Annahme (18) ist. Weil also $l \nmid x^2 - y^2$ ist, erhält man mit Hilfe von Satz 5, b)

$$(x + y)^l \equiv x + y \pmod{l^{n+1}}$$

und ferner

$$(x + y)^{l^n} \equiv x + y \pmod{l^{n+1}}.$$

Unter Berücksichtigung dieser Kongruenz und der Kongruenzen (20) folgern wir aus (19) die Bedingung

$$(x + y)^{l^n} \equiv x^{l^n} + y^{l^n} \equiv cz^{l^n} \pmod{l^{n+1}}$$

und daraus ferner $c^{l-1} \equiv 1 \pmod{l^{n+1}}$, was der Annahme (18) widerspricht. Damit ist Satz 8 bewiesen.

Satz 8 enthält als Spezialfall den Lubelskischen Satz 6 ([5], S. 19). Auch folgender Satz ist eine Erweiterung eines Lubelskischen Satzes ([5], Satz 8, S. 22). Lubelski hat seine Sätze mit Hilfe der Theorie der bekannten logarithmischen Kongruenzen von KUMMER bewiesen. Unsere Beweise sind wesentlich einfacher, weil wir von dieser Theorie nicht Gebrauch machen.

Satz 9. *Ist c eine zu l prime ganze Zahl, die keinen Primteiler der Form $kl + 1$ hat, und erfüllen die ganzen zu l primen Zahlen x, y, z die Bedingungen* (11), *so besteht die Kongruenz*

$$3^{l-1} \equiv 1 \pmod{l^{n+1}} \tag{22}$$

in folgenden Fällen:

a) $l \nmid x - y$;

b) $c^{l-1} \not\equiv 2^{l-1} \pmod{l^{n+1}}$.

Beweis. Da die Zahlen x, y, z durch l nicht teilbar sind, so folgt aus Satz 4, dass die Kongruenzen (20) bestehen. Gilt nun b), so gilt auch a). Denn wäre $l \mid x - y$, so folgte aus (20) ebenso wie im Beweis von Satz 6, dass $l^{n+1} \mid x - y$ und daher wegen (11)

$$2x^l \equiv cz^{l^n} \pmod{l^{n+1}}$$

oder (21) gültig wäre, weil nach (20) $x^{l^n} \equiv x^l \pmod{l^{n+1}}$ ist. Aus (21) folgt aber $c^{l-1} \equiv 2^{l-1} \pmod{l^{n+1}}$, gegen b). Es genügt also, nur den Fall a) zu betrachten.

Ist jetzt $3 \nmid xy$, so ist $x^2 \equiv y^2 \equiv 1 \pmod 3$, also $3 \mid x^2 - y^2$. Somit ist eine der Zahlen x, y und $x^2 - y^2$ durch 3 teilbar. Da $l \nmid cz$ besteht, ist auch $l \nmid x + y$, also $l \nmid x^2 - y^2$. Die Richtigkeit unserer Behauptung (22) folgt nun aus Satz 3, wenn man da $p = 3$ setzt.

6. Als Anwendung betrachten wir die Gleichung

$$x^2 = y^{l^n} + z^{2l^n} \quad (l > 3) . \tag{23}$$

Falls die ganzen rationalen Zahlen x, y, z dieser Gleichung genügen, so gibt es auch eine solche Lösung x, y, z, dass $(x, y, z) = 1$ erfüllt ist. Wenn nämlich die Primzahl $p \mid (x, y, z)$, so ist

$$\frac{x^2}{p^{l^n}} = \left(\frac{y}{p}\right)^{l^n} + \left(\frac{z^2}{p}\right)^{l^n} ,$$

woraus man leicht sieht, dass $p^2 \mid y$ und daher

$$\left(\frac{x}{p^{l^n}}\right)^2 = \left(\frac{y}{p^2}\right)^{l^n} + \left(\frac{z}{p}\right)^{2l^n}$$

mit den ganzen Grundzahlen $\frac{x}{p^{l^n}} , \frac{y}{p^2} , \frac{z}{p}$ bestehen muss.

Wir zeigen nun, dass (14) gelten muss, wenn die Bedingungen

$$x^2 = y^{l^n} + z^{2l^n} , (x , y , z) = 1 , l \nmid xyz$$

erfüllt sind. Aus der Gleichung

$$(x - z^{l^n})(x + z^{l^n}) = y^{l^n}$$

folgt:

$$x \mp z^{l^n} = y_1^{l^n} , x \pm z^{l^n} = y_2^{l^n} , y = y_1 y_2 , (y_1 , y_2) = 1 \quad \text{für} \quad 2 \nmid y ,$$

und

$$x \mp z^{l^n} = 2y_1^{l^n} , x \pm z^{l^n} = 2^{l^n - 1} y_2^{l^n} , y = 2y_1 y_2 , (y_1 , 2y_2) = 1 \quad \text{für} \quad 2 \mid y .$$

Man erhält somit

$$\mp 2z^{l^n} = y_1^{l^n} - y_2^{l^n} \quad \text{für} \quad 2 \nmid y ,$$
$$\mp z^{l^n} = y_1^{l^n} - 2^{l^n - 2} y_2^{l^n} \quad \text{für} \quad 2 \mid y .$$

Im ersteren Fall können wir Satz 5, b) anwenden und erhalten (14), denn $2 \mid y_1^2 - y_2^2$ und $l \nmid y_1^2 - y_2^2$ gelten, weil wir $l \nmid y_1 - y_2$ wegen $l \nmid z$ und $l \nmid y_1 + y_2$ wegen der Bedingungen

$$2x = y_1^{l^n} + y_2^{l^n} , l \nmid x$$

haben. Im letzteren Fall kann man Satz 6 benutzen. Nehmen wir an, dass

(14) nicht gültig wäre. Dann wäre $\frac{c}{2} = 2^{l^n-3}$ ein m^{ter} Potenznichtrest (mod l^{n+1}), denn sonst müsste 8 ein m^{ter} Potenzrest sein und daher

$$8^{l-1} \equiv 1 \pmod{l^{n+1}}$$

und (14) gelten, weil $4^{l-1} + 2^{l-1} + 1 \equiv 3 \not\equiv 0 \pmod{l}$ ist. Die Voraussetzungen von Satz 6 sind mithin gültig, weshalb (14) richtig wäre, gegen unsere Annahme.

Wir haben also den folgenden Satz bewiesen:

Satz 10. *Wenn die zu l primen Zahlen x, y, z die Gleichung* (23) *befriedigen, so gilt die Kongruenz* (14).

Ein Spezialfall der Gleichung (23) ist

$$x^2 - 1 = y^{l^n}, (x > 3), \tag{23}'$$

die an das bekannte Catalansche Problem anschliesst. Bekanntlich kann (23)′ in ganzen rationalen Zahlen x, y, z höchstens dann lösbar sein, wenn $2/y$ und l/x (vgl. [9]) bestehen.

Angenommen, (x, y) sei eine Lösung von (23)′. Wie oben, erhält man jetzt, wenn man bei Bedarf die Vorzeichen der Zahlen x, u, v wechselt,

$$x - 1 = 2u^{l^n}, x + 1 = 2^{l^n-1} v^{l^n}, y = 2uv, (u, v) = 1 \tag{24}$$

und mithin

$$u^{l^n} + 1 = 2^{l^n-2} v^{l^n}. \tag{25}$$

Weil l/x ist, sieht man sofort, dass $l \nmid uv$ und auch $l \nmid u \pm 1$ ist, denn wäre $u \equiv 1 \pmod{l}$, so ergäbe sich aus (24) $x \equiv 3 \pmod{l}$ und somit $l = 3$. Für $l = 3$ ist (23)′ jedoch unmöglich [8].

Da $2/u + 1$ wegen (25) ist, so schliesst man mit Hilfe von Satz 5, b), dass (14) gilt.

Eine der Zahlen $u - 1, u, u + 1$ ist durch 3 teilbar. Daher folgt aus Satz 5, dass (22) gilt. Offenbar enthalten (14) und (22) das anfangs genannte Ergebnis von Oblath.

Mit Hilfe der Kongruenzen (14) und (22) stellen wir fest (vgl. [3], S. 39—40), dass (23)′ in ganzen Zahlen unmöglich ist, falls (1)′ gilt. HYYRÖ [2] hat jedoch neulich mit einer ganz andersartigen Methode beweisen können, dass schon $n > 1$ dafür hinreichend ist. Es sei erwähnt (vgl. [4], [12]), dass im Fall $n = 1$ für die Lösbarkeit von (23)′ z.B. folgende Bedingungen notwendig sind:

1) $x \equiv \pm (2^{l-1} - 1) \pmod{l^3}$, $y \equiv -1 \pmod{l^3}$;
2) $l > 200\,000$, $l \equiv 1 \pmod{8}$;
3) $x > 2^{l(l-2)} > 10^{12 \cdot 10^9}$, $y > 4^{l-2} > 10^{12 \cdot 10^4}$.

Überdies hat (23)′ höchstens eine Lösung, wie Obláth [11] gezeigt hat.

Literatur

[1] DÉNES, P.: Über die Diophantische Gleichung $x^l + y^l = cz^l$. - Acta Math. 88, 1952, S. 241–251.

[2] HYYRÖ, S.: Über die Diophantische Gleichung $ax^n - by^n = z$ und über das Catalansche Problem (unveröffentlicht).

[3] INKERI, K.: Untersuchungen über die Fermatsche Vermutung. - Ann. Acad. Sci. Fenn. A I 33, 1946, S. 1–60.

[4] –»– and HYYRÖ, S.: On the congruence $3^{p-1} \equiv 1 \pmod{p^2}$ and the diophantine equation $x^2 - 1 = y^p$. - Ann. Univ. Turku, A 50, 1961, S. 1–4.

[5] LUBELSKI, S.: Studien über den grossen Fermatschen Satz.-Prace Mat. - Fizyczne, 42, 1935, S. 1–34.

[6] MAILLET, E.: Sur l'équation indéterminée $ax^{\lambda^t} + by^{\lambda^t} = cz^{\lambda^t}$. - Assoc. Franc. Sci., St. Etienne, 26, 1897, S. 156–168.

[7] –»– Sur les équations indéterminées de la forme $x^\lambda + y^\lambda = cz^\lambda$. Acta Math. 24, 1901, S. 247–256.

[8] NAGELL, T.: Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$. - Norsk. Mat. Forenings Skr. I, 2, 1921, S. 1–14.

[9] –»– Sur une équation diophantienne à deux indéterminées. - Norske Vid. Selsk. Forh., Trondheim, VII, 38, 1935, S. 136–139.

[10] OBLÁTH, R.: Sobre ecuaciones diofánticas imposibles de la forma $x^m + 1 = y^n$. - Rev. Mat. Hisp.-Amer., IV, 1, 1941, S. 122–140.

[11] –»– Über die Zahl $x^2 - 1$. - Mathematica B, VIII, 1939–1940, S. 161–172.

[12] PEARSON, E. H.: On the congruences $(p-1)! \equiv -1$ and $2^{p-1} \equiv 1 \pmod{p^2}$. – Math. Comp. 17, 1963, S. 194–195.

[13] VANDIVER, H. S.: On trionomial diophantine equations connected with the Fermat relation. - Monatsh. Math. 43, 1936, S. 317–320.

Gedruckt September 1963