Allgemeiner Beweis des Fermatschen Satzes, daß die Gleichung x... durch ganze Zahlen unlösbar ist, f...

Kummer, E.E.

in: Journal für die reine und angewandte Mathematik | Journal für die reine und angewandte Mathemati...
9 Seite(n) (138 - 146)

Email: info@digizeitschriften.de

8.

Allgemeiner Beweis des Fermatschen Satzes, dafs die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Factoren nicht vorkommen.

(Von Herrn *E. E. Kummer,* Professor in Breslau.)

In den vorhergehenden Abhandlungen haben wir die Theorie der complexen Zahlen bis zu dem Puncte geführt, dafs mit Hülfe derselben der Beweis dieses Fermatschen Satzes, wenn gleich noch nicht vollkommen allgemein, so doch für alle diejenigen Potenzen, deren Exponenten die in der Überschrift bezeichnete Bedingung erfüllen, leicht und sicher geführt werden kann. Da es hierbei wenig Unterschied macht, ob man x, y, z nur als reale ganze Zahlen, oder, allgemeiner, als complexe, aus λten Wurzeln der Einheit gebildete Zahlen annimmt, so wollen wir den Beweis sogleich für complexe Zahlen geben. Die zu untersuchende Gleichung sei demnach

$$1. \qquad u^\lambda + v^\lambda + w^\lambda = 0;$$

wo u, v und w wirkliche complexe Zahlen bezeichnen. Ferner sei λ eine Primzahl, welche in keiner der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Factor des Zählers vorkommt. Unter dieser Voraussetzung haben die hier vorkommenden complexen Zahlen nach den in der vorhergehenden Abhandlung bewiesenen Sätzen, erstens, die Eigenschaft, dafs die Anzahl aller nichtäquivalenten Classen nicht durch λ theilbar ist; woraus wir sogleich die für den folgenden Beweis bemerkenswerthe Folgerung ziehen, dafs hier niemals eine λte Potenz einer *idealen* complexen Zahl zu einer wirklichen werden kann, oder dafs, wenn eine λte Potenz einer complexen Zahl gleich einer *wirklichen* ist, diese complexe Zahl selbst eine wirkliche sein mufs (Man sehe die Abhandlung No. 16. Band 35. S. 356 dieses Journals). Zweitens ist bei dieser Voraussetzung, nach dem letzten Satze der vorhergehenden Abhandlung, jede complexe Einheit, welche für den Modul λ einer realen ganzen Zahl con-

gruent wird, stets eine λte Potenz einer andern Einheit. Dafs die complexen Zahlen u, v und w so angenommen werden, dafs sie nicht alle drei einen gemeinschaftlichen Factor haben und dafs darum auch nicht zwei derselben einen gemeinschaftlichen Factor haben dürfen, versteht sich von selbst.

Der Beweis der Unmöglichkeit der Gleichung (1.) zerfällt nun in zwei Theile, deren erster den Fall betrifft, wo von den drei complexen Zahlen u, v und w keine den Factor $1-\alpha$ hat, der zweite aber den Fall, wo eine derselben durch $1-\alpha$ theilbar ist.

Es sei erstens in der Gleichung

$$u^\lambda + v^\lambda + w^\lambda = 0$$

keine der complexen Zahlen u, v, w durch $1-\alpha$ theilbar. Da in der gegebenen Gleichung nur die λten Potenzen von u, v, w vorkommen, so kann man diese complexen Zahlen mit beliebigen λten Wurzeln der Einheit multipliciren; man kann also $\alpha^h u$ statt u setzen, wo h eine beliebige ganze Zahl ist, welche sich, wie leicht zu zeigen, immer so bestimmen läfst, dafs $\alpha^h u$ die Form $a+(1-\alpha)^2 P$ erhält; wo a eine reale ganze Zahl und P eine complexe ganze Zahl ist. Dieselbe Form kann auch dem v und w gegeben werden. Es sollen deshalb hier überall für u, v und w folgende Formen angenommen werden:

$$2. \quad \begin{cases} u = a+(1-\alpha)^2 P \\ v = b+(1-\alpha)^2 Q \\ w = c+(1-\alpha)^2 R. \end{cases}$$

Die realen ganzen Zahlen a, b, c sind wegen der Voraussetzung, dafs u, v, w nicht durch $1-\alpha$ theilbar sein sollen, nicht durch λ theilbar. Ich zerlege nun die Form $u^\lambda + v^\lambda$ in ihre Factoren und erhalte so aus der Gleichung $u^\lambda + v^\lambda + w^\lambda = 0$ folgende:

$$3. \quad (u+v)(u+\alpha v)(u+\alpha^2 v) \ldots (u+\alpha^{\lambda-1} v) = -w^\lambda.$$

Diese λ Factoren haben keinen gemeinschaftlichen Theiler: denn hätten $u+\alpha^r v$ und $u+\alpha^s v$ einen solchen, so müfsten auch $(\alpha^r-\alpha^s)u$ und $(\alpha^r-\alpha^s)v$ denselben Theiler haben, und da u und v relative Primzahlen sind, so könnte nur $\alpha^r-\alpha^s$ der gemeinschaftliche Theiler sein. Es ist aber $\alpha^r-\alpha^s$ gleich $1-\alpha$, multiplicirt mit einer complexen Einheit, und dieses kann nicht Theiler eines jener λ Factoren sein, weil sonst, gegen die Annahme, auch w^λ und folglich auch w durch $1-\alpha$ theilbar sein müfste. Da nun alle diese Factoren auf der Seite links der Gleichung (3.) relative Primzahlen sind und ihr

Product gleich einer λten Potenz ist, so müssen sie alle einzeln gleich λten Potenzen gewisser idealen complexen Zahlen sein, multiplicirt mit irgend welchen complexen Einheiten. Es folgt dies unmittelbar, eben so wie für gewöhnliche ganze Zahlen, aus dem in der Abhandlung No. 16. Band. 35. pag. 348 bewiesenen Satze, dafs, abgesehen von den Einheiten, welche als Factoren zutreten können, jede complexe Zahl sich nur auf eine einzige bestimmte Weise als Product ihrer idealen Primfactoren darstellen läfst. Man erhält daher allgemein für alle Werthe $r = 0, 1, 2, \ldots \lambda - 1$:

$$4. \quad u + \alpha^r v = \alpha^\varrho \boldsymbol{E}_r(\alpha) . t_r^\lambda;$$

wo t_r eine complexe Zahl ist, Factor von w, und $\alpha^\varrho \boldsymbol{E}_r(\alpha)$ eine Einheit, von der Art, dafs $\boldsymbol{E}_r(\alpha) = \boldsymbol{E}_r(\alpha^{-1})$ ist. In zwei Factoren, α^ϱ und $\boldsymbol{E}_r(\alpha)$, deren einer nur eine λte Wurzel der Einheit ist, der andere die Eigenschaft hat, bei der Verwandlung des α in α^{-1} ungeändert zu bleiben, läfst sich nämlich, wie bekannt, jede beliebige complexe Einheit zerlegen. Da nach Gleichung (4.) t_r^λ gleich einer wirklichen complexen Zahl ist, so schliefsen wir sogleich, nach Dem, was oben gezeigt, dafs auch t_r selbst eine wirkliche complexe Zahl sein mufs; und da jede λte Potenz einer wirklichen complexen Zahl bekanntlich einer realen ganzen Zahl congruent ist, für den Modul λ, so setze ich $t_r^\lambda \equiv m$, mod. λ; wo m eine reale ganze Zahl ist. Die Gleichung (4.) geht dadurch in die Congruenz

$$5. \quad u + \alpha^r v \equiv \alpha^\varrho . \boldsymbol{E}_r(\alpha) m, \text{ mod. } \lambda,$$

über. Wird nun α in α^{-1} verwandelt, wodurch u in u', v in v', w in w' übergehen mag, so ist

$$6. \quad u' + \alpha^{-r} v' \equiv \alpha^{-\varrho} \boldsymbol{E}_r(\alpha) m, \text{ mod. } \lambda;$$

aus welchen beiden Congruenzen durch Elimination des m

$$7. \quad \alpha^{-\varrho}(u + \alpha^r v) \equiv \alpha^\varrho (u' + \alpha^{-r} v'), \text{ mod. } \lambda,$$

folgt. Nimmt man statt des Moduls λ den Modul $(1-\alpha)^2$, welcher ein Divisor von λ ist, und bemerkt, dafs nach den Gleichungen (2.) $u \equiv a$, $v \equiv b$, $u' \equiv a$, $v' \equiv b$, für den Modul $(1-\alpha)^2$ ist, so erhält man

$$8. \quad \alpha^{-\varrho}(a + \alpha^r b) \equiv \alpha^\varrho (a + \alpha^{-r} b), \text{ mod. } (1-\alpha)^2,$$

und da allgemein $\alpha^h \equiv 1 - h(1-\alpha)$, mod. $(1-\alpha)^2$, ist, so geht diese Congruenz in die folgende über:

$$2(a+b)\varrho \equiv 2br, \text{ mod. } (1-\alpha).$$

Da nun reale ganze Zahlen, welche durch $1-\alpha$ theilbar sind, auch durch λ

theilbar sein müssen, so ist

$$9. \quad (a+b)\varrho \equiv br, \text{ mod. } \lambda.$$

Nennt man nun k diejenige ganze Zahl, welche der Congruenz

$$10. \quad (a+b)k \equiv b, \text{ mod. } \lambda,$$

genügt, so ist k von r unabhängig und $\varrho \equiv k.r$, also giebt die Congruenz (7.)

$$11. \quad \alpha^{-kr}(u+\alpha^r v) \equiv \alpha^{+kr}(u'+\alpha^{-r}v'), \text{ mod. } \lambda.$$

Für den besondern Fall $r=0$ hat man, da $a+b$ nicht $\equiv 0$, mod. λ, sein kann, aus der Congruenz (9.): $\varrho \equiv 0$, mod. λ, also

$$12. \quad u+v \equiv u'+v', \text{ mod. } \lambda,$$

und da u, v, w in der gegebenen Gleichung $u^\lambda+v^\lambda+w^\lambda=0$ beliebig vertauscht werden können, so ist auch

$$13. \quad \left\{\begin{matrix} u+w \equiv u'+w' \\ v+w \equiv v'+w' \end{matrix}\right\} \text{ mod. } \lambda,$$

und aus diesen Congruenzen folgen die drei einfacheren:

$$14. \quad \left\{\begin{matrix} u \equiv u' \\ v \equiv v' \\ w \equiv w' \end{matrix}\right\} \text{ mod. } \lambda.$$

Hiernach verwandelt sich die für jeden beliebigen Werth von r geltende Congruenz (11.) in folgende:

$$15. \quad \alpha^{-kr}(u+\alpha^r v) \equiv \alpha^{kr}(u+\alpha^{-r}v), \text{ mod. } \lambda,$$

oder in

$$u(\alpha^{kr}-\alpha^{-kr})+v(\alpha^{(k-1)r}-\alpha^{-(k-1)r}) \equiv 0, \text{ mod. } \lambda.$$

Ich setze $r=1$ und $r=2$, und erhalte dadurch:

$$16. \quad \left\{\begin{matrix} u(\alpha^k-\alpha^{-k})+v(\alpha^{(k-1)}-\alpha^{-(k-1)}) \equiv 0, \\ u(\alpha^{2k}-\alpha^{-2k})+v(\alpha^{2(k-1)}-\alpha^{-2(k-1)}) \equiv 0, \end{matrix}\right\} \text{ mod. } \lambda,$$

und wenn die erste dieser beiden Congruenzen mit $\alpha^k+\alpha^{-k}$ multiplicirt und die zweite davon abgezogen wird, so ist nach Weghebung des gemeinschaftlichen Factors v, welcher nicht durch $1-\alpha$ theilbar, also zu λ relative Primzahl ist,

$$(\alpha^k+\alpha^{-k})(\alpha^{(k-1)}-\alpha^{-(k-1)})+(\alpha^{2(k-1)}-\alpha^{-2(k-1)}) \equiv 0, \text{ mod. } \lambda,$$

also

$$(\alpha^{k-1}-\alpha^{-(k-1)})(\alpha^k+\alpha^{-k}-\alpha^{k-1}-\alpha^{-(k-1)}) \equiv 0, \text{ mod. } \lambda,$$

folglich

$$17. \quad (\alpha^{k-1}-\alpha^{-(k-1)})(\alpha^{-k}-\alpha^{k-1})(1-\alpha) \equiv 0, \text{ mod. } \lambda.$$

Wenn nun keiner dieser drei Factoren für sich gleich Null ist, so enthält das Product derselben den Factor $1-\alpha$ dreimal: es müfste denselben aber ebensovielmal enthalten als λ, also $\lambda-1$ mal, damit die Congruenz wirklich Statt habe. Mit Ausschlufs des einzigen Falles $\lambda=3$ kann also diese Congruenz (17.) nicht Statt finden, wenn nicht

$$18. \quad \begin{cases} \text{entweder} & \alpha^{k-1}-\alpha^{-(k-1)}=0, \\ \text{oder} & \alpha^{-k}-\alpha^{k-1}=0 \end{cases}$$

ist. Es mufs also entweder $k\equiv 1$, oder $2k\equiv 1$, mod. λ, sein. Der erste Fall $k\equiv 1$ würde aber der Congruenz (10.) zufolge $a\equiv 0$, mod. λ, geben, und kann deshalb nicht Statt haben. Der zweite Fall $2k\equiv 1$ giebt, der Congruenz (10.) zufolge $a\equiv b$, mod. λ, woraus durch blofse Vertauschung der Buchstaben folgt, dafs auch $a\equiv c$ und $b\equiv c$, mod. λ, sein mufs. Aus der Gleichung $u^\lambda+v^\lambda+w^\lambda=0$ folgt aber, nach den bei (2.) angenommenen Ausdrücken von u, v und w, dafs auch $a^\lambda+b^\lambda+c^\lambda\equiv 0$, mod. λ, sein mufs, also auch $a+b+c\equiv 0$, mod. λ, und da a, b und c congruent sind, endlich $3a\equiv 0$, mod. λ, welches, mit Ausnahme des schon oben ausgeschlossenen Falles $\lambda=3$, ebenfalls unmöglich ist, weil nach der Voraussetzung u den Factor $1-\alpha$ nicht enthalten und also auch a nicht durch λ theilbar sein darf. Hiermit ist nun der erste Theil des Beweises vollständig gegeben, indem gezeigt worden ist, dafs die Gleichung $u^\lambda+v^\lambda+w^\lambda=0$, wenn keine der complexen Zahlen u, v und w den Factor $1-\alpha$ enthält, immer eine unmögliche Congruenz für den Modul λ nach sich zieht; mit Ausnahme des Falles $\lambda=3$, welchen wir hier nicht besonders betrachten wollen.

Es sei zweitens in der Gleichung $u^\lambda+v^\lambda+w^\lambda=0$ eine der drei Zahlen u, v, w durch $1-\alpha$ theilbar; zu welcher w genommen werden soll. Dieselbe kann den Factor $1-\alpha$ auch mehrmals enthalten. Setzt man daher $(1-\alpha)^m w$ statt w, so dafs nun w den Factor $1-\alpha$ nicht weiter enthält, so ist die zu untersuchende Gleichung:

$$u^\lambda+v^\lambda+(1-\alpha)^{m\lambda}.w^\lambda=0.$$

Statt dieser aber setze ich die etwas allgemeinere

$$19. \quad u^\lambda+v^\lambda=E(\alpha)(1-\alpha)^{m\lambda}.w^\lambda,$$

in welcher $E(\alpha)$ eine beliebige complexe Einheit bezeichnet. Durch Zerlegung des Ausdrucks $u^\lambda+v^\lambda$ in Factoren erhält man

$$20. \quad (u+v)(u+\alpha v)(u+\alpha^2 v)\ldots.(u+\alpha^{\lambda-1}v)=E(\alpha)(1-\alpha)^{m\lambda}.w^\lambda.$$

Die λ Factoren $u+v$, $u+\alpha v$, u. s. w. haben hier alle den gemeinschaftlichen gröfsten Factor $1-\alpha$; aufser diesem haben je zwei derselben keinen gemeinschaftlichen Theiler. Nimmt man nämlich für u und v wieder, wie oben, die Formen $u=a+(1-\alpha)^2\boldsymbol{P}$ und $v=b+(1-\alpha)^2\boldsymbol{Q}$ an, so erhält man

$$21.\quad u+\alpha^r v = a+b-rb(1-\alpha),\ \text{mod.}\,(1-\alpha)^2;$$

es mufs aber $u+\alpha^r v$ wenigstens für einen Werth von r durch $1-\alpha$ theilbar sein, weil das Product aller dieser Factoren durch $(1-\alpha)^{m\lambda}$ theilbar ist: also mufs $a+b$ durch $1-\alpha$, folglich auch durch λ theilbar sein, und die Congruenz (21.) verwandelt sich in

$$22.\quad u+\alpha^r v \equiv rb(1-\alpha),\ \text{mod.}\,(1-\alpha)^2;$$

woraus zunächst folgt, dafs für jeden Werth von r, $u+\alpha^r v$ den Factor $1-\alpha$ enthalten mufs, statt dessen auch der Factor $1-\alpha^r$ genommen werden kann, welcher sich von diesem nur durch eine complexe Einheit unterscheidet, die als Factor hinzutritt: ferner, dafs $u+\alpha^r v$ diesen Factor $1-\alpha^r$ oder $1-\alpha$ nur einmal enthalten kann, mit Ausnahme des Falles $r=0$. Die Gröfse $u+v$ aber enthält wirklich den Factor $1-\alpha$ mehrmals, und zwar vermöge der Gleichung (20.) genau $m\lambda-\lambda+1$ mal, indem die übrigen $\lambda-1$ Factoren ihn jeder einmal enthalten und das Product aller $m\lambda$ mal. Setzt man nun

$$23.\quad u+v = (1-\alpha)^{m\lambda-\lambda+1}.\varphi$$

und

$$24.\quad u+\alpha^r v = (1-\alpha^r)\varphi_r,$$

so geht die Gleichung (20.) in folgende über:

$$25.\quad \varphi.\varphi_1.\varphi_2\ldots\varphi_{\lambda-1} = E(\alpha)w^\lambda$$

und es müssen nun die Factoren φ, φ_1, φ_2, $\ldots$ $\varphi_{\lambda-1}$, welche unter sich alle relative Primzahlen sind und deren Product gleich einer mit einer Einheit multiplicirten λten Potenz ist, alle einzeln ebenfalls solche mit Einheiten multiplicirte λte Potenzen sein. Demnach kann man setzen:

$$\varphi = e(\alpha)w_1^\lambda \text{ und } \varphi_r = e_r(\alpha)t_r^\lambda,$$

woraus

$$26.\quad u+v = e(\alpha)(1-\alpha)^{m\lambda-\lambda+1}.w_1^\lambda$$

und

$$27.\quad u+\alpha^r v = e_r(\alpha)(1-\alpha^r)t_r^\lambda$$

für alle Werthe $r=1, 2, 3, \ldots \lambda-1$ folgt. Die complexen Zahlen w_1 und t_r sind hier ebenfalls nur wirkliche complexe Zahlen, weil die λten Potenzen

derselben wirkliche complexe Zahlen sind. Giebt man dem r einen andern Werth s, so erhält man ebenfalls

$$28. \quad u+\alpha^s v = e_s(\alpha)(1-\alpha^s).t_s^\lambda,$$

und wenn man aus diesen drei Gleichungen u und v eliminirt, so erhält man

$$29. \quad e_r(\alpha)t_r^\lambda - e_s(\alpha)t_s^\lambda = \frac{e(\alpha)(\alpha^r-\alpha^s)(1-\alpha)}{(1-\alpha^r)(1-\alpha^s)}(1-\alpha)^{(m-1)\lambda}.w_1^\lambda.$$

Dividirt man durch $e_r(\alpha)$ und setzt

$$\frac{-e_s(\alpha)}{e_r(\alpha)} = \varepsilon(\alpha) \text{ und}$$

$$\frac{e(\alpha)(\alpha^r-\alpha^s)(1-\alpha)}{e_r(\alpha)(1-\alpha^r)(1-\alpha^s)} = E_1(\alpha),$$

wo $\varepsilon(\alpha)$ und $E_1(\alpha)$ ebenfalls nur complexe Einheiten sind, so ergiebt sich

$$30. \quad t_r^\lambda+\varepsilon(\alpha)t_s^\lambda = E_1(\alpha)(1-\alpha)^{(m-1)\lambda}.w_1^\lambda.$$

Ist nun $m>1$, so ist bekanntlich $(1-\alpha)^{(m-1)\lambda} \equiv 0$, mod. λ. Ferner, da t_r und t_s wirkliche complexe Zahlen sind, so müssen die λten Potenzen derselben realen ganzen Zahlen congruent sein für den Modul λ, also mufs $t_r^\lambda \equiv c$ und $t_s^\lambda \equiv k$, mod. λ, sein. Die Gleichung (30.) giebt daher folgende Congruenz:

$$c+\varepsilon(\alpha)k \equiv 0, \text{ mod. } \lambda,$$

aus welcher folgt, dafs die Einheit $\varepsilon(\alpha)$ einer realen ganzen Zahl congruent ist, für den Modul λ, dafs also $\varepsilon(\alpha)$ eine λte Potenz einer andern Einheit sein mufs, mithin $\varepsilon(\alpha)=\varepsilon_1(\alpha)^\lambda$. Setzt man nun $\varepsilon_1(\alpha)t_s=v_1$ und statt t_r das Zeichen u_1, so geht die Gleichung (30.) in folgende über:

$$31. \quad u_1^\lambda+v_1^\lambda = E_1(\alpha)(1-\alpha)^{(m-1)\lambda}.w_1^\lambda.$$

Diese Gleichung ist aber der Form nach der Gleichung (19.), aus welcher sie abgeleitet ist, vollkommen gleich und unterscheidet sich von ihr nur dadurch, dafs m um eine Einheit kleiner ist. Wendet man also auf die Gleichung (31.) dieselbe Methode an, so erhält man aus ihr wieder eine Gleichung von derselben Form, in welcher m um zwei Einheiten kleiner ist, als in der Gleichung (19.) u. s. w. Durch Wiederholung dieses Verfahrens gelangt man stets zu einer Gleichung von derselben Form wie (19.), in welcher $m=1$ ist: auf diese aber ist sodann die Methode, welche, wie wir oben ausdrücklich bemerkt haben, $m>1$ voraussetzt, nicht weiter anwendbar. Man erhält also eine Gleichung von der Form

$$32. \quad u^\lambda+v^\lambda = E(\alpha).(1-\alpha)^\lambda.w^\lambda.$$

Die Unmöglichkeit dieser Gleichung läfst sich einfach dadurch beweisen, dafs gezeigt wird: die Form $u^\lambda+v^\lambda$, wenn sie überhaupt den Factor $1-\alpha$ enthält, müsse denselben wenigstens $\lambda+1$ mal enthalten. Um dies zu beweisen, setze ich für u und v wieder wie oben die Formen

$$u = a+(1-\alpha)^2 P, \quad v = b+(1-\alpha)^2 Q,$$

so ergiebt sich wieder

$$33. \quad u+\alpha^r v \equiv a+b-rb(1-\alpha), \text{ mod. } (1-\alpha)^2.$$

Da nun $u^\lambda+v^\lambda$ durch $1-\alpha$ theilbar ist und deshalb auch wenigstens einer der Factoren dieses Ausdrucks, welche alle die Form $u+\alpha^r v$ haben, durch $1-\alpha$ theilbar sein mufs, so folgt, dafs $a+b$ durch $1-\alpha$ und deshalb auch durch λ theilbar ist. Die Congruenz (33.) geht demnach, eben so wie oben, in folgende über:

$$34. \quad u+\alpha^r v \equiv rb(1-\alpha), \text{ mod. } (1-\alpha)^2.$$

Für $r=0$ ist insbesondere

$$35. \quad u+v \equiv 0, \text{ mod. } (1-\alpha)^2.$$

Es sind also alle die Factoren der Form

$$u^\lambda+v^\lambda = (u+v)(u+\alpha v)(u+\alpha^2 v) \ldots (u+\alpha^{\lambda-1} v)$$

durch $1-\alpha$ theilbar; der Factor $u+v$ aber ist durch $(1-\alpha)^2$ theilbar. Die Anzahl aller in $u^\lambda+v^\lambda$ enthaltenen Factoren $1-\alpha$ ist demnach mindestens gleich $\lambda+1$; was zu beweisen war. Die Gleichung (32.), in welcher w nicht durch $1-\alpha$ theilbar ist, enthält also den Widerspruch in sich, dafs die Seite derselben links durch $(1-\alpha)^{\lambda+1}$ theilbar ist, die rechts aber nicht. Diese Gleichung ist also eine unmögliche, und darum ist auch die Gleichung (19.), aus welcher sie abgeleitet wurde, unmöglich: d. h. eine solche, welche durch complexe ganze Zahlen auf keine Weise erfüllt werden kann.

Die Gleichung $u^\lambda+v^\lambda+w^\lambda=0$ ist also in beiden Fällen unmöglich, sowohl wenn keine der complexen Zahlen u, v, w durch $1-\alpha$ theilbar ist, als auch wenn eine derselben durch $1-\alpha$ theilbar angenommen wird. Der *Fermat*sche Satz ist demnach nicht nur für reale ganze Zahlen, sondern sogar für complexe, aus λten Wurzeln der Einheit gebildete ganze Zahlen bewiesen, für alle diejenigen Potenzen, deren Exponenten λ Primzahlen sind und welche die Bedingung erfüllen, dafs sie in keiner der ersten $\frac{1}{2}(\lambda-3)$ *Bernoulli*schen

Zahlen als Factoren des Zählers vorkommen. Da $\lambda = 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43$ diese Bedingung erfüllen, so ist namentlich für alle diese der *Fermat*sche Satz bewiesen. Für $\lambda = 37$ aber, wird die angegebene Bedingung nicht erfüllt: also ist auch der *Fermat*sche Satz für 37te Potenzen nicht bewiesen. Meine gegenwärtigen Kenntnisse der Theorie der complexen Zahlen haben mir auch noch nicht die Mittel gewährt, für $\lambda = 37$ und für die übrigen Primzahlen, welche der angegebenen Bedingung nicht genügen, die Nicht-Auflösbarkeit oder Auflösbarkeit der *Fermat*schen Gleichung zu ergründen.

Breslau, den 19ten Juni 1849.