ÜBER DIE LÖSUNG DER KONGRUENZ

$$(\lambda + 1)^p - \lambda^p - 1 \equiv 0 \pmod{p^2}$$

VON

A. ARWIN

in LUND.

Der Versuch das Fermat'sche Problem $x^p + y^p = z^p$ in zur Primzahl p prime ganzen Zahlen zu lösen führt leicht zur Untersuchung der Möglichkeit der Kongruenz $(\lambda + 1)^p - \lambda^p - 1 \equiv 0 \pmod{p^2}$, und diese ist eben der Gegenstand einer Untersuchung in dieser Abhandlung. Die Ausführung, die das Problem mit sich zog und unten angegeben worden ist, wurde eine Folge vom Zusammenführen ganzzahliger Werte $(\mathrm{mod}\, p)$ und $(\mathrm{mod}\, p^2)$ und von dem Verhältnis dieser Werte zu einander. Hierin liegt das Neue, das in dieser Abhandlung zu finden ist, wie auch in der Übersicht der Natur der Lösungen, die daraus ersichtlich ist. Dass endlich wirklich solche Lösungen in den verschiedenen Fällen und damit Gruppen $(\mathrm{mod}\, p^2)$ mit gewissen Eigenarten existieren können, ist ein Resultat vom reinen experimentellen Prüfen. Dazu sei nur bemerkt, dass die Giltigkeit von $2^{p-1} \equiv 1\,(p^2)$ für $p = 1093$ von W. MEISSNER beispielsweise in Archiv der Math. u. Physik 1914 angegeben worden ist, während das zweite Beispiel für das, was ich "v-Gruppen innerhalb eines Systemes $(a)\,(\mathrm{mod}\, p^2)$" genannt habe, nämlich die Primzahl $p = 59$, wohl die erste Primzahl zu sein scheint, die solche Gruppen besitzt, aber gar nicht so eigenartig wie $p = 1093$ ist, sondern von vielen anderen begleitet wird, wenn diese auch nicht zu zahlreich sind.

Aus der Identität

$$(\lambda + 1)^p - \lambda^p - 1 = p\,\lambda\,(\lambda + 1)\,(\lambda^2 + \lambda + 1)^\varepsilon\, f_p(\lambda, 1) \tag{1}$$

wo p eine Primzahl sein soll, $\varepsilon = 1$ oder 2, je nachdem $p = 6n - 1$ oder $6n + 1$ ist, geht hervor, dass sich $f_p(\lambda, 1)$ relativ invariant für die Substitutionsgruppe

$$\lambda,\ \frac{1}{\lambda},\ -\overline{1+\lambda},\ -\frac{1}{1+\lambda},\ -\frac{\lambda}{1+\lambda},\ -\frac{1+\lambda}{\lambda} \tag{2}$$

verhält. Infolge (2) lässt sich, wie gezeigt werden kann, $f_p(\lambda, 1)$ homogen mittels $(\lambda^2+\lambda+1)^3 = K(\lambda)$ und $[\lambda(\lambda+1)]^2 = L(\lambda)$ darstellen, d. h. $f_p(\lambda, 1) = \psi_p(K, L)$ gilt. Die Lösung von $f_p(\lambda, 1) \equiv 0\,(p)$ erfordert also auch die Zerlegung von $\psi_p(K, L)$ in Linearfaktoren $\prod_\nu (K(\lambda) + h_\nu L(\lambda))\ (\mathrm{mod}\, p)$, und man erhält alle Lösungen zu $f_p(\lambda, 1) \equiv 0\,(p)$ durch Auflösen jener Kongruenzen sechsten Grades $K(\lambda) + h_\nu L(\lambda) \equiv 0\,(p)$, die als Invarianten für jede Substitutionsgruppe (2) betrachtet werden können, wo h_ν ein für jede Gruppe bestimmter, charakteristischer Zahlenfaktor ist, der die Invariantenkonstante genannt werden mag. Man findet leicht, dass $\frac{\lambda^{p-1}-1}{\lambda+1}$ sich $(\mathrm{mod}\, p)$ mittels solcher Invarianten $K(\lambda) + h_\nu L(\lambda)$ aufbauen lässt, weil ja immer die Werte $\lambda = +1, \pm 2$ etc, die sämtlich $\frac{\lambda^{p-1}-1}{\lambda+1} \equiv 0\,(p)$ lösen, hinsichtlich der Substitutionsgruppe (2) zusammengefasst werden können, und zwei Gruppen infolge des Gruppencharakters ein Element nicht gemein haben können, ohne identisch zu werden. Ausser den vollständigen Gruppen sechsten Grades existieren auch zwei Nebengruppen vom Grade 2 und 3, deren Elemente als Lösungen respektive aus $\lambda^2+\lambda+1 \equiv 0\,(p)$, also nur für Primzahlen $p = 6n+1$ vorhanden sind, und aus

$$\frac{(\lambda-1)(\lambda+2)(2\lambda+1)}{2} = \frac{2\lambda^3+3\lambda^2-3\lambda-2}{2} \equiv 0 \qquad (\mathrm{mod}\, p)$$

wo $p = 6n \pm 1$ ist, erhalten werden können. Weil das Quadrat des letzten Ausdruckes sich auch für die Substitutior $\lambda : -\overline{1+\lambda}$) invariant verhält, so erhält man

$$\left[\frac{(\lambda-1)(\lambda+2)(2\lambda+1)}{2}\right]^2 \equiv K(\lambda) + h_q L(\lambda) \qquad (\mathrm{mod}\, p) \tag{3}$$

wo h_q aus

$$K(1) + h_q L(1) \equiv 0 \qquad (\mathrm{mod}\, p)$$

bestimmt wird, d. h. den Wert

$$h_q \equiv -\frac{27}{4} \qquad (\mathrm{mod}\, p) \tag{4}$$

erhält. Man hat also

$$\frac{\lambda^{p-1}-1}{\lambda+1} \equiv (\lambda^2+\lambda+1)^{\varepsilon} \sqrt{K(\lambda) - \frac{27}{4} L(\lambda)} \prod_{(\nu)}^{n-1} [K(\lambda) + h_\nu L(\lambda)] \pmod{p} \quad (5)$$

weil die Anzahl der vollständigen Gruppen immer gleich $n-1$ ist. Es sei noch bemerkt, dass es nur für die aus (5) genommenen Invariantenkonstanten h_ν zutrifft, dass eine Kongruenz $K(\lambda) + m L(\lambda) \equiv 0 (p)$ überhaupt auflösbar werden kann. Auf dieselbe Weise lassen sich nun auch die Werte aus

$$\frac{\lambda^{\varphi(p^2)}-1}{\lambda+1} \equiv 0 \pmod{p^2} \quad (6)$$

zu Gruppen und Invarianten zusammenführen. Als beleuchtendes Beispiel teile ich die folgende Zahlentabelle für $p = 11$ mit, wo die Werte also (mod 121) zusammengefasst worden sind.

Eingang-Elemente:	λ	$-\lambda$	$\frac{\lambda}{\lambda+1}$	$-\frac{\lambda}{\lambda+1}$	$\frac{\lambda}{-\lambda-1}$	$\frac{\lambda}{-\lambda+1}$	Invarianten
$4+n.11$	—	—	—	—	—	—	— —
$4+0.11$	4	−30	− 5	+ 24	− 25	+ 29	$K_1 - 41 . L$
$4+1.11$	15	− 8	− 16	− 53	+ 52	+ 7	$K - 30 . L$
$4+2.11$	26	14	− 27	− 9	+ 8	− 15	$K - 19 . L$
$4+3.11$	37	36	− 38	+ 35	− 36	− 37	$K - 8 . L$
$4+4.11$	48	58	− 49	− 42	+ 41	− 59	$K + 3 . L$
$4+5.11$	59	− 41	− 60	+ 2	− 3	+ 40	$K + 14 . L$
$4+6.11$	− 51	− 19	+ 50	+ 46	− 47	+ 18	$K + 25 . L$
$4+7.11$	− 40	+ 3	+ 39	− 31	+ 30	− 4	$K + 36 . L$
$4+8.11$	− 29	+ 25	+ 28	+ 13	− 14	− 26	$K + 47 . L$
$4+9.11$	− 18	+ 47	+ 17	+ 57	− 58	− 48	$K + 58 . L$
$4+10.11$	− 7	− 52	+ 6	− 30	+ 19	+ 51	$K - 52 . L$
$1+n.11$	—	—	—	—	—	—	— —
$1+0.11$	1	1	− 2	+ 60	+ 60	− 2	$\sqrt{K - 37 . L}$
$1+1.11$	12	− 10	− 13	− 28	+ 27	+ 9	$K - 37 . L$
$1+2.11$	23	− 21	− 24	+ 5	− 6	+ 20	$K - 37 . L$
$1+3.11$	34	− 32	− 35	+ 38	− 39	+ 31	$K - 37 . L$
$1+4.11$	45	− 43	− 46	− 30	− 50	+ 42	$K - 37 . L$
$1+5.11$	56	− 54	− 57	− 17	+ 16	+ 53	$K - 37 . L$
$-1+n.11$	—	—	—	—	—	—	— —
$-1+1.11$	10	− 12	—	—	—	—	$(\lambda+1)^2$
$-1+2.21$	21	− 23	—	—	—	—	$(\lambda+1)^2$
$-1+3.11$	32	− 34	—	—	—	—	$(\lambda+1)^2$
$-1+4.21$	43	− 45	—	—	—	—	$(\lambda+1)^2$
$-1+5.11$	54	− 76	—	—	—	—	$(\lambda+1)^2$

Alles in allem bilden die Elemente dieser Tabelle $6 \cdot 11 + 6 \cdot 5 + 2 \cdot 5 + 3 = 109$ verschiedene zu 121 relativ prime Werte, die also mit den $\varphi(11^2) - 1 = 109$ überhaupt existierenden zusammenfallen. Weiter findet man, dass die Gruppen mit den Eingangelementen $4 + 11n$ die Folge der Invarianten konstanten $-41 + 11n, n = 0, 1, .., 10$ haben, d. h. dass die elf Gruppen mit dem ersten Kolonnenelemente $4 + 11n$ sich (mod 11) zu der Gruppe $4, 3, -5, 2, -3, -4$ mit der Invariantkonstante -8 zusammenziehen. Die Elemente $1 + 11n$ haben dagegen alle dieselbe Invariante, deren Konstante $\equiv -4 \pmod{11}$ ist, und die Werte $-1 + 11n$ haben die Invariante $(\lambda + 1)^2$. Ehe ich zu prüfen übergehe, in wie weit die oben angegebenen Eigenschaften allgemein giltig sind, will ich auf folgenden Sachen hinweisen. Aus

$$\begin{aligned} K - 41L &\equiv K - 8L + 8 \cdot 11 \\ K - 30L &\equiv K - 8L + 7 \cdot 11 \qquad \pmod{121} \end{aligned}$$

etc.

folgt

$$\prod_{n=0}^{10} [K - (41 + 11n)L] \equiv (K - 8L)^{11} + (K - 8L)^{10} \, 11 \sum_{1}^{10} n + \cdots \equiv \tag{7}$$

$$\equiv (K - 8L)^{11} \qquad \pmod{121}$$

Man erhält also

$$\frac{\lambda^{110} - 1}{\lambda + 1} \equiv \frac{[(K - 8L)\sqrt{K - 37L}\,(\lambda + 1)]^{11}}{\lambda + 1} \qquad \pmod{121} \tag{8}$$

d. h. die elfte Potenz der Invarianten zu $\frac{\lambda^{10} - 1}{\lambda + 1} \equiv 0 \pmod{11}$. Mit Hülfe der oben gegebenen Andeutungen kann die allgemeine Untersuchung auf folgende Weise durchgefürt werden. Man wähle zum Eingangelemente $a + np, n = 0, 1, \ldots p - 1$, wo a einer Nebengruppe (mod p) nicht gehören darf, und führe auf diesen Kolonnenelementen die Gruppenoperationen aus. Es entsteht daraus ein Gruppensystem (a) von Werten, wo infolge des Gruppencharakters alle Gruppen verschieden sind, und kein Element zweimal in derselben Gruppe auftreten kann. Beim Übergange zu (mod p) würde nämlich eine Nebengruppe hervorkommen, was dem Auswahle des Elementes a wiederspricht. In diesem Systeme (a) stehen also $6p$ zu p^2 relativ prime und unter einander verschiedene Werte. Wählt man ein Element b, das nicht in der vorigen Gruppe a liegt, und verfährt man wie oben, so erhält man noch $6p$ verschiedene Werte, von denen keiner im System (a) vorkommen kann, denn beim Übergange zu (mod p) würden sonst die Gruppen a und b zusammenfallen. In der Weise erhält man zu jeder vollständigen Gruppe a

vom sechsten Grade $(\mathrm{mod}\, p)$ ein Gruppensystem (a) $(\mathrm{mod}\, p^2)$. Das System, das $(\mathrm{mod}\, p)$ zu der Nebengruppe dritten Grades gehört, nenne ich System (1), und zweiten Grades System (c). Vom Kolonnenelemente $1+np, n=0,1,\ldots\frac{p-1}{2}$ ausgehend findet man, dass dasselbe Element nicht zweimal in derselben Gruppe ausser in $1,-2,-\frac{1}{2}$ $(\mathrm{mod}\, p^2)$ vorkommen kann. Man hat nur noch zu zeigen, dass für Eingangelemente $1+np$, wo $n\leq\frac{p-1}{2}$ ist, nicht zwei Elemente dieses Typus in derselben Gruppe stehen können, denn sie können nur so mit einander zusammenstehen, dass $(1+n_1p)(1+n_2p)\equiv 1 \pmod{p^2}$ gilt, d. h. $n_1+n_2\equiv 0\,(p)$, was ausgeschlossen sein muss, weil n_1 und $n_2\leq\frac{p-1}{2}$ sind. Man erhält also von den Eingangelementen $1+np, \frac{p-1}{2}$ verschiedene, vollständige Gruppen sechsten Grades $(\mathrm{mod}\, p^2)$, und so die Nebengruppe $(\mathrm{mod}\, p^2)$ selbst vom dritten Grade. Die Kolonnenelemente $-1+np, n=0,1,\ldots\frac{p-1}{2}$ ergeben nur zweielementige Gruppen, denn die übrigen Elemente können nicht zu p^2 prim auftreten. Weil $(-1+np)x\equiv 1$ (p^2) die Lösung $x\equiv-(1+np)$ besitzt, so folgt $(\lambda+1-np)(\lambda+1+np)\equiv(\lambda+1)^2$ (p^2) als die Invariante jener Gruppen. Sind in der Weise alle Werte $-1+np$ genommen worden, so sind also für $p=6n-1$, wo keine Nebengruppe zweiten Grades auftreten kann, alle zu p^2 prime Werte gefunden, deren Anzahl also gleich

$$6(n-1)p+6\frac{p-1}{2}+3+2\frac{p-1}{2}=(6n-2)p-1=\varphi(p^2)-1$$

ist, und die Zahl der Gruppen

$$(n-1)p+\frac{p-1}{2}+1+\frac{p-1}{2}=n\cdot p,$$

wie zu erwarten war. Das Zusammenrechnen der Elemente für $p=6n+1$ wird erst folgen, wenn das der Nebengruppe zweiten Grades $(\mathrm{mod}\, p)$ gehörige System (c) eingehend diskutiert worden ist.

In der folgenden Darstellung möge mit $a_m^{(b)}$ ein Element genannt werden, das in b:ter Kolonne und $m+1$:ter Zeile steht, und statt $a_0^{(b)}$ wird einfach $a^{(b)}$ geschrieben. In der Tabelle oben ging ich vom Eingangelemente $a_m^{(1)}=a^{(1)}+mkp$ aus, wo k gleich Eins gewählt wurde, aber doch beliebig zu wählen war.

Aus

$$\begin{matrix} a_m^{(1)} \quad a_m^{(2)} \equiv 1 \\ a_{m+1}^{(1)} a_{m+1}^{(2)} \equiv 1 \end{matrix} \quad (p^2)$$

ergibt sich nach Subtraktion und Anwendung von

$$a_{m+1}^{(1)} - a_m^{(1)} = kp$$

$$a_m^{(1)}\left(a_{m+1}^{(2)} - a_m^{(2)}\right) + kpa_{m+1}^{(2)} \equiv 0 \quad (p^2)$$

oder auch

$$a_{m+1}^{(2)} - a_m^{(2)} \equiv -kpa_{m+1}^{(2)} a_m^{(2)} \quad (p^2). \tag{9}$$

Es ist aber

$$a_{m+1}^{(1)} a_m^{(1)} \equiv (a^{(1)})^2 + ka^{(1)} p(2m+1)$$

oder

$$a_{m+1}^{(1)} a_m^{(1)} \equiv (a^{(1)})^2 \quad (p)$$

und aus

$$a_{m+1}^{(1)} a_m^{(1)} a_{m+1}^{(2)} a_m^{(2)} \equiv 1 \quad (p)$$

ergibt sich

$$a_{m+1}^{(2)} a_m^{(2)} \equiv \left(\frac{1}{a^{(1)}}\right)^2 \equiv (a^{(2)})^2 \quad (p)$$

d. h. (9) lässt sich schreiben

$$a_{m+1}^{(2)} - a_m^{(2)} \equiv [-k(a^{(2)})^2]p \quad (p^2),$$

wo

$$-k(a^{(2)})^2 = [-k(a^{(2)})^2] + lp$$

ist, und also $[-k(a^{(2)})^2]$ der Rest, nachdem $-k(a^{(2)})^2$ nach (mod p) reduziert worden ist. In ähnlicher Weise können die Kolonnenwerte der übrigen Kolonnen bestimmt werden, so dass man das folgende Schema aller Werte erhält

$$
\begin{aligned}
a_m^{(1)} &\equiv a^{(1)}+m\,kp, & k &= \text{beliebig}\\
a_m^{(2)} &\equiv a^{(2)}+mk_2p, & k_2 &= [-k(a^{(2)})^2]\\
a_m^{(3)} &\equiv a^{(3)}+mk_3p, & k_3 &= -k\\
a_m^{(4)} &\equiv a^{(4)}+mk_4p, & k_4 &= [+k(a^{(4)})^2] \qquad (p^2)\\
a_m^{(5)} &\equiv a^{(5)}+mk_5p, & k_5 &= -k_4\\
a_m^{(6)} &\equiv a^{(6)}+mk_6p, & k_6 &= -k_2
\end{aligned}
\tag{10}
$$

In der Tabelle für $p=11$ waren $k=1$, $a^{(2)}\equiv -30$, $(a^{(2)})^2\equiv 900\equiv -2$ (11) d. h. $[-k(a^{(2)})^2]=2$. Also werden die Elemente der zweiten Kolonne gleich $a_m^{(2)}\equiv -30+2.11m$, und $(a^{(4)})^2\equiv 576\equiv 4$, $[+k(a^{(4)})^2]\equiv 4$, d. h. $a_m^{(4)}\equiv 24+4.11m$, $a_m^{(5)}\equiv -25-4.11m$, $a_m^{(6)}\equiv 20-2.11m$, Werte, die in der Tabelle leicht gefunden werden können. Ähnliche Resultate erhält man für das Gruppensystem (1). Mit Hülfe dieser Resultate kann ohne weiteres eine Tabelle (mod 169) über ein System (c) aus den Lösungen der Kongruenz $\lambda^2+\lambda+1\equiv 0$ (13) ausgeführt werden, d. h. in diesem Falle haben wir ein System (3), weil $3^2+3+1\equiv 0$ (13) ist. Die erste Gruppenzeile (mod 169) wird also, $+3, -56, -4, +42, -43, +55$ (mod 169) und daraus nach (10) die übrigen

$$
\begin{aligned}
a_m^{(1)} &\equiv +\ 3+13m & a_m^{(4)} &\equiv +42-4.13m\\
a_m^{(2)} &\equiv -56-\ 3.13m & a_m^{(5)} &\equiv -43+4.13m\\
a_m^{(3)} &\equiv -\ 4-13m & a_m^{(6)} &\equiv +55+3.13m
\end{aligned}
\tag{169}
$$

Infolge des Charakters des Systems (3), aus Lösungen zu $\lambda^2+\lambda+1\equiv 0$ (13) hervorgegangen zu sein, folgt, dass es für alle m $a_m^{(2)}\equiv a_m^{(3)}\equiv a_m^{(5)}$ und $a_m^{(1)}\equiv a_m^{(4)}\equiv a_m^{(6)}$ (13) gelten muss.

Weil aber zwei Zeilen nicht dasselbe Element enthalten können ohne identisch zu werden, und weil dasselbe Element nur zweimal in Kolonnen, die einander (mod 13) kongruent sind, auftreten kann, denn nur jene führen zum selben Werte für (mod p) über, so erhält man die Zahl der doppelt vorkommenden Zeilen durch Lösen der diophantischen Gleichung

$$a_x^{(1)}\equiv a_y^{(4)}\equiv a_z^{(6)}$$

d. h.

$$4y+x\equiv 3 \pmod{13}$$

oder

$$y = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12$$
$$x = 3,\ 12,\ 8,\ 4,\ 0,\ 9,\ 5,\ 1,\ 10,\ 6,\ 2,\ 11,\ 7.$$

Gehe ich also von der ersten Zeile als behalten aus, dann muss die dritte gestrichen werden, weil $a_0^{(1)} \equiv a_3^{(4)}$ die Identität dieser Zeilen mit sich führt. Mit der dritten muss dann auch infolge $a_4^{(1)} \equiv a_3^{(4)}$, die aus $y \equiv 3$ und $x \equiv 4$ hervorgeht, gestrichen werden. Mit $y \equiv 4$ und $x \equiv 0$ sind wir nun in der ersten Zeile wieder, und es sollen also folgende Zeilen als doppelt auftretend gestrichen werden

behaltene Zeile	gestrichene Zeile
$m = 0$	$m = 3$ und 4
$m = 1$	$m = 12$ » 7
$m = 2$	$m = 8$ » 10
$m = 5$	$m = 9$ » 6

d. h. für jede behaltene Zeile müssen zwei gestrichen werden, eine Eigenschaft, deren Allgemeinheit für jedes System (c) auf folgende Weise dargelegt werden kann. Aus

$$c_m^{(1)} \equiv c^{(1)} + mp \text{ und } c_m^{(4)} \equiv c^{(4)} + mk_4 p$$

erhält man nach (10)

$$k_4 \equiv [+k(c^{(4)})^2] \equiv \left[\frac{1}{(1+c^{(1)})^2}\right] \equiv \frac{1}{c^{(1)}} \equiv -(1+c^{(1)})$$

d. h. aus

$$c_x^{(1)} \equiv c_y^{(4)};\ c^{(1)} + xp \equiv -\frac{1}{1+c^{(1)}} + yk_4 p \quad (p^2)$$

$$x \equiv -\frac{(c^{(1)})^2 + c^{(1)} + 1}{p(1+c^{(1)})} + yk_4 \equiv b + yk_4 \quad (p).$$

Für

$y \equiv r$	erhält man	$x \equiv b + rk_4$
$y \equiv b + rk_4$	» »	$x \equiv b + k_4(b + rk_4) \equiv rk_4^2 + b(1 + k_4)$ (p)
$y \equiv rk_4^2 + b(1 + k_4)$	» »	$x \equiv rk_4^3 + b(1 + k_4 + k_4^2) \equiv r$

weil, wie oben gezeigt wurde, $k_4 \equiv -(1 + c^{(1)}) \pmod p$ gilt, wo

$$(c^{(1)})^2 + c^{(1)} + 1 \equiv 0 \quad (p)$$

ist. Mit $m=r$ als behaltene Zeile müssen also $m\equiv b+rk_4$ und $m\equiv rk_4^2+b(1+k_4)$ (p) gestrichen werden, d. h. nur ein Drittel der Zeilen sollen behalten werden, wenn die Nebengruppe zweiten Grades $(\mathrm{mod}\, p^2)$ selbst nicht gerechnet wird. Man kann natürlich auch $c_x^{(1)}\equiv c_x^{(6)}(p)$ gebrauchen. Es lässt sich dann auch leicht zeigen, dass dabei dieselben Zeilen gestrichen werden müssen. In einem Systeme (c) kommen also $\frac{p-1}{3}$ vollständige Gruppen vor und das Zusammenrechnen der Elemente im Falle $p=6n+1$ ergibt also:

Elemente

$$6p(n-1)+6\frac{p-1}{2}+2\frac{p-1}{2}+3+6\frac{p-1}{3}+2=p(p-1)-1=\varphi(p^2)-1,$$

Zahl der Gruppen

$$p(n-1)+\frac{p-1}{2}+1+\frac{p-1}{2}+\frac{p-1}{3}+1=np+2n+1.$$

Voll ausgeschrieben sieht die Tabelle für das System (3) (mod 169), wie auf der folgenden Seite angegeben worden ist, aus.

Die Untersuchung der Invariantenkonstanten schreitet auf folgende Weise fort.

Für ein System (a) möge k_{τ_v} die Invariantenkonstanten $(\mathrm{mod}\, p^2)$ heissen und k_τ die der Gruppe a $(\mathrm{mod}\, p)$. Dann gilt für alle v, $k_{\tau_v}\equiv k_\tau$ $(\mathrm{mod}\, p)$, und man erhält, wenn die Invariante der Gruppe v in der Form $\varphi(a_{v-1}^{(1)}, k_{\tau_v})$, wo $k_{\tau_v}\equiv k_{\tau_1}+ +r_v p$ ist, geschrieben wird, folgende Entwicklungen

$$\varphi(a_{v-1}^{(1)}, k\,)\equiv\varphi(a^{(1)}+vkp, k_{\tau_1}+r_v p)\equiv$$

$$\equiv\varphi(a^{(1)}, k_{\tau_1})+vkp\varphi'_a(a^{(1)}, k_{\tau_1})+r_v p\varphi'_k(a^{(1)}, k_{\tau_1})\equiv 0 \quad (p^2)$$

wo $\varphi'_a(a^{(1)}, k_{\tau_1})$ die Derivierte der Funktion $\varphi(a^{(1)}, k_{\tau_1})$ nach $a^{(1)}$ als Variabel ist. Ähnliches gilt für $\varphi'_k(a^{(1)}, k_{\tau_1})$.

Aus der vorigen Kongruenz erhält man

$$vk\varphi'_a(a^{(1)}, k_{\tau_1})+r_v\varphi'_k(a^{(1)}, k_{\tau_1})\equiv 0 \quad (p). \tag{11}$$

Wäre es möglich, dass in einem System (a) $k_{\tau_\mu}\equiv k_{\tau_v}$ (p^2) für $\mu\neq v$ gelten könnte, so ergäbe (11) für $r_\mu\equiv r_v$ (p)

$$\mu k\varphi'_a(a^{(1)}, k_{\tau_1})+r_v\varphi'_k(a^{(1)}, k_{\tau_1})\equiv 0 \quad (p).$$

Nach Subtraktion erhält man

$$k(\mu-v)\varphi'_a(a^{(1)}, k_{\tau_1})\equiv 0 \quad (p)$$

d. h weil $\mu\neq v$ und $k_{\tau_1}\equiv k_\tau$ (p) ist, ergibt sich

1 λ	2 $\frac{1}{\lambda}$	3 $-(1+\lambda)$	4 $-\frac{1}{1+\lambda}$	5 $-\frac{\lambda}{1+\lambda}$	6 $-\frac{\lambda+1}{\lambda}$
$3+0\cdot 13\equiv +3$	$-56-0\cdot 39\equiv -56$	$-4-0\cdot 13\equiv -4$	$42-0\cdot 52\equiv +42$	$-43+0\cdot 52\equiv -43$	$55+0\cdot 39\equiv +55$
$3+1\cdot 13\equiv +16$	$-56-1\cdot 39\equiv +74$	$-4-1\cdot 13\equiv -17$	$42-1\cdot 52\equiv -10$	$-43+1\cdot 52\equiv +9$	$55+1\cdot 39\equiv -75$
$3+2\cdot 13\equiv +29$	$-56-2\cdot 39\equiv +35$	$-4-2\cdot 13\equiv -30$	$42-2\cdot 52\equiv -62$	$-43+2\cdot 52\equiv +61$	$55+2\cdot 39\equiv -36$
$3+3\cdot 13\equiv +42$	steht in der Zeile 1, Kolonne 4, und deshalb wird diese Zeile gestrichen $m=0$				
$3+4\cdot 13\equiv +55$	» » » » 1, » 5, » » » » » » $m=0$				
$3+5\cdot 13\equiv +68$	$-56-5\cdot 39\equiv -82$	$-4-5\cdot 13\equiv -69$	$42-4\cdot 52\equiv -49$	$-43+5\cdot 52\equiv +48$	$55+5\cdot 39\equiv +81$
$3+6\cdot 13\equiv +81$	steht in der Zeile 6, Kolonne 6, und deshalb wird diese Zeile gestrichen $m=5$				
$3+7\cdot 13\equiv -75$	» » » » 2, » 6, » » » » » » $m=1$				
$3+8\cdot 13\equiv -62$	» » » » 3, » 4, » » » » » » $m=2$				
$3+9\cdot 13\equiv -49$	» » » » 6, » 4, » » » » » » $m=5$				
$3+10\cdot 13\equiv -36$	» » » » 3, » 6, » » » » » » $m=2$				
$3+11\cdot 13\equiv -23$	$-56-11\cdot 39\equiv +22$	$-4-11\cdot 13\equiv +22$	$42-11\cdot 52\equiv -23$	$-43+11\cdot 52\equiv +22$	$55+11\cdot 39\equiv -23$
$3+12\cdot 13\equiv -10$	steht in der Zeile 2, Kolonne 4, und deshalb wird diese Zeile gestrichen $m=1$				

(mod 169).

$$\begin{matrix}\varphi'_a(a^{(1)},k_\tau)\equiv 0\\ \varphi\ \ (a^{(1)},k_\tau)\equiv 0\end{matrix}\quad (p)$$

die gleichzeitig gelten müssen, was nur für Nebengruppen zutreffen kann. In einem System (a) können also die k_{τ_v} in folgender Form gesetzt werden

$$k_{\tau_v}\equiv k_{\tau_1}+vrp\quad (p^2) \tag{12}$$

wo r aus der Kongruenz

$$k\varphi'_a(a^{(1)},k_{\tau_1})+r\varphi'_k(a^{(1)},k_{\tau_1})\equiv 0\quad (p)$$

bestimmt worden ist. Auf dieselbe Weise kann auch gezeigt werden, dass in einem Systeme (1) alle Invariantenkonstanten gleich werden, denn setzen wir $\varphi(1,k_\tau)\equiv 0\,(p)$ und $\varphi(1+\mu p,k_{\tau_\mu})\equiv 0\,(p^2)$, so ergibt sich für $k_{\tau_\mu}\equiv k_{\tau_1}+r_\mu p\ (p^2)$

$$\varphi(1+\mu p,k_{\tau_1}+r_\mu p)\equiv\varphi(1,k_{\tau_1})+\mu p\varphi'(1,k_{\tau_1})+r_\mu p\varphi'_k(1,k_{\tau_1})\equiv 0\quad (p^2)$$

d. h.

$$r_\mu p\varphi'_k(1,k_{\tau_1})\equiv r_\mu p[(1+\mu p)(2+\mu p)]^2\equiv 0\quad (p^2)$$

oder $r_\mu\equiv 0\ (p)$ d. h. $r_\mu=0$, und es gelten also für alle diese Gruppen

$$k_{\tau_v}\equiv k_{\tau_a}\equiv -\frac{27}{4}\qquad (\mathrm{mod}\ p^2) \tag{12}$$

und die Invariante der Nebengruppe selbst mag

$$\sqrt{K(\lambda)+k_{\tau_a}L(\lambda)}$$

geschrieben werden.

Weil also in einem System (a) für $v\neq\mu$ auch immer $k_{\tau_v}\not\equiv k_{\tau_\mu}\ (p^2)$ gilt, so erhält man

$$\prod_v[K(\lambda)+k_{\tau_v}L(\lambda)]\equiv[K(\lambda)+k_{\tau_s}L(\lambda)]^p+[\ ]^{p-1}Lp\sum_1^{h-1}n+\cdots\equiv$$

$$\equiv[K(\lambda)+k_{\tau_s}L(\lambda)]^p\quad (p^2)$$

wo k_{τ_s} eine beliebige Invariantenkonstante innerhalb des Systems (a) ist, das also als Lösung aus der Kongruenz

$$[K(\lambda)+k_{\tau_s}L(\lambda)]^p\equiv 0\quad (p^2)$$

erhalten werden kann. Man sieht aber leicht ein, dass schon

$$[K(\lambda)+k_{\tau_s}L(\lambda)]^2\equiv 0\quad (p^2) \tag{13}$$

dies tut, da jeder Faktor für sich $\equiv 0\,(\mathrm{mod}\,p)$ wird.

In derselben Weise kann auch das ganze System (1) und die Nebengruppe selbst doppelt als Lösung aus

$$[\sqrt{K(\lambda)+k_{\tau_a}L(\lambda)}]^2\equiv 0 \quad (p^2) \tag{14}$$

erhalten werden.

Es sei jetzt angenommen, dass in

$$(\lambda+1)^p-\lambda^p-1=p\lambda(\lambda+1)(\lambda^2+\lambda+1)^e f_p(\lambda,1)$$

$f_p(\lambda,1)\equiv 0\ (p)$ für $\lambda\equiv a\ (p)$ lösbar wäre, d. h. dass $\lambda\equiv a$ eine Lösung der Kongruenz

$$(\lambda+1)^p-\lambda^p-1\equiv 0 \quad (p^2) \tag{15}$$

ist. Dann muss infolge des Invariantencharakters von $f_p(\lambda,1)$ das ganze System die (a) Kongruenz (15) lösen. Schreiben wir also System (a) wie gewöhnlich, dann stehen folgende Elemente in Zeile $m=0$

$$a, \frac{1}{a}, \quad -(1+a), \quad -\frac{1}{1+a}, \quad -\frac{a}{1+a}, \quad -\frac{1+a}{a}$$

und in Zeile $m=v$

$$a^p\equiv a+vp, \quad \frac{1}{a^p}, \quad -(1+a^p), \quad -\frac{1}{1+a^p}, \quad -\frac{a^p}{1+a^p}, \quad -\frac{1+a^p}{a^p}.$$

Infolge (15) kann diese Zeile auch so geschrieben werden

$$a^p, \quad \frac{1}{a^p}, \quad -(1+a)^p, \quad -\frac{1}{(1+a)^p}, \quad -\left(\frac{a}{1+a}\right)^p, \quad -\left(\frac{1+a}{a}\right)^p.$$

Die erste Art die Gruppe $m=v$ zu schreiben ist daraus veranlasst, dass mit a immer $a^p\equiv a+vp$, infolge $\frac{a^{p-1}-1}{p}\equiv\frac{v}{a}\ (p)$ als erstes Kolonnenelement auftreten muss, und die zweite, wie gesagt, weil a eine Lösung zu (15) sein soll. Mit Hülfe der Formeln (10) findet man, dass das System (a), das (15) löst, notwendig die Eigenschaft haben muss, dass die Elemente jeder Gruppe zur p:ten Potenz erhoben kolonnenweise in die einzige Gruppe $m=v$ übergehen, die dabei in sich selbst übergeht. Ich nenne diese spezielle Gruppe innerhalb eines Systemes (a) ihre v-Gruppe und ihre Invariantenkonstante k_{τ_v}. Das Charakteristische der Elemente einer v-Gruppe sind also die beiden Kongruenzen

$$\left.\begin{aligned} \lambda^{p-1} &\equiv 1 \\ (\lambda+1)^{p-1} &\equiv 1 \end{aligned}\right\} \pmod{p^2} \tag{16}$$

die gleichzeitig gelten müssen.

Nun können wir also die notwendige und hinreichende Bedingung dafür, dass das System (*a*) (15) löst, so formulieren, dass es eine v-Gruppe haben muss.

Angenommen, dass eine v-Gruppe existieren kann, was im Falle eines Systems (*c*) unmittelbar einleuchtet, so können folgende Entwicklungen durchgeführt werden. Es sei τ ein Faktor in $p-1$ von der Art, dass schon

$$\left.\begin{aligned} a_v^{(\varrho)^\tau} &\equiv 1 \\ (-1)^\tau \left(1 + a_v^{(\varrho)}\right)^\tau &\equiv 1 \end{aligned}\right\} \pmod{p^2}$$

gelten, dann ergibt sich

$$1 \equiv a_v^{(\varrho)^{r\tau}} \equiv (a^{(\varrho)} + vkp)^{r\tau} \equiv a^{(\varrho)^{r\tau}} + \frac{rv\tau k}{a^{(\varrho)}} p \qquad (p^2)$$

für beliebiges r. Also

$$a^{(\varrho)^{r\tau}} \equiv 1 - \frac{rv\tau k}{a^{(\varrho)}} p \qquad \pmod{p^2} \tag{17}$$

Auf dieselbe Weise erhält man

$$\left(1 + a_v^{(\varrho)}\right)^{r\tau} \equiv (1 + a^{(\varrho)} + vkp)^{r\tau} \equiv$$

$$\equiv (1 + a^{(\varrho)})^{r\tau} \left[1 + \frac{rv\tau k}{1 + a^{(\varrho)}} p\right] \qquad \pmod{p^2}$$

d. h.

$$(1 + a^{(\varrho)})^{r\tau} \equiv (-1)^{r\tau} \left(1 - \frac{rv\tau k}{1 + a^{(\varrho)}} p\right) \qquad \pmod{p^2}.$$

Daraus erhält man für ein beliebiges Gruppenelement $a_m^{(\varrho)}$

$$a_m^{(\varrho)^{r\tau+1}} \equiv (a^{(\varrho)} + mkp)^{r\tau+1} \equiv$$

$$\equiv a^{(\varrho)^{r\tau+1}} + a^{(\varrho)^{r\tau}} mk(r\tau + 1) p \equiv$$

$$\equiv a^{(\varrho)} + k[m(r\tau + 1) - rv\tau] p \equiv$$

$$\equiv a^{(\varrho)} + k[(m - v)(r\tau + 1) + v] p \qquad \pmod{p^2} \tag{18}$$

und so auch

$$(-1)^{r\tau}\left(1+a_m^{(\varrho)}\right)^{r\tau+1}\equiv(1+a^{(\varrho)})+k[(m-v)(r\tau+1)+v]\,p \quad (p^2). \qquad (18^1)$$

Aus (18) und (18^1) ersieht man, dass

$$(-1)^{r\tau}\left(1+a_m^{(\varrho)}\right)^{r\tau+1}\equiv 1+a_m^{(\varrho)r\tau+1} \qquad (\mathrm{mod}\ p^2)$$

gilt, d. h. System $(a^{(1)})$ löst die Kongruenzen

$$(-1)^{r\tau}(1+\lambda)^{r\tau+1}\equiv\lambda^{r\tau+1}+1 \qquad (\mathrm{mod}\ p^2) \qquad (19)$$

für alle r. Die Werte $r=1$ und $\tau=p-1$ ergeben (15). Im Falle $\tau=3$ d. h. $p=6n+1$ drückt (19) eine bekannte Tatsache aus, nähmlich dass alle diese Ausdrücke mit $(\lambda^2+\lambda+1)^2$ teilbar werden.

Weiter folgt aus (18) und (18^1), weil $[(m-v)(r\tau+1)+v]\equiv k_1\ (p)$ eindeutig in k_1 und m lösbar ist, wenn die eine gegeben wird (denn v und τ haben konstante Werte im Gruppensysteme), dass die Elemente einer Gruppe m zur Potenz $(r\tau+1)$ erhoben wieder eine Gruppe desselben Systems bilden, wo die Gruppenzeile aus der obigen Kongruenz gefunden wird. Wiederholt man diese Operation, die man Subst. $\overline{r\tau+1}$ nennen kann, so werden die Gruppenzeilen wieder mit behaltener Kolonnenordnung permutiert und $k_2\equiv(m-v)(r\tau+1)^2+v\ (p)$. Nach s Substitutionen erhält man also die Gruppenzeile $k_s\equiv(m-v)(r\tau+1)^s+v\ (p)$, d. h. die anfängliche, wenn $(r\tau+1)^s\equiv 1\ (p)$ gilt. In derselben Weise kann das System der Subst. $\overline{r\tau-1}$ unterworfen werden. Dabei wird aber die Kolonnenordnung verändert und die Gruppenzeile aus $k_1\equiv(v-m)(r\tau-1)+v\ (p)$ gefunden. Durch Wiederholen ergibt sich $k_2\equiv(m-v)(r\tau-1)^2+v\ (p)$, d. h. weil $(r\tau-1)^2$ eine Substitution von Art $(r\tau+1)$ ist, so haben also die Kolonnen wieder ihre ursprüngliche Ordnung erhalten.

Um das eben angeführte mit Beispielen zu beleuchten, kann man sich der Tabelle des Systems (3) (mod 169) bedienen. Weil $p=13$ die primitiven Wurzeln ± 2 haben und τ gleich 3 ist, so muss die Subst. $\overline{-3+1}$ = Subst. $\overline{-2}$ von der Art sein, alle Gruppenzeilen mit behaltener Kolonnenordnung zu permutieren, und die Elemente nach zwölf Wiederholungen wieder in der anfänglichen Zeile stehen. Man bestätigt dies aus

$3^{-2}\equiv-75$	in	der	Zeile	8		$49^{-2}\equiv+29$	in	der	Zeile	3
$75^{-2}\equiv+81$	»	»	»	7		$29^{-2}\equiv+42$	»	»	»	4
$81^{-2}\equiv-62$	»	»	»	9		$42^{-2}\equiv+16$	»	»	»	2
$62^{-2}\equiv+55$	»	»	»	5		$16^{-2}\equiv+68$	»	»	»	6
$55^{-2}\equiv-10$	»	»	»	13		$68^{-2}\equiv-36$	»	»	»	11
$10^{-2}\equiv-49$	»	»	»	10		$36^{-2}\equiv+3$	»	»	»	1

(mod 169)

Die wiederholte Anwendung der Subst. $\overline{3-1}$ soll dagegen ein Element aus der ersten Kolonne abwechselnd in die zweite und erste Kolonne hineinlegen. In unserer Tabelle für $p=13$ ist $v=11\equiv -2 \pmod{13}$. Setzen wir also in $k_1\equiv(v-m)(r\tau-1)+v$ (13) $v=-2$, $r\tau-1=2$, so ist k_1+1 die Zeile, und die Werte ergeben sich wie hier unten angegeben wird.

Man erhält nähmlich (mod 169)

$3^2\equiv+9$	steht	für	$m=$	0	und	$k_1\equiv$	7	in	der	Zeile	8,	Kol.	2
$9^2\equiv+81$	»	»	$=$	7	»	$\equiv$	6	»	»	»	7,	»	1
$81^2\equiv-30$	»	»	$=$	6	»	$\equiv$	8	»	»	»	9,	»	2
$30^2\equiv+55$	»	»	$=$	8	»	$\equiv$	4	»	»	»	5,	»	1
$55^2\equiv-17$	»	»	$=$	4	»	$\equiv$	12	»	»	»	13,	»	2
$17^2\equiv-49$	»	»	$=$	12	»	$\equiv$	9	»	»	»	10,	»	1
$49^2\equiv+35$	»	»	$=$	9	»	$\equiv$	2	»	»	»	3,	»	2
$35^2\equiv+42$	»	»	$=$	2	»	$\equiv$	3	»	»	»	4,	»	1
$42^2\equiv+74$	»	»	$=$	3	»	$\equiv$	1	»	»	»	2,	»	2
$74^2\equiv+68$	»	»	$=$	1	»	$\equiv$	5	»	»	»	6,	»	6
$68^2\equiv+61$	»	»	$=$	5	»	$\equiv$	10	»	»	»	11,	»	2
$61^2\equiv+3$	»	»	$=$	10	»	$\equiv$	0	»	»	»	1,	»	1

Die Subst. $\overline{3+1}=4$ soll nur Werte aus der ersten Kolonne geben und, da $4^6\equiv 1$ (13) ist, so werden die Gruppenzeilen in zwei Zyklen mit sechs Reihen in jedem Zyklus verteilt etc.

Zuletzt sei noch folgendes hinzugefügt. Vorausgesetzt, dass eine v-Gruppe existiert, so findet man, dass das ganze System (a) die Kongruenz

$$(\lambda^{2p}+\lambda^p+1)^3+h_{\tau_v}[\lambda^p(\lambda^p+1)]^2\equiv 0 \pmod{p^3} \qquad (20)$$

löst, denn sie hat die sechs Lösungen $\lambda^p\equiv a+vp$, $\frac{1}{a+vp}$ etc. (p^3), die infolge $(a+vp)^{p-1}\equiv 1$ etc. (p^3) alle sechs lösbar werden, das ganze System (a) ergebend. Aus der Formel

$$[K(\lambda)+h_{\tau_v}L(\lambda)]^p=K(\lambda)^p+h_{\tau_v}^p L(\lambda)^p+p[K(\lambda)+h_{\tau_v}L(\lambda)]\chi(\lambda)$$

geht hervor, dass das System (a) ebenfalls die Kongruenz

$$(\lambda^3+\lambda+1)^{3p}+h_{\tau_v}^p\,\overline{\lambda(\lambda+1)}^{3p}\equiv 0 \qquad (p^3)$$

löst, weil $K(\lambda)+h_{\tau_v}L(\lambda)\equiv 0 \pmod p$ für das System giltig ist. Also löst das System (a) auch ihre Differenz, die, wenn $\lambda(\lambda+1)\equiv\alpha$ gesetzt wird, infolge (15) sich so schreiben lässt

$$(\alpha^p+1)^3+h_{\tau_v}\alpha^{2p}\equiv(\alpha+1)^{3p}+h_{\tau_v}^p\,\alpha^{2p} \qquad (\mathrm{mod}\ p^2). \tag{21}$$

Trifft es überhaupt zu, dass $h_{\tau_v}^{p-1}\equiv 1\ (p^2)$ ausfällt, dann wird

$$(\alpha+1)^p-\alpha^p-1\equiv 0 \qquad (\mathrm{mod}\ p^2) \tag{22}$$

d. h. wenn das System (λ_s) eine v-Gruppe hat, deren Invariantenkonstante $h_{\tau_v}^{p-1}\equiv 1$ (p^2) genügt, so muss $\lambda_s(\lambda_s+1)\equiv\alpha_s \pmod p$ wieder ein System (α_s) mit einer v-Gruppe geben, von deren Invariantenkonstante aber nichts ausgesagt werden kann.

Was endlich die Existenz der v-Gruppen betrifft, so haben wir gesehen, dass im Falle eines Systems (c) immer v-Gruppe vorhanden ist, im Falle eines Systems (1) zeigt $2^{1092}\equiv 1\ (1093^2)$, dass v-Gruppe vorhanden sein kann, und im Falle eines Systems (a) gibt $p=59$ ein sehr lehrreiches Beispiel, denn es kommen nämlich hier zwei verschiedene v-Gruppen vor, was gar nicht immer unter den mit v-Gruppe versehenen, doch ziemlich seltenen Primzahlen der Fall ist. Man hat die Gruppen

$$\begin{aligned} &4,\ 15,\ -5,\ -12,\ +11,\ -16,\ h_{\tau_v}\equiv 18\\ &3,\ 20,\ -4,\ -15,\ +14,\ -21,\ h_{\tau_v}\equiv\ 4 \end{aligned} \qquad (59) \tag{23}$$

Hier sind:

$$\begin{aligned} 3^{59}&\equiv\ 3+\ 5\cdot 59\\ 4^{59}&\equiv\ 4+\ 5\cdot 59\\ 5^{59}&\equiv\ 5+\ 5\cdot 59\\ 11^{59}&\equiv 11-24\cdot 59\\ 12^{59}&\equiv 12-24\cdot 59\\ 14^{59}&\equiv 14-19\cdot 59\\ 15^{59}&\equiv 15-19\cdot 59\\ 16^{59}&\equiv 16-19\cdot 59\\ 20^{59}&\equiv 20-14\cdot 59\\ 21^{59}&\equiv 21-14\cdot 59\\ 18^{59}&\equiv 18+27\cdot 59 \end{aligned} \qquad (59^2) \tag{24}$$

Die respektiven v-Gruppen sind

$$\begin{matrix}3^{59}\equiv 3+5\cdot 59\\ 4^{59}\equiv 4+5\cdot 59\end{matrix} h_{\tau_v}\equiv 4+17\cdot 59; \quad \begin{matrix}4^{59}\equiv 4+5\cdot 59\\ 5^{59}\equiv 5+5\cdot 59\end{matrix} h_{\tau_v}\equiv 18-32\cdot 59 \qquad (59^2)$$

und im letzten Falle wird h_{τ_v} aus

$$\overline{[4+5\cdot 59^2+4+5\cdot 59+1]^3}+h_{\tau_v}\overline{(4+5\cdot 59)(5+5\cdot 59)^2}\equiv 0 \qquad (59^2)$$

bestimmt d. h.

$$(21-14\cdot 59)^3+h_{\tau_v}(20-14\cdot 59)^2\equiv 0 \qquad (59^2).$$

Schon daraus ersieht man nach den obigen Werten (24), dass

$$h_{\tau_v}^{58}\equiv 1 \qquad (\text{mod } 59^2)$$

gelten muss, was ja auch der Fall ist. Es sollen also die $\lambda(\lambda+1)\equiv\alpha$ (59), wo λ ein Element der Gruppe $h_{\tau_v}\equiv 18$ (59) ist, wieder Gruppen bilden, die als System (α) nach (21) und (22) wieder v-Gruppen haben. In der Tat erhält man, dass $4\cdot 5\equiv 20$, $11\cdot 12\equiv 14$ und $15\cdot 16\equiv 4 \pmod{59}$ sind.

Zusatz.

Endlich wollen wir noch zusehen, unter welchen Bedingungen

$$(\lambda+1)^p-\lambda^p-1\equiv 0 \qquad (\text{mod } p^3)$$

lösbar werden kann. Von demn oben gezeigten ausgehend, sieht man ein, dass sie die Form

$$\begin{matrix}\lambda\equiv a^p\equiv a+mp+np^2\\ (a+1)^p\equiv a+1+mp+np^2\end{matrix} \pmod{p^3}$$

haben müssen, denn

$$(a+mp+np^2+1)^p-(a+mp+np^2)^p-1\equiv 0 \qquad (\text{mod } p^3)$$

gibt

$$(a+1)^p-a^p-1+mp^2((a+1)^{p-1}-a^{p-1})\equiv 0 \qquad (p^3)$$

d. h.

$$(a+1)^p-a^p-1\equiv 0 \qquad (p^3).$$

Von den Lösungen (mod p^2) ausgehend, sieht man ohne weiteres ein, dass sie die obige Form haben müssen. Im Falle $p = 59$ ergibt sich

$$\begin{aligned} 3^{59} &\equiv 3 + 5 \cdot 59 + 34 \cdot 59^2 \\ 4^{59} &\equiv 4 + 5 \cdot 59 - 17 \cdot 59^2 \qquad (\text{mod } 59^3) \\ 5^{59} &\equiv 5 + 5 \cdot 59 + 18 \cdot 59^2 \end{aligned}$$

Es existieren also keine Lösungen zu

$$(\lambda + 1)^{59} - \lambda^{59} - 1 \equiv 0 \qquad (\text{mod } 59^3)$$

Die Kriterien der Lösungen (mod p^4) werden nicht mehr so einfach und übersichtlich.