Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 23 (1949)

Artikel: Über ein Kriterium zur Fermatschen Vermutung.
Autor: Kapferer, Heinrich
DOI: https://doi.org/10.5169/seals-19753

Über ein Kriterium zur Fermatschen Vermutung

Von Heinrich Kapferer, Schwäbisch-Hall

Der Zweck der vorliegenden Arbeit ist der Beweis des Satzes:

Die Gleichung $x^p + y^p + z^p = 0$ *ist für keine Primzahl* $p > 7$ *in ganzen rationalen Zahlen lösbar, für die weder die Diskriminante des Polynoms*

$$\sum_{(r)} \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r+1} \cdot t^r$$

noch $xyz(x-y)(y-z)(z-x)(x^2+y^2+z^2)$ *durch* p *teilbar ist.*

Dieser Satz folgt aus dem *Kriterium*:

Notwendig und hinreichend für die Existenz von drei ganzen rationalen Zahlen x, y, z *und einer Primzahl* $p > 7$, *welche der Kongruenz* $x^p + y^p + z^p \equiv 0 \pmod{p^2}$ *und gleichzeitig der Bedingung*

$$xyz(x-y)(y-z)(z-x)(x^2+y^2+z^2) \not\equiv 0 \pmod{p}$$

genügen, ist die Teilbarkeit der Diskriminante des p *zugeordneten Polynoms*:

$$p \equiv 1 \pmod 3: \quad \sum_{r=0}^{r=\frac{p-7}{6}} \binom{\frac{p-3}{2} - r}{2r} \cdot \frac{1}{2r+1} u^{\frac{p-7}{6}-r} \cdot v^r ;$$

$$p \equiv 2 \pmod 3: \quad \sum_{r=0}^{r=\frac{p-5}{6}} \binom{\frac{p-3}{2} - r}{2r} \cdot \frac{1}{2r+1} u^{\frac{p-5}{6}-r} \cdot v^r$$

durch die Primzahl p. *Die Diskriminante* $\Delta(p)$ *ist stets eine ganze, von* 0 *verschiedene Zahl.*

Die Bedingung $(x-y)(y-z)(z-x) \not\equiv 0 \pmod{p}$ bedeutet nur für solche Primzahlen p eine Einschränkung, für welche $2^p \equiv 2^1 \pmod{p^2}$ erfüllt ist, also erstmals für $p = 1093$. Die Bedingung $x^2 + y^2 + z^2 \not\equiv 0$

(mod p) bedeutet für die Primzahlen $p \equiv 1 \pmod 3$, und nur für diese, eine Einschränkung; denn sie ist ein symmetrischer Ausdruck für die *dreifache* Bedingung $x^2 + xy + y^2 \not\equiv 0 \pmod p$, $y^2 + yz + z^2 \not\equiv 0 (p)$, $z^2 + zx + x^2 \not\equiv 0 \pmod p$, von denen jede mit der ersteren äquivalent ist vermöge $x + y + z \equiv 0 \pmod p$.

Nach meinen tabellarischen Rechnungen ist die Diskriminante für $p < 100$ nur für 59, 79 und 83 durch p teilbar.

Im *Kummer*schen Kriterium gibt es unterhalb 100 ebenfalls genau drei Ausnahmezahlen, drei nicht reguläre Primzahlen: 37, 59, 67.

Weder durch mein Kriterium noch durch dasjenige von Kummer ist bewiesen, daß es unendlich viele Primzahlen gibt, die das Kriterium nicht erfüllen. Aus ersterem folgt u. a. — für $x = 1$, $y = 2$, $z = -3$ —, daß die Kongruenz $1^p + 2^p - 3^p \equiv 0 \pmod{p^2}$, $p > 7$, höchstens dann eine Lösung haben kann, wenn $\Delta(p)$ durch p teilbar ist[1]). Nun folgt aber aus $x^p + y^p + z^p = 0$ bekanntlich $2^p \equiv 2 \pmod{p^2}$, falls nur keine der Zahlen x, y, z durch $2p$ teilbar ist, und analog folgt $3^p \equiv 3 \pmod{p^2}$, falls nur keine der Zahlen x, y, z durch $3p$ teilbar ist, beides leichte Folgerungen aus dem „ersten" und dem „zweiten" *Furtwängler*schen Satz (in der Wiedergabe von Landaus Vorlesungen über Zahlentheorie, III. Bd.). Verbindet man diese beiden Tatsachen mit unserem obigen Ergebnis, so gelangt man zu der Erkenntnis: *Die Fermatsche Vermutung ist wahr für jede Primzahl p, die nicht in der Diskriminante des p zugeordneten Polynoms*

$$\sum_{(r)} \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r+1} \cdot t^r$$

aufgeht, falls unter den Zahlen x, y, z keine durch $2p$ und auch keine durch $3p$ teilbar ist.

Bemerkenswert ist ferner, daß das Kriterium eine Verschärfung in folgender Richtung zuläßt: Falls es k Zahlentripel x, y, z von der im Kriterium genannten Art geben sollte, von denen keine zwei einander proportional und von denen keine zwei durch Permutation von x, y, z auseinander hervorgehen, so ist die Diskriminante notwendig durch p^k teilbar. Jedoch wollen wir uns in dem nunmehr folgenden Beweis auf die *grundsätzliche* Tatsache beschränken, wie sie in der oben gegebenen Formulierung des Kriteriums ausgesprochen ist.

---

[1]) Aus $3^p \equiv 3 (p^2)$ und $p \equiv 1 (3)$ *allein* folgt schon — so teile ich hier, ohne Beweis, mit — $\Delta(p) \equiv 0 \pmod p$, während bei $3^p \equiv 3 \pmod{p^2}$ und $p \equiv 2 (3)$ $\Delta(p)$ *nicht durch* p teilbar zu sein braucht, wie das Beispiel $p = 11$ zeigt.

Die Frage nach der Existenz von Lösungen der *ternären* Kongruenz $x^p + y^p + z^p \equiv 0 \pmod{p^2}$ wird, vermöge der unmittelbaren Folgerung aus ihr: $x + y + z \equiv 0 \pmod{p}$, auf die *binäre* Kongruenz zurückgeführt: $(x + y)^p - x^p - y^p \equiv 0 \pmod{p^2}$. Wir haben es also nur noch mit den zerlegbaren Polynomen $A_p(x, y) = (x + y)^p - x^p - y^p$ zu tun. Wenn wir dieselben auf ihre Teilbarkeit durch p untersuchen wollen, so ist es zweckmäßig, zuerst etwaige algebraische Teiler mit Koeffizienten aus dem Körper der rationalen Zahlen abzuspalten. Als solche erkennt man sofort x und y und $(x + y)$. Daß überdies noch ein quadratischer Faktor dieser Art stets vorhanden ist, bei $p > 3$, nämlich $x^2 + xy + y^2$, darauf hat zuerst *A. Cauchy* hingewiesen und er hat auch gezeigt, daß sogar $(x^2 + xy + y^2)^2$ als Teiler vorhanden ist jedesmal dann, und nur dann, wenn $p \equiv 1 \pmod 3$ ist. Wesentlich ist ferner, daß p selbst als Faktor des nach Potenzprodukten von x, y geordneten Polynoms heraustritt. Demnach hat man es nur zu tun mit der Kongruenz:

$$C_p(x, y) = \frac{(x + y)^p - x^p - y^p}{pxy(x + y)(x^2 + xy + y^2)^s} \equiv 0 \pmod{p^1} ,$$

wobei $2s \equiv p \pmod 3$, und s die kleinste natürliche Zahl dieser Art ist. Wir wollen diese ganze Klasse von Polynomen $C_p(x, y)$, die eineindeutig der unendlichen Reihe der Primzahlen zugeordnet sind, kurz als *Cauchy*sche Polynome bezeichnen. Eine explizite Entwicklung dieser Polynome nach Potenzprodukten von x, y hat Cauchy allerdings nicht gegeben, auch, wie es scheint, kein anderer Autor seither. Wie man sie trotzdem auf ihre Teilbarkeit durch p prüfen kann, dazu werde ich im folgenden einen sicheren Weg zeigen. Zunächst stellen wir folgendes fest:

1. *Jedesmal, wenn überhaupt die Kongruenz* $C_p(x, y) \equiv 0 \pmod p$ *eine Lösung besitzt, etwa* $x \equiv \alpha y \pmod p$, *mit* $\alpha(\alpha + 1)(\alpha^2 + \alpha + 1) \not\equiv 0 \pmod p$, *so sind gleichzeitig* $\frac{\partial C}{\partial x} \equiv 0 \pmod p$ *und* $\frac{\partial C}{\partial y} \equiv 0 \pmod p$ *erfüllt, für ein und dasselbe* α; *mit anderen Worten: Jede etwa vorhandene Kongruenzwurzel zählt doppelt.*

Beweis: $\frac{1}{p} A_p(x, y) = xy(x + y)(x^2 + xy + y^2)^s \cdot C_p(x, y) = U(x, y) \cdot C_p(x, y)$

$$\frac{1}{p} \cdot \frac{\partial A}{\partial x} = (x + y)^{p-1} - x^{p-1} = U \cdot C'_x + U'_x \cdot C ;$$

$$\frac{1}{p} \cdot \frac{\partial A}{\partial y} = (x + y)^{p-1} - y^{p-1} = U \cdot C'_y + U'_y \cdot C ;$$

$$(x+y)^{p-1} - x^{p-1} \equiv y(x-y)(x-2y)\ldots(x-(p-2)y) \pmod{p};$$
$$(x+y)^{p-1} - y^{p-1} \equiv x(x-y)(x-2y)\ldots(x-(p-2)y) \pmod{p}.$$

Aus vorstehenden fünf Zeilen folgt unmittelbar die Behauptung (1).

Jetzt erst machen wir von dem fundamentalen Satz Gebrauch, daß jede beliebige binäre Form mit rationalen Koeffizienten, $P(x, y)$, nach Wahl einer beliebigen Primzahl p als Modul, eindeutig als Produkt von Primfunktionen (mod p) zerlegt werden kann, d. h. als Produkt von solchen homogenen Polynomen in x, y mit ganzen rationalen Koeffizienten, die selbst nicht mehr weiter (mod p) zerlegt werden können: $P(x, y) \equiv q_1^{r_1}(x, y) \cdot q_2^{r_2}(x, y) \ldots q_t^{r_t}(x, y) \pmod{p}$. Wegen der Eindeutigkeit der Zerlegung (unter Voraussetzung einer gewissen Normierung der Polynome, die hier keine Rolle spielt) können die beiden abgeleiteten Polynome $\frac{\partial P}{\partial x}$ und $\frac{\partial P}{\partial y}$, vermöge $x \cdot \frac{\partial P}{\partial x} + y \frac{\partial P}{\partial y} = mP$, dann und nur dann ein und dieselbe Primfunktion $q(x, y) \pmod{p}$ als *gemeinsamen* Teiler besitzen, wenn eben dieselbe Primfunktion in der Zerlegung von P selbst mindestens die Multiplizität 2 besitzt. Daraus resultiert die bekannte Tatsache:

2a. *Eine binäre Form $P(x, y)$, mit ganzen rationalen Koeffizienten, ist dann und nur dann durch das Quadrat einer Primfunktion (mod p) teilbar, wenn ihre Diskriminante durch p teilbar ist.*

Ein Satz, der selbst wieder Spezialfall des nachstehenden Satzes ist:

2b. *Zwei homogene ganzzahlige Polynome $f(x, y)$, $g(x, y)$ haben in der ihnen eigentümlichen Zerlegung (mod p) dann und nur dann wenigstens eine Primfunktion (mod p) als gemeinsamen Teiler, wenn ihre Resultante durch p teilbar ist.*

Speziell für unsere Polynome $C_p(x, y)$ folgt aus (2a), in Verbindung mit dem Ergebnis (1), daß die Existenz einer Lösung von $C_p(x, y) \equiv 0 \pmod{p}$ notwendig die Teilbarkeit der Diskriminante von $C_p(x, y)$ nach sich zieht. Daß aber auch *umgekehrt* die Teilbarkeit der Diskriminante durch p die Existenz von wenigstens einer Lösung der Kongruenz $C_p(x, y) \equiv 0 \pmod{p}$ anzeigt, ist erst dann gewiß, wenn es feststeht, daß in der kanonischen Zerlegung von $C_p(x, y) \pmod{p}$ *kein Quadrat* einer Primfunktion *von höherem als 1. Grade* in x, y vorkommt. Dies trifft für die $C_p(x, y)$ tatsächlich zu, und darauf beruht wesentlich unser Kriterium; denn jedesmal, wenn überhaupt $C_p(x, y)$ durch das Quadrat einer Primfunktion (mod p) teilbar ist, so muß ebendieselbe Primfunktion auch in

der Zerlegung von $\frac{\partial C}{\partial x}$, sowie in derjenigen von $\frac{\partial C}{\partial y}$ wenigstens einmal vorkommen, also, nach der Beweisführung von (1), auch in der Zerlegung von $\frac{1}{p} \cdot \frac{\partial A}{\partial x}$ und in derjenigen von $\frac{1}{p} \cdot \frac{\partial A}{\partial y}$. Von letzteren beiden Polynomen aber kennen wir bereits die vollständige Zerlegung; dieselbe liegt ja explizite vor (4. und 5. Zeile des Beweises vor (1)), und zwar besteht sie aus lauter *linearen* Primfunktionen. q. e. d. Somit haben wir folgende *1. Form des Existenzkriteriums* bewiesen:

3. *Notwendig und hinreichend für die Existenz wenigstens einer Lösung* x, y *für die Kongruenz* $(x+y)^p - x^p - y^p \equiv 0 \pmod{p^2}$, $p>7$, *welche gleichzeitig die Bedingung* $xy(x+y)(x^2+xy+y^2) \not\equiv 0 \pmod{p}$ *erfüllt, ist die Teilbarkeit der Diskriminante von* $C_p(x, y)$ *durch* p.

Für $p = 5$ und $p = 7$ gibt es überhaupt keine Lösung, ohne daß gleichzeitig $xy(x+y)(x^2+xy+y^2) \equiv 0 \pmod{p}$ ist; erst bei $p>7$ spielt die Diskriminante eine Rolle.

Alles weitere gründet sich auf eine besondere Darstellung der Cauchyschen Polynome, und zwar nicht als Summe von Potenzprodukten $x^r \cdot y^s$, sondern als „zusammengesetzte" Funktion, ausgedrückt durch eine algebraische Identität folgender Art: $C_p(x, y) = K_p(u, v)$, mit $u = u(x, y) = (x^2 + xy + y^2)^3$, $v = v(x, y) = x^2 y^2 (x+y)^2$.

$K_p(x, y)$ ist also eine binäre Form in u, v, welche ihrerseits binäre Formen vom 6. Grade in x, y sind. Da $C_p(x, y)$ vom Grade $(p-5)$ bzw. $(p-7)$, so wird $K_p(u, v)$ vom Grad $\frac{p-5}{6}$ bzw. $\frac{p-7}{6}$ in u, v, je nachdem $p \equiv 2 \pmod 3$ bzw. $p \equiv 1 \pmod 3$ ist.

Während die Polynome $C_p(x, y)$ bisher noch sehr unübersichtlich zu sein scheinen, erhalten sie nunmehr eine explizite Darstellung durch den folgenden Satz:

4. *Jedesmal, wenn* $p \equiv 1 \pmod 3$, *so ist:*

$$\frac{(x+y)^p - x^p - y^p}{pxy(x+y)(x^2+xy+y^2)^2} = \sum_{r=0}^{r=\frac{p-7}{6}} \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r+1} \cdot u^{\frac{p-7}{6}-r} \cdot v^r.$$

Jedesmal, wenn $p \equiv 2 \pmod 3$, *so ist:*

$$\frac{(x+y)^p - x^p - y^p}{pxy(x+y)(x^2+xy+y^2)^1} = \sum_{r=0}^{r=\frac{p-5}{6}} \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r+1} \cdot u^{\frac{p-5}{6}-r} \cdot v^r.$$

Beweis von (4). Zunächst beachte man, daß das Polynom $A_p(x, y) = (x + y)^p - x^p - y^p$ auch als p-te Potenzsumme der drei Größen $-x$, $-y$, $(x + y)$ angesehen werden kann, also auch als die p-te Potenzsumme der Wurzeln derjenigen algebraischen Gleichung 3. Grades, welche jene drei Größen zu Wurzeln hat, und deren Koeffizienten demnach lauten:

$$a_1 = 0\,; \quad a_2 = -(x^2 + xy + y^2)\,; \quad a_3 = -xy(x + y)\,.$$

Daher liefert *Warings* Formel für die Potenzsummen der Wurzeln, speziell für jene Gleichung 3. Grades, sofort den fertigen Ausdruck:

$$A_p(x, y) = p \cdot \sum_{(\lambda_2, \lambda_3)} \frac{(\lambda_2 + \lambda_3 - 1)!}{\lambda_2!\,\lambda_3!} \cdot (-a_2)^{\lambda_2} \cdot (-a_3)^{\lambda_3}\,.$$

Die Summation ist zu erstrecken über alle natürlichen Zahlen λ_2, λ_3, welche der Bedingung $2\lambda_2 + 3\lambda_3 = p$ genügen. Diese Formel für $A_p(x, y)$ findet sich schon bei *Th. Muir* (Quarterl. Journal XI, 1879), jedoch keineswegs die weitgehenden Folgerungen, die sich aus ihr für die von uns so bezeichneten Cauchyschen Polynome ergeben, auf welche sich das Interesse der vorliegenden Abhandlung konzentriert.

Zunächst führen wir das rechnerisch zugängliche Symbol $\binom{a}{b}$ ein und erhalten

$$\frac{(\lambda_2 + \lambda_3 - 1)!}{\lambda_2!\,\lambda_3!} = \binom{\lambda_2 + \lambda_3 - 1}{\lambda_3 - 1} \frac{1}{\lambda_3}$$

und wollen diesen, immer noch unübersichtlichen, allgemeinen Koeffizienten so umformen, daß er explizite als Funktion von p erkennbar wird. Alles dazu Nötige entnehmen wir der Bedingung $2\lambda_2 + 3\lambda_3 = p$. Aus ihr folgt zunächst, daß mit ungeradem p auch stets λ_3 ungerade, also $\lambda_3 = 1 + 2r$ sein muß; ferner entnehmen wir aus ihr, daß stets $2\lambda_2 \equiv p \pmod 3$ ist. Demnach sind *zwei Fälle* zu unterscheiden:

1. Fall: $p = 1\,(3)$: $\lambda_2 = 2 + 3q$,

$$\text{daher } 2\lambda_2 + 3\lambda_3 = 7 + 6(q + r) = p\,; \quad q + r = \frac{p - 7}{6}\,;$$

$$\frac{1}{\lambda_3} \cdot \binom{\lambda_2 + \lambda_3 - 1}{\lambda_3 - 1} = \binom{2 + 3q + 2r}{2r} \frac{1}{2r + 1} =$$

$$= \binom{2 + \frac{p-7}{2} - r}{2r} \frac{1}{2r + 1} = \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r + 1}\,.$$

2. Fall: $p = 2\,(3)$: $\underline{\lambda_2 = 1 + 3q}$;

$$2\lambda_2 + 3\lambda_3 = 5 + 6(q + r) = p \; ; \quad q + r = \frac{p-5}{6} \; ;$$

$$\frac{1}{\lambda_3} \cdot \binom{\lambda_2 + \lambda_3 - 1}{\lambda_3 - 1} = \binom{1 + 3q + 2r}{2r} \frac{1}{2r+1} =$$

$$= \binom{1 + \frac{p-5}{2} - r}{2r} \frac{1}{2r+1} = \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r+1} \; .$$

Wir haben also das befriedigende Ergebnis, daß für *beide* Primzahlarten, d. h. für alle $p > 3$, der allgemeine Koeffizient jener Polynomentwicklung durch ein und dieselbe Formel als Funktion von p ausgedrückt werden kann.

Aus der so erhaltenen Entwicklung für $A_p(x, y)$:

$$p = 1\,(3): \quad (x + y^p) - x^p - y^p =$$

$$= p \cdot \sum_{r+q = \frac{p-7}{6}} \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r+1} \cdot (x^2 + xy + y^2)^{2+3q} \cdot \big(xy \cdot (x+y)\big)^{1+2r}$$

$$p = 2\,(3): \quad (x + y)^p - x^p - y^p =$$

$$= p \cdot \sum_{r+q = \frac{p-5}{6}} \binom{\frac{p-3}{2} - r}{2r} \frac{1}{2r+1} \cdot (x^2 + xy + y^2)^{1+3q} \cdot \big(xy(x+y)\big)^{1+2r},$$

erkennt man, daß in jedem Fall ein gemeinsamer Faktor aller Summenglieder sich abspalten läßt, nämlich im ersten Fall: $(x^2+xy+y^2)^2xy(x+y)$; im zweiten Fall: $(x^2 + xy + y^2)^1xy(x + y)$. Geschieht dies, so ergibt sich, mit Rücksicht auf die Definition der $C_p(x, y)$ als Quotienten, genau jene in Satz 4 behauptete Entwicklung für die Cauchyschen Polynome.

Ausgehend von der nunmehr bewiesenen algebraischen Identität $C_p(x, y) = K_p(u, v)$ werden wir in wenigen Schritten zum vollständigen Beweis unseres Kriteriums gelangen. Aus $m \cdot K = uK'_u + v \cdot K'_v$ einerseits, wo m den Grad von K in u, v bedeutet, und andererseits aus

$$C'_x = K'_u u'_x + K'_v v'_x \; ; \qquad C'_y = K'_u u'_y + K'_v v'_y \; ,$$

erkennt man, daß die beiden simultanen Kongruenzen $C'_x(x, y) \equiv 0 \pmod p$ und $C'_y(x, y) \equiv 0 \pmod p$, *wenn überhaupt*, so nur für solche Wertepaare x, y befriedigt werden können, für welche

entweder: $K'_u(u, v) \equiv 0 \pmod p$ und zugleich $K'_v(u, v) \equiv 0 \pmod p$

oder: welche sowohl $K'_u(u,v) \not\equiv 0 \pmod p$ als auch $K'_v(u,v) \not\equiv 0 \pmod p$, aber gleichzeitig

$$D(x, y) = \begin{vmatrix} u'_x , & v'_x \\ u'_x , & v'_x \end{vmatrix} \equiv 0 \pmod p$$

befriedigen.

$$u'_x = 3(x^2 + x\,y + y^2)^2 \cdot (2x + y) \; ; \qquad v'_x = 2x\,y^2 \cdot (x + y)\;(2x + y) \; ;$$

$$u'_y = 3(x^2 + x\,y + y^2)^2 \cdot (2y + x) \; ; \qquad v'_y = 2y\,x^2 \cdot (x + y) \cdot (2y + x) \; .$$

Daher $D(x, y) = 6 \cdot (x^2 + x\,y + y^2)^2 \cdot (2x + y) \cdot (2y + x) \cdot (y - x)$.

Hiermit ist schon folgender Satz bewiesen (in Verbindung mit (3)):

5. *Die Kongruenz* $(x + y)^p - x^p - y^p = 0 \pmod{p^2}$ $p > 7$ *ist höchstens für solche Wertepaare* x, y *erfüllbar, für die entweder (gemäß 2b) die Resultante der beiden abgeleiteten Polynome* $K'_u(u, v)$, $K'_v(u, v)$, *als Polynome in* x, y *betrachtet, durch* p *teilbar, oder für die*

$$6xy(x + y)(2x + y)(2y + x)(y - x)(x^2 + x\,y + y^2) \equiv 0 \pmod p$$

erfüllt ist.

Zwischen der Resultante von $K'_u(u, v)$ und $K'_v(u, v)$, als Funktionen von u, v betrachtet, und der Resultante ebenderselben Polynome, jedoch als Funktionen von x, y betrachtet, besteht eine genaue Abhängigkeit, nämlich die Relation (7). Zu deren Beweis dient ein *Hilfssatz*, den ich gleich in einer etwas allgemeinerer Form aufstellen will, als er unmittelbar gebraucht wird, weil der Beweis dadurch nicht schwieriger, sondern durchsichtiger wird.

$F(x, y)$ und $G(x, y)$ seien zwei beliebige binäre Formen in x, y, mit der speziellen Eigenschaft, daß sie sich gleichzeitig als binäre Formen von $u_k(x, y)$ und $v_k(x, y)$ darstellen lassen, wo u und v selbst binäre Formen k-ten Grades in x, y sind: $F = P\big(u(x, y), v(x, y)\big)$; $G = Q\big(u(x. y), v(x, y)\big)$; F vom Grade $m \cdot k$, G vom Grade $n \cdot k$ in x, y. Ich *behaupte*, daß zwischen den drei Resultanten $\begin{pmatrix} x, y \\ F, G \end{pmatrix}$,

$\begin{pmatrix} x, y \\ u, v \end{pmatrix}$ und $\begin{pmatrix} u, v \\ P, Q \end{pmatrix}$ nachstehende algebraische Beziehung besteht:

$$\begin{pmatrix} x, y \\ F, G \end{pmatrix} = \begin{pmatrix} u, v \\ P, Q \end{pmatrix}^k \cdot \begin{pmatrix} x, y \\ u, v \end{pmatrix}^{m \cdot n} . \tag{6}$$

Der nachfolgende Beweis benützt nur allgemeine Eigenschaften der Resultanten, welche, bei Gebrauch des Symbols (f, g) für die Resultante von zwei in x, y homogenen Polynomen f, g, kurz so sich ausdrücken lassen:

(a) Falls $f = g \cdot h$ ist, so ist $(f, k) = (g, k) \cdot (h, k)$ insbesondere ist $(c \cdot f, g) = c^n \cdot (f, g)$, falls c von x, y unabhängig ist und n den Grad von g in x, y bedeutet.

(b) Falls der Grad m von f mindestens so groß als derjenige von g, und falls λ eine beliebig gewählte binäre Form des Grades $(m - n)$ ist, so gilt:

$$(f, g) = (f - \lambda g, g) .$$

Als binäre Formen in u, v besitzen P und Q je eine Zerlegung in lauter Linearfaktoren:

$$P = \prod_{r=1}^{r=m} (u - \gamma_r v) \; ; \qquad Q = \prod_{s=1}^{s=n} (u - \delta_s v) .$$

Die Behauptung (6) läßt sich nun durch folgende Rechnung mit Resultantensymbolen verifizieren. Einerseits ist

$$\begin{pmatrix} u, v \\ P, Q \end{pmatrix} = \prod_{r,s} \begin{pmatrix} u, v \\ u - \gamma_r v, u - \delta_s v \end{pmatrix} = \prod_{r,s} \begin{pmatrix} u, v \\ u - \gamma_r v, v \cdot (\gamma_r - \delta_s) \end{pmatrix} =$$

$$= \prod_{r,s} (\gamma_r - \delta_s) \cdot \prod_{r,s} \begin{pmatrix} u, v \\ u, v \end{pmatrix} = \prod_{r,s} (\gamma_r - \delta_s) .$$

Andererseits:

$$\begin{pmatrix} x, y \\ F, G \end{pmatrix} = \begin{pmatrix} x, y \\ P, Q \end{pmatrix} = \prod_{r,s} \begin{pmatrix} x, y \\ u - \gamma_r v, u - \delta_s v \end{pmatrix}$$

$$= \prod_{r,s} \begin{pmatrix} x, y \\ u - \gamma_r v, v \cdot (\gamma_r - \delta_s) \end{pmatrix} = \left(\prod_{r,s} (\gamma_r - \delta_s) \right)^k \cdot \prod_{r,s} \begin{pmatrix} x, y \\ u, v \end{pmatrix}$$

$$= \begin{pmatrix} u, v \\ P, Q \end{pmatrix}^k \cdot \begin{pmatrix} x, y \\ u, v \end{pmatrix}^{m \cdot n} . \qquad \text{q. e. } d.$$

Die Anwendung von (6) auf unsere Polynome $K'_u(u, v) = P(u, v) = F(x, y)$ und $K'_v(u, v) = Q(u, v) = G(x, y)$ ergibt sofort:

$$\begin{pmatrix} x, y \\ K'_u, K'_v \end{pmatrix} = \begin{pmatrix} u, v \\ K'_u, K'_v \end{pmatrix}^6 , \tag{7}$$

da $\begin{pmatrix} x, y \\ u, v \end{pmatrix} = 1$ ist, bei $u = (x^2 + xy + y^2)^3$ und $v = x^2 \cdot y^2 \cdot (x+y)^2$.
Die Verbindung der Ergebnisse (5) und (7) mit $x + y + z \equiv 0 \pmod p$ liefert nunmehr einen in x, y, z symmetrischen Satz:

8. *Notwendig und hinreichend dafür, daß die Kongruenz* $x^p + y^p + z^p \equiv 0 \pmod{p^2}$ *eine Lösung* x, y, z *besitzt, die der Bedingung*

$$x\,y\,z\,(x - y)\,(y - z)\,(z - x)\,(x^2 + y^2 + z^2) \not\equiv 0 \pmod{p^1}$$

genügt, $p > 7$, *ist die Teilbarkeit der Resultante von* $\frac{\partial K}{\partial u}$, $\frac{\partial K}{\partial v}$, *letztere als Polynome in* u, v *betrachtet, durch* p.

Dieser Satz (8) ist aber bereits inhaltlich identisch mit unserem zu Anfang formulierten Kriterium, abgesehen von dem noch fehlenden allgemeinen Nachweis, daß obige Resultate, d. h. die Diskriminante von $K(u, v)$, niemals identisch verschwindet. Darüber weiter unten!

Die *praktische* Prüfung der Diskriminante $\Delta(p)$ auf ihre Teilbarkeit durch p ist identisch mit der Untersuchung, ob die beiden abgeleiteten Polynome $\frac{\partial K}{\partial u}$, $\frac{\partial K}{\partial v}$, als Polynome in u, v betrachtet, einen größten gemeinsamen Teiler $T(u, v) \pmod p$ besitzen, der wirklich von u, v abhängig ist, d. h. sich nicht auf eine Konstante reduziert. Liegt dieser Fall vor, so zerfällt $T(u, v)$ *a priori* in lauter in u, v lineare Faktoren (mod p), und jeder der letzteren, wiederum (mod p), in je sechs lineare Faktoren in x, y. Hierbei spielt die *Invarianz* des Quotienten

$$\varphi(\delta) = \frac{(\delta^2 + \delta^1 + 1)^3}{\delta^2 \cdot (\delta + 1)^2}$$

gegenüber den Transformationen der harmonischen Gruppe:

$$\delta,\ \frac{1}{\delta},\ -1-\delta,\ -\frac{1}{1+\delta},\ \frac{-\delta}{\delta+1},\ -\frac{\delta+1}{\delta}$$

eine wesentliche Rolle. Auf Grund jener Invarianz wird

$$u - \varphi(\delta)\cdot v = (x-\delta y)\left(x-\frac{1}{\delta}y\right)(x+(\delta+1)y)$$
$$\left(x+\frac{1}{\delta+1}\cdot y\right)\left(x+\frac{\delta}{\delta+1}\cdot y\right)\left(x+\frac{\delta+1}{\delta}\cdot y\right)$$

eine algebraische Identität in x, y und δ.

Wie bereits mitgeteilt, finden sich unter den Primzahlen $p<100$ *nur drei*, für welche die Diskriminante des zugeordneten Polynoms $K_p(u,v)$ durch p teilbar ist, nämlich 59, 79, 83. Bei $p=59$ ergibt sich $T(u,v)$ als Polynom zweiten Grades in u, v, bei $p=79$ und $p=83$ berechnet sich $T(u,v)$ je als ein Ausdruck ersten Grades in u, v.

Zu $p=79$. $T(u,v)\equiv u+5v \pmod{79}$; die sechs einzigen Lösungen von $(t+1)^{79}-t^{79}-1^{79}\equiv 0 \pmod{79^2}$ mit $t(t+1)(t^2+t^1+1)\not\equiv 0(79)$ sind identisch mit denjenigen der Kongruenz sechsten Grades $-5\equiv\varphi(\delta)$ (mod 79), also mit $t=\delta=(11,36;-12,-33;32,-37)$. In der Tat ist $12^{79}-11^{79}-1^{79}\equiv 0\,(79^2)$; $33^{79}-32^{79}-1^{79}\equiv 0\,(79^2)$; $37^{79}-36^{79}-1^{79}\equiv 0\,(79^2)$.

Zu $p=83$. $T(u,v)\equiv u-13v \pmod{83}$. Der zugehörige einzige Sechserverband von Lösungen mit $t(t+1)\not\equiv 0(83)$ besteht aus $(8,-31;-9,-37;36,30)$. In der Tat ist: $9^{83}-8^{83}-1^{83}\equiv 0\,(83^2)$; $31^{83}-30^{83}-1^{83}\equiv 0\,(83^2)$; $37^{83}-36^{83}-1^{83}\equiv 0\,(83^2)$.

Zu $p=59$. $T(u,v)\equiv(u-4v)(u+18v) \pmod{59}$; es gibt also *zwei Sechserverbände* von Lösungen für $(t+1)^{59}-t^{59}-1^{59}\equiv 0\,(59^2)$ mit $t(t+1\not\equiv 0(59)$, nämlich $(3,20;-4,-15;+14,-21)$ und $(4,15;-5,-12;11,-10)$. In der Tat ist z. B.

$$4^{59}-3^{59}-1^{59}\equiv 0 \pmod{59^2} \quad \text{und} \quad 5^{59}-4^{59}-1^{59}\equiv 0\,(59^2).$$

Aus vorstehender Untersuchung der Primzahlen $p<100$ folgt implizite, daß wenigstens für sie niemals $\Delta(p)$ identisch Null wird. Daß dies auch *stets* der Fall ist, für alle Primzahlen p, läßt sich in wenigen Schritten beweisen, z. B. in folgender Weise:

$$\frac{1}{p}\cdot\frac{\partial A}{\partial x}=(x+y)^{p-1}-x^{p-1}=\prod_{k=1}^{k=p-1}(x+y-x\cdot\varepsilon^k);$$
$$\frac{1}{p}\cdot\frac{\partial A}{\partial y}=(x+y)^{p-1}-y^{p-1}=\prod_{l=1}^{l=p-1}(x+y-y\cdot\varepsilon^l),$$

falls ε eine primitive Wurzel von $z^{p-1}=1$ bedeutet.

Das Vorhandensein eines *gemeinsamen* algebraischen Teilers beider Produkte würde verlangen, daß für wenigstens *ein* k und für wenigstens *ein* l:

$$x(1-\varepsilon^k)+y=\lambda\cdot\left(x+y(1-\varepsilon^l)\right),$$

d. h. daß

$$\lambda=1-\varepsilon^k \quad \text{und} \quad 1=(1-\varepsilon^k)\,(1-\varepsilon^l)$$

ist. Weder ε^k noch ε^l kann reell, d. h. hier: $\pm l$, sein; sie müssen also konjugiert komplex, also $k+1=p-1$ sein. Dann folgt nacheinander:

$$1=(1-\varepsilon^k)\cdot(1-\varepsilon^{-k})\;;\quad \varepsilon^k+\varepsilon^{-k}=1\;;\quad \cos\frac{2k\pi}{p-1}=\tfrac{1}{2}$$

für $1\leqq k<p$, mit den beiden einzigen Lösungen $k=\dfrac{p-1}{6}$ und $k=5\cdot\dfrac{p-1}{6}$. Da überdies k eine *ganze* Zahl sein muß, so folgt notwendig $p\equiv 1 \pmod 6$, falls überhaupt ein gemeinsamer algebraischer Teiler existiert. Für jene beiden Werte von k ist aber $\varepsilon^k=$ primitive Wurzel von $z^6=1$, und daher $-\varepsilon^k$ primitive Wurzel von $z^3=1$, also $-\varepsilon^k=\alpha$ mit $\alpha^2+\alpha+1=0$. Die beiden einzigen, möglicherweise gemeinsamen Linearfaktoren sind also diese $x+y+x\cdot\alpha$ und $x+y+x\cdot\alpha^{-1}$, deren Produkt x^2+xy+y^2, während gleichzeitig $p\equiv 1(6)$ ist. Daß dieser Fall tatsächlich eintritt, und zwar stets im Fall $p\equiv 1(6)$, ist ja bekannt aber auch leicht direkt zu bestätigen. q. e. d.

(Eingegangen den 1. Juni 1948.)