Sitzungsberichte

der

mathematisch-physikalischen Klasse

der

K. B. Akademie der Wissenschaften

zu München.

Band XXXVII. Jahrgang 1907.

München
Verlag der K. B. Akademie der Wissenschaften
1908.

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

Über das sogenannte letzte Fermatsche Theorem.

Von **F. Lindemann.**

(*Eingelaufen 7. Dezember 1907.*)

In einer früheren Mitteilung[1]) hatte ich die von Abel ohne Beweis mitgeteilten Formeln abgeleitet, welche drei der Gleichung $x^n = y^n + z^n$ genügende ganze Zahlen x, y, z durch die n^{ten} Potenzen dreier anderer Zahlen darstellen. Die weiteren daran geknüpften Folgerungen waren aber nicht korrekt. Trotzdem hielt ich an der Überzeugung fest, daß die damals benutzten Hilfsmittel geeignet sein müßten, der Lösung des Problems näher zu kommen, und glaube dies Ziel nunmehr erreicht zu haben.

Zur Erleichterung der Übersicht wiederhole ich im folgenden meine frühere Ableitung der Abelschen Formeln (deren Aufstellung durch Abel mir damals erst nachträglich bekannt wurde) unter Hinzufügung einiger Ergänzungen.

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[2])

[1]) Diese Sitzungsberichte, Jahrgang 1901.

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

überliefert, in welcher gelegentliche Randbemerkungen aus Fermats Handexemplare abgedruckt wurden. Die Quaestio VIII im zweiten Buche von Diophants Arithmetik handelt nämlich von der Aufgabe, ein gegebenes Quadrat in die Summe zweier Quadrate zu zerlegen; und am Schlusse dieser Quaestio findet sich folgender Passus:[1])

„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 „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,[2]) in einem anderen Briefe vom 15. August 1657 stellt er die Aufgabe eine Zahl x^3 in der Form $y^3 + z^3$ darzustellen.[3])

Für eine gewisse Klasse von Zahlen n (zu welcher z. B. alle Zahlen unter 100 gehören) hat bekanntlich Kummer bei Gelegenheit anderer Untersuchungen den Fermatschen Satz verifiziert.[4]) Einzelne einfache Fälle sind schon vielfach behandelt worden.

---

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

[2]) Vgl. Wallis, Opera Mathematica, t. II, p. 844, Oxford 1693.

[3]) Beide Briefe abgedruckt in den Oeuvres de Fermat, t. II, p. 343 ff. und p. 376; vgl. 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; vgl. dazu Mansion, Nouvelle correspondance de mathématiques, t. V.

[4]) Monatsberichte der Berliner Akademie, April 1847 und Crelles Journal, Bd. 45, p. 93. 1847. ferner Abhandlungen der K. Akademie der Wissenschaften zu Berlin, 1857; vgl. die Darstellung bei H. J. Stephen Smith: Report on the theory of numbers, Part II, Reports of the Brit. Association for the advancement of science for 1860, London 1861, sowie

§ 1. Zerlegung der Zahlen x, y, z in Faktoren.

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

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

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

zerlegbar; es muß deshalb auch die Zahl z in entsprechender Weise in Faktoren zerfallen. Ist die Zahl R ein Faktor von z, so müssen die beiden Ausdrücke (4) zusammen den Faktor R^n enthalten; ist R eine Primzahl und kommt die Potenz R^{n-i} in $x - y$ vor, so muß die Potenz R^i in dem anderen Ausdrucke (4) enthalten sein. Ist R Potenz einer Primzahl, etwa $R = M^m$, so kann die Potenz $M^{(n-i)m+k}$ in $x - y$ vorkommen, und dann muß die Potenz M^{im-k} in dem anderen Faktor enthalten sein. Eine solche Zerlegung wird auf mannigfache Weise möglich

---

bei Hilbert: Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker-Vereinigung, Bd. 4, 1894/95, p. 517 ff., wo auch die ältere Literatur angegeben ist; hinzuzufügen sind die Arbeiten von Genocchi in Band 3 und 6 der Annali di matematica und Crelles Journal, Bd. 99, ferner Pepin, Comptes rendus, t. 82. Einen eingehenden Bericht über Fermats Nachlaß gibt Henry: Bulletino di bibliografia, a. a. O.; einzelne Notizen findet man auch bei Rouse Ball: Mathematical recreations and problems. 2nd edit. London 1892.

sein; jedenfalls kann man die folgende Darstellung der drei in Betracht kommenden Faktoren erreichen.

Eine solche Zahl R werde mit r_i bezeichnet; dann ist

$$z = r \cdot r_1 \cdot r_2 \ldots r_n, \tag{5}$$

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

wobei also:

$$\varrho = r_1^{n-1} \cdot r_2^{n-2} \ldots r_{n-2}^2 \cdot r_{n-1}$$

gesetzt ist, ferner:

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

Jede dieser Zahlen r_i kann wieder in verschiedene Faktoren zerfallen; für das Folgende kommen hauptsächlich die Zahlen ϱ, r und r_n in Betracht. Ist die hier angegebene Zerlegung auf mehrfache Weise möglich, so gelten für jede einzelne Zerlegung dieser Art die folgenden Betrachtungen.

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

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

ferner:

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

$$y = q \cdot q_1 \ldots q_n. \tag{5a}$$

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

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

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

$$x = p \cdot p_1 \cdot p_2 \ldots p_n. \tag{5b}$$

§ 2. Ableitung einer Hilfsformel.

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 Produkt xy teilbar wird; und zwar ergibt sich:

$$N_1 = 1.$$

Ferner kann N_2 so gewählt werden, daß der Ausdruck:

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

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

$$N_2 = n.$$

Der Faktor von xy^{n-1} fällt dann von selbst heraus. Um ebenso das Aggregat:

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

durch $x^3 y^3$ teilbar zu machen, muß man den Faktor von $x^{n-2} y^2$ (welcher bis auf das Vorzeichen gleich dem Faktor 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:

$$x^n - y^n - N_1 (x-y)^n - N_2 xy (x-y)^{n-2} - N_3 x^2 y^2 (x-y)^{n-4} - N_4 x^3 y^3 (x-y)^{n-6}$$

durch $x^4 y^4$ teilbar, 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, daß das Aggregat:

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

durch $x^s y^s$ teilbar ist, wenn N_s durch die Gleichung:

$$N_1 \binom{n}{s-1} - N_2 \binom{n-2}{s-2} + N_3 \binom{n-4}{s-3} - \ldots + (-1)^s N_{s-1} \binom{n-2s+4}{1} + (-1)^{s+1} N_s = 0 \tag{8a}$$

bestimmt wird, welche aussagt, daß in dem Aggregate (8) der Faktor von $x^{n-s+1} y^{s-1}$ (oder $x^{s-1} y^{n-s+1}$) verschwindet; und durch ein Rekursionsverfahren erhält man leicht (wie wir sogleich auch direkt bestätigen werden):

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

Aus der Rekursionsformel (8a) folgt sofort: Sind N_1, N_2, $\ldots N_{s-1}$ ganze Zahlen, so ist auch N_s eine ganze Zahl.

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

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

und wir haben identisch:

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

wo N noch zu bestimmen ist; die linke Seite nämlich ist teilbar durch $x^\nu y^\nu$ und ist gleich Null für $x = y$. Der Wert von N wird schließlich durch Fortsetzung derselben Schlußweise gefunden, die wir bisher anwandten, nämlich 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:

$$N = N_{\nu+1} = 2\nu + 1 = n. \tag{11}$$

Zwischen beliebigen Zahlen x und y besteht hiernach die folgende Identität:

$$nx^{\nu}y^{\nu}(x-y) = x^n - y^n - (x-y)^n - \sum_{s=2}^{s=\nu} N_s x^{s-1} y^{s-1} (x-y)^{n-2s+2}. \tag{12}$$

Ist n eine Primzahl, so sind nach obigem N_2 und N_3 durch n teilbar; aus der Rekursionsformel (8^a) folgt also dann:

Die in der Identität (11) auftretenden und durch (9) gegebenen Zahlen N_s sind sämtlich ganze Zahlen und (wenn $s > 1$) durch die Primzahl n teilbar.

Die Bestimmung der Zahlenfaktoren N_s hätte übrigens auch in der folgenden einfachen Weise geschehen können, indem man x und y durch spezielle Werte ersetzt und so die Aufgabe auf ein bekanntes Resultat zurückführt. Nehmen wir

$$x = e^{i\varphi},\ y = -e^{-i\varphi},$$

so wird:

$$x \cdot y = -1,\ \ x - y = 2 \cdot \cos\varphi,\ \ x^n - y^n = 2 \cdot \operatorname{cosin} n\varphi;$$

und aus (12) folgt (für n ungerade):

$$\operatorname{cosin} n\varphi = 2^{n-1} \operatorname{cosin}^n \varphi + \sum_{s=2}^{\nu} N_s 2^{n-2s+1} (-1)^{s-1} (\operatorname{cosin}\varphi)^{n-2s+2} + n(-1)^{\nu} \operatorname{cosin}\varphi;$$

und diese Formel ist in der Tat mit der bekannten Entwicklung von cosin $n\varphi$ nach Potenzen von cosin φ identisch,[1]) wenn man unter N_s die obigen Zahlenwerte versteht.

---

[1]) Vgl. z. B. Serret, Traité d'algèbre, vol. 1, Nr. 109.

§ 3. Die Abelschen Formeln.

Setzen wir nun in (12) für z und $x - y$ die Werte (5) und (6) ein, so ergibt sich die Relation:

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

oder, wenn beiderseits mit ϱr^n dividiert wird:

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

wobei die Zahlen N_i sämtlich ganze Zahlen sind.

Die relativen Primzahlen x und y können wegen (6) mit den Zahlen $r_1, r_2, \ldots r_{n-1}$ keinen Faktor gemein haben. Jedes Glied der rechten Seite von (13) ist durch jede dieser Zahlen teilbar, 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 $r_1, r_2, \ldots r_{n-1}$ teilbar sein, so muß die Zahl n diese Faktoren 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 nämlich dann die rechte Seite von (13) mindestens durch n^2 teilbar, folglich auch die linke Seite; d. h. es müßte x oder y durch n teilbar sein; dann aber wären nach (6) beide Zahlen

durch n teilbar, während sie doch als relative Primzahlen vorausgesetzt sind. Die Zahl r_n bleibt zunächst beliebig.

Da die Gleichung (12), wenn N_s durch (9) bestimmt wird, eine Identität ist, können wir in ihr y durch z ersetzen und erhalten so in Rücksicht auf (6^a) und (7^a) an Stelle von (13) die Beziehung:

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

auf welche wir die gleichen Überlegungen anwenden können, Es ist also entweder:

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

oder:

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

Endlich können wir in der Identität (12) auch x durch y und y durch $-z$ ersetzen; dann ergibt sich mit Rücksicht auf (6^b) und (7^b):

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

und die nochmalige Wiederholung der gleichen Schlußweise führt zu dem Resultate, daß entweder:

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

oder:

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

sein muß.

Da x, y, z keinen gemeinsamen Faktor enthalten sollen, so ergibt die Kombination der Gleichungen (15), (17), (15^a), (17^a), (15^b), (17^b), daß nur drei Fälle noch näher zu untersuchen sind. Die Annahme (15) nämlich ist mit (15^a) oder (15_b) nicht vereinbar, so daß aus der Annahme (15) notwendig die Gleichungen (17^a) und (17^b) folgen. Gehen wir aber von (17) aus, so kann sowohl (15^a) als (15^b) möglich sein. Betrachten wir diejenigen Möglichkeiten als gleichwertig, die durch Ver-

tauschung von y mit z auseinander hervorgehen, so bleiben die folgenden drei Fälle:

$$\begin{aligned}
&\text{I)} \quad && x - y = r^n \cdot n^{n-1}, && z = n \cdot r \cdot r_n,\\
&&& x - z = q^n, && y = q \cdot q_n,\\
&&& y + z = p^n, && x = p \cdot p_n;\\
&\text{II)} && x - y = r^n, && z = r \cdot r_n,\\
&&& x - z = q^n, && y = q \cdot q_n,\\
&&& y + z = p^n \cdot n^{n-1}, && x = n \cdot p \cdot p_n;\\
&\text{III)} && x - y = r^n, && z = r \cdot r_n,\\
&&& x - z = q^n, && y = q \cdot q_n,\\
&&& y + z = p^n, && x = p \cdot p_n.
\end{aligned}$$

Hieraus folgt im Falle I):

$$\begin{aligned}
x &= \tfrac{1}{2}(p^n + q^n + n^{n-1} r^n),\\
\text{I}^a) \qquad y &= \tfrac{1}{2}(p^n + q^n - n^{n-1} r^n),\\
z &= \tfrac{1}{2}(p^n - q^n + n^{n-1} r^n),
\end{aligned}$$

im Falle II):

$$\begin{aligned}
x &= \tfrac{1}{2}(n^{n-1} p^n + q^n + r^n),\\
\text{II}^a) \qquad y &= \tfrac{1}{2}(n^{n-1} p^n + q^n - r^n),\\
z &= \tfrac{1}{2}(n^{n-1} p^n - q^n + r^n),
\end{aligned}$$

und im Falle III):

$$\begin{aligned}
x &= \tfrac{1}{2}(p^n + q^n + r^n),\\
\text{III}^a) \qquad y &= \tfrac{1}{2}(p^n + q^n - r^n),\\
z &= \tfrac{1}{2}(p^n - q^n + r^n).
\end{aligned}$$

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

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

$$x = \tfrac{1}{2}[p^n + n^{n-1}(q^n + r^n)],$$
$$y = \tfrac{1}{2}[p^n + n^{n-1}(q^n - r^n)],$$
$$z = \tfrac{1}{2}[p^n - n^{n-1}(q^n - r^n)],$$

welche bei uns ausgeschlossen ist, da sie auf das nicht statthafte Zusammenbestehen der Gleichungen (15) und (15ª) führen würde.

§ 4. Der Fall I); Darstellung von x, y, z.

Wir machen zuerst die Annahme I). Die Gleichung (13ª) 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 nach obigem durch n teilbar; auch z ist durch n teilbar; vom dritten Gliede ab sind also alle Terme der rechten Seite durch n^2 teilbar. Die linke Seite ist mindestens durch $n^{\nu+1}$ teilbar; folglich ist auch:

$$(19) \qquad q_n^n - q^{n(n-1)} \equiv 0 \mod n^2.$$

Nach dem Fermatschen Satze ist:

$$(20) \qquad q^{n(n-1)} \equiv 1 \mod n^2,$$

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

$$q_n^n \equiv 1 \mod n^2,$$

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

$$(21) \qquad q_n \equiv 1 \mod n.$$

Ebenso folgt aus (13ᵇ):

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

und die Anwendung derselben Schlußweise führt zu der Kongruenz:

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

Folglich ist auch:

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

Ferner ist:

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

also auch:

$$p^n \equiv q^n \mod n^2. \tag{25}$$

Weiter folgt aus den Gleichungen I):

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

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

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

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

Setzen wir die der Annahme I) entsprechenden, in (14) und (15) gegebenen Werte 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:

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

Wäre also $r_n \equiv 0 \mod n$, so müßte eine der Zahlen x oder y durch n teilbar sein, was nicht angeht. Es kann

also nur r den Faktor n enthalten und r_n kann nicht durch n teilbar sein. Es muß also r den Faktor n enthalten, so daß wir:

$$r = n \cdot r' \tag{29}$$

zu setzen haben, und z mindestens durch n^2 teilbar ist. Es wird dann:

$$\begin{aligned} x^\nu y^\nu &= r_n^n - \sum_{i=1}^{\nu} N_i x^{i-1} y^{i-1} r'^n (n-2i+1) n^{2n^2-(4i-1)n+2i-2} \\ &= r_n^n - r'^n(n-1)\, n^{2n^2-3n} - \ldots - N_\nu x^{\nu-1} y^{\nu-1} r'^{2n} n^{4n-3}, \end{aligned} \tag{29a}$$

oder, da N_ν nach obigem durch n teilbar ist:

$$x^\nu y^\nu \equiv r_n^n \mod. n^{4n-2}. \tag{30}$$

Da aber nach I):

$$x - y = n^{n-1} r^n = n^{2n-1} r'^n \tag{30a}$$

ist, so haben wir auch:

$$x^\nu - y^\nu \equiv n^{2n-1} \cdot \nu \cdot r'^n \cdot y^{\nu-1} \mod. n^{4n-2},$$

also nach (30):

$$y^\nu (y^\nu + \nu n^{2n-1} r'^n y^{\nu-1}) \equiv r_n^n \mod. n^{4n-2}$$

oder, wenn wir sogleich die entsprechende Kongruenz für x hinzufügen:

$$\begin{aligned} y^{n-1} &\equiv r_n^n - \nu n^{2n-1} r'^n y^{2\nu-1} \mod. n^{4n-2}, \\ x^{n-1} &\equiv r_n^n + \nu n^{2n-1} r'^n x^{2\nu-1} \quad , \quad n^{4n-2}. \end{aligned} \tag{30b}$$

Nach I) war ferner:

$$\begin{aligned} x &= q^n + z = q^n + n^{2n} r'^n r_n^n, \\ y &= p^n - z = p^n - n^{2n} r'^n r_n^n; \end{aligned}$$

die Zahlen $p^{n(n-1)} - 1$ und $q^{n(n-1)} - 1$ sind durch n^2 teilbar; folglich haben wir:

$$x^{n-1} \equiv y^{n-1} \equiv 1 \mod. n^2,$$

und somit aus (30b):

$$r_n^n \equiv 1 \mod n^2$$

und weiter:

$$r_n \equiv 1 \mod n. \tag{30^c}$$

Von diesem Resultate werden wir weiterhin Gebrauch machen, nachdem wir zuvor die Zahlen x, y, z noch in anderer Weise werden dargestellt haben.

Nach dem Fermatschen Satze und infolge der Relationen (21) und (23) können wir setzen:

$$\begin{aligned} p^{n-1} &= 1 + n\pi, & q^{n-1} &= 1 + n\varkappa, \\ p_n &= 1 + n\pi', & q_n &= 1 + n\varkappa'. \end{aligned} \tag{31}$$

Es wird dann, wenn noch $r = n \cdot r'$ gesetzt wird:

$$\begin{aligned} x - z &= pp_n - nrr_n = pp_n - n^2 r' r_n, \\ y + z &= qq_n + nrr_n = qq_n + n^2 r' r_n. \end{aligned} \tag{32}$$

Die linken Seiten sind wegen I) bzw. gleich q^n und p^n; also folgt:

$$\begin{aligned} q^n &= q + nq\varkappa = p + np\pi' - n^2 r' r_n, \\ p^n &= p + np\pi = q + nq\varkappa' + n^2 r' r_n, \end{aligned}$$

und hieraus:

$$p - q - n^2 r' r_n = n(q\varkappa - p\pi') = n(q\varkappa' - p\pi), \tag{32^a}$$

oder:

$$p(\pi' - \pi) + q(\varkappa' - \varkappa) = 0.$$

Es bestehen demnach zwei Gleichungen der folgenden Form:

$$\begin{aligned} Mp &= (\varkappa' - \varkappa), \\ Mq &= -(\pi' - \pi); \end{aligned} \tag{33}$$

und hierin ist M eine ganze Zahl, denn p und q können keinen gemeinsamen Faktor enthalten, da sonst nach I) auch x und y denselben Faktor enthalten müßten.

Zu den Gleichungen (32) fügen wir aus I) die dritte hinzu:

$$x - y = n^{2n-1} r'^n = pp_n - qq_n = p - q + n(p\pi' - q\varkappa'). \tag{33^a}$$

Der Vergleich mit (32ª) zeigt, daß auch die Relation:

$$\frac{p-q}{n} = q\varkappa - p\pi' + nr'r_n = q\varkappa' - p\pi + nr'r_n$$
$$= q\varkappa' - p\pi' + n^{2n-2}r'^n$$

bestehen muß. Multiplizieren wir beiderseits mit M und benutzen die Gleichungen (33), so folgt:

$$(33^b) \quad M(r_n - n^{2n-3}r'^{n-1})r' \cdot n = -(\varkappa - \varkappa')(\pi - \pi').$$

Es ist also mindestens eine der beiden Zahlen $(\varkappa - \varkappa')$ und $(\pi - \pi')$ durch n teilbar; dann aber ist nach (33) M durch n teilbar (da p und q den Faktor n nicht enthalten dürfen), und es folgt aus denselben Gleichungen (33), daß auch die andere dieser beiden Zahlen den Faktor n enthält. Es bestehen demnach die Kongruenzen:

$$(33^c) \qquad \pi' \equiv \pi, \quad \varkappa' \equiv \varkappa \mod n,$$

so daß die Gleichungen (31) durch die folgenden ersetzt werden dürfen:

$$(34) \quad \begin{aligned} p^{n-1} &= 1 + n\pi, & q^{n-1} &= 1 + n\varkappa, \\ p_n &= 1 + n\pi + n^2\pi_1, & q_n &= 1 + n\varkappa + n^2\varkappa_1. \end{aligned}$$

Bildet man wieder die Ausdrücke $x - z$ und $y + z$, so ergibt sich jetzt aus I):

$$q^n = q + nq\varkappa = p + np\pi + n^2p\pi_1 - n^2r'r_n,$$
$$p^n = p + np\pi = q + nq\varkappa + n^2q\varkappa_1 + n^2r'r_n,$$

und hieraus an Stelle von (32ª):

$$(35) \quad p - q + n(p\pi - q\varkappa) - n^2r'r_n = -n^2p\pi_1 = n^2q\varkappa_1.$$

Es ist folglich auch:

$$(36) \qquad -p\pi_1 = q\varkappa_1.$$

Die dritte Gleichung (nämlich $x - y = n^{2n-1}r'^n$) gibt jetzt:

$$n^{2n-1}r'^n = pp_n - qq_n = p - q + n(p\pi - q\varkappa) + n^2(p\pi_1 - q\varkappa_1).$$

Wir haben so die Differenz $p - q$ auf doppelte Weise berechnet; es ist:

$$(37)\qquad \begin{aligned} p-q &= -n(p\pi - q\varkappa) + n^2 r' r_n - n^2 p\pi_1 \\ &= -n(p\pi - q\varkappa) + n^{2n-1} r'^n - n^2(p\pi_1 - q\varkappa_1); \end{aligned}$$

und somit erhalten wir, unter Benutzung von (36):

$$(38)\qquad q\varkappa_1 = -p\pi_1 = r' r_n - n^{2n-3} r'^n.$$

Da x, y, z zueinander relativ prim sind, so können keine zwei der Zahlen p, q und r' einen gemeinsamen Faktor enthalten; bezeichnet R eine ganze Zahl, so kann man deshalb setzen:

$$(39)\qquad \pi_1 = -qRr',\ \varkappa_1 = pRr',\ r_n - n^{2n-3} r'^{n-1} = pqR.$$

Die Gleichungen (34) werden demnach:

$$(40)\qquad \begin{aligned} p_n &= p^{n-1} - n^2 q r' R, \\ q_n &= q^{n-1} + n^2 p r' R. \end{aligned}$$

Es wird somit nach I) und I[a]):

$$(41)\qquad \begin{aligned} 2x &= p^n + q^n + n^{2n-1} r'^n = 2p^n - 2n^2 pqr' R, \\ 2y &= p^n + q^n - n^{2n-1} r'^n = 2q^n + 2n^2 pqr' R, \\ 2z &= p^n - q^n + n^{2n-1} r'^n = 2n^{2n-1} r'^n + 2n^2 pqr' R. \end{aligned}$$

Aus jeder dieser Relationen folgt:

$$(42)\qquad p^n - q^n = 2n^2 pqr' R + n^{2n-1} r'^n,$$

was sich in Übereinstimmung damit befindet, daß die Differenz $p^n - q^n$ nach (25) durch n^2 teilbar sein muß.

§ 5. Der Fall I), wenn r' nicht durch n teilbar ist.

Unter Anwendung der Gleichungen (31) erhalten wir aus (41) durch Potenzieren:

$$(43)\qquad \begin{aligned} x^{n-1} &\equiv 1 + n^2(\pi + qRr') \\ y^{n-1} &\equiv 1 + n^2(\varkappa - pRr') \end{aligned} \quad \text{mod. } n^3.$$

Da nun $x - y$ nach I) durch n^{2n-1} teilbar ist, so folgt durch Subtraktion:[1])

[1]) Dasselbe Resultat findet man, wenn man die Differenz $p^{n^2} - q^{n^2}$ einmal aus den Gleichungen (41) und (3) bildet, das anderemal durch Potenzieren aus der Gleichung (42).

$$(44) \quad \varkappa - \pi \equiv (p+q)\,Rr' \equiv 2p\,Rr' \equiv 2q\,Rr' \mod n.$$

Wir kehren nunmehr zu dem in der Kongruenz (30^c) vorliegenden Resultate zurück. Mit Rücksicht auf den in (39) gegebenen Wert von r_n ist:

$$(45) \qquad r_n^n \equiv p^n q^n R^n \mod n^{2n-2},$$

also nach (30^c):

$$(46) \qquad pqR \equiv 1 \mod n,$$

woraus hervorgeht, daß R nicht durch n teilbar sein kann. Setzen wir demnach:

$$(47) \qquad R^{n-1} = 1 + n\varrho,$$

wodurch die Zahl ϱ definiert sei, so wird nach (31):

$$(48) \quad p^{n-1} q^{n-1} R^{n-1} \equiv 1 + n(\pi + \varkappa + \varrho) \mod n^2,$$

und folglich wegen (46):

$$(49) \qquad pqR \equiv 1 - n(\pi + \varkappa + \varrho) \mod n^2,$$

und durch Potenzieren:

$$(49^a) \qquad p^n q^n R^n \equiv 1 - n^2(\pi + \varkappa + \varrho) \mod n^3.$$

Nach (30^b) ist ferner:

$$(49^b) \qquad x^{n-1} \equiv y^{n-1} \equiv r_n^n \mod n^{2n-1},$$

also infolge von (45) und (49):

$$(50) \quad x^{n-1} \equiv y^{n-1} \equiv 1 - n^2(\pi + \varkappa + \varrho) \mod n^3;$$

und der Vergleich mit (43) läßt jetzt die Kongruenzen (44) in folgender Weise schreiben:

$$\pi + \varkappa + \varrho \equiv -\varkappa + pRr' \equiv -\pi - qRr' \mod n,$$

und hieraus erhalten wir:

$$(51) \qquad \begin{aligned} 2\pi + \varkappa + \varrho &\equiv -qRr' \mod n, \\ \pi + 2\varkappa + \varrho &\equiv pRr' \quad \text{„} \quad n. \end{aligned}$$

Von den hier zuletzt abgeleiteten Relationen, d. h. den Kongruenzen (48) bis (51), werden wir keinen Gebrauch weiter machen; man würde indessen auf sie

rekurrieren müssen, wenn man das Produkt pqR nicht, wie es nunmehr zunächst geschehen soll, auf das Produkt $p^r q^r$ reduziert.

Unsere Relation (28) erlaubt noch weitere Schlüsse; gemäß den Gleichungen I) können wir x durch $z + q^n$ und y durch $p^n - z$ ersetzen; dann ist:

$$(51^b) \qquad \begin{aligned} x^r y^r &= (z+q^n)^r (p^n - z)^r = [p^n q^n + z(p^n - q^n) - z^2]^r \\ &\equiv p^{nr} q^{nr} \mod n^4, \end{aligned}$$

denn $p^n - q^n$ ist nach (42) durch n^2 teilbar und z enthält ebenfalls den Faktor n^2. Wir erhalten somit aus (28) bzw. (30):

$$(52) \qquad p^{nr} q^{nr} \equiv r_n^n \mod n^4,$$

also auch:

$$(52^a) \qquad p^r q^r \equiv r_n \mod n^3,$$

und nach (39):

$$(53) \qquad p^r q^r \equiv pqR \mod n^3;$$

folglich gemäß (42):

$$(53^a) \qquad p^n - q^n \equiv 2n^2 pqr' R \equiv 2n^2 p^r q^r r' \mod n^5.$$

Ersetzen wir andererseits in der allgemeinen Identität (12) die Zahlen x und y bzw. durch p und q, so wird:

$$(53^b) \qquad \begin{aligned} &npq(p-q) \\ &= p^n - q^n - (p-q)^n - \sum_{s=2}^{r} N_s p^{s-1} q^{s-1} (p-q)^{n-2s+2}, \end{aligned}$$

folglich:

$$(53^c) \qquad p^n - q^n \equiv npq(p-q) \mod n^4,$$

und durch Vergleichung mit (53^a):

$$(54) \qquad p - q \equiv 2nr' \mod n^3.$$

Mit Hilfe dieser Kongruenz können wir zunächst ein früheres Resultat bestätigen; es ergibt sich nämlich aus (42), daß man setzen darf:

$$(54^a) \qquad p - q = 2pqr' Rn + \delta n^2,$$

wo δ eine Zahl bezeichnet, die sich durch Potenzieren, d. h. durch Zurückgehen auf (42) leicht bestimmen läßt; es wird nämlich:

$$p^n - q^n \equiv 2n^2 pqr' Rq^{n-1} + 4n^3 \nu (pqr' R)^2 q^{n-2} + \delta n^3 q^{n-1} \quad \text{mod. } n^4$$

$$\equiv 2n^2 pqr' R + n^3 [2\varkappa r' - 2r'^2 q^{n-2} + \delta] \quad \text{mod. } n^4,$$

wobei benutzt ist, daß pqR nach (47) im Faktor von n^3 durch 1 ersetzt werden darf. Durch Vergleichung mit (42) folgt dann:

$$(54^b) \qquad \delta \equiv 2r'^2 q^{n-2} - 2\varkappa r' \quad \text{mod. } n.$$

Mittels (49) erhalten wir daher aus (54^a):

$$(54^c) \quad p - q \equiv 2r'n + 2n^2 r' [r' q^{n-2} - \varkappa - (\pi + \varkappa + \varrho)] \quad \text{mod. } n^3.$$

Hier muß nach (54) die eckige Klammer durch n teilbar sein; d. h. wir haben:

$$\pi + 2\varkappa + \varrho \equiv r' q^{n-2} \quad \text{mod. } n.$$

Multiplizieren wir beiderseits mit q, so kommen wir wegen der Relation (46) auf die Kongruenz (51) zurück, wodurch letztere von neuem bewiesen wird.

Aus den drei Kongruenzen, von denen die dritte eine Folge der Relationen (46) und (30^c) ist:

$$p^{2\nu} \equiv 1, \quad q^{2\nu} \equiv 1, \quad p^\nu q^\nu \equiv 1 \quad \text{mod. } n,$$

folgt, daß man:

$$(55) \qquad p^\nu \equiv q^\nu \equiv \varepsilon \quad \text{mod. } n$$

setzen darf, wenn ε eine Zahl bezeichnet, die entweder durch $+1$ oder durch -1 in Bezug auf den Modul n ersetzt werden darf. Sei also:

$$(55^a) \qquad p^\nu = \varepsilon + n\pi', \quad q^\nu = \varepsilon + n\varkappa',$$

so folgt durch Quadrieren:

$$(56) \qquad \pi = 2\varepsilon\pi' + n\pi'^2, \quad \varkappa = 2\varepsilon\varkappa' + n\varkappa'^2.$$

Zunächst soll die Kongruenz (44) für das Quadrat des Moduls n ergänzt werden. Es ist nach (53^a), (54) und (55^a):

$$(57)\qquad \begin{aligned} p^n - q^n &= p - q + n(p\pi - q\varkappa) \\ &\equiv 2n^2 r' p^\nu q^\nu \equiv 2n^2 r'[1 + \varepsilon(\pi' + \varkappa')n + n^2\pi'\varkappa'] \\ &\qquad \text{mod. } n^5. \end{aligned}$$

Die linke Seite ist nach (54) in Bezug auf den Modul n^3:

$$\begin{aligned} &\equiv 2nr' + n\pi(q + 2nr') - nq\varkappa \\ &\equiv 2nr' + nq(\pi - \varkappa) + 2n^2 r'\pi. \end{aligned}$$

Wir erhalten also:

$$(57^a)\qquad q(\pi - \varkappa) \equiv -2r' + 2nr'(1 - \pi) \quad \text{mod. } n^2$$

und ebenso, indem man p und q vertauscht:

$$(57^b)\qquad p(\pi - \varkappa) \equiv -2r' + 2nr'(1 - \varkappa) \quad \text{mod. } n^2.$$

Die eine dieser Kongruenzen geht aus der anderen durch Anwendung der Relation (54) hervor.

Auch die Kongruenz (54) können wir für die nächst höhere Potenz des Moduls erweitern. Setzen wir:

$$(58)\qquad p - q = 2nr' + r'\vartheta n^3,$$

so läßt sich ϑ durch folgende Überlegung bis auf Vielfache von n bestimmen. Nach (58) ist:

$$\begin{aligned} (58^a)\quad p^n - q^n \equiv{}& 2n^2 r' q^{n-1} + r'\vartheta n^4 q^{n-1} + 4n^3 \nu r'^2 q^{n-2} \\ &+ 8n^3 \binom{n}{3} r'^3 q^{n-3} \quad \text{mod. } n^5. \end{aligned}$$

Der Vergleich mit (57) ergibt dann:

$$\begin{aligned} &2\varkappa + n\vartheta + 4\nu r' q^{n-2} + 8\binom{n}{3} r'^2 q^{n-3} \\ &\equiv 2\varepsilon(\pi' + \varkappa') + 2n\pi'\varkappa' \quad \text{mod. } n^2, \end{aligned}$$

oder, wenn wir 2ν durch $n - 1$ und $\varkappa$ gemäß (56) durch $2\varepsilon\varkappa' + n\varkappa'^2$ ersetzen:

$$\begin{aligned} (58^b)\qquad 2\varepsilon(\varkappa' - \pi') \equiv{}& 2r' q^{n-2} - n\Big[\vartheta + 2\varkappa'^2 + 2r' q^{n-2} \\ &+ 8\binom{n}{3}\frac{1}{n} r'^2 q^{n-3} - 2\pi'\varkappa'\Big] \quad \text{mod. } n^2. \end{aligned}$$

Rechts und links addieren wir die Zahl $n(\varkappa'^2 - \pi'^2)$, multiplizieren mit q und ersetzen im ersten Gliede rechts q^{n-1} durch $1 + n\varkappa$; dann wird:

$$(\varkappa - \pi)\, q \equiv 2r' - n\left[\vartheta q + 2r'(1-\varkappa) + (\varkappa' - \pi')^2 q + 8\binom{n}{3}\frac{1}{n} r'^2 q^{n-2}\right] \mod n^2.$$

Auf der rechten Seite ist gemäß (57ª):

$$-2r'\varkappa \equiv -2r'\pi - 4r'^2 q^{n-2} \mod n,$$

ferner nach (58ᵇ):

$$(\varkappa' - \pi')^2 \equiv r'^2 q^{2n-4} \equiv r'^2 q^{n-3} \mod n.$$

Ferner ist:

$$8\binom{n}{3}\frac{1}{n} - 3 = 4\frac{(n-1)(n-2)}{3} - 3 \equiv -\frac{1}{n}\binom{n}{3} \mod n.$$

Es ergibt sich somit:

$$(\pi - \varkappa)\, q \equiv -2r' + n\left[\vartheta q + 2r'(1-\pi) - \frac{1}{n}\binom{n}{3} r'^2 q^{n-2}\right] \mod n^2. \tag{58ᶜ}$$

Diese Kongruenz muß mit (57ª) übereinstimmen; es folgt also:

$$\vartheta \equiv \frac{(n-1)(n-2)}{2\cdot 3} r'^2 q^{n-3} \mod n, \tag{59}$$

so daß die vervollständigte Kongruenz (54) lautet:

$$p - q \equiv 2nr' + n^3 \frac{(n-1)(n-2)}{2\cdot 3} r'^3 q^{n-3} \mod n^4. \tag{59ª}$$

Die vorstehende Betrachtung erleidet eine Ausnahme im Falle $n = 3$; dann nämlich lautet die Kongruenz (58ᶜ), da die Zahl $\binom{n}{3}$ dann gleich 1, also nicht durch n teilbar ist:

$$(\pi - \varkappa)\, q \equiv -2r' - r'^2 q^{n-2} \mod 3,$$

und die Vergleichung mit (57ª) oder (44) führt zu dem Resultate: $r' \equiv 0 \mod 3$.

Das entsprechende Resultat läßt sich für jede Primzahl n gewinnen. Wenden wir die Kongruenz (59) auf die Kongruenz (58ª) an, so ergibt sich:

$$p^n - q^n = p - q + n(p\pi - q\varkappa)$$

$$\equiv 2n^2 r' q^{n-1} + 4n^3 r r'^2 q^{n-2} + 9n^3 \binom{n}{3} r'^3 q^{n-3} \mod n^5$$

und die linke Seite ist nach (59ª):

$$\equiv 2nr' + n^2 \binom{n}{3} r'^3 q^{n-3} + nq(\pi - \varkappa) + 2n^2 \pi r' \mod n^4.$$

Wir erhalten also:

$$(\pi - \varkappa) q \equiv -2r' + 2nr'(1 - \pi)$$

$$(60) \quad + n^2 r' \left[2\varkappa + 2(n-1) r' q^{n-2} - \frac{1}{n} \binom{n}{3} r'^2 q^{n-3} \right] \mod n^3,$$

womit die Kongruenz (57ª) für den Modul n^3 vervollständigt ist. Setzt man dann weiter:

$$(60^a) \qquad p - q = 2nr' + n^3 r' \vartheta + n^4 \vartheta_1,$$

so läßt sich in analoger Weise ϑ_1 bestimmen, indem man durch Potenzieren den Ausdruck $p^n - q^n$ bildet und das Resultat mit demjenigen vergleicht, wie es sich ergeben würde, wenn man den Wert von $p - q$ in die Identität (53ᵇ) einsetzt. Man erhält so einen zu (58ᶜ) analogen Ausdruck für $\pi - \varkappa$, der mit dem Ausdrucke (60) übereinstimmen muß, woraus sich dann eine Berechnung von ϑ_1 (bis auf Vielfache von n) ergibt. Offenbar kann man mit einem solchen Pendelverfahren fortfahren, und so die Kongruenzen (60) und (60ª) für immer höhere Potenzen des Moduls ergänzen.

Zur Durchführung dieser Schlußreihen ist es notwendig, die in (57) benutzte Kongruenz (53) zuvor für höhere Potenzen des Moduls sukzessive zu erweitern. Das kann auf folgende Weise geschehen. Infolge der Annahme (3) ist, wenn wir die Werte von x, y, z aus (41) einsetzen:

$$(p^n - n^2 p q R r')^n - (q^n + n^2 p q R r')^n \equiv 0 \mod n^{2n},$$

also:

$$p^{n^2} - q^{n^2} \equiv n^3 p q r' R (p^{n(n-1)} + q^{n(n-1)})$$
$$- n^5 \nu p^3 q^3 r'^2 R^2 (p^{n(n-2)} - q^{n(n-2)}) \mod n^7.$$

Die zweite Klammer der rechten Seite ist durch n^2, das betreffende Glied also durch n^7 teilbar; es wird somit einfach:

$$p^{n^2} - q^{n^2} \equiv n^3 p q R r' [2 + n^2 (\pi + \varkappa) + n^3 \nu (\pi^2 + \varkappa^2)] \mod n^7,$$

oder, wenn wir entsprechend (53), den Wert:

$$(60^b) \qquad p q R = p^\nu q^\nu (1 + n^3 \eta)$$

einführen, wo η eine zu bestimmende Zahl bezeichnet:

$$p^{n^2} - q^{n^2} \equiv 2 n^3 p^\nu q^\nu r' + n^5 p^\nu q^\nu (\pi + \varkappa) r' + 2 n^6 r' p^\nu q^\nu \eta$$
$$+ n^3 \nu (\pi^2 + \varkappa^2) \mod n^7.$$

So erhalten wir eine Kongruenz, durch welche die ganze Zahl η definiert und mittels der Zahlen $p, q, \pi, \varkappa$ ausgedrückt ist; die wirkliche Berechnung von η kann aber einfacher in folgender Weise geschehen. Aus (51^b) erhalten wir, da gemäß (52^a):

$$(60^c) \qquad z = n^2 r' r_n \equiv n^2 r' p^\nu q^\nu \mod n^5$$

gesetzt werden darf, unter Benutzung von (53^a):

$$(60^d) \qquad x^\nu y^\nu \equiv [p^n q^n + n^4 r'^2 p^{2\nu} q^{2\nu}]^\nu \mod n^7,$$

also nach (30):

$$r_n^n \equiv p^{n\nu} q^{n\nu} + n^4 \nu r'^2 p^{2\nu + n(\nu-1)} q^{2\nu + n(\nu-1)} \mod n^7,$$

und zufolge (39) lautet sonach die vervollständigte Kongruenz (53):

$$p q R \equiv r_n \equiv p^\nu q^\nu + n^3 \nu r'^2 p^{\nu-1} q^{\nu-1} \mod n^6.$$

Die Vergleichung mit (60^b) ergibt demnach:

$$\eta \equiv \nu r'^2 p^{\nu-1} q^{\nu-1} \mod n,$$

so daß die vervollständigte Kongruenz (53) jetzt lautet:

$$(60^e) \qquad p q R \equiv p^\nu q^\nu [1 + n^3 \nu r'^2 p^{\nu-1} q^{\nu-1}] \mod n^4.$$

Mit Hilfe dieses Resultates ist man in der Lage, die Kongruenz (57) für den Modul n^6 aufzustellen; sie lautet:

$$(60^f)\qquad \begin{aligned} p^n - q^n &\equiv 2\,n^2 r' p\,q\,R \mod n^{2n-1} \\ &\equiv 2\,n^2 r' p^r q^r + 2\,n^{5\nu} r'^3 p^{2\nu-1} q^{2\nu-1} \mod n^6. \end{aligned}$$

Um ϑ_1 zu bestimmen, hat man also diesen Ausdruck (60^f) mit demjenigen zu vergleichen, der sich aus (60^a) durch Potenzieren ergibt; das führt zu einer Relation für $\pi - \varkappa$ für den Modul n^3, die mit (60) übereinstimmen muß, woraus dann ϑ_1 gefunden wird; und mit Hilfe dieses Wertes gelingt es weiter, mittels der Kongruenz (60^b) und durch eine zu (60^d) analoge Relation, die Kongruenz (60^e) auf den Modul n^5 und dadurch die Kongruenz (60^f) auf den Modul n^7 zu erweitern; u. s. f.

Nehmen wir an, es sei gefunden:

$$(61)\qquad p - q = r'(2\,n + n^3\,\vartheta + n^4\,\vartheta_1 + \ldots + n^s\,\vartheta_{s-3}),$$

wo nun alle Zahlen ϑ_i bis auf ϑ_{s-3} bekannt sind: es handle sich also um die Bestimmung von ϑ_{s-3}; dann wird, wenn wir die rechte Seite dieser Gleichung mit Θ_s bezeichnen und wenn:

$$(61^a)\qquad \Theta_i = r'(2\,n + n^3\,\vartheta + \ldots + n^i\,\vartheta_{i-3})$$

gesetzt wird:

$$(61^b)\qquad \begin{aligned} p^n - q^n &\equiv n\,\Theta_s\,q^{n-1} \\ &+ \binom{n}{2}\Theta_{s-1}^2\,q^{n-2} + \ldots + \binom{n}{s-2}\Theta_3^{s-2}\,q^{n-s+2} \\ &+ \binom{n}{s-1}(2\,n\,r')^{s-1}\,q^{n-s+1} + \binom{n}{s}(2\,n\,r')^s\,q^{n-s} \\ &\mod n^{s+2}. \end{aligned}$$

Ferner setzen wir voraus, man habe gefunden:

$$(61^c)\qquad (\pi - \varkappa)\,q \equiv -2\,r' + Q_1\,n + Q_2\,n^2 + \ldots + Q_{s-2}\,n^{s-2} \mod n^{s-1}.$$

Endlich habe man gefunden, und zwar durch sukzessive Erweiterung der Kongruenzen (53) und (60^e):

$$(61^d)\qquad p\,q\,R \equiv p^r q^r (1 + n^3\,\eta + n^4\,\eta_1 + \ldots + n^{s-1}\,\eta_{s-4}) \mod n^s,$$

also nach (42):

$$(61^e)\quad p^n - q^n \equiv 2n^3 r'[1 + \varepsilon(\pi' + \varkappa')n + n^2\pi'\varkappa'](1 + n^3\eta + \ldots + n^{s-1}\eta_{s-4}) \mod n^{s+2}.$$

Subtrahiert man nun die Kongruenzen (61^b) und (61^e) voneinander, so muß wieder die obige Kongruenz (61^c) entstehen, nachdem beiderseits mit $n^3 r'$ dividiert und mit q multipliziert wurde. Der Faktor von n^{s-2} in der so gebildeten neuen Kongruenz enthält die unbekannte Zahl ϑ_{s-3}, und diese ist dadurch bestimmt. Diese Zahl ϑ_{s-3} kommt nämlich auf der rechten Seite von (61^b) nur im ersten Gliede, nämlich in Θ_s, vor und ist hier in $r' n^{s+1} q^{n-1}$ multipliziert; bei Bildung der genannten Differenz erscheint ϑ_{s-3} also auch nur im Faktor der höchsten Potenz von n, d. h. (da mit n^3 dividiert wurde) im Faktor von n^{s-2}; die Zahlen η_i in (61^e) enthalten die Unbekannte ϑ_{s-3} nicht. Die so gefundene neue Form der Kongruenz (61^c) lautet also:

$$(62)\quad (\pi - \varkappa)q \equiv -2r' + Q_1 n + Q_2 n^2 + \ldots + Q_{s-3} n^{s-3} + (P + \vartheta_{s-3} q) n^{s-2} \mod n^{s-1},$$

wo sich die Zahl P aus den bekannten Zahlen ϑ_i und η_i zusammensetzt, und zwar kommen in P alle diejenigen Zahlen aus der rechten Seite von (61^b) vor, welche dort in n^{s+1} multipliziert sind. Zu ihnen gehört auch das Glied:

$$\binom{n}{s}(2nr')^s q^{n-s},$$

aber nur dann, wenn die Zahl $s < n$ ist; setzen wir also:

$$nP = nP' + \binom{n}{s}(2r')^s q^{n-s},$$

so wird nach (62):

$$(\pi - \varkappa)q \equiv -2r' + Q_1 n + Q_2 n^2 + \ldots + Q_{s-3} n^{s-3} + \left[P' + \frac{1}{n}\binom{n}{s}(2r')^s q^{n-s} + \vartheta_{s-3} q\right] n^{s-2} \mod n^{s-1},$$

wo nun die Zahlen $Q_1, \ldots Q_{s-3}$ durch die vorhergehenden (d. h. die als durchgeführt vorausgesetzten) Rechnungen schon völlig bestimmt sind. Wählt man aber $s = n$, so erhält man:

$$(\pi - \varkappa)\, q \equiv -2r' + Q_1 n + \ldots + [Q_{n-3} + (2r')^n]\, n^{n-3} + (P' + \vartheta_{n-3}\, q)\, n^{n-2} \mod n^{n-1}.$$

Der schon durch die Betrachtung für $s = n - 1$ völlig (d. h. bis auf Vielfache) von n festgelegte Wert von Q_{n-3} müßte also eine nachträgliche Korrektur erfahren, was nicht möglich ist; wir müssen somit schließen, daß die Zahl r' den Faktor n enthalte, daß also die Kongruenz:

$$(62^a) \qquad r' \equiv 0 \mod n$$

erfüllt sei. Die bisher gemachte Annahme, es sei die Zahl r' nicht durch n teilbar, erweist sich somit als nicht haltbar; die aus der Kongruenz (62^a) weiter zu ziehenden Konsequenzen werden wir im nächsten Paragraphen verfolgen.

§ 6. Der Fall I), wenn r' durch n teilbar ist.

Das Resultat (62^a) ergibt nun zufolge der Kongruenz (44) unmittelbar:

$$(62^b) \qquad \pi - \varkappa \equiv 0 \mod n,$$

also auch nach (56):

$$(62^c) \qquad \pi' - \varkappa' \equiv 0 \mod n$$

und weiter nach (55^a):

$$p^\nu \equiv q^\nu \equiv \varepsilon \mod n^2.$$

Dann aber folgt aus (52^a) und (53):

$$r_n \equiv p^{2\nu} \equiv p\, q\, R \mod n^2$$

und folglich erhalten wir aus (49):

$$\pi \equiv -(\pi + \varkappa + \varrho) \mod n,$$

wie sich jetzt auch aus (51) ergeben würde. Um nun ein Rekursionsverfahren durchführen zu können, ersetzen wir die Kongruenzen (62^a), (62^c), (62^b) durch die folgenden Relationen:

$$(63) \quad r' = r_1 n^\lambda, \quad p^\nu \equiv q^\nu \equiv \varepsilon \mod n^{\lambda+1}, \quad p^{n-1} - q^{n-1} = \mu\, n^{\lambda+1};$$

wir wollen zeigen, daß dann entsprechende Relationen auch gültig sein müssen, wenn man λ durch $\lambda + 1$ ersetzt.

Wir befolgen dabei genau die im Falle $\lambda = 0$ angewandte Schlußweise und werden, um die Analogie deutlich hervortreten zu lassen, die gleichen Nummern für die einzelnen Gleichungen und Kongruenzen verwenden, indem wir nur einen Stern hinzufügen.

Setzen wir in die Relation (29ª) für r' den Wert $n^\lambda r_1$ ein, so ergibt sich:

$$(30)^* \qquad x^\nu y^\nu \equiv r_n^n \mod n^{(2\lambda+4)n-2};$$

nun ist jetzt:

$$(30^a)^* \qquad x - y = n^{2n-1} r'^n = n^{(\lambda+2)n-1} r_1^n,$$

also:

$$x^\nu - y^\nu \equiv n^{(\lambda+2)n-1} \cdot r_1^n \cdot \nu \cdot y^{\nu-1} \mod n^{(2\lambda+4)n-2};$$

und nach (30)*:

$$(30^b)^* \qquad \begin{aligned} y^{n-1} &\equiv r_n^n - \nu\, n^{(\lambda+2)n-1} \cdot r_1^n \cdot y^{2\nu-1} \\ x^{n-1} &\equiv r_n^n + \nu\, n^{(\lambda+2)n-1} \cdot r_1^n \cdot x^{2\nu-1} \end{aligned} \mod n^{(2\lambda+4)-2}.$$

Infolge der Ansätze (63) ist das Produkt $p^\nu q^\nu$ in Bezug auf den Modul $n^{\lambda+1}$ mit 1 äquivalent; aus den Gleichungen:

$$x = q^n + z = q^n + n^{(\lambda+2)n} r_1^n r_n^n$$
$$y = p^n - z = p^n - n^{(\lambda+2)n} r_1^n r_n^n$$

ergibt sich also:

$$x^\nu y^\nu \equiv p^{n\nu} q^{n\nu} \equiv 1 \mod n^{\lambda+2},$$

und somit aus (30):

$$(30^c)^* \qquad r_n \equiv 1 \mod n^{\lambda+1}.$$

Weiterhin folgten in § 5 zunächst Überlegungen, bei denen nicht Kongruenzen, sondern Gleichungen benutzt wurden, die also hier sich unverändert wiederholen lassen. Wir finden so die folgenden Resultate:

$$(39)^* \qquad r_n = p\,q\,R + n^{(\lambda+2)(n-1)-1} r_1^{n-1}$$

und:

$$(41)^* \qquad \begin{aligned} x &= p^n - n^{\lambda+2} p\, q\, r_1\, R, \\ y &= q^n + n^{\lambda+2} p\, q\, r_1\, R, \\ z &= n^{(\lambda+2)n-1} r_1^n + n^{\lambda+2} p\, q\, r_1\, R; \end{aligned}$$

aus jeder dieser Relationen folgt jetzt:

$$(42)^* \qquad p^n - q^n = 2\, n^{\lambda+2} p\, q\, r_1\, R + n^{(\lambda+2)n-1} r_1^n.$$

Die Gleichungen (43) werden jetzt:

$$(43)^* \qquad \begin{aligned} x^{n-1} &\equiv p^{n(n-1)} + n^{\lambda+2} q\, R\, r' \\ y^{n-1} &\equiv q^{n(n-1)} - n^{\lambda+2} p\, R\, r' \end{aligned} \quad \text{mod. } n^{\lambda+3}$$

und durch Subtraktion erhalten wir gemäß (63):

$$(44)^* \quad p^{n(n-1)} - q^{n(n-1)} = n^{\lambda+2}\, \mu \equiv 2\, q\, R\, r'\, n^{\lambda+2} \text{ mod. } n^{\lambda+3},$$

oder:

$$(44^a)^* \qquad \mu \equiv 2\, q\, R\, r' \equiv 2\, p\, R\, r' \text{ mod. } n,$$

Aus (39)* erhalten wir:

$$(45)^* \qquad r_n \equiv p\, q\, R \text{ mod. } n^{(\lambda+2)n-3},$$

also nach $(30^c)^*$:

$$(46)^* \qquad p\, q\, R \equiv 1 \text{ mod. } n^{\lambda+1}.$$

Es gilt die Gleichung bzw. Kongruenz:

$$(51^b)^* \qquad \begin{aligned} x^\nu\, y^\nu &= (z + q^n)^\nu\, (p^n - z)^\nu = [p^n\, q^n + z\,(p^n - q^n) - z^2]^\nu \\ &\equiv p^{n\nu} q^{n\nu} \text{ mod. } n^{2\lambda+4}, \end{aligned}$$

denn die Zahlen z und $p^n - q^n$ sind hier je durch $n^{\lambda+2}$ teilbar. Aus (30)* ergibt sich somit:

$$(52^a)^* \qquad r_n \equiv p^\nu\, q^\nu \text{ mod. } n^{2\lambda+3}$$

und nach (39)* bzw. (45)*

$$(53)^* \qquad p^\nu\, q^\nu \equiv p\, q\, R \text{ mod. } n^{2\lambda+3},$$

folglich gemäß (42)*:

$$(53^a)^* \qquad p^n - q^n \equiv 2\, n^{\lambda+2} p^\nu\, q^\nu\, r_1 \text{ mod. } n^{3\lambda+5}.$$

Die Gleichung (53^b) gilt unverändert, und aus ihr folgt jetzt, da $p - q$ durch $n^{\lambda+1}$ teilbar ist:

$$(53^c)^* \qquad p^n - q^n \equiv n\,p^\nu\,q^\nu\,(p-q) \mod n^{3\lambda+4},$$

also durch Vergleichung mit $(53^a)^*$:

$$(54)^* \qquad p - q \equiv 2\,n^{\lambda+1}\,r_1 \mod n^{3\lambda+3}.$$

Nach $(30^c)^*$ und $(52^a)^*$ haben wir die schon benutzte Relation:

$$(54^a)^* \qquad p^\nu\,q^\nu \equiv 1 \mod n^{\lambda+1}.$$

Nun ist nach (54)* die Differenz $p-q$, also auch die Differenz $p^\nu - q^\nu$ durch $n^{\lambda+1}$ teilbar; es folgt deshalb aus $(54^a)^*$:

$$p^{n-1} \equiv q^{n-1} \equiv 1 \mod n^{\lambda+1},$$

d. h. es ist zu setzen:

$$\pi = n^\lambda\,\pi_1, \quad \varkappa = n^\lambda\,\varkappa_1,$$

und aus den Relationen:

$$p^{2\nu} \equiv q^{2\nu} \equiv p^\nu\,q^\nu \equiv 1 \mod n^{\lambda+1}$$

folgt dann weiter:

$$(55^a)^* \qquad p^\nu = \varepsilon + n^{\lambda+1}\,\pi_1', \quad q^\nu = \varepsilon + n^{\lambda+1}\,\varkappa_1'$$

also:

$$(56)^* \qquad \pi_1 = 2\,\varepsilon\,\pi_1' + n^{\lambda+1}\,\pi_1'^2, \quad \varkappa_1 = 2\,\varepsilon\,\varkappa_1' + n^{\lambda+1}\,\varkappa_1'^2.$$

An Stelle von (57) erhalten wir daher:

$$(57)^* \qquad \begin{gathered} p - q + n^{\lambda+1}\,(p\,\pi_1 - q\,\varkappa_1) \\ \equiv 2\,n^{\lambda+2}\,r_1\,[1 + \varepsilon\,n^{\lambda+1}\,(\pi_1' + \varkappa_1') + n^{2\lambda+2}\,\pi_1'\,\varkappa_1'] \\ \mod n^{3\lambda+5}. \end{gathered}$$

Nach (54)* ist die linke Seite (mod. $n^{3\lambda+3}$):

$$\equiv 2\,n^{\lambda+1}\,r_1 + n^{\lambda+1}\,\pi_1\,(q + 2\,n^{\lambda+1}\,r_1) - n^{\lambda+1}\,q\,\varkappa_1,$$

so daß wir erhalten:

$$(57^a)^* \qquad q\,(\pi_1 - \varkappa_1) \equiv -2\,r_1 + 2\,n\,r_1 - 2\,n^{\lambda+1}\,r_1\,\pi_1 \mod n^{2\lambda+2}.$$

Jetzt sind wir in der Lage, die Kongruenz (54)* für den nächst höheren Modul zu erweitern; wir setzen:

$$(58)^* \qquad p - q = 2\,n^{\lambda+1}\,r_1 + r_1\,\vartheta_1\,n^{3\lambda+3},$$

wo nun ϑ_1 zu bestimmen ist. Zunächst ergibt sich:

$$p^n - q^n \equiv 2\,n^{\lambda+2} r_1 q^{n-1} + 4\,n^{2\lambda+3}\nu r_1^2 q^{n-2}$$

$$(58^a)^* \qquad + 8\,n^{3\lambda+3}\binom{n}{3} r_1^3 q^{n-3} + r_1 \vartheta_1 n^{3\lambda+4} q^{n-1}$$

$$\text{mod. } n^{4\lambda+5}.$$

Durch Vergleichung mit (57)* erhalten wir also (nach Division mit $r_1 n^{2\lambda+3}$):

$$2\varkappa_1 + n^{\lambda+1}\vartheta_1 + 4\nu r_1 q^{n-2} + 8\binom{n}{3} r_1 n^{\lambda} q^{n-3}$$

$$\equiv 2\varepsilon(\varkappa_1' + \varkappa_1') + 2\,n^{\lambda+1}\pi_1'\varkappa_1' \quad \text{mod. } n^{2\lambda+2},$$

oder nach (56)*:

$$2\varepsilon(\varkappa_1' - \pi_1') \equiv 2 r_1 q^{n-2} - 2\,n\,r_1 q^{n-2}$$

$$(58^b)^* - n^{\lambda+1}\left[\vartheta_1 + 2\varkappa_1'^2 + 2 r_1 q^{n-2} + 8\binom{n}{3}\frac{1}{n} r_1^2 q^{n-2} - 2\pi_1'\varkappa_1'\right]$$

$$\text{mod. } n^{2\lambda+2}$$

und, wenn wir links π_1 und $\varkappa_1$ einführen und mit q multiplizieren:

$$(\varkappa_1 - \pi_1) q \equiv 2 r_1 - 2\,n\,r_1 q^{n-1}$$

$$(58^c)^* - n^{\lambda+1}\left[\vartheta_1 q + 2 r_1 \varkappa_1 + (\varkappa_1' - \pi_1')^2 q + 8\binom{n}{3}\frac{1}{n} r_1^2 q^{n-2}\right]$$

$$\text{mod. } n^{2\lambda+2},$$

oder endlich, wenn wir in der eckigen Klammer die Relation $(58^b)^*$ zur Umformung benutzen, und im zweiten Gliede der rechten Seite q^{n-1} durch $1 + n^{\lambda+1}\varkappa_1$ ersetzen:

$$(\pi_1 - \varkappa_1) q \equiv -2 r_1 + 2\,n\,r_1$$

$$(58^d)^* \quad + n^{\lambda+1}\left[\vartheta_1 q + 2 r_1 \varkappa_1 + r_1^2 q^{n-2} + 8\binom{n}{3}\frac{1}{n} r_1^2 q^{n-2}\right]$$

$$\text{mod. } n^{\lambda+2}.$$

Indem man die rechte Seite mit der rechten Seite von $(57^a)^*$ vergleicht, ergibt sich die Bestimmung von ϑ_1. Eine Ausnahme tritt im Falle $n = 3$ ein, da man dann das Glied mit dem Faktor $\binom{n}{3}$ nicht in die eckige Klammer bringen kann; dann lautet vielmehr die letzte Kongruenz:

$$(\pi_1 - \varkappa_1)\, q \equiv -2 r_1 + 2 \cdot 3\, r_1 + 8 \cdot 3^{\lambda} r_1^3 q + 3^{\lambda+1} [\vartheta_1 q + 2 r_1 \varkappa_1 + r_1^2 q] \mod 3^{\lambda+2},$$

und jetzt folgt durch Vergleichung mit (57ª):

$$r_1 \equiv 0 \mod 3.$$

Von hier ab kann die Reihe von Schlüssen unseres Rekursionsverfahrens in ganz gleicher Weise wie oben durchgeführt werden; man setze:

$$(60^{a})^* \qquad p - q = 2 n^{\lambda+1} r_1 + r_1 \vartheta_1 n^{3\lambda+3} + r_1 \vartheta_1' n^{3\lambda+4}$$

und verfahre in ganz entsprechender Weise, so wird man die Zahl ϑ_1' bis auf Vielfache von n bestimmen können. Es ist dabei nur nötig, auch die Kongruenz (53)* für immer höhere Moduln zu erweitern. Zu dem Zwecke gehen wir wieder von der Gleichung $x^n = y^n + z^n$ aus; das Einsetzen der Werte (41)* gibt eine Relation, die zur Definition von η_1 dienen kann, wenn wir gemäß (53)* setzen:

$$(60^{b})^* \qquad p\, q\, R = p^{\nu}\, q^{\nu}\, (1 + n^{2\lambda+3}\, \eta_1).$$

Einfacher geschieht die Bestimmung von η_1 wieder auf folgende Weise. Auf Grund der Kongruenz (52ª)* haben wir:

$$(60^{c})^* \qquad z = n^{\lambda+2} r_1\, r_n \equiv n^{\lambda+2} r_1\, p^{\nu}\, q^{\nu} \mod n^{3\lambda+5},$$

also nach (51ᵇ)* und (53ª)*:

$$(60^{d})^* \qquad \begin{aligned} x^{\nu}\, y^{\nu} &\equiv [p^n\, q^n + n^{2\lambda+4} r_1^3 p^{2\nu} q^{2\nu}]^{\nu} \mod n^{4\lambda+7} \\ &\equiv p^{n\nu}\, q^{n\nu} + n^{2\lambda+4} \cdot \nu \cdot r_1^3 (p\, q)^{2\nu+n(\nu-1)} \mod n^{4\lambda+7}, \end{aligned}$$

also nach (30)*:

$$r_n^n \equiv p^{n\nu}\, q^{n\nu} + n^{2\lambda+4} \cdot \nu \cdot r_1^2\, p^{n\nu-1}\, q^{n\nu-1} \mod n^{4\lambda+7}$$

und somit:

$$r_n \equiv p^{\nu}\, q^{\nu} + n^{2\lambda+3} \cdot \nu \cdot r_1^2\, p^{\nu-1}\, q^{\nu-1} \mod n^{4\lambda+6},$$

folglich nach (39)* und (54ª)*:

$$(60^{e})^* \qquad \begin{aligned} p\, q\, R &\equiv p^{\nu}\, q^{\nu} + n^{2\lambda+3} \cdot \nu \cdot r_1^2\, p^{\nu-1}\, q^{\nu-1} \mod n^{4\lambda+6} \\ &\equiv p^{\nu}\, q^{\nu} + n^{2\lambda+3} \cdot \nu \cdot r_1^2\, p^{2\nu-1}\, q^{2\nu-1} \mod n^{3\lambda+4}, \end{aligned}$$

wodurch η_1 bestimmt ist:

$$\eta_1 \equiv \nu r_1^2 p^{\nu-1} q^{\nu-1} \mod. n^{\lambda+1},$$

und die Kongruenz (53ª)* kann nun auch für einen höheren Modul aufgestellt werden; sie lautet dann:

$$(60^f)^* \quad p^n - q^n \equiv 2 n^{\lambda+2} r_1 p^\nu q^\nu + 2 n^{3\lambda+5} \nu r_1^3 p^{2\nu-1} q^{2\nu-1} \mod. n^{4\lambda+6}.$$

Durch ein Pendelverfahren, analog demjenigen, das am Schlusse von § 5 eingehend geschildert wurde, wird man so die Kongruenzen für die Werte von $p - q$, von $\pi - \varkappa$ und von $p^n - q^n$ auf immer höhere Potenzen des Moduls n erweitern können. Ist man bei der Kongruenz für $p - q$, d. h. in (58)*, bis zum Modul $n^{n\lambda+n+1}$ gelangt, so daß der Koeffizient von $n^{n\lambda+n}$ bestimmt werden soll, so tritt in der entsprechenden Kongruenz (58ª)* rechts das Glied:

$$2^n n^{n\lambda+n} \binom{n}{n} r_1^n$$

auf, das einen Faktor n weniger enthält, als man nach dem Verlauf der Rechnungen bis zu diesem Modul erwarten durfte, indem der Binomialkoeffizient $\binom{n}{s}$ für $s < n$ durch n teilbar ist, für $s = n$ aber nicht. Hierdurch ist es dann wieder bedingt, daß sich bei Aufstellung der Kongruenz für $\pi_1 - \varkappa_1$, d. h. der zu (58ᶜ)* analogen Kongruenz, für den Modul:

$$n^{(n+1)\lambda+n+2-(2\lambda+3)} = n^{(n-1)\lambda+n-1}$$

ein Glied ergibt, welches die schon vollständig definierten Glieder der entsprechenden niedrigeren Kongruenz noch beeinflussen würde, welches also noch einen Faktor n mehr enthalten muß; und dies kann nur erreicht werden, wenn der andere Faktor dieses Gliedes, der sich aus einer Potenz von r_1 und einer Potenz von q zusammensetzt, den Faktor n enthält. Wir kommen so, da q nicht durch n teilbar sein kann, zu dem Schlusse (vgl. auch unten § 12):

$$r_1 \equiv 0 \mod. n.$$

Aus (44)* folgt dann, daß $\pi_1 - \varkappa_1$ durch $n^{\lambda+1}$, und aus (55ª)*, daß $p^r - q^r$ durch $n^{\lambda+1}$ teilbar sein muß, d. h. daß die Relationen (63) für die Zahl $\lambda + 1$ bestehen, wenn sie für die Zahl λ gelten.

Wenn man also annimmt, es sei r' durch n^λ teilbar, so folgt, daß r' auch durch $n^{\lambda+1}$ teilbar ist. Die Zahl r' ist somit durch jede beliebige Potenz von n teilbar, d. h. wir haben:

$$r' = 0.$$

Dann aber geben die Gleichungen (41) bzw. (41)*:

$$x = p^n, \quad y = q^n, \quad z = 0$$

und aus (42) folgt: $p^n = q^n$.

Wenn also die drei Zahlen x, y, z der Gleichung:

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

genügen, so kann z (und ebenso y) nicht durch n teilbar sein, es sei denn, daß die betreffende Zahl gleich Null ist, wo sich dann die genannte Gleichung auf eine Identität reduziert.

§ 7. Der Fall II).

Der Fall II) läßt sich in genau der gleichen Weise erledigen. Aus den Identitäten (13) und (17ª) erhalten wir bzw.:

$$\begin{aligned} n\,x^\nu\,y^\nu &= r_n^n - \sum_{i=1}^{\nu} N_i\,x^{i-1}\,y^{i-1}\,r^{n(n-2i+1)}, \\ n\,x^\nu\,z^\nu &= q_n^n - \sum_{i=1}^{\nu} N_i\,x^{i-1}\,z^{i-1}\,q^{n(n-2i+1)}, \end{aligned} \tag{64}$$

und schließen aus ihnen, wie in (21), (23) und (24) die Kongruenzen:

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

also auch, entsprechend zu (25):

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

ferner aus II[a]):

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

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

$$(-1)^r y^r z^r = p_n^n - p^{n(n-1)} n^{n(n-2)}$$

$$(64^a) \quad + \sum_{i=2}^{r} (-1)^i N_i x^{i-1} y^{i-1} p^{n(n-2i+1)} n^{n^2-2in+2i-2}.$$

Hieraus folgt, wie oben entsprechend aus (28), daß p durch n teilbar sein muß, während p_n den Faktor n nicht enthalten kann. Wir setzen demnach:

$$x = n \cdot p p_n = n^2 p' p_n.$$

An Stelle von (29) haben wir hier die Gleichungen:

$$(65) \quad \begin{aligned} q^{n-1} &= 1 + n\varkappa, & r^{n-1} &= 1 + n\varrho, \\ q^n &= 1 + n\varkappa', & r^n &= 1 + n\varrho', \end{aligned}$$

und an Stelle von (30):

$$(66) \quad \begin{aligned} x - y &= r^n = n^2 p' p_n - q q_n, \\ x - z &= q^n = n^2 p' p_n - r r_n, \end{aligned}$$

also infolge von (35):

$$\begin{aligned} r^n &= r + n r \varrho = n^2 p' p_n - q - n q \varkappa', \\ q^n &= q + n q \varkappa = n^2 p' p_n - r - n r \varrho', \end{aligned}$$

somit:

$$(67) \quad q + r - n^2 p' p_n = -n(r\varrho + q\varkappa') = -n(r\varrho' + q\varkappa).$$

An Stelle von (32) erhalten wir also:

$$(68) \quad q(\varkappa' - \varkappa) = r(\varrho' - \varrho),$$

und an Stelle von (33):

$$(69) \quad \begin{aligned} Nq &= \varrho' - \varrho, \\ Nr &= \varkappa' - \varkappa, \end{aligned}$$

wo N eine ganze Zahl bezeichnet. Die Berechnung der Summe $y + z$ gibt hier:

$$n^{2n-1}p'^n = qq_n + rr_n = q + r + n(q\varkappa' + r\varrho');$$

analog zu (33) erhalten wir hieraus:

$$N(p_n - n^{2n-3}p'^{n-1})p' \cdot n = -(\varrho - \varrho')(\varkappa - \varkappa'),$$

und daran lassen sich dieselben Schlüsse anknüpfen, wie oben an die entsprechende Gleichung, so daß wir zu dem Ansatze:

$$(70)\quad \begin{aligned} q^{n-1} &= 1 + n\varkappa, & r^{n-1} &= 1 + n\varrho, \\ q_n &= 1 + n\varkappa + n^2\varkappa_1, & r_n &= 1 + n\varrho + n^2\varrho_1 \end{aligned}$$

berechtigt sind. Die Bildung der Ausdrücke $x - y$ und $x - z$ ergibt jetzt:

$$(71)\quad \begin{aligned} r^n &= r + nr\varrho = p_n p' n^2 - q - nq\varkappa - n^2 q\varkappa_1 \\ q^n &= q + nq\varkappa = p_n p' n^2 - r - nr\varrho - n^2 r\varrho_1, \end{aligned}$$

also:

$$(72)\quad q + r + n(r\varrho + q\varkappa) - p_n p' \cdot n^2 = -n^2 q\varkappa_1 = -n^2 r\varrho_1.$$

Die Summe $y + z = n^{2n-1}p'^n$ gibt hier:

$$n^{2n-1}p'^n = qq_n + rr_n = q + r + n(q\varkappa + r\varrho) + n^2(q\varkappa_1 + r\varrho_1);$$

wir erhalten demnach:

$$(73)\quad \begin{aligned} q + r &= -n(q\varkappa + r\varrho) - n^2(q\varkappa_1 + r\varrho_1) + n^{2n-1}p'^n \\ &= -n(q\varkappa + r\varrho) - n^2 q\varkappa_1 + n^2 p_n p', \end{aligned}$$

und folglich, unter Benutzung von (72):

$$(74)\qquad q\varkappa_1 = r\varrho_1 = -p_n p' + n^{2n-3}p'^n,$$

wodurch wir zu den Gleichungen (P bezeichnet eine ganze Zahl):

$$(75)\quad \varkappa_1 = Prp', \quad \varrho_1 = Pqp', \quad p_n - n^{2n-3}p'^{n-1} = -Pqr$$

geführt werden, aus denen sich sofort die folgenden ergeben:

$$(76)\quad \begin{aligned} 2x &= n^{2n-1}p'^n + q^n + r^n = 2n^{2n-1}p'^n - 2n^2 qrp'P, \\ 2y &= n^{2n-1}p'^n + q^n - r^n = 2q^n + 2n^2 qrp'P, \\ 2z &= n^{2n-1}p'^n - q^n + r^n = 2r^n + 2n^2 qrp'P, \end{aligned}$$

und es ist klar, daß man aus diesen Gleichungen dieselben Schlüsse ziehen kann, wie oben aus den Gleichungen (42), so daß man zu der Annahme $p' = 0$ als der einzig möglichen

geführt wird; bei der Durchführung des Beweises würde es sich nur darum handeln, in den Betrachtungen von § 5 und § 6 einige Buchstaben zu vertauschen und Vorzeichen zu ändern; wir können deshalb diese Wiederholung ersparen. Es folgt so, da y und z positiv vorausgesetzt wurden, auch $q = 0$, $r = 0$. Der Fall II) kann daher, wenn x, y, z positiv vorausgesetzt werden, nicht vorkommen.

§ 8. Hilfsformeln zur Erledigung des Falles III).

Die Erledigung der durch die Gleichungen III) bis III^a) in § 3 gegebenen Möglichkeiten werden wir in § 10 auf den folgenden Satz zurückführen, bzw. auf die zu diesem Satze führenden Formeln:

Sind p, q, r drei nicht durch n teilbare ganze Zahlen, und besteht zwischen ihnen und einer ungeraden Primzahl $n (= 2\nu + 1)$ die Relation:

$$p^n - q^n - r^n \equiv 0 \mod n^2 \tag{77}$$

(d. h. läßt sich von drei Wurzeln der Kongruenz $X^{n-1} \equiv 1 \mod n^2$ eine als Summe der beiden anderen darstellen), so bestehen die Kongruenzen:

$$q^\nu \equiv r^\nu \equiv (-1)^\nu p^\nu \mod n, \tag{77^a}$$

ausgenommen die Fälle, wo $q \equiv r$ oder $p \equiv -r$ oder $p \equiv -q$ ist.

Entsprechend der Kongruenz (77) setzen wir:[1])

$$p^n - q^n - r^n \equiv 2\alpha n^2 \mod n^3, \tag{78}$$

wo α eine ganze Zahl bezeichne, die zunächst nicht durch n teilbar sei. Ersetzen wir nun in der fundamentalen Identität (12) die willkürlichen Zahlen x, y bzw. durch p^n, q^n, so wird:

[1]) Daß auf der rechten Seite von (78) eine gerade Zahl 2α eingeführt wurde, ist keine Spezialisierung, da jede ungerade Zahl durch Hinzufügen von Vielfachen von n zu einer geraden gemacht werden kann und sich dadurch die rechte Seite von (78) nur um Vielfache von n^3 ändern würde.

$$(79)\quad p^{n^2} - q^{n^2} - (p^n - q^n)^n = \sum_{i=2}^{\nu+1} N_i\, p^{n(i-1)}\, q^{n(i-1)}\, (p^n - q^n)^{n-2i+2},$$

und dies ist eine identische Gleichung. Die linke Seite ist nach dem erweiterten Fermatschen Satze mit $p^n - q^n - (p^n - q^n)^n$ in Bezug auf den Modul n^2 äquivalent, also nach (78) mit $p^n - q^n - r^n$ und somit durch n^2 teilbar; die rechte Seite enthält den Faktor n, da nach § 2 alle Zahlen N_i durch n teilbar sind. Setzen wir also:

$$(80)\quad n\,T = \sum_{i=2}^{\nu+1} N_i\, p^{n(i-1)}\, q^{n(i-1)}\, r^{n(n-2i+1)},$$

so ist T eine ganze Zahl, und es wird die rechte Seite von (79) gleich $n\,r^n\,T$, und es folgt:

$$0 \equiv n \cdot r^n \cdot T \mod n^2,$$

also:

$$(81)\quad T \equiv 0 \mod n.$$

Durch Differentiation der Identität (79) nach p^n entsteht die Relation:

$$(82)\quad \begin{aligned} & n\,[p^{n(n-1)} - (p^n - q^n)^{n-1}] \\ &= \sum_{i=2}^{\nu+1} N_i\,(n - 2i + 2)\, p^{n(i-1)}\, q^{n(i-1)}\, (p^n - q^n)^{n-2i+1} \\ &+ \sum_{i=2}^{\nu+1} N_i\,(i-1)\, p^{n(i-2)}\, q^{n(i-1)}\, (p^n - q^n)^{n-2i+2}, \end{aligned}$$

welche ebenfalls identisch erfüllt ist. Setzen wir also:[1])

$$(83)\quad n\,T_1 = \sum_{i=2}^{\nu+1} N_i\,(i-1)\, p^{n(i-2)}\, q^{n(i-2)}\, r^{n(n-2i+1)},$$

wo dann T_1 eine ganze Zahl bedeutet, so wird in Rücksicht auf (77):

$$(83^a)\quad n\,(p^{n(n-1)} - r^{n(n-1)}) \equiv n^2\,T + n\,(q^n r^n - 2\,p^n q^n)\,T_1 \mod n^3.$$

---

[1]) Die hier eingeführten Zahlen T und T_1 werden später zum Unterschiede von anderen analogen Zahlen mit T_r und T_{1r} bezeichnet werden.

Die linke Seite ist wegen der Kongruenzen:

$$p^{n(n-1)} \equiv q^{n(n-1)} \equiv 1 \mod n^2$$

durch n^3 teilbar, T nach (81) durch n; es wird also:

$$(r^n - 2p^n)\, T_1 \equiv 0 \mod n^2, \tag{84}$$

denn der Faktor q^n kann der Voraussetzung nach nicht durch n teilbar sein. Es ist also T_1 durch n^2 teilbar, ausgenommen den Fall, wo die Zahl $r^n - 2p^n$ [$\equiv -(p^n + q^n)$] durch n teilbar ist.

Zu weiteren Resultaten gelangen wir, indem wir auf der linken und rechten Seite von (82) auch die dritte Potenz von n berücksichtigen. Wir führen drei Zahlen π, $\varkappa$, ϱ ein, die durch die folgenden Gleichungen definiert seien:

$$p^{n-1} = 1 + n\pi, \quad q^{n-1} = 1 + n\varkappa, \quad r^{n-1} = 1 + n\varrho. \tag{85}$$

Dann wird auf der linken Seite von (82):

$$\begin{aligned} & n\,[p^{n(n-1)} - (p^n - q^n)^{n-1}] \\ \equiv\ & n\,(p^{n(n-1)} - r^{n(n-1)} + 2a\,n^2\, r^{n(n-2)}) \mod n^4 \\ \equiv\ & n^3\,(\pi - \varrho + 2a\, r^{n-2}) \mod n^4. \end{aligned} \tag{86}$$

Auf der rechten Seite von (82) ist:

$$\begin{aligned} & \sum_{i=2}^{\nu+1} N_i (n - 2i + 2)\, p^{n(i-1)}\, q^{n(i-1)}\, (p^n - q^n)^{n-2i+1} \\ \equiv\ & \sum_{i=2}^{\nu+1} N_i (n - 2i + 2)\, p^{n(i-1)}\, q^{n(i-1)}\, [r^{n(n-2i+1)} \\ & \qquad + 2a\,n^2\,(n - 2i + 1)\, r^{n(n-2i)}] \\ \equiv\ & n^2\, T - 2n\, p^n\, q^n\, T_1 + 2a\, n^3\, p^n\, q^n\, T_2 \mod n^4, \end{aligned} \tag{87}$$

wenn T wieder durch (80) und die ganze Zahl T_2 durch die Gleichung:

$$n\, T_2 = \sum_{i=2}^{\nu} N_i (2i - 1)(2i - 2)\, p^{n(i-2)}\, q^{n(i-2)}\, r^{n(n-2i)} \tag{88}$$

definiert wird (denn das für $i = \nu + 1$ entstehende letzte Glied hat den Faktor $n - 2i + 1$, d. h. den Faktor Null). Die andere Summe auf der rechten Seite von (82) ist nach (78):

$$\sum_{i=2}^{\nu+1} N_i (i-1)\, p^{n(i-2)}\, q^{n(i-1)}\, (p^n - q^n)^{n-2i+2}$$

$$\equiv \sum_{i=2}^{\nu+1} N_i (i-1)\, p^{n(i-2)}\, q^{n(i-1)} \left[r^{n(n-2i+2)} + 2\,a\,n^2\,(n-2i+2)\, r^{n(n-2i+1)} \right]$$

$$\equiv q^n r^n \cdot n\, T_1 - 4\,a\,n^3\, T_3\, q^n \mod n^4,$$

wenn:

$$n\, T_3 = \sum_{i=2}^{\nu+1} N_i (i-1)^2\, p^{n(i-2)}\, q^{n(i-2)}\, r^{n(n-2i+1)}$$

gesetzt wird. Wegen der Relation:

$$(2i-1)(2i-2) = 4(i-1)^2 + 2(i-1)$$

ist aber (da $N_{\nu+1} = n$ war):

$$(88^a) \qquad n\, T_2 r^n = 4\,n\, T_3 + 2\,n\, T_1 - 2\,n^2\,\nu\, p^{n(\nu-1)}\, q^{n(\nu-1)}.$$

Es wird demnach:

$$(89) \qquad \sum_{i=2}^{\nu+1} N_i (i-1)\, p^{n(i-2)}\, q^{n(i-1)}\, (p^n - q^n)^{n-2i+2}$$

$$\equiv n q^n r^n T_1 + 2\,a\,n^3 q^n T_1 - a\,n^2 q^n r^n T_2 \mod n^4.$$

Setzen wir die Werte (86), (87) und (89) in (82) ein, so ergibt sich:

$$(90) \qquad (\pi - \varrho + 2\,a\,r^{n(n-2)})\, n^2 \equiv n\, T + q^n (r^n - 2\,p^n)(T_1 - a\,n^2\, T_2) + 2\,a\,n^2 q^n\, T_1 \mod n^3,$$

wobei zu beachten ist, daß nach (81) die Zahl T durch n, und nach (84) das Produkt:

$$(r^n - 2\,p^n)(T_1 - a\,n^2\, T_2)$$

durch n^2 teilbar ist.

Ähnliche Gleichungen und Kongruenzen erhält man, indem man die Identität (79) nach q^n differenziert und analoge Entwicklungen anstellt. Wenn man aber die so entstehenden Relationen benutzen will, so ergeben sich keine brauchbaren

Resultate, wenn man nicht zuvor noch eine weitere Potenz von n bei der Entwicklung berücksichtigt.

Zur Vereinfachung der Rechnungen ersetzen wir im folgenden die Kongruenz (78) durch die Gleichung:

$$p^n - q^n - r^n = 2an^2. \tag{91}$$

In Rücksicht auf die späteren Untersuchungen, bei denen die Zahl a als durch eine Potenz von n teilbar angenommen wird, empfiehlt es sich, statt der Zahlen π, ϱ die Zahlen p, r beizubehalten. Die Kongruenz (90) lautet dann (da T_1 durch n^2 teilbar ist und da $r^n - 2p^n \equiv -(q^n + r^n)$ mod. n^2 ist):

$$\begin{aligned} &p^{n(n-1)} - r^{n(n-1)} + 2an^2 r^{n(n-2)} \\ &\equiv nT - q^n(q^n + p^n)(T_1 - an^2 T_2) \mod n^3. \end{aligned} \tag{92}$$ [1])

Hierbei ist vorausgesetzt, daß $q^n + p^n$ nicht durch n teilbar sei, denn nur dann ist nach (84) die Zahl T_1 notwendig durch n^2 teilbar. Es soll demnach im folgenden zunächst angenommen werden, daß keine der drei Zahlen $p^n + q^n$, $p^n + r^n$, $q^n - r^n$ durch n teilbar sei.

Differenzieren wir die Identität (79) nach q^n, so wird, analog zu (82):

$$\begin{aligned} &n\left[(p^n - q^n)^{n-1} - q^{n(n-1)}\right] \\ &= -\sum_{i=1}^{\nu+1} N_i (n - 2i + 2) p^{n(i-1)} q^{n(i-1)} (p^n - q^n)^{n-2i+1} \\ &\quad + \sum_{i=2}^{\nu+1} N_i (i-1) p^{n(i-1)} q^{n(i-2)} (p^n - q^n)^{n-2i+2}, \end{aligned} \tag{93}$$

Die eckige Klammer der linken Seite ist hier:

$$\equiv \left[r^{n(n-1)} - q^{n(n-1)} - 2an^2 r^{n(n-2)}\right] \mod n^3$$

und auf der rechten Seite die erste Summe wieder durch (87) gegeben, die zweite Summe unterscheidet sich von der Summe (89) nur um einen Faktor; sie ist also:

---

[1]) Hätten wir in (91) den Faktor von n^2 als ungerade Zahl angenommen, so hätten wir hier rechts und links mit 2 multiplizieren müssen; etwas wesentliches würde dadurch nicht geändert werden.

$$\equiv n\,p^n r^n\,T_1 + 2\,a\,n^3\,p^n\,T_1 - a\,n^3\,p^n r^n\,T_2 \mod n^4,$$

so daß wir erhalten:

$$\begin{aligned}(94)\quad & r^{n(n-1)} - q^{n(n-1)} - 2\,a\,n^2 r^{n(n-2)} \\ & \equiv -n\,T + p^n(r^n + 2q^n)(T_1 - a\,n^2\,T_2) \\ & \equiv -n\,T + p^n(p^n + q^n)(T_1 - a\,n^2\,T_2) \mod n^3.\end{aligned}$$

In allen unseren Rechnungen kommen die Zahlen q und r symmetrisch vor; in vorstehenden Formeln darf daher auch überall q mit r vertauscht werden. Bezeichnen wir demnach mit T_q, T_{1q}, T_{2q} die Zahlen, welche aus T, T_1, T_2 durch diese Vertauschung entstehen, d. h. setzen wir:

$$(95)\quad n\,T_q = \sum_{i=2}^{\nu+1} N_i\,p^{n(i-1)}\,r^{n(i-1)}\,q^{n(n-2i+1)},$$

$$(96)\quad n\,T_{1q} = \sum_{i=2}^{\nu+1} N_i(i-1)\,p^{n(i-2)}\,r^{n(i-2)}\,q^{n(n-2i+1)},$$

$$(97)\quad n\,T_{2q} = \sum_{i=2}^{\nu} N_i(2i-1)(2i-2)\,p^{n(i-2)}\,r^{n(i-2)}\,q^{n(n-2i)},$$

und bezeichnen dementsprechend die früher eingeführten Zahlen T, T_1, T_2 jetzt bzw. mit T_r, T_{1r}, T_{2r}, so bestehen auch die folgenden beiden Kongruenzen:

$$\begin{aligned}(98)\quad & p^{n(n-1)} - q^{n(n-1)} + 2\,a\,n^3\,q^{n(n-2)} \\ & \equiv n\,T_q - r^n(r^n + p^n)(T_{1q} - a\,n^2\,T_{2q}) \mod n^3\end{aligned}$$

und:

$$\begin{aligned}(99)\quad & q^{n(n-1)} - r^{n(n-1)} - 2\,a\,n^2\,q^{n(n-2)} \\ & \equiv -n\,T_q + p^n(p^n + r^n)(T_{1q} - a\,n^2\,T_{2q}) \mod n^3.\end{aligned}$$

Multiplizieren wir die Kongruenz (92) mit p^n, die Kongruenz (93) mit q^n und bilden die Summe, so wird:

$$\begin{aligned}& p^{n^2} - q^{n^2} - r^{n^2} - r^{n(n-1)}(p^n - q^n) + 2\,a\,n^2 r^{n(n-2)}(p^n - q^n) \\ & \equiv n\,T_r(p^n - q^n) \mod n^3,\end{aligned}$$

oder:

$$(100)\quad p^{n^2} - q^{n^2} - r^{n^2} \equiv n\,T_r\,r^n \mod n^3.$$

Dasselbe Resultat erhält man auch leicht direkt aus (79); wie es nach dem Eulerschen Theoreme über homogene Funktionen sein muß. Durch Anwendung der Gleichung (91) auf die Identität (79) und Entwicklung nach Potenzen von n erhalten wir genauer:

$$\begin{aligned} & p^{n^2} - q^{n^2} - r^{n^2} - 2\,a\,n^3\,r^{n(n-1)} \\ & \equiv \sum_{i=2}^{\nu+1} N_i\, p^{n(i-1)}\, q^{n(i-1)}\,(r^n + 2\,a\,n^2)^{n-2i+2} \mod n^5, \end{aligned}$$

oder:

$$\begin{aligned} (100^a) \qquad p^{n^2} - q^{n^2} - r^{n^2} & \equiv 2\,a\,n^3 + n\,r^n\,T_r - 4\,a\,n^3\,p^n\,q^n\,T_{1r} \\ & \equiv 2\,a\,n^3 + n\,r^n\,T_r \mod n^5. \end{aligned}$$

Ebenso ist:

$$(101) \qquad p^{n^2} - q^{n^2} - r^{n^2} \equiv 2\,a\,n^3 + n\,q^n\,T_q \mod n^5,$$

und folglich:

$$(101^a) \qquad r^n\,T_r \equiv q^n\,T_q \mod n^4.$$

Dieselben Rechnungen lassen sich auch durchführen, indem man von der zwischen q^n und r^n, analog zu (79), bestehenden Identität ausgeht; dieselbe lautet:

$$(102)\quad q^{n^2} + r^{n^2} - (q^n + r^n)^n = \sum_{i=2}^{\nu+1} N_i (-1)^{i-1}\, q^{n(i-1)}\, r^{n(i-1)}\,(q^n + r^n)^{n-2i+2}.$$

Setzt man also, analog zu (80):

$$(102^a) \qquad n\,T_p = \sum_{i=2}^{\nu+1} N_i (-1)^{i-1}\, q^{n(i-1)}\, r^{n(i-1)}\, p^{n(n-2i+1)},$$

so folgt wieder:

$$(102^b) \qquad T_p \equiv 0 \mod n.$$

Die Differentiation der Identität (102) nach q^n ergibt:

$$\begin{aligned} & n\,[q^{n(n-1)} - (q^n + r^n)^{n-1}] \\ & = \sum_{i=2}^{\nu+1} N_i (-1)^{i-1} (n - 2i + 2)\, q^{n(i-1)}\, r^{n(i-1)}\,(q^n + r^n)^{n-2i+1} \\ (103) \qquad & + \sum_{i=2}^{\nu+1} N_i (-1)^{i-1} (i-1)\, q^{n(i-2)}\, r^{n(i-1)}\,(q^n + r^n)^{n-2i+2} \\ & \equiv n^2\,T_p + n\,r^n\,(p^n - 2\,q^n)\,T_{1p} \mod n^3, \end{aligned}$$

wenn:

$$(104)\quad n\,T_{1p} = \sum_{i=2}^{\nu+1} N_i (-1)^{i-1} (i-1)\, q^{n(i-2)} r^{n(i-2)} p^{n(n-2i+1)}$$

gesetzt wird; und aus (102) folgt, analog zu (84):

$$(105)\qquad (p^n - 2q^n)\, T_{1p} \equiv 0 \mod n^2.$$

Berücksichtigen wir auch die dritte Potenz von n, so ist die linke Seite von (103):

$$(106)\quad \equiv n\,[q^{n(n-1)} - p^{n(n-1)} - 2\,a\,n^2\, p^{n(n-2)}] \mod n^4.$$

Auf der rechten Seite (103) ist die erste Summe:

$$(107)\quad \equiv n^2\, T_p - 2n\, q^n r^n\, T_{1p} - 2\,a\,n^3\, q^n r^n\, T_{2p} \mod n^4,$$

wenn, analog zu (88):

$$(108)\quad n\,T_{2p} = \sum_{i=2}^{\nu} N_i (-1)^{i-1} (2i-1)(2i-2)\, q^{n(i-2)} r^{n(i-2)} p^{n(n-2i)}.$$

Die zweite Summe auf der rechten Seite von (103) ist:

$$(109)\qquad \equiv n\,p^n r^n\, T_{1p} + 4\,a\,n^3\, T_{3p}\, r^n \mod n^5,$$

wo:

$$n\,T_{3p} = \sum_{i=2}^{\nu+1} N_i (i-1)^2 (-1)^{i-1}\, q^{n(i-2)} r^{n(i-2)} p^{n(n-2i+1)}.$$

Diese Zahl läßt sich auf T_{2p} mittels der zu (88ª) analogen Relation:

$$n\,T_{2p}\,p^n = 4n\,T_{3p} + 2n\,T_{1p} - 2n^2\nu(-1)^\nu\, q^{n(\nu-1)} r^{n(\nu-1)}$$

zurückführen; folglich wird der Ausdruck (109):

$$(110)\quad \equiv n\,p^n r^n\, T_{1p} - 2\,a\,n^3 r^n\, T_{1p} + a\,n^3 p^n r^n\, T_{2p} \mod n^4.$$

Durch Einsetzen der Werte (106), (107) und (110) in die Identität (103) findet man (da T_{1p} durch n^2 teilbar ist):

$$(111)\quad \begin{aligned} &q^{n(n-1)} - p^{n(n-1)} - 2\,a\,n^2\, p^{n(n-2)} \\ &\equiv n\,T_p - r^n (q^n - r^n)(T_{1p} + a\,n^2\, T_{2p}) \mod n^4. \end{aligned}$$

Durch Vertauschung von q mit r ergibt sich ebenso:

$$(112)\quad \begin{aligned} &r^{n(n-1)} - p^{n(n-1)} - 2\,a\,n^2\, p^{n(n-2)} \\ &n\,T_p + q^n (q^n - r^n)(T_{1p} + a\,n^2\, T_{2p}) \mod n^4. \end{aligned}$$

Durch Anwendung der Gleichung (91) auf die Identität (102), erhalten wir ferner die zu (100ª) analoge Kongruenz:

$$(113) \qquad p^{n^2} - q^{n^2} - r^{n^2} \equiv 2\,a\,n^3 - n\,T_p\,p^n \mod n^5.$$

Die Kongruenz (101ª) können wir demnach in der folgenden Form erweitern; es ist:

$$(114) \qquad -p^n\,T_p \equiv q^n\,T_q \equiv r^n\,T_r \mod n^4.$$

Die hier aufgestellten Kongruenzen sind sämtlich eine Folge der Gleichung (91), unter der Voraussetzung, daß keine der Zahlen $p^n + q^n$, $p^n + r^n$, $q^n - r^n$ durch n teilbar sei.

Um die Übersicht zu erleichtern, wollen wir noch folgende Bezeichnungen einführen; es sei:

$$(114^a) \qquad \begin{aligned} (q^n - r^n)\,(T_{1p} + a\,n^2\,T_{2p}) &= n^2\,S_p, \\ (r^n + p^n)\,(T_{1q} - a\,n^2\,T_{2q}) &= n^2\,S_q, \\ (q^n + p^n)\,(T_{1r} - a\,n^2\,T_{2r}) &= n^2\,S_r. \end{aligned}$$

Die Kongruenzen (92), (94), (98), (99), (111), (112) lauten dann (mod. n^3):

$$(115) \quad p^{n(n-1)} - r^{n(n-1)} + 2\,a\,n^2\,r^{n(n-2)} \equiv n\,T_r - n^2\,q^n\,S_r,$$

$$(115^a) \quad r^{n(n-1)} - q^{n(n-1)} - 2\,a\,n^2\,r^{n(n-2)} \equiv -n\,T_r + n^2\,p^n\,S_r,$$

$$(115^b) \quad p^{n(n-1)} - q^{n(n-1)} + 2\,a\,n^2\,q^{n(n-2)} \equiv n\,T_q - n^2\,r^n\,S_q,$$

$$(115^c) \quad q^{n(n-1)} - r^{n(n-1)} - 2\,a\,n^2\,q^{n(n-2)} \equiv -n\,T_q + n^2\,p^n\,S_q,$$

$$(115^d) \quad q^{n(n-1)} - p^{n(n-1)} - 2\,a\,n^2\,p^{n(n-2)} \equiv n\,T_p - n^2\,r^n\,S_p,$$

$$(115^e) \quad r^{n(n-1)} - p^{n(n-1)} - 2\,a\,n^2\,p^{n(n-2)} \equiv n\,T_p + n^2\,q^n\,S_p.$$

Multiplizieren wir nun (115) mit r^n, (115^b) mit q^n und bilden die Summe, so ergibt sich:

$$\begin{aligned} &p^{n(n-1)}(q^n + r^n) - r^{n^2} - q^{n^2} + 2\,a\,n^2\,(r^{n(n-1)} + q^{n(n-1)}) \\ &\equiv n\,(r^n\,T_r + q^n\,T_q) - n^2\,q^n\,r^n\,(S_r + S_q) \mod n^3, \end{aligned}$$

oder, da $q^n + r^n = p^n - 2\,a\,n^2$ ist:

$$(116) \qquad \begin{aligned} p^{n^2} - q^{n^2} - r^{n^2} + 2\,a\,n^2 &\equiv n\,(r^n\,T_r + q^n\,T_q) \\ &- n^2\,q^n\,r\,(S_r + S_q) \mod n^3. \end{aligned}$$

Analog erhält man aus (115[a]) und (115[d]), indem man bzw. mit r^n und p^n multipliziert und die Summe bildet:

$$r^{n^2} - p^{n^2} - q^{n(n-1)}(r^n - p^n) - 2an^2(r^{n(n-1)} + p^{n(n-1)})$$
$$\equiv n(p^n T_p - r^n T_r) + n^2 p^n r^n (S_r - S_p) \mod n^3,$$

oder:

$$p^{n^2} - q^{n^2} - r^{n^2} + 2an^2 \equiv n(r^n T_r - p^n T_p) - n^2 p^n r^n (S_r - S_p) \mod n^3, \tag{117}$$

endlich analog durch Vertauschung von q mit r, wobei S_p sein Zeichen wechselt, oder direkt aus (115[c]) und (115[e]):

$$p^{n^2} - q^{n^2} - r^{n^2} + 2an^2 \equiv n(q^n T_q - p^n T_p) - n^2 p^n q^n (S_q + S_p) \mod n^3. \tag{118}$$

In Rücksicht auf (113) lassen sich diese letzten Kongruenzen in folgender Form schreiben:

$$p^{n^2} - q^{n^2} - r^{n^2} + 2an^2 - 2nr^n T_r \equiv 2an^2 - nr^n T_r$$
$$\equiv n^2(S_p - S_r)p^n r^n \equiv -n^2(S_p + S_q)q^n p^n$$
$$\equiv -n^2 q^n r^n (S_q + S_r) \mod n^3, \tag{119}$$

und hieraus leitet man die folgende Relation ab:

$$S_p p^n \equiv S_r r^n - S_q q^n \mod n. \tag{120}$$

Multiplizieren wir jetzt die Kongruenz (115) mit r^n, (115[e]) mit p^n und bilden die Summe, so wird unter Benutzung von (114):

$$nr^n T_r - n^2 q^n r^n S_r + n^2 p^n q^n S_p + np^n T_p$$
$$\equiv n^2 q^n (S_p p^n - S_r r^n) \equiv (r^n - p^n)(p^{n(n-1)} - r^{n(n-1)}) \mod n^3, \tag{120[a]}$$

also nach (120) und (91), oder direkt aus (115[b]) und (115[c]):

$$p^{n(n-1)} - r^{n(n-1)} \equiv n^2 S_q q^n \mod n^3; \tag{121}$$

ebenso ist:

$$p^{n(n-1)} - q^{n(n-1)} \equiv n^2 S_r r^n \mod n^3. \tag{121[a]}$$

und, indem man (115[a]) mit r^n, (115[c]) mit q^n multipliziert, ergibt sich durch Subtraktion:

$$q^{n(n-1)} - r^{n(n-1)} \equiv -n^2 S_p p^n \mod n^3. \tag{121[b]}$$

Vermöge dieser drei Relationen werden die Kongruenzen (115) . . . (115^e) auf die Relationen (119) und (120) reduziert.

Die von uns aufgestellten Gleichungen und Kongruenzen sind sämtlich Folge des Bestehens der Gleichung (91) bzw. der Kongruenz (78). Für die Anwendung, welche wir im Auge haben, ist es wichtig, die Kongruenz (77) mit der Kongruenz:

$$p^{n^2} - q^{n^2} - r^{n^2} \equiv 0 \mod n^3 \tag{122}$$

in Verbindung zu bringen. Es fragt sich, ob beide Kongruenzen gleichzeitig bestehen können.

Infolge von (122) sind nach (100^a), bzw. (101) oder (113) jetzt die Zahlen T_r, T_q und T_p durch n^2 teilbar. Wir setzen:

$$p^{n^2} - q^{n^2} - r^{n^2} = 2\gamma n^3. \tag{123}$$

Dann ist nach (113) und (114):

$$2\gamma n^2 \equiv 2\alpha n^2 - p^n T_p \equiv 2\alpha n^2 + r^n T_r \mod n^4. \tag{123^a}$$

Alle vorstehenden Überlegungen und Rechnungen können in ganz derselben Weise durchgeführt werden, wenn man überall p^n, q^n, r^n, bzw. durch p^{n^2}, q^{n^2}, r^{n^2} ersetzt. Besteht die Relation (123), d. h. wird gleichzeitig α durch γn ersetzt, so hat man offenbar in allen vorstehenden Kongruenzen die Potenz des Moduls um eine Einheit zu erhöhen.[1]) Seien also T_r', S_r' die Zahlen, welche aus T_r, S_r entstehen, wenn man p^{n^2}, q^{n^2}, r^{n^2} für p^n, q^n, r^n einsetzt, so ist z. B. analog zu (92), wie man mittels der erwähnten Substitution aus (82) findet:

$$p^{n^2(n-1)} - r^{n^2(n-1)} + 2\gamma n^3 r^{n^2(n-2)}$$
$$\equiv n T_r' - q^{n^2}(p^{n^2} + q^{n^2})(T_1' - \gamma n^3 T_2') \equiv n T_r' - q^{n^2} S_r' n^3 \mod n^4.$$

Gemäß (83) ist hier also $T_{1r} \equiv T_{1r}' \mod n^2$, und somit auch T_{1r}' durch n^2 teilbar. Die links stehende Differenz ist durch n^3 teilbar und deshalb folgt, daß T_r' auch durch n^2 teilbar ist, wie es wegen der Kongruenz $T_r \equiv T_r' \mod n^2$ selbstverständlich war, denn nach (123^a) ist jetzt:

$$T_r \equiv 0 \mod n^2. \tag{123^b}$$

---

[1]) Vgl. auch die Rechnungen im folgenden Paragraphen.

In obiger Kongruenz können wir rechts und links mit n dividieren und erhalten dadurch:

$$(123^c)\quad p^{n(n-1)} - r^{n(n-1)} + 2\gamma n^2 r^{n(n-2)} \equiv T_r' - n q^n S_r' \mod n^3.$$

Hierin haben nach obigem die Zahlen T' folgende Werte:

$$n T_r' = \sum_{i=2}^{\nu+1} N_i p^{n^2(i-1)} q^{n^2(i-1)} r^{n^2(n-2i+1)},$$

$$(123^d)\quad n T_{1r}' = \sum_{i=2}^{\nu+1} N_i (i-1) p^{n^2(i-2)} q^{n^2(i-2)} r^{n^2(n-2i+1)},$$

$$n T_{2r}' = \sum_{i=2}^{\nu} N_i (2i-1)(2i-2) p^{n^2(i-2)} q^{n^2(i-2)} r^{n^2(n-2i)},$$

und es ist zu setzen, analog zu (114^a):

$$n^2 S_r' = (q^{n^2} + p^{n^2})(T_{1r}' - \gamma n^3 T_{2r}').$$

Da T_{1r}' durch n^2 teilbar ist, so haben wir auch:

$$(123^e)\quad n^2 S_r' \equiv (q^n + p^n)(T_{1r}' - \gamma n^3 T_{2r}') \mod n^4.$$

Die Zahlen T' lassen sich in folgender Weise auf die Zahlen T zurückführen. Gemäß (85) ist:

$$p^{n^2} = p^n (1 + n\pi)^n \equiv p^n (1 + n^2\pi + n^3 \nu \pi^2) \mod n^4;$$

setzen wir also zur Abkürzung:

$$n M_i = N_i p^{n(i-1)} q^{n(i-1)} r^{n(n-2i+1)},$$

$$P = \pi + \varkappa - 2\varrho, \quad Q = \pi^2 + \varkappa^2 - 2\varrho^2,$$

so erhalten wir aus (123^d):

$$T_r' \equiv \sum M_i [1 + n^2 (i-1)(P + n\nu Q) + n^3 \varrho - n^2 \varrho - n^3 \nu \varrho^2] \mod n^4,$$

$$(123^f)\quad p^{n^2} q^{n^2} T_{1r}' \equiv \sum (i-1) M_i [1 + n^2 (i-1)(P + n\nu Q) + n^3 \varrho - n^2 \varrho - n^3 \nu \varrho^2] \mod n^4,$$

$$p^{n^2} q^{n^2} T_{2r}' \equiv \sum (2i-1)(2i-2) M_i [1 + n^2 (i-1)(P + n\nu Q) + n^3 \varrho - 2 n^2 \varrho - 2 n^3 \nu \varrho^2] \mod n^4,$$

und durch Auflösung der Klammern:

$$T'_r \equiv T_r + n^2(P + n\nu Q)T_{1r} + (n^3 - n^2 - n^3\nu\varrho)\varrho T_r \mod. n^4,$$

(123g) $$T'_{1r} \equiv T_{1r} + n^2(P + n\nu Q)T_{3r} + (n^3 - n^2 - n^3\nu\varrho)\varrho T_r \quad , \quad n^4,$$

$$T'_{2r} \equiv T_{2r} \quad , \quad n^2,$$

wo T_{3r} wieder nach (88a) auf T_{2r} zurückgeführt werden kann. Da nun T_r und T_{1r} je durch n^2 teilbar sind, so folgt schließlich:

$$T'_r \equiv T_r \mod. n^4,$$

(123h) $$T'_{1r} \equiv T_{1r} + n^2(\pi + \varkappa - 2\varrho)T_{3r} \quad , \quad n^4,$$

$$T'_{2r} \equiv T_{2r} \quad , \quad n^2.$$

Die erste dieser Kongruenzen gibt uns zusammen mit (123a) das Resultat:

(123i) $$2(\gamma - \alpha)n^2 \equiv r^n T'_r \mod. n^4.$$

Subtrahieren wir jetzt die Kongruenz (123e) von (115), so wird:

$$(2\alpha - 2\gamma)n^2 \equiv (n T_r - T'_r - n^2 q^n S_r + n q^n S'_r)r^n \mod. n^3,$$

und in Rücksicht auf (123b) und (123i) folgt weiter:

(123k) $$S'_r \equiv n S_r \mod. n^2,$$

so daß aus der Kongruenz (123e) die folgende hervorgeht:

(123l) $$n^3 S_r \equiv (p^n + q^n)(T'_{1r} - \gamma n^3 T'_{2r}) \mod. n^4,$$

wonach T'_{1r} jetzt durch n^3 teilbar ist, und weiter durch Vergleichung mit der dritten Gleichung (114a):

(123m) $$T'_{1r} - \gamma n^3 T'_{2r} \equiv n(T_{1r} - \alpha n^2 T_{2r}) \mod. n^4.$$

In Rücksicht auf die dritte der Kongruenzen (123h) kann die mittlere der letzteren demnach in der folgenden Form geschrieben werden:

(123n) $$(\gamma - \alpha)n^3 T_{2r} + n T_{1r} \equiv T_{1r} + n^2(P + n\nu Q)T_{3r} \mod. n^4.$$

Ganz analoge Relationen ergeben sich, wenn man von den Zahlen T', S' zu Zahlen T'', S'' übergeht, indem man wieder p, q, r bzw. durch p^n, q^n, r^n ersetzt. Um dann diese neuen Zahlen auf T' und S' zurückzuführen, hat man in den eckigen

Klammern der Kongruenzen (123^f) nur die Exponenten von n um eine Einheit zu erhöhen und den Modul n^4 durch n^5 zu ersetzen, ferner die Definition von M_i entsprechend abzuändern. An Stelle von (123^h) findet man so:

$$(123^o)\qquad \begin{aligned} T_r^* &\equiv T_r' && \text{mod. } n^5,\\ T_{1r}^* &\equiv T_{1r}' + n^3(P + n\nu Q)T_{3r}' && \text{„ } n^5,\\ T_{2r}^* &\equiv T_{2r}' && \text{„ } n^3. \end{aligned}$$

Gleichzeitig haben wir jetzt γ durch $\gamma - \alpha$ zu ersetzen; denn es ist:

$$p^{n^3} - q^{n^3} - r^{n^3} \equiv p^{n^2} - q^{n^2} - r^{n^2} + n^3(p^n\pi - q^n\varkappa - r^n\varkappa) \mod n^4,$$

und:

$$p^{n^2} - q^{n^2} - r^{n^2} \equiv p^n - q^n - r^n + n^2(p^n\pi - q^n\varkappa - r^n\varrho) \mod n^3,$$

also zunächst:

$$p^n\pi - q^n\varkappa - r^n\varrho \equiv -2\alpha \mod n$$

und dann:

$$(123^p)\qquad p^{n^3} - q^{n^3} - r^{n^3} \equiv 2(\gamma - \alpha)n^3 \mod n^4.$$

Bei Aufstellung der zu (115) analogen Kongruenz ist daher α durch $\gamma - \alpha$ zu ersetzen und der Modul n^3 wieder durch n^4; es wird also:

$$(123^q)\qquad \begin{aligned} p^{n^3(n-1)} - r^{n^3(n-1)} + 2(\gamma - \alpha)n^3 r^{n^3(n-2)}\\ \equiv n\,T_r^* - n^2 q^{n^3} S_r^* \mod n^4, \end{aligned}$$

wo, analog zu (123^e):

$$(123^r)\qquad n^3 S_r^* \equiv (q^n + p^n)(T_{1r}^* - (\gamma - \alpha)n^3 T_{2r}^*) \mod n^4$$

gesetzt ist. Da in (123^q) die Differenz der ersten beiden Glieder der linken Seite durch n^4 teilbar ist, so erhalten wir:

$$2(\gamma - \alpha)n^3 \equiv n\,T_r^* r^n - n^2 q^n r^n S_r^* \mod n^4.$$

Nach (123^i) und (123^o) ist aber die linke Seite mit dem ersten Gliede der rechten Seite in Bezug auf den Modul n^5 äquivalent; wir erhalten also:

$$(123^s) \qquad S_r' \equiv 0 \mod n^2,$$

und somit aus (123^r) und (123^o):

$$(123^t) \quad T_{1r}' \equiv n^3(\gamma - \alpha) T_{2r} - n^3(P + n\nu Q) T_{3r} \mod n^4,$$

denn für T_{3r}' und T_{3r}' gilt vermöge einer zu (123^f) analogen Umformung dieselbe Relation (123^o), wie für T_{2r}'; setzen wir hier noch den Wert von T_{1r}' aus (123^h) ein, so wird:

$$(123^u) \qquad T_{1r} \equiv -n^2(\pi + \varkappa - 2\varrho) T_{3r} \mod n^3,$$

was mit (123^n) in Übereinstimmung ist. Letztere Relation gibt uns aber mehr, wenn wir sie mit den Kongruenzen (123^e) und (123^r) verbinden; durch Subtraktion der letzteren voneinander erhalten wir nämlich unter Benutzung von (123^s):

$$n^2 S_r' \equiv (q^n + p^n)[T_{1r}' - T_{1r}'' + \alpha n^3 T_{2r}] \mod n^4,$$

oder, wenn wir den Wert der Differenz $T_{1r}' - T_{1r}''$ aus (123^o) entnehmen:

$$n^2 S_r' \equiv (q^n + p^n)[\alpha T_{2r} - (\pi + \varkappa - 2\varrho) T_{3r}] n^3 \mod n^4$$

und wenn wir S_r' gemäß (123^k) durch S_r ausdrücken und sodann S_r mittels (123^l) und (123^m) auf T_{1r} und T_{2r} zurückführen:

$$n(T_{1r} - \alpha n^2 T_{2r}) + n^3(\pi + \varkappa - 2\varrho) T_{3r} \equiv \alpha n^3 T_{2r} \mod n^4.$$

Der Vergleich mit (123^k) ergibt demnach:

$$n^2(\pi + \varkappa - 2\varrho) T_{3r} \equiv 2\alpha n^2 T_{2r} - T_{1r} \equiv -T_{1r} \mod n^3,$$

und hieraus folgt, daß entweder α oder T_{2r} durch n teilbar sein muß. Es läßt sich aber zeigen, daß die Zahl T_{2r} den Faktor n nicht enthalten kann. Aus (115) und (115^a) ergibt sich nämlich durch Subtraktion (da T_r durch n^2 teilbar ist):

$$(\pi + \varkappa - 2\varrho) r^n + 4\alpha \equiv -S_r(p^n + q^n) r^n \mod n;$$

berücksichtigen wir also, daß nach (88^a):

$$4\,T_{3r}\,r^n \equiv T_{2r} \mod n$$

ist, so finden wir aus (123^b):

$$4\,T'_{1r} \equiv n^3\,T_{2r}\,[4\,\gamma + S_r\,(p^n + q^n)\,r^n] \mod n^4,$$

und durch Vergleichung mit (123^d):

$$T_{2r}\,r^n\,(p^n + q^n)^2 \equiv 4 \mod n,$$

so daß in der Tat T_{2r} nicht durch n teilbar sein kann. Somit erhalten wir das für uns wichtige Resultat:

$$a \equiv 0 \mod n. \tag{124}$$

Betrachten wir noch den bisher ausgeschlossenen Fall, wo $q - r$ durch n teilbar ist. Dann reduziert sich die Kongruenz (77) auf:

$$p^n \equiv 2\,q^n \mod n^2. \tag{125}$$

In (84) kann dann der Faktor $r^n - 2\,p^n\,(\equiv q^n - 2\,p^n)$ nicht durch n teilbar sein; es folgt also $T_{1r} \equiv 0 \mod n$ und ebenso: $T_{1q} \equiv 0 \mod n$. Aus (125) erhalten wir durch Potenzieren:

$$2^{n-1} \equiv 1 \mod n^2. \tag{125a}$$

Nur für Zahlen n, die dieser Bedingung genügen, kann also der Fall $q \equiv r$ eintreten. Eine Bestätigung dieses Resultates geben auch unsere allgemeinen Summenformeln. Die Gleichung (82) war für die Größen p^n und q^n identisch erfüllt; wir dürfen also p^n durch 2, q^n durch 1 ersetzen; das gibt:

$$\begin{aligned} n(2^{n-1} - 1) &= \sum N_i(n - 2i + 2)\,2^{i-1} + \sum N_i(i-1)\,2^{i-2} \\ &= n\sum N_i 2^{i-1} - 3\sum N_i\,(i-1)\,2^{i-2}. \end{aligned} \tag{126}$$

Machen wir andererseits in (93) dieselbe Substitution, so wird:

$$0 = \sum N_i(i-1)\,2^{i-1} - \sum N_i(n - 2i + 2)\,2^{i-1}$$

oder:

$$n\sum N_i 2^{i-1} = 6\sum N_i(i-1)\,2^{i-2}. \tag{126a}$$

Drücken wir so die erste Summe durch die zweite aus, so erhalten wir aus (126):

$$(126^b) \qquad n(2^{n-1}-1) \equiv 3 \sum N_i (i-1)\, 2^{i-2}.\ ^1)$$

Ferner ist nach (83) in unserem Falle (d. h. für $q \equiv r$):

$$n\, T_{1\,q} \equiv q^{n(n-3)} \sum N_i (i-1)\, 2^{i-2}.$$

Man ersieht hieraus, daß die Bedingung $T_{1\,q} \equiv 0 \mod. n^2$ im Falle $q \equiv r$ in der Tat mit der Bedingung (125^a) übereinstimmt.

Analog folgt aus (102), wenn man q^n und r^n durch 1 ersetzt:

$$(127) \qquad 2(1-2^{n-1}) \equiv \sum N_i (-1)^{i-1}\, 2^{n-2i+2}$$

und aus (103) erhält man dasselbe Resultat. Beiläufig finden wir also die Relation:

$$n \sum N_i (-1)^{i-1}\, 2^{n-2i+1} \equiv -3 \sum N_i (i-1)\, 2^{i-2}.$$

Soll im Falle $q \equiv r \mod. n$ auch die Bedingung (122) erfüllt sein, so ist:

$$p^{n^2} \equiv 2\, q^{n^2} \mod. n^3,$$

während sich aus (125) durch Potenzieren ergibt:

$$p^{n^2} \equiv 2^n q^{n^2} \mod. n^3.$$

Es müßte also die Bedingung:

$$(127^a) \qquad 2^{n-1} \equiv 1 \mod. n^3$$

erfüllt sein. Wir fassen das Vorstehende in folgendem Satze zusammen:

Wenn zugleich mit der Kongruenz (77) auch die Kongruenz (122) bestehen soll und die erstere Kongruenz nur für den Modul n^2 (also nicht für n^3) gilt, so ist das nur möglich, wenn eine der Zahlen $p + r$,

---

[1]) Hieraus folgt beiläufig, daß die Zahl $2^{n-1} - 1$ für jede ungerade Zahl n durch 3 teilbar ist, wie man auch direkt leicht erkennt.

$q + r$, $q - r$ durch n teilbar ist und die ungerade Primzahl n der Bedingung (127ᵃ) genügt.[1])

§ 9. Erweiterung der in § 8 aufgestellten Hilfsformeln für höhere Potenzen des Moduls.

Wir haben bisher ausgeschlossen, daß die Zahl a durch n teilbar sei. Setzen wir jetzt, entsprechend dem in (125) gewonnenen Resultate:

$$a = \beta \cdot n^{\lambda},$$

so geht die Gleichung (91) in die folgende über:

$$p^n - q^n - r^n = 2\beta n^{\lambda+2}. \tag{128}$$

Wir haben nun die entsprechenden Fragen zu untersuchen. Wir gehen zu der Relation (82) zurück; die linke Seite derselben wird jetzt:

$$\equiv n\,[p^{n(n-1)} - r^{n(n-1)} + 2\beta n^{\lambda+2} r^{n(n-2)}] \mod n^{\lambda+4}, \tag{86}^*$$

und die erste Summe der rechten Seite von (82):

$$\equiv n^2 T_r - 2n p^n q^n T_{1r} + 2\beta n^{\lambda+3} p^n q^n T_{2r} \mod n^{\lambda+4}, \tag{87}^*$$

ferner die zweite Summe:

$$\begin{aligned} &= n q^n r^n T_{1r} + 2\beta n^{\lambda+3} q^n T_{1r} - \beta n^{\lambda+3} q^n r^n T_{2r} \\ &\quad - \beta n^{\lambda+3} \nu^2 p^{n(\nu-1)} q^{n(\nu-1)} \mod n^{\lambda+4}, \end{aligned} \tag{89}^*$$

so daß wir aus (82) erhalten (da T_{1r} wieder durch n^2 teilbar ist):

$$\begin{aligned} &p^{n(n-1)} - r^{n(n-1)} + 2\beta n^{\lambda+2} r^{n(n-2)} \\ &\equiv n T_r - q^n (q^n + p^n)(T_{1r} - \beta n^{\lambda+2} T_{2r}) \mod n^{\lambda+3}; \end{aligned} \tag{92}^*$$

---

[1]) Der zu Anfang dieses Paragraphen ausgesprochene Satz hatte sich mir als beiläufige Folgerung ergeben; es zeigte sich aber, daß der Beweis eine Lücke hatte; leider konnte ich den ausgesprochenen Satz nicht mehr unterdrücken. Er ist übrigens für die einfachsten Fälle richtig; so hat man für $n = 7$: $3^7 - 2^7 - 1^7 \equiv 0 \mod 7^2$ (auch mod. 7^3) und $2^3 \equiv 1^3 \equiv -3^3 \equiv 1 \mod 7$, und für $n = 13$: $6^{13} - 8^{13} - 11^{13} \equiv 0 \mod 13^2$ (auch mod. 13^3) und: $11^6 \equiv 8^6 \equiv 6^6 \equiv 1 \mod 13$; für $n = 19$: $5^{19} - 2^{19} - 3^{19} \equiv 0 \mod 19^2$ und $2^9 \equiv 3^9 \equiv -5^9 \equiv -1 \mod 19$.

ebenso ergibt sich an Stelle von (94):

$$(94)^* \quad \begin{aligned} & r^{n(n-1)} - q^{n(n-1)} - 2\beta n^{\lambda+2} r^{n(n-2)} \\ & \equiv -n T_r + p^n (p^n + q^n)(T_{1r} - \beta n^{\lambda+2} T_{2r}) \mod n^{\lambda+3}. \end{aligned}$$

Ebenso behalten die Kongruenzen (98) und (99), ferner (111) und (112) ihre Gültigkeit, wenn man nur überall α durch βn^λ und den Modul n^4 durch $n^{\lambda+4}$ ersetzt. Die Kongruenzen (100[a]) und (113) werden:

$$\begin{aligned} p^{n^2} - q^{n^2} - r^{n^2} &\equiv 2\beta n^{\lambda+3} - n T_p p^n \\ &\equiv 2\beta n^{\lambda+3} + n T_q q^n \end{aligned} \mod n^{\lambda+5},$$

so daß auch die Kongruenzen (114) für den Modul $n^{\lambda+4}$ gültig bleiben. In gleicher Weise lassen sich offenbar alle folgenden Betrachtungen erweitern. Nimmt man dann eine Gleichung:

$$(123)^* \qquad p^{n^2} - q^{n^2} - r^{n^2} = \gamma_1 n^{\lambda+3}$$

hinzu, so ergibt sich durch die genau entsprechenden Schlüsse das Resultat:

$$(124)^* \qquad \beta \equiv 0 \mod n,$$

und damit der Satz:

Sollen also die Kongruenzen:

$$p^n - q^n - r^n \equiv 0 \mod n^{\lambda+2}$$

und:

$$p^{n^2} - q^{n^2} - r^{n^2} \equiv 0 \mod n^{\lambda+3}$$

gleichzeitig bestehen, so muß die erstere auch für den Modul $n^{\lambda+3}$ gültig sein, oder es muß eine der Zahlen $p+q$, $p+r$, $q-r$ durch n teilbar sein.

§ 10. Der Fall III).

Wir kehren nach diesen Vorbereitungen zu unserer ursprünglichen Aufgabe zurück, indem wir den Fall III) untersuchen. Die Gleichungen (13), (13[a]) und (13[b]) geben hier:

$$
\begin{aligned}
n x^\nu y^\nu &= r_n^n - r^{n(n-1)} - \sum_{i=2}^{\nu} N_i x^{i-1} y^{i-1} r^{n(n-2i+1)},\\
n x^\nu z^\nu &= q_n^n - q^{n(n-1)} - \sum N_i x^{i-1} z^{i-1} q^{n(n-2i+1)},\\
(-1)^\nu n y^\nu z^\nu &= p_n^n - p^{n(n-1)} - \sum (-1)^{i-1} N_i y^{i-1} z^{i-1} p^{n(n-2i+1)}.
\end{aligned}
\tag{129}
$$

Nehmen wir zunächst an, es sei eine der Zahlen p, q, r durch n teilbar. Es sei etwa r diese Zahl. In der ersten Gleichung sind dann alle Glieder der rechten Seite, mit Ausnahme des ersten, durch n^{2n+1} teilbar, die linke Seite ist durch n teilbar; es ist folglich auch r_n^n durch n teilbar. Dann aber enthält r_n^n den Faktor n^n, folglich muß auch $x^\nu y^\nu$ durch $n^{n-1} = n^{2\nu}$ teilbar sein, d. h. x oder y müßte durch n teilbar sein; das aber ist unmöglich, da x, y, z zueinander relativ prim sein sollen und da $z = r \cdot r_n$ jetzt schon den Faktor n enthält.

Wäre umgekehrt r_n durch n teilbar, so müßte wegen der ersten Gleichung (129) auch r durch n teilbar sein, und wir kommen auf die soeben diskutierte Annahme zurück.

Im Falle III) kann also keine der Zahlen x, y, z und keine der Zahlen p, q, r den Faktor n enthalten.

Infolgedessen ergeben sich aus den Gleichungen (129) sofort die Kongruenzen:

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

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

$$p_n \equiv p^{n-1}, \quad q_n \equiv q^{n-1}, \quad r_n \equiv r^{n-1} \quad \text{mod. } n \tag{130}$$

und hieraus:

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

Es ist aber nach III):

$$x = p p_n \equiv p, \quad y = q q_n \equiv q, \quad z = r r_n \equiv r \mod n$$

und durch Potenzieren erhält man:

$$x^n \equiv p^n, \quad y^n \equiv q^n, \quad z^n \equiv r^n \mod n^2,$$

also aus der vorausgesetzten Gleichung (3):

$$p^n \equiv q^n + r^n \mod n^2. \tag{131}$$

Zufolge der Gleichungen III) ist $y + z = p^n$, etc., folglich:

$$y + z \equiv (x - z) + (x - y) \mod n^2,$$

oder:

$$x \equiv y + z \mod n^2, \tag{131a}$$

also auch, da die rechte Seite gleich p^n ist:

$$x = p p_n \equiv p^n \mod n^2,$$

und hieraus:

$$p_n \equiv p^{n-1} \mod n^2.$$

Entsprechendes erhält man aus (131a) für q und r, so daß:

$$p_n \equiv p^{n-1}, \quad q_n \equiv q^{n-1}, \quad r_n \equiv r^{n-1} \mod n^2.$$

Um die Zahlen p_n, q_n, r_n bzw. von den Zahlen p^{n-1}, q^{n-1}, r^{n-1} zu unterscheiden, müssen wir daher auch das Quadrat von n berücksichtigen. Wir setzen demnach:

$$p^{n-1} = 1 + n\pi, \quad q^{n-1} = 1 + n\varkappa, \quad r^{n-1} = 1 + n\varrho, \tag{132}$$

folglich gemäß (130):

$$\begin{aligned} p_n &= 1 + n\pi + n^2\pi_1, \quad q_n = 1 + n\varkappa + n^2\varkappa_1, \\ r_n &= 1 + n\varrho + n^2\varrho_1. \end{aligned} \tag{133}$$

Andererseits ist nach den Gleichungen IIIa):

$$\begin{aligned} 2x = 2pp_n &= p^n + q^n + r^n = 2p^n - (p^n - q^n - r^n), \\ 2y = 2qq_n &= p^n + q^n - r^n = 2q^n + (p^n - q^n - r^n), \\ 2z = 2rr_n &= p^n - q^n + r^n = 2r^n + (p^n - q^n - r^n). \end{aligned} \tag{134}$$

Die Vergleichung mit (133) ergibt:

$$(134^a) \quad p^n - q^n - r^n = -2p\pi_1 n^2 = 2q\varkappa_1 n^2 = 2r\varrho_1 n^2,$$

woraus hervorgeht, daß $p^n - q^n - r^n$ durch n^2 teilbar ist, wie es schon in (131) gefunden wurde. Wir setzen demnach:

$$(135) \qquad p^n - q^n - r^n = 2an^3,$$

wo nun a eine ganze Zahl bezeichnet, die durch p, q und r teilbar sein muß; und dann wird:

$$(136) \quad x = p^n - an^2, \quad y = q^n + an^2, \quad z = r^n + an^2.$$

Es soll gezeigt werden, daß die Zahl a gleich Null sein muß.

Setzen wir diese Werte von x, y, z in die vorausgesetzte Gleichung (3) ein, so ergibt sich:

$$0 = x^n - y^n - z^n = (p^n - an^2)^n - (q^n + an^2)^n - (r^n + an^2)^n$$
$$\equiv p^{n^2} - q^{n^2} - r^{n^2} - an^3(p^{n(n-1)} + q^{n(n-1)} + r^{n(n-1)}) \mod n^5,$$

also, da jede der drei Zahlen innerhalb der letzten Klammer nach dem erweiterten Fermatschen Satze durch 1 ersetzt werden darf:

$$\equiv p^{n^2} - q^{n^2} - r^{n^2} - 3an^3 \mod n^5.$$

Es besteht folglich die Kongruenz:

$$(137) \qquad p^{n^2} - q^{n^2} - r^{n^2} \equiv 3an^3 \mod n^5$$

neben der Gleichung (135). Nach dem Resultat von § 8 kann dies nur eintreten, wenn entweder die Zahl a, oder eine der Zahlen $p+q$, $p+r$, $q-r$ durch n teilbar ist. Letztere Möglichkeit ist aber auszuschließen, wie jetzt noch zu beweisen ist. Wenn z. B. $p+q$ den Faktor n enthielte, d. h. wenn:

$$(138) \qquad p \equiv -q \mod n$$

wäre, so erhielte man durch Potenzieren:

$$139) \qquad p^n \equiv -q^n \mod n^2.$$

Wir knüpfen zu dem Zwecke wieder an unsere allgemeinen Formeln an. Das Bestehen der Kongruenzen (92) und (94) wird durch unsere jetzige Annahme nicht gestört; sie vereinfachen sich nur dadurch, daß jetzt das Glied $a n^2 T_2 q^n (p^n + q^n)$ gestrichen werden kann; die Kongruenzen (98), (99), (111) und (112) bleiben vollkommen ungeändert. Auch die Kongruenzen (115), ... (115^c) bleiben demnach bestehen; in ihnen kann nur S_r jetzt durch die einfachere Gleichung:

$$n^2 S_r = -(r^n - 2p^n) T_{1r} \tag{142}$$

definiert werden, welche an Stelle der letzten Gleichung (114^a) tritt; im übrigen lauten letztere hier:

$$n^2 S_q = -(q^n - 2p^n)(T_{1q} - a n^2 T_{2q})$$
$$n^2 S_p = (p^n - 2r^n)(T_{1p} + a n^2 T_{2p}).$$

Eine Änderung erfährt hingegen die Kongruenz (100^a); sie lautet jetzt:

$$p^{n^2} - q^{n^2} - r^{n^2} \equiv 2a n^3 + n r^n T_r - 4 a n^3 p^n q^n T_{1r} \mod n^5, \tag{143}$$

während die Kongruenzen (101) und (113) unverändert fortbestehen. An Stelle von (114) erhalten wir somit jetzt:

$$r^n T_r - 4 a n^2 p^n q^n T_{1r} \equiv q^n T_q \equiv -p^n T_p \mod n^4. \tag{144}$$

Die Gültigkeit der aus (115) ... (115^e) abgeleiteten Kongruenzen (116), (117), (118) wird nicht gestört; es ist nur dort S_r jetzt durch (142) definiert. An Stelle der Kongruenz (119) finden wir aus (116) und (143):

$$2a n^2 \equiv n r^n T_r - n^2 q^n r^n (S_q + S_r) \mod n^3, \tag{145}$$

also ein mit (119) übereinstimmendes Resultat. Aus (117) ergibt sich ebenso:

$$2a n^2 \equiv n r^n T_r - n^2 p^n r^n (S_r - S_p) \mod n^3, \tag{146}$$

ebenfalls in Übereinstimmung mit (119); endlich aus (118), (113) und (143):

$$\begin{aligned} 2a n^2 &\equiv n q^n T_q - n^2 p^n q^n (S_p + S_q) \\ &\equiv n r^n T_r - 4 a n^2 p^n q^n T_{1r} - n^2 p^n q^n (S_p + S_q) \mod n^3. \end{aligned} \tag{147}$$

Die Kongruenzen (119) sind also jetzt durch (145), (146) und (147) zu ersetzen. An Stelle von (120) erhalten wir hier aus (146) und (147):

$$4\,a\,q^n\,T_{1r} + p^n\,S_p + q^n\,S_q - r^n\,S_r \equiv 0 \mod n,$$

dagegen aus (145) und (146):

$$p^n\,S_p + q^n\,S_q - r^n\,S_r \equiv 0 \mod n.$$

Es ist folglich T_{1r} jetzt durch n teilbar, wie auch aus (125[a]) und (126[b]) hervorgeht, und somit ist nach (142) die Zahl S_r durch n teilbar. Infolge dieses Resultates gelten die Kongruenzen (119) vollständig unverändert, und ebenso alle anderen früheren Relationen, insbesondere werden die Kongruenzen (143) und (144) jetzt bzw. mit den entsprechenden früheren Kongruenzen (100[a]) und (113) identisch.

Besteht wieder die Relation (123), so folgt aus (143) wieder, daß T_r durch n^2 teilbar ist, somit aus (115):

$$p^{n(n-1)} - r^{n(n-1)} + 2\,a\,n^2 \equiv 0 \mod n^3,$$

ebenso aus (123[b]):

$$p^{n(n-1)} - r^{n(n-1)} + 2\,\gamma\,n^2 \equiv 0 \quad , \quad n^3,$$

folglich:

(147[a]) $$a \equiv \gamma \mod n.$$

Dasselbe Resultat leitet man als eine Folge des Zusammenbestehens der Relationen:

$$p^n - q^n - r^n = 2\,a\,n^2$$
$$p^{n^2} - q^{n^2} - r^{n^2} = 2\,\gamma\,n^2$$
$$r^n = 2\,p^n + \beta\,n^2, \qquad 2^{n-1} \equiv 1 \mod n^3$$

leicht direkt ab. Infolge der vorausgesetzten Gleichung (3) war aber nach (137) $2\gamma \equiv 3a \mod n$; aus (147[a]) folgt also wieder das Resultat: $a \equiv 0 \mod n$, auf dem alles folgende beruht.

Auch das weitere Rekursionsverfahren bleibt im wesentlichen ungeändert.

Aus vorstehendem geht hervor, daß die Fälle, wo eine der Zahlen $p+q$, $p+r$, $q-r$ durch n teilbar ist, von

uns nicht weiter berücksichtigt zu werden brauchen; und wir kommen zu folgendem Resultate:

Infolge der Gleichung $x^n = y^n + z^n$ müssen die Kongruenzen:

$$p^n - q^n - r^n \equiv 0 \mod n^{\lambda+2}$$
$$p^{n^2} - q^{n^2} - r^{n^2} \equiv 0 \quad , \quad n^{\lambda+3}$$

zunächst für $\lambda = 0$ bestehen; dann gelten sie nach unserem Hilfssatze auch für $\lambda = 1$, dann für $\lambda = 2$, u. s. f. Es bleibt also nur die Möglichkeit, daß die Zahl a, welche als Faktor von $n^{\lambda+2}$ bzw. $n^{\lambda+3}$ auftritt, wenn man die Kongruenzen als Gleichungen schreibt, gleich Null ist; wo wir dann aus Gleichung (135) das Resultat:

$$p^n - q^n - r^n = 0 \tag{148}$$

erhalten. Mit Rücksicht auf die Gleichungen (134) können wir sonach folgenden Satz aussprechen:

Sollen also drei Zahlen x, y, z existieren, deren keine durch n teilbar ist, und die der Gleichung:

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

genügen, so ist jede von ihnen gleich der n^{ten} Potenz einer anderen Zahl; und zwischen diesen drei anderen Zahlen p, q, r besteht dieselbe Relation:

$$p^n - q^n - r^n = 0.$$

Für diese Zahlen p, q, r gilt also dasselbe; man hat:

$$p = p_1^n, \quad q = q_1^n, \quad r = r_1^n$$

und es ist:

$$p_1^n - q_1^n - r_1^n = 0.$$

Die Zahlen p_1, q_1, r_1 sind kleiner als die Zahlen p, q, r; letztere kleiner als die Zahlen x, y, z. So wird man zu immer kleineren Zahlen p_i, q_i, r_i fortschreiten, bis eine dieser Zahlen gleich 1 geworden ist, wo dann eine Gleichung der Form:

$$P^n = Q^n + 1$$

bestehen müßte, die offenbar nur möglich ist, wenn $P = 1$, $Q = 0$ genommen wird.

Hiermit ist auch der Fall III) als unmöglich nachgewiesen.

§ 11. Schlussbemerkung

Somit ist die Unmöglichkeit dargetan, 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 teilbar sein soll. Der Fall aber, wo eine dieser Zahlen durch n teilbar ist, wurde schon oben (p. 297 ff.; vgl. auch unten § 12) erledigt.

Da nun die Unmöglichkeit des Falles $n = 4$ von Lamé nachgewiesen wurde, kann n auch keine Potenz von 2 sein;[1]) es bleibt also in der Tat nur die eine Möglichkeit $n = 2$.

Die im vorstehenden herangezogenen Hilfsmittel sind durchaus elementarer Natur; außer dem Fermatschen Satze der Zahlentheorie sind nur einfache algebraische Umformungen benutzt worden. Es ist daher immerhin möglich, daß Fermat bereits im Besitze eines Beweises für seine Behauptung gewesen ist, denn die von uns benutzten Hilfsmittel sind der binomische Satz, der Fermatsche Satz, nach welchem $p^{n-1} \equiv 1 \bmod. n$, und der sogenannte erweiterte Fermatsche Satz.

Das gewonnene Resultat kann man auch dahin aussprechen, daß die Kurve:

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

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

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

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

welche durch den Punkt $1, 1, 0$ hindurchgeht, so kann die resultierende Gleichung nicht durch rationale Werte erfüllt werden. Es ergibt sich aber durch Elimination von z:

[1]) Vgl. hierfür auch den Schluß des oben zitierten Werkes von Hilbert.

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

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 Werte von t und λ erfüllt werden, ausgenommen die Werte $t = 1$, $\lambda = 0$ und $t = 0$, $\lambda = +1$, oder -1, je nachdem die Zahl n ungerade oder gerade ist.

§ 12. Nachtrag zu § 7. — Erläuterung der allgemeinen Schlüsse an dem Falle $n = 5$.

Die oben angewandte Schlußweise möge hier noch an dem Beispiele $n = 5$ erläutert werden.

Durch Vergleich der rechten Seite von $(58^d)^*$ mit $(57^a)^*$ erhalten wir:

$$\vartheta_1 q + 2 r_1 \varkappa_1 + r_1^2 q^{n-2} + \tfrac{4}{3}(n-1)(n-2) r_1^2 q^{n-2} \equiv -2 r_1 \pi_1 \mod n.$$

Wir können hier die Entwicklung sogleich weiter verfolgen, wenn wir in $(58^c)^*$ gemäß $(58^b)^*$ setzen:

$$(\varkappa_1' - \pi_1')^2 \equiv (r_1 - 2n r_1)^2 q^{2n-4};$$

dann wird:

$$(\pi_1 - \varkappa_1) q \equiv -2 r_1 + 2 n r_1 + n^{\lambda+1} [\vartheta_1 q + 2 r_1 \varkappa_1 + r_1^2 (2n-1)^2 q^{n-2} + \tfrac{4}{3}(n-1)(n-2) r_1^2 q^{n-2}] \mod n^{2\lambda+2},$$

also nach $(57^a)^*$:

$$(A) \quad \vartheta_1 q \equiv -2 r_1 (\pi_1 + \varkappa_1) - r_1^2 (2n-1)^2 q^{n-2} - \tfrac{4}{3}(n-1)(n-2) q^{n-2} r_1^3 \mod n^{\lambda+1}.$$

Die Zahl ϑ_1 in $(58)^*$ ist hierdurch bis auf Vielfache von $n^{\lambda+1}$ bestimmt; wir haben demnach zu setzen:

$$(B) \qquad p - q = 2n^{\lambda+1} r_1 + r_1 \vartheta_1 n^{3\lambda+3} + r_1 \vartheta_1' n^{4\lambda+4},$$

und nun ϑ_1' zu suchen. Durch Potenzieren finden wir, analog zu (58ª)*:

$$(C) \qquad \begin{aligned} p^n - q^n \equiv{}& n q^{n-1} \Theta_4 + \binom{n}{2} q^{n-2} \Theta_3^2 + \binom{n}{3} 8 r_1^3 n^{3\lambda+3} q^{n-3} \\ &+ 16 r_1^4 n^{4\lambda+4} \binom{n}{4} q^{n-4} \mod n^{5\lambda+6}, \end{aligned}$$

und hierin ist:

$$(D) \qquad \begin{aligned} \Theta_4 &= 2n^{\lambda+1} r_1 + r_1 \vartheta_1 n^{3\lambda+3} + r_1 \vartheta_1' n^{4\lambda+4}, \\ \Theta_3 &= 2n^{\lambda+1} r_1 + r_1 \vartheta_1 n^{3\lambda+3}. \end{aligned}$$

Andererseits ist analog zu (57)*, gemäß (60ᵉ)*:

$$(E) \qquad \begin{aligned} p^n - q^n \equiv{}& 2n^{\lambda+2} r_1 [1 + \varepsilon n^{\lambda+1} (\pi_1' + \varkappa_1') + n^{2\lambda+2} \pi_1' \varkappa_1'] \\ &+ 2 n^{3\lambda+5} \cdot \nu \cdot r_1^3 p^{\nu-1} q^{\nu-1} \mod n^{5\lambda+8}, \end{aligned}$$

oder wenn wir die Relation (B) zur Umformung benutzen, und beiderseits mit $r_1 n^{2\lambda+3}$ dividieren:

$$\begin{aligned} &2\varkappa_1 + n^{\lambda+1} \vartheta_1 + n^{2\lambda+2} \vartheta_1' + n^{2\lambda+2} \vartheta_1 \varkappa_1 + 4\nu r_1 q^{n-2} + n^{2\lambda+2} \cdot 4\nu \cdot r_1 \vartheta_1 q^{n-2} \\ &+ n^{\lambda+1} \tfrac{1}{3}(n-1)(n-2) 4 r_1^2 q^{n-3} + n^{2\lambda+2} \tfrac{1}{3}(n-1)(n-2)(n-3) 2 r_1^3 q^{n-4} \\ &\equiv 2\varepsilon(\pi_1' + \varkappa_1') + 2n^{\lambda+1} \pi_1' \varkappa_1' + n^{2\lambda+2} \cdot 2\nu \cdot r_1^3 p^{\nu-1} q^{\nu-1} \mod n^{3\lambda+3} \end{aligned}$$

oder, analog zu (58ᶜ)*:

$$(F) \qquad \begin{aligned} (\varkappa_1 - \pi_1) q \equiv{}& 2r_1 - 2n r_1 q^{n-1} \\ &- n^{\lambda+1} [\vartheta_1 q + 2 r_1 \varkappa_1 + (\varkappa_1' - \pi_1')^2 q + \tfrac{4}{3}(n-1)(n-2) r_1^2 q^{n-2}] \\ &+ n^{2\lambda+2} [2\nu r_1^3 p^{\nu-1} q^{\nu-1} - \vartheta_1 \varkappa_1 q - \vartheta_1' q - 4\nu r_1 \vartheta_1 q^{n-1} \\ &- \tfrac{2}{3} r_1^3 (n-1)(n-2)(n-3) q^{n-3}] \mod n^{3\lambda+3}. \end{aligned}$$

Hierin ist $(\pi_1' - \varkappa_1')^2$ gemäß (58ᵇ)* durch die Zahlen $r_1, q, \vartheta_1, \pi_1', \varkappa_1'$ auszudrücken. Einen anderen Wert für $\varkappa_1 - \pi_1$ finden wir, indem wir in (E) die linke Seite durch:

$$\begin{aligned} p - q + n^{\lambda-1} (p\pi_1 - q\varkappa_1) \equiv{}& 2n^{\lambda+1} r_1 + n^{\lambda+1} q (\pi_1 - \varkappa_1) \\ &+ n^{2\lambda+2} 2 r_1 \pi_1 + n^{3\lambda+3} r_1 \vartheta_1 \mod n^{4\lambda+4} \end{aligned}$$

ersetzen, wobei zur Umformung die Kongruenz (58)* benutzt wurde; wir erhalten dann aus (E), nach Division mit $n^{\lambda+1}$, analog zu (57ª)*:

(G) $$q(\pi_1 - \varkappa_1) \equiv -2r_1 + 2nr_1 - 2n^{\lambda+1} r_1 \pi_1 - n^{2\lambda+2} r_1 \vartheta_1 + n^{\lambda+2} \cdot 2\varepsilon r_1 (\pi_1' + \varkappa_1') + n^{2\lambda+3} \cdot 2 r_1 \pi_1' \varkappa_1' \mod n^{3\lambda+3}.$$

Macht man in (F) die angedeutete Substitution, nämlich:

$$4(\pi_1' - \varkappa_1')^2 \equiv 4 r_1^2 q^{2n-2} + 4 n^2 r_1^2 q^{2n-2} - 8 n r_1^2 q^{2n-2} - 2 r_1 (n-1) n^{\lambda+1} q^{n-1} [\vartheta_1 + 2\varkappa_1'^2 + 2 r_1 q^{n-2} + \tfrac{4}{3}(n-1)(n-2) r_1^2 q^{n-2} - 2\pi_1' \varkappa_1'] \mod n^{2\lambda+2}$$

und ersetzt noch q^{n-1} durch $1 + n^{\lambda+1} \varkappa_1$, so stimmt die rechte Seite von (F) mit der rechten Seite von (G) bis auf die Glieder mit dem Faktor $n^{2\lambda+2}$ überein (denn so war ϑ_1 bestimmt); die Vergleichung der letzteren gibt also eine Bestimmung von ϑ_1 bis auf Vielfache von $n^{\lambda+1}$.

Sodann hätten wir die Kongruenz (60^e) zu erweitern. Wir setzen demnach:

(H) $$pq\,R = p^r q^r + n^{2\lambda+3} \cdot \nu \cdot r_1^2 p^{r-1} q^{r-1} + n^{4\lambda+6} \eta_2.$$

In der Gleichung:

$$x^r y^r \equiv [p^n q^n + z(p^n - q^n) - z^2]^r$$

ist nach der auf Seite 317 für r_n abgeleiteten Relation:

$$z \equiv n^{\lambda+2} r_1 p^r q^r + n^{3\lambda+5} \nu r_1^2 p^{r-1} q^{r-1} \mod n^{4\lambda+8};$$

also folgt:

$$x^r y^r \equiv p^{nr} q^{nr} + n^{2\lambda+4} \cdot \nu \cdot r_1^2 (pq)^{2r+n(r-1)} + n^{4\lambda+8} \binom{r}{2} r_1^4 (pq)^{4r+n(r-2)} \mod n^{6\lambda+10},$$

und nach (30)*:

$$r_n^n \equiv p^{nr} q^{nr} + n^{2\lambda+4} \cdot \nu \cdot r_1^2 p^{nr-1} q^{nr-1} + n^{4\lambda+8} \binom{r}{2} r_1^4 (pq)^{nr-2} \mod n^{6\lambda+10},$$

und somit:

(I) $$r_n \equiv pq\,R \equiv p^r q^r + n^{2\lambda+3} \cdot \nu \cdot r_1^2 p^{r-1} q^{r-1} - n^{4\lambda+6} \cdot \nu^2 \cdot r_1^4 (pq)^{2r-2} + n^{4\lambda+7} \binom{r}{2} r_1^4 (pq)^{r-2} \mod n^{6\lambda+9}.$$

Durch den Vergleich mit (H) ist dann η_2 bestimmt:

$$(K)\quad \eta_2 \equiv -\nu^2 r_1^4 p^{2\nu-2} q^{2\nu-2} + n\binom{\nu}{2} r_1^4 p^{\nu-2} q^{\nu-2} \mod n^{2\lambda+3}.$$

Für die Differenz $p^n - q^n$ finden wir hieraus:

$$(L)\quad \begin{aligned} p^n - q^n \equiv\ & 2n^{\lambda+2} p^\nu q^\nu r_1 + 2n^{3\lambda+5} \cdot \nu \cdot r_1^3 p^{\nu-1} q^{\nu-1} \\ & - 2n^{5\lambda+8} \cdot \nu^2 \cdot r_1^5 (pq)^{2\nu-2} + 2n^{5\lambda+9}\binom{\nu}{2} r_1^5 (pq)^{\nu-2} \\ & \mod n^{7\lambda+11}. \end{aligned}$$

Nach (B) dürfen wir, unter Einführung einer noch unbekannten Zahl ϑ_1'', setzen:

$$(M)\quad p - q = 2n^{\lambda+1} r_1 + n^{3\lambda+3} r_1 \vartheta_1 + n^{4\lambda+4} r_1 \vartheta_1' + n^{5\lambda+5} r_1 \vartheta_1'';$$

und durch Potenzieren ergibt sich hieraus:

$$(N)\quad \begin{aligned} p^n - q^n \equiv\ & n\Theta_5 q^{n-1} + \binom{n}{2}\Theta_4^2 q^{n-2} + \binom{n}{3}\Theta_3^2 q^{n-3} \\ & + \binom{n}{4} 2^4 n^{4\lambda+4} r_1^4 + \binom{n}{5} 2^5 r_1^5 n^{5\lambda+5} \mod n^{6\lambda+7}, \end{aligned}$$

wo Θ_4, Θ_3 durch obige Gleichungen (D) definiert sind, während Θ_5 die rechte Seite von (M) bezeichnet. Entwickelt man die rechte Seite von (N) nach Potenzen von n, so stimmen alle Glieder bis zu demjenigen mit dem Faktor $n^{5\lambda+5}$ einschließlich mit den entsprechenden Gliedern von (L) bzw. den schon in der Kongruenz (C) so weit schon berechneten Gliedern überein; der Faktor von $n^{5\lambda+6}$ auf der rechten Seite von n enthält in Θ_5 die unbekannte Zahl ϑ_1'', während diese Zahl auf der rechten Seite von (L) nicht vorkommt; dadurch ergibt sich eine Bestimmung dieser Zahl bis auf Vielfache der Zahl $n^{\lambda+1}$. Ist $n > 5$, so enthält der Faktor $n^{5\lambda+6}$ auf der rechten Seite von (N) auch das Glied:

$$\frac{1}{n}\binom{n}{5} 2^5 r_1^5.$$

Wenn aber $n = 5$ ist, so gibt dies Glied einen Beitrag zum Faktor von $n^{5\lambda+5}$, der durch die Kongruenz (C) schon

bestimmt ist, und deshalb keine nachträgliche Korrektur erfahren kann. Im Falle $n = 5$ ist also die Kongruenz (N) mit den Kongruenzen (C) oder (L) nur verträglich, wenn r_1 den Faktor n enthält; es folgt also für $n = 5$: $r_1 \equiv 0 \bmod. n$, q. e. d.

Bei dem letzten Schlusse hatten wir unsere obige allgemeine Regel etwas vereinfacht, indem wir die Kongruenzen (L) und (N) direkt miteinander verglichen, ohne ihre Differenz explizite zu bilden, ohne also auf Bildung der Differenz $(\pi_1 - \varkappa_1)q$ zurückzugehen; in ähnlicher Weise wird man allgemein verfahren können.

Verbesserungen.

Seite 322. Für den zu Beginn von § 8 ausgesprochenen Satze vgl. die Anmerkung auf Seite 339.

„ 323. Z. 10 v. o.: Lies „äquivalent“ statt „gleich“.