Sitzungsberichte

der

mathematisch-physikalischen Classe

der

k. b. Akademie der Wissenschaften

zu München.

1901. Heft I.

München.
Verlag der k. Akademie.
1901.

In Commission des G. Franz'schen Verlags (J. Roth).

Ueber den Fermat'schen Satz betreffend die Unmöglichkeit der Gleichung $x^n = y^n + z^n$.

Von **F. Lindemann.**

(*Eingelaufen 8. Juni.*)

Bekanntlich hat Fermat, ohne einen Beweis anzugeben, den Satz aufgestellt, dass die Gleichung $x^n = y^n + z^n$ nicht durch drei ganze Zahlen x, y, z befriedigt werden könne, sobald die ganze Zahl n grösser als 2 ist. Diese Angabe wird uns in der von Bachet veranstalteten Diophant-Ausgabe[1]) überliefert, in welcher gelegentliche Randbemerkungen aus Fermat's Handexemplare abgedruckt wurden. Die Quaestio VIII im zweiten Buche von Diophant's Arithmetik handelt nemlich von der Aufgabe, ein gegebenes Quadrat in die Summe zweier Quadrate zu zerlegen; und am Schlusse dieser Quaestio findet sich folgender Passus:[2])

„Observatio Domini Petri De Fermat.

„Cubum autem in duos cubos, aut quadratoquadratum „in duos quadratoquadratos et generaliter nullam in infini-„tum ultra quadratum potestatem in duos eiusdem nominis

---

[1]) Diophanti Alexandri arithmeticorum libri sex, et de numeris multangulis liber unus. Cum commentariis C. G. Bacheti V. C. et obversationibus D. P. de Fermat Senatoris Tolosani. Accessit Doctrinae Analyticae inventum novum, collectum ex varijs eiusdem D. de Fermat epistolis. Tolosae, MDCLXX.

[2]) Vgl. auch Oeuvres de Fermat, publiés par Paul Tannery et Charles Henry, 1891, t. I, p. 291.

„fas est dividere cuius rei demonstrationem mirabilem sane „detexi. Hanc marginis exiguitas non caperet."

Für den Fall $n = 3$ betont Fermat seinen Satz auch in einem Briefe an Digby vom 7. April 1658,[1]) in einem andern Briefe vom 15. August 1657 stellt er die Aufgabe eine Zahl x^3 in der Form $y^3 + z^3$ darzustellen.[2])

Für eine gewisse Klasse von Zahlen n (zu welcher z. B. alle Zahlen unter 100 gehören) hat bekanntlich Kummer bei Gelegenheit anderer Untersuchungen den Fermat'schen Satz verificirt.[3]) Einzelne einfache Fälle sind schon vielfach behandelt worden.

Mit x, y, z seien drei ganze positive Zahlen bezeichnet, welche der Grösse nach geordnet sind, so dass:

$$x > y > z. \tag{1}$$

Es bedeute n eine ungerade Primzahl; es ist also

$$n > 2. \tag{2}$$

Wir nehmen an, es bestehe eine Gleichung der Form

$$x^n = y^n + z^n \tag{3}$$

und wollen zeigen, dass diese Annahme zu Widersprüchen

---

[1]) Vergl. Wallis, Opera Mathematica, t. II, p. 844, Oxford 1693.

[2]) Beide Briefe abgedruckt in den Oeuvres de Fermat, t. II, p. 343 ff. und p. 376; vergl. ferner Henry, Recherches sur les manuscripts de Pierre de Fermat, Bulletino di bibliographia e di storia delle scienze matematiche e fisiche publ. da B. Boncompagni, Bd. XII, 1879, wo insbesondere auch die Frage erörtert wird, ob Fermat im Besitze von Beweisen für seine Sätze war; vergl. dazu Mansion, Nouvelle correspondance de mathématiques t. V.

[3]) Monatsberichte der Berliner Akademie, April 1847 und Crelle's Journal Bd. 45, p. 93, 1847; vergl. dazu Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 4, 1894/95, p. 517 ff., wo auch die ältere Litteratur angegeben ist; hinzuzufügen sind die Arbeiten von Genocchi im Bd. 3 und 6 der Annali di matematica und Crelle's Journal Bd. 99, ferner Pepin, Comptes rendus t. 82.

führt. Da gemeinsame Factoren aus dieser Gleichung herausfallen, so können die Zahlen x, y, z jedenfalls als relativ prim zu einander vorausgesetzt werden.

Die Differenz $x^n - y^n$ ist sofort in die Factoren

$$(4) \qquad x - y \text{ und } x^{n-1} + x^{n-2}y + \ldots + y^{n-1}$$

zerlegbar; es muss deshalb auch die Zahl z in entsprechender Weise in Factoren zerfallen. Ist R ein Factor von z, so müssen die beiden Ausdrücke (4) zusammen den Factor R^n enthalten; es wird also eine Potenz R^{n-i} in der Differenz $x - y$, eine Potenz R^i in dem andern Ausdrucke (4) enthalten sein; eine solche Zahl R werde mit r_i bezeichnet; dann ist

$$(5) \qquad z = r \cdot r_1 \cdot r_2 \ldots . r_n,$$

$$(6) \qquad x - y = r^n \cdot r_1^{n-1} \cdot r_2^{n-2} \ldots . r_{n-2}^2 \cdot r_{n-1} = r^n \cdot \varrho,$$

$$(7) \qquad x^{n-1} + x^{n-2}y + \ldots . + y^{n-1} = r_1 \cdot r_2^2 \cdot r_3^3 \ldots . r_{n-1}^{n-1} \cdot r_n^n.$$

Jede dieser Zahlen r_i kann wieder in verschiedene Primfactoren zerfallen. Für das Folgende sind die Zahlen r und r_n von besonderer Wichtigkeit; beide sind offenbar durch die Gleichungen (5), (6) und (7) eindeutig bestimmt: r_n als derjenige Factor von z, welcher in $x - y$ nicht vorkommt, und r als derjenige Factor von z, welcher in dem Quotienten $\frac{x^n - y^n}{x - y}$ nicht enthalten ist. Die übrigen Zahlen r_i sind nicht nothwendig eindeutig festgelegt, sind auch für das Folgende von geringerer Bedeutung.

In gleicher Weise kann die Differenz $x - z$ in Factoren zerlegt werden; es ist:

$$(6^a) \qquad x - z = q^n \cdot \varkappa = q^n \cdot q_1^{n-1} \cdot q_2^{n-2} \ldots . q_{n-2}^2 \cdot q_{n-1},$$

wo $\varkappa$ keine n^{te} Potenz mehr enthält, ferner

$$(7^a) \qquad x^{n-1} + x^{n-2}z + \ldots . + z^{n-1} = q_1 \cdot q_2^2 \ldots . q_{n-1}^{n-1} \cdot q_n^n,$$

$$(5^a) \qquad y = q \cdot q_1 \ldots . q_n.$$

Eine analoge Zerlegung kann auch für die Summe $y + z$ zur Anwendung kommen, so dass:

$$(6^b) \qquad y + z = p^n \cdot \pi = p^n \cdot p_1^{n-1} \cdot p_2^{n-2} \cdot \ldots \cdot p_{n-2}^2 \cdot p_{n-1},$$

$$(7^b) \qquad \begin{aligned} y^{n-1} - y^{n-2} z + y^{n-3} z^2 - \ldots + (-1)^{n-1} z^{n-1} \\ = p_1 \cdot p_2^2 \cdot \ldots \cdot p_{n-1}^{n-1} \cdot p_n^n, \end{aligned}$$

$$(5^b) \qquad x = p \cdot p_1 \cdot p_2 \ldots p_n.$$

Offenbar lässt sich, wenn n eine ungerade Zahl bezeichnet, die Zahl N_1 so bestimmen, dass die Differenz

$$x^n - y^n - N_1 (x - y)^n$$

durch das Product $x y$ theilbar wird; und zwar ergibt sich

$$N_1 = 1.$$

Ferner kann N_2 so gewählt werden, dass der Ausdruck

$$x^n - y^n - N_1 (x - y)^n - N_2 x y (x - y)^{n-2}$$

durch $x^2 y^2$ theilbar wird. Man muss zu dem Zwecke den Factor von $x^{n-1} y$ gleich Null setzen und findet $N_1 n - N_2 = 0$, oder

$$N_2 = n.$$

Der Factor von $x y^{n-1}$ fällt dann von selbst heraus. Um ebenso das Aggregat

$$x^n - y^n - N_1 (x-y)^n - N_2 x y (x-y)^{n-2} - N_3 x^2 y^2 (x-y)^{n-4}$$

durch $x^3 y^3$ theilbar zu machen, muss man den Factor von $x^{n-2} y^3$ (welcher bis auf das Vorzeichen gleich dem Factor von $x^2 y^{n-2}$ ist) zum Verschwinden bringen, d. h. es muss

$$-N_1 \binom{n}{2} + N_2 (n-2) - N_3 = 0,$$

also

$$N_3 = \frac{n(n-3)}{2}$$

sein. In gleicher Weise wird

$$\begin{aligned} x^n - y^n - N_1 (x-y)^n - N_2 x y (x-y)^{n-2} - N_3 x^2 y^2 (x-y)^{n-4} \\ - N_4 x^3 y^3 (x-y)^{n-6} \end{aligned}$$

durch $x^4 y^4$ theilbar, wenn

$$N_1 \binom{n}{3} - N_2 \binom{n-2}{2} + N_3 (n-4) - N_4 = 0$$

ist, oder:

$$N_4 = \frac{n(n-4)(n-5)}{1 \cdot 2 \cdot 3}.$$

Ebenso kann man weiter schliessen und findet durch ein Recursionsverfahren leicht, dass das Aggregat

$$(8) \qquad \begin{aligned} x^n - y^n - N_1 (x-y)^n - N_2 x y (x-y)^{n-2} \ldots\ldots \\ - N_s x^{s-1} y^{s-1} (x-y)^{n-2s+2} \end{aligned}$$

durch $x^s y^s$ theilbar ist, wenn

$$(9) \qquad N_s = \frac{n(n-s)(n-s-1)\ldots\ldots(n-2s+4)(n-2s+3)}{1 \cdot 2 \cdot 3 \ldots\ldots (s-1)}$$

gesetzt wird.

Sei nun die Primzahl n gleich $2\nu + 1$, und setzen wir $s = \nu$, so wird

$$(10) \qquad N_\nu = \frac{(2\nu+1)\nu(\nu+1)}{1 \cdot 2 \cdot 3}.$$

Es ist also identisch

$$(11) \qquad \begin{aligned} x^n - y^n - N_1 (x-y)^n - N_2 x y (x-y)^{n-2} - \ldots\ldots \\ - N_\nu x^{\nu-1} y^{\nu-1} (x-y)^3 = N x^\nu y^\nu (x-y), \end{aligned}$$

wo N noch zu bestimmen ist, denn die linke Seite ist theilbar durch $x^\nu y^\nu$ und ist Null für $x = y$. Der Werth von N wird aber durch Fortsetzung derselben Schlussweise gefunden, die wir bisher anwandten, nemlich indem wir verlangen, dass aus dem Ausdrucke

$$x^n - y^n - N_1 (x-y)^n - \ldots - N_\nu x^{\nu-1} y^{\nu-1} (x-y)^3 - N x^\nu y^\nu (x-y)$$

der Term $x^{\nu+1} y^\nu$ (und folglich auch $x^\nu y^{\nu+1}$) herausfalle; es wird daher

$$(12) \qquad N = N_{\nu+1} = 2\nu + 1 = n.$$

Unter Benutzung von (6) und (7) erhalten wir sonach die Identität:

$$n\,x^{\nu}\,y^{\nu}\,r^{n}\,\varrho = r^{n}\cdot r_1^{n}\ldots r_n^{n} - \sum_{i=1}^{i=\nu} N_i\,x^{i-1}\,y^{i-1}\,r^{n(n-2i+2)}\,\varrho^{n-2i+2},$$

oder, wenn beiderseits mit $\varrho\,r^{n}$ dividirt wird:

$$(13)\quad n\,x^{\nu}\,y^{\nu} = r_1\cdot r_2^2\,r_3^3\ldots r_n^n - \sum_{i=1}^{\nu} N_i\,x^{i-1}\,y^{i-1}\,r^{n(n-2i+1)}\,\varrho^{n-2i+1},$$

wobei die Zahlen N_i offenbar sämmtlich ganze Zahlen sind.

Die relativen Primzahlen x und y können wegen (6) mit den Zahlen $r_1, r_2, \ldots r_{n-1}$ keinen Factor gemein haben. Jedes Glied der rechten Seite von (13) ist durch jede dieser Zahlen theilbar, da mit ϱ die Zahl $r_1^{n-1}\,r_2^{n-2}\ldots r_{n-1}$ bezeichnet wurde. Soll daher auch die linke Seite durch $r_1, r_2, \ldots r_{n-1}$ theilbar sein, so muss die Zahl n diese Factoren enthalten. Nun sollte aber n eine Primzahl bedeuten; also bleiben nur folgende Möglichkeiten:

Entweder es ist

$$(14)\qquad r_1 = n,\ r_2 = r_3 = \ldots = r_{n-1} = 1,$$

und dann folgt aus (5) und (6)

$$(15)\qquad z = n\cdot r\cdot r_n,\quad x - y = r^{n}\cdot n^{n-1}.$$

Oder es ist

$$(16)\qquad r_1 = r_2 = r_3 = \ldots = r_{n-1} = 1,$$

und dann folgt

$$(17)\qquad z = r\cdot r_n,\quad x - y = r^{n}.$$

Eine andere Möglichkeit bleibt nicht offen, denn von den Zahlen $r_2, r_3, \ldots r_{n-1}$ kann keine gleich n sein; es wäre nemlich dann die rechte Seite von (13) mindestens durch n^2 theilbar, folglich auch die linke Seite; d. h. es müsste x oder y durch n theilbar sein; dann aber wären nach (6) beide Zahlen durch n theilbar, während sie doch als relative Primzahlen vorausgesetzt sind. Die Zahl r_n bleibt zunächst beliebig.

Da die Gleichung (11), wenn N durch (12) bestimmt wird, eine Identität ist, können wir in ihr y durch z ersetzen und

erhalten so in Rücksicht auf (6ª) und (7ª) an Stelle von (13) die Beziehung:

$$(13^a)\quad n\,x^r\,z^r = q_1\cdot q_2^2\cdot\ldots\cdot q_n^n - \sum_{i=1}^{r} N_i\,x^{i-1}\,z^{i-1}\,q^{n(n-2i+1)}\,\varkappa^{n-2i+1},$$

auf welche wir die gleichen Ueberlegungen anwenden können. Es ist also entweder

$$(15^a)\qquad y = n\cdot q\cdot q_n,\quad x - z = q^n\cdot n^{n-1},$$

oder:

$$(17^a)\qquad y = q\cdot q_n,\quad x - z = q^n.$$

Endlich können wir in der Identität (11) auch x durch y und y durch $-z$ ersetzen; dann ergibt sich mit Rücksicht auf (6ᵇ) und (7ᵇ):

$$(13^b)\quad \begin{aligned}(-1)^r\,n\,y^r\,z^r &= p_1\,p_2^2\cdot\ldots\cdot p_n^n\\ &- \sum_{i=1}^{r} N_i\,(-1)^{i-1}\,y^{i-1}\,z^{i-1}\,p^{n(n-2i+1)}\,\pi^{n-2i+1};\end{aligned}$$

und die nochmalige Wiederholung der gleichen Schlussweise führt zu dem Resultate, dass entweder:

$$(15^b)\qquad x = n\cdot p\cdot p_n,\quad y + z = p^n\cdot n^{n-1}$$

oder

$$(17^b)\qquad x = p\cdot p_n,\quad y + z = p^n$$

sein muss.

Da x, y, z keinen gemeinsamen Factor enthalten sollen, so ergibt die Combination der Gleichungen (15), (17), (15ª), (17ª), (15ᵇ), (17ᵇ), dass nur drei Fälle noch näher zu untersuchen sind. Die Annahme (15) nemlich ist mit (15ª) oder (15ᵇ) nicht vereinbar, so dass aus der Annahme (15) nothwendig die Gleichungen (17ª) und (17ᵇ) folgen. Gehen wir aber von (17) aus, so kann sowohl (15ª) als (15ᵇ) möglich sein. Betrachten wir diejenigen Möglichkeiten als gleichwerthig, die durch Vertauschung von y mit z aus einander hervorgehen, so bleiben die folgenden drei Fälle:

I) $x - y = r^n \cdot n^{n-1}$, $z = n \cdot r \cdot r_n$,
$x - z = q^n$, $y = q \cdot q_n$,
$y + z = p^n$, $x = p \cdot p_n$;

II) $x - y = r^n$, $z = r \cdot r_n$,
$x - z = q^n$, $y = q \cdot q_n$,
$y + z = p^n \cdot n^{n-1}$, $x = n \cdot p \cdot p_n$;

III) $x - y = r^n$, $z = r \cdot r_n$,
$x - z = q^n$, $y = q \cdot q_n$,
$y + z = p^n$, $x = p \cdot p_n$.

Hieraus folgt im Falle I):

$$x = \frac{p^n + q^n + n^{n-1} r^n}{2},$$

im Falle II):

$$x = \frac{r^n + q^n + n^{n-1} p^n}{2}$$

und im Falle III):

$$x = \frac{p^n + q^n + r^n}{2}.$$

Dass x sich durch drei Zahlen p, q, r in einer dieser Formen darstellen lassen müsse, hat schon Abel ohne Mittheilung eines Beweises angegeben.[1]) Er erwähnt ausserdem noch die Möglichkeit

$$x = \frac{p^n + n^{n-1}(q^n + r^n)}{2},$$

welche bei uns ausgeschlossen ist.

Wir machen zuerst die Annahme I). Die Gleichung (13[a]) wird hier

$$(18) \qquad n x^\nu z^\nu = q_n^n - \sum_{i=1}^{\nu} N_i x^{i-1} z^{i-1} q^{n(n-2i+1)}.$$

Alle Zahlen N_i mit Ausnahme von $N_1 = 1$ sind durch n theilbar; auch z ist durch n theilbar; vom dritten Gliede ab

[1]) Lettre à Holmboe vom 3. August 1823, Oeuvres t. II, p. 255.

sind also alle Terme der rechten Seite durch n^3 theilbar. Die linke Seite ist mindestens durch $n^{\nu+1}$ theilbar; folglich ist auch

$$q_n^n - q^{n(n-1)} \equiv 0 \mod n^3. \tag{19}$$

Nach dem Fermat'schen Satze ist

$$q^{n(n-1)} \equiv 1 \mod n^3, \tag{20}$$

denn q kann, da y zu z relativ prim ist, nicht durch n theilbar sein. Es ergibt sich

$$q_n^n \equiv 1 \mod n^3,$$

und da identisch $q_n^n \equiv q_n \mod n$ ist

$$q_n \equiv 1 \mod n. \tag{21}$$

Ebenso folgt aus (13^b):

$$(-1)^\nu n y^\nu z^\nu = p_n^n - \sum_{i=1}^{\nu} N_i (-1)^{i-1} y^{i-1} z^{i-1} p^{n(n-2i+1)}, \tag{22}$$

und die Anwendung derselben Schlussweise führt zu der Congruenz

$$p_n \equiv 1 \mod n. \tag{23}$$

Folglich ist auch

$$\begin{aligned} x = p \cdot p_n &\equiv p \mod n, \\ y = q \cdot q_n &\equiv q \quad \text{„} \quad n. \end{aligned} \tag{24}$$

Ferner ist

$$\begin{aligned} x - y = p\,p_n - q\,q_n &\equiv p - q \mod n \\ = r^n \cdot n^{n-1} &\equiv 0 \quad \text{„} \quad n, \end{aligned}$$

also auch:

$$p^n \equiv q^n \mod n^3. \tag{25}$$

Weiter folgt aus den Gleichungen I):

$$2z = p^n - q^n + r^n \cdot n^{n-1}, \tag{26}$$

also nach (25), da $n > 2$:

$$2z \equiv 0 \mod n^3. \tag{27}$$

Es wäre also z nicht nur durch n, sondern durch n^2 theilbar, d. h. eine der beiden Zahlen r oder r_n müsste den Factor n enthalten.

Setzen wir die der Annahme I) entsprechenden, in (14) und (15) gegebenen Werthe der Zahlen r_i in (13) ein, so ergibt sich:

$$n x^\nu y^\nu = n r_n^n - \sum_{i=1}^{\nu} N_i x^{i-1} y^{i-1} r^{n(n-2i+1)} n^{(n-1)(n-2i+1)},$$

und nach Division mit n:

$$\begin{aligned} x^\nu y^\nu &= r_n^n - \sum_{i=1}^{\nu} N_i x^{i-1} y^{i-1} r^{n(n-2i+1)} n^{n^2-2in+2i-2} \\ &= r_n^n - r^{n(n-1)} n^{n(n-2)} - x y r^{n(n-3)} n^{n^2-4n+3} - \dots\dots \\ &\qquad - \frac{\nu(\nu+1)}{2 \cdot 3} x^{\nu-1} y^{\nu-1} r^{2n} n^{2(n-1)}. \end{aligned} \tag{28}$$

Wäre also $r_n \equiv 0 \bmod. n$, so müsste eine der Zahlen x oder y durch n theilbar sein, was nicht angeht. Es kann also nur r den Factor n enthalten, so dass z mindestens durch n^2 theilbar ist.

Wir wollen allgemein annehmen, dass r durch $n^{\lambda-1}$, also z durch n^λ theilbar sei, wobei also λ mindestens gleich 2 wäre. Durch diese Annahme modificiren sich auch die soeben an die Relation (18) geknüpften Schlüsse. Da jetzt z durch n^λ theilbar ist, ergibt sich nemlich an Stelle von (19):

$$q_n^n - q^{n(n-1)} \equiv 0 \quad \text{mod. } n^{\lambda+1}, \tag{29}$$

also auch

$$q_n \equiv q^{n-1} \quad \text{mod. } n^\lambda.$$

Ebenso folgt aus (22)

$$p_n \equiv p^{n-1} \quad \text{mod. } n^\lambda.$$

Ferner mit Hülfe der Gleichungen I)

$$\begin{aligned} x &= p \cdot p_n \equiv p^n \quad \text{mod. } n^\lambda, \\ y &= q \cdot q_n \equiv q^n \quad \text{„ } n^\lambda. \end{aligned}$$

Nun ist nach I)

$$x = q^n + z \equiv q^n \mod n^\lambda$$
$$= p\,p_n \equiv p^n \quad , \quad n^\lambda,$$

also auch

$$p^n \equiv q^n \mod n^\lambda, \tag{30}$$

folglich:

$$p \equiv q \mod n^{\lambda-1},$$
$$p^{n^2} - q^{n^2} \equiv 0 \mod n^{\lambda+1}, \tag{30a}$$

wobei $\lambda > 2$ ist. Andererseits aus I) und (1):

$$p^{n^2} - q^{n^2} = (y+z)^n - (x-z)^n$$
$$\equiv n\,z\,(x^{n-1} + y^{n-1}) \mod n^{2\lambda+1}, \tag{31}$$

denn alle anderen Terme der rechten Seite enthalten höhere Potenzen von z, multiplicirt in Binomialcoefficienten des Exponenten n.

Aus den Identitäten (18) und (23) folgt durch Subtraction

$$p_n^n - q_n^n \equiv p^{n(n-1)} - q^{n(n-1)} - n\,z\,(y\,p^{n(n-3)} - x\,q^{n(n-3)}) \mod n^{2\lambda+1}.$$

Wir multipliciren beiderseits mit $p^n q^n$ und benutzen wieder die Relationen $x = p\,p_n$, $y = q\,q_n$, sowie die Congruenz (31); dann ergibt sich

$$q^n x^n - p^n y^n \equiv q^{n^2}(q^n - p^n) + n\,z\,q^n(x^{n-1} + y^{n-1})$$
$$- n\,z\,p^n q^n (y\,p^{n(n-3)} - x\,q^{n(n-3)}) \mod n^{2\lambda+1}.$$

Da nun r durch $n^{\lambda-1}$ theilbar sein sollte, und da nach I) $x - y$ durch $r^n n^{n-1}$ theilbar ist, kann hier (indem $n\lambda - 1 > 2\lambda + 1$ ist) überall x durch y ersetzt werden; es ist also auch

$$(q^n - p^n)(y^n - q^{n^2}) \equiv 2\,n\,z\,y^{n-1} q^n - n\,z\,y\,p^n q^n (p^{n(n-3)} - q^{n(n-3)}) \mod n^{2\lambda+1}.$$

Der erste Factor der linken Seite ist nach (30) durch n^λ, der zweite Factor (da $y = q\,q_n$) nach (29) durch $n^{\lambda+1}$ theilbar; der letzte Factor des zweiten Gliedes der rechten Seite enthält nach (30) den Factor n^λ, das ganze Glied also (da z durch n^λ theilbar ist) auch den Factor $n^{2\lambda+1}$; es folgt also

$$0 \equiv 2\, n\, z\, y^{n-1}\, q^n \mod n^{2\lambda+1}$$

oder, da n nicht durch 2 theilbar ist:

$$z\, y^{n-1}\, q^n \equiv 0 \mod n^{2\lambda}. \tag{32}$$

Nach unseren Annahmen sollten y und q nicht durch n theilbar sein; es muss demnach z den Factor $n^{2\lambda}$ enthalten.

Nimmt man also an, dass die Zahl z durch n^λ theilbar sei, so müsste sie auch durch $n^{2\lambda}$ theilbar sein, was nur mit der Voraussetzung $z = 0$ verträglich ist. Der Fall I) ist damit als unzulässig nachgewiesen.

Der Fall II) lässt sich in genau der gleichen Weise erledigen. Aus den Identitäten (13) und (17[a]) erhalten wir bez.

$$\begin{aligned} n\, x^\nu\, y^\nu &= r_n^n - \sum_{i=1}^{\nu} N_i\, x^{i-1}\, y^{i-1}\, r^{n(n-2i+1)}, \\ n\, x^\nu\, z^\nu &= q_n^n - \sum_{i=1}^{\nu} N_i\, x^{i-1}\, z^{i-1}\, q^{n(n-2i+1)}, \end{aligned} \tag{33}$$

und schliessen aus ihnen, wie in (21), (23) und (24) die Congruenzen

$$\begin{aligned} q_n \equiv\ r_n \ &\equiv 1 && \mod n, \\ y = q \cdot q_n &\equiv q && \mod n, \\ z = r \cdot r_n &\equiv r && \mod n, \\ y + z = q\, q_n + r\, r_n &\equiv q + r && \mod n, \\ = p^n \cdot n^{n-1} \ &\equiv 0 && \mod n, \end{aligned}$$

also auch, entsprechend zu (25):

$$q^n + r^n \equiv 0 \mod n^2,$$

ferner aus II)

$$2\, x = q^n + r^n + p^n\, n^{n-1} \equiv 0 \mod n^2.$$

Die Identität (13[b]) gibt nach Division mit n

$$\begin{aligned} (-1)^\nu\, y^\nu\, z^\nu &= p_n^n - p^{n(n-1)}\, n^{n(n-2)} \\ &+ \sum_{i=2}^{\nu} (-1)^i\, N_i\, x^{i-1}\, y^{i-1}\, p^{n(n-2i+1)}\, n^{n^2-2in+2i-2}. \end{aligned} \tag{34}$$

Hieraus folgt, wie oben entsprechend aus (28), dass p durch n theilbar sein muss. Sei allgemein p durch $n^{\lambda-1}$, also x durch n^λ theilbar; dann folgt aus (33)

$$\begin{aligned}
r_n^n - r^{n(n-1)} &\equiv q_n^n - q^{n(n-1)} \equiv 0 && \text{mod. } n^{\lambda+1},\\
r_n \equiv r^{n-1},\ q_n &\equiv q^{n-1} && \text{mod. } n^\lambda,\\
y = x + r^n &\equiv r^n && \text{mod. } n^\lambda,\\
z = x - q^n &\equiv -q^n && \text{mod. } n^\lambda,\\
r^n + q^n &\equiv 0 && \text{mod. } n^\lambda,\\
r^{n^2} + q^{n^2} &\equiv 0 && \text{mod. } n^{\lambda+1}.
\end{aligned}$$

Endlich aus II) und (1):

$$\begin{aligned}
r^{n^2} + q^{n^2} &= (x-y)^n + (x-z)^n\\
&\equiv -n\,x\,(y^{n-1} + z^{n-1}) \quad \text{mod. } n^{\lambda+1}.
\end{aligned}$$

Durch Benutzung dieser Relation und durch Addition der Gleichungen (33) wird man schliesslich, wie bei (32), zu der Congruenz

$$x\,y^{n-1}\,q^n \equiv 0 \quad \text{mod. } n^{2\lambda}$$

geführt. Also müsste x durch $n^{2\lambda}$ theilbar sein, was nicht angeht, wenigstens nur zu der identischen Lösung $x = 0$ führen würde.

Wir haben endlich den Fall III) zu untersuchen. Es gelten wieder die Gleichungen (33) und ausserdem Gleichung (22). In jeder dieser Gleichungen sind alle Glieder der rechten Seite durch n theilbar bis auf das erste und zweite; auch die linke Seite ist durch n theilbar. Es bestehen demnach die Congruenzen

$$(35)\quad p_n^n \equiv p^{n(n-1)},\ q_n^n \equiv q^{n(n-1)},\ r_n^n \equiv r^{n(n-1)} \quad \text{mod. } n,$$

also auch nach dem Fermat'schen Satze (nach welchem $p^n \equiv p$ ist)

$$p_n \equiv p^{n-1},\ q_n \equiv q^{n-1},\ r_n \equiv r^{n-1} \quad \text{mod. } n$$

und hieraus

$$p_n \equiv 1,\ q_n \equiv 1,\ r_n \equiv 1 \quad \text{mod. } n.$$

Nehmen wir allgemein an, es sei

$$p_n \equiv q_n \equiv r_n \equiv 1 \mod n^\lambda,\ \lambda \geq 1, \tag{36}$$

so ist

$$x = p \cdot p_n \equiv p\ ,\ y \equiv q\ ,\ z \equiv r \mod n^\lambda\ , \tag{37}$$

$$x^n \equiv p^n,\ y^n \equiv q^n,\ z^n \equiv r^n \mod n^{\lambda+1}. \tag{38}$$

also folgt aus (3)

$$p^n \equiv q^n + r^n \mod n^{\lambda+1} \tag{39}$$

und aus den Gleichungen III):

$$y + z \equiv (x - z) + (x - y) \mod n^{\lambda+1}$$

folglich

$$y + z \equiv x \mod n^{\lambda+1} \tag{40}$$

oder, da $y + z = p^n$ ist:

$$x = p \cdot p_n \equiv p^n \mod n^{\lambda+1} \tag{41}$$

also

$$p^{n-1} \equiv p_n \mod n^{\lambda+1} \tag{42}$$

und wegen (36):

$$p^{n-1} \equiv 1 \mod n^\lambda. \tag{43}$$

Ebenso ist

$$q^{n-1} \equiv 1,\ r^{n-1} \equiv 1 \mod n^\lambda. \tag{44}$$

Die weitere Betrachtung knüpft sich wieder an die beiden Gleichungen (33), zu denen noch die aus (13) hervorgehende Relation (22), nemlich

$$(-1)^\nu n y^\nu z^\nu = p_n^n - p^{n(n-1)} - \sum_{i=2}^{\nu} N_i (-1)^{i-1} y^{i-1} z^{i-1} p^{n(n-2i+1)} \tag{45}$$

hinzutritt. Durch Addition der Gleichungen (33) ergibt sich

$$n x^\nu (y^\nu + z^\nu) = q_n^n + r_n^n - (r^{n(n-1)} + q^{n(n-1)}) - P, \tag{46}$$

wo zur Abkürzung:

$$P = \sum_{i=2}^{\nu} N_i x^{i-1} (y^{i-1} r^{n(n-2i+1)} + z^{i-1} q^{n(n-2i+1)}).$$

Nun ist nach III)

$$y = x - r^n, \quad z = x - q^n.$$

Nach Anwendung des binomischen Satzes wird daher:

$$P = \sum_{i=2}^{i=\nu} N_i x^{i-1} \sum_{s=0}^{s=i-1} (-1)^{i-1-s} x^s \binom{i-1}{s} [r^{n(n-i-s)} + q^{n(n-i-s)}].$$

Ferner folgt aus (37) und (40)

$$p \equiv q + r \mod n^\lambda, \tag{47}$$

also durch Potenziren

$$p^{n(n-i-s)} \equiv q^{n(n-i-s)} + r^{n(n-i-s)} \mod n. \tag{48}$$

Da alle in P vorkommenden Zahlen N_i durch n theilbar sind, ist demnach

$$P \equiv \sum_{i=2}^{i=\nu} N_i x^{i-1} \sum_{s=0}^{s=i-1} (-1)^{i-1-s} x^s \binom{i-1}{s} p^{n(n-i-s)} \mod n^2$$

$$\equiv \sum_{i=2}^{\nu} N_i x^{i-1} (x - p^n)^{i-1} p^{n(n-2i+1)} \mod n^2.$$

Nach (41) ist $x - p^n$ durch $n^{\lambda+1}$ theilbar, also folgt:

$$P \equiv 0 \mod n^2.$$

Aus (36) und (44) erhalten wir

$$q^{n(n-1)} - q_n^n \equiv 0, \quad r^{n(n-1)} - r_n^n \equiv 0 \mod n^{\lambda+1}.$$

Die Gleichung (46) führt demnach zu folgender Congruenz:

$$x^\nu (y^\nu + z^\nu) \equiv 0 \mod n. \tag{49}$$

Durch Addition von (45) zu der ersten Gleichung (33) ergibt sich in analoger Weise

$$n y^\nu (x^\nu - (-1)^\nu z^\nu) = r_n^n - p_n^n + p^{n(n-1)} - r^{n(n-1)} - Q, \tag{50}$$

wo

$$Q = \sum_{i=2}^{\nu} N_i y^{i-1} (x^{i-1} r^{n(n-2i+1)} - (-1)^{i-1} z^{i-1} p^{n(n-2i+1)}).$$

Hierin setzen wir nach III)

$$x = y + r^n, \quad z = -y + p^n;$$

dann wird

$$Q = \sum_{i=2}^{\nu} N_i y^{i-1} \sum_{s=0}^{i-1} \binom{i-1}{s} y^s \left[r^{n(n-i-s)} - (-1)^{i-1-s} p^{n(n-i-s)}\right].$$

Erheben wir die beiden Seiten der Congruenz (47) zur Potenz $n(n-i-s)$, so folgt:

$$r^{n(n-i-s)} + (-1)^{n(n-i-s)} p^{n(n-i-s)} \equiv q^{n(n-i-s)} (-1)^{n(n-i-s)} \text{ mod. } n.$$

Der Voraussetzung nach ist n eine ungerade Zahl, also $(-1)^n = (-1)^{n^2} = -1$, und somit auch

$$r^{n(n-i-s)} - (-1)^{i-1-s} p^{n(n-i-s)} \equiv q^{n(n-i-s)} (-1)^{i-1-s} \text{ mod. } n.$$

Es wird daher

$$Q \equiv \sum_{i=2}^{\nu} N_i y^{i-1} \sum_{s=0}^{i-1} \binom{i-1}{s} y^s q^{n(n-i-s)} (-1)^{i-1-s} \text{ mod. } n^2$$

$$\equiv \sum_{i=2}^{\nu} N_i y^{i-1} (y - q^n)^{i-1} q^{n(n-2i+1)} \text{ mod. } n^2.$$

Da nach III) $x - z = q^n$ ist, so folgt aus (40)

$$y - q^n \equiv 0 \text{ mod. } n^{\lambda+1}.$$

Es wäre demnach auch

$$Q \equiv 0 \text{ mod. } n^2.$$

Da ferner analog zu (41) die Congruenzen

$$y = q\, q_n \equiv q^n, \quad z = r\, r_n \equiv r^n \text{ mod. } n^{\lambda+1}$$

bestehen und nach (35)

$$q_n^n \equiv q^{n(n-1)}, \quad r_n^n \equiv r^{n(n-1)} \text{ mod. } n^{\lambda+2},$$

ist, so würde aus (50) folgen:

$$y^\nu (x^\nu - (-1)^\nu z^\nu) \equiv 0 \text{ mod. } n. \tag{51}$$

In derselben Weise würde man aus der zweiten Gleichung (33) in Verbindung mit (45) die Congruenz

$$z^\nu (x^\nu - (-1)^\nu y^\nu) \equiv 0 \text{ mod. } n \tag{52}$$

ableiten können. Die Zahlen x, y, z sollten der Voraussetzung

nach nicht durch n theilbar sein; es müssten also wegen (49), (51) und (52) auch die Congruenzen

$$\begin{aligned} y^r + \qquad z^r &\equiv 0 \mod n, \\ x^r - (-1)^r z^r &\equiv 0 \mod n, \\ x^r - (-1)^r y^r &\equiv 0 \mod n \end{aligned}$$

gleichzeitig Geltung haben. Multiplicirt man die erste dieser Congruenzen mit $(-1)^r$ und addirt sodann die linken Seiten, so ergibt sich

$$2x^r \equiv 0 \mod n.$$

Es müsste also x durch n theilbar sein, was der Voraussetzung widerspricht.

Hiermit ist die Unmöglichkeit dargethan, eine Gleichung der Form (3), d. h. eine Gleichung

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

durch ganze Zahlen x, y, z zu befriedigen, wenn n eine ungerade Primzahl bedeutet, und wenn keine der Zahlen x, y, z durch n theilbar sein soll. Der Fall aber, wo eine dieser Zahlen durch n theilbar ist, wurde schon oben (p. 192 ff.) erledigt.

Da nun die Unmöglichkeit des Falles $n = 4$ von Lamé nachgewiesen wurde, kann n auch keine Potenz von 2 sein; es bleibt also in der That nur die eine Möglichkeit $n = 2$.

Die im Vorstehenden herangezogenen Hülfsmittel sind durchaus elementarer Natur; ausser dem Fermat'schen Satze der Zahlentheorie sind nur einfache algebraische Umformungen benutzt worden. Es ist daher sehr wohl möglich, dass Fermat bereits im Besitze eines Beweises für seine Behauptung gewesen ist.

Das gewonnene Resultat kann man auch dahin aussprechen, dass die Curve

$$x^n - y^n - z^n = 0$$

ausser den drei Punkten $0, 1, -1$; $1, 0, 1$; $1, 1, 0$ keinen weiteren Punkt mit rationalen Coordinaten besitzt.

Bedeutet daher λ eine rationale Zahl, und schneiden wir die Curve mit der geraden Linie

$$(x - y) - \lambda z = 0,$$

welche durch den Punkt 1, 1, 0 hindurchgeht, so kann die resultirende Gleichung nicht durch rationale Werthe erfüllt werden. Es ergibt sich aber

$$\lambda^n (x^n - y^n) - (x - y)^n = 0,$$

oder nach Division mit $x - y$, wenn noch

$$\frac{x}{y} = t$$

gesetzt wird,

$$\lambda^n (t^{n-1} + t^{n-2} + \ldots + t + 1) - (t - 1)^{n-1} = 0.$$

Ist die ganze Zahl n grösser als 2, so kann demnach diese Gleichung nicht durch rationale Werthe von t und λ erfüllt werden, ausgenommen die Werthe $t = 1$, $\lambda = 0$ und $t = 0$, $\lambda = \pm 1$, wobei das obere Zeichen für eine ungerade, das untere für eine gerade Zahl gilt.