Über die Kongruenz axe + bye + cze ... 0 (mod. p).

Hurwitz, A.

in: Journal für die reine und angewandte Mathematik - 136 | Periodical
21 page(s) (272 - 292)

Über die Kongruenz $ax^e+by^e+cz^e\equiv 0 \pmod{p}$.

Von Herrn *A. Hurwitz* in Zürich.

Es liegt nahe, zu versuchen, den Beweis des „großen“ *Fermat*schen Satzes von der Unmöglichkeit der Gleichung

$$x^e+y^e+z^e=0$$

dadurch zu führen, daß man die Existenz von unendlichvielen Primzahlen p nachweist, für welche die Kongruenz

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

nicht anders bestehen kann, als wenn eine der Zahlen x, y, z durch p teilbar ist. Herr *Dickson* hat nun im Bd. 135 dieses Journals mit Hilfe der Theorie der Kreisteilung gezeigt, daß dieser Weg ungangbar ist, daß nämlich die erwähnte Kongruenz, sobald p eine gewisse Grenze überschritten hat, stets Lösungen zuläßt, für welche keine der drei Zahlen x, y, z durch p teilbar ist.

Ich will nun in den folgenden Zeilen den allgemeineren Satz beweisen:

Es seien a, b, c ganze von Null verschiedene Zahlen, e eine ungerade Primzahl. Dann besitzt die Kongruenz

$$(1.)\qquad ax^e+by^e+cz^e\equiv 0 \pmod{p}$$

für jede Primzahl p, die eine gewisse Grenze übersteigt, eine solche Lösung, für welche keine der drei Zahlen x, y, z durch p teilbar ist.

Dabei werde ich den Beweis dieses Satzes mit ganz elementaren zahlentheoretischen Hilfsmitteln führen und z. B. von der Theorie der Kreisteilung keinen Gebrauch machen.

§ 1.

Sehr einfach gestaltet sich die Diskussion der Kongruenz (1.), wenn die Primzahl e kein Teiler von $p-1$, also zu $p-1$ teilerfremd ist. Man kann dann nämlich die positiven ganzen Zahlen r und s so bestimmen, daß

$$re = s(p-1)+1$$

wird, worauf für jede ganze Zahl ξ die Kongruenz

$$\xi \equiv \xi^{1+s(p-1)} \equiv (\xi^r)^e \qquad (\mathrm{mod.}\ p)$$

gilt. Da nun die Kongruenz

$$a\xi + b\eta + c\zeta \equiv 0 \qquad (\mathrm{mod.}\ p)$$

offenbar durch ganze, durch p nicht teilbare Zahlen ξ, η, ζ befriedigt werden kann, so wird die Kongruenz (1.) ebenfalls durch drei zu p teilerfremde Zahlen x, y, z, nämlich

$$x = \xi^r,\ y = \eta^r,\ z = \zeta^r$$

befriedigt werden können.

Es bleibt demnach nur zu beweisen, daß unter denjenigen Primzahlen p, für welche

$$(2.) \qquad p-1 = ef,$$

für die also $p-1$ durch e teilbar ist, sich nur endlichviele befinden können, für welche die Kongruenz (1.) nicht anders bestehen kann, als wenn wenigstens eine der Zahlen x, y, z durch p teilbar ist.

§ 2.

Bevor ich dieses beweise, will ich einige Bezeichnungen erklären, deren ich mich dabei bedienen werde.

Bedeutet n eine ganze Zahl, die positiv, negativ oder Null sein darf, so setze ich

$$\varphi(n) = 1 \text{ oder } = 0, \tag{3.}$$

je nachdem n durch p teilbar ist oder nicht. Diese zahlentheoretische Funktion $\varphi(n)$ gestattet es, in sehr bequemer Weise die Anzahl der Lösungen von Kongruenzen nach dem Modul p auszudrücken. Beispielsweise wird die Anzahl der Lösungen der Kongruenz (1.)

$$\mathfrak{A} = \sum_{x,y,z} \varphi(ax^e + by^e + cz^e) \tag{4.}$$

sein, wobei die Summationsbuchstaben x, y, z je ein vollständiges System zu p teilerfremder Reste durchlaufen müssen. Dabei habe ich nur solche Lösungen gezählt, bei welchen die drei Zahlen x, y, z nicht durch p teilbar sind, und zwei Lösungen (x, y, z) und (x', y', z') dann und nur dann als nicht verschieden angesehen, wenn $x' \equiv x$, $y' \equiv y$, $z' \equiv z \pmod{p}$ ist. Der zu beweisende Satz besagt nichts anderes, als daß

$$\mathfrak{A} > 0 \tag{5.}$$

ist, falls die Primzahl $p = ef + 1$ eine gewisse Grenze überschritten hat.

Aus der Bedeutung von $\varphi(n)$ geht unmittelbar hervor, daß

$$\varphi(kn) = \varphi(n) \text{ und } \varphi(pn) = 1 \tag{6.}$$

ist, unter n eine beliebige ganze Zahl, unter k eine durch p nicht teilbare ganze Zahl verstanden.

Ich erweitere ferner den Begriff der Kongruenz der Zahlen auf Zahlsysteme. Zwei Systeme

$$(t_1, t_2, \dots t_r),\ (t_1', t_2', \dots t_r')$$

von je r ganzen Zahlen will ich nämlich nach der positiven ganzen Zahl m als Modul kongruent nennen, in Zeichen

$$(7.) \qquad (t_1, t_2, \dots t_r) \equiv (t_1', t_2', \dots t_r') \pmod{m},$$

wenn die r Kongruenzen

$$(8.) \qquad t_1 \equiv t_1',\ t_2 \equiv t_2',\ \dots\ t_r \equiv t_r' \pmod{m}$$

erfüllt sind. Die eine Kongruenz (7.) bedeutet also nichts anderes als die r Kongruenzen (8.). Von den Zahlsystemen

$$(9.) \qquad (t_1', t_2', \dots t_r'),\ (t_1'', t_2'', \dots t_r''), \dots (t_1^{(s)}, t_2^{(s)}, \dots t_r^{(s)})$$

sage ich, daß sie ein vollständiges System inkongruenter Zahlsysteme (mod. m) bilden, wenn jedes beliebig gewählte Zahlsystem $(t_1, t_2, \dots t_r)$ einem und nur einem der Zahlsysteme (9.) nach dem Modul m kongruent ist, wenn also die Kongruenz

$$(t_1, t_2, \dots t_r) \equiv (t_1^{(i)}, t_2^{(i)}, \dots t_r^{(i)}) \pmod{m}$$

für einen und nur einen Index i besteht.

Durchläuft jede der Zahlen $t_1, t_2, \dots t_r$ unabhängig von den anderen die Glieder eines Restsystems (mod. m), so entstehen im ganzen m^r Zahlsysteme $(t_1, t_2, \dots t_r)$, die offenbar ein vollständiges System (9.) bilden. Hieraus ergibt sich leicht der Satz:

„*Die s Zahlsysteme* (9.) *werden stets und nur dann ein vollständiges System inkongruenter Zahlsysteme (mod. m) bilden, wenn ihre Anzahl $s = m^r$ ist und unter ihnen keine zwei (mod. m) kongruente vorhanden sind.*“

Eine spezielle Folgerung aus diesem Satz ist diese:

Durchläuft das Zahlsystem $(t_1, t_2, \dots t_r)$ ein vollständiges System inkongruenter Zahlsysteme (mod. m), so gilt das nämliche von dem Zahlsysteme $(t_1 + t_r, t_2 + t_r, \dots t_{r-1} + t_r, t_r)$.

§ 3.

Es sei nun g eine Primitivwurzel der Primzahl

$$p = ef + 1,$$

so daß die Potenzen

$$g^0 = 1, g, g^2, \ldots g^{p-2}$$

ein vollständiges System durch p nicht teilbarer Reste (mod. p) bilden.

Diejenigen, in endlicher Anzahl vorhandenen Primzahlen p, welche in einer der Zahlen a, b, c aufgehen, schließe ich von der weiteren Betrachtung aus, so daß

$$(10.) \qquad a \equiv g^\alpha, \; b \equiv g^\beta, \; c \equiv g^\gamma \qquad (\text{mod. } p)$$

gesetzt werden kann.

Die Anzahl $\mathfrak{A}$ der Lösungen der Kongruenz (1.) drückt sich dann nach (4.) in der Form

$$(11.) \qquad \mathfrak{A} = \sum_{\xi, \eta, \zeta} \varphi(g^{e\xi+\alpha} + g^{e\eta+\beta} + g^{e\zeta+\gamma})$$

aus, wobei die Summationsbuchstaben ξ, η, ζ je ein vollständiges Restsystem (mod. $p-1$) durchlaufen müssen. Nun durchläuft

$$\xi = r_1 f + r$$

ein solches Restsystem, wenn r_1 ein vollständiges Restsystem (mod. e) und r ein solches (mod. f) durchläuft. Denn es entstehen auf diese Weise $ef = p-1$ Zahlen ξ, die untereinander (mod. $p-1$) inkongruent sind. Entsprechend kann man

$$\eta = s_1 f + s, \; \zeta = t_1 f + t$$

setzen. Da nun

$$g^{ef}=g^{p-1}\equiv 1 \qquad (\text{mod. } p),$$

so geht durch diese Substitutionen die Gleichung (11.) in

$$(12.) \qquad \mathfrak{A}=e^3 \sum_{r,s,t} \varphi\,(g^{er+\alpha}+g^{es+\beta}+g^{et+\gamma})$$

über, wobei nun die Summationsbuchstaben r, s, t je ein vollständiges Restsystem (mod. f) durchlaufen müssen. Da das Argument von φ sich (mod. p) nicht ändert, wenn r, s, t durch ihnen bezüglich (mod. f) kongruente Zahlen ersetzt werden, so darf die Summation in (12.) allgemeiner über irgendein vollständiges System (mod. f) inkongruenter Zahlentripel (r,s,t) erstreckt werden.

Es sei nun

$$(13.) \qquad [\alpha, \beta, \gamma]=\frac{1}{f}\sum_{r,s,t} \varphi\,(g^{er+\alpha}+g^{es+\beta}+g^{et+\gamma}),$$

so daß die Gleichung (12.) in

$$(14.) \qquad \mathfrak{A}=e^3 f[\alpha, \beta, \gamma]=(p-1)e^2[\alpha, \beta, \gamma]$$

übergeht. Die Definition des Symboles $[\alpha, \beta, \gamma]$ verallgemeinere ich sogleich durch die Festsetzung, daß für r beliebige ganze Zahlen

$$\alpha_1, \alpha_2, \ldots \alpha_r$$

das Symbol $[\alpha_1, \alpha_2, \ldots \alpha_r]$ die Bedeutung

$$(15.) \qquad [\alpha_1, \alpha_2, \ldots \alpha_r]=\frac{1}{f}\sum \varphi\,(g^{et_1+\alpha_1}+g^{et_2+\alpha_2}+\cdots+g^{et_r+\alpha_r})$$

haben soll, wobei die Summation über ein vollständiges System (mod. f) inkongruenter Zahlsysteme $(t_1, t_2, \ldots t_r)$ zu erstrecken ist. Hiernach bezeichnet offenbar

$$[\alpha_1, \alpha_2, \ldots \alpha_r]$$

den f-ten Teil der Anzahl derjenigen Glieder $(t_1, t_2, \ldots t_r)$ eines solchen vollständigen Systemes, für welche die Kongruenz

$$(16.) \qquad g^{et_1+\alpha_1} + g^{et_2+\alpha_2} + \cdots + g^{et_r+\alpha_r} \equiv 0 \pmod{p}$$

erfüllt ist.

In den Fällen $r = 1$ und $r = 2$ ist es leicht, den Wert des Symbols (15.) anzugeben. Da nämlich die Kongruenz

$$g^{et+\alpha} \equiv 0 \pmod{p}$$

niemals erfüllt ist, wird

$$(17.) \qquad [\alpha] = 0$$

sein. Ferner wird die Kongruenz

$$g^{et_1+\alpha_1} + g^{et_2+\alpha_2} \equiv 0 \pmod{p}$$

dann und nur dann erfüllt sein, wenn

$$(18.) \qquad et_1 + \alpha_1 \equiv et_2 + \alpha_2 + \frac{p-1}{2} \pmod{p-1}$$

ist. Da e ungerade ist, so wird $\frac{p-1}{2} = \frac{ef}{2}$ durch e teilbar (also f eine gerade Zahl) sein und die vorstehende Kongruenz erfordert

$$\alpha_1 \equiv \alpha_2 \pmod{e}$$

Ist letztere Bedingung erfüllt, so wird jedem Werte von t_2 eine (mod. f) bestimmte Zahl t_1 entsprechen, die der Kongruenz (18.) genügt. Hieraus folgt nun (wenn noch α, β statt α_1, α_2 geschrieben wird):

Man hat

$$[\alpha, \beta] = 1 \text{ oder } = 0, \tag{19.}$$

je nachdem die beiden Zahlen α, β *nach dem Modul* e *kongruent oder inkongruent sind.*

§ 4.

Die Zahlen $[\alpha_1, \alpha_2, \dots \alpha_r]$ besitzen eine Reihe von Eigenschaften, zu deren Ableitung ich mich jetzt wende.

1. *Der Wert von* $[\alpha_1, \alpha_2, \dots \alpha_r]$ *hängt in symmetrischer Weise von den Zahlen* $\alpha_1, \alpha_2, \dots \alpha_r$ *ab, ändert sich also nicht, wenn diese Zahlen irgendeiner Permutation unterworfen werden.*

2. *Sind die Zahlsysteme* $(\alpha_1, \alpha_2, \dots \alpha_r)$ *und* $(\beta_1, \beta_2, \dots \beta_r)$ *kongruent (mod. e), d. h. ist*

$$\alpha_1 \equiv \beta_1, \alpha_2 \equiv \beta_2, \dots \alpha_r \equiv \beta_r \pmod{e},$$

so gilt

$$[\alpha_1, \alpha_2, \dots \alpha_r] = [\beta_1, \beta_2, \dots \beta_r]. \tag{20.}$$

In der Tat darf man in der Summe (15.) die Summationsbuchstaben $t_1, t_2, \dots t_r$ bez. ersetzen durch $t_1 + k_1, t_2 + k_2, \dots t_r + k_r$, unter $k_1, k_2, \dots k_r$ beliebig gewählte ganze Zahlen verstanden. Dies kommt aber darauf hinaus, die Zahlen $\alpha_1, \alpha_2, \dots \alpha_r$ durch die ihnen bez. (mod. e) kongruenten Zahlen $\alpha_1 + k_1 e, \alpha_2 + k_2 e, \dots \alpha_r + k_r e$ zu ersetzen.

3. *Bezeichnet* α *eine beliebige ganze Zahl, so ist*

$$[\alpha_1 + \alpha, \alpha_2 + \alpha, \dots \alpha_r + \alpha] = [\alpha_1, \alpha_2, \dots \alpha_r]. \tag{21.}$$

Denn die Summe (15.) ändert nicht ihren Wert, wenn man das Argument von φ mit der zu p teilerfremden Zahl g^α multipliziert.

Nimmt man $\alpha = -\alpha_r$, so folgt aus (21.)

$$[\alpha_1, \alpha_2, \dots \alpha_{r-1}, \alpha_r] = [\alpha_1 - \alpha_r, \alpha_2 - \alpha_r, \dots \alpha_{r-1} - \alpha_r, 0]. \tag{22.}$$

4. *Die Zahl* $[\alpha_1, \alpha_2, \ldots \alpha_r]$ *gibt an, wie viele (mod. f) inkongruente Zahlsysteme* $(t_1, t_2, \ldots t_{r-1})$ *die Kongruenz*

$$(23.) \quad g^{t_1 e + \alpha_1} + g^{t_2 e + \alpha_2} + \cdots + g^{t_{r-1} e + \alpha_{r-1}} + g^{\alpha_r} \equiv 0 \pmod{p}$$

befriedigen.

Nach der Bemerkung am Schluß von § 3 darf man nämlich in der Summe (15.) $t_1, t_2, \ldots t_{r-1}, t_r$ ersetzen durch $t_1 + t_r, t_2 + t_r, \ldots t_{r-1} + t_r, t_r$. Dadurch kommt

$$[\alpha_1, \alpha_2, \ldots \alpha_r] = \frac{1}{f} \Sigma \varphi (g^{e t_r} (g^{e t_1 + \alpha_1} + g^{e t_2 + \alpha_2} + \cdots + g^{e t_{r-1} + \alpha_{r-1}} + g^{\alpha_r}))$$

$$= \Sigma \varphi (g^{e t_1 + \alpha_1} + g^{e t_2 + \alpha_2} + \cdots + g^{e t_{r-1} + \alpha_{r-1}} + g^{\alpha_r}),$$

wo nun die Summation über ein vollständiges System (mod. f) inkongruenter Zahlsysteme $(t_1, t_2, \ldots t_{r-1})$ auszudehnen ist. Diese Darstellung von $[\alpha_1, \alpha_2, \ldots \alpha_r]$ beweist die aufgestellte Behauptung. Beiläufig folgt, daß die Zahlen $[\alpha_1, \alpha_2, \ldots \alpha_r]$ nicht negative ganze Zahlen sind.

5. *Die Zahl* $[\alpha_1, \alpha_2, \ldots \alpha_r]$ *gibt auch an, wie viele (mod. f) inkongruente Zahlsysteme* $(t_1, t_2, \ldots t_{r-1})$ *die Kongruenz*

$$(24.) \quad g^{t_1 e + \alpha_1} + g^{t_2 e + \alpha_2} + \cdots + g^{t_{r-1} e + \alpha_{r-1}} \equiv g^{\alpha_r} \pmod{p}$$

befriedigen.

Nach dem vorhergehenden Satze ist nämlich die in Rede stehende Anzahl von Zahlsystemen $(t_1, t_2, \ldots t_{r-1})$ gleich $\left[\alpha_1, \alpha_2, \ldots \alpha_{r-1}, \alpha_r + \frac{p-1}{2}\right]$, weil

$$g^{\alpha_r + \frac{p-1}{2}} \equiv -g^{\alpha_r} \pmod{p}$$

ist. Da aber $\frac{p-1}{2} = \frac{ef}{2}$ ein Multiplum von e ist, so wird nach (2.)

$$\left[\alpha_1, \alpha_2, \ldots \alpha_{r-1}, \alpha_r + \frac{p-1}{2}\right] = [\alpha_1, \alpha_2, \ldots \alpha_r].$$

6. *Es seien*

$$\alpha_1, \alpha_2, \ldots \alpha_r, \beta_1, \beta_2, \ldots \beta_s$$

$r+s$ *beliebige ganze Zahlen. Dann gilt die Gleichung*

$$(25.)\quad [\alpha_1, \alpha_2, \ldots \alpha_r,\ \beta_1, \beta_2, \ldots \beta_s] = f[\alpha_1, \alpha_2, \ldots \alpha_r][\beta_1, \beta_2, \ldots \beta_s] + \sum_{\varrho} [\alpha_1, \alpha_2, \ldots \alpha_r, \varrho][\beta_1, \beta_2, \ldots \beta_s, \varrho],$$

wobei der Summationsbuchstabe ϱ *ein vollständiges Restsystem (mod.* e*) zu durchlaufen hat.*

Um den Beweis hierfür zu erbringen, zerlege ich die

$$f[\alpha_1, \alpha_2, \ldots \alpha_r, \beta_1, \beta_2, \ldots \beta_s]$$

Lösungssysteme $(t_1, t_2, \ldots t_r, u_1, u_2, \ldots u_s)$ der Kongruenz

$$g^{t_1 e + \alpha_1} + \cdots + g^{t_r e + \alpha_r} + g^{u_1 e + \beta_1} + \cdots + g^{u_s e + \beta_s} \equiv 0 \pmod{p}$$

in p Gruppen, indem ich ein Lösungssystem in die erste, oder zweite,... oder p-te Gruppe rechne, je nachdem für dasselbe

$$g^{t_1 e + \alpha_1} + \cdots + g^{t_r e + \alpha_r} \equiv 0 \text{ oder } \equiv g^0, \ldots \text{ oder } \equiv g^{p-2} \pmod{p}$$

ist. Für die Lösungssysteme innerhalb derselben Gruppe ist dann bezüglich

$$g^{u_1 e + \beta_1} + \cdots + g^{u_s e + \beta_s} \equiv 0 \text{ oder } \equiv -g^0, \ldots \text{ oder } \equiv -g^{p-2} \pmod{p}.$$

In Rücksicht auf die Sätze 4 und 5 finde ich so:

$$f[\alpha_1, \alpha_2, \ldots \alpha_r, \beta_1, \beta_2, \ldots \beta_s] = f^2[\alpha_1, \ldots \alpha_r][\beta_1, \ldots \beta_s] + \sum_{\lambda} [\alpha_1, \alpha_2, \ldots \alpha_r, \lambda][\beta_1, \beta_2, \ldots \beta_s, \lambda],$$

wo λ ein Restsystem (mod. $p-1$) durchläuft. Nun setze ich

$$\lambda = te + \varrho$$

und lasse t ein Restsystem (mod. f) und ϱ ein Restsystem (mod. e) durchlaufen. Dann geht die vorstehende Gleichung nach Division durch f in die zu erweisende Gleichung (25.) über. Diese Gleichung gibt übrigens, wenn $r=1$ oder $s=1$ ist, vermöge der Relationen (19.) eine nichtssagende Identität. Der erste Fall, welcher Interesse bietet, entspricht daher der Annahme $r=s=2$. In diesem Falle lautet die Gleichung (25.), wenn die Zahlen β_1, β_2 jetzt durch α_3, α_4 bez. bezeichnet werden:

$$(26.)\quad [\alpha_1, \alpha_2, \alpha_3, \alpha_4] = f[\alpha_1, \alpha_2][\alpha_3, \alpha_4] + [\alpha_1, \alpha_2, 0][\alpha_3, \alpha_4, 0]$$
$$+ [\alpha_1, \alpha_2, 1][\alpha_2, \alpha_3, 1] + \cdots + [\alpha_1, \alpha_2, e-1][\alpha_3, \alpha_4, e-1].$$

Vermöge dieser Gleichung werden die „viergliedrigen" Zahlen $[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ durch „dreigliedrige" dargestellt. (Die Werte der zweigliedrigen Zahlen $[\alpha_1, \alpha_2]$ und $[\alpha_3, \alpha_4]$ sind nach Gleichung (19.) bekannt.) Offenbar kann man mit Hilfe der Gleichung (25.) überhaupt alle Zahlen

$$[\alpha_1, \alpha_2, \ldots \alpha_r]$$

für $r \geqq 4$ durch die dreigliedrigen Zahlen ausdrücken.

7. *Es seien wieder*

$$\alpha_1, \alpha_2, \ldots \alpha_r, \beta_1, \beta_2, \ldots \beta_s$$

irgend $r+s$ *ganze Zahlen, und es durchlaufe* ϱ *ein Restsystem nach dem Modul* e. *Dann gilt die folgende Gleichung:*

$$(27.)\quad \sum_{\varrho} [\alpha_1 + \varrho, \alpha_2 + \varrho, \ldots \alpha_r + \varrho, \beta_1, \beta_2, \ldots \beta_s]$$
$$= (p-1)\,[\alpha_1, \ldots \alpha_r]\,[\beta_1, \ldots \beta_s] + (f^{r-1} - [\alpha_1, \ldots \alpha_r])\,(f^{s-1} - [\beta_1, \ldots \beta_s]).$$

Bezeichnet S die auf der linken Seite stehende Summe, so ist nach Satz (4.)

$$S = \Sigma\varphi\,(g^{t_1 e + \alpha_1 + \varrho} + \cdots + g^{t_r e + \alpha_r + \varrho} + g^{u_1 e + \beta_1} + \cdots + g^{u_{s-1} e + \beta_{s-1}} + g^{\beta_s}),$$

wobei die Summation über $t_1, t_2, \ldots t_r, u_1, \ldots u_{s-1}, \varrho$ auszudehnen ist. Ich ersetze nun, was offenbar erlaubt ist, $t_1, t_2, \ldots t_{r-1}$ bez. durch $t_1 + t_r$, $t_2 + t_r, \ldots t_{r-1} + t_r$. Dadurch kommt

$$S = \Sigma\varphi\,(\lambda A + B),$$

wobei

$$\lambda = g^{t_r e + \varrho},\ A = g^{t_1 e + \alpha_1} + \cdots + g^{t_{r-1} e + \alpha_{r-1}} + g^{\alpha_r},$$
$$B = g^{u_1 e + \beta_1} + \cdots + g^{u_{s-1} e + \beta_{s-1}} + g^{\beta_s}$$

gesetzt ist. Durchläuft nun t_r ein Restsystem (mod. f) und ϱ ein Restsystem (mod. e), so durchläuft $t_r e + \varrho$ ein Restsystem (mod. $ef = p-1$) und folglich λ ein vollständiges System durch p nicht teilbarer Reste (mod. p). Die Summe S läßt sich demnach so bilden, daß man λ ein solches Restsystem (mod. p) (also z. B. die Zahlen $1, 2, \ldots p-1$) und $t_1, t_2, \ldots t_{r-1}$, $u_1, \ldots u_{s-1}$ je ein vollständiges Restsystem (mod. f) durchlaufen läßt.

Nun wird für eine bestimmte Kombination $t_1, \ldots t_{r-1}, u_1, \ldots u_{s-1}$

$$\lambda A + B$$

durch p teilbar sein

a) für alle $p-1$ Werte von λ, wenn

$$A \equiv 0,\ B \equiv 0 \pmod{p};$$

b) für einen der $p-1$ Werte von λ, wenn

$$A \not\equiv 0,\ B \not\equiv 0 \pmod{p};$$

c) für keinen der $p-1$ Werte von λ in jedem anderen Falle.

Der Fall a) tritt für

$$[\alpha_1, \alpha_2, \ldots \alpha_r]\,[\beta_1, \beta_2, \ldots \beta_s]$$

Kombinationen $t_1, \ldots t_{r-1}, u_1, \ldots u_{s-1}$ ein, der Fall b) für

$$(f^{r-1} - [\alpha_1, \alpha_2, \ldots \alpha_r])\,(f^{s-1} - [\beta_1, \beta_2, \ldots \beta_s])$$

Kombination $t_1, \ldots t_{r-1}, u_1, \ldots u_{s-1}$. Demnach ist

$$S = (p-1)[\alpha_1, \alpha_2, \ldots \alpha_r][\beta_1, \beta_2, \ldots \beta_s] + (f^{r-1} - [\alpha_1, \alpha_2, \ldots \alpha_r])\,(f^{s-1} - [\beta_1, \beta_2, \ldots \beta_s]),$$

w. z. b. w.

In den Fällen $r = 1$ und $r = 2$ nimmt die Gleichung (27.) mit Berücksichtigung von (17.) und (19.) folgende Formen an:

$$(28.) \qquad \sum_{\varrho=0}^{e-1} [\alpha_1 + \varrho, \beta_1, \ldots \beta_s] = f^{s-1} - [\beta_1, \ldots \beta_s],$$

$$(29.) \qquad \sum_{\varrho=0}^{e-1} [\alpha_1 + \varrho, \alpha_2 + \varrho, \beta_1, \ldots \beta_s] = \begin{cases} f(f^{s-1} - [\beta_1, \ldots \beta_s]), \\ \qquad \text{wenn } \alpha_1 \not\equiv \alpha_2 \pmod{e}, \\ (f-1) f^{s-1} + (p-f)[\beta_1, \ldots \beta_s], \\ \qquad \text{wenn } \alpha_1 \equiv \alpha_2 \pmod{e}. \end{cases}$$

§ 5.

Unter n und m irgend zwei ganze Zahlen verstanden, betrachte ich nun die Summe

$$(30.) \qquad a_{n,m} = \sum_{\varrho} [\varrho, m + n\varrho, 0],$$

in welcher ϱ ein Restsystem (mod. e) (also z. B. die Zahlen $0, 1, 2, \ldots e-1$) durchlaufen soll.

Der Wert von $a_{n,m}$ ist eine nicht negative ganze Zahl und ändert sich offenbar nicht, wenn n und m durch ihnen bez. (mod. e) kongruente Zahlen ersetzt werden.

Überdies gilt noch die Gleichung

$$(31.) \qquad a_{n,m} = a_{1-n,m}.$$

In der Tat ist nach Gleichung (21.)

$$a_{n,m} = \Sigma[0, m+n\varrho-\varrho, -\varrho] = \Sigma[-\varrho, m+n\varrho-\varrho, 0],$$

und die letztere Summe geht, wenn man ϱ durch $-\varrho$ ersetzt, in $a_{1-n,m}$ über.

Der Wert von $a_{0,m}$ ergibt sich sofort aus Gleichung (28.), indem man in ihr $s=2$ und $\alpha_1=0, \beta_1=m, \beta_2=0$ setzt. Man findet so

$$(32.) \qquad a_{0,m} = a_{1,m} = f-[m,0] = \begin{cases} f, & \text{wenn } m \not\equiv 0 \pmod{e}, \\ f-1, & \text{wenn } m \equiv 0 \pmod{e}. \end{cases}$$

Zwischen den Zahlen $a_{n,m}$ herrschen nun merkwürdige quadratische Relationen, die sich auf folgende Weise ergeben:

Es sei

$$(33.) \qquad s_{n,m} = \sum_{\varrho} a_{n,\varrho}\, a_{n,\varrho+m},$$

wo ϱ ein Restsystem (mod. e) durchlaufen soll. Setzt man nun gemäß (30.)

$$a_{n,\varrho} = \sum_{\sigma}[\sigma, \varrho+n\sigma, 0],$$

$$a_{n,\varrho+m} = \sum_{\tau}[\tau, \varrho+m+n\tau, 0],$$

so kommt

$$(34.) \qquad s_{n,m} = \sum_{\varrho,\sigma,\tau}[\sigma, \varrho+n\sigma, 0][\tau, \varrho+m+n\tau, 0],$$

wo die Summationsbuchstaben ϱ, σ, τ je ein Restsystem (mod. e) zu durchlaufen haben.

Beachtet man nun, daß (nach § 4, Satz 1 und 3)

$$[\sigma, \varrho + n\sigma, 0][\tau, \varrho + m + n\tau, 0] = [\sigma - n\sigma, \varrho, -n\sigma][\tau - m - n\tau, \varrho, -m - n\tau]$$
$$= [\sigma - n\sigma, -n\sigma, \varrho][\tau - m - n\tau, -m - n\tau, \varrho]$$

ist, so erkennt man, daß die Summation nach ϱ vermöge der Gleichung (26.) ausgeführt werden kann. Man hat in dieser Gleichung $\alpha_1 = \sigma - n\sigma$, $\alpha_2 = -n\sigma$, $\alpha_3 = \tau - m - n\tau$, $\alpha_4 = -m - n\tau$ zu nehmen.

Da hierbei $[\alpha_1, \alpha_2] = [\sigma, 0]$, $[\alpha_3, \alpha_4] = [\tau, 0]$ wird, so geht die Gleichung (34.) über in

$$s_{n,m} = \sum_{\sigma,\tau} \{[\sigma - n\sigma, -n\sigma, \tau - m - n\tau, -m - n\tau] - f[\sigma, 0][\tau, 0]\}$$

oder, unter Anwendung der Gleichungen (19.) und (21.):

$$s_{n,m} = \sum_{\sigma,\tau} [\sigma, 0, \tau + n(\sigma - \tau) - m, n(\sigma - \tau) - m] - f.$$

Die Summation kann hier so ausgeführt werden, daß man (σ, τ) ein vollständiges System inkongruenter Zahlenpaare (mod. e) durchlaufen läßt. Daher darf man auch τ durch $\sigma - \tau$ ersetzen, denn gleichzeitig mit (σ, τ) durchläuft auch $(\sigma, \sigma - \tau)$ ein solches vollständiges System von Zahlenpaaren.

Somit ist

$$s_{n,m} = \sum_{\varrho,\tau} [\sigma, 0, \sigma - \tau + n\tau - m, n\tau - m] - f.$$

Hier findet nun bei der Summation nach σ die Gleichung (27.) Anwendung, in welcher $r = s = 2$ und

$$\alpha_1 = -\tau + n\tau - m, \quad \alpha_2 = 0, \quad \beta_1 = n\tau - m, \quad \beta_2 = 0$$

zu nehmen ist. So findet sich weiter

$$s_{n,m} = \sum_{\tau} \{(p-1)[(n-1)\tau - m, 0][n\tau - m, 0] + (f - [(n-1)\tau - m, 0])(f - [n\tau - m, 0])\} - f.$$

Jetzt nehme ich an, daß n weder $\equiv 0$ noch $\equiv 1 \pmod{e}$ sei. Dann wird im allgemeinen

$$[n\tau - m, 0] = [(n-1)\tau - m, 0] = 0,$$

und nur für *einen* Wert von τ, nämlich für denjenigen, welcher die Kongruenz $n\tau - m \equiv 0 \pmod{e}$ befriedigt,

$$[n\tau - m, 0] = 1,$$

und ebenfalls nur für *einen* Wert von τ, nämlich für denjenigen, welcher die Kongruenz $(n-1)\tau - m \equiv 0 \pmod{e}$ befriedigt,

$$[(n-1)\tau - m, 0] = 1$$

sein. Diese beiden besonderen Werte von τ sind voneinander verschieden, wenn m nicht $\equiv 0 \pmod{e}$ ist, dagegen fallen sie zusammen, wenn $m \equiv 0 \pmod{e}$ ist.

Demnach ergibt sich für die Summe $s_{n,m}$, falls m nicht durch e teilbar ist,

$$s_{n,m} = (e-2)f^2 + 2f(f-1) - f = (ef-3)f = (p-4)f;$$

dagegen kommt, falls m durch e teilbar ist,

$$s_{n,m} = (p-1) + (f-1)^2 + (e-1)f^2 - f = (p-4)f + p.$$

Es gilt demnach der folgende Satz:

Zwischen den Zahlen $a_{n,m}$, *die durch Gleichung* (30.) *definiert werden, bestehen die quadratischen Relationen:*

$$(35.) \qquad a_{n,0}\, a_{n,m} + a_{n,1}\, a_{n,m+1} + \cdots + a_{n,e-1}\, a_{n,m+e-1} = (p-4)f,$$

$$(36.) \qquad a_{n,0}^2 + a_{n,1}^2 + \cdots + a_{n,e-1}^2 = (p-4)f + p.$$

Dabei wird vorausgesetzt, daß weder n *noch* $n-1$ *durch* e *teilbar ist und daß die in der Relation* (35.) *auftretende Zahl* m *ebenfalls nicht durch* e *teilbar ist.*

Aus den Relationen (35.) und (36.) folgt unmittelbar die weitere

$$(37.) \qquad (a_{n,0} - a_{n,m})^2 + (a_{n,1} - a_{n,m+1})^2 + \cdots + (a_{n,e-1} - a_{n,m+e-1})^2 = 2p,$$

in welcher n und m nur der Bedingung unterliegen, daß n, m, $n-1$ durch e nicht teilbar sein dürfen. Die Zahlen $a_{n,m}$ ergeben also eine gewisse Anzahl von Darstellungen der Zahl $2p$ als Summe von e Quadraten.

Schließlich bemerke ich noch, daß für jeden Index n die Gleichung besteht

$$(38.) \qquad a_{n,0} + a_{n,1} + \cdots + a_{n,e-1} = p-2.$$

In der Tat ist nach (30.) und (28.)

$$\sum_{\varrho=0}^{e-1} a_{n,\varrho} = \sum_{\varrho,\sigma} [\sigma, \varrho + n\sigma, 0] = \sum_{\sigma} |f - [\sigma, 0]| = ef - 1 = p-2.$$

§ 6.

Bezeichne jetzt r einen bestimmten Index. Die Zahl $a_{n,r}$ kommt dann auf der linken Seite der Relation (37.) in den beiden Gliedern

$$(a_{n,r} - a_{n,r+m})^2, \quad (a_{n,r-m} - a_{n,r})^2$$

vor. Es ist aber

$$(a_{n,r} - a_{n,r+m})^2 + (a_{n,r-m} - a_{n,r})^2 = 2\left\{\left(a_{n,r} - \frac{a_{n,r+m} + a_{n,r-m}}{2}\right)^2 + \left(\frac{a_{n,r+m} - a_{n,r-m}}{2}\right)^2\right\}.$$

Die Relation (37.) kann ich daher so schreiben:

$$\left(a_{n,r} - \frac{a_{n,r+m} + a_{n,r-m}}{2}\right)^2 + P = p,$$

wo P eine Summe von nicht negativen Termen bezeichnet; ja es muß sogar $P > 0$ (nicht $= 0$) sein weil p als Primzahl keinem Quadrat gleich sein kann.

Es folgt hieraus, daß $a_{n,r} - \frac{a_{n,r+m} + a_{n,r-m}}{2}$ absolut genommen kleiner als $\sqrt{p}$ ist; d. h.:

Ist n weder $\equiv 0$ *noch* $\equiv 1$ *(mod. e), ferner m nicht* $\equiv 0$ *(mod. e), r aber beliebig, so gilt die Beziehung*

$$(39.) \qquad -\sqrt{p} < a_{n,r} - \frac{a_{n,r+m} + a_{n,r-m}}{2} < \sqrt{p}.$$

Hier setze ich der Reihe nach $m = 1, 2, \ldots e-1$ und summiere die $e-1$ dadurch entstehenden Beziehungen. Da nach (38.)

$$\sum_{m=1}^{e-1} \frac{a_{n,r+m} + a_{n,r-m}}{2} = \sum_{m=0}^{e-1} \frac{a_{n,r+m} + a_{n,r-m}}{2} - a_{n,r} = \frac{1}{2}\left(\sum_{\varrho=0}^{e-1} a_{n,\varrho} + \sum_{\varrho=0}^{e-1} a_{n,\varrho}\right) - a_{n,r}$$

$$= p - 2 - a_{n,r}$$

ist, so kommt

$$(40.) \qquad -(e-1)\sqrt{p} < e a_{n,r} - (p-2) < (e-1)\sqrt{p},$$

oder:

Ist n weder $\equiv 0$, *noch* $\equiv 1$ *(mod. e), r aber beliebig, so gilt die Beziehung*

$$(41.) \qquad (p-2) - (e-1)\sqrt{p} < e a_{n,r} < (p-2) + (e-1)\sqrt{p}.$$

§ 7.

Aus den Zahlen $a_{n,m}$ lassen sich nun die Zahlen $[\alpha, \beta, \gamma]$ zusammensetzen, wodurch es möglich wird, die Beziehung (41.) auf die letzteren

Zahlen zu übertragen. Durchläuft n ein Restsystem (mod. e), so ist zufolge der Definitionsgleichung (30.)

$$\sum_n a_{n,\,\alpha-n\beta} = \sum_{\varrho,n} [\varrho,\ \alpha-n\beta+n\varrho,\ 0].$$

Summiert man zunächst über n bei festgehaltenem ϱ, so ist zu unterscheiden, ob $\varrho \equiv \beta \pmod{e}$ ist, oder nicht. Im ersteren Falle ist beständig

$$\alpha-n\beta+n\varrho \equiv \alpha \pmod{e},$$

während im zweiten Falle $\alpha-n\beta+n\varrho = \sigma$ gleichzeitig mit n ein Restsystem (mod. e) durchläuft. Demnach kommt

$$\sum_n a_{n,\,\alpha-n\beta} = e[\beta,\ \alpha,\ 0] + \sum_\varrho{}' \sum_\sigma [\varrho,\ \sigma,\ 0],$$

wo das Komma am Summenzeichen bedeutet, daß ϱ ein Restsystem (mod. e) mit Ausschluß des Restes $\varrho \equiv \beta \pmod{e}$ durchlaufen soll.

Nach Gleichung (28.) ist nun

$$\sum_\sigma [\varrho,\ \sigma,\ 0] = f-[\varrho,\ 0]$$

und offenbar

$$\sum_\varrho{}' \{f-[\varrho,\ 0]\} = (e-1)f+[\beta,\ 0]-1 = p-2-f+[\beta,\ 0].$$

Hiernach wird jetzt

$$\sum_n a_{n,\,\alpha-n\beta} = e[\beta,\ \alpha,\ 0]+p-2-f+[\beta,\ 0].$$

Von der Summe trenne ich die $n=0$ und $n=1$ entsprechenden Glieder ab, deren Werte nach (32.)

$$a_{0,\,\alpha} = f-[\alpha,\ 0],\quad a_{1,\,\alpha-\beta} = f-[\alpha-\beta,\ 0] = f-[\alpha,\ \beta]$$

sind. Auf diese Weise kommt:

$$\sum_{n=2}^{e-1} a_{n,\,\alpha-n\beta} + 3f - (p-2) - [\alpha, 0] - [\alpha, \beta] - [\beta, 0] = e[\beta, \alpha, 0].$$

Schließlich setze ich noch $\alpha-\gamma$ für α und $\beta-\gamma$ für β und finde so:

Die Zahl $[\alpha, \beta, \gamma]$ *läßt sich durch die Zahlen* $a_{n,m}$ *ausdrücken vermöge der Gleichung*

$$(42.) \quad e[\alpha, \beta, \gamma] = 3f + 2 - p - [\alpha, \beta] - [\beta, \gamma] - [\gamma, \alpha] + \sum_{n=2}^{e-1} a_{n,\,\alpha-\gamma+n(\beta-\gamma)}.$$

Hier bedeuten α, β, γ drei beliebige ganze Zahlen, und nach (19.) ist

$$[\alpha, \beta] + [\beta, \gamma] + [\gamma, \alpha] = 0 \text{ oder } 1 \text{ oder } 3,$$

je nachdem α, β, γ untereinander inkongruent (mod. e), oder zwei unter diesen Zahlen einander kongruent (mod. e) oder endlich alle drei einander kongruent (mod. e) sind.

Die Beziehung (41.) liefert nun für die in (42.) auftretende Summe die Grenzen

$$\frac{e-2}{e}[(p-2) \mp (e-1)\sqrt{p}],$$

und da

$$e(3f + 2 - p) = 3(p-1) - e(p-2)$$

ist, so ergibt sich der Satz:

Für die Zahl $[\alpha, \beta, \gamma]$ *gilt die Beziehung*

$$(43.) \quad p + 1 - (e-1)(e-2)\sqrt{p} - \eta e < e^2[\alpha, \beta, \gamma] < p + 1 + (e-1)(e-2)\sqrt{p} - \eta e,$$

wobei

$$\eta = [\alpha, \beta] + [\beta, \gamma] + [\gamma, \alpha]$$

gleich** 0 **oder** 1 **oder** 3 **ist, je nachdem die drei Zahlen** α, β, γ **untereinander inkongruent (mod. e), oder zwei unter diesen Zahlen einander kongruent (mod. e) oder alle drei einander kongruent (mod. e) sind.

Für die Anzahl $\mathfrak{A}$ der Lösungen der Kongruenz

$$ax^e + by^e + cz^e \equiv 0 \pmod{p}$$

in durch p nicht teilbaren Zahlen x, y, z folgt insbesondere nach (14.)

$$\frac{\mathfrak{A}}{p-1} > p + 1 - (e-1)(e-2)\sqrt{p} - \eta e$$

und daher

$$\mathfrak{A} > 0,$$

sobald die Primzahl p eine gewisse von e abhängende Grenze überschritten hat.

Die Beziehung (43.) zeigt des näheren, daß die Anzahl $\mathfrak{A}$ mit p derart ins Unendliche wächst, daß

$$\operatorname{Lim} \frac{\mathfrak{A}}{p^2} = 1$$

ist.