| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Mod. | 15312 | 16068 | 18938 | 9426 | 3387 | 3539 | 16677 | 18339 | 4901 | 13358 | 12453 | 1582 | 22723 | 14117 | 15628 |
| $151^2 = 22801$ | | | | | | | | | | | | | | | |
| $157^2 = 24649$ | 1 | 1101 | 19628 | 4400 | 14606 | 17904 | 7386 | 13196 | 19163 | 10058 | 325 | 17753 | 17754 | 22465 | 18698 |
| | 10535 | 4413 | 23568 | 22313 | 6457 | 11639 | 12739 | 22160 | 24045 | 22790 | 497 | 12273 | 11018 | 500 | 4583 |
| | 22639 | 14005 | 19658 | 2860 | 15892 | 17620 | 22331 | 16209 | 12599 | 10245 | 18410 | 21708 | 19040 | 358 | 5383 |
| | 20299 | 9467 | 519 | 4759 | 23757 | 1778 | 4919 | 6961 | 4921 | 14342 | 3510 | 20781 | 8222 | 10578 | 17487 |
| | 20157 | 5400 | 3360 | 13880 | 7444 | 1636 | 13726 | 18437 | 226 | 20951 | 13259 | 857 | 9022 | 11378 | 16717 |
| | 233 | 9497 | 18761 | | | | | | | | | | | | |
| $163^2 = 26569$ | 1 | 21844 | 5219 | 7665 | 1635 | 22826 | 12069 | 22991 | 4736 | 6204 | 12399 | 17290 | 22344 | 17618 | 4416 |
| | 8166 | 19903 | 20067 | 10288 | 18276 | 19581 | 25939 | 2794 | 4425 | 16325 | 9806 | 8014 | 22196 | 2474 | 17634 |
| | 6551 | 20407 | 14866 | 12585 | 18617 | 8186 | 14381 | 10470 | 1995 | 21719 | 1182 | 19602 | 18462 | 1022 | 11781 |
| | 3143 | 7056 | 1678 | 9503 | 20751 | 15536 | 2986 | 20428 | 21244 | 218 | 18312 | 23692 | 710 | 711 | 26303 |
| | 24022 | 25979 | 8865 | 22395 | 65 | 6586 | 10988 | 23866 | 22074 | 4634 | 25173 | 5614 | 3170 | 13277 | 19961 |
| | 728 | 6923 | 5620 | 26485 | 13772 | 5460 | | | | | | | | | |
| $181^2 = 32761$ | 1 | 20817 | 26610 | 17742 | 4711 | 17382 | 28062 | 20461 | 28607 | 15214 | 31143 | 28610 | 27887 | 5263 | 16124 |
| | 10876 | 7076 | 15222 | 3458 | 9251 | 8347 | 29163 | 14141 | 12151 | 14324 | 31520 | 30435 | 7087 | 9622 | 16863 |
| | 3832 | 27182 | 25735 | 7636 | 9447 | 11982 | 1485 | 9269 | 3659 | 8909 | 29363 | 27916 | 6921 | 24841 | 21584 |
| | 15612 | 27921 | 32447 | 32448 | 24847 | 14893 | 14532 | 11637 | 416 | 10915 | 7296 | 24492 | 420 | 27752 | 2956 |
| | 22867 | 30470 | 26851 | 32463 | 4047 | 17623 | 9479 | 2240 | 31925 | 26677 | 12741 | 19801 | 21793 | 19622 | 20166 |
| | 23244 | 2430 | 78 | 22523 | 31393 | 23430 | 27594 | 29043 | 12754 | 17099 | 24340 | 14205 | 15473 | 26877 | 29774 |
| $193^2 = 37249$ | 1 | 2897 | 11776 | 11584 | 35517 | 32237 | 22009 | 34748 | 33398 | 11011 | 36295 | 7346 | 28191 | 27034 | 16420 |
| | 18158 | 1947 | 18353 | 33794 | 13723 | 36691 | 29937 | 17007 | 12183 | 19904 | 19519 | 19906 | 20100 | 6205 | 1767 |
| | 16050 | 8138 | 14894 | 15860 | 23388 | 14318 | 13354 | 10846 | 14128 | 10848 | 813 | 22430 | 6026 | 11817 | 2361 |
| | 26101 | 13364 | 19348 | 10085 | 436 | 19737 | 2561 | 22634 | 6230 | 13372 | 9513 | 27077 | 21867 | 35571 | 15886 |
| | 5272 | 10098 | 22065 | 34418 | 6627 | 13576 | 34228 | 18403 | 23808 | 36354 | 36355 | 21109 | 18022 | 22076 | 18796 |
| | 19955 | 11850 | 29414 | 4325 | 25749 | 5099 | 8574 | 276 | 17454 | 17455 | 24790 | 24791 | 2018 | 30583 | 23250 |
| | 36375 | 36376 | 3374 | 13797 | 24220 | 28660 | | | | | | | | | |
| $199^2 = 39601$ | 1 | 14131 | 9157 | 16919 | 35626 | 21100 | 27469 | 11152 | 15332 | 23094 | 9165 | 8171 | 19714 | 35038 | 33845 |
| | 16533 | 21111 | 39022 | 25889 | 29074 | 27682 | 15345 | 28082 | 27486 | 39427 | 25100 | 9579 | 30276 | 30078 | 2418 |
| | 19732 | 21524 | 9386 | 5208 | 30283 | 15558 | 6604 | 3421 | 19740 | 23920 | 36856 | 35265 | 13774 | 24720 | 1239 |
| | 24722 | 16763 | 37659 | 28108 | 36069 | 20946 | 21544 | 28311 | 4631 | 2045 | 20553 | 13987 | 34286 | 39262 | 32696 |
| | 19563 | 2251 | 37674 | 19964 | 7229 | 9817 | 37877 | 15590 | 17581 | 667 | 6240 | 24947 | 24550 | 21168 | 30323 |
| | 28931 | 9828 | 36097 | 37292 | 18985 | 38289 | 19385 | 22769 | 30332 | 37895 | 1479 | 38892 | 37500 | 10835 | 4667 |
| | 19792 | 26161 | 26162 | 24372 | 14224 | 1091 | 29549 | 35719 | 13432 | | | | | | |



# Studien über den grossen Fermatschen Satz

## (Studja nad wielkiem twierdzeniem Fermata)

von

S. Lubelski

Das Ziel der vorliegenden Arbeit ist, durch Verallgemeinerung der bekannten Sätze der Fermatschen Gleichung zu beweisen, was in dieser Theorie für jene charakteristisch ist. Hierbei ergeben sich Sätze für die allgemeine Gleichung $x^p + y^p = c\,z^p$.

Im zweiten Teile erörtern wir die elementaren Methoden dieses Problems, um auch hier das für sie Charakteritische hervorzuheben.

## ERSTER TEIL.

### Einführung.

Die Verteilung der $p$-*ten* Potenzreste und Nichtreste (mod $p^2$) ergibt für $p \neq 1 \pmod 6$ und $p < 200$ unmittelbare Beweise der Lösbarkeit der Fermatschen Gleichung [1]). Ein tieferes Eindringen in die Eigenschaften dieser Zahlen gibt uns die Möglichkeit, Bedingungen für die Lösbarkeit der Gleichung

$$x^p + y = c\,z^p, \tag{1}$$

wo $p$ eine ungerade Primzahl und $c$ eine belielige ganze rationale Zahl

[1]) s. R. Niewiadomski: Zur Fermatschen Vermutung (die Arbeit ist in diedem Bande enthalten).

ist, in ganzen rationalen Zahlen aufzustellen. Dazu benötigen wir die Furtwänglersche, Kummersche und Mirimanoffsche Theorie der Gleichung $x^p+y^p+z^p=0$. Und zwar weisen wir darauf hin, welche Sätze von diesen Theorien auf die Theorie der Gleichung (1) angewandt werden können und beweisen (s. Satz 3):

*„Ist die Gleichung (1), wo $p\geqq 3$ eine Primzahl und $c$ eine ganze rationale Zahl ist, welche keine Primteiler der Form $pt+1$ hat und welche entweder ein $p$-ter Potenzrest (mod $p^2$) oder ein solcher $p$-ter Potenznichtrest, für welche zugleich $\frac{c}{2}$ ein $p$-ter Potenznichtrest (mod $p^2$) ist, in ganzen rationalen durch $p$ nicht teilbaren Zahlen $x, y, z$ lösbar, so ist*

$$2^{p-1}-1\equiv 0 \pmod{p^2}.$$

Diesen Satz erhalten wir mittels der Furtwänglerschen Theorie. Benutzen wir die Kummer-Mirimanoffsche Theorie bei Erwägung der Gleichung (1), so erhalten wir im Falle, wenn $c$ und $\frac{c}{2}$ gleichzeitig keine $p$-te Potenzreste (mod $p^2$) sind, den folgenden Satz:

*„Ist $c$ eine beliebige ganze rationale Zahl, welche keine Primteiler der Form $pt+1$ hat und welche zugleich mit $\frac{c}{2}$ ein $p$-ter Potenznichtrest (mod $p^2$) ist, so ist die Gleichung (1) im Falle:*
*„I: wenn $p$ eine ungerade Primzahl ist, in ganzen rationalen $x, y, z$, wobei $(z, p)=1$, nicht lösbar;*
*„II: wenn $p=2q$, wo $q$ eine beliebige Primzahl der Form $q\equiv -1 \pmod 4$, in ganzen rationalen Zahlen, nicht lösbar (s. Satz 6 und auch Folgerung dieses Satzes).*

Demnach haben wir für unendlich viele Exponenten unendlich viele der Fermatschen sehr ähnliche Gleichungen, welche in ganzen Zahlen nicht lösbar sind. Zugleich erhält man einigermassen eine Grundlage für die Erforschung der Formen höheren Grades.

Zuletzt geben wir eine Anwendung der Wieferich-Mirimanoff-Frobeniusschen Kriterien, und zwar wollen wir auf einfachstem Wege beweisen, dass $x^p+y^p+z^p=0$ für $p=6857$ in ganzen, durch $p$ nicht teilbaren Zahlen, nicht lösbar ist. (s. Satz 8). Dadurch haben wir für alle $p<7000$ kontrollierbare Beweise der Nichtlösbarkeit des ersten Falles der Fermatschen Vermutung (Für alle





$p\neq 6857$ und $<7000$ hat L. Dickson kontrollierbare Beweise gegeben s. L. Dickson: On the least theorem of in the Messenger of Mathem., new series 1908, Nr. 445 und in Quarterly J. of Math. 1908, Nr. 157).

## § 1

1. R. Niewiadomski [1]) hat für Systeme $p$-ter Potenzreste (mod $p^2$) Tafeln aufgestellt, wo $p<200$ eine Primzahl ist. Im Falle, wenn $p\equiv -1 \pmod 6$ und $p\neq 59, 83, 179$ erhielt Niewiadomski ohne weiteres den Beweis des ersten Teiles der Fermatschen Vermutung. Und zwar ergibt sich, dass in allen genannten $p$ (mod $p^2$), eine Summe zweier Reste niemals einem dritten gleich ist. Somit bewies Niewiadomski, dass in allen obigen Fällen das genannte Problem,— eine sozusagen reine Kalkulationsaufgabe ist.

2. Die Benutzung der von Niewiadomski aufgestellten Tafeln kann sehr erleichtert werden. Es ergibt sich nämlich, dass zugleich mit der Gleichung $x^p+y^p=z^p$, wo $x, y, z$ ganzzahlig und $(p, xyz)=1$, die Kongruenz

$$t^p+1\equiv t_1^p \pmod{p^k}$$

besteht, wo $k$ eine beliebige natürliche Zahl ist. Es genügt also, in den obigen Tafeln, $p$-te Potenzreste zu suchen, welche „Zwillinge" bilden, d. h, Paare unmittelbar aufeinander folgender natürlicher Zahlen.

Nehmen wir $l\equiv\frac{x}{y} \pmod p$ an, so erhalten wir, da

$$(x+y)^p\equiv z^p \pmod{p^2},$$

dass

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

also müssen sich zwischen den Potenzrestzwillingen auch solche ergeben, welche „Zwillinge" in noch einer Hinsicht sind: sie müssen als $p$-te Potenzreste zweier aufeinanderfolgender Zahlen $l$ und $l+1$ hervorgehen, wo $l<p$ angenommen werden kann. Damit sehen wir auch, dass die Bezeichnung (in den Niewiadomskischen Tafeln), aus welcher Potenz eine Zahl Rest ist, von Nutzen ist.

Finden sich für gewisse Moduln keine solche $p$-te Potenzreste, so ist evident, dass der erste Teil der Fermatschen Vermutung für die entsprechende Zahl wahr ist. Demzufolge ergibt sich sehr einfach aus den Niewiadomskischen Tafeln, dass für die Zahlen $p<200$, wo $p\equiv -1 \pmod 6$ und $p\neq 59, 83, 179$, solche $p$-te Potenzrestzwillinge nicht zu finden sind.

**3.** Aus den Abelschen Formeln der Zahlen $x$, $y$, $z$ der Gleichung $x^p+y^p+z^p=0$, im Falle, wenn $(p, xyz)=1$ ist, erhält man unmittelbar (s. z. B [2]) S. 15 und 54), dass

$$x+y+z\equiv 0 \pmod{p^2},$$

also ist

$$(x+y)^p\equiv z^p \pmod{p^3}$$

und demnach

$$(t+1)^p-t^p-1\equiv 0 \pmod{p^3}, \tag{1}$$

wo $t\equiv\frac{x}{y} \pmod{p^2}$ ist. Nun beweisen wir, dass wenn $v\equiv\frac{x}{y} \pmod{p}$ ist, so ist es desgleichen

$$(v+1)^p-v^p-1\equiv 0 \pmod{p^3}.$$

Und zwar ist, da $t=v+kp$, wo $k$ eine gewisse ganze Zahl ist, dass

$$(v+1)^p-v^p-1\equiv 0 \pmod{p^2}. \tag{2}$$

Bezeichnen wir mit $f(v)$ das Polynom

$$f(v)=(v+1)^p-v^p-1,$$

so erhalten wir, der Taylorschen Reihe gemäss, dass

$$f(t)=f(v+kp)=f(v)+kpf'(v)+Ap^3,$$

wo $A$ eine gewisse ganze rationale Zahl ist. Da

$$f'(v)=p[(v+1)^{p-1}-v^{p-1}],$$

so ergibt sich

$$f(t)\equiv f(v)\equiv 0 \pmod{p^3}.$$

**4.** Offenbar sind zugleich mit $t$ auch

$$-1-t,\quad \frac{-t}{1+t},\quad \frac{1}{t},\quad -\frac{1}{1+t},\quad -1-\frac{1}{t} \tag{3}$$

Lösungen der Kongruenz (1). Wenn $t\not\equiv 1 \pmod{p}$ und

$$t^2+t+1\not\equiv 0 \pmod{p},$$

sind alle Zahlen der Folge (3) zueinander inkongruent. Da jeder Lösung

[2]) P. Bachmann: Das Fermatproblem in seiner bisherigen Entwicklung; Berlin und Leipzig 1919.





der Kongruenz (1) eine Zahl $v$ aus (2) entspricht, welche man auch $v<p$ annehmen kann, so existieren, wenn die Folge (3) aus lauter (mod $p$) verschiedenen Zahlen besteht, sechs solche Zahlen $v<p$. Demnach können wir jetzt sehr einfach die Ausnahmefälle

$$p=59,\ 83,\ 179$$

erledigen. Und zwar, um den ersten Teil des Fermatschen Satzes für diese Exponenten zu beweisen, genügt es zu beweisen, dass die Kongruenz

$$x^p+y^p+z^p\equiv 0 \pmod{p^3}$$

nicht bestehen kann. Da für diese $p\not\equiv 1 \pmod 6$ ist, so ist die Kongruenz

$$x^2+x+1\equiv 0 \pmod{p}$$

nicht lösbar. Ferner ist, wie sich aus den Niewiadomskischen Tafeln ergibt, $t\not\equiv 1 \pmod{p}$ (und zwar ergibt sich aus $x\equiv y \pmod{p}$, dass $2^p\equiv 2 \pmod{p^2}$). Somit sind die Zahlen der Folge (3) miteinander inkongruent. Für $p=59$ ergeben sich aus den Niewiadomskischen Tafeln 12 Lösungen der Kongruenz, (2) d. h. zwei volle Gruppen von je sechs Lösungen. In der einer Gruppe findet sich als Lösung

$$v\equiv 2 \pmod{59}.$$

Offenbar findet sich nicht die Zahl 3, welche auch aus den N.—Tafeln entnommen ist, in der entsprechenden Gruppe (3), welche $v=2$ bildet. Es genügt also zu beweisen, dass die Kongruenz (1) für $t=2$ und $t=3$ (mod $59^3$) nicht besteht. Tatsächlich haben wir

$$2^{59}\equiv 70566 \pmod{59^3},$$

$$3^{59}\equiv 118652 \pmod{59^3},$$

$$4^{59}\equiv 146501 \pmod{59^3}.$$

Für die Moduln 83 und 179 gibt es nur einzelne Gruppen von Lösungen, und es genügt z. B. für $p=83$ zu beweisen (den N.—Tafeln gemäss), dass

$$9^{83}-8^{82}\not\equiv 1 \pmod{83^3};$$

und für $p=179$, dass

$$3^{73}-2^{73}\not\equiv 1 \pmod{73^3}.$$

Und zwar haben wir

$$9^{83}\equiv 12957 \pmod{83^3};$$

$$8^{83} \equiv 6067 \pmod{83^3};$$

$$2^{179} \equiv 3446289 \pmod{179^3};$$

$$3^{179} \equiv 4183233 \pmod{179^3}.$$

Damit sind alle Fälle $p \equiv -1 \pmod 6$, wo $p < 200$, erledigt.

**Anmerkung**: Die Berechnungen der Zahlen $8^{83}$, $9^{83}$, $2^{179}$, $3^{179}$ sind durch R. Niewiadomski durchgeführt.

Die Existenz einer vollen Gruppe (3) von Lösungen, für die Moduln $p = 59, 85$, hat zuerst A. Arwin (s. A. Arwin: Die Kongruenzen $(\lambda+1)^p - \lambda^p - 1 \equiv 0 \pmod{p^v}$ und die Natur ihrer Lösungen; Lunds Universitets Arsskrift N. F. Avd. 2 Bd, Nr. 17/2 (1921). a) S. 19 und 24; b) S. 7—11).

5. Anders verhält sich die Frage im Falle, wenn $p \equiv 1 \pmod 6$, und zwar, wie Niewiadomski mittels einleuchtender Rechnungen bewiesen hat, solche $p$-te Potenzreste stets zu finden sind. Dies kann man auch unmittelbar aus der wohlbekannten Cauchyschen Identität schliessen:

$$(l+1)^p - l^p - 1 = p\,l\,(l^2+l+1)^\varepsilon f(l),$$

wo $p$ prim und $>3$ ist, für $p \not\equiv 1 \pmod 6$, $\varepsilon = 1$; für $p \equiv 1 \pmod 6$, $\varepsilon = 2$ ist, dabei ist $f(l)$ eine ganze rationale Funktion mit ganzen Koeffizienten. Da für Primzahlen $p$, wo $p \equiv 1 \pmod 6$, die Kongruenz

$$l^2 + l + 1 \equiv 0 \pmod{p^k} \tag{4}$$

immer lösbar ist, wo $k$ eine beliebige natürliche Zahl ist, so sind hier $p$-te „Potenzrestzwillinge" stets zu finden, welche stets paarweise erscheinen. Denn ist $l_0$ eine Lösung der Kongruenz (4), so ist $(p^k - 1 - l_0)$ desgleichen eine solche Lösung.

6. Die Niewiadomskischen Tafeln sind aber auch in Falle $p \equiv 1 \pmod 6$ von Nutzen, und nämlich: wollen wir die Gleichung

$$x^p + y^p + A\,z^p = 0,$$

wo $A$ eine ganze rationale Zahl ist, in ganzen, durch die Primzahl $p$ nicht teilbaren Zahlen lösen, so genügt es in den Tafeln die Unmöglichkeit der Kongruenz

$$r_p + R_p + A \equiv 0 \pmod p \tag{5}$$

zu verifizieren, wo $r_p$ und $R_p$ entsprechende $p$-te Potenzreste $(\mathrm{mod}\ p^2)$ sind. Ist z. B. $A = 3$, so sieht man unmittelbar aus den Tafeln, dass





für alle Primzahlen $p$, wo

$$p = 1,\ 7,\ 11,\ 19,\ 31,\ 41,\ 61,\ 67,\ 71,\ 83,$$

die Kongruenz (5) nicht möglich ist,

## § 2

Von besonderer Wichtigkeit sind die $p$-te Rest und Nichtpotenzreste $(\mathrm{mod}\ p^2)$, welche keine Primteiler der Form $pt+1$ haben. Und zwar bieten wir einige in dieser Klassifikation geltende Sätze, Zuvor wollen wir einige Hilfssätze beweisen, welche dem Furtwänglerschen Ideenkreis entnommen sind:

*Fortan sei die Primzahl $p > 2$ fest gegeben, auch werde $r$ eine natürliche Primzahl,*

$$\rho = e^{\frac{2\pi i}{p}}, \quad \lambda = 1 - \rho, \quad \Omega = P(\rho)$$

*der zugrundegelegte Kreisteilungskörper gesetzt.*

**Hilfssatz 1:** *Ist $K(\rho)$ der Kreisteilungskörper $w$ eine beliebige Zahl dieses Körpers und $\mathfrak{q}$ ein beliebiges zu $pw$ relatives Primideal, so besteht die Kongrueuz*

$$w^{N(\mathfrak{q})-1} - 1 \equiv \prod_{j=1}^{p-1} \left(w^{\frac{N(\mathfrak{q})-1}{p}} - \rho^j\right) \equiv 0 \pmod{\mathfrak{q}}.$$

*(s. [3]) S. 294—5, Satz 1021).*

Also muss für einen eindeutig bestimmten Exponent $i$

$$w^{\frac{N(\mathfrak{q})-1}{p}} \equiv \rho^i \pmod{\mathfrak{q}}. \tag{1}$$

**Definition 1:** *Die Potenz von $\rho$, für welche (1) besteht, nennt man Potenzcharakter von $w$ in Bezug auf $\mathfrak{q}$ und wird durch das Symbol*

$$\rho^i = \left(\frac{w}{\mathfrak{q}}\right)$$

*bezeichnet.*

**Hilfssatz 2:** *Wenn $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_k$ beliebige Primideale bedeuten, so ist (offenbar, s. [3]) S. 297, Satz 1029).*

$$\left(\frac{w}{\mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_k}\right) = \left(\frac{w}{\mathfrak{q}_1}\right)\left(\frac{w}{\mathfrak{q}_2}\right)\ldots\left(\frac{w}{\mathfrak{q}_k}\right) \tag{2}$$

[3]) E. Landau: Vorlesungen über Zahlentheorie B. III (1927)

**Hilfssatz 3:** *Ist*

$$w \equiv \omega' \pmod{\mathfrak{q}},$$

*so ist (offenbar, s. [3]) S. 295—6, Sätze 1022—4)*

$$\left(\frac{w}{\mathfrak{q}}\right) = \left(\frac{\omega'}{\mathfrak{q}}\right). \tag{3}$$

**Hilfssatz 4:** *Es seien $\alpha$ und $\gamma$ ganz. Dann ist*

$$\left(\frac{\alpha}{\mathfrak{A}}\right)\left(\frac{\gamma}{\mathfrak{A}}\right) = \left(\frac{\alpha\gamma}{\mathfrak{A}}\right)$$

*falls eine Seite einen Sinn hat (s. [3]) S. 297, Satz 1027).*

**Definition 2:** *$\alpha$ heisst primär, wenn $\alpha$ durch $\lambda$ nicht teilbar ist und*

$$\alpha \equiv a \pmod{\lambda},$$

*bei passendem ganzem rationalem $a$ (s. [3]) S. 227 Def. 120).*

**Hilfssatz 5:** *Es sei $r$ eine Primzahl $\neq p$, $\alpha$ primär*

$$([r],[\alpha]) = 1, \quad [\alpha] = \mathfrak{A}^p.$$

*Dann ist $\left(\frac{\alpha}{r}\right) = 1$ (s. [3]) S. 310—1, Satz 1033).*

**Hilfssatz 6:** *Es sei $\gamma$ eine ganze reelle Körperzahl uud*

$$([r],[\gamma]) = 1.$$

*Dann ist $\left(\frac{\gamma}{r}\right) = 1$. (s. [3]) S. 312—3, Satz, 1034).*

**Hilfssatz 7:** *Aus $\left(\frac{\rho}{r}\right) = 1$ folgt*

$$r^{p-1} - 1 \equiv 0 \pmod{p^2}$$

*(s. [3]) S. 314, Satz, 1036).*

**Hilfssatz 8:** *Sind $x$, $y$ und $z$ ganze rationale Zahlen, für welche*

$$\frac{x^p + y^p}{x+y} = z^p \quad (x,y) = 1, \quad (rp, z) = 1,$$

*wo $p > 2$ und $r$ verschiedene Primzahlen sind, so ist*

$$\left(\frac{\rho^{yu}x + \rho^{-xu}}{r}\right) = 1,$$

*wo $u$ eine beliebige durch $p$ nicht teilbare ganze Zahl ist.*





**Beweis** (vgl., für $u = 1$, [3]) S. 314—5). Nach Voraussetzung ist

$$\prod_{m=1}^{p-1} [x + \rho^m u] = [z]^p.$$

Da $(p, z) = 1$, so sind links je zwei Faktoren teilerfremd und somit ist jeder dieser $(p-1)$ Faktoren, $p$-te Potenz eines Ideals. Es ist evident, dass

$$x + y \not\equiv 0 \pmod{p},$$

denn andernfalls wird $p|z$ sein. Somit haben wir, dass

$$[x + \rho^{u(-x-y)} y] = \mathfrak{A}^p,$$

wo $\mathfrak{A}$ ein gewisses Ideal ist. Desgleichen ist auch

$$[\rho^{yu}x + \rho^{-xu}y] = \mathfrak{A}^p.$$

Nun ist

$$\rho^{-xu} = \rho^{kp-xu} = (1-\lambda)^{kp-xu} = 1 + ux\lambda \pmod{\lambda^2},$$

wo $k$ eine beliebige natürliche Zahl ist, für welche

$$kp - ux > 0$$

ist. Somit haben wir

$$\rho^{yu}x \equiv (1 - u\lambda y)x \pmod{\lambda^2};$$

$$\rho^{-ux}y \equiv (1 + u\lambda x)y \pmod{\lambda^2},$$

folglich

$$\rho^{uy}x + \rho^{-xu}y \equiv (x+y)u \pmod{\lambda^2}$$

und demnach ist die Zahl $(\rho^{uy}x + \rho^{-xu}y)$ primär und zugleich durch $\lambda$ nicht teilbar. Da mit $r$ auch $\rho^{uy}x + \rho^{-xu}y$ zu $z$ relativ prim ist, so ist, dem Hilfssatze 5 gemäss, der Satz bewiesen.

Jetzt gehen wir zu den Sätzen über, welche für das Weitere grundlegend sind:

**Satz 1:** *Ist $p$ eine Primzahl und $x$, $y$, $z$, $r$ ganze rationale Zahlen, für welche*

$$\frac{x^p + y^p}{x+y} = z^p; \quad (x,y) = 1, \quad r|x, \quad (p, xz) = 1,$$

*so ist*

$$r^{p-1} - 1 \equiv 0 \pmod{p^2}.$$

**Beweis.** Dem vorigen Satze und den Eigenschaften (2) und (3) des Symbols $\left(\frac{w}{r}\right)$ gemäss, erhalten wir:

$$1=\left(\frac{\rho^y x+\rho^{-x}y}{r}\right)=\left(\frac{\rho^{-x}y}{r}\right)=\left(\frac{\rho^{-x}}{r}\right)\cdot\left(\frac{y}{r}\right).$$

Dem Hilfssatze 6 gemäss ist $\left(\frac{y}{r}\right)=1$. Da $(x,p)=1$, so ist

$$1=\left(\frac{\rho^{-x}}{r}\right)=\left(\frac{\rho}{r}\right)^{-x}=\left(\frac{\rho}{r}\right)=1.$$

Folglich ist nach Hilfssatz 7, der Satz bewiesen.

**Satz 2:** *Ist $p$ eine ungerade, $r$ eine beliebige Primzahl $\neq p$ und sind $x$, $y$, $z$ ganze rationale Zahlen, für welche*

$$\frac{x^p+y^p}{x+y}=z^p;\quad (x,y)=1,\quad r|(x^k-y^k),\quad (x^2-y^2,p)=1,$$

*wo $k=1$, wenn $xy$ ungerade ist und $k=2$, wenn $xy$ gerade ist, so ist*

$$r^{p-1}-1\equiv 0 \pmod{p^2}.$$

**Beweis.** Aus der Voraussetzung des Satzes folgt unmittelbar $(r,z)=1$. Denn ist $r|(x+y)$ und $r|z$, so ergibt sich aus der Gleichung

$$z^p=\frac{[(x+y)-y]^p+y^p}{x+y}=(x+y)^{p-1}+p\,(x+y)^{p-2}+\ldots\ldots+p,$$

dass $r|p$. Desgleichen folgt aus

$$z^p=x^{p-1}+x^{p-2}y+\ldots\ldots+y^{p-1},$$

dass, wenn $r|(x-y)$ und $r|z$, die Kongruenzen

$$x\equiv y\equiv 0 \pmod{r}$$

sich ergeben, welche, da $(x,y)=1$, unmöglich sind. Wir betrachten jetzt den Fall $k=2$, wobei $r|(x+y)$. Gemäss Hilfssatz 8 ist

$$1=\left(\frac{\rho^y x+\rho^{-x}y}{r}\right)=\left(\frac{\rho^y x-\rho^{-x}x}{r}\right)=\left(\frac{x}{r}\right)\left(\frac{\rho^y-\rho^{-x}}{r}\right)=\left(\frac{\rho^y-\rho^{-x}}{r}\right).$$

Da im Falle $r|(x+y)$ eine der Zahlen $x$, $y$ gerade ist, so können wir, wegen der Symmetrie, z. B. $x$ ungerade und $y$ gerade annehmen. Somit folgt

$$\left(\frac{\rho^y-\rho^{-x}}{r}\right)=\left(\frac{(-\rho)^y+(-\rho)^{-x}}{r}\right)$$

$$=\left(\frac{-\rho}{r}\right)^{\frac{p+1}{2}(y-x)}\left(\frac{(-\rho)^{\frac{p+1}{2}(y+x)}+(-\rho)^{-\frac{p+1}{2}(y+x)}}{r}\right)=1.$$





Es ist evident, dass die Zahl

$$(-\rho)^{\frac{p+1}{p}(y-x)}+(-\rho)^{-\frac{p+1}{p}(y+x)}$$

reell ist und es ergibt sich

$$\left(\frac{-\rho}{r}\right)^{\frac{p+1}{2}(y-x)}=\left(\frac{\rho}{r}\right)^{\frac{p+1}{2}(y-x)}=1.$$

Da $\left(p,\frac{p+1}{2}(y-x)\right)=1$, so haben wir $\left(\frac{\rho}{r}\right)=1$, folglich ist nach Hilfssatz 7

$$r^{p-1}-1\equiv 0 \pmod{p^2}.$$

Ist $r|(x-y)$, so ergibt sich analog (und sogar auf kürzerem Wege, da die Unterscheidung $x$ ungerade oder gerade hier überflüssig ist), dass desgleichen die Relation (1) besteht.

w. z. b. w.

Wir wollen jetzt diese Sätze auf die verallgemeinerte Fermatsche Gleichung

$$x^p+y^p=c\,z^p,\quad (c,p)=1$$

anwenden. Und zwar werden wir zuerst annehmen, dass $c$ entweder ein $p$-ter Potenzrest (mod $p^2$) oder ein $p$-ter Nichtpotenzrest (mod $p^2$), für welche $\frac{c}{2}$ (mod $p^2$) zugleich ein $p$-ter Potenznichtrest ist.

**Bemerkung:** Fast alle Reste (mod $p^2$) haben die genannte Eigenschaft, nämlich:

1) wenn 2 ein Potenzrest (mod $p^2$) ist, so sind es alle Zahlen welche nicht Potenzreste (mod $p^2$).

2) und wenn 2 ein Potenznichtrest (mod $p^2$), sind es auch alle der Form $2g$, wo $g$ ein $p$-ter Potenzrest (mod $p^2$) ist.

Im ersteren Falle beträgt die Anzahl (mod $p^2$):

$$\varphi(p^2)-\varphi(p)=(p-1)^2.$$

Im zweiten Falle:

$$\varphi(p^2)-2\varphi(p)=(p-2)(p-1).$$

**Satz 3:** *Ist die Gleichung*

(1) $$x^p+y^p=c\,z^p,\quad (c,p)=1,$$

*wo $p\geqq 3$ eine Primzahl und $c$ eine ganze rationale Zahl ist, welche keine Primteiler der Form $pt+1$ hat und welche entweder ein $p$-ter Potenz-*

*rest (mod $p^2$) oder ein solcher p-ter Potenznichtrest, für welchen zugleich* $\frac{c}{2}$ *ein p-ter Potenznichtrest (mod $p^2$) ist, in ganzen rationalen durch p nicht teilbaren Zahlen x, y, z lösbar, so ist*

$$2^{p-1}-1\equiv 0 \pmod{p^2}.$$

**Beweis.** Es ist evident, dass man $x, y, z$ als paarweise teilerfremd annehmen kann. Denn ist $(y,z)=a$, so ist auch $(x,y,z)=a$ und man kann beide Seiten der Gleichung (1) durch $a^p$ dividieren. Wir können also $(x,y,z)=1$ annehmen. Ist aber $(x,y)=b$, so muss demnach $c$ durch $b^p$ teilbar sein. Setzt man

$$x=b\,x_1,\quad y=b\,y_1,\quad c=b^p c_1,$$

so erhält man, dass in der Gleichung

$$x_1^p+y_1^p=c_1 z^p$$

die Zahlen $x_1, y_1, z_1$ paarweise teilerfremd sind. Somit ergibt sich aus der Gleichung (1), dass für eine gewisse ganze rationale Zahl $u$ (da $c$ keine Primteiler der Form $p\,t+1$ hat und $\frac{x^p+y^p}{x+y}$ nur solche Primteiler haben kann), dass

$$x+y=c\,u^p,$$

also ist für eine gewisse ganze rationale Zahl $v$:

$$\frac{x^p+y^p}{x+y}=v^p.$$

Wäre $(x+y)$ durch $p$ teilbar, so wäre auch $z$ durch $p$ teilbar, was der Annahme widerspricht. Desgleichen können wir annehmen, dass $(x-y)$ durch $p$ nicht teilbar ist. Und zwar ergibt sich im Falle, wenn $c$ Nichtrest ist, da aus

(2) $$2x^p\equiv 2y^p\equiv c z^p \pmod{p^2}$$

folgt, dass

$$\frac{c}{2}\equiv\left(\frac{x}{z}\right)^p \pmod{p^2}$$

ist entgegen der Voraussetzung, dass $\frac{c}{2}$ kein $p$-ter Potenzrest (mod $p^2$) ist.

Ist aber $c$ ein $p$-ter Potenzrest, so ergibt sich aus (2) dass 2 $p$-ter Potenzrest ist, d. h., dass

$$2^p\equiv 2 \pmod{p^2}.$$





Man kann also annehmen, dass $x^2-y^2$ durch $p$ nicht teilbar ist und somit wird im Falle, wenn eine der Zahlen $x, y$ gerade ist, dem Satze 1 gemäss, und im Falle, wenn $x, y$ ungerade sind, dem Satze 2 gemäss:

$$2^{p-1}-1\equiv 0 \pmod{p^2}.$$

**Satz 4:** *Die Gleichung*

$$x^{2p}+y^{2p}=c\,z^p,$$

*wo p eine beliebige Primzahl der Form $p\equiv -1$ (mod 4), c eine ganze rationale Zahl, welche entweder ungerade oder durch 4 teilbar ist, keine Primteiler der Form $p\,t+1$ hat und welche gleichzeitig mit* $\frac{c}{2}$ *(mod $p^2$) ein p-ter Potenznichtrest ist, ist in ganzen rationalen Zahlen nicht lösbar.*

**Beweis.** Es ist evident (s, Beweis des vorigen Satzes), dass man $(x,y)=1$ annehmen kann. Da $p\equiv -1$ (mod 4) ist, so kann $p$ kein Teiler einer Summe zweier Quadrate sein, und somit ist $z$ durch $p$ nicht teilbar.

Wie im vorstehenden Beweise (s. Relation (2)), sehen wir, dass man $(x-y,p)=1$ annehmen kann. Nun folgt aus den Eigenschaften der Zahl $c$, dass $c\,z^p$ entweder ungerade oder durch 4 teilbar ist. Demnach können die Zahlen $x, y$ niemals gleichzeitig ungerade sein, sonst wird

$$x^{2p}+y^{2p}\equiv 2 \pmod 8$$

sein. Gemäss Satz 2 ergibt, sich für jede Primzahl $r$, welche Teiler der Zahl $(x^2+y^2)$ ist, dass

(1) $$r^{p-1}-1\equiv 0 \pmod{p^2}.$$

Da das Produkt zweier Lösungen der Kongruenz (1) zugleich eine Lösung dieser Kongruenz ist, erhält man

$$(x^2+y^2)^p\equiv x^2+y^2 \pmod{p^2}.$$

Nun ist weder $x$ noch $y$ durch $p$ teilbar, denn andernfalls wird z. B.

$$x^{2p}\equiv c\,z^p \pmod{p^2}$$

sein, was, da $c$ ein $p$-ter Potenznichtrest ist, unmöglich ist. Somit haben wir, dem Satze 1 gemäss:

$$x^{2p}\equiv x^2 \pmod{p^2},$$

$$y^{2p}\equiv y^2 \pmod{p^2}$$

und wir erhalten

$$(x^2+y^2)^p \equiv x^{2p}+y^{2p} \equiv c\,z^p \pmod{p^2},$$

was ergibt

$$c \equiv \left(\frac{x^2+y^2}{z}\right) \pmod{p^2},$$

entgegen der Annahme, dass $c$ ein $p$-ter Potenznichtrest ist.

w. z. b. w.

Um die letzten zwei Sätze zu verallgemeinern, müssen wir die Kummersche Theorie anwenden. Dazu benutzen wir die folgenden Sätze, welche sich aus der Kummerschen Theorie unmittelbar ergeben.

**Hilfssatz 9:** *Ist die Gleichung*

$$x^p+y^p=cz^p, \quad (c,p)=1, \tag{1}$$

*wo $p$ eine ungerade Primzahl, $c$ eine ganze rationale Zahl ist, welche keine Primteiler der Form $pt+1$ hat, in ganzen durch $p$ nicht teilbaren Zahlen lösbar, so bestehen die Kongruenzen*

$$\frac{d_0^{p-2s}\log(x+e^v y)}{d\,v^{p-2s}} B_s \equiv 0 \pmod{p}, \tag{2}$$

$$s = 1,\ 2,\ \ldots\ldots,\ \frac{p-1}{2}-1,$$

*wo $B_s$ die $s$-te Bermoullische Zahl ist.*

**Beweis.** Wie im Satze 2 (s. Anfang des Beweises) kann man die Zahlen $x$, $y$, $z$ als paarweise teilerfremd annehmen. Somit existiert eine ganze rationale Zahl $v$, für welche die Gleichung

$$\prod_{m=1}^{p-1}(x+\rho^m y) = v^p \tag{1}$$

besteht, demnach ist jedes Ideal $[x+\rho^m y]$ $p$-te Potenz eines gewissen Ideals des Körpers $K(\rho)$:

$$[x+\rho^m y] = j_m^p = j(\rho^m).$$

Nun hat Kummer gezeigt [4]), dass das Produkt

$$\prod_i j(\rho g^i) \tag{2}$$

[4]) E. Kummer: Jour. f. Math. v. Cr. Bd. 35 S. 364 vgl. auch.

[5]) D. Hilbert: Theorie des corps de nombres algebraïques. Paris 1913; Note VI par Th. Got S. 326—330.





ausgedehnt über alle Werte des Index $i$ aus der Reihe

$$0,\ 1,\ 2,\ \ldots\ldots\ p-2,$$

für welche

$$g_{\pi-i}+g_{\pi-i+indr} > p; \qquad \pi=\frac{p-1}{2},$$

unter $r$ eine beliebige natürliche Zahl aus der Reihe (3), und unter indr den auf die primitive Wurzel $g$ bezüglichen Index (mod $p$) verstanden, einem Hauptideal gleich ist. Da

$$g^i \not\equiv 0 \pmod{p},$$

so figuriert jeder Faktor von (2) auch in (1) und man erhält

$$\prod_i (x+\rho g^i) = \varepsilon f(\rho)^p,$$

wo $\varepsilon$ eine Einheit ist. Nun kann man beweisen, dass für eine gewisse natürliche Zahl $k$

$$\varepsilon = \rho^k$$

(s. [5]) S. 331 und vgl. mit der Kummerschen Arbeit in Abh. d. Berl. Akad. d. Wiss. 1857).

Man erhält somit

$$\prod_i (x+u\varepsilon^i y) = \pm u^k . f(u)^p + F(u)\,M(u),$$

wo $u$ eine unabhängige Variable ist und

$$F(u) = u^{p-1}+u^{p-2}+\ldots\ldots+u+1.$$

Für $u=e^v$ ergibt dies

$$\sum_i \log(x+e^{v\varepsilon^i}y) = \log(\pm 1)+mv+p\log f(e^v)+\log\left(1\pm\frac{F(e^v)M(e^v)}{e^{mv}f(e^v)^p}\right).$$

Differenzieren wir diese Gleichung $n$-mal, so erhalten wir, wenn man $v=0$ setzt, da

$$\frac{d_0^i F(e^v)}{d\,v^i} = (p-1)^i+(p-2)^i+\ldots\ldots+2^i+1^i \equiv 0 \pmod{p},$$

dass

$$\sum \frac{d_0^n \log(x+e^{v\varepsilon^i}y)}{d\,v^n} \equiv 0 \pmod{p}$$

(vgl. [5]) S. 215 Fussnote auch [3]) S. 113), welches ergibt

$$\sum \frac{d_0^n \log(x+e^{v\varepsilon^i}y)}{d\,v^n} \equiv 0 \pmod{p}$$

$$s = 1, 2, \ldots\ldots \frac{p-1}{2}.$$

(s. [2]) S. 112—4) oder

$$\frac{d_0^n \log(x + e^v y)}{dv^n} \sum_i g^{ni} \equiv 0 \pmod p;$$

$$\frac{d_0^{p-2s} \log(x + e^v y)}{dv^n} \cdot \sum_i g^{(p-2s)i} \equiv 0 \pmod p,$$

wo $p - 2s = n$ ist. Nun ist (s. [2]) S. 114—7 oder [4]) b) S. 331—3),

$$\sum_i g^{(p-2s)i} \equiv B_s \pmod p$$

und somit erhalten wir die Kongruenz (2).

**Folgerung:** *Damit die Gleichung (1), wo p eine ungerade Primzahl, c eine ganze rationale Zahl, welche keine Primteiler der Form $pt+1$ hat, in ganzen durch p nicht teilbaren Zahlet lösbar sei, ist es notwendig, dass die Kongruenzen*

$$\varphi_{p-2s}(t) B_s \equiv 0 \pmod p$$

*oder*

$$\varphi_i(t) B_{\frac{p-i}{2}} \equiv 0 \pmod p$$

$$i = 3, 5, 7, \ldots\ldots p-2,$$

*wo*

$$\varphi_i(t) = t - 2^{i-1} t^2 + 3^{i-1} t^3 - + \ldots\ldots (-1)^{p-2} (p-1)^{i-1} t^{p-1},$$

*mit $t \equiv \frac{x}{y}$ (mod p), bestehen sollen.*

**Beweis.** Definieren wir das Polynom $P_i(x, y)$ mittels der Gleichung

$$\frac{d_0^i \log(x + e^v y)}{dv^i} = \frac{P_i(x, y)}{(x+y)^i},$$

so sehen wir, dass $P_i(x, y)$ eine ganze homogene Funktion bezüglich $x, y$ von dem $i$—ten Grade ist, welche für $i > 1$ durch $xy$ teilbar ist, so dass, wenn man

$$P_i(x, y) = x^i P_i(1, t)$$

oder kurz

$$P_i(x, y) = x^i P_i(t)$$

setzt, $P_i(t)$ die Form

$$P_i(t) = a_{i,1} t + a_{i,1} t^2 + \ldots\ldots + a_{i,i-1} t^{i-1}$$

[6]) D. Mirimanoff: L'equation indéterminée $x^e + y^e + z^e = 0$, ..., Journ. f. Math. 128 (1905) S. 45—68.





hat. Wie D. Mirimanoff bewies [6]) ist

$$a_{i,k} = k^{i-1} - \binom{i}{1}(k-1)^{i-1} + \binom{i}{2}(k-2)^{i-1} + \ldots\ldots (-1)^{k-1}\binom{i}{k-1}.$$

Bezeichnen wir mit $\varphi_i(t)$ die Funktion

$$\varphi_i(t) = (1+t)^{p-i} P_i(t),$$

so erhalten wir

$$\varphi_i(t) = t - 2^{i-1} t^2 + 3^{i-1} t^3 - \ldots\ldots (-1)^{p-2} (p-1)^{i-1} t^{p-1}.$$

**Satz 5:** *Ist die Gleichung*

$$x^p + y^p = c z^p, \quad (c, p) = 1,$$

*wo p eine ungerade Primzahl, c eine ganze rationale Zahl, welche keine Primteiler der Form $pt+1$ hat und welche entweder ein p-ter Potenzrest (mod $p^2$) oder zugleich mit $\frac{c}{2}$ p-ter Potenznichtrest (mod $p^2$) ist, in ganzen dnrch p nicht teilbaren Zahlen lösbar, so ist die Kongruenz*

$$(1) \qquad \frac{(t+1)^p - t^p - 1}{p} \equiv 0 \pmod p$$

*mit $t \equiv \frac{x}{y}$ (mod p) lösbar.*

**Beweis.** Ist $c$ ein $p$-ter Potenzrest (mod $p^2$), so ist der Satz klar (sogar dann, wenn die Primteiler der Zahl $c$ nicht alle der Form $pt+1$ sind). Denn ist

$$c \equiv c_1^p \pmod{p^2},$$

so haben wir aus

$$x^p + y^p + z_1^p \equiv 0 \pmod{p^2},$$

wo

$$z_1 \equiv -az \pmod{p^2},$$

dass

$$x + y + z_1 \equiv 0 \pmod p,$$

was

$$(x+y)^p \equiv (-z_1)^p \pmod{p^2}$$

ergibt oder

$$(x+y)^p - x^p - y^p \equiv 0 \pmod{p^2}.$$

Setzen wir $t \equiv \frac{x}{y} \pmod p$, so erhalten wir aus der letzten Kongruenz, die Kongruenz (1).

II. Ist $c$ zugleich mit $\frac{c}{2}$ $p$-ter Potenznichtrest (mod $p^2$), so ist

$$x \not\equiv y \pmod p,$$

denn andernfalls wird

$$2x^p \equiv 2y^p \equiv cz^p \pmod{p^2}$$

sein, was

$$\frac{c}{2} \equiv \left(\frac{z}{y}\right)^p \equiv \left(\frac{z}{x}\right)^p \pmod{p^2},$$

ergibt — der Annahme entgegen.

Der vorigen Folgerung gemäss gelten die Kongruenzen:

$$\varphi_i(t)\, B_{\frac{p-i}{2}} \equiv 0 \pmod{p}$$

$$i = 3,\ 5,\ 7,\ \ldots\ldots,\ p-2,$$

wo

$$\varphi_i(t) = t - 2^{i-1}t^2 + 3^{i-1}t^3 - + \ldots\ldots (-1)^{p-2}(p-1)^{i-1}t^{p-1}.$$

Nun haben wir

$$\varphi_{p-1}(t) \equiv t - \frac{1}{2}t^2 + \frac{1}{3}t^3 - + \ldots\ldots - \frac{1}{p-1}t^{p-1} \equiv$$

$$\equiv t + \frac{p-1}{2!}t^2 + \frac{(p-1)(p-2)}{3!}t^3 + \ldots\ldots + \frac{(p-1)(p-2)\ldots\ldots 3.2}{(p-1)!}$$

$$\equiv \frac{(t+1)^p - t^p - 1}{p}.$$

Die Kongruenz (1) ist also mit der Kongruenz

$$\varphi_{p-1}(t) \equiv 0 \pmod{p}$$

gleichbedeutend. Aus einfacher Erwägung ergibt sich

$$\frac{\varphi_{p-1}(t)}{1+t} \equiv t - (1^{p-2} + 2^{p-2})t^2 + (1^{p-2} + 2^{p-2} + 3^{p-2})t^3$$

$$+ \ldots\ldots - (1^{p-2} + 2^{p-2} + \ldots\ldots + (p-1)^{p-2})t^{p-1}$$

denn aus

$$-k^{p-2} \equiv (p-k)^{p-2} \pmod{p}$$

folgt

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

Bezeichnen wir mit $s_j(n)$ die Summe der $j$-ten Potenzen der ersten $n$ Zahlen, so erhalten wir

$$\frac{\varphi_{p-1}(t)}{1+t} = \sum_{n=1}^{p-1} (-1)^{n-1} s_{p-2}(n)\, t^n.$$

Nun haben wir nach der Bernoullischen Formel (s. z. B. Niels Nielsen





Traitè élémentaire des Nombres de Bernoulli. Paris 1923, S. 296)

$$s_{p-2}(n) = \frac{n^{p-1}}{p-1} + \frac{n^{p-2}}{2} + \sum_{s=1}^{\leq \frac{p-2}{2}} \frac{(-1)^{s-1}}{p-1} \binom{p-1}{2s} n^{p-2s-1}.$$

Setzen wir dies in der letzten Gleichung an, so nimmt sie die Gestalt:

$$\frac{\varphi_{p-1}(t)}{1+t} = \frac{1}{p-1}\varphi_1(t) + \frac{1}{2}\varphi_{p-1}(t) + \sum \frac{(-1)^{s-1}}{p-1} \binom{p+1}{2s} B_s \varphi_{p-2s},$$

wo

$$\varphi_1(t) = t - t^2 + t^3 - \ldots - t^{p-1} = \frac{t(1-t^{p-1})}{1+t}.$$

Da $z$ durch $p$ nicht teilbar ist, so ist

$$1 + t \not\equiv 0 \pmod{p}$$

und somit ist

$$\varphi_1(t) \equiv 0 \pmod{p}$$

mit $t \equiv \frac{x}{y} \pmod{p}$. Dem vorigen Satze gemäss (s. Folgerung) ist

$$B_s \varphi_{p-2s}(t) \equiv 0 \pmod{p}.$$

Nun ist

$$t \not\equiv 1 \pmod{p},$$

und somit folgt aus

$$\frac{1}{1+t} \not\equiv \frac{1}{2} \pmod{p},$$

$$\left(\frac{1}{1+t} - \frac{1}{2}\right)\varphi_{p-1}(t) \equiv 0 \pmod{p},$$

dass

$$\varphi_{p-1}(t) \equiv 0 \pmod{p}$$

w. z. b. w.

Wir können jetzt die Sätze 3 und 4 verallgemeinern, und zwar gelten, die folgenden Sätze:

**Satz 6:** *Ist $p$ eine ungerade Primzahl, $c$ eine beliebige ganze rationale Zahl, welche keine Primteiler der Form $pt+1$ hat und welche zugleich mit $\frac{c}{2}$ $p$-ter Potenznichtrest (mod $p^2$) ist, so ist die Gleichung*

$$x^p + y^p = cz^p, \quad (c,p) = 1$$

*in ganzen rationalen Zahlen $x$, $y$, $z$, wobei $z$ durch $p$ nicht teilbar ist, nicht lösbar.*

**Beweis.** Es ist evident, dass weder $x$ noch $y$ durch $p$ teilbar ist.

Denn wäre $p|x$, so folgt aus

$$y^p \equiv c\, z^p \pmod{p^2},$$

dass $c$ ein $p$-ter Potenzrest (mod $p^2$) ist. Damit ergibt sich dem vorigen Satze gemäss, dass

$$\frac{(t+1)^p - t^p - 1}{p} \equiv 0 \pmod{p}$$

mit $t \equiv \frac{x}{y} \pmod{p}$, d. h. dass

$$(x+y)^p - x^p - y^p \equiv 0 \pmod{p^2}$$

und demnach

$$(x+y)^p \equiv c\, z^p \pmod{p^2},$$

$$c \equiv \left(\frac{x+y}{z}\right)^p \pmod{p^2},$$

was der Annahme widerspricht.

Als unmittelbare Folgerung dieses Satzes erhalten wir den Satz:

**Folgerung.** *Die Gleichung*

$$x^{2q} + y^{2q} = c\, z^q,$$

*wo $q$ eine beliebige Primzahl der Form $q \equiv -1$ (mod 4), $c$ eine ganze rationale Zahl, welche keine Primteiler der Form $qt+1$ hat und welche zugleich mit $\frac{c}{2}$ (mod $q^2$). $q$-ter Potenznichtrest ist, ist in ganzen Zahlen nicht lösbar.*

Der Beweis ergibt sich aus der Bemerkung, dass $z$, wenn nur $(x,y)=1$, durch $q$ nicht teilbar sein kann, denn $q$ kann kein Teiler einer Summe zweier Quadrate sein.

Als weitere Anwendung des Satzes 5 können wir die folgende Verallgemeinerung eines Mirimanoffschen Satzes angeben:

**Satz 7:** *Ist die Gleichung*

$$x^p + y^p = c\, z^p, \quad (c,p) = 1,$$

*wo $p$ eine ungerade Primzahl ist, $c$ eine ganze rationale Zahl, welche keine Primteiler der Form $pt+1$ hat, in ganzen durch $p$ nicht teilbaren Zahlen lösbar, so ist.*

$$\varphi_{p-1}(-t) \equiv \varphi_{p-1}(-t^2) \equiv 0 \pmod{p},$$





*wo* $t \equiv \frac{x}{y} \pmod{p}$ *und*

$$\varphi_{p-1}(t) \equiv \frac{(t+1)^p - t^p - 1}{p} \pmod{p}. \tag{1}$$

**Erster Beweis.** Ist

$$x \equiv y \pmod{p},$$

so folgt aus der Kongruenz (1), dass

$$\varphi_{p-1}(-t) \equiv \varphi_{p-1}(-t^2) \equiv \varphi_{p-1}(-1) \equiv (-1+1)^p + 1 - 1 \equiv 0 \pmod{p}.$$

Es sei also

$$x \not\equiv y \pmod{p}.$$

Da das Produkt zweier Lösungen der Kongruenz

$$r^{p-1} \equiv 1 \pmod{p^2},$$

zugleich eine Lösung dieser Kongruenz ist, so folgt, dem Satze 2 gemäss, dass

$$(x-y)^p \equiv x - y \pmod{p^2}.$$

Dem Satze 1 gemäss ist aber

$$x^p \equiv x \pmod{p^2}$$

und

$$y^p \equiv y \pmod{p^2},$$

somit ergibt sich

$$(x-y)^p \equiv x^p - y^p \pmod{p^2},$$

d. h.

$$(-t+1)^p \equiv -t^p + 1 \pmod{p^2}. \tag{2}$$

Nun ist die Tatsache zu beachten, dass der Satz 5 immer, d. h. für jede Zahl $c$, welche keine Primteiler der Form $pt+1$ hat, wahr ist, wenn nur

$$x \not\equiv y \pmod{p}$$

ist, also ist auch

$$(t+1)^p \equiv t^p + 1 \pmod{p^2}. \tag{3}$$

Multiplizieren wir die Kongruenzen (2) und (3) miteinander, so erhalten wir:

$$(-t^2+1)^p \equiv -t^{2p} + 1 \equiv 0 \pmod{p^2}. \tag{4}$$

**Zweiter Beweis.** Man kann den vorigen Beweis nur mittels der Kummerschen Theorie führen. Und zwar haben wir aus der Kummerschen Theorie die Kongruenz

$$\varphi_{p-1}(t) \equiv \frac{(t+1)^p - t^p - 1}{p} \equiv 0 \pmod{p}$$

(s. Satz 5) und die Kongruenzbedingungen:

$$\varphi_i(t)\, B_{\frac{p-i}{2}} \equiv 0 \pmod p$$

$$(i = 3,\ 5,\ 7,\ \ldots\ldots,\ p-2)$$

(s. Folgerung des Hilfssatzes 9). Von diesen Kongruenzen ausgehend, erhielt D. Mirimanoff [7]) das folgende System der Kongruenzen (s. auch [2]) S. 127—9)

(5) $$\varphi_{p-i}(t)\, \varphi_i(t) \equiv 0 \pmod p$$

$$i = 2,\ 3,\ \ldots\ldots,\ \frac{p-1}{2}.$$

Nun ergibt sich aus einer einfachen Erwägung (s. [7]) S. 315 und [2]) S. 137), dass

$$\sum_{n-1}^{p-1} \varphi_n(t)\, \varphi_{p-n}(t) = \varphi_{p-1}(-t^2).$$

Teilen wir die Kongruenz (4) durch (3), so erhalten wir die Kongruenz (2).

w. z. b.w

Nun beweisen wir aus der Kummer-Mirimanoffschen Theorie ausgehend den folgenden Satz

**Satz 8:** *Ist*

(1) $$x^p + y^p = c\, z^p,$$

*wo p eine ungerade Primzahl, c eine ganze rationale Zahl, welche keine Primteiler der Form pt+1 hat, in ganzen durch p nicht teilbaren Zahlen lösbar und ist*

$$x \not\equiv y \pmod p,$$

*so ist*

$$3^{p-1} - 1 \equiv 0 \pmod{p^2}.$$

**Beweis.** Die Zahl $t$, wo $t \equiv \frac{x}{y} \pmod p$, ist, wie es schon im vorigem Satze erwähnt war, eine Lösung der Kongruenzen (1) und (4). Demnach hat Mirimanoff bewiesen (s. [7]) S. 317), dass solche $t$ auch der Kongruenz

$$\Phi(t) = \Pi(t+\alpha_l) \sum_{i-1}^{i=m-1} \frac{R_l}{t+\alpha_l} \equiv 0 \pmod p$$

genügen, wo $\alpha_l$ die verschiedenen Wurzeln der Gleichung

$$\frac{z^m - 1}{z - 1} = 0$$

[7]) D. Mirimanoff: Sur le dernier théorème de Fermat: Jour. f. Math. 139 (1911) S. 309—324.





bezeichnen und

$$R_l = \frac{\varphi_{n-1}(-\alpha_l)}{(1-\alpha_l)^{p-1}}.$$

Letztere Kongruenz ist aber für $m = 3$ linear. Für ungerade $m$ ist

$$\Phi(1) \equiv 0 \pmod p$$

(s. [7]) S. 318 oder [2]) S. 142). Da $z$ durch $p$ nicht teilbar ist, so ist der Voraussetzung gemäss

$$\pm 1 \not\equiv t \not\equiv \frac{1}{t} \pmod p,$$

und es muss identisch

$$\Phi(t) \equiv 0 \pmod p$$

sein, also auch

$$\Phi(-1) \equiv 0 \pmod p$$

sein. Nun ist aber (s. [7]) S. 317 oder [2]) S. 141):

$$\frac{m^{p-1} - 1}{p} \equiv \sum \frac{R_l}{1-\alpha_l} \pmod p$$

und somit muss für $m = 3$

$$\frac{3^{p-1} - 1}{p} \equiv \Phi(-1) \equiv 0 \pmod p$$

sein *)

w. z. b. w.

Die Mirimanoffsche Theorie ist durch Frobenius [8]) fortgeführt worden, welcher bewiesen hat, dass für alle Primzahlen $p$, wo $p \equiv 5 \pmod 6$:

$$q^{p-1} = 5^{p-1} \equiv 7^{p-1} \equiv 13^{p-1} \equiv 1 \pmod{p^2}.$$

(dies war durch F. Pollaczek, für alle $q \leqq 31$, bis auf endlich viele Ausnahmen bez. $p$, verallgemeinert [9])). Wir werden dies benutzen um den folgenden Satz zu beweisen:

**Satz 9:** *Die Gleichung* $x^p + y^p + z^p = 0$, *für* $p = 6857$, *ist durch p nicht teilbare Zahlen, nicht lösbar.*

*) Mit dem Fall, $p$ eine reguläre Primzahl d. h. ist die Klassenzahl von $k(p)$ durch $p$ nicht teilbar, hat sich mit der Gleichung (1) E. Maillet (s. Acta Math. 24: 247—256 (1901)) befasst. Man kann diesen Fall unmittelbar ausgehend von den Kummerschen Erwägungen (s. [3]) S. 232—4, 271—4) erledigen. Für $p > 100$ ist es aber sehr schwierig zu erkennen, ob eine Primzahl $p$ regulär ist. Dabei ist beachtungswert, dass bei Maillet, $c$ höchstens aus $p-3$ verschiedenen Primidealfaktoren zusammengesetzt ist.

[8]) G. Frobenius: Über den Fermatschen Satz I, II, III. Berliner Akad.-Ber. 1909, 1910, 1914.

[9]) F. Pollaczek: Über den grossen Fermatschen Satz. Wiener Akad. Ber. B. 126 (1917).

**Beweis.** Es ist

$$6857 \equiv 5 \pmod 6,$$

also ist s. [8]) und [9]):

$$5^{6856} \equiv 7^{6856} \equiv 13^{6856} \equiv 1 \pmod{6857^2}.$$

Nun ist

$$5^6 = 15625 = 2 \cdot 6857 + 1911; \quad 1911 = 3 \cdot 7^2 \cdot 13,$$

Wir haben also

$$5^{6p} \equiv 1911^p \equiv 1911 = 3 \cdot 7^2 \cdot 13 \pmod{p^2},$$

wo $p = 6857$. Da

$$5^{6 \cdot 6857} \equiv 5^6 \pmod{6857^2},$$

so ist dies unmöglich, denn

$$5^6 \not\equiv 1911 \pmod{6857^2}.$$

**Anmerkung:** L. Dickson [10]) hat mittels der Sophie Germainschen Theorie bewiesen, dass für alle Primzahlen $p$, wo $p < 7000$, ausser im Falle $p = 6857$ der erste Teil der Fermatschen Vermutung wahr ist. Benutzen wir das Wieferichsche Kriterium, so kann man, wie es Beeger [11]) getan hat, beweisen, dass auch für $p = 6857$ der Satz wahr ist. Die Rechnuungen welche man durchführen muss, um die Relation

$$2^{p-1} - 1 \not\equiv 0 \pmod{6857^2},$$

zu verifizieren, sind aber kompliziert. Dagegen ist der obige Beweis unmittelbar und auch allgemein auwendbar.

## ZWEITER TEIL.

Wir erörtern zuerst einen Kapfererschen Satz bezüglich der Lösbarkeit der Gleichung

$$z^3 - y^2 = 3^3 \cdot 2^{2n-2} x^{2n} \tag{1}$$

in drei ganzen rationalen Zahlen $x$, $y$, $z$ von denen je zwei teilerfremd sind. Kapferer [12]) hat nämlich bewiesen, dass die Lösbarkeit der Gleichung (1) mit der Lösbarkeit der Fermatschen Gleichung $x^n + y^n + z^n = 0$ äquivalent ist. Nun weisen wir auf einen Jermakoffschen [13]) Satz hin,

[10]) L. Dickson: Messenger of Math. (2), 38 (1908) 14—32; Quart. Jour. Math. 40, 1908, 27—45.

[11]) N. G. W. Beeger: Mess. of Math. 55: 17—21 (1925), Assoc. Française Liége (1924), 105—6.

[12]) H. Kapferer: Über die diophantischen Gleichungen $z^3 - y^2 = 3^3 2^{\lambda} \cdot x^{\lambda+2}$ und deren Abhängigkeit von der Fermatschen Vermutung s. B. Heidelberg. Akad. Wiss. Abh. B. 2 S. 32—7 (1933) vgl. Zntrbl. für Math. B. 7 Heft 1. S. 4.

[13]) V. Jermakow: Wiestnik opytnoj fizyki i element. mat. 1912 S. 87.





welcher als Ausgangspunkt des vorigen Satzes angeschen werden kann. Auf Grund dieses Satzes verallgemeinern wir leicht den Kapfererschen Satz folgendermassen:

*Damit die Gleichung*

$$x^n + y^n + Pz^n = 0,$$

*wo $n$ eine natürliche Zahl und $P$ eine Primzahlpotenz ist, in ganzen rationalen Zahlen, $x$, $y$, $z$ lösbar sei, ist es notwendig und hinreichend, dass die Gleichung*

$$u^3 - v^2 = 3^3 2^{-2} P^2 w^{2n}$$

*in drei ganzen rationalen Zahlen $u$, $v$, $w$, von denen je zwei teilerfremd sind, lösbar sei.*

Um das bekannte Wendtsche Kriterium zu verallgemeinern und ein Bachmannsches Kriterium zu widerlegen, benutzen wir die folgenden, an und für sich charakteristischen, Hilfssätze:

*Haben die Kongruenzen*

$$f(z) \equiv f_1(z) \equiv 0 \pmod p,$$

*wo $f(z)$ und $f_1(z)$ ganzzahlige Polynomen sind und $p$ eine Primzahl ist, (mod $p$) $g$ gemeinsame Wurzeln, so ist (mod $p$) der Rang der Matrix der Sylvestreschen Resultante gleich $m + n - g$. (s. Hilfssatz 10).*

*Haben die Polynome $f(x)$ und $f_1(x)$ (mod $p$) einen gemeinsamen Teiler, welcher mindestens vom zweiten Grade ist, so muss die Resultante dieser Polynome durch $p^2$ teilbar sein (s. Hilfssatz 11).*

Das verallgemeinerte Wendtsche [14]) Kriterium lautet:

*Ist die aus den Zahlen $(1, \binom{2h}{1}, \ldots\ldots \binom{2h}{2h-2}, \binom{2h}{2h-1})$ gebildete zyklische Determinante durch $\pi^2$ nicht teilbar oder ist mindestens ein Minor $(2h-2)$-ten Grades dieser Determinante durch $\pi$ nicht teilbar, wo $\pi = 2hp + 1$ zugleich mit $p$ ungerade Primzahlen sind, und $(h, p) = 1$ so ist, in der Gleichung $x^p + y^p + z^p = 0$, wo $x$, $y$, $z$ ganze rationale Zahlen sind, eine Zahl z. B. $x$, durch $p\pi$ teilbar.*

Bei Wendt ist die zyklische Determinante nur durch $p$ teilbar. Ferner werden bei Wendt die Minoren nicht berücksichtigt. Ausserdem muss gleichzeitig verifiziert werden, ob $p^{2h} \equiv 1 \pmod \pi$ und eine gewisse komplizierte zyklische Determinante (s. Anmerkung zum Satze 12) durch $\pi$ teilbar sei.

[14]) E. Wendt: Jour. f. Math. 113 (1894) S. 335—347.

Schliesslich widerlegen wir das Bachmannsche Kriterium folgendermassen:

*Die aus den Zahlen* $[1, \binom{p}{1}^{-1}, \binom{p}{2}^{-2}, \ldots, \binom{p}{p-2}^{-1}]$ *gebildete zyklische Determinante, wo* $p \geqq 7$ *eine Primzahl ist, ist stets durch* $p^3$ *teilbar.*

Bachmann hat bewiesen, dass im Falle, wenn die Fermatsche Vermutung, mit durch $p$ nicht teilbare Zahlen $x, y, z$ lösbar ist, die zyklische Determinante durch $p^3$ teilbar ist.

---

Der Kapfererersche Satz:

*„Die Existenz einer Lösung der Gleichung*

$$z^3 - y^2 = 3^3 \cdot 2^{2n-2} x^{2n}$$

*in drei ganzen rationalen Zahlen* $x, y, z$ *von denen jd zwei teilerfremd sind, ist für jede natürliche Zahl* $n = 2, 3 \ldots\ldots$, *gleichbedeutend mit der Existenz einer Lösung der Fermatschen Gleichung* $u^n + v^n = w^n$."

(wie wir glauben) wird, in einem neuem Lichte erscheinen, wenn wir seinen Zusammenhang mit einem sehr interessanten, aber wenig bekannten Jermakoffschen Satz aufdecken. Dies wird uns auch ermöglichen den Kapferrerschen Satz zu verallgemeinern. Der Jermakoffsche Satz [13]) lautet:

*Damit die Gleichung*

(1) $$x^3 = Ax + 2B,$$

*wo* $A$ *und* $B$ *teilerfremde ganze rationale Zahlen sind, in ganzen rationalen Zahlen lösbar sei, ist es notwendig und hinreichend, dass die Diskriminante dieser Gleichung eine Quadratzahl sei".*

Der Beweis dieses Satzes ist bei Jermakoff im Falle, wenn $3|A$, in komplizierter Weise durchgeführt. Nun bieten wir unseren Beweis des Jermakoffschen Satzes für diesen Fall:

**Beweis.** Der Voraussetzung gemäss ist die Diskriminante der Gleichung (1) gleich:

$$4A^3 - 27B^2 = D^2,$$

wo $D$ eine gewisse ganze rationale Zahl ist. Setzt man

$$A = 3A_1, \quad D = 2D_1,$$

so erhält man

$$A_1^3 = B^2 + 3D^2.$$

Da $A$ und $B$ teilerfremd sind, so ist $(A_1, 3) = 1$ und somit ist jeder





Primteiler der Zahl $A_1$ durch die Form $x^2 + 3y^2$ darstellbar. Daraus ergibt sich, dass man alle Darstellungen der Zahl $A_1^3$ durch die Form $x^2 + 3y^2$ mittels der Formel

$$x + \sqrt{-3}\, y = (u + \sqrt{-3}\, v)^3$$

erhalten kann, wo

$$A_1 = u^2 + 3v^2 \ [15]).$$

Nun ist es leicht zu verifizieren, dass

$$2u, \quad -u - 3v, \quad -u + 3v$$

Wurzeln der Gleichung (1) sind, und zwar ist:

$$2u + (-u - 3v) + (-u + 3v) = 0;$$

$$2u(-u - 3v) + 2u(-u + 3v) + u^2 - 9v^2 = -3(u^2 + 3v^2) = -A.$$

(Der Fall $(3, A) = 1$ verläuft gänzlich analog und ergibt sich sogar viel einfacher).

Als unmittelbare Folgerung dieses Satzes erhalten wir eine Verallgemeinerung des Kapfererschen Satzes.

**Satz 9:** *Ist die Gleichung*

(1) $$ax^n + by^n + cz^n = 0,$$

*wo* $a, b, c$ *ganze rationale Zahlen sind und* $n$ *eine beliebige natürliche Zahl ist, in ganzen rationalen Zahlen* $x, y, z$ *lösbar, so ist die Gleichung*

(2) $$u^3 - v^2 = 3^3 \cdot 2^{-2} a^2 b^2 c^2 w^{2h}$$

*in ganzen rationalen Zahlen* $u, v, w$ *lösbar. Ist* $n$ *ungerade,* $a = \pm 1$, $b = \pm 1$ *und* $c$ *Potenz einer Primzahl, so muss auch umgekehrt aus der Lösbarkeit der Gleichung* (2) *in ganzen rationalen* $u, v, w$, *von denen je zwei teilerfremd sind, auch die Lösbarkeit der Gleichung* (1) *in ganzen von Null verschiedenen Zahlen* $x, y, z$ *folgen.*

**Beweis.** Wir beachten die Gleichung

$$t^3 = ut + 2W$$

deren Wurzeln die Zahlen $ax^n$, $by^n$, $cz^n$ sind, also

$$W = \frac{1}{2} abc(xyz)^n.$$

---

[15]) s. d. Verfassers: Beweis und Verallgemeinerung eines Waring-Legendreschen Satzes. Math. Zeitsch. B. 33 (193) S. 326 (= Defin. 5 und Bemerkungen zu dieser Defin.; auch S. 335—6; Satz 3.

Die Diskriminante dieser Gleichung ist bekanntlich gleich $4u^3 - 27(2W)^2$, dabei muss sie Quadrat einer rationalen Zahl sein (denn die Wurzeln der Gleichung (2) ganze rationale Zahlen sind). Es existiert also eine ganze rationale Zahl $v$, für welche $u^3 - 27W^2 = v^2$ oder

$$u^3 - v^2 = 27W^2.$$

Ist umgekehrt die Gleichung

$$u^3 - v^2 = 3^3 2^{-2} c^2 w^{2n}$$

in ganzen rationalen $u, v, w$, von denen je zwei teilerfremd sind, lösbar, so ist, dem Jermakoffschen Satze gemäss, die Gleichung (3), wo $W = cw^n$, in ganzen, zueinander relativ primen rationalen Zahlen, lösbar. Sind dies $t_1, t_2, t_3$, so folgt aus

$$t_1 t_2 t_3 = c w^n,$$

da $c$ — Primzahlpotenz ist und $t_1, t_2, t_3$ teilerfremd sind, dass für gewisse ganze rationale Zahlen $x, y, z$, z. B.:

$$t_1 = x^n, \qquad t_2 = y^n, \qquad t_3 = cz^n$$

ist.

Wir gehen jetzt zu der Verallgemeinerung des Wendtschen Satzes über, dazu benötigen wir die folgenden zwei Hilffssätze:

**Hilfssatz 10:** *Haben die ganzzahligen Polynome $f(x)$ und $f_1(x)$ (mod p), wo p ein Primzahl ist, g gemeinsame Wurzeln, so ist, (wenn nur $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$, $f_1(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m$, der Rang der Matrix:*

(1)
$$\left.\begin{array}{llllllll} a_0, & a_1, & \ldots & a_n, & 0, & \ldots & 0 \\ 0, & a_0, & \ldots & a_{n-1}, & a_n, & \ldots & 0 \\ 0, & 0, & a_0, \ldots & & a_{n-1} & a_n \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0, & 0, & \ldots & & & a_n \end{array}\right\} m$$
$$\left.\begin{array}{llllllll} b_0, & b_1, & b_2, & \ldots & b_m, & 0, & \ldots & 0 \\ 0, & b_0, & b_1, & \ldots & b_{m-1}, & b_m & \ldots & 0 \\ 0, & 0, & b_0, \ldots & & b_{m-1} & b_m \ldots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0, & 0 & & & & b_{m-1}, & b_m \end{array}\right\} n,$$

*(mod p) gleich $m + n - g$.*





**Beweis.** Es sei

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n;$$

$$f_1(x) = b_0 x^m + b_1 x^{m-1} + \ldots + b_m,$$

wo

$$a_0, a_1, \ldots a_n; \qquad b_0, b_1, \ldots b_m$$

ganze rationale Zahlen sind. Wollen wir in der Gleichung

(2) $$f(x)\psi_1(x) + f_1(x)\psi(x) = R,$$

wo $R$ die Resultante der Polynome $f(x)$ und $f_1(x)$ ist, und $\psi(x)$ vom Grade $n-1$ und $\psi_1(x)$ vom Grade $m-1$ ist, die Koeffizienten von $\psi(x)$ und $\psi_1(x)$ finden, so erhalten wir $m+n$ folgende Gleichungen:

(3)
$$\begin{array}{llll} a_0 u_1 + & \ldots + b_0 v_1 + & \ldots & = 0 \\ a_1 u_1 + a_0 u_2 + \ldots + b_1 v_1 + b_0 v_2 + & \ldots & = 0 \\ \cdot & & & \\ \cdot & & & \\ \cdot & & & \\ o \cdot u_1 + o \cdot u_2 + \ldots + a_n u_m + o \cdot v_1 + o \cdot v_2 + \ldots + b_m v_n = R. & & & \end{array}$$

wo

$$\psi(x) = v_1 x^{n-1} + v_2 x^{n-2} + \ldots + v_n;$$

$$\psi_1(x) = u_1 x^{m-1} + u_2 x^{m-2} + \ldots + u_m.$$

Haben die Polynome $f(x)$ und $f_1(x)$ (mod $p$) einen gemeinsamen Teiler genau vom Grade $g$, so finden sich zwei (mod $p$) eindeutig bestimmbare Polynome $\varphi(x)$ und $\varphi_1(x)$, deren Grade entsprechend gleich sind $n-g$ und $m-g$, so dass

$$f(x)\varphi_1(x) + f_1(x)\varphi(x) \equiv 0 \pmod{p}.$$

Wir können jetzt die letzte Kogruenz mit einem Polynom vom Grade $g-1$ mit willkürlichen Koeffizienten, multiplizieren. Wir erhalten somit $m+n$ Kongruenzen (3), wobei die Koeffizienten

(4) $$u_1, u_2, \ldots u_m; \qquad v_1, v_2, \ldots v_n$$

durch $g$ Parameter linear (mod $p$) bestimmt werden. Die Determinante der Gleichungen (resp. Kongruenzen) (3) ist identisch mit der Determinante (1). Der Rang der letzten Matrix muss also vom Grade $m+n-g$ sein.

Umgekehrt ist die Matrix (1) (mod $p$) vom Range $m+n-g$, so

haben die Polynome $f(x)$ uud $f_1(x) \pmod p$ einen gemeinsamem Teiler vom Grade $g$ [16]).

**Hilfssatz 11:** *Haben die ganzzahligen Polynome $f(x)$ und $f_1(x) \pmod p$, wo $p$ eine Primzahl ist, einen gemeinsamen Teiler, welcher mindestens vom zweiten Grade ist, so muss die Resultante dieser Polynome durch $p^2$ teilbar sein.*

**Beweis.** Bezeichnet $\alpha$ eine Zahl der Reihe (4), so erhalten wir, den Gleichungen (3) gemäss, dass

$$\alpha = \frac{o\,.\,M_1 + o\,M_2 + \ldots R\,M_k + \ldots o\,M_{m+n}}{R} = M_k,$$

wo $M_1, M_2, \ldots M_k, \ldots M_{m+n}$ entsprechende Minoren vom Grade $m+n-1$ sind (bekanntlich ist die Determinante (1) genau gleich der Resultante der Polynome $f(x)$ und $f_1(x)$). Die Koeffizienten von $\psi(x)$ und $\psi_1(x)$ in der Gleichung (2) sind also entsprechend gleich den Minoren $(m+n-1)$-ten Grades von (1). Haben die Polynome $f(x)$ und $f_1(x) \pmod p$ einen gemeinsamen Teiler, dessen Grad mindestens zwei ist, so müssen, dem vorigen Hilfssatze gemäss, diese Minoren und die Resultante durch $p$ teilbar sein. Teilen wir, in der Gleichung (1), beide Seiten durch $p$, so erhalten wir:

$$f(x)\frac{1}{p}\psi_1(x) + f_1(x)\frac{1}{p}\psi(x) = \frac{1}{p}R,$$

wo die Koeffizienten von $\frac{1}{p}\psi_1(x)$ und von $\frac{1}{p}\psi(x)$ ganze rationale Zahlen sind. Da aber $f(x)$ und $f_1(x) \pmod p$ einen gemeinsamen Teiler haben, so muss $p \mid \frac{R}{p}$ sein, d. h., $R$ ist durch $p^2$ teilbar.

Die Verallgemeinerung des Wendtschen Satzes lautet also folgendermassen:

**Satz 12:** *Ist die zyklische Determinante*

$$(2) \qquad \begin{vmatrix} \binom{2h}{1}, \binom{2h}{2}, \ldots \binom{2h}{2h-1}, & 1 \\ \binom{2h}{1}, \binom{2h}{3}, \ldots & 1 \quad , \binom{2h}{1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ 1 \quad , \binom{2h}{1}, \ldots \binom{2h}{2h-2}, & \binom{2h}{2h-1} \end{vmatrix}$$

[16]) G. Darboux hat diesen Satz für algebraische Funktionen bewiesen (s. Bull. d. sc. math. et astr. I-ère serie. 10 (1876). II-me série, 1 (1878)). Obwohl sein Satz weniger allgemein ist, ist sein Beweis doch viel komplizierter.





*durch $\pi^2$, wo $\pi = 2hp+1$, zugleich mit $p$ Primzahlen sind, nicht teilbar, oder ist mindestens eine Unterdeterminante $(2h-2)$-ten Grades der Determinante (1) durch $\pi$ nicht teilbar, so ist, wenn nur $(p, h) = 1$, die Gleichung*

$$(2) \qquad x^p + y^p + z^p = 0$$

*in ganzen rationalen Zahlen $x, y, z$ nur dann lösbar, wenn eine der Zahlen $x, y, z$ durch $p\pi$ teilbar ist.*

**Beweis.** Ist die Gleichung (2) in ganzen rationalen, durch $\pi$ nicht teilbaren Zahlen, lösbar, so wird z. B.

$$\left(\frac{x}{z}\right)^p = \left(\frac{y}{z}\right)^p + 1 \pmod \pi$$

sein. Somit haben die Kongruenzen

$$(3) \qquad t^{2h} - 1 \equiv 0, \quad (t+1)^{2h} - 1 \equiv 0 \pmod \pi$$

die folgenden Wurzeln gemein:

$$\left(\frac{x}{y}\right)^p, \left(\frac{x}{z}\right)^p, \left(\frac{y}{x}\right)^p, \left(\frac{y}{z}\right)^p, \left(\frac{z}{x}\right)^p, \left(\frac{z}{y}\right)^p.$$

Nun kann

$$x^p \equiv y^p \equiv z^p \pmod \pi$$

gleichzeitig nicht bestehen, denn andernfalls ist

$$x^p + y^p + z^p \equiv 3x^p \equiv 3y^p \equiv 3z^p \equiv 0 \pmod \pi,$$

d. h. $(x, y, z) \neq 1$ Es müssen somit unter den Wurzeln (4) drei verschiedene geben. Die Matrix (1) aus Hilfssatz 10 mit

$$f(x) = t^{2h} - 1 \quad \text{und} \quad f_1(x) = (t+1)^{2h} - t^{2h}$$

ist also höchstens vom Range $m+n-3$ und von der Gestalt

$$(3) \qquad \begin{vmatrix} 1 & 0 & 0 & \ldots 0 & -1 & 0 & 0 \ldots & 0 \\ 0 & 1 & 0 & \ldots 0 & 0 & -1 & 0 \ldots & 0 \\ 0 & 0 & 0 & \ldots 0 & 0 & 0 & -1 \ldots & 0 \\ \cdot & & & & & & & \\ \cdot & & & & & & & \\ \cdot & & & & & & & \\ \binom{2h}{1}, & \binom{2h}{2}, & \ldots & & & & & 0 \\ 0 & \binom{2h}{1}, & \binom{2h}{2}, & \ldots & & & & 0 \\ 0 & 0 & \binom{2h}{1}, & \ldots & & & & 0 \\ \cdot & & & & & & & \\ \cdot & & & & & & & \\ \cdot & & & & & & \ldots \binom{2h}{2h-2}, & \binom{2h}{2h-1} \end{vmatrix}$$

Addieren wir die $k$-te Kolonne, wo $k=1, 2, \ldots 2h-1$, mit der $(2h+k)$-ten, so erhält die letzte Matrix die folgende Gestalt.

$$(4)\qquad \begin{vmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 \ldots & 0 & \ldots & 0 & 0 \\ \cdot & & & & & & \\ \cdot & & & & & & \\ \cdot & & & & & & \\ 0 & 0 & \ldots 1 & & & 0 & 0 \\ \binom{2h}{1}, & \binom{2h}{2}, & 1 \ldots 1 & \binom{2h}{2h-1}, & \binom{2h}{1} & \ldots & \binom{2h}{2h-2} \\ 0, & 0, & \ldots & \binom{2h}{2h-2}, & \binom{2h}{2h-1}, & \ldots & \binom{2h}{2h-3} \\ \cdot & & & \cdot & & & \cdot \\ \cdot & & & \cdot & & & \cdot \\ \cdot & & & \cdot & & & \cdot \\ 0, & 0, & \ldots & \binom{2h}{1}, & \binom{2h}{2}, & \ldots & \binom{2h}{2h-1} \end{vmatrix}.$$

Es ist evident, dass die Matrix (4) desgleichen höchstens vom Range $m+n-3$ ist. Und zwar, addieren wir eine Kolonne (resp. Zeile) $K_1$ mit dem $a$-fachen einer beliebigen Kolonne (resp. Zeile) $K_2$, so ist die neue Matrix von demselben Range, wie die vorige. Denn nehmen wir eine beliebige Unterdeterminante $(r+1)$-ten Grades, wo $r$ der Rang der ersten Matrix ist, so ist die Unterdeterminante im Falle, wenn in ihr die Kolonne $K_1+aK_2$ nicht repräsentiert ist, offenbar $=0$. Ist aber $K_1+aK_2$ repräsentiert, so kann man $U=U_1+aU_2$ setzen, wo $U_1$ und $U_2$ Unterdeterminanten, welche aus der Zerlegung der Kolonne $K_1+aK_2$ entspringen. Es ist evident, dass $U_1=U_2=0$ und demnach auch $U=0$ ist. Offenbar ist die Determinante (4) der Determinante (1) gleich und jede Unterdeterminante $(2h-2)$-ten Grades von (1) ist zugleich einer Unterdeterminante $(4h-3)$-ten Grades von (4) gleich und ebenso muss sie $=0$ sein. Ist also die zyklische Determinante (1) durch $\pi^2$ nicht teilbar oder ist mindestens eine Unterdeterminante $(2h-2)$-ten Grades von (1) durch $\pi$ nicht teilbar, so muss in der Gleichung (2) eine Zahl z. B. x durch $\pi$ teilbar sein. Somit muss auch $p|x$ sein, denn andernfalls wird dem Furtwänglerschen Satze gemäss (s. Satz 1)

$$\pi^p \equiv \pi \pmod{p^2}$$

sein, was unmöglich ist, da

$$\pi^p \equiv 1 \not\equiv \pi \pmod{p^2}$$

ist.

**Anmerkung:** Bei W e n d t [14]) ist die zyklische Determinante nur durch $p$ teilbar. Ferner werden bei W e n d t die Minoren nicht berück-





sichtigt. Bei ihm tritt die Voraussetzung $(h, p)=1$ (welche in der Praxis, z. B. beim Beweise der Fermatschen Vermutung für $p<7000$ keinen Einfluss hat) nicht hervor. Ausserdem muss bei W e n d t gleichzeitig verifiziert werden, ob gleichzeitung

$$\Delta_{2h} \equiv p^{2h}-1 \equiv 0 \pmod{\pi},$$

wo $\Delta_{2h}$ die folgende äusserst komplizierte zyklische Determinante ist:

$$\Delta_{2h} = \begin{vmatrix} \binom{2h}{1}, & \binom{2h}{2}, \ldots & \binom{2h}{2h-1}, & 2-p^{2h(p-1)} \\ \binom{2h}{2}, & \binom{2h}{3}, \ldots 2-p^{2h(p-1)}, & & \binom{2h}{1} \\ \cdot & \cdot & \cdot & \cdot \\ 2-p^{2h(p-1)}, & \binom{2h}{1}, \ldots & \binom{2h}{2h-1}, & \binom{2h}{2h-1} \end{vmatrix}.$$

Dadurch kann man z. B. für alle $p<4000$ unmittelbar und ziemlich schnell, mittels der Primzahlentafeln, den ersten Teil der Fermatschen Vermutung beweisen.

Es ist zu beachten, dass es (wie wir in einer anderen Arbeit beweisen wollen) genügt zu verifizieren, ob die zwei ersten Hauptminoren der zyklischen Determinante (1), d. h. die Unterdeterminanten, welche aus (1) entstehen, indem man die $j$ ersten Zeilen und $j$ ersten Kolonnen streicht, durch $p$ teilbar seien. Und zwar sind dann (im Falle, wenn diese zwei Minoren durch $p$ teilbar sind) alle Minoren $(2h-2)$-ten Grades durch $p$ teilbar.

Nun ist es jetzt leicht (gemäss Hilfssatz 10), das Bachmannsche Kriterium zu widerlegen und den folgenden Satz aufzustellen:

**Folgerung:** *Für jede Primzahl $p \geq 7$ ist die zyklische Determinante*

$$(1)\qquad \begin{vmatrix} 1, & \binom{p-1}{1}, & \binom{p-1}{2}, \ldots & \binom{p-1}{p-2} \\ \binom{p-1}{1}, & \binom{p-1}{2}, & \binom{p-2}{3}, \ldots & 1 \\ \cdot & \cdot & \cdot & \cdot \\ \binom{p-1}{p-2}, & 1, & \binom{p-1}{1}, \ldots & \binom{p-1}{p-3} \end{vmatrix}$$

*durch $p^8$ teilbar.*

**Beweis.** Die zyklische Determinante (1) ist (s. Satz 12, (3) und (4)) der Resultante der Polynome

$$f(t)=t^{p-1}-1 \quad \text{und} \quad f_1(t)=(t+1)^{p-1}-1$$

gleich. Offenbar ist:

$$R(f, f_1) = R(f^{(1)}, f_1^{(1)})\, R(f^{(1)}, f_1^{(2)})\, R(f^{(2)}, f_1^{(1)})\, R(f^{(2)}, f_1^{(2)}),$$

wo

$$f^{(1)} = t^{\frac{p-1}{2}} - 1, \quad f^{(2)} = t^{\frac{p-1}{2}} + 1; \quad f_1^{(1)} = (t+1)^{\frac{p-1}{2}} - 1; \quad f_1^{(2)} = (t+1)^{\frac{p-1}{2}} + 1,$$

und $R(f^{(i)}, f^{(j)})$ die entsprechende Resultante bezeichnet. Da für $p \geqslant 7$ für mindestens zwei quadratische Reste, resp. Nichtreste, ein Rest oder Nichtrest nachfolgt [17]), so haben die Polynome

$$(f^{(i)}(t), \quad f_1^{(j)}(t) \quad i = 1,2; \quad j = 1,2,$$

(mod $p$) mindestens zwei gemeinsame Wurzeln. Dem Hilfssatze 11 gemäss ist demnach, jeder Faktor der rechten Seite von (2), durch $p^2$ teilbar.

**Anmerkung:** Bachmann [18]) S. 57—9 hat bewiesen, dass im Falle, wenn $x^p + y^p + z^p = 0$ in ganzen, durch die Primzahl $p$ nicht teilbaren Zahlen lösbar ist, die zyklische Determinante (1) durch $p^3$ teilbar sein muss.

---


**Streszczenie.**

W niniejszej pracy staramy się teorję wielkiego zagadnienia Fermata, stworzoną przez Furtwänglera, Kummera, Mirimanoffa i Kapferera, zastosować do ogólnego równania $x^n + y^n = c z^n$. W ten sposób teorja zagadnienia Fermata wychodzi z ram teorji odosobnionego zagadnienia i staje się podstawą teorji wyższych stopni.

W końcu I-ej części dowodzimy, że równanie $x^p + y^p + z^p = 0$ dla $p = 6857$ jest niemożliwe w liczbach całkowitych niepodzielnych przez $p$, z czego wynika, że pierwsza część wielkiego zagadnienia Fermata jest udowodniona dla wszystkich wykładników $< 7000$.

W II-ej części między innemi tak dalece uproszczamy teorję Wendta, że skomplikowane uzupełnienia do niej podane przez L. Dicksona stają się zbyteczne i jest ona bezpośrednio w praktyce stosowalna.

W końcu obalamy kryterjum Bachmanna rozwiązalności pierwszej części wielkiego zagadnienia Fermata.


---

[17]) s. z. B. E. Cahen: Theorie des nombres II (1924) S. 102—4.

[18]) a. a. O.



# Sur une démonstration du théorème de M. Borel concernant les probabilités dénombrables

**(O pewnym dowodzie twierdzenia Borela, dotyczącego prawdopodobieństw przeliczalnych.)**


Par

Stanisław Ruziewicz


M. Emile Borel a démontré le théorème suivant concernant les probabilités dénombrables [1]):

$n(\gamma)$ désignant le nombre de chiffres égaux à $\gamma$ parmi les $n$ premiers chiffres du développement du nombre $x$ à base $g$, on a pour tous les $x$ réels sauf pour les nombres $x$ formant un ensemble de mesure lebesguienne nulle, l'égalité

$$\lim_{n \to \infty} \frac{n(\gamma)}{n} = \frac{1}{g}.$$

Le but de la présente Note est démontrer comment on peut déduire ce théorème du théorème connu de M, H. Lebesgue d'après lequel toute fonction monotone a une dérivée finie partout, sauf peut être aux points formant un ensemble de mesure lebesguienne nulle,

Il suffit évidemment de prouver que pour tout nombre positif $\alpha < \frac{1}{2}$ l'ensemble $E$ de tous les nombres de l'intervalle (0,1) pour lesquels on a pour un chiffre $\gamma$ de la base $g$ ($g \geqslant 2$)

---

[1]) *Les probabilités dénombrables et leurs applications arithmétiques.* Rend. Circ. Mat. Palermo XXVII, 1° sem. 1909, pp. 247—271.