Neue Beweismethoden für einen Doppelsatz der Theorie der Potenzreste, sowie über die Erweiterung des Congruenzbegriffes.

Von

FRITZ HOFMANN in München.

Nach Gauss' disqu. ar. 81 hat man: „Wenn p eine Primzahl, so ist die Summe aller primitiven Wurzeln der Congruenz $x^{p-1} \equiv 1 \pmod{p}$ entweder $\equiv 0 \pmod{p}$ — wenn nämlich $p - 1$ durch ein Quadrat theilbar ist —; oder $\equiv (-1)^n \pmod{p}$ — wenn $p - 1$ ein Product aus n verschiedenen Factoren ist.“

Für diesen Satz sollen im Folgenden neue Beweismethoden mitgetheilt werden, bei deren Formulirung eine kaum noch verwendete Darstellung der Folge jener $p - 1$ Reste, die einer Primzahl p durch Potenzirung einer ihrer primitiven Wurzeln zugeordnet werden, gute Dienste leisten wird.

Da diese Reste, nachdem sie alle Werthe von 1 bis $p - 1$ durchlaufen haben, bei Fortsetzung des Potenzirens über die $(p - 1)^{\text{te}}$ Potenz hinaus in derselben Reihenfolge wiederkehren, so liegt der Gedanke nahe, dieselben auf der Peripherie eines Kreises zu verzeichnen, wie es aus den beifolgenden Figuren ersichtlich ist.*)

Ist es nun möglich mehrere Punkte der so eingetheilten Peripherie zu regelmässigen Polygonen zu vereinigen, mit einer Ecke bei dem Reste 1, so berühren solche Polygone die Wurzeln einer Congruenzgleichung von der Form $x^\alpha \equiv 1 \pmod{p}$, wo α ein Theiler von $p - 1$.

In den beigegebenen Figuren sind nicht alle möglichen geschlossenen Polygone dieser Art eingezeichnet, sondern nur sovieler als $p - 1$ Primfactoren besitzt — und zwar zeigen jene Polygone, wenn $p - 1 = a^\alpha b^\beta \dots l^\lambda$, die Centriwinkel resp. $\frac{360^\circ \cdot a}{p - 1}$, $\frac{360^\circ \cdot b}{p - 1}$, $\dots$, $\frac{360^\circ \cdot l}{p - 1}$.

*) Schon Poinso't weist übrigens an einer Stelle (p. 178) seines „Mémoire sur l'application de l'algèbre à la théorie des nombres (mém. de l'acad. des sc., t. IV)“ auf die Nothwendigkeit hin sich die Vorstellung von den verwickelten Beziehungen der Potenzreste durch Auftragen derselben auf einer Peripherie zu erleichtern.

Mit andern Worten, die Seiten der eingeschriebenen Polygone überspringen resp. $(a-1)$, $(b-1)$, $\dots$, $(l-1)$ Punkte der Eintheilung um die Verbindung zweier Ecken herzustellen.

Die von solchen eingeschriebenen regulären Polygonen ausgeschiedenen Reste geben als Wurzeln einer binomischen Gleichung immer eine Summe $\equiv 0 \pmod{p}$, und zwar bis zum Polygon der Gleichung $x^2 \equiv 1 \pmod{p}$ herab (Zweieck 1,22 in Figur d), während allerdings der Fall $x^1 \equiv 1 \pmod{p}$, der auf die einzige Wurzel $x \equiv 1$ führen würde, auszuschliessen ist.

Die *Drehung* eines Polygons lässt seine Ecken mit neuen Resten zusammenfallen — da jene Drehung aber äquivalent ist einer *Multiplication* der sämtlichen ausgeschiedenen Reste mit einer und derselben Zahl, so ist auch für die neue Lage des Polygons die Summe der berührten Reste $\equiv 0 \pmod{p}$. Ein zweiter Beweis hierfür findet sich am Schlusse des Aufsatzes.

Beispiel. In die Figur a kann man ein reguläres Sechseck einschreiben, welches die Reste 3, 16, 13, 28, 15, 18 verbindet. Und

Figur a.

in der That findet sich $3 + 16 + 13 + 28 + 15 + 18 \equiv 0 \pmod{31}$, denn jene Zahlen sind resp. $\equiv 3 \cdot (1)$, $3 \cdot (26)$, $3 \cdot (25)$, $3 \cdot (30)$, $3 \cdot (5)$, $3 \cdot (6) \pmod{31}$; d. h. ihre Summe ist congruent $\pmod{31}$ der 3-fachen Summe der Wurzeln der Gleichung $x^6 \equiv 1 \pmod{31}$, welche Wurzelsumme $\equiv 0 \pmod{31}$. —

Mit Hülfe des bis jetzt bemerkten kann bereits der erste Theil des Satzes von Gauss erledigt werden:

I. Lehrsatz. „Ist $p-1$ durch ein Quadrat theilbar, so ist die

Summe der primitiven Wurzeln der Gleichung $x^{p-1} \equiv 1 \pmod{p}$ durch p theilbar“.

Erster Beweis. Ist $p - 1 = a^\alpha b^\beta \dots l^\lambda$, wo wenigstens einer der Exponenten $\alpha, \beta, \dots, \lambda$, z. B. $\alpha, > 1$, so giebt es eine kleinere Zahl als $p - 1$ selbst, nämlich die Zahl $a^{\alpha-1} b^\beta \dots l^\lambda$, in welcher alle

Figur a'.

Primfactoren von $p - 1$ enthalten sind: bildet man die regulären Polygone von den Centriwinkeln $\frac{360^\circ \cdot a}{p-1}, \frac{360^\circ \cdot b}{p-1}, \dots, \frac{360^\circ \cdot l}{p-1}$, so vereinigen sich die Peripherien dieser Polygone bereits vor dem Zurückkommen in den gemeinschaftlichen Ausgangspunkt „Rest 1“ in einem bestimmten Punkte, der sich nun in Bezug auf die Figur des Kreises mit den eingezeichneten Polygonen genau verhält, wie der Punkt „Rest 1“.

Daher können sämtliche von den Polygonen berührten Reste wiederum unter sich zu regulären geschlossenen Polygonen vom Centriwinkel $\frac{360^\circ}{p-1} a^{\alpha-1} b^\beta \dots l^\lambda$ verbunden werden, demnach auch die *nicht berührten* Reste (die *primitiven* Wurzeln der Gleichung $x^{p-1} \equiv 1 \pmod{p}$) — letztere ergeben daher nach dem oben Gesagten eine Summe $\equiv 0 \pmod{p}$.

Beispiel. (Fig. b, siehe folgende Seite). Schon beim Reste 27 vereinigen sich die Peripherien der beiden von 1 ausgehenden Polygone wieder.

Man kann daher die Figur des Kreises mit den beiden eingezeichneten Polygonen durch eine Drehung um $\frac{360^\circ}{36} \cdot 6$ mit sich selbst zur Deckung bringen — demnach müssen sich die nicht berührten Reste

zu geschlossenen Sechsecken vereinigen lassen, deren Eckensumme immer einzeln $\equiv 0 \pmod{37}$. In der That hat man:

Figur b.

$$2 + 17 + 15 + 35 + 20 + 42 \equiv 0 \pmod{37},$$

$$32 + 13 + 18 + 5 + 24 + 19 \equiv 0 \pmod{37}.$$

Zweiter Beweis. Indem wir uns nochmals daran erinnern, dass bei der bis jetzt gemachten Voraussetzung der Punkt des Restes 1 noch nicht dadurch ausgezeichnet ist, dass in ihm mehr Polygone als in irgend einem andern Punkte der Eintheilung zusammenlaufen, sondern dass sich noch immer wenigstens *ein* andrer Punkt finden muss, der die vollständige Anzahl der von 1 ausgehenden Peripherien auch in sich vereinigt aufzuweisen hat, können wir dem Obigen eine etwas verschiedene Fassung geben.

Wir denken uns, dass wir die Summe der berührten Reste dadurch zu ermitteln suchten, dass wir in die Figur des eingetheilten Kreises nach einander die n auf die n Primfactoren von $p - 1$ bezüglichen (primären) Polygone legten, deren jedes Reste ausscheidet, deren Summe für jedes Polygon je $\equiv 0 \pmod{p}$.

Wollten wir hieraus die Summe der uneigentlichen Wurzeln von p ohne Weiteres $\equiv 0 \pmod{p}$, annehmen, so hätten wir — möglicherweise — einen Fehler gemacht durch Nichtberücksichtigung des Umstandes, dass von der eben vollzogenen Operation des Einschreibens der n Polygone einige Reste mehrfach betroffen und demnach mehr-

mals gezählt wurden, während sie sich doch in der vorliegenden Figur nur je einmal vorfinden.

Demnach ist eine Correctur des Resultates vorzunehmen, die sich zunächst auf jene Punkte erstrecken wird, die von *wenigstens zwei* jener primären Polygone berührt werden.

Ueber solche Punkte lassen sich aber wieder reguläre geschlossene — secundäre — Polygone mit den Centriwinkeln $\frac{360^\circ}{p-1} \cdot ab, \frac{360^\circ}{p-1} \cdot ac, \frac{360^\circ}{p-1} \cdot bc \dots$ legen, welche allerdings ihrerseits wieder einige Punkte mehrfach berühren können. Mit Ausserachtlassung des in den letzten Worten erwähnten Umstandes, der uns alle „wenigstens dreifachen“ Punkte der primären Figur als zu einer sie gleichmässig treffenden, durch Ueberlegung zu ermittelnden und später noch zu berücksichtigenden Verbesserung Anlass gebend erkennen lässt, ergibt sich demnach jene zunächst als nothwendig erkannte Correctur von der Grösse $\equiv 0 \pmod{p}$.

Das nunmehrige Resultat ist nun noch zu corrigiren mit Berücksichtigung jener Punkte, in welchen *wenigstens drei* Peripherien der ursprünglich gegebenen n Polygone sich vereinigen — welche Punkte aber wieder zu regelmässigen, geschlossenen, eigentlichen Polygonen sich verbinden lassen (Centriwinkel beispielsweise $= \frac{360^\circ}{p-1} \cdot abc$).

Und so kann man weiter gehen, ohne befürchten zu müssen, dass jemals das uneigentliche Polygon der einzigen Ecke 1 bei dieser Betrachtungsweise auftritt, das dann allerdings nicht mehr die Summe $\equiv 0$, sondern $\equiv 1$ ergeben würde.

So sind also fortwährend neue Correcturen des ursprünglichen Resultates 0 über einander gelagert zu denken, die aber alle als in der Vereinigung der Eckpunkte geschlossener Polygone bestehend, dasselbe nicht verändern.

Um zu wiederholen: die Existenz eines jeden weitem Polygon-systems höherer Ordnung führt eine neue Verbesserung des Resultates herbei, in welche aber immer nur die sämmtlichen Eckpunkte regulärer Polygone durch Multiplication mit einer für das betreffende System für alle Punkte gleichen, durch Abzählen zu ermittelnden Grösse eingehen. Der Werth der Correctur f für jedes System ist für diesen ersten Theil des Satzes noch ohne Bedeutung; im Folgenden wird er dagegen das Hauptziel unserer Ueberlegung zu bilden haben.

Beispiel. (Fig. c, siehe folgende Seite). Hier wurden, da

$$60 = 2^2 \cdot 3 \cdot 5,$$

3 primäre Polygone übereinandergelegt, deren Eckensumme einzeln $\equiv 0 \pmod{61}$; dabei sind nun jene Punkte als zu einer Verbesserung Anlass gebend zu berücksichtigen, die von *wenigstens zweien* solcher

Polygone berührt werden; dieselben lassen sich aber vereinigen zu drei Polygonen von den Centriwinkeln $\frac{360^\circ}{60} \cdot 6$, $\frac{360^\circ}{60} \cdot 10$, $\frac{360^\circ}{60} \cdot 15$.

Demnach ändert die Berücksichtigung der Punkte, in welchen *wenigstens zwei* Peripherien sich vereinigen, noch nichts am Resultat $\equiv 0$ der ersten Addition.

Wir bemerken schliesslich noch, dass Punkte vorhanden sind, in welchen mehrere jener secundären Polygone zusammentreffen, nämlich die Reste 1 und 60. Dies erfordert allerdings eine letzte Verbesserung,

Figur c.

in welche aber die beiden Reste 1 und 60 gleichmässig durch Multiplication mit einer uns nicht weiter beschäftigenden corrigirenden Grösse f eingehen; das Resultat $\equiv 0$ ändert sich daher um $f \cdot (1 + 60)$, bleibt also dem Werthe 0 congruent (mod. 61).

II. Lehrsatz. „Ist $p - 1 = abc \dots l$, ein Product von n linearen verschiedenen Factoren, dann ist $(-1)^n \equiv$ der Summe der primitiven Wurzeln der Gleichung $x^{p-1} \equiv 1 \pmod{p}$, $\pmod{p}$.“

Erster Beweis. Wir arbeiten besser auf die Summe der uneigentlichen Wurzeln hin, die mit s bezeichnet sein möge.

Wir denken uns wieder, dass wir die Summe der uneigentlichen Wurzeln dadurch zu ermitteln suchten, dass wir in die Figur des Kreises mit seinen $(p - 1)$ Punkten die sämtlichen auf die Primfactoren $abc \dots l$ bezüglichen n Polygone von den Centriwinkeln resp. $= \frac{360^\circ}{p-1} \cdot a$, $\frac{360^\circ}{p-1} \cdot b$, $\dots$, $\frac{360^\circ}{p-1} \cdot l$ legten.

Jedes solche Polygon scheidet Reste aus, deren Summe $\equiv 0 \pmod{p}$.

Diesen Werth benutzen wir als erste Annäherung für s .

Wir scheiden dann zunächst jene Punkte aus, in welchen wenigstens 2 Polygone sich wieder vereinigen, diese Punkte liegen wiederum ihrerseits auf Polygonen vereinigt von den Centriwinkeln $\frac{360^\circ}{p-1} \cdot ab$, $\frac{360^\circ}{p-1} \cdot ac$, $\frac{360^\circ}{p-1} \cdot bc \dots$

Bei jedem solchen Punkte wurde die dazu gehörige Restzahl doppelt gezählt; es ist daher ihr Betrag einmal abzuziehen, um das ursprüngliche Resultat 0 zu verbessern.

Nach Ausführung dieser zunächst als nothwendig erkannten Verbesserung haben wir demnach $s \equiv 0 - \binom{n}{2} \cdot 0 \pmod{p}$.

Für Punkte, welche wenigstens 3 Peripherien vereinigt zeigen, wird man folgenden Schluss machen: Sie wurden vor Allem $\binom{3}{1}$ mal bei der Abzählung der Ecken der primären Polygone berücksichtigt, ferner subtractiv $\binom{3}{2}$ mal bei der Aufstellung der secundären Polygone.

Nun ist aber $\binom{3}{1} - \binom{3}{2} = 0$. Man hat daher der Existenz eines jeden solchen wenigstens-dreifachen Punktes nach Multiplication mit $+1$ durch Addition zum bisher gefundenen Resultate zur Geltung zu verhelfen — da er ja bis jetzt eben durch die letzte $\binom{3}{2}$ malige Subtraction in seiner Wirkung auf das Gesamtergebnis ganz verschwand.

Man hat demnach als weitere Annäherung zu setzen:

$$s \equiv 0 - \binom{n}{2} \cdot 1 \cdot 0 + \binom{n}{3} \cdot 1 \cdot 0 \pmod{p}.$$

Dieses letzte 0 folgt aus dem Umstande, dass die wenigstens-dreifachen Punkte sich wieder zu — tertiären — Polygonen vom Centriwinkel $\frac{360^\circ}{p-1} \cdot abc, \dots$ zusammenschliessen.

Die wenigstens-vierfachen Punkte wurden bei der ersten Addition $\binom{4}{1}$ mal berücksichtigt, sie wurden dann $\binom{4}{2}$ mal nach Aufindung der secundären Polygone durch Subtraction in Rechnung gebracht; da sie aber auch durch $\binom{4}{3}$ maliges Zusammentreffen eines Vereins von je 3 Peripherien ausgezeichnet sind, wurde dieses letzte Resultat (nach der Subtraction) schliesslich noch durch Addition vom $\binom{4}{3}$ fachen Werthe des Restes für jeden solchen Punkt verbessert — während er doch im Endresultate unserer Ueberlegung als einfacher

Punkt figuriren soll. Es ist aber $\binom{4}{1} - \binom{4}{2} + \binom{4}{3} = 2$; daher sind, so lange noch wenigstens-vierfache Punkte vorhanden, die zugehörigen Reste *einmal* abzuziehen, um eine weitere Annäherung an die unbekannte Summe s zu liefern.

Man hätte demnach $s \equiv 0 - \binom{n}{2} \cdot 1 \cdot 0 + \binom{n}{3} \cdot 1 \cdot 0 - \binom{n}{4} \cdot 1 \cdot 0$ (mod. p) als letzte Näherung.

So kann man weitergehen, bis man zu dem vom Punkte 1 dargestellten, uneigentlichen Polygone gelangt, dessen Eckensumme dann allerdings nicht mehr $\equiv 0$, sondern $\equiv 1$ zu nehmen wäre.

Und zwar sind die Schlüsse für das System μ^{ter} Ordnung (der wenigstens μ fachen Punkte) die folgenden:

Diese Punkte wurden bedacht bei der Aufstellung der primären, secundären . . . Polygone; sie wurden von Anfang an, wo sie μ fach gezählt wurden, bei der Aufstellung jedes höhern Systems in Mitleiden-

Figur d.

schaft gezogen, indem jeder bei einem solchen Punkte stehende Rest *abwechselnd* mit $+1$ oder -1 multiplicirt dem Resultat zugefügt wurde; nun vereinigen sich in einem wenigstens- μ fachen Punkte $\binom{\mu}{1}$ Polygone des ersten, $\binom{\mu}{2}$ des 2. Systems und so fort — statt den Punkt mit $+1$ multiplicirt in die Berechnung des Endresultats eingeführt zu sehen, finden wir ihn multiplicirt mit

$$\binom{\mu}{1} - \binom{\mu}{2} + \binom{\mu}{3} - \dots - \binom{\mu}{\mu-1} (-1)^{\mu-1} = 1 + (-1)^{\mu}.$$

Nach Auffindung des μ^{ten} Systems hat man also das bis dorthin gefundene Resultat zu verbessern durch Subtraction von $(-1)^{\mu} \cdot \binom{n}{\mu} \cdot k$, wo k die Summe der von einem Polygon μ^{ter} Ordnung berührten Reste bedeutet. Dieses k wird für alle $\mu < n$ zu 0, da man dann eigentliche

(wenigstens-zweieckige) Polygone vor sich hat. Für $\mu = n$ dagegen wird $k = 1$ und man hat demnach endgültig:

$$s \equiv \binom{n}{1} \cdot 0 - \binom{n}{2} \cdot 0 + \binom{n}{3} \cdot 0 - \dots - (-1)^n \cdot 1 \\ \equiv (-1)^{n+1} \pmod{p}.$$

Dies ist der Satz von Gauss; es ergibt sich nämlich aus obiger Beziehung die Summe der eigentlichen Wurzeln $\equiv (-1)^n \pmod{p}$.

Zweite Beweismethode. Auch die Betrachtung solcher (Rumpf-) Polygone, bei welchen die Ecke 1 fehlt, für welche also die Eckensumme $\equiv (-1) \pmod{p}$, führt zum Ziele.

Wir denken uns die Figur der berührten (nicht primitiven) Reste dadurch entstanden, dass wir zunächst n solche unvollständige Polygone einschrieben, hierauf noch den Rest 1 markirten.

Die wirkliche Summe der durch diese Operation berührten Punkte lässt sich sofort angeben; sie ist mit Anwendung aller der successiven Correcturen $\equiv$

$$\binom{n}{1} \cdot (-1) - \binom{n}{2} \cdot (-1) + \binom{n}{3} \cdot (-1) - \dots + \binom{n}{n-1} \cdot (-1) \cdot (-1)^n,$$

wo wegen der Entstehung der Zahlen (-1) als Eckensumme, sowie wegen der abwechselnden Vorzeichen ohne Weiteres auf die früheren Ueberlegungen verwiesen werden darf. Demnach hat man (nach Hinzufügung des Restes 1)

$$s \equiv 1 - \binom{n}{1} + \binom{n}{2} - \dots + \binom{n}{n-1} (-1)^{n-1} \\ \equiv (-1)^{n+1} \pmod{p}.$$

Beispiel. (Fig.e; siehe folgende Seite). In den Kreis der 42 Punkte wurden 3 primäre Polygone eingezeichnet. Die Summe der von ihnen berührten Punkte ist zunächst, so lange man sich gestattet einen einfach vorhandenen, aber mehrfach berührten Punkt mehrfach mitzuzählen, $\equiv 3 \cdot 0 \pmod{43}$.

Sucht man die Punkte auf, welche wenigstens 2 Peripherien vereinigt zeigen, so erkennt man, dass dieselben wieder auf regulären, geschlossenen Polygonen vertheilt sind; deren Anzahl $= \binom{3}{2} = 3$ und deren Eckensumme je $\equiv 0 \pmod{43}$.

(Es sind das die secundären Polygone

$$1, 4, 16, 21, 41, 35, 11; \quad 1, 6, 36; \quad 1, 42).$$

Wollte man nun setzen $s \equiv 3 \cdot 0 - 3 \cdot 0 \equiv 0 \pmod{43}$, so würde die Nichtberücksichtigung des Umstandes, dass der Punkt 1 noch eine ausgezeichnete Stellung einnimmt, zu einem Fehler Anlass geben.

Dieses 1 wurde von Anfang an 3mal berührt; da es auch von

$\binom{3}{2}$ Polygonen des zweiten Systems berührt wird, so wurde der Restpunkt 1 auch 3mal von der Subtraction der ersten Correctur betroffen. Man hat also, um seine Existenz überhaupt im Resultate zur Geltung gelangen zu lassen, jenes 1 schliesslich wieder zu addiren und erhält $s \equiv 1 \pmod{43}$; daher die Summe der primitiven Wurzeln

$$\equiv (-1) \pmod{43}.$$

Oder: Man denkt sich die 3 primären Rumpfpolygone gelegt, die sich von den oben aufgestellten durch Fehlen der Ecke 1 unterscheiden.

Figur e.

Die Summe der von ihnen berührten Reste ist $\equiv 3 \cdot (-1) \pmod{43}$ — oder mit Berücksichtigung der Existenz von 3 Rumpfpolygonen der zweiten Ordnung $\equiv 3 \cdot (-1) - 3 \cdot (-1) \equiv 0 \pmod{43}$. Schliesslich addirt man noch das 1 hinzu und hat $s \equiv 1 \pmod{43}$.

In der That ist die Summe der primitiven Wurzeln

$$34 + 33 + 3 + 28 + 12 + 26 + 5 + 18 + 20 + 29 + 30 + 19 = 257 = 6 \cdot 43 - 1. —$$

Der Schwerpunkt der bis jetzt angestellten Betrachtungen möge im Nachweis der Nothwendigkeit gefunden werden, die Correcturen, zu denen das Auftreten immer höherer Classen von Combinationen der vorgegebenen Primfactoren Anlass giebt, *abwechselnd im entgegengesetzten Sinne* vorzunehmen.

An dieser Stelle angelangt ist uns ein zusammenfassender Rückblick über die gewonnenen Resultate möglich; derselbe begreift die

beiden Theile des Gauss'schen Satzes in sich. Und zwar stellt sich der von uns gegebene Beweis analytisch formulirt folgendermaassen dar:

„Die primitiven Wurzeln von $x^{p-1} \equiv 1 \pmod{p}$ sind identisch mit den Wurzeln der Congruenz:

$$(1) \quad \frac{(x^{p-1} - 1) \left(x^{\frac{p-1}{ab}} - 1\right) \left(x^{\frac{p-1}{ac}} - 1\right) \dots}{\left(x^{\frac{p-1}{a}} - 1\right) \left(x^{\frac{p-1}{b}} - 1\right) \dots \left(x^{\frac{p-1}{abc}} - 1\right) \dots} \equiv 0 \pmod{p}.$$

Daher ist ihre Summe congruent der Summe der Wurzeln der Congruenzen:

$$x^{p-1} - 1 \equiv 0 \pmod{p}, \quad x^{\frac{p-1}{ab}} - 1 \equiv 0 \pmod{p} \dots$$

vermindert um die Summe der Wurzeln der Congruenzen

$$x^{\frac{p-1}{a}} - 1 \equiv 0 \pmod{p}, \dots, x^{\frac{p-1}{abc}} - 1 \equiv 0 \pmod{p} \dots$$

Unter diesen Congruenzen tritt nur dann die Congruenz

$$x^1 - 1 \equiv 0 \pmod{p}$$

auf, wenn die Primfactoren von $p - 1$ sämmtlich nur im ersten Grade auftreten — dieser Fall lässt $+1$ oder -1 als Resultat erscheinen; andernfalls ist die Wurzelsumme von sämmtlichen obigen Congruenzen $\equiv 0 \pmod{p}$.*)

Die analytische Formulirung (I) unserer geometrischen Betrachtung zeigt vollständige Uebereinstimmung mit der in *Bachmann's Kreistheilung*, p. 16, auf anderem Wege gefundenen Gleichung:

$$F_n(x) = \frac{f(n) \prod f\left(\frac{n}{pp'}\right) \dots}{\prod f\left(\frac{n}{p}\right) \dots \prod f\left(\frac{n}{pp'p''}\right) \dots},$$

in welcher $F_n(x)$ die linke Seite jener Gleichung bezeichnet, welche die primitiven Wurzeln der Gleichung $x^n - 1 = 0$ zu Wurzeln besitzt, während die Ausdrücke $f(n)$ identisch mit $(x^n - 1)$ u. s. w. zu denken sind.

Es sei überhaupt wegen der analytischen Darstellung dieser Verhältnisse auf die 2. und 3. Vorlesung des citirten Werkes, sowie auf das 7. Supplement zu *Dirichlet's Zahlentheorie* II. Auflage verwiesen, wo sich Betrachtungen finden, die mit den uns hier vorliegenden Analogie zeigen, jedoch ohne dass der Nachweis des uns beschäftigenden Satzes ihr Ziel bildete. — Wir sind damit von selbst vom Gebiete der Theorie der Potenzreste auf das der *Kreistheilung* hinübergeleitet worden.

Für die primitiven Wurzeln der Einheit, d. h. der Gleichung

*) Die analytischen Formulirungen dieser Seite verdanken ihre Entstehung der freundlichen Mitarbeiterschaft des Herrn Adolf Hurwitz in Göttingen.

$x^n = 1$ existiren analoge Sätze, für welche die Beschränkung wegfällt, dass $n + 1$ eine Primzahl sein muss. Dieselben lauten:

„Die Summe aller primitiven Wurzeln der Gleichung $x^n = 1$ ist entweder $= 0$; wenn nämlich n durch ein Quadrat theilbar ist; — oder $= (-1)^{\frac{1}{2}}$, — wenn n ein Product aus λ verschiedenen Factoren ist.“

Der Beweis kann sofort auf dem oben verfolgten Wege durchgeführt werden.

Mit Einhaltung des von Gauss bei seinem Beweise benutzten Gedankenganges kann man kürzer so verfahren:

Man hat nach Lipschitz, Lehrbuch der Analysis, § 38, 6:

„Wenn die Zahl n gleich dem Product von Potenzen verschiedener Primzahlen $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_\lambda^{\alpha_\lambda}$ ist, und wenn aus je einer primitiven Wurzel von jeder der Gleichungen $\xi^{a_1^{\alpha_1}} = 1$, $\eta^{a_2^{\alpha_2}} = 1$, $\dots$, $\varrho^{a_\lambda^{\alpha_\lambda}} = 1$ ein Product gebildet wird, so stellen die verschiedenen Producte die verschiedenen primitiven Wurzeln der Gleichung $\omega^n = 1$ dar.“

Demnach kann die Summe der Wurzeln einer solchen Gleichung $x^n = 1$ dargestellt werden als Product von λ algebraischen Summen — wo λ die Anzahl der Primfactoren von n .

Treten die Primfactoren von n alle nur linear auf, so ist eine jede Summe der Art $= -1$, denn dann sind die *sämmtlichen* Wurzeln der Gleichungen $\xi^{a_1} = 1$, $\eta^{a_2} = 1$, $\dots$, $\varrho^{a_\lambda} = 1$ mit Ausschluss von 1 ohne Weiteres auch die *primitiven* Wurzeln dieser Gleichungen, daher die Summe dieser letzteren je $= -1$. Hieraus folgt direct der zweite Theil des oben ausgesprochenen Satzes: $s = (-1)^{\frac{1}{2}}$, wenn n kein Quadrat enthält.

Enthält dagegen n ein Quadrat, d. h. ist einer der Exponenten $\alpha_1 \alpha_2 \dots \alpha_\lambda > 1$, so wird eine von jenen Summen primitiver Wurzeln einer Gleichung niedrigeren Grades zu 0 und lässt also das ganze Product der λ algebraischen Summen, welches die Summe der primitiven Wurzeln von $x^n = 1$ liefert, verschwinden.

Diese letztere Behauptung bedarf noch des Beweises; er wird sich am besten mit Hilfe der bis jetzt benutzten Sprechweise führen lassen:

In jenes Polygon, welches die *sämmtlichen* Wurzelpunkte der Gleichung $x^{a_1^{\alpha_1}} = 1$, $\alpha_1 > 1$, verbindet, lässt sich wiederum ein reguläres, geschlossenes Polygon, das der Wurzelpunkte der Gleichung $x^{a_1^{\alpha_1-1}} = 1$ einschreiben — die von letzterem nicht berührten Punkte des primären Polygons sind dann die *primitiven* Wurzeln der Gleichung $x^{a_1^{\alpha_1}} = 1$.

Hieraus folgt, dass sich jene übrigbleibenden Wurzelpunkte auf $a_1 - 1$ regulären geschlossenen Polygonen anordnen lassen, daher zusammen die Summe 0 ergeben.

Beispiel. Die Wurzeln der Gleichung $x^{27} = 1$ liefern ein primäres Polygon, in welches sich das Polygon der Gleichung $x^9 = 1$ einschreiben lässt; die von letzterem nicht berührten Wurzelpunkte des primären Polygons sind, wenn $e^{\frac{2\pi i}{27} \cdot \varrho}$ mit $[\varrho]$ bezeichnet wird:

$$[1] [2] [4] [5] [7] [8] [10] [11] [13] [14] [16] [17] [19] [20] \\ [22] [23] [25] [26].$$

Sie lassen sich auf 2 Neunecke vertheilen: $[1] [4] \dots [25]$ und $[2] [5] \dots [26]$ und ergeben daher die Summe 0. —

Es sei noch darauf hingewiesen, dass für den Fall wo $n + 1$ eine Primzahl ist, die im Anfang des Artikels erklärte Aufzeichnung der primitiven Wurzeln der Congruenzgleichung $x^n \equiv 1 \pmod{n + 1}$ eine Correspondenz zwischen jenen (ganzzahligen) Resten und den (complexen) Wurzeln der Gleichung $x^n = 1$ darstellt, die man am bequemsten so aussprechen kann:

Bringt man jene Figur zur Deckung mit der Figur der in n Theile getheilten Peripherie des Kreises vom Radius 1, deren Theilpunkte uns in einer z -Ebene die complexen Einheitswurzeln darstellen — wobei der Rest 1 auf die Zahl 1 zu liegen kommt, — so ist jede Einheitswurzel mit dem sie deckenden Reste *congruent* $\pmod{n + 1}$, wobei allerdings die letzte Ausdrucksweise noch eine Rechtfertigung erfordert.

Wenn wir sagen: $17 \equiv e^{\frac{2\pi i}{30} \cdot 7} \pmod{31}$ (Fig. a), so hat das seine Berechtigung darin, dass nach Erheben auf die 30. Potenz in der That $17^{30} \equiv e^{2\pi i \cdot 7} \equiv 1 \pmod{31}$; ebenso setzen wir $25 \equiv e^{\frac{2\pi i}{3} \cdot 10} \pmod{31}$, oder $\equiv e^{\frac{2\pi i}{30} \cdot 10} \pmod{31}$, weil $25^3 \equiv e^{2\pi i} \equiv 1 \pmod{31}$.

[Die Schreibweise $\frac{95}{118} \equiv 204 \pmod{211}$ lässt sich vertheidigen durch die Existenz der Beziehung $95 \equiv 118 \cdot 204 \pmod{211}$].

Diese Zuweisungsart scheint zunächst noch eine Willkürlichkeit zu enthalten, wenn man bemerkt, dass solcher Anordnungsarten der Reste in Bezug auf 31 nicht weniger als $\varphi(30) = 8$ existiren; mit der in der Figur a gebotenen Anordnung ist auch die in Figur a' gegebene vollkommen gleichberechtigt — so kommen demnach bei Anwendung des zweiten Schemas andere Reste mit den Ecken der Figur in der complexen Zahlenebene zur Deckung. (Vergl. Poinso't a. a. O., p. 175).

Trotzdem herrscht ein recht einfaches Gesetz in diesen Dingen: jene Reste, welche in Fig. a von den eingezeichneten regulären, den Punkt 1 enthaltenden Polygonen berührt werden, finden sich am Umfange des gleichen Polygons in der Figur a' wieder: das in a vor-

kommende Dreieck 1, 25, 5 scheidet bei der Uebertragung in die Figur a' dieselben Reste aus.

Man kann also immerhin sagen: dem *Vereine* jener Wurzeln der Gleichung $x^n = 1$, welche einer Gleichung niedrigeren Grades $x^\mu = 1$ genügen, entspricht ein und derselbe unveränderliche *Verein* von Resten, und zwar die Wurzeln der Gleichung $x^\mu \equiv 1 \pmod{n+1}$.

Für die soeben benützte Thatsache, dass bei anderer Wahl der primitiven Wurzel zur Herstellung der Restfolge immer wieder dieselben Zahlen, die in der ursprünglichen Figur auf den Ecken eines regulären die 1 enthaltenden Polygons erschienen waren, die Ecken eines ebensolchen Polygons von gleicher Seitenzahl bilden, könnte man einen Beweis wünschen, der, im Zusammenhange mit der vorliegenden Figur sich der bisher gebrauchten Darstellungsweise bedienend, ein geometrischer zu nennen wäre — wir würden in seinem Verlaufe beispielsweise von „Polygonen mit sich selbst schneidender Peripherie“ zu reden haben.

An Stelle jenes „geometrischen“ Beweises tritt diesmal die Analysis mit einfachen Mitteln ein: das Zusammenhalten des Umstandes, dass eine Congruenzgleichung vom Grade μ höchstens μ Wurzeln hat (*Dirichlet, Zahlentheorie* § 26.) mit dem andern, dass schon von vornherein noch vor Aufstellung der Resttabellen für die Wurzeln einer jeden Gleichung niedern Grades als n die *Stellen* des Wurzelvereins durch ein und dasselbe *feste* reguläre Polygon fixirt sind, führt eben schon den Beweis für die von der Wahl der primitiven Wurzel unabhängige Zusammengehörigkeit jenes Wurzelvereins mit sich.

Dieses Correspondenzprincip ist nicht neu*); es findet sich in Kummer's Abhandlung: Ueber die ... Congruenzwurzeln, *Crelle's J.* Bd. 53, in Poinso't's öfters citirtem *Mémoire*, und ist beispielsweise in *Bachmann, Kreistheilung* zu ausgedehnten Untersuchungen verwendet (pp. 248, 272). Immerhin sei auf den neugewonnenen Gesichtspunkt hingewiesen, unter welchem alle diese Verhältnisse erscheinen — die Bezeichnung „congruent“, ursprünglich der Geometrie entnommen, ohne dass man beabsichtigte sich jemals auf des Wortes eigentliche Bedeutung zu stützen und mit ihrer Hilfe neue Thatsachen abzuleiten, erlangt nun neuen Werth, da ihr die geometrische Bedeutung zurückgegeben ist. —

Uebrigens ist es — trotzdem das man verschiedene primitive Wurzeln zur Bildung unserer Figur zur Verfügung hätte — nicht für jede Primzahl p möglich die primitiven Wurzeln der Gleichung $x^{p-1} = 1$ so zu trennen, dass, wenn eine von der Analysis gelieferte Form einer

*) Schon Gauss selbst verwendete die Bezeichnungen

$$\sqrt[p]{a} \equiv b \pmod{p}, \text{ sowie } \frac{a}{b} \equiv c \pmod{p}.$$

einzelnen Einheitswurzel vorliegt, $e^{\frac{2\pi i}{6}} = \frac{1}{2} + \frac{\sqrt{-3}}{2}$, und man die von jener Form geforderten indirecten Operationen an der Figur der Restzahlen vorzunehmen versucht, das für letztere schliesslich erhaltene Resultat gerade an jener Stelle sich vorfindet, die der gewählten Stelle der Kreistheilung entspricht.

Die Primzahl 7 z. B. liefert zwei gleichberechtigte Anordnungen der 6 Reste:

Die Durchführung der Operationen $\frac{1}{2} + \frac{\sqrt{-3}}{2}$ ergibt in dem einen Falle: $4 + \frac{2}{2} \equiv 5$, welche Zahl nicht an der Stelle von $e^{\frac{2\pi i}{6}}$ auftritt, bei der andern Anordnung aber $4 + \frac{5}{2} \equiv 4 + 6 \equiv 10 \equiv 3$, mit derselben Abweichung.

Man wird sich hier damit zu begnügen haben, jenen Sätzen, die immer nur ganze *Gruppen* von eigentlichen oder uneigentlichen Einheitswurzeln zum Gegenstande haben, solche über die entsprechenden Gruppen der Congruenzwurzeln gegenüberzustellen —: man schliesst

aus $e^{\frac{2\pi i}{6}} + e^{-\frac{2\pi i}{6}} = 1$, und $e^{\frac{2\pi i}{6}} \cdot e^{-\frac{2\pi i}{6}} = 1$, dass $5 + 3 \equiv 1$ und $5 \cdot 3 \equiv 1 \pmod{7}$. —

Unter den 4 möglichen Figuren der Potenzreste für 13 ist die folgende bemerkenswerth, zu deren Bildung die primitive Wurzel 11

verwendet wurde; sie ermöglicht es, die einzelnen eigentlichen und uneigentlichen 12^{ten} Wurzeln der Einheit zu *trennen*, wie das soeben definirt wurde.

Die Berechnung der Wurzel $e^{\frac{2\pi i}{12}} = \frac{\sqrt{3}}{2} + \frac{\sqrt{-1}}{2}$ gestaltet sich wie folgt:

$$\sqrt{3} \equiv 4, \quad \frac{\sqrt{3}}{2} \equiv 2; \quad \frac{\sqrt{-1}}{2} = \frac{\sqrt{12}}{2} \equiv \frac{5}{2} \equiv 9; \quad 2 + 9 \equiv 11.$$

Dieses 11 erscheint an der richtigen Stelle der ersten eigentlichen 12^{ten} Wurzel der Einheit.

Diese Eigenschaft ist von grosser Tragweite. Einem jeden Punkte der complexen Zahlenebene, der durch *rationale* Verbindung der obigen vorgegebenen 12 Wurzelpunkte erreicht werden kann, ist ein bestimmter Rest in Bezug auf 13 zugeordnet — denn jenen rationalen Operationen geht eine *eindeutige* Verbindung der entsprechenden Reste parallel. So erscheint die ganze Zahlenebene mit einem Netze von — theils rationalen, theils irrationalen — Zahlen überdeckt; jedem erreichbaren Punkte ist durch die Operationenfolge, welche ihn bestimmt, ein gewisser Rest eindeutig zugewiesen.

Da diesem Gebilde die *Stetigkeit* fehlt, so scheinen die Grenzen seiner Verwendbarkeit enge gezogen; immerhin möge noch ein *Beispiel* zeigen, wie man nach dem soeben ausgesprochenen Principe operiren kann.

Um zu beweisen, dass die Summe der von den Ecken eines regulären Polygons berührten Potenzreste $\equiv 0$ ist, lege man das Polygon auf die Figur des entsprechenden in den eingetheilten Kreis eingeschriebenen Polygons der z -Ebene; dieses letztere hat als regelmässige Figur seinen Schwerpunkt im Anfangspunkt, wenn man sich auf seine Ecken gleiche Gewichte vertheilt denkt.

Daher ist die Summe der berührten *Einheitswurzel* $= 0$; auch das mit dem Kreistheilungspolygon congruente Polygon der *Potenzreste* hat daher eine Eckensumme $\equiv 0$.

München, Anfang Mai 1882.