Heidelberger Akademie der Wissenschaften

Mathematische Abhandlungen

Autor: **Landau, Edmund** (1877 – 1938)

Titel: **Über einen zahlentheoretischen Satz und seine Anwendung auf die hypergeometrische Reihe**

Sitzungsberichte der Heidelberger Akademie der Wissenschaften, Mathematisch-naturwissenschaftliche Klasse : Abt. A ; 1911, 18
Signatur UB Heidelberg: L 1486-19

Nachdem Schwarz im Jahre 1873 alle Fälle ermittelt hatte, in denen die hypergeometrische Reihe eine algebraische Funktion darstellt, hatte der Verfasser schon im Jahre 1904 Teile dieses Ergebnisses von neuem auf einem anderen, arithmetischen Wege bewiesen; er setzt jetzt jene Untersuchung fort. Unter Anwendung des bekannten Eisensteinschen Kriteriums, des Dirichletschen Satzes von den Primzahlen einer arithmetischen Progression und eines neuen, an sich interessanten zahlentheoretischen Hilfssatzes, wird der Transzendenzbeweis für gewisse weitere Fälle geführt.

(Zsfassung aus: Sitzungsberichte der Heidelberger Akademie der Wissenschaften / Jahresheft Juli 1910 bis Dezember 1911, S. XLVII)

Sitzungsberichte
der Heidelberger Akademie der Wissenschaften
Stiftung Heinrich Lanz
Mathematisch-naturwissenschaftliche Klasse
Jahrgang 1911. 18. Abhandlung.

Über einen zahlentheoretischen Satz und seine Anwendung auf die hypergeometrische Reihe

von

Edmund Landau

in Göttingen

Eingegangen am 2. Juli 1911

Vorgelegt von Leo Koenigsberger

Heidelberg 1911
Carl Winter's Universitätsbuchhandlung

Verlags-Nr. 621.

§ 1.

Definition: Es seien a, b und m reelle Zahlen[1]), davon m nicht 0. Es sei A der kleinste positive Rest von a modulo m, d. h. die durch

$$a = q\,m + A,\ q \text{ ganz},\ 0 < A \leqq |m|$$

eindeutig bestimmte Zahl; es sei B der kleinste positive Rest von b modulo m. Wenn $A < B$ ist, sagen wir

(1) $$a < b \pmod{m}$$

und

$$b > a \pmod{m}.$$

Wenn $A > B$ ist, sagen wir also

(2) $$a > b \pmod{m}$$

und

$$b < a \pmod{m}.$$

Wenn $A = B$ ist, sagt man üblicherweise

(3) $$a \equiv b \pmod{m}.$$

Genau einer der drei Fälle (1), (2), (3) muß immer vorliegen.

Diese Zeichen $<$ (mod. m) und $>$ (mod. m), sowie auch $\leqq$ (mod. m) und $\geqq$ (mod. m) sind offenbar transitiv; d. h. aus

$$a < b \pmod{m}$$

nebst

$$b < c \pmod{m}$$

folgt

$$a < c \pmod{m}$$

und entsprechend für die drei anderen Zeichen. Man kann also Relationen mit einem der Zeichen und auch dem Zeichen $\equiv$ dabei fortlaufend schreiben, z. B.

$$0 > 11 > 4 \equiv 10 \equiv -2 > 1 \equiv 7 \pmod{6}.$$

---

[1]) Im Folgenden wird übrigens m stets positiv und ganzzahlig sein.

Dagegen darf man nicht etwa Ungleichungen modulo m stets gliedweise addieren. Doch darf man z. B. aus

$$a < b \pmod{m}$$

offenbar schließen, daß

$$b - a < b \pmod{m}$$

ist.

Die folgenden Betrachtungen mögen von dem Spezialfalle $m = 60$ ausgehen. Die $\frac{\varphi(60)}{2} = 8$ zu 60 teilerfremden Restklassen, deren Elemente $< 30 \pmod{60}$ sind, werden durch

$$\rho = 1, 7, 11, 13, 17, 19, 23, 29$$

repräsentiert. Jede dieser Zahlen ρ hat die Eigenschaft, daß ihr 11-faches modulo 60 auch < 30 ist; da 11 zu 60 teilerfremd ist, also die acht Produkte 11ρ inkongruent (mod. 60) und zu 60 teilerfremd sind, heißt dies, daß die acht Produkte 11ρ den Zahlen ρ abgesehen von der Reihenfolge kongruent sind. In der Tat ist

$$11\rho = 11, 77, 121, 143, 187, 209, 253, 319$$
$$\equiv 11, 17, 1, 23, 7, 29, 13, 19 \pmod{60}.$$

In Formeln: Für $m = 60$ hat $k = 11$ die Eigenschaft, daß folgende $\frac{\varphi(m)}{2}$ Bedingungen[2]) erfüllt sind:

Aus

$$(\rho, m) = 1, \quad \rho < \frac{m}{2} \pmod{m} \tag{4}$$

ergibt sich

$$k\rho < \frac{m}{2} \pmod{m}. \tag{5}$$

Ich stelle nun das Problem, alle ganzzahligen Wertepaare m, k zu finden, für welche $m \geq 3$ ist und obige Eigenschaft („aus (4) folgt (5)") besteht. Von $m = 1$ und $m = 2$, wo $\frac{\varphi(m)}{2}$ gar keine ganze Zahl ist und auch keine teilerfremde Restklasse unterhalb $\frac{m}{2} \pmod{m}$ liegt, kann dabei keine Rede sein.

---

[2]) Ich rede von $\frac{\varphi(m)}{2}$ Bedingungen, nicht von unendlich vielen, da es nur von der Restklasse des ρ abhängt, ob $k\rho < \frac{m}{2} \pmod{m}$ ist oder nicht.

Dabei ist klar, daß mit jedem k auch jede zu k (mod. m) kongruente Zahl die $\frac{\varphi(m)}{2}$ Bedingungen erfüllt, so daß bei der Fragestellung $1 \leqq k \leqq m$ angenommen werden kann; da auch ρ modulo m festgelegt werden kann, lautet also das Problem:

Alle Paare ganzer Zahlen m, k zu finden, so daß

$$1 \leqq k \leqq m,\ 3 \leqq m$$

ist und die $\frac{\varphi(m)}{2}$ Bedingungen erfüllt sind: Aus

$$(\rho, m) = 1,\ 1 \leqq \rho < \frac{m}{2} \tag{6}$$

folgt

$$k\rho < \frac{m}{2} \text{ (mod. m)}. \tag{5}$$

In dieser Hinsicht bemerke ich zunächst folgende vier ziemlich trivialen Tatsachen:

Erstens: $k = 1$ hat natürlich für jedes $m \geqq 3$ die Eigenschaft. Denn aus

$$1 \leqq \rho < \frac{m}{2}$$

folgt

$$k\rho = \rho < \frac{m}{2} \text{ (mod. m)}.$$

Zweitens: Wenn k die Eigenschaft hat, so ist

$$1 \leqq k < \frac{m}{2}. \tag{7}$$

Denn man setze $\rho = 1$, was (6) erfüllt und

$$k < \frac{m}{2} \text{ (mod. m)}$$

liefert, somit zu (7) führt.

Drittens: Für ungerades $m \geqq 3$ hat nur die Zahl $k = 1$ die Eigenschaft. Denn es sei m ungerade,

$$1 < k < \frac{m}{2}$$

und (5) für alle vorgeschriebenen ρ erfüllt. Dann verstehe ich unter ρ diejenige wohlbestimmte Potenz 2^s von 2, für welche

$$\frac{m}{2} < 2^s k < m$$

ist; dies 2^s erfüllt wirklich (6), da

$$2^s < \frac{m}{k} \leq \frac{m}{2}$$

ist, stellt aber einen Widerspruch zu (5) dar.

Das Problem ist damit für ungerade m völlig erledigt.

Viertens: Für gerades m hat mit k auch $\frac{m}{2} - k$ die Eigenschaft; denn aus (5) folgt für die ρ, welche (6) erfüllen, weil sie ungerade sind,

$$\left(\frac{m}{2} - k\right)\rho = \frac{m}{2}\rho - k\rho \equiv \frac{m}{2} - k\rho < \frac{m}{2} \pmod{m}.$$

Also haben wir für gerades m jedenfalls die trivialen Lösungen $k = 1$ und $k = \frac{m}{2} - 1$ (welche im Falle $m = 4$ zusammenfallen) und dürfen bei Aufsuchung der übrigen Lösungen uns auf das Studium des Intervalls

$$2 \leq k \leq \frac{m}{4}$$

beschränken, also insbesondere $m \geq 8$ annehmen.

Der zahlentheoretische Satz, um den es sich in dieser Arbeit handelt, besagt nun, daß es außer den genannten unendlich vielen trivialen Fällen nur endlich viele weitere Fälle gibt, indem es zu jedem geraden $m > 60$ nur die beiden trivialen k gibt. D. h. es besteht der

Satz: Zu keiner ganzen Zahl $m > 60$ gibt es ein ganzes k derart, daß

$$k \not\equiv 1 \pmod{m},$$

ferner für gerades m

$$k \not\equiv \frac{m}{2} - 1 \pmod{m}$$

ist und aus

$$(\rho, m) = 1, \quad \rho < \frac{m}{2} \pmod{m} \tag{4}$$

jedesmal

$$k\rho < \frac{m}{2} \pmod{m} \tag{5}$$

folgt.

Vorbemerkung: Nach dem Vorangehenden ist es gleichbedeutend, statt (4)

$$(6) \qquad (\rho, m) = 1,\ 1 \leqq \rho < \frac{m}{2}$$

anzusetzen, und für den Unmöglichkeitsbeweis erlaubt, m gerade und

$$2 \leqq k \leqq \frac{m}{4}$$

anzunehmen. Es lautet also die

Behauptung: Zu keiner geraden Zahl $m > 60$ gibt es ein ganzes k derart, daß

$$2 \leqq k \leqq \frac{m}{4}$$

ist und aus

$$(6) \qquad (\rho, m) = 1,\ 1 \leqq \rho < \frac{m}{2}$$

die Ungleichung

$$(5) \qquad k\rho < \frac{m}{2} \pmod{m}$$

folgt.

Zugleich wird (was eine Abkürzung des Ausprobierens der endlich vielen Fälle $m = 8, 10, 12, \ldots, 58, 60$ ist) der folgende Beweis ergeben, daß bis 60 nur folgende vier nicht trivialen Fälle vorhanden sind:

$m = 12,\ k = 3;\ \rho = 1, 5;\ k\rho \equiv 3, 3.$
$m = 20,\ k = 3;\ \rho = 1, 3, 7, 9;\ k\rho \equiv 3, 9, 1, 7.$
$m = 24,\ k = 5;\ \rho = 1, 5, 7, 11;\ k\rho \equiv 5, 1, 11, 7.$
$m = 60,\ k = 11;$ siehe oben.

Gleichzeitig ergibt sich aus dem zu beweisenden Satz, daß nur für endlich viele m die $\frac{\varphi(m)}{2}$ Zahlen ρ eine Gruppe bilden; denn, wenn sie eine Gruppe bilden, ist jede von ihnen ein k (sc. mit der Eigenschaft) im Intervall $1 \leqq k < \frac{m}{2}$; also ist die Anzahl der zu m teilerfremden k dieses Intervalls $= \frac{\varphi(m)}{2}$. Nun ist die Anzahl der zu m teilerfremden k des Intervalls $1 \leqq k < \frac{m}{2}$ nach dem Obigen

1 für ungerade $m \geq 3$, $m = 4$ und alle[3]) $m \equiv 2 \pmod 4$;

2 für alle $m \equiv 0 \pmod 4$ exkl. $m = 4$, $m = 20$, $m = 24$ und $m = 60$;

4 für $m = 20$, $m = 24$ und $m = 60$.

Die Gleichung $\frac{\varphi(m)}{2} = 1$ für die m der ersten Art gilt nur bei $m = 3$, $m = 4$ und $m = 6$; die Gleichung $\frac{\varphi(m)}{2} = 2$ für die m der zweiten Art nur bei $m = 8$ und $m = 12$; die Gleichung $\frac{\varphi(m)}{2} = 4$ für die m der dritten Art nur bei $m = 20$ und $m = 24$. Also kann eine Gruppe höchstens vorliegen: Für $m = 3, 4, 6, 8, 12, 20, 24$, und sie liegt tatsächlich in diesen 7 Fällen vor:

$$\begin{aligned} m &= 3; \quad \rho = 1. \\ m &= 4; \quad \rho = 1. \\ m &= 6; \quad \rho = 1. \\ m &= 8; \quad \rho = 1, 3. \\ m &= 12; \quad \rho = 1, 5. \\ m &= 20; \quad \rho = 1, 3, 7, 9. \\ m &= 24; \quad \rho = 1, 5, 7, 11. \end{aligned}$$

Der Satz sagt aber viel mehr aus als, daß die ρ bei $m = 24$ aufhören, eine Gruppe zu bilden; er sagt u. a. aus, daß der Komplex der ρ abgesehen von $m = 60$ (nebst $k = 11$ oder $k = 19$) für kein $m > 24$ einen von den trivialen Werten $k = 1$ und (für gerades m) $k = \frac{m}{2} - 1$ verschiedenen Multiplikator besitzt, der ihn modulo m in sich überführt.

Beweis: Es sei also m gerade, $m \geq 8$, und es gebe ein k derart, daß

$$2 \leq k \leq \frac{m}{4}$$

und für

$$(\rho, m) = 1, \quad 1 \leq \rho < \frac{m}{2} \tag{6}$$

stets

$$k\rho < \frac{m}{2} \pmod m \tag{5}$$

---

[3]) In der Tat ist für $m \equiv 2 \pmod 4$ das triviale $k = \frac{m}{2} - 1$ nicht zu m teilerfremd.

ist. Dann soll bewiesen werden, daß m einen der Werte 12, 20, 24, 60 hat und entsprechend $k = 3, 3, 5, 11$ ist.

m hat jedenfalls die Form

$$m = 2^\alpha u,$$

wo

$$\alpha \geq 1, \; u \equiv 1 \pmod 2$$

ist.

I. **k sei gerade.**

1. Es sei $\alpha = 1$. Dann wähle ich

$$\rho = \frac{m}{2} - 2,$$

was offenbar (6) erfüllt. Dann ist nach (5)

$$k\rho = k\frac{m}{2} - 2k \equiv -2k < \frac{m}{2} \pmod m,$$

was der Tatsache

$$0 < 2k \leq \frac{m}{2}$$

widerspricht.

2. Es sei $\alpha = 2$.

a) k sei nicht durch 4 teilbar. Dann wähle ich

$$\rho = \frac{m}{4} + 2,$$

was offenbar (6) erfüllt. Dann ist nach (5)

$$k\rho = k\frac{m}{4} + 2k \equiv \frac{m}{2} + 2k < \frac{m}{2} \pmod m,$$

was der Tatsache

$$\frac{m}{2} < \frac{m}{2} + 2k \leq m$$

widerspricht.

b) k sei durch 4 teilbar. Dann wähle ich

$$\rho = \frac{m}{4} - 2$$

und erhalte

$$k\rho = k\frac{m}{4} - 2k \equiv -2k < \frac{m}{2} \pmod m,$$

einen Widerspruch.

3. Es sei $\alpha \geq 3$.

a) k sei nicht durch 4 teilbar. Ich nehme

$$\rho = \frac{m}{4} + 1$$

und erhalte den Widerspruch

$$k\rho = k\frac{m}{4} + k \equiv \frac{m}{2} + k < \frac{m}{2} \pmod{m}.$$

b) k sei durch 4 teilbar. Für

$$\rho = \frac{m}{4} - 1$$

kommt der Widerspruch

$$k\rho = k\frac{m}{4} - k \equiv -k < \frac{m}{2} \pmod{m}$$

heraus.

II. (Hauptfall, der u. a. sämtliche zu m teilerfremden k umfaßt): **k sei ungerade.** Ich werde zunächst beweisen, daß

$$k \equiv 1 \pmod{2^{\alpha-1}} \tag{8}$$

ist. Dies ist für $\alpha = 1$ und $\alpha = 2$ trivial und bedarf nur für $\alpha \geq 3$ eines Beweises, Es sei also $\alpha \geq 3$.

Die $\alpha - 2$ Zahlen

$$\frac{m}{4} + 1, \frac{m}{8} + 1, \ldots, \frac{m}{2^{\alpha-1}} + 1 \tag{9}$$

sind ρ-Zahlen, d. h. positiv, zu m teilerfremd und $< \frac{m}{2}$. Also ist zunächst

$$k\left(\frac{m}{4} + 1\right) < \frac{m}{2} \pmod{m},$$

folglich

$$k \equiv 1 \pmod{4}.$$

(Denn, wäre $k \equiv 3 \pmod{4}$, so wäre $k\left(\frac{m}{4} + 1\right) \equiv \frac{3}{4}m + k > \frac{m}{2} \pmod{m}$.) Wenn $\alpha = 3$ ist, ist (8) damit bewiesen. Wenn aber $\alpha \geq 4$ ist, liefert die zweite der Zahlen (9)

$$k\left(\frac{m}{8} + 1\right) < \frac{m}{2} \pmod{m},$$

also

$$k \equiv 1 \pmod{8}$$

nicht $k \equiv 5 \pmod{8}$). Usf. bis zu

$$k\left(\frac{m}{2^{\alpha-1}}+1\right)<\frac{m}{2} \pmod{m},$$

$$k \equiv 1 \pmod{2^{\alpha-1}}. \tag{8}$$

Nun läßt (8) modulo 2^α für $\alpha \geqq 2$ zwei Möglichkeiten zu: Erstens

$$k \equiv 1 \pmod{2^\alpha},$$

zweitens

$$k \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha};$$

für $\alpha = 1$ ist nur erstere zu berücksichtigen, da k ungerade ist.

1. Es sei

$$k \equiv 1 \pmod{2^\alpha}.$$

Dann bezeichne ich mit 2^n die höchste Potenz von 2 unterhalb u:

$$2^n < u < 2^{n+1}; \tag{10}$$

dies n existiert und ist $\geqq 1$, weil u nicht $= 1$ ist; sonst wäre ja $m = 2^\alpha$, $k = 1$.

Die n Zahlen

$$u - 2, \ldots, u - 2^n$$

sind offenbar ρ-Zahlen. Daher ist für $1 \leqq \nu \leqq n$

$$k(u-2^\nu) = ku - 2^\nu k = k\frac{m}{2^\alpha} - 2^\nu k \equiv \frac{m}{2^\alpha} - 2^\nu k < \frac{m}{2} \pmod{m}. \tag{11}$$

Für $\nu = 1$ gibt (11)

$$\frac{m}{2^\alpha} - 2k < \frac{m}{2} \pmod{m};$$

wegen

$$0 < 2k \leqq \frac{m}{2}$$

ist daher

$$\frac{m}{2^\alpha} - 2k > 0,$$

$$2k < \frac{m}{2^\alpha},$$

$$k < \frac{m}{2^{\alpha+1}}.$$

Ich behaupte, daß

$$k < \frac{m}{2^{\alpha+n}} \tag{12}$$

ist. Falls $n = 1$ ist, ist dies soeben bewiesen. Falls $n \geq 2$ ist, liefert (11) für $\nu = 2$

$$\frac{m}{2^\alpha} - 4k < \frac{m}{2} \pmod{m};$$

wegen

$$\frac{m}{2^\alpha} - 4k > \frac{m}{2^\alpha} - \frac{4m}{2^{\alpha+1}} = -\frac{m}{2^\alpha} \geq -\frac{m}{2}$$

ist

$$\frac{m}{2^\alpha} - 4k > 0,$$

$$k < \frac{m}{2^{\alpha+2}}.$$

Falls $n = 2$ ist, ist (12) bewiesen. Falls $n \geq 3$ ist, liefert (11) für $\nu = 3$

$$\frac{m}{2^\alpha} - 8k < \frac{m}{2} \pmod{m};$$

wegen

$$\frac{m}{2^\alpha} - 8k > \frac{m}{2^\alpha} - \frac{8m}{2^{\alpha+2}} = -\frac{m}{2^\alpha} \geq -\frac{m}{2}$$

ist

$$8k < \frac{m}{2^\alpha},$$

$$k < \frac{m}{2^{\alpha+3}}.$$

Usf. bis zu (12).

Aus (12) folgt nun aber nach (10)

$$k < \frac{u}{2^n} < \frac{2^n+1}{2^n} = 2,$$

was ein Widerspruch ist.

2. Es sei

$$k \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}, \quad \alpha \geq 2.$$

a) (Schwierigster Unterfall.) Es sei $\alpha = 2$. Dann ist

$$m = 4u, \quad k \equiv 3 \pmod{4}.$$

Es werde ein positives ganzes n so bestimmt, daß

$$2^n < \frac{m}{4} = u < 2^{n+1}$$

ist; das geht wegen $u \geq 3$. Die n Zahlen

$$\frac{m}{4} - 2, \frac{m}{4} - 4, \ldots, \frac{m}{4} - 2^n$$

sind ρ-Zahlen. Für $1 \leq \nu \leq n$ ist also

$$k\left(\frac{m}{4} - 2^\nu\right) \equiv \frac{3m}{4} - 2^\nu k < \frac{m}{2} \text{ (mod. m)},$$

$$\frac{m}{4} < 2^\nu k < \frac{3m}{4} \text{ (mod. m)}. \tag{13}$$

(13) gibt für $\nu = 1$

$$\frac{m}{4} < 2k < \frac{3m}{4} \text{ (mod. m)};$$

daher ist

$$\frac{m}{4} < 2k \leq \frac{m}{2},$$

$$\frac{m}{8} < k \leq \frac{m}{4}. \tag{14}$$

Ich setze nun

$$k = \frac{m}{6} + \kappa,$$

wobei natürlich κ nicht ganz zu sein braucht, und behaupte, daß

$$|\kappa| \leq \frac{m}{6 \cdot 2^n} \tag{15}$$

ist.

Aus (14) folgt

$$-\frac{m}{24} = \frac{m}{8} - \frac{m}{6} < \kappa \leq \frac{m}{4} - \frac{m}{6} = \frac{m}{12},$$

also

$$|\kappa| \leq \frac{m}{6 \cdot 2}.$$

Im Falle $n = 1$, d. h. $8 < m < 16$, ist (15) damit bewiesen, und (15) wird überhaupt bewiesen sein, wenn für $1 \leq \nu < n$ aus

$$|\kappa| \leq \frac{m}{6 \cdot 2^\nu} \tag{16}$$

die Richtigkeit von

$$|\kappa| \leq \frac{m}{6 \cdot 2^{\nu+1}} \tag{17}$$

gefolgert werden kann. Dies geschieht so. Nach (13), worin ja $\nu + 1$ statt ν (wegen $\nu + 1 \leq n$) geschrieben werden kann, ist

$$\frac{m}{4} < 2^{\nu+1} k < \frac{3m}{4} \pmod{m},$$

also entweder

$$\frac{m}{8} < 2^{\nu} k < \frac{3m}{8} \pmod{m}$$

oder

$$\frac{5m}{8} < 2^{\nu} k < \frac{7m}{8} \pmod{m};$$

durch Vergleich mit der ursprünglichen Form von (13) ersieht man, daß entweder

$$\frac{m}{4} < 2^{\nu} k < \frac{3m}{8} \pmod{m}$$

oder

$$\frac{5m}{8} < 2^{\nu} k < \frac{3m}{4} \pmod{m}$$

ist. Nun ist wegen

$$2^{\nu} k = 2^{\nu} \frac{m}{6} + 2^{\nu} \kappa$$

und (16)

$$2^{\nu} \frac{m}{6} - \frac{m}{6} < 2^{\nu} k \leq 2^{\nu} \frac{m}{6} + \frac{m}{6}.$$

Für ungerades ν ist (wegen $2^{\nu} \equiv 2 \pmod{6}$)

$$2^{\nu} \frac{m}{6} \equiv \frac{m}{3} \pmod{m},$$

$$\frac{m}{6} \leq 2^{\nu} k \leq \frac{m}{2} \pmod{m},$$

$$\frac{m}{4} < 2^{\nu} k \equiv \frac{m}{3} + 2^{\nu} \kappa < \frac{3m}{8} \pmod{m}.$$

Für gerades ν ist (wegen $2^{\nu} \equiv 4 \pmod{6}$)

$$2^{\nu} \frac{m}{6} \equiv \frac{2m}{3} \pmod{m},$$

$$\frac{m}{2} \leq 2^{\nu} k \leq \frac{5m}{6} \pmod{m},$$

$$\frac{5m}{8} < 2^{\nu} k \equiv \frac{2m}{3} + 2^{\nu} \kappa < \frac{3m}{4} \pmod{m}.$$

In beiden Fällen ist daher

$$| 2^{\nu} \kappa | < \frac{m}{12}.$$

Damit ist aus (16) die Relation (17) bewiesen.

Also ist (15) richtig und liefert weiter

$$| k - \frac{m}{6} | = | \kappa | \leq \frac{m}{6 \cdot 2^n} = \frac{m}{3 \cdot 2^{n+1}} < \frac{m}{3\frac{m}{4}} = \frac{4}{3}.$$

Da nun $k - \frac{m}{6}$ entweder eine ganze Zahl ist oder den Bruchbestandteil $\frac{1}{3}$ oder $\frac{2}{3}$ hat, sind nur 7 Fälle möglich:

$$k - \frac{m}{6} = -1, \; -\frac{2}{3}, \; -\frac{1}{3}, \; 0, \; \frac{1}{3}, \; \frac{2}{3}, \; 1.$$

Hiervon geht

$$k = \frac{m}{6}$$

nicht, da k gerade wäre.

$$k = \frac{m}{6} \pm \frac{2}{3} = \frac{2u \pm 2}{3}$$

geht nicht, da k auch gerade wäre.

$$k = \frac{m}{6} + \frac{1}{3} = \frac{2u + 1}{3}$$

geht nicht, da $k \equiv 1 \pmod 4$ wäre.

$$k = \frac{m}{6} - \frac{1}{3} = \frac{2u - 1}{3}$$

geht aus folgendem Grunde nur für ein einziges u. Diese Zahl $\frac{2u-1}{3}$ ist zu u, also auch zu m teilerfremd; k^2 hätte also auch die charakteristische Eigenschaft (5), da die zu m teilerfremden k mit dieser Eigenschaft offenbar eine Gruppe bilden. Also wäre wegen $k^2 \equiv 1 \pmod 4$ nach dem Ergebnis des Falles 1) entweder $k^2 \equiv 1 \pmod m$ oder $k^2 \equiv \frac{m}{2} - 1 \pmod m$. Das ergäbe aber

$$k^2 \equiv \pm 1 \pmod u,$$

$$\left(\frac{2u-1}{3}\right)^2 \equiv \pm 1 \pmod u,$$

$$1 \equiv \pm 9 \pmod u,$$

was nur für $u = 5$ möglich ist und wirklich den oben angeführten Fall $m = 20$, $k = 3$ liefert.

$$k = \frac{m}{6} - 1$$

geht nicht, da dies $\equiv 1 \pmod 4$ wäre.

Es bleibt

$$k = \frac{m}{6} + 1,$$

so daß m durch 12 teilbar ist.

a) Es sei m nicht durch 5 teilbar. Dann liefert $\rho = 5$

$$k\rho = \frac{5m}{6} + 5 < \frac{m}{2} \pmod m,$$

$$\frac{5m}{6} + 5 > m,$$

$$30 > m,$$

$$m = 12,$$

wofür wirklich $k = 3$ die Eigenschaft hat.

b) Es sei m durch 5 teilbar, also durch 60 teilbar. Dann ist $m = 5^\beta M$, wo $\beta \geq 1$ und $(M, 5) = 1$ ist. Es liefert

$$\rho = \frac{m}{2 \cdot 5^\beta} + 5 = \frac{M}{2} + 5$$

$$k\rho = \left(\frac{m}{6} + 1\right)\left(\frac{m}{2 \cdot 5^\beta} + 5\right) = m \cdot \frac{m}{12 \cdot 5^\beta} + \frac{m}{2 \cdot 5^\beta} + \frac{5m}{6} + 5$$

$$\equiv \frac{m}{2 \cdot 5^\beta} + \frac{5m}{6} + 5 < \frac{m}{2} \pmod m.$$

Wegen

$$\frac{m}{2} < \frac{m}{2 \cdot 5^\beta} + \frac{5m}{6} + 5 \leq \frac{m}{10} + \frac{5m}{6} + 5$$

ist also

$$\frac{m}{10} + \frac{5m}{6} + 5 > m,$$

$$5 > \frac{m}{15},$$

$$m < 75,$$

$$m = 60,$$

wozu wirklich $k = 11$ gehört.

b) Es sei $\alpha \geqq 3$. Der Wert

$$\rho = \frac{m}{2^\alpha} + 2$$

ergibt

$$k\left(\frac{m}{2^\alpha} + 2\right) = k\frac{m}{2^\alpha} + 2k \equiv \frac{m}{2} + \frac{m}{2^\alpha} + 2k < \frac{m}{2} \pmod{m},$$

$$\frac{m}{2^\alpha} + 2k > \frac{m}{2},$$

$$2k > \frac{m}{2} - \frac{m}{2^\alpha} \geq \frac{m}{2} - \frac{m}{8} = \frac{3m}{8},$$

$$k > \frac{3m}{16}. \tag{18}$$

a) Es sei $\alpha = 3$. Für $m = 8$ gibt es kein $k \equiv 5 \pmod{8}$ zwischen 2 und $\frac{m}{4}$. Für $m = 24$ hat wirklich $k = 5$ die Eigenschaft. Es darf also jetzt $m \geqq 40$ angenommen werden. Dann gibt

$$\rho = \frac{m}{8} - 4$$

das Folgende:

$$k\left(\frac{m}{8} - 4\right) = k\frac{m}{8} - 4k \equiv \frac{5m}{8} - 4k < \frac{m}{2} \pmod{m},$$

$$\frac{5m}{8} - 4k > 0,$$

$$k < \frac{5m}{32},$$

was (18) widerspricht.

b) Es sei $\alpha \geqq 4$. Dann gibt

$$\rho = \frac{m}{8} - 1$$

das Folgende:

$$k\left(\frac{m}{8} - 1\right) = k\frac{m}{8} - k \equiv \frac{m}{8} - k < \frac{m}{2} \pmod{m},$$

$$k < \frac{m}{8},$$

was (18) widerspricht.

Damit ist der Satz auf S. 6 bewiesen.

§ 2.

Eisenstein und Heine haben den Satz[4]) bewiesen: Wenn die Potenzreihe

$$c_0 + c_1 x + \ldots + c_n x^n + \ldots$$

mit rationalen Koeffizienten Element einer algebraischen Funktion ist, so gibt es eine ganze Zahl q derart, daß $c_n q^n$ für alle $n > 1$ ganz ist.

Daraus folgt insbesondere: Wenn die obige Potenzreihe Element einer algebraischen Funktion ist, so enthalten die c_n, in reduzierter Form geschrieben, nur endlich viele verschiedene Primzahlen in den Nennern.

Von diesem Kriterium hatte ich schon in einer früheren Arbeit[5]) eine Anwendung auf die Theorie der hypergeometrischen Reihe gemacht. Jetzt will ich in Verbindung mit dem Satz aus § 1 eine neue Anwendung geben und dazu zunächst einiges aus meiner früheren Arbeit, das ich brauche, mit etwas vereinfachten Beweisen wiederholen, so daß der Leser jene Abhandlung nicht zu kennen braucht.

Ich nehme an, daß in der hypergeometrischen Reihe

$$F(\alpha, \beta, \gamma, x) = 1 + \frac{\alpha \cdot \beta}{1 \cdot \gamma} x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1 \cdot 2 \cdot \gamma(\gamma+1)} x^2 + \ldots$$
$$+ \frac{\alpha(\alpha+1)\ldots(\alpha+n)\beta(\beta+1)\ldots(\beta+n)}{1 \cdot 2 \ldots (1+n)\gamma(\gamma+1)\ldots(\gamma+n)} x^{n+1} + \ldots$$

die drei Zahlen α, β, γ rational sind, aber keine der Zahlen α, β, γ, $\gamma-\alpha$, $\gamma-\beta$ ganz. Der (positive) Hauptnenner der drei Brüche α, β, γ sei m; es sei also

$$\alpha = \frac{a}{m}, \quad \beta = \frac{b}{m}, \quad \gamma = \frac{c}{m},$$

wo a, b, c, m ganz sind, $(a, b, c, m) = 1$ ist und weder a noch b noch c noch $c-a$ noch $c-b$ durch m teilbar ist; eo ipso ist dabei $m \geq 3$. Zufällig wird $(a, b, c, m) = 1$ nicht einmal im Folgenden verwendet. Wird

$$F(\alpha, \beta, \gamma, x) = \sum_{n=0}^{\infty} c_n x^n$$

---

[4]) Literaturangaben vgl. in meiner Arbeit: *Eine Anwendung des* Eisensteinschen *Satzes auf die Theorie der* Gaussschen *Differentialgleichung* [Journal für die reine und angewandte Mathematik, Bd. CXXVII (1904), S. 92—102], S. 92—93.

[5]) L. c.

gesetzt, so ist für $n \geq 0$

$$c_{n+1} = \frac{\frac{a}{m}\left(\frac{a}{m}+1\right)\ldots\left(\frac{a}{m}+n\right)\frac{b}{m}\left(\frac{b}{m}+1\right)\ldots\left(\frac{b}{m}+n\right)}{1 \cdot 2 \quad \ldots \quad (1+n)\ \frac{c}{m}\left(\frac{c}{m}+1\right)\ldots\left(\frac{c}{m}+n\right)}$$

$$= \frac{a\,(a+m)\ldots(a+n\,m)\,b\,(b+m)\ldots(b+n\,m)}{m \cdot 2\,m \ \ldots (m+n\,m)\,c\,(c+m)\ldots(c+n\,m)}.$$

Ich nehme nun an, daß dies $F(\alpha, \beta, \gamma, x)$ algebraisch ist, und frage zunächst, was nach dem EISENSTEIN-HEINE'schen Kriterium in seiner speziellen Fassung („endlich viele Primzahlen in den Nennern") daraus folgt.

Nach jenem Satz gibt es eine Zahl N derart, daß jede Primzahl $p > N$ den Zähler

$$a\,(a+m)\ldots(a+n\,m)\,b\,(b+m)\ldots(b+n\,m)$$

jedes c_{n+1} mindestens so oft teilt als den zugehörigen Nenner

$$m \cdot 2\,m \ldots (m+n\,m)\,c\,(c+m)\ldots(c+n\,m).$$

Ich nehme — aus nachher ersichtlichen Gründen — N oberhalb der vier Zahlen m, $2\,|\,a\,|$, $2\,|\,b\,|$, $2\,|\,c\,|$ an, was erlaubt ist.

Aus dem Vorigen folgt insbesondere: Wenn p eine Primzahl $> N$, ferner $n \geq 1$ und

$$c + n\,m \equiv 0 \pmod{p}$$

ist, so ist mindestens eine der beiden Kongruenzen

$$a\,(a+m)\ldots(a+n\,m) \equiv 0 \pmod{p}$$

und

$$b\,(b+m)\ldots(b+n\,m) \equiv 0 \pmod{p}$$

erfüllt. Mit anderen Worten: Wenn x_0 die kleinste positive Wurzel der (wegen $p > N > m$ lösbaren und wegen $p > N > 2\,|\,a\,| > |\,a\,|$ nicht die Wurzel 0 besitzenden) Kongruenz

$$a + x\,m \equiv 0 \pmod{p} \tag{19}$$

und ebenso y_0 die kleinste positive Wurzel der Kongruenz

$$b + y\,m \equiv 0 \pmod{p} \tag{20}$$

ist, so ist mindestens eine der beiden Ungleichungen

$$x_0 \leq n, \quad y_0 \leq n$$

erfüllt.

Daraus ergibt sich: Ist p eine Primzahl $> N$ und bezeichnen x_0, y_0 und z_0 die kleinsten positiven Wurzeln der Kongruenzen (19), (20) und

$$c + z\,m \equiv 0 \pmod{p},$$

so ist mindestens eine der beiden Ungleichungen

$$x_0 \leq z_0,\ y_0 \leq z_0 \tag{21}$$

erfüllt.

Diese schon in meiner älteren Arbeit hergeleitete Tatsache hatte ich seinerzeit auf die Primzahlen p der Linearform $m\,t + 1$ angewandt. Heute werde ich sie auf die Primzahlen einer beliebigen Linearform $m\,t + q$ anwenden, wo q irgendein vollständiges Restsystem teilerfremder Zahlen modulo m durchläuft.

Es sei also $(q, m) = 1$. Nach dem DIRICHLET'schen Satz gibt es eine Primzahl

$$p = m\,t_0 + q > N.$$

Es bedeute ρ diejenige Zahl, für welche

$$1 \leq \rho \leq m - 1,\ \rho\,q \equiv 1 \pmod{m}$$

ist, so daß ρ mit q ein Restsystem teilerfremder Zahlen modulo m durchläuft. Dann ist die Zahl

$$x = a\,\frac{\rho\,p - 1}{m}$$

ganz wegen

$$\rho\,p - \rho\,q \equiv 1 \pmod{m},$$

und sie genügt der Kongruenz (19), da ja für sie

$$a + x\,m = a + a\,(\rho\,p - 1) = a\,\rho\,p$$

ist. Es ist also x_0 der kleinste positive Rest von $a\,\frac{\rho\,p - 1}{m}$ modulo p und läßt sich in folgender Form darstellen. Es bezeichne a_0 (bzw. nachher b_0 und c_0) den kleinsten positiven Rest[6]) von $\rho\,a$ (bzw. $\rho\,b$ und $\rho\,c$) modulo m, so daß (weil $\frac{a}{m}$ nicht ganz ist),

$$1 \leq a_0 \leq m - 1$$

ist, und es werde die ganze Zahl

$$\frac{\rho\,a - a_0}{m} = A$$

gesetzt. Dann ist

$$a\,\frac{\rho p - 1}{m} = \rho\,a\,\frac{p}{m} - \frac{a}{m} = (a_0 + A\,m)\,\frac{p}{m} - \frac{a}{m} = \left(a_0\,\frac{p}{m} - \frac{a}{m}\right) + A\,p$$

$$\equiv a_0\,\frac{p}{m} - \frac{a}{m} \pmod{p}.$$

---

[6]) Es ist also $\frac{a_0}{m}$ der kleinste positive Rest von $\rho\,a$ modulo 1.

Diese ganze Zahl $a_0 \frac{p}{m} - \frac{a}{m}$ ist x_0, da sie offenbar zwischen 0 (exkl.) und p (exkl.) gelegen ist; in der Tat ist wegen $p > |a|$

$$a_0 \frac{p}{m} - \frac{a}{m} \leqq (m-1)\frac{p}{m} + \frac{|a|}{m} = p - \frac{p - |a|}{m} < p$$

und

$$a_0 \frac{p}{m} - \frac{a}{m} \geqq \frac{p}{m} - \frac{|a|}{m} = \frac{p - |a|}{m} > 0.$$

Es ist also

$$x_0 = a_0 \frac{p}{m} - \frac{a}{m}$$

und ebenso

$$y_0 = b_0 \frac{p}{m} - \frac{b}{m},$$

$$z_0 = c_0 \frac{p}{m} - \frac{c}{m}.$$

Da nun $\left(\text{wegen } |a| < \frac{p}{2},\ |b| < \frac{p}{2},\ |c| < \frac{p}{2}\right)$ die Zahlen x_0, y_0, z_0 mit einem Fehler $< \frac{p}{2m}$ durch $a_0 \frac{p}{m}$, $b_0 \frac{p}{m}$, $c_0 \frac{p}{m}$ approximiert werden, ergibt sich aus (21), daß mindestens eine der beiden Ungleichungen

$$a_0 \leqq c_0,\ b_0 \leqq c_0$$

gilt. Das Gleichheitszeichen ist hier ausgeschlossen, da z. B. aus $a_0 = c_0$ folgen würde

$$\rho a \equiv \rho c \pmod{m},$$
$$a \equiv c \pmod{m},$$

während $\gamma - \alpha$ als nicht ganz vorausgesetzt wurde.

Also ist mindestens eine der beiden Ungleichungen

$$a_0 < c_0,\ b_0 < c_0$$

erfüllt.

Das sind $\varphi(m)$ notwendige Bedingungen dafür, daß $F(\alpha, \beta, \gamma, x)$ unter den gemachten Annahmen algebraisch ist; denn ρ kann einen beliebigen seiner $\varphi(m)$ Werte bedeuten. Ich finde also, in den Bezeichnungen des § 1 ausgedrückt: Für jede der $\varphi(m)$ zu m teilerfremden Restklassen ρ ist

(22) $\rho a < \rho c \pmod{m}$ oder $\rho b < \rho c \pmod{m}$ oder beides.

In meiner erwähnten Arbeit[7]) hatte ich nur $\rho = 1$, d. h. (wegen $q = 1$) den elementar beweisbaren DIRICHLET'schen Satz für die Progression $m\,t \dotplus 1$ benutzt; ich hatte daher damals geschlossen:

$$a < c \pmod m \text{ oder } b < c \pmod m \text{ oder beides.}$$

In jener Arbeit gebrauchte ich dann die Tatsache, daß genau eine dieser beiden Ungleichungen gilt, d. h. die andere nicht (so daß modulo m entweder $a < c < b$ oder $b < c < a$ sein muß); um diese Tatsache zu beweisen, hatte ich auf die Theorie der hypergeometrischen Reihe zurückgegriffen. Dies läßt sich auch vermeiden und durch meine obigen Schlüsse in Verbindung mit dem (auch elementar[8]) beweisbaren) Spezialfall $q = m - 1$ des DIRICHLET'schen Satzes ersetzen; für $q = m - 1$ ist $\rho = m - 1$, also

$$(m-1)\,a < (m-1)\,c \pmod m \text{ oder } (m-1)\,b < (m-1)\,c \pmod m$$
$$\text{oder beides,}$$

d. h.

$$-a < -c \pmod m \text{ oder } -b < -c \pmod m \text{ oder beides,}$$

d. h.

$$a > c \pmod m \text{ oder } b > c \pmod m \text{ oder beides,}$$

also c modulo m zwischen a und b gelegen, was zu beweisen war.

Überhaupt schließe ich allgemein aus (22) so weiter: Wenn mit q die Zahl $m - q$ betrachtet wird, die ja auch zu m teilerfremd ist, so geht ρ in $m - \rho$ über. Es ist also nach (22)

$$(m-\rho)\,a < (m-\rho)\,c \pmod m \text{ oder } (m-\rho)\,b < (m-\rho)\,c \pmod m$$
$$\text{oder beides,}$$

d. h.

$$-\rho\,a < -\rho\,c \pmod m \text{ oder } -\rho\,b < -\rho\,c \pmod m \text{ oder beides,}$$

folglich

(23) $\rho\,a > \rho\,c \pmod m$ oder $\rho\,b > \rho\,c \pmod m$ oder beides.

Aus (22) und (23) folgt

(24) $\boldsymbol{\rho\,a < \rho\,c < \rho\,b \pmod m}$ **oder** $\boldsymbol{\rho\,a > \rho\,c > \rho\,b \pmod m}$**;**

dies hat sich als notwendige Bedingung dafür ergeben, daß

---

[7]) Deren Ziel war, auf Grund des EISENSTEIN-HEINE'schen Satzes den Transzendenzbeweis in dem Fall zu führen, daß die Winkelsumme des SCHWARZ'schen reduzierten Kreisbogendreiecks $< \pi$ ist.

[8]) Das hat GENOCCHI zuerst gemacht; vgl. die von Herrn BAUER herrührende Darstellung auf S. 440–446 und die auf $q = 1$ und $q = m - 1$ bezüglichen Literaturangaben auf S. 897 meines *Handbuchs der Lehre von der Verteilung der Primzahlen* [Leipzig und Berlin (Teubner), 1909].

$F(\alpha, \beta, \gamma, x)$ bei rationalen, nicht ganzen α, β, γ, $\gamma - \alpha$, $\gamma - \beta$ algebraisch ist.[9])

(24) muß also für alle $\varphi(m)$ zu m teilerfremden Restklassen ρ gelten. Es ist aber, da (24) für ρ genau dasselbe besagt wie für $m - \rho$, klar, daß diese $\varphi(m)$ Bedingungen sich sofort auf $\frac{\varphi(m)}{2}$ reduzieren; man braucht z. B. nur die $\frac{\varphi(m)}{2}$ Bedingungen mit $1 \leq \rho < \frac{m}{2}$, $(\rho, m) = 1$ beizubehalten.

§ 3.

Es werde nun — ganz unabhängig von der Beziehung zur hypergeometrischen Reihe — einiges über das Problem gesagt, wann ein System a, b, c, m, wo $m \geq 3$ ist und weder a noch b durch m teilbar ist, die $\frac{\varphi(m)}{2}$ Bedingungen

(24) $\rho a < \rho c < \rho b \pmod{m}$ oder $\rho a > \rho c > \rho b \pmod{m}$

für $1 \leq \rho < \frac{m}{2}$, $(\rho, m) = 1$ erfüllt. Eo ipso ist dabei weder c noch $c - a$ noch $c - b$ durch m teilbar; darum habe ich diese Einschränkungen soeben nicht besonders erwähnt.

Das Erfülltsein bzw. Nichterfülltsein von (24) bleibt offenbar gegenüber einer Änderung einer der Zahlen a, b, c modulo m invariant[10]); daher darf bei der Diskussion

---

[9]) Natürlich läßt sich (24) ohne Einführung von a, b, c, m so schreiben:

$$\rho\alpha < \rho\gamma < \rho\beta \pmod{1} \text{ oder } \rho\alpha > \rho\gamma > \rho\beta \pmod{1}$$

für alle zum Hauptnenner von α, β, γ teilerfremden ρ.

[10]) Diese Tatsache ist analog (aber weder gleichbedeutend, noch darin enthalten, noch sie enthaltend) mit der bekannten und leicht erweislichen Tatsache, daß bei nicht ganzen α, β, γ, $\gamma - \alpha$, $\gamma - \beta$ mit $F(\alpha, \beta, \gamma, x)$ auch erstens $F(\alpha + 1, \beta, \gamma, x)$, zweitens $F(\alpha - 1, \beta, \gamma, x)$, drittens $F(\alpha, \beta, \gamma + 1, x)$, viertens $F(\alpha, \beta, \gamma - 1, x)$, folglich bei ganzen A, B, C auch $F(\alpha + A, \beta + B, \gamma + C, x)$ algebraisch ist. Diese vier Tatsachen folgen unmittelbar aus den Identitäten

$$F(\alpha + 1, \beta, \gamma, x) = F(\alpha, \beta, \gamma, x) + \frac{x}{\alpha} F'(\alpha, \beta, \gamma, x),$$

$$F(\alpha, \beta, \gamma - 1, x) = F(\alpha, \beta, \gamma, x) + \frac{x}{\gamma - 1} F'(\alpha, \beta, \gamma, x)$$

nebst den zwei Gauss'schen „relationes inter functiones contiguas"

$$(\gamma - 2\alpha - (\beta - \alpha)x) F(\alpha, \beta, \gamma, x) + \alpha(1 - x) F(\alpha + 1, \beta, \gamma, x) - (\gamma - \alpha) F(\alpha - 1, \beta, \gamma, x) = 0,$$

$$\gamma(\gamma - 1 - (2\gamma - \alpha - \beta - 1)x) F(\alpha, \beta, \gamma, x) + (\gamma - \alpha)(\gamma - \beta) x F(\alpha, \beta, \gamma + 1, x) - \gamma(\gamma - 1)(1 - x) F(\alpha, \beta, \gamma - 1, x) = 0.$$

$$0 < a < m,\ 0 < b < m,\ 0 < c < m$$

angenommen werden. Da ferner Symmetrie in bezug auf a und b stattfindet, darf $a \leq b$, d. h. (mit Rücksicht auf das Erfülltsein von (24) bei $\rho = 1$)

(25) $$0 < a < c < b < m$$

angenommen werden.

Ich bezeichne Systeme wie $\{a, b, c\}$ durch geschweifte Klammern. Zunächst ist es interessant, daß (24) nebst (25) mit $\{a, b, c\}$ auch für $\{c - a,\ m - a,\ b - a\}$ giltig bleibt. In der Tat folgt aus

(26) $$0 < x < y < z < m,$$

daß

$$0 < y - x < z - x < m - x < m$$

ist; diese Tatsache ist im Falle

$$\rho a < \rho c < \rho b \pmod{m}$$

auf die kleinsten positiven Reste x, y, z von ρa, ρc, ρb modulo m anzuwenden und liefert

$$\rho (c - a) < \rho (b - a) < \rho (m - a) \pmod{m};$$

im Falle

$$\rho a > \rho c > \rho b \pmod{m}$$

ist sie auf die kleinsten positiven Reste x, y, z von $-\rho a$, $-\rho c$, $-\rho b$ anzuwenden und liefert

$$-\rho (c - a) < -\rho (b - a) < -\rho (m - a) \pmod{m},$$

d. h.

$$\rho (c - a) > \rho (b - a) > \rho (m - a) \pmod{m}.$$

Die Iteration dieses Übergangs von $\{a, b, c\}$ zu $\{c - a,\ m - a,\ b - a\}$ führt nach vier Schritten zum Anfang zurück, nämlich insgesamt zu den vier Systemen[11])

(27) $$\{a, b, c\},\ \{c - a,\ m - a,\ b - a\},\ \{b - c,\ m - c + a,\ m - c\},$$
$$\{m - b,\ m - b + c,\ m - b + a\}.$$

Ferner ist mit $\{a, b, c\}$ auch $\{c - a, b, b - a\}$ eine Lösung; denn aus (26) folgt

$$0 < y - x < z - x < z < m.$$

Durch Iteration entstehen

(28) $$\{a, b, c\},\ \{c - a,\ b,\ b - a\},\ \{b - c,\ b,\ b - c + a\}.$$

Andererseits ist mit $\{a, b, c\}$ auch $\{c - a, b, c\}$ eine Lösung, da aus (26)

$$0 < y - x < y < z < m$$

[11]) Hier wie mehrfach in der Folge können natürlich für spezielle Werte von a, b, c, m Systeme zusammenfallen.

folgt. Durch Iteration kommt nichts Neues hinzu; durch Kombination dieser Operation mit den drei Systemen (28) haben wir sechs Systeme mit festgehaltenem zweiten Element:

$$(29)\quad \begin{matrix}\{a, b, c\},\ \{c-a, b, c\},\ \{c-a, b, b-a\},\ \{b-c, b, b-a\},\\ \{b-c, b, b-c+a\},\ \{a, b, b-c+a\}.\end{matrix}$$

Jedes der vier Systeme (27) liefert also sechs Systeme nach dem Schema (29). Ich habe also insgesamt durch die vorangehenden Überlegungen vierundzwanzig zusammengehörige und eine Gruppe bildende Systeme[12]) gefunden, die ich hier ausführlich zusammenstellen werde:

$$(30)\quad \left\{\begin{matrix}
\{a, b, c\},\ \{c-a, m-a, b-a\},\ \{b-c, m-c+a, m-c\},\\
\quad \{m-b, m-b+c, m-b+a\},\\
\{c-a, b, c\},\ \{b-c, m-a, b-a\},\ \{m-b, m-c+a, m-c\},\\
\quad \{a, m-b+c, m-b+a\},\\
\{c-a, b, b-a\},\ \{b-c, m-a, m-c\},\\
\quad \{m-b, m-c+a, m-b+a\},\ \{a, m-b+c, c\},\\
\{b-c, b, b-a\},\ \{m-b, m-a, m-c\},\\
\quad \{a, m-c+a, m-b+a\},\ \{c-a, m-b+c, c\},\\
\{b-c, b, b-c+a\},\ \{m-b, m-a, m-b+c-a\},\\
\quad \{a, m-c+a, b-c+a\},\\
\quad \{c-a, m-b+c, m-b+c-a\},\\
\{a, b, b-c+a\},\ \{c-a, m-a, m-b+c-a\},\\
\quad \{b-c, m-c+a, b-c+a\},\\
\quad \{m-b, m-b+c, m-b+c-a\}.
\end{matrix}\right.$$

---

[12]) Daß unter den 24 Systemen für spezielle Werte der Buchstaben mehrfache auftreten können, ist selbstverständlich. Die Tatsache, daß mit einem alle 24 Systeme den Bedingungen (24), (25) genügen, ist analog (aber weder gleichbedeutend noch mehr oder weniger bedeutend) zu der durch Kummer bekannten Tatsache, daß bei nicht ganzen γ, $\gamma-\alpha-\beta$, $\beta-\alpha$ mit $F(\alpha, \beta, \gamma, x)$ gewisse 24 partikuläre Integrale der zugehörigen Gauss'schen Differentialgleichung von der Gestalt $x^u(1-x)^v F(\alpha', \beta', \gamma', y)$ vorhanden sind, wo $y = x$ oder $= 1-x$ oder $= \frac{1}{x}$ oder $= \frac{1}{1-x}$ oder $= \frac{x}{x-1}$ oder $= \frac{x-1}{x}$ ist, u und v Konstanten sind (bei rationalen α, β, γ rational) und α', β', γ' modulo 1 genau die 24 homogenen linearen Funktionen von $\alpha, \beta, \gamma, 1$ sind, welche den 24 homogenen linearen Funktionen von a, b, c, m des Textes entsprechen. Da im Falle, daß $\alpha, \beta, \gamma-\alpha, \gamma-\beta$ nicht ganz sind, leicht gezeigt werden kann, daß mit $F(\alpha, \beta, \gamma, x)$ das allgemeine Integral der zugehörigen Gauss'schen Differentialgleichung algebraisch ist, so ist bei rationalen α, β, γ, für welche $\alpha, \beta, \gamma, \beta-\alpha, \gamma-\alpha, \gamma-\beta, \gamma-\alpha-\beta$ nicht ganz sind, mit $F(\alpha, \beta, \gamma, x)$ die Funktion $F(\alpha', \beta', \gamma', x)$ alle 24 Male algebraisch. Das ist das Analogon zur Tabelle des Textes.

Jedes einzelne dieser 24 Systeme als Ausgang führt natürlich wegen der Gruppeneigenschaft zu denselben 24 Systemen. Man hat also eine Übersicht über alle Lösungen von (24), (25), wenn man von jeder Gruppe ein System beibehält. Ohne Beschränkung der Allgemeinheit darf daher gleichzeitig dreierlei angenommen werden:

1. Es hat $\{a, b, c\}$ von den 24 Systemen sein drittes Element am größten; d. h. es ist

$$c \geqq b - a,\ c \geqq b - c + a,\ c \geqq m - c,\ c > m - b + c - a,\ c \geqq m - b + a,$$

also

$$(31)\quad c \geqq b - a,\ 2c \geqq b + a,\ 2c > m,\ b + a > m,\ c \geqq m - b + a.$$

2. Es hat $\{a, b, c\}$ von den 4 Systemen mit c am Schluß sein zweites Element am kleinsten:

$$b \leqq m - b + c,$$

d. h.

$$(32)\quad c > 2b - m.$$

3. Es hat $\{a, b, c\}$ von den 2 Systemen mit b, c am Schluß sein erstes Element am kleinsten:

$$a < c - a,$$

d. h.

$$(33)\quad c \geqq 2a.$$

Von den 7 Relationen (31), (32), (33) kann

$$2c \geqq m$$

fortgelassen werden, als Folge aus

$$2c \geqq b + a,\ b + a \geqq m;$$

ferner kann

$$2c > b + a$$

fortgelassen werden, als Folge aus

$$c \geqq b - a,\ c \geqq 2a;$$

endlich kann

$$c > b - a$$

und

$$c \geqq m - b + a$$

fortbleiben, als Folge aus

$$c \geqq 2b - m,\ b + a \geqq m$$

bzw.

$$c \geqq 2a,\ b + a \geqq m.$$

Es bleibt also übrig:

(34) $$c \geq 2a,\ c \geq 2b - m,\ b + a \geq m,$$

nebst

(25) $$0 < a < c < b < m.$$

§ 4.

Nun hat (24), (25) für jedes gerade $m \geq 4$ die Lösung

(35) $$a, b = m - a,\ c = \frac{m}{2},$$

wo $1 \leq a < \frac{m}{2}$ ist. In der Tat ist (25) erfüllt, und für $(\rho, m) = 1$, $\rho a < \frac{m}{2} \pmod m$ ist

$$\rho b \equiv -\rho a > \frac{m}{2} \pmod m,$$

also

$$\rho a < \rho c < \rho b \pmod m;$$

für $(\rho, m) = 1$, $\rho a > \frac{m}{2} \pmod m$ ist

$$\rho b \equiv -\rho a < \frac{m}{2} \pmod m,$$

$$\rho a > \rho c > \rho b \pmod m.$$

Die Lösung (35) gibt Anlaß zu den 24 Lösungen (30), von denen aber nur höchstens sechs verschieden sind, nämlich

(36) $$\left\{a, m-a, \frac{m}{2}\right\},\ \left\{\frac{m}{2}-a, m-a, m-2a\right\},\ \left\{\frac{m}{2}-a, \frac{m}{2}+a, \frac{m}{2}\right\},$$
$$\left\{a, \frac{m}{2}+a, 2a\right\},\ \left\{\frac{m}{2}-a, m-a, \frac{m}{2}\right\},\ \left\{a, \frac{m}{2}+a, \frac{m}{2}\right\}.$$

Da nun a eine beliebige Zahl zwischen 0 (exkl.) und $\frac{m}{2}$ (exkl.) ist und die Substitution von $\frac{m}{2} - a$ an Stelle von a das erste bzw. zweite bzw. fünfte der Systeme (36) mit dem dritten bzw. vierten bzw. sechsten vertauscht, so brauchen nur drei beibehalten zu werden, z. B. das erste, vierte und sechste.

Jedem geraden $m \geq 4$ entsprechen also mindestens die folgenden Lösungen von (24), (25):

(37) $$\left\{a, m-a, \frac{m}{2}\right\},\ \left\{a, \frac{m}{2}+a, 2a\right\},\ \left\{a, \frac{m}{2}+a, \frac{m}{2}\right\}\left(1 \leq a \leq \frac{m}{2} - 1\right).$$

Der Satz des § 1 gestattet nun, den Nachweis zu führen:

Es hat (24), (25) für gerades $m > 60$ keine weitere Lösung mit den Nebenbedingungen $a = 1$, $c = \frac{m}{2}$ als die durch (37) gelieferten Lösungen

$$\left\{1, m-1, \frac{m}{2}\right\}, \quad \left\{1, \frac{m}{2}+1, \frac{m}{2}\right\}.$$

Also ist $F\left(\frac{1}{m}, \frac{b}{m}, \frac{1}{2}, x\right)$ für gerades $m > 60$, $\frac{m}{2}+1 < b < m-1$ transzendent.

Beweis: Es sei m gerade und $\left\{1, b, \frac{m}{2}\right\}$ eine Lösung von (24), (25). Dann ist

$$\frac{m}{2} < b < m$$

und für $(\rho, m) = 1$, $1 < \rho < \frac{m}{2}$

$$\rho < \frac{m}{2} < \rho\, b \pmod{m} \text{ oder } \rho > \frac{m}{2} > \rho\, b \pmod{m},$$

d. h., da $\rho < \frac{m}{2}$ ist,

$$\frac{m}{2} < \rho\, b \pmod{m}.$$

Wird

$$b = \frac{m}{2} + k$$

gesetzt, so ist

$$\rho\, b = \rho\frac{m}{2} + \rho\, k = \frac{m}{2} + \rho\, k \pmod{m},$$

$$k\rho < \frac{m}{2} \pmod{m}.$$

Das Zahlenpaar k, m erfüllt also genau die im § 1 gemachten Voraussetzungen: aus (6) folgt (5). Für gerades $m > 60$ kann also nur $k = 1$ oder $k = \frac{m}{2} - 1$ sein, was auf die schon oben hervorgehobenen, für alle geraden $m > 4$ giltigen (bei $m = 4$ zusammenfallenden) Systeme $\left\{1, \frac{m}{2}+1, \frac{m}{2}\right\}$ und $\left\{1, m-1, \frac{m}{2}\right\}$ führt.

Für die geraden m von 4 bis 60 gibt es nach den Resultaten des § 1 neben diesen Systemen nur noch die folgenden:

$$\begin{array}{llll} m = 12, & a = 1, & b = 9, & c = 6; \\ m = 20, & a = 1, & b = 13, & c = 10; \\ m = 20, & a = 1, & b = 17, & c = 10; \\ m = 24, & a = 1, & b = 17, & c = 12; \\ m = 24, & a = 1, & b = 19, & c = 12; \\ m = 60, & a = 1, & b = 41, & c = 30; \\ m = 60, & a = 1, & b = 49, & c = 30. \end{array}$$

Daß $F(\alpha, \beta, \gamma, x)$ für jene zwei Klassen und in diesen endlich vielen Fällen wirklich algebraisch ist, ergibt sich natürlich nicht aus dem Vorangehenden, ist aber direkt feststellbar; vgl. den § 5, wo (24) in allen durch die berühmte SCHWARZ'sche[13]) Tabelle gelieferten Fällen verifiziert wird. Das Wesentliche war, daß ich durch meinen Satz aus § 1 in Verbindung mit dem EISENSTEIN-HEINE'schen Satz in allen unendlich vielen übrigen Fällen den Transzendenzbeweis von $F\left(\frac{1}{m}, \frac{b}{m}, \frac{1}{2}, x\right)$, wo m gerade und $\frac{m}{2} < b < m$ ist, führen konnte.[14]) Es ist sehr interessant, daß hier die Anwendung des EISENSTEIN-HEINE'schen Kriteriums alle algebraischen Fälle liefert, daß also die notwendige Bedingung hier eine hinreichende ist. Das Hauptziel dieser Arbeit ist: 1. diesen Teil der SCHWARZ'schen Ergebnisse rein arithmetisch zu beweisen (was hiermit geschehen ist); 2. den an sich interessanten Satz des § 1 zu beweisen; 3. die am Schluß des § 5 ausgesprochene offene Frage zu formulieren und in ihrer Stellung zur Theorie der hypergeometrischen Reihe darzulegen.

§ 5.

Ich will nun verifizieren, daß (24) in allen der Bedingung (25) genügenden Fällen erfüllt ist, in denen auf Grund der SCHWARZ'schen Resultate $F(\alpha, \beta, \gamma, x)$ algebraisch ist. Das kann natürlich nicht anders sein, da ja (24) eine notwendige Bedingung

[13]) *Ueber diejenigen Fälle, in welchen die* GAUSS*sche hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt* [Journal für die reine und angewandte Mathematik, Bd. LXXV (1873), S. 292—335; Gesammelte Mathematische Abhandlungen, Bd. II (1890), S. 211—259], S. 323 bzw. S. 246.

[14]) Nach dem Vorangehenden ist damit natürlich auch der Transzendenzbeweis für alle $F(\alpha, \beta, \gamma, x)$ geliefert, wo α, β, γ sich von obigen Werten um ganze Zahlen unterscheiden.

dafür ist, daß $F(\alpha, \beta, \gamma, x)$ algebraisch ist; die Angabe der in Betracht kommenden Systeme a, b, c, m ist jedoch an sich interessant und wird auch Beziehungen zwischen verschiedenen Fällen der SCHWARZ'schen Tabelle liefern.

Das SCHWARZ'sche Ergebnis gipfelt in folgender Tabelle. Es werde angenommen, daß α, β, γ, $\gamma - \alpha$, $\gamma - \beta$, $\alpha - \beta$ und $\gamma - \alpha - \beta$ nicht ganz sind, und es werde

$$\lambda = |1 - \gamma|, \quad \mu = |\alpha - \beta|, \quad \nu = |\gamma - \alpha - \beta|$$

gesetzt, so daß keine der Zahlen λ, μ, ν ganz ist. Es sei λ' (bzw. μ', ν') der positiv gemessene Abstand der Zahl λ (bzw. μ, ν) von der nächstgelegenen geraden Zahl, so daß insbesondere

$$0 < \lambda' < 1, \quad 0 < \mu' < 1, \quad 0 < \nu' < 1$$

ist. Es werde dasjenige der vier Systeme

λ', μ', ν'; λ', $1 - \mu'$, $1 - \nu'$; $1 - \lambda'$, μ', $1 - \nu'$; $1 - \lambda'$, $1 - \mu'$, ν'

gewählt, welches die kleinste Summe hat[15]); diese drei Zahlen seien λ'', μ'', ν'' und zwar so geordnet, daß $\lambda'' \geq \mu'' \geq \nu''$ ist. Das SCHWARZ'sche Resultat lautet: $F(\alpha, \beta, \gamma, x)$ ist dann und nur dann algebraisch, wenn λ'', μ'', ν'' eines der folgenden 15 Systeme ist, von denen im ersten ein willkürlicher Buchstabe ν'' stehen bleibt, der eine beliebige positive rationale Zahl $< \frac{1}{2}$ bezeichnet:

	I	II	III	IV	V	VI	VII	VIII	IX	X
λ''	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{1}{2}$	$\frac{2}{3}$	$\frac{1}{2}$	$\frac{2}{5}$	$\frac{2}{3}$	1	3
μ''	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	1	1	$\frac{1}{3}$	1	2	$\frac{1}{3}$
ν''	ν''	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{5}$	3	$\frac{1}{5}$	$\frac{1}{5}$	$\frac{1}{5}$

	XI	XII	XIII	XIV	XV
λ''	$\frac{2}{5}$	$\frac{2}{3}$	$\frac{4}{5}$	$\frac{1}{2}$	$\frac{3}{5}$
μ''	$\frac{2}{5}$	$\frac{1}{3}$	$\frac{1}{5}$	$\frac{2}{5}$	$\frac{2}{5}$
ν''	$\frac{2}{5}$	$\frac{1}{5}$	$\frac{1}{5}$	1	1

[15]) Mit anderen Worten: Wenn unter den Zahlen λ', μ', ν' mindestens zwei zusammen > 1 sind, so werden die beiden größten Zahlen durch ihre Komplemente zu 1 ersetzt.

Ich behaupte zunächst, daß jedem dieser 15 Systeme genau ein System α, β, γ mit den durch (25) und (34) statuierten — erlaubten — Einschränkungen

$$(38) \quad 0 < \alpha < \gamma < \beta < 1, \ \gamma \geq 2\alpha, \ \gamma \geq 2\beta - 1, \ \beta + \alpha \geq 1$$

entspricht.

In der Tat ergibt sich aus (38) zunächst

$$\lambda = 1 - \gamma, \ \mu = \beta - \alpha, \ \nu = \beta - \gamma + \alpha,$$
$$\lambda' = 1 - \gamma, \ \mu' = \beta - \alpha, \ \nu' = \beta - \gamma + \alpha,$$

da ja die drei Zahlen $1 - \gamma$, $\beta - \alpha$, $\beta - \gamma + \alpha$ zwischen 0 und 1 liegen. Abgesehen von der Reihenfolge stimmt auch das System λ'', μ'', ν'' mit diesen drei Zahlen überein; denn es ist

$\lambda' + \mu' = 1 - \gamma + \beta - \alpha \leq 1$ wegen $\gamma \geq (2\beta - 1) + (1 - \beta - \alpha) = \beta - \alpha$,
$\lambda' + \nu' = 1 - 2\gamma + \beta + \alpha \leq 1$ wegen $2\gamma = \gamma + \gamma \geq (\beta - \alpha) + 2\alpha = \beta + \alpha$,
$\mu' + \nu' = 2\beta - \gamma \quad \leq 1$ wegen $\gamma \geq 2\beta - 1$.

Also ist λ'', μ'', ν'' abgesehen von der Reihenfolge gleich $1 - \gamma$, $\beta - \alpha$, $\beta - \gamma + \alpha$. Was nun die Reihenfolge betrifft, so ist

$$1 - \gamma \leq \beta - \gamma + \alpha \quad \text{wegen} \quad \beta + \alpha \geq 1,$$
$$\beta - \gamma + \alpha \leq \beta - \alpha \quad \text{wegen} \quad \gamma \geq 2\alpha.$$

Daher ist

$$\lambda'' = \beta - \alpha, \ \mu'' = \beta - \gamma + \alpha, \ \nu'' = 1 - \gamma,$$

$$(39) \quad \alpha = \frac{-\lambda'' + \mu'' - \nu'' + 1}{2}, \ \beta = \frac{\lambda'' + \mu'' - \nu'' + 1}{2}, \ \gamma = 1 - \nu'',$$

so daß einem System λ'', μ'', ν'' der Tabelle höchstens ein System α, β, γ mit den Nebenbedingungen (38) entspricht. Dies System (39) ist nun für jeden Fall der Schwarz'schen Tabelle tatsächlich so beschaffen, daß (38) gilt. Denn es ist in der Tabelle

$$1 > \lambda'' \geq \mu'' \geq \nu'' > 0, \ \lambda'' + \mu'' \leq 1, \ \lambda'' + \mu'' + \nu'' > 1,$$

und die zu verifizierenden Relationen (38) lauten, in die Bezeichnung λ'', μ'', ν'' übertragen,

$$0 < \frac{-\lambda'' + \mu'' - \nu'' + 1}{2} < \frac{2 - 2\nu''}{2} < \frac{\lambda'' + \mu'' - \nu'' + 1}{2} < 1,$$

$$1 - \nu'' \geq -\lambda'' + \mu'' - \nu'' + 1, \ 1 - \nu'' \geq \lambda'' + \mu'' - \nu'', \ \mu'' - \nu'' + 1 \geq 1.$$

Jede Nummer der Schwarz'schen Tabelle von II bis XV liefert also ein System $\{\alpha, \beta, \gamma\}$ mit den obigen Nebenbedingungen (38), d. h. $(a, b, c, m) = 1$ angenommen, genau ein System a, b, c, m mit den Nebenbedingungen (25) und (34). Bei Nr. I gilt dies auch für

jede bestimmte Wahl des willkürlichen positiven rationalen $\nu'' \leq \frac{1}{2}$; indem ich $\nu'' = \frac{u}{v}$ setze, wo $(u, v) = 1$, $0 < u < \frac{v}{2}$ ist, ist das entsprechende m offenbar $2v$.

So entsteht die Tabelle:

	I	II	III	IV	V	VI	VII	VIII	IX
α	$\frac{1}{2} - \frac{\nu''}{2}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{7}{24}$	$\frac{1}{6}$	$\frac{19}{60}$	$\frac{3}{10}$	$\frac{1}{6}$	$\frac{7}{20}$
β	$1 - \frac{\nu''}{2}$	$\frac{3}{4}$	$\frac{5}{6}$	$\frac{19}{24}$	$\frac{5}{6}$	$\frac{49}{60}$	$\frac{7}{10}$	$\frac{5}{6}$	$\frac{17}{20}$
γ	$1 - \nu''$	$\frac{2}{3}$	$\frac{2}{3}$	$\frac{3}{4}$	$\frac{3}{4}$	$\frac{4}{5}$	$\frac{2}{3}$	$\frac{4}{5}$	$\frac{4}{5}$
m	$2v$	12	6	24	12	60	30	30	20
a	$v - u$	3	1	7	2	19	9	5	7
b	$2v - u$	9	5	19	10	49	21	25	17
c	$2v - 2u$	8	4	18	9	48	20	24	16

	X	XI	XII	XIII	XIV	XV
α	$\frac{4}{15}$	$\frac{3}{10}$	$\frac{7}{30}$	$\frac{1}{10}$	$\frac{17}{60}$	$\frac{7}{30}$
β	$\frac{13}{15}$	$\frac{7}{10}$	$\frac{9}{10}$	$\frac{9}{10}$	$\frac{47}{60}$	$\frac{5}{6}$
γ	$\frac{4}{5}$	$\frac{3}{5}$	$\frac{4}{5}$	$\frac{4}{5}$	$\frac{2}{3}$	$\frac{2}{3}$
m	15	10	30	10	60	30
a	4	3	7	1	17	7
b	13	7	27	9	47	25
c	12	6	24	8	40	20

Nun bilden wir die bis zu 24 konjugierten Lösungen nach dem Schema (30); dabei wird sich zeigen, daß jede Nummer zu ganz anderen Lösungen Anlaß gibt[16]), und daß in jedem System konjugierter Lösungen das m dasselbe bleibt, d. h. kein gemeinsamer Teiler von m mit den drei Zahlen eines der 23 anderen Systeme (30) auftreten kann, wenn $(a, b, c, m) = 1$ ist.[17])

[16]) Dies ließe sich auch a priori einsehen, indem jedes der konjugierten Systeme, wenn man direkt aus den zugehörigen α, β, γ die Zahlen λ'', μ'', ν'' bildet, denselben λ'', μ'', ν'' entspricht.

[17]) Dies läßt sich auch der Tabelle (30) allgemein ansehen.

Nr. I hat als Ausgangssystem $\left\{\frac{m}{2} - u,\ m - u,\ m - 2u\right\}$ bei beliebigem geraden m und $1 \leq u \leq \frac{m}{4}$, $\left(u, \frac{m}{2}\right) = 1$. Die weiteren neuen konjugierten Systeme auf Grund von (30) sind

$$\left\{\frac{m}{2} - u,\ m - u,\ \frac{m}{2}\right\},\ \left\{u,\ m - u,\ \frac{m}{2}\right\},\ \left\{\frac{m}{2} - u,\ \frac{m}{2} + u,\ \frac{m}{2}\right\},$$

$$\left\{u,\ \frac{m}{2} + u,\ \frac{m}{2}\right\},\ \left\{u,\ \frac{m}{2} + u,\ 2u\right\}.$$

Diese Systeme kamen schon im § 4 vor.

Ich ordne nun die folgenden Nummern II bis XV nach wachsendem m. Es tritt auf: $m = 6$ bei III; $m = 10$ bei XI, XIII; $m = 12$ bei II, V; $m = 15$ bei X; $m = 20$ bei IX; $m = 24$ bei IV; $m = 30$ bei VII, VIII, XII, XV; $m = 60$ bei VI, XIV.

Nach dem Schema (30) ist die Anzahl der verschiedenen Fälle, zu denen die Nummern Anlaß geben, in folgender Aufstellung enthalten:

Nummer:	III	XI	XIII	II	V	X	IX	IV	VII	VIII	XII	XV	VI	XIV
Anzahl:	4	4	4	12	12	24	24	24	12	12	12	12	24	24

Also insgesamt[18]):

m:	6	10	12	15	20	24	30	60
Anzahl:	4	8	24	24	24	24	48	48

Die Aufzählung dieser Fälle verschiebe ich noch einen Augenblick, um zuvor zu sagen, wie sich ohne umständliche Rechnungen das Erfülltsein von (24) in ihnen verifizieren läßt. Es tritt näm-

[18]) Hierbei ist nicht zu vergessen, daß außerdem Nr. I noch Fälle liefert. Nämlich für jedes gerade m die Systeme

$$\left\{\frac{m}{2} - u,\ m - u,\ m - 2u\right\},\ \left\{\frac{m}{2} - u,\ m - u,\ \frac{m}{2}\right\},\ \left\{\frac{m}{2} - u,\ \frac{m}{2} + u,\ \frac{m}{2}\right\},$$

$$\left\{u,\ \frac{m}{2} + u,\ 2u\right\},\ \left\{u,\ m - u,\ \frac{m}{2}\right\},\ \left\{u,\ \frac{m}{2} + u,\ \frac{m}{2}\right\},$$

wo $1 \leq u \leq \frac{m}{4}$, $\left(u, \frac{m}{2}\right) = 1$ ist. Von diesen Systemen sind gleiche höchstens für $u = \frac{m}{4}$ (also im Falle $m \equiv 2 \pmod 4$ nie) vorhanden, wo sogar alle sechs zusammenfallen; $\frac{m}{4}$ ist aber nur im Falle $m = 4$ zu $\frac{m}{2}$ teilerfremd. Also liefert Nr. I für $m = 4$ ein System, für gerades $m \geq 6$ jedoch $6 \cdot \frac{1}{2}\varphi\left(\frac{m}{2}\right) = 3\varphi\left(\frac{m}{2}\right)$ Systeme.

lich der merkwürdige Umstand ein, daß die $\varphi(m)$ bei jeder einzelnen Verifikation aufzustellenden Hilfssysteme[19]) selbst schon in der Tabelle vorkommen. Deutlicher gesagt: Es ist für jede der $\varphi(m)$ Zahlen ρ, die den Relationen

$$(\rho, m) = 1,\ 1 < \rho < m$$

genügen, zu verifizieren, daß

$$\rho a < \rho c < \rho b \pmod{m} \text{ oder } \rho a > \rho c > \rho b \pmod{m}$$

ist; d. h. wenn die kleinsten positiven Reste von ρa, ρb, ρc (modulo m) mit a', b', c' bzw. b', a', c' bezeichnet werden, je nachdem $\rho a < \rho b \pmod{m}$ oder $\rho a > \rho b \pmod{m}$ ist, so ist zu verifizieren, daß jedesmal

$$a' < c' < b'$$

ist. Und nun trifft es sich zufällig, daß $\{a', b', c'\}$ jedesmal ein System der Tabelle ist, und zwar zu demselben m (aber nicht stets zu derselben römischen Nummer) gehört. Je $\varphi(m)$ bzw. weniger der Systeme meiner Tabelle sind also zusammengehörig; jedes erzeugt offenbar[20]) durch Multiplikation mit den ρ denselben Komplex. Ich habe also nur nötig, die Systeme meiner Tabelle übersichtlich in Komplexe zusammengehöriger zu ordnen, um nicht nur alle aufgezählt, sondern zugleich auch für jedes die Verifikation des Kriteriums (24) ausgeführt zu haben. Dabei entsteht eine neue Gruppierung der Schwarz'schen Resultate, bei der allerdings nur zwischen solchen verschiedenen Nummern seiner Tabelle manchmal ein Zusammenhang hergestellt wird, welche demselben regulären Polyeder entsprechen, wie z. B. bei $m = 30$ die Systeme $\{19, 25, 20\}$ und $\{5, 17, 10\}$ demselben Komplex angehören, aber den verschiedenen Fällen VIII und XV der Schwarz'schen Tabelle entsprechen.

Es werden sich, von den oben erledigten zu Nr. I gehörigen abgesehen, die sämtlichen Systeme, bei denen ich bisher nur die Anzahl genannt habe, gruppieren

bei $m = 6$ in 2 Komplexe von je 2 [zusammen 4],
bei $m = 10$ in 2 Komplexe von je 4 [zusammen 8],
bei $m = 12$ in 4 Komplexe von je 2 und 4 Komplexe von je 4 [zusammen 24],

[19]) Wenn auch nach dem Früheren die Verifikation für die erste Hälfte jener ρ genügt, so ist es mir doch jetzt bequem, sie alle in Betracht zu ziehen.

[20]) Denn wenn ρ_0 ein festes zu m teilerfremdes ρ zwischen 0 und m ist, so ist die Gesamtheit der Systeme $\{\rho_0 \rho a, \rho_0 \rho b, \rho_0 \rho c\}$ offenbar mit der Gesamtheit der Systeme $\{\rho a, \rho b, \rho c\}$ modulo m identisch.

bei m = 15 in 2 Komplexe von je 4 und 2 Komplexe von je 8 [zusammen 24],
bei m = 20 in 2 Komplexe von je 4 und 2 Komplexe von je 8 [zusammen 24],
bei m = 24 in 6 Komplexe von je 4 [zusammen 24],
bei m = 30 in 4 Komplexe von je 4 und 4 Komplexe von je 8 [zusammen 48],
bei m = 60 in 6 Komplexe von je 8 [zusammen 48].[21])

Die Komplexe sind nun folgende; ich bin bei der Aufzählung von irgendeinem System des Komplexes ausgegangen und habe über allen angegeben, durch Multiplikation mit welchen ρ (nebst Reduktion modulo m sowie eventueller Vertauschung der beiden ersten Elemente, damit $a < b$ ist) die einzelnen Systeme des Komplexes entstehen.

m = 6.

ρ	1	5	1	5
a	1	3	1	1
b	3	5	5	5
c	2	4	2	4

m = 10.

ρ	1	3	7	9	1	3	7	9
a	3	1	1	3	1	1	7	3
b	7	9	9	7	7	3	9	9
c	6	8	2	4	4	2	8	6

m = 12.

ρ	1	5	1	7	1	5	1	7	1	5	7	11	1	5	7	11
a	3	3	2	2	1	5	1	7	5	1	3	3	1	5	3	3
b	9	9	10	10	7	11	5	11	9	9	11	7	9	9	7	11
c	8	4	9	3	4	3	3	9	6	6	6	6	4	8	4	8

ρ	1	5	7	11	1	5	7	11
a	7	2	1	2	7	2	1	2
b	10	11	10	5	10	11	10	5
c	8	4	8	4	9	9	3	3

[21]) Zählt man die aus Nr. I entspringenden $3\varphi\left(\frac{m}{2}\right)$ bzw. 0 (letzteres für m = 15) Systeme hinzu, so ist die Gesamtzahl für m = 6, 10, 12, 15, 20, 24, 30, 60, bzw. 10, 20, 30, 24, 36, 36, 72, 72.

m = 15.

ρ	1	2	4	8	1	2	4	8	1	2	4	7	8	11	13	14
a	8	1	2	4	8	1	2	4	4	8	1	1	2	8	4	2
b	13	11	7	14	13	11	7	14	13	11	7	13	14	14	7	11
c	12	9	3	6	9	3	6	12	12	9	3	9	6	12	6	3

ρ	1	2	4	7	8	11	13	14
a	1	2	4	1	8	8	4	2
b	13	11	7	7	14	11	13	14
c	5	10	5	5	10	10	5	10

m = 20.

ρ	1	3	7	9	1	3	7	9	1	3	7	9	11	13	17	19
a	7	1	9	3	1	3	7	9	9	7	3	1	3	9	1	7
b	17	11	19	13	11	13	17	19	13	19	11	17	19	17	13	11
c	16	8	12	4	4	12	8	16	10	10	10	10	10	10	10	10

ρ	1	3	7	9	11	13	17	19
a	3	9	1	7	1	3	7	9
b	11	13	17	19	13	19	11	17
c	4	12	8	16	4	12	8	16

m = 24.

ρ	1	5	7	11	1	5	7	11	1	5	7	11	1	5	7	11
a	11	7	5	1	7	11	1	5	7	11	1	5	5	1	11	7
b	23	19	17	13	13	17	19	23	23	19	17	13	13	17	19	23
c	18	18	6	6	12	12	12	12	18	18	6	6	12	12	12	12

ρ	1	5	7	11	1	5	7	11
a	5	1	11	7	11	7	5	1
b	23	19	17	13	23	19	17	13
c	16	8	16	8	16	8	16	8

m = 30.

ρ	1	7	11	17	1	7	11	17	1	7	13	19	1	7	13	19
a	9	3	9	3	1	7	11	17	5	5	5	5	1	7	13	19
b	21	27	21	27	19	13	29	23	25	25	25	25	11	17	23	29
c	20	20	10	10	10	10	20	20	24	18	12	6	6	12	18	24

ρ	1	7	11	13	17	19	23	29	1	7	11	13	17	19	23	29
a	11	17	1	3	7	9	3	9	11	17	1	3	7	9	3	9
b	21	27	21	23	27	29	13	19	21	27	21	23	27	29	13	19
c	12	24	12	6	24	18	6	18	20	20	10	20	10	20	10	10

ρ	1	7	11	13	17	19	23	29	1	7	11	13	17	19	23	29
a	19	13	5	7	5	1	5	5	19	13	5	7	5	1	5	5
b	25	25	29	25	23	25	17	11	25	25	29	25	23	25	17	11
c	20	20	10	20	10	20	10	10	24	18	24	12	18	6	12	6

m = 60.

ρ	1	7	11	13	17	19	23	29	1	7	11	13	17	19	23	29
a	19	13	29	7	23	1	17	11	29	23	19	17	13	11	7	1
b	49	43	59	37	53	31	47	41	41	47	31	53	37	59	43	49
c	48	36	48	24	36	12	24	12	30	30	30	30	30	30	30	30

ρ	1	7	11	13	17	19	23	29	1	7	11	13	17	19	23	29
a	29	23	19	17	13	11	7	1	1	7	11	13	17	19	23	29
b	49	43	59	37	53	31	47	41	41	47	31	53	37	59	43	49
c	48	36	48	24	36	12	24	12	30	30	30	30	30	30	30	30

ρ	1	7	11	13	17	19	23	29	1	7	11	13	17	19	23	29
a	1	7	11	13	17	19	23	29	19	13	24	7	23	1	17	11
b	49	43	59	37	53	31	47	41	49	43	59	37	53	31	47	41
c	20	20	40	20	40	20	40	40	20	20	40	20	40	20	40	40

Der Fall I enthält unendlich viele Systeme {a, b, c} derart, daß die Bedingungen (24), (25) erfüllt sind. Abgesehen von diesen unendlich vielen Lösungen kenne ich nur die oben aufgezählten endlich vielen (es sind 204); diese entstanden aus den Nummern II bis XV der SCHWARZ'schen Tabelle. Es wäre sehr interessant festzustellen, ob es kein weiteres oder endlich viele weitere oder unendlich viele weitere gibt; ich weiß es nicht. Das Problem, alle Fälle zu finden, in denen $F(\alpha, \beta, \gamma, x)$ mit den Nebenbedingungen, daß α, β, γ rational, aber α, β, γ, $\gamma - \alpha$, $\gamma - \beta$ nicht ganz sind, algebraisch ist, würde rein arithmetisch gelöst sein, wenn es gelingt, zu beweisen: Für jedes ungerade $m > 60$ hat kein System und für gerades $m > 60$ haben nur die oben unter Nr. I gefundenen Systeme die Eigenschaft, daß

$$0 < a < c < b < m,\ (a,\ b,\ c,\ m) = 1$$

ist und mit jedem ρ, welches die Bedingungen

$$(\rho,\ m) = 1,\ 1 \quad \rho < \frac{m}{2}$$

erfüllt,

$$\rho a < \rho c < \rho b \pmod{m} \text{ oder } \rho a > \rho c > \rho b \pmod{m}$$

ist.

Göttingen, den 30. Juni 1911.

C. F. Wintersche Buchdruckerei.