ZAHLENTHEORETISCHE LÖSUNG EINER FUNCTIONENTHEORETISCHEN FRAGE.

Von **Alfred Errera** (Bruxelles).

Adunanza del 28 luglio 1912.

EINLEITUNG.

Gegeben sei die hypergeometrische Reihe:

$$(A) \qquad F = F(\alpha, \beta, \gamma, x) = 1 + \frac{\alpha\beta}{1\gamma}x + \frac{\alpha(\alpha+1)\beta(\beta+1)}{1 \quad 2 \quad \gamma(\gamma+1)}x^2 + \cdots.$$

Für welche Werte von α, β, γ ist die durch F bestimmte analytische Function algebraisch? Auf diese Frage, die man schon bei GAUSS [1]) auftauchen sieht, und die er für ganz specielle Werte gelöst hat, gab zuerst Herr SCHWARZ, in seiner grundlegenden Arbeit [2]), eine vollständige Antwort.

Um gewisse Specialfälle von vornherein ausschliessen zu können, möchte ich folgendes vorausschicken:

1. γ darf überhaupt nicht Null oder eine negative ganze Zahl sein; dies sei ein für allemal gesagt.

2. Ist α Null oder eine negative ganze Zahl, so ist F stets algebraisch; dasselbe gilt für β.

3. Ist α eine positive ganze Zahl, so ist F stets algebraisch; dies folgt aus 2. und aus einer der « relationes [3]) inter functiones contiguas »:

$$(B) \qquad \begin{cases} (\gamma - 2\alpha - (\beta - \alpha)x)F(\alpha, \beta, \gamma, x) \\ + \alpha(1-x)F(\alpha+1, \beta, \gamma, x) - (\gamma - \alpha)F(\alpha - 1, \beta, \gamma, x) = 0; \end{cases}$$

dasselbe gilt für β.

---

[1]) GAUSS, *Disquisitiones generales circa seriem infinitam* $1 + \frac{\alpha\beta}{1.\gamma}x + \ldots$ [Commentationes societatis regiae scientiarum Gottingensis recentiores, Bd. II (1813); *Werke*, Bd. III, pp. 123-162].

[2]) H. A. SCHWARZ, *Ueber diejenigen Fälle, in welchen die* GAUSS*sische hypergeometrische Reihe eine algebraische Function ihres vierten Elementes darstellt* [Journal für die reine und angewandte Mathematik, Bd. LXXV (1873), pp. 292-335; *Gesammelte mathematische Abhandlungen* (Berlin, Springer), Bd. II (1890), pp. 211-259].

[3]) L. c. [1]), p. 9 bezw. p. 130.

4. Ist $\alpha - \gamma$ eine ganze Zahl m, also $\alpha = \gamma + m$, so ist F eine rationale Function von $F(\gamma, \beta, \gamma, x)$, $F(\gamma+1, \beta, \gamma, x)$ und x: im Allgemeinen ist die mehrmalige Anwendung der Relation (B) nötig, um dies einzusehen. Aber man sieht leicht, dass

$$F(\gamma, \beta, \gamma, x) = (1 - x)^{-\beta}$$

und dass

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

ist. F ist also algebraisch, wenn β rational ist. Ebenso, wenn $\beta - \gamma$ ganz ist, so ist F, für rationales α, algebraisch.

Es sei jetzt keine der Zahlen α, β, $\alpha - \gamma$, $\beta - \gamma$ ganz. Dann hat Herr SCHWARZ [4]) zunächst gezeigt, dass α, β, γ rational sein müssen. Diese Bedingungen wollen wir von jetzt ab als erfüllt betrachten.

Unter Benutzung des EISENSTEIN-HEINEschen Satzes gab Herr LANDAU [5]) in diesem allgemeinen Falle [6]) ein einfaches notwendiges Criterium dafür, dass die Reihe algebraisch ist: setzt man nämlich

$$\alpha = \frac{a}{m}, \qquad \beta = \frac{b}{m}, \qquad \gamma = \frac{c}{m}, \qquad (a, b, c, m) = 1$$

und sind a_1, b_1, c_1 die kleinsten positiven Reste von a, b, c (mod. m), so muss c_1 zwischen a_1 und b_1 liegen.

Von zwei verschiedenen Seiten wurde kürzlich dies Criterium ergänzt: von Herrn STRIDSBERG [7]) und von Herrn LANDAU [8]) selbst. Um LANDAUS bequeme Schreibweise [9]) zu benutzen, wollen wir es nun so aussprechen: notwendig ist, dass für jede Zahl ρ, die zu m teilerfremd ist,

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

gilt. Dies wollen wir kurz die « ρ-Bedingung » nennen. Für $\rho = 1$ erhalten wir das alte Criterium von Herrn LANDAU [10]).

---

4) L. c. [2]), p. 298 bezw. p. 218.

5) E. LANDAU, *Eine Anwendung des* EISENSTEIN*schen Satzes auf die Theorie der* GAUSS*schen Differentialgleichung* [Journal für die reine und angewandte Mathematik, Bd. CXXVII (1904), pp. 92-102].

6) Den Fall, dass γ eine positive ganze Zahl ist, werden wir etwas später [1]) besprechen.

7) E. STRIDSBERG, *Sur le théorème d'*EISENSTEIN *et l'équation différentielle de* GAUSS [Arkiv för Matematik, Astronomi och Fysik, Bd. VI (1910-1911), Nr. 35: pp. 1-17].

8) E. LANDAU, *Über einen zahlentheoretischen Satz und seine Anwendung auf die hypergeometrische Reihe* [Sitzungsberichte der Heidelberger Akademie der Wissenschaften, 1911, 18. Abhandlung].

9) L. c. [8]), p. 3; auch hier gegen Ende der Einleitung.

10) STRIDSBERG, l. c. [7]), p. 3, nimmt an, dass auch keine der Zahlen γ, $\alpha - \beta$, $\alpha + \beta - \gamma$ ganz ist, LANDAU, l. c. [5]), p. 96 und l. c. [8]), p. 18, dass γ nicht ganz ist. Diese Nebenbedingungen sind überflüssig, die zweite und die dritte, weil LANDAU sie nicht benutzt hat; er hat sie in seiner Arbeit, l. c. [5]), p. 96, nur erwähnt; die erste, weil seine Beweise auch ohne sie fast ungeändert gelten: denn, es sei γ eine ganze Zahl, also m ein Teiler von c; so braucht man in diesem Falle nur $\gamma_0 = p - \frac{c}{m}$ zu setzen; es ist also $c_0 = m$; dann schreitet der Beweis fort und führt zur ρ-Bedingung. Diese schliesst

Diese Bedingung ist also notwendig: wenn man alle Fälle, die ja Herr SCHWARZ [11]) aufgezählt hat (wobei α, β, $\gamma-\alpha$, $\gamma-\beta$ nicht ganz sind) in eine Tabelle für a, b, c, m umschreibt, so ist jedesmal die ρ-Bedingung erfüllt.

Herr STRIDSBERG [12]) hatte schon folgendes gezeigt: die ρ-Bedingung ist hinreichend dafür, dass das EISENSTEIN-HEINEsche Criterium erfüllt ist. Es fehlte aber noch der Nachweis, dass das letztere für die Algebraicität bürgt, um diese Reihe von Sätzen abzuschliessen.

Vor etwa zwei Jahren stellte mir Herr LANDAU in Anschluss an seine noch nicht erschienene Arbeit [8]) folgende Frage: Was sind alle Systeme von vier Zahlen a, b, c, m, die die ρ-Bedingung erfüllen? Lautet die Antwort: es gibt kein System ausser den SCHWARZschen, (die man sich wieder in a, b, c, m umgeschrieben denken muss), so folgt aus dem Erfülltsein der ρ-Bedingung, dass die Reihe algebraisch ist; sonst nicht.

Es ist mir jetzt gelungen, dies Problem der elementaren Zahlentheorie zu lösen, und zwar in dem oben angeführten Sinn: es ist in der Tat die ρ-Bedingung notwendig und hinreichend [13]). Die vorliegende Arbeit soll diese Behauptung rechtfertigen.

Ich möchte noch hinzufügen, dass für folgende Specialfälle der Satz schon bewiesen war: von Herrn STRIDSBERG [14]), falls m höchstens etwa sechs verschiedene Primfactoren enthält; von Herrn LANDAU [15]), falls $c=\frac{m}{2}$ und a (oder b) zu m teilerfremd ist. Von diesen schon bekannten Sätzen wird hier kein Gebrauch gemacht, wohl aber von LANDAUS Bezeichnungen und von vielen Gedanken, die seine Arbeit enthält.

Von der Einteilung des Beweises will ich folgendes sagen: § 1 enthält zwei Hilfssätze sehr verschiedener Natur, die nachher oft angewandt werden; § 2 einen speciellen Hilfssatz und fünf Sätze über die Verteilung gewisser Zahlen modulo m; dies genügt, um das Problem in Angriff zu nehmen und in den verschiedenen Fällen zu lösen, was in § 3 geschieht. Gewisse Hilfssätze werden etwas allgemeiner gefasst, als für das übrige nötig wäre, da ihre Beweise dabei nicht wesentlich geändert werden.

Ich möchte folgende nicht überall gebräuchliche Bezeichnungen aufzählen:
$(a_1, a_2, \ldots, a_n)$ ist der grösste gemeinsame Teiler aller Zahlen a $(n>1)$;
$a \mid b$, bezw. $a \nmid b$: a teilt b, bezw. a teilt nicht b;
$x<y$, bezw. $x>y$ (mod. z): von den kleinsten positiven Resten von x und y (mod. z) hat x bezw. y den kleineren.

Bis auf Weiteres soll man sich alle Zahlen ganz und positiv denken.

Ich möchte diese Gelegenheit benutzen, um meinen verbindlichsten Dank Herrn Prof.

---

von selbst die drei fraglichen Fälle aus: γ ganz, denn c_0 muss $<a_0$ oder b_0, also $<m$ sein; $\alpha-\beta$ ganz, denn dann wäre $a\equiv b$ (mod. m); $\alpha+\beta-\gamma$ ganz, denn dann wäre $a+b\equiv c$ (mod. m), was nicht der Fall sein kann, denn es ist $c_0<a_0+b_0<c_0+m$.

[1]) L. c. [2]), p. 323 bezw. p. 246. Für die umgeschriebene Tabelle s. l. c. [8]), p. 33 und pp. 35-37.

[12]) L. c. [7]), pp. 8-10.

[13]) Dies vermutete Herr STRIDSBERG, l. c. [7]), pp. 15-16.

[14]) L. c. [7]), p. 15.

[15]) L. c. [8]), pp. 28-29.

Dr. LANDAU, für die grosse Liebenswürdigkeit, die er mir stets, und auch im Falle dieser Arbeit, bewiesen hat, auszusprechen.

Diese, meine erste selbständige Arbeit, widme ich in tiefster Ehrfurcht dem Andenken meines lieben Vaters.

§ 1.

1. HILFSSATZ I [16]). — *Gegeben die positiven Zahlen* c, n, k. *Man bezeichne mit* $N(c, n, k)$ *die Anzahl der zu* c *teilerfremden Glieder unter* c *consecutiven Gliedern der Progression*

$$k + xn \qquad (x = 0, 1, 2, \ldots).$$

Behauptung:

I) $N(c, n, k) = 0$, *falls* $(c, n, k) > 1$ *ist.*

II) $N(c, n, k) = \frac{\varphi(cn)}{\varphi(n)}$, *für alle* k, *für welche* $(c, n, k) = 1$ *ist.*

Beweis: Wir dürfen natürlich annehmen, dass $k \leqq n$ ist.

I) Der Beweis ist evident.

II) Es sei $(k, n) = d > 1$, $k = dk_1$, $n = dn_1$, wobei $(c, d) = 1$ und $(k_1, n_1) = 1$ sind. Wir dürfen alle Glieder der Progression durch d teilen, ohne Einfluss auf die Teilerfremdheit zu c. Und:

$$N(c, n, k) = N(c, n_1, k_1).$$

Aber aus $(c, d) = 1$ folgt:

$$\frac{\varphi(cn)}{\varphi(n)} = \frac{\varphi(cdn_1)}{\varphi(dn_1)} = \frac{\varphi(cn_1)}{\varphi(n_1)}.$$

Es bleibt zu beweisen, dass $N(c, n_1, k_1) = \frac{\varphi(cn_1)}{\varphi(n_1)}$ ist, d. h.: dass der Satz im Falle $d = 1$ gilt.

Es sei also $(k, n) = 1$.

Ist $n = 1$, also $k = 1$, so ist

$$N(c, n, k) = \varphi(c) = \frac{\varphi(cn)}{\varphi(n)}.$$

Es sei $n > 1$, also $n > k \geqq 1$, wobei es $\varphi(n)$ Möglichkeiten für k gibt, welche $\varphi(n)$ Progressionen liefern, deren Glieder alle zu n teilerfremd sind. In diesen Progressionen liegen $\varphi(cn)$ zu cn, also zu c teilerfremde Zahlen. Es bleibt also nur zu beweisen, dass in irgend zwei der Progressionen ebensoviele zu c teilerfremde Zahlen liegen.

Es sei also $(k, n) = 1$, $(k', n) = 1$, $k < k' < n$, $k' - k = l$. Und es sei $c = c_1 c_2$, wo $(c_1, n) = 1$ ist und c_2 nur Primfaktoren von n enthält.

Die Bestimmungscongruenz $ny + l \equiv 0 \pmod{c_1}$ hat stets eine Lösung y_1. Zu

[16]) Dieser Satz rührt von Herrn FROBENIUS her; er hat ihn in etwas anderer Form entdeckt, aber nicht publiciert; er soll ihn in einer Vorlesung erwähnt haben.

jeder zu c teilerfremden Zahl $k + xn$ addieren wir $l + y_1 n$; das ergibt eine Zahl $k' + x'n$, $(x' = x + y_1)$, die zu c_1 und zu n, also auch zu c teilerfremd ist. Diese Beziehung zwischen den zwei Progressionen ist ein-eindeutig.

$$N(c, n, k) \text{ ist also von } k \text{ unabhängig und} = \frac{\varphi(cn)}{\varphi(n)}, \qquad \text{Q. E. D.}$$

Corollar: im Falle $(c, n, k) = 1$ ist stets $N(c, n, k) \geqq 1$.

2. HILFSSATZ II. — *Gegeben die Zahlen c und m, $0 < c < m$. Es heissen ρ-Zahlen die Zahlen, die zu m teilerfremd sind.*

Behauptung: Es existiert stets ein ρ, sodass der kleinste positive Rest von ρc (mod. m) *in m aufgeht.*

Beweis: Ist c ein ρ, so gibt es ein ρ' mit der Bedingung:

$$\rho\rho' \equiv 1 \pmod{m}.$$

Es sei jetzt $(c, m) = d > 1$, $c = \gamma d$, $m = \mu d$, wobei $(\gamma, \mu) = 1$ ist. Wir definieren γ' durch die Congruenz:

$$\gamma\gamma' \equiv 1 \pmod{\mu}.$$

Es ist also $(\mu, \gamma') = 1$. Nach dem Corollar zum ersten Hilfssatze gibt es, wegen $(d, \mu, \gamma') = 1$, mindestens ein Glied in der Progression $\gamma' + x\mu$, $(x < d)$, das zu d teilerfremd ist. $\rho_1 = \gamma' + x_1\mu$ sei ein solches. Hieraus folgt:

$$c\rho_1 = \gamma\gamma' d + x_1\gamma\mu d \equiv d \pmod{\mu d = m}, \qquad \text{Q. E. D.}$$

§ 2.

3. HILFSSATZ III. — *Gegeben sei eine feste Zahl $a > 1$. Es sei b eine Zahl, die mindestens einen Primfactor $p \equiv 1$* (mod. a) *enthält. Es heissen t_b die Zahlen, die zu b teilerfremd sind und T_b die Anzahl der t_b mit der Bedingung:*

$$x\frac{b}{a} < t_b < (x+1)\frac{b}{a}, \qquad (x \geqq 0).$$

Behauptung: $T_b = \frac{\varphi(b)}{a}$, unabhängig von x.

Beweis: Wir benutzen folgende Induction:

1) ist der Satz richtig für eine Zahl $b > a$, so ist er es auch für qb, wo q irgend eine Primzahl ist; hieraus folgt, dass er für jedes Multiplum von b gilt; 2) er ist richtig für jede Primzahl p, wo $p \equiv 1$ (mod. a) ist; es ist $p > a$.

1) Voraussetzung:

$$T_b = \frac{\varphi(b)}{a}, \quad b > a.$$

Behauptung:

$$T_{qb} = \frac{\varphi(qb)}{a}.$$

1, 1) $q \mid b$. Die t_{qb} sind genau die t_b. Es ist also T_{qb} die Anzahl der t_b:

$$\frac{x\,q\,b}{a} < t_b < \frac{(x+1)\,q\,b}{a}.$$

Dies Intervall mit der Länge $\frac{q\,b}{a}$ zerfällt in q Intervalle mit der Länge $\frac{b}{a}$, und die t_b zerfallen in q Classen τ_i, $i = 1, 2, \ldots, q$:

$$\frac{xqb}{a} < \tau_1 \leqq \frac{(xq+1)b}{a} < \tau_2 \leqq \cdots \leqq \frac{(xq+i-1)b}{a} < \tau_i \leqq \frac{(xq+i)b}{a} < \cdots < \tau_q < \frac{(xq+q)b}{a}.$$

Die Gleichheitszeichen sind aber ausgeschlossen; denn: entweder ist eine Zahl $\frac{(x\,q+i)\,b}{a}$ nicht ganz, also kein t_b; oder sie ist ganz; dann ist sie, wegen $b > a$, nicht zu b teilerfremd, also wieder kein t_b. Es ist also:

$$T_{qb} = q\,T_b = \frac{q\,\varphi(b)}{a} = \frac{\varphi(q\,b)}{a}.$$

Die Induction ist erlaubt, weil a fortiori $q\,b > a$ ist.

1, 2) $q \nmid b$. Die t_{qb} sind genau diejenigen t_b, die zu q teilerfremd sind. Genau wie vorhin beweisen wir, dass $q\,T_b$ die Gesamtanzahl der t_b

$$\frac{x\,q\,b}{a} < t_b < \frac{(x+1)\,q\,b}{a}$$

ist. Bezeichnen wir mit X die Anzahl der t_b, die nicht zu q teilerfremd sind, so ist also:

$$T_{qb} = q\,T_b - X.$$

Aber es ist X die Anzahl der t_b, die durch q teilbar sind, wo wiederum

$$\frac{x\,q\,b}{a} < t_b < \frac{(x+1)\,q\,b}{a}$$

ist. Wenn wir diese t_b durch q dividieren, so bekommen wir genau alle t_b, wo

$$\frac{x\,b}{a} < t_b < \frac{(x+1)\,b}{a}$$

ist. Es ist daher $X = T_b$, also:

$$T_{qb} = (q-1)\,T_b = \frac{(q-1)\,\varphi(b)}{a} = \frac{\varphi(q\,b)}{a}.$$

Und es ist wieder, wegen $q\,b > a$, die Induction erlaubt.

2) $b = p \equiv 1 \pmod{a}$. Behauptung:

$$T_b = \frac{b-1}{a}.$$

Es gibt keine ganze Zahl y, sodass $\frac{x}{a} < y < \frac{x+1}{a}$ ist, also auch kein Multiplum by von b, sodass $\frac{x\,b}{a} < by < \frac{(x+1)\,b}{a}$ ist. Es ist also, da b eine Primzahl ist,

jede ganze Zahl ζ:

$$\frac{xb}{a} < \zeta < \frac{(x+1)b}{a},$$

zu b teilerfremd, also ein t_b. Es ist also T_b die Anzahl der ganzen Zahlen ζ, also die Anzahl der Multipla ζa von a, für welche $xb < \zeta a < (x+1)b$ ist. Anderseits ist $\frac{b-1}{a}$ die Anzahl der Multipla von a unter $b-1$ consecutiven Zahlen, wegen $a \mid b-1$. Es ist also:

$$T_b = \frac{b-1}{a} = \frac{\varphi(b)}{a},$$ Q. E. D.

Anmerkung: diesen Satz werden wir für $a = 6$ benutzen [17]).

4. SATZ I. — *Gegeben sind die Zahlen* $c > 1$ *und* $n \geq k \geq 1$ *mit der Bedingung*

$$(k, n) = 1. \tag{1}$$

Es heissen R-Zahlen die Zahlen

$$k, \quad k+n, \quad k+2n, \ \ldots, \ k+(c-1)n;$$

ihre Anzahl ist c; *es heissen r-Zahlen diejenigen unter den R, die zu c teilerfremd sind; die r sind also durch folgende Bedingungen definiert:*

$$0 < r < cn, \tag{2}$$

$$r \equiv k \pmod{n}, \tag{3}$$

$$(r, c) = 1. \tag{4}$$

Es heisse q *ihre Anzahl und* s *die Anzahl der* r, *welche* $< c$ *sind.*

Behauptung:

A) Im Falle $n > k$:

I) *Falls* $c > n$ *ist, so ist stets* $s \leq \frac{q}{2}$;

II) *Falls* $c \leq n$ *ist, so ist auch* $s \leq \frac{q}{2}$ *oder* $s = q$.

B) Im Falle $n = k$ *ist stets* $s = q$.

Vorbemerkungen:

1) Im Laufe des Beweises wollen wir in der Form von eingeschachtelten Zusätzen, die wenigen Fälle aufzählen, wo $s = \frac{q}{2}$ oder $s = q$ ist, da eben dies für das Spätere am wichtigsten ist.

2) Der Sinn des Satzes ist, dass im Allgemeinen mehr r-Zahlen zwischen c und nc als zwischen 0 und c liegen.

---

[17]) Derselbe Satz gilt auch wenn b durch a^2, statt durch p, teilbar ist. Es gilt dieselbe Induction, da wiederum $b > a$ ist, und es ist nur noch zu zeigen, dass der Satz für $b = a^2$ richtig ist. Das ist aber eine Trivialität: T_{a^2} ist die Anzahl der t_{a^2}, also der t_a: $xa < t_a < xa + a$. Es ist also $T_{a^2} = \varphi(a) = \frac{\varphi(a^2)}{a}$. Dagegen genügt es nicht, dass $a \mid \varphi(b)$ ist, um den Satz behaupten zu können: für $a = 4$, $b = 21$ ist $\frac{\varphi(b)}{a} = 3$; für $x = 0$ ist $T_{21} = 4 \neq 3$.

3) Die Buchstaben $R', \ldots, r', \ldots$ wollen wir für specielle R- und r-Zahlen reservieren.

4) Wegen (1) ist $(c, n, k) = 1$. Also nach dem Corollar des 1. Hilfssatzes ist

$$q = \frac{\varphi(cn)}{\varphi(n)} \geqq 1.$$

Beweis:

A) $n > k$, also $n > k \geqq 1$.

Wir setzen $(c, n) = d$, $c = dc_1$, $n = dn_1$; es ist $(c_1, n_1) = 1$.

I) $c > n$ also $c_1 > n_1$ folglich $c_1 \geqq 2$.

1) $d > 1$.

Bezeichnen wir mit r' die r-Zahlen $< cn_1 = c_1 n$; so können wir jedem r' ein

$$\zeta = r' + cn_1 = r' + c_1 n, \quad cn_1 < \zeta < 2cn_1$$

zuordnen; ζ ist eine r-Zahl. Jedem $r < cn_1$ entspricht also ein $r > cn_1$; a fortiori, jedem $r < c$ ein $r > c$. Es gibt also mindestens soviele $r > c$ als $r < c$, in Zeichen:

$$q - s \geqq s, \quad \text{folglich} \quad s \leqq \frac{q}{2}.$$

Zusatz: Wann gilt das Gleichheitszeichen?

1, 1) $d \geqq 3$.

Jedem r' ordnen wir noch die Zahl $r' + 2cn_1 = r' + 2c_1 n$ zu; sie ist auch ein r; hieraus folgt analog $s \leqq \frac{q}{3} < \frac{q}{2}$.

1, 2) $d = 2$.

Es ist $c = 2c_1$, $n = 2n_1$, k ungerade. Wegen $c > 1$ und (4) sind c und cn_1 keine r-Zahlen. Wegen $2cn_1 = cn$ ist $\frac{q}{2}$ die Anzahl der $r < cn_1$. Aber s ist die Anzahl der $r < c$. Es ist also $s = \frac{q}{2}$ dann und nur dann, wenn das Intervall $c \leqq x < cn_1$ oder, was dasselbe ist, $c < x < cn_1$ von r-Zahlen frei ist. Wann ist dies erfüllt?

Die Antwort wird lauten:

$$\text{für} \quad n_1 = 1;$$

$$\text{für} \quad n_1 = 2, \quad c_1 = 3;$$

sonst nie. Beweis:

1, 2, 1) Für $n_1 = 1$ ist es klar, da $c = cn_1$ ist. Es ist also $s = \frac{q}{2}$ für $n = 2$, c gerade, $k = 1$.

1, 2, 2) Für $n_1 = 2$ ist $n = 4$. Aus $(c_1, n_1) = 1$ folgt: c_1 ungerade, $c \equiv 2 \pmod 4$; aus $c > n$ folgt: $c \geqq 6$; aus (1) folgt: $k = 3$ oder 1.

$k = 3$ ist unzulässig, denn sonst wäre $2c - 1$ ein r zwischen c und $2c$.

Es sei jetzt $k = 1$: es soll kein r zwischen c und $2c$ geben; aber mit jedem $r > 2c$ ist $r - 2c$ auch eine r-Zahl; es darf also kein r zwischen $3c$ und $4c$ liegen. Dafür ist notwendig und hinreichend, dass es kein x gibt, sodass:

$$0 < x < c, \qquad (x, c) = 1, \qquad x \equiv 3 \pmod 4$$

ist.

Entweder ist $\frac{c}{2} \equiv 1 \pmod 4$: so ist $\frac{c}{2} - 2$ ein x.

Oder $\frac{c}{2} \equiv 3 \pmod 4$, $c > 6$: so ist $\frac{c}{2} - 4$ ein x.

Oder $c = 6$: dann gibt es kein x. Und in der Tat ist $s = \frac{q}{2}$ für $n = 4$, $c = 6$, $k = 1$, da $r = 1, 5, 13, 17$ ist.

1, 2, 3) Für $n_1 \geqq 3$ ist $n \geqq 6$, $c \geqq 8$. Behauptung: das Intervall ist nicht frei.

1, 2, 3, 1) Es sei c_1 gerade. Nach dem Corollar des 1. Hilfssatzes gibt es mindestens eine Zahl x, sodass

$$0 < x < n c_1, \qquad x \equiv k \pmod n, \qquad (x, c_1) = 1$$

ist, da $(c_1, n, k) = 1$ ist, wegen (1). Jedes solche x ist zu n, also zu $d = 2$, also zu c teilerfremd; daher ist es ein r.

Es gibt also mindestens ein $r < n c_1$. Ist dies $r > c$, so sind wir fertig. Ist dagegen dies $r < c$, so ist $r + c_1 n_1 = y$ ein r im Intervall, denn:

$$0 < c < 3 c_1 \leqq c_1 n_1 < y < c + c_1 n_1 < 2 c_1 n_1 = c n_1 < cn;$$

$$y \equiv r \equiv k \pmod n,$$

da c_1 gerade ist;

$$(y, c_1) = (r, c_1) = 1,$$

also $(y, c) = 1$, da y ungerade ist, wegen c_1 gerade. Es gibt also ein r im Intervall.

1, 2, 3, 2) Es sei c_1 ungerade, also $(c_1, n) = 1$. In diesem Falle bilden diejenigen R-Zahlen, die $< c_1 n = c n_1$ sind, nämlich

$$k, \quad k + n, \quad \ldots, \quad k + (c_1 - 1)n,$$

ein vollständiges Restsystem mod. c_1. Unter diesen ist eine, sie heisse R', durch c_1 teilbar. Es gibt zwei Möglichkeiten:

$$\text{entweder} \quad R' \neq c_1:$$

dann ist $c = 2 c_1 \leqq R' < n c_1$; aber der Bedingung $2 c_1 \leqq R < n c_1$ genügen mindestens zwei consecutive R-Zahlen, da die Länge des Intervalls

$$(n - 2) c_1 \geqq 4 c_1 = 2 c > 2 n$$

ist; zu diesem Intervalle gehört also mit R', auch $R' - n$ oder $R' + n$ (oder beide); diese Zahlen sind ungerade, weil n gerade, k ungerade ist, und zu c_1, also zu c teilerfremd; es gibt also mindestens ein r im Intervalle;

$$\text{oder} \quad R' = c_1:$$

dann ist $c_1 \equiv k \pmod n$; aber die Zahl

$$x = c_1 + \frac{c_1 - 1}{2} n = c_1 + (c_1 - 1) n_1 = c_1 n_1 + c_1 - n_1$$

hat folgende Eigenschaften:

$$x \equiv k \pmod n,$$

da $\frac{c_1 - 1}{2}$ ganz ist;

$$(x, c) = 1,$$

da $(x, c_1) = (n_1, c_1) = 1$ ist und da $(x, 2) = 1$ ist, wegen c_1 ungerade;

$$c = 2c_1 < 3c_1 \leqq c_1 n_1 < x < (n_1 + 1)c_1 < nc_1 < cn;$$

es ist also x ein r im Intervalle.

Es ergeben sich also im Falle 1) für $s = \frac{q}{2}$ nur zwei Möglichkeiten: $n = 2$, c gerade, $k = 1$ oder $n = 4$, $c = 6$, $k = 1$.

Fortsetzung des Beweises: 2) $d = 1$ oder $(c, n) = 1$. Nach der 4. Vorbemerkung ist $q = \varphi(c)$.

In diesem Falle bilden die R ein vollständiges Restsystem (mod. c); also belegen die r alle teilerfremden Restclassen (mod. c). Es heisse x das R, das c als Factor enthält. Wir bestimmen y durch $y \equiv x + \frac{cn}{2}$ (mod. cn) und $0 \leqq y < cn$, wobei y nicht ganz zu sein braucht.

$x - z$ sei eine r-Zahl. Wir behaupten, dass der Rest von $x + z$ (mod. cn) auch eine r-Zahl ist; denn, wegen $x - z \equiv k$ und $x \equiv k$, ist $x + z \equiv k$ (mod. n), und, wegen $(x - z, c) = 1$ und $c \mid x$, ist $(x + z, c) = 1$. Dies gilt auch umgekehrt; wir können kurz sagen, dass die r-Zahlen in Bezug auf x symmetrisch liegen. Es gibt also genau soviele r-Zahlen zwischen x excl. und y excl. (mod. cn) als zwischen y excl. und x excl. (mod. cn). Ferner: x ist kein r, wegen $c \mid x$; und y ist kein r, denn: entweder c ist ungerade; dann ist $y \not\equiv x \equiv k$ (mod. n); oder c ist gerade; also, wegen $c > n > 1$ und n ungerade, ist $c \geqq 4$; also ist $(y, c) = \frac{c}{2} \neq 1$. Da die Endpunkte der Intervalle $x \ldots y$ und $y \ldots x$ (mod. cn) keine r-Zahlen sind, und da es im ganzen q Werte von r gibt, so können wir sagen, dass genau $\frac{q}{2}$ Werte von r in jedem dieser Intervalle excl. Endpunkte liegen.

Es ist $x \not\equiv 0$ (mod. cn), sonst wäre $n \mid x$ also $n \mid k$. Es ist also $c \leqq x < cn$.

2, 1) n gerade, also c ungerade.

y ist ganz; $c \mid x$ und $c \mid y$. Das Intervall $0 \ldots c$ liegt ganz in einem der zwei Intervalle $x \ldots y$ oder $y \ldots x$ (mod. cn), wobei ein oder gar zwei gemeinsame Endpunkte nicht ausgeschlossen sind. Also kann $0 \ldots c$ excl. Endpunkte höchstens $\frac{q}{2}$ Werte von r enthalten, in Zeichen: $s \leqq \frac{q}{2}$.

Zusatz: Wann ist genau $s = \frac{q}{2}$?

Es sei $n = 2$, also $x = c$, $y = 0$. Hier ist stets $s = \frac{q}{2}$.

Es sei $n > 2$, also $n \geqq 4$. Behauptung: $s < \frac{q}{2}$.

2, 1, 1) $y = 0$, also $x = \frac{cn}{2} \geqq 2c$. Es wäre $s = \frac{q}{2}$ dann und nur dann, wenn es kein r zwischen c und x gäbe. Aber $x - n$ ist ein solches r.

2, 1, 2) $c \leqq y < x < cn$. Wir wollen die r zwischen y und x mit r' bezeichnen; ihre Anzahl ist $\frac{q}{2} > 0$; zu jedem r' gibt es ein symmetrisches in Bezug auf x, es heisse r'', wobei entweder $0 < r'' < y$ oder $x < r'' < cn$ ist. Aber es sind alle $r' > c$. Soll $s = \frac{q}{2}$ sein, so müssen alle $r'' < c$, also alle $r'' < y$, also kein $r > x$ sein, was nicht der Fall ist, da

$$x + n \leqq (n-1)c + n < cn$$

ein solches r liefert.

2, 1, 3) $c < x < y < cn$. Zu jedem r', $(x < r' < y)$, gibt es ein symmetrisches, r'', wo $r'' < x$ oder $r'' > y$ ist. Es müssten alle $r'' < c$ sein, also kein r zwischen c und $x \geqq 2c$ liegen. Aber $x - n$ ist ein solches.

2, 1, 4) $c = x < y < cn$, also $y = c + \frac{cn}{2}$. Es sei $s = \frac{q}{2}$. Es liegt also die Hälfte aller r zwischen 0 und x, also, nach der Symmetrie, die zweite Hälfte zwischen x und $2x = 2c$, d. h.: es gibt kein $r > 2c$. Aber die Zahl $\zeta = c + \frac{c-1}{2}n$ hat folgende Eigenschaften:

$$\frac{c-1}{2}n > c, \text{ da } cn > 3c > 2c + n \text{ ist; also } \zeta > 2c;$$

$$\zeta < cn, \text{ da } 2c - n < cn \text{ ist;}$$

$$\zeta \equiv c = x \equiv k \pmod{n}, \qquad \text{wegen } c \text{ ungerade;}$$

$$(\zeta, c) = 1, \qquad \text{wegen } (c, n) = 1.$$

Es ist also ζ ein $r > 2c$.

Also ist $s = \frac{q}{2}$ nur für $n = 2$, c ungerade, $k = 1$.

Fortsetzung des Beweises: 2, 2) n ungerade, also $n \geqq 3$, $c > 3$.

Es ist $y \equiv x + \frac{cn}{2} \equiv \frac{c}{2} \pmod{c}$, also $y > c$ oder $y = \frac{c}{2}$.

2, 2, 1) $y > c$. Das Intervall $0 \ldots c$ liegt wieder ganz in $x \ldots y$ oder $y \ldots x$ (mod. cn), wobei ein gemeinsamer Endpunkt nicht ausgeschlossen ist. Also kann $0 \ldots c$ excl. Endpunkte höchstens $\frac{q}{2}$ Werte von r enthalten, d. h.: $s \leqq \frac{q}{2}$.

Zusatz: Wann ist $s = \frac{q}{2}$?

2, 2, 1, 1) $y < x$ also $c < y < x < cn$. Wir wollen die r zwischen y und x mit r' bezeichnen; ihre Anzahl ist $\frac{q}{2} > 0$; zu jedem r' gibt es ein symmetrisches in Bezug auf x, es heisse r'', wobei entweder $0 < r'' < y$ oder $x < r'' < cn$ ist. Aber es sind alle $r' > c$. Soll $s = \frac{q}{2}$ sein, so müssen alle $r'' < c$, also alle $r'' < y$, also kein $r > x$ sein, was nicht der Fall ist, da $x + n \leqq (n-1)c + n < cn$ ein solches r liefert.

2, 2, 1, 2) $c < x < y < cn$. Zu jedem r', $(x < r' < y)$, gibt es ein symmetrisches, r'', wo $r'' < x$ oder $r'' > y$ ist. Es müssten alle $r'' < c$ sein, also kein r zwischen c und $x \geqq 2c$ liegen. Aber $x - n$ ist ein solches.

2, 2, 1, 3) $c = x < y < cn$, c ungerade, also $y = c + \frac{cn}{2}$. Es sei $s = \frac{q}{2}$. Es liegt also die Hälfte aller r zwischen o und x, also, nach der Symmetrie, die zweite Hälfte zwischen x und $2x = 2c$, d. h.: es gibt kein $r > 2c$. Aber die Zahl $\zeta = c + \frac{c-1}{2} n$ hat folgende Eigenschaften:

$$\frac{c-1}{2} n > c, \text{ da } cn \geq 3c > 2c + n \text{ ist; also } \zeta > 2c;$$

$$\zeta < cn, \text{ da } 2c - n < cn \text{ ist;}$$

$$\zeta \equiv c = x \equiv k \pmod{n}, \quad \text{wegen } c \text{ ungerade;}$$

$$(\zeta, c) = 1, \text{ wegen } (c, n) = 1.$$

Es ist also ζ ein $r > 2c$.

2, 2, 1, 4) $c = x < y < cn$, c gerade. Jetzt ist $c + \frac{c-1}{2} n$ keine ganze Zahl, und der Beweis von 2, 2, 1, 3) gilt nicht. Wir unterscheiden zwei Fälle:

2, 2, 1, 4, 1) $c \equiv 0 \pmod 4$. Wir setzen $\zeta = c + \left(\frac{c}{2} - 1\right) n$. Es ist ζ eine r-Zahl, denn:

$$\zeta < cn, \text{ da } \zeta < c + \frac{cn}{2} \text{ und } n > 2 \text{ ist;}$$

$$\zeta \equiv c = x \equiv k \pmod{n};$$

$$(\zeta, c) = 1, \text{ nicht} = 2, \text{ da } \zeta \text{ mit } \left(\frac{c}{2} - 1\right) n \text{ ungerade ist.}$$

Es ist aber $\zeta > 2c$, falls $\frac{cn}{2} - n > c$ oder $\frac{cn}{2} > c + n$ ist. Für $n > 4$ ist dies erfüllt; für $n = 3$ und $c > 2n = 6$ auch. In diesen Fällen ist ζ ein $r > 2c$, und es ist $s < \frac{q}{2}$. Ist dagegen $n = 3$, $c = 4$, also, wegen $k \equiv x = c = 4 \pmod{n = 3}$, $k = 1$, so ist $\zeta < 2c$. Hier ist in der Tat $s = \frac{q}{2}$, da nur $r = 1$ oder 7 ist.

2, 2, 1, 4, 2) $c \equiv 2 \pmod 4$. Hier setzen wir:

$$\zeta = c + \left(\frac{c}{2} - 2\right) n.$$

Es ist ζ ein r; denn:

$$\zeta < cn, \text{ da } \zeta < c + \frac{cn}{2} \text{ und } n > 2 \text{ ist;}$$

$$\zeta \equiv c = x \equiv k \pmod{n};$$

$$(\zeta, c) = 1, \text{ da } \zeta \text{ mit } \left(\frac{c}{2} - 2\right) n \text{ ungerade ist.}$$

Es ist $\zeta > 2c$, falls $\frac{cn}{2} - 2n > c$ oder $\frac{cn}{2} > c + 2n$ ist. Für $n > 6$ ist dies erfüllt; für $n = 5$, falls $\frac{3c}{2} > 10$ oder $c > 6$ ist; auch für $n = 3$, falls $\frac{c}{2} > 6$

oder $c > 12$ ist. Nicht aber für $n = 5$, $c = 6$, noch für $n = 3$, $c = 10$ ($c = 6$ wäre nicht zu $n = 3$ teilerfremd, also nicht zulässig).

Es ist in der Tat $s = \frac{q}{2}$ für $n = 5$, $c = 6$, also $k \equiv 6 \pmod 5$, also $k = 1$, da $r = 1$ oder 11 ist; oder für $n = 3$, $c = 10$, $k \equiv 10 \pmod 3$, also $k = 1$, da $r = 1, 7, 13$ oder 19 ist.

Fortsetzung des Beweises: 2, 2, 2) Es sei jetzt $y = \frac{c}{2}$, $x = c\frac{n+1}{2}$.

Die Symmetrie besagt nur, dass es $\frac{s}{2}$ Werte von r unterhalb $\frac{c}{2}$ und ebensoviele zwischen $\frac{c}{2}$ und c gibt.

2, 2, 2, 1) c ungerade. Es ist $k \equiv x = \frac{cn+c}{2} \equiv \frac{c+n}{2} \pmod n$.

Die R-Zahlen sind:

$$k,\quad k+n,\ \ldots,\ \frac{c-n}{2},\quad \frac{c+n}{2},\ \ldots,\ c-k-n,\quad c-k,\quad c-k+n,\ \ldots.$$

Die r-Zahlen zwischen $\frac{c}{2}$ und c sind alle von der Form

$$r = \frac{c+tn}{2},$$

wo t den folgenden drei notwendigen Bedingungen unterworfen ist:

$$\frac{c}{2} < \frac{c+tn}{2} < c,$$

also

$$0 < t < \frac{c}{n};$$

$$r \equiv \frac{c+n}{2} \pmod n,$$

also t ungerade;

$$\left(\frac{c+tn}{2},\ c\right) = 1,$$

also $(c, t) = 1$, da c ungerade ist.

Diese Bedingungen sind auch hinreichend dafür, dass $\frac{c+tn}{2}$ ein r zwischen $\frac{c}{2}$ und c ist. Es gibt also ebensoviele Zahlen r im Intervalle, als Zahlen t, die den Bedingungen genügen; daher ist $\frac{s}{2}$ die Anzahl der zu c teilerfremden ungeraden Zahlen $t < \frac{c}{n}$.

Es sei jetzt u die Anzahl der zu c teilerfremden ungeraden Zahlen $t < \frac{c}{3}$. Aus $n \geq 3$ folgt $\frac{s}{2} \leq u$.

Wir wollen u nach oben abschätzen: zu jedem $t < \frac{c}{3}$ gibt es eine Zahl t', die

zu c teilerfremd, ungerade und $> \frac{c}{3}$ ist, nämlich $t' = c - 2t$. Da es genau $\frac{\varphi(c)}{2}$ ungerade, zu c teilerfremde Zahlen gibt, so ist $2u \leqq \frac{\varphi(c)}{2}$.

Hieraus folgt

$$s \leqq 2u \leqq \frac{\varphi(c)}{2} = \frac{q}{2}.$$

Zusatz: Damit $s = \frac{q}{2}$ ist, ist notwendig, dass $u = \frac{\varphi(c)}{4}$ ist. Wegen $c > 3$ ist $\frac{c}{3}$ entweder nicht ganz oder nicht zu c teilerfremd. Wenn $u = \frac{\varphi(c)}{4}$ ist, so ist die Gesamtheit der ungeraden zu c teilerfremden Zahlen identisch mit den $t < \frac{c}{3}$ und den $t' = c - 2t > \frac{c}{3}$. Also kann es kein gerades, teilerfremdes $t_1 < \frac{c}{3}$ geben, indem sonst $c - 2t_1$ eine neue ungerade teilerfremde Zahl ist; die Zahl $t_1 = 2$ darf also nicht $< \frac{c}{3}$ sein. Es ist also $u = \frac{\varphi(c)}{4}$ nur bei $c = 5$.

Mit $c = 5$ sind nur $n = 3$, $k \equiv \frac{c+n}{2} = 4 \pmod 3$, also $k = 1$ zulässig; dann ist in der Tat $s = \frac{q}{2}$, da $r = 1, 4, 7$ oder 13 ist.

Fortsetzung des Beweises: 2, 2, 2, 2) c gerade. Es ist $k \equiv x = \frac{cn+c}{2} \equiv \frac{c}{2} \pmod n$.

$\frac{c}{2}$ ist also ein R, aber kein r, da $c > 3 > 2$ ist. Die $\frac{s}{2}$ Zahlen r zwischen $\frac{c}{2}$ und c sind alle von der Form:

$$r = \frac{c}{2} + tn,$$

mit den Bedingungen:

$$(5) \qquad \frac{c}{2} < \frac{c}{2} + tn < c \quad \text{also} \quad 0 < t < \frac{c}{2n};$$

wegen $n \geqq 3$ ist also a fortiori $t < \frac{c}{6} < \frac{c}{4}$;

$$(4') \qquad \left(\frac{c}{2} + tn,\ c\right) = 1.$$

2, 2, 2, 2, 1) Ist $c \equiv 0 \pmod 4$, so folgt aus (4'):

$$(4'') \qquad (c,\ t) = 1,$$

denn $\frac{c}{2} + tn$ muss ungerade, also t ungerade sein.

Ist (4'') erfüllt, so ist t ungerade, $\frac{c}{2} + tn$ ungerade, und (4') erfüllt. Die Bedingungen (4'') und (5) sind also notwendig und hinreichend dafür, dass $\frac{c}{2} + tn$ ein r

ist. Es gibt also $\frac{s}{2}$ solche t. Aber zu jeder teilerfremden Zahl $t < \frac{c}{4}$, gibt es ein teilerfremdes $t' = \frac{c}{2} - t$ zwischen $\frac{c}{4}$ und $\frac{c}{2}$. Es ist also $s \leqq \frac{\varphi(c)}{2} = \frac{q}{2}$.

Zusatz: $s = \frac{q}{2}$ erfordert, dass es genau $\frac{\varphi(c)}{4}$ Werte von t unterhalb $\frac{c}{2n}$ liegen. Es darf also keine zu c teilerfremde Zahl zwischen $\frac{c}{2n}$ excl. und $\frac{c}{4}$ excl. liegen, a fortiori zwischen $\frac{c}{6}$ und $\frac{c}{4}$, und übrigens darf keine der Zahlen $\frac{c}{2n}$ und $\frac{c}{4}$, falls sie ganz ist, zu c teilerfremd sein. Wegen $(c, n) = 1$, und $n > 1$ ist niemals $\frac{c}{2n}$ ganz. Es darf aber auch nicht $c = 4$ sein, sonst wäre eben $\left(\frac{c}{4}, c\right) = 1$.

Ist $c \equiv 0 \pmod 8$, so ist $\frac{c}{4} - 1$ eine zu c teilerfremde Zahl zwischen $\frac{c}{6}$ excl. und $\frac{c}{4}$ excl., ausser für $\frac{c}{4} - 1 \leqq \frac{c}{6}$, also $c = 8$.

Ist $c \equiv 4 \pmod 8$, so liefert $\frac{c}{4} - 2$ denselben Widerspruch zu $s = \frac{q}{2}$, ausser für $\frac{c}{4} - 2 \leqq \frac{c}{6}$, also $c = 12$ oder 20.

Bei diesen Werten von c muss aber noch n so beschaffen sein, dass die zu c teilerfremden Zahlen t, die $< \frac{c}{4}$ sind, auch alle $< \frac{c}{2n}$ sind, sonst gibt es eine zu c teilerfremde Zahl, die zwar nicht zwischen $\frac{c}{6}$ und $\frac{c}{4}$, aber doch zwischen $\frac{c}{2n}$ und $\frac{c}{4}$ liegt. Also:

$$c = 8, \quad t = 1 < \frac{8}{2n}, \quad \text{also} \quad n < 4;$$

$$c = 12, \quad t = 1 < \frac{12}{2n}, \quad \text{also} \quad n < 6;$$

$$c = 20, \quad t = 3 < \frac{20}{2n}, \quad \text{also} \quad n < 4.$$

Es ist in der Tat $s = \frac{q}{2}$ für:

$c = 8$, $n = 3$, $k \equiv \frac{c}{2} = 4 \pmod 3$, also $k = 1$, wo $r = 1, 7, 13, 19$ ist;

$c = 12$, $n = 5$, $k \equiv \frac{c}{2} = 6 \pmod 5$, also $k = 1$, wo $r = 1, 11, 31, 41$ ist, nicht $n = 3$, wegen $(c, n) = 1$;

$c = 20$, $n = 3$, $k \equiv \frac{c}{2} = 10 \pmod 3$, also $k = 1$, wo $r = 1, 7, 13, 19, 31, 37, 43, 49$ ist.

Fortsetzung des Beweises: 2, 2, 2, 2, 2) Ist $c \equiv 2 \pmod 4$, so folgt aus (4'):

$$(4''') \qquad (c,\ t) = 2,$$

denn $\frac{c}{2} + tn$ muss ungerade, also t gerade sein. Die Bedingungen (4''') und (5) sind auch wieder hinreichend, und es gibt $\frac{s}{2}$ solche t.

Wir setzen $c = 2\gamma$ und nennen τ alle Zahlen $(\tau,\ \gamma) = 1$, $\tau < \gamma$; für jedes $t < \frac{c}{2n}$ ist $\frac{t}{2}$ ein τ und zwar $< \frac{\gamma}{2n}$; und umgekehrt.

Es ist γ ungerade, $(n,\ \gamma) = 1$ und $\varphi(c) = \varphi(\gamma)$. Es sind $q = \varphi(\gamma)$ bezw. $\frac{s}{2}$ die Anzahlen der $\tau < \gamma$ bezw. der $\tau < \frac{\gamma}{2n}$. Und wir behaupten:

$$\frac{s}{2} < \frac{q}{4} = \frac{\varphi(\gamma)}{4}.$$

Der Beweis erledigt also mit einem Schlage den Satz und den Zusatz.

Wir unterscheiden drei Fälle, wobei sich die zwei ersten nicht gegenseitig ausschliessen: $3 \mid \gamma$; γ enthält mindestens einen Primfactor $\equiv 1 \pmod 6$; γ enthält lauter Primfactoren $\equiv 5 \pmod 6$.

Erstens, $3 \mid \gamma$; es ist also $n \geqq 5$, wegen $(n,\ \gamma) = 1$.

Es heissen τ_1 die Zahlen $\tau < \frac{\gamma}{10}$ und es sei u ihre Anzahl. Es ist $\frac{s}{2} \leqq u$. Jedem τ_1 ordnen wir die Zahlen $\tau_2 = \frac{\gamma}{3} + \tau_1$ und $\tau_3 = \frac{2\gamma}{3} + \tau_1$ zu. Ist $9 \mid \gamma$, so sind τ_2 und τ_3 beide τ-Zahlen; sonst genau eine der zwei für jedes τ_1. In beiden Fällen haben wir mindestens $2u$ Zahlen τ aufgezählt; zu jeder von diesen ist das zugehörige $\gamma - \tau$ auch eine τ-Zahl, und sie ist sicher stets von den $2u$ erstgezählten verschieden. Das gibt stets mindestens $4u$ Zahlen τ, unter welchen $\frac{\gamma - 1}{2}$ nicht aufgezählt ist, ausser eventuell für $\frac{\gamma - 1}{2} < \frac{\gamma}{3} + \frac{\gamma}{10}$, $2\gamma < 15$, also $\gamma = 3$, wo aber $u = 0$ ist. Es ist also jedenfalls $\frac{s}{2} \leqq u < \frac{\varphi(\gamma)}{4}$.

Zweitens, γ enthält einen Primfactor $p \equiv 1 \pmod 6$; es ist $n \geqq 3$.

u sei die Anzahl der $\tau < \frac{\gamma}{6}$. Es ist $\frac{s}{2} \leqq u$. Nach dem 3. Hilfssatze ist $u = \frac{\varphi(\gamma)}{6}$, also $\frac{s}{2} < \frac{\varphi(\gamma)}{4}$, indem $a = 6$, $b = \gamma$, $x = 0$, $T_b = u$ gesetzt wird, wobei die $t_b < \frac{b}{a}$ genau die $\tau < \frac{\gamma}{6}$ sind.

Drittens, γ enthält lauter Primfactoren $\equiv 5 \pmod 6$; es ist $n \geqq 3$.

Es heissen τ_1 die Zahlen $\tau < \frac{\gamma}{6}$ und u sei ihre Anzahl. Wir greifen irgend einen Primfactor von γ heraus, er heisse p, und bestimmen eine Zahl z, derart dass

$\frac{4}{24} < \frac{\chi}{p} < \frac{5}{24}$ ist: für $p > 24$ ist die Existenz eines χ klar; für $p = 5$ nehmen wir $\chi = 1$; für $p = 11$, $\chi = 2$; für $p = 17$, $\chi = 3$; für $p = 23$, $\chi = 4$. Wir setzen:

$$\tau_i = (i-1)\chi\frac{\gamma}{p} + \tau_1, \qquad (i = 2, 3, 4, 5).$$

Es sind also die Zahlen τ_i definiert für $i = 1, 2, 3, 4, 5$: zu jeder Zahl τ_1 gehört ein τ_2, ein τ_3, ein τ_4 und ein τ_5. Es sind alle τ_i verschieden und alle $< \gamma$.

p ist der einzige Primfactor von γ, der ein τ_i teilen könnte; dies kann nur eintreten, falls $p^2 \nmid \gamma$ ist; und auch dann höchstens ein τ_i für jedes τ_1. Es ist also $4u \leqq \varphi(\gamma)$. Übrigens ist die Gleichheit ausgeschlossen; denn:

Es sei $\gamma \equiv 5 \pmod 6$; so ist $\frac{\gamma+1}{6}$ ganz und zu γ teilerfremd. Aber es sind alle $\tau_1 < \frac{\gamma}{6} < \frac{\gamma+1}{6}$ und alle $\tau_2 > \frac{4}{24}\gamma + 1 > \frac{\gamma+1}{6}$. Es ist also $\frac{\gamma+1}{6}$ ein neues τ. Also $\frac{s}{2} \leqq u < \frac{\varphi(\gamma)}{4} = \frac{q}{4}$.

Es sei jetzt $\gamma \equiv 1 \pmod 6$. Falls $5 \nmid \gamma$ ist, so ist $\frac{\gamma+5}{6}$ ganz und zu γ teilerfremd. Diese Zahl ist grösser als alle τ_1 und kleiner als alle τ_2. So folgt wieder $\frac{s}{2} < \frac{q}{4}$. Ist dagegen $5 \mid \gamma$, so nehmen wir $p = 5$, $\chi = 1$. Alle τ_i sind

$$< \frac{4}{5}\gamma + \frac{1}{6}\gamma = \frac{29}{30}\gamma;$$

für $\gamma > 30$ ist $\gamma - 1$ nicht mitgezählt worden, also $\frac{s}{2} < \frac{q}{4}$; für $\gamma < 30$ ist $\gamma = 25$, $p = 5$, $p^2 \mid \gamma$; alle τ_i sind τ-Zahlen, und es ist $5u \leqq \varphi(\gamma)$, $\frac{s}{2} \leqq u < \frac{\varphi(\gamma)}{4} = \frac{q}{4}$.

So ist der Beweis im Falle $c > n$ erledigt.

II) $c \leqq n$.

Für $c \leqq k$ sind alle R-Zahlen $\geqq c$. Es ist also $s = 0 < \frac{q}{2}$. Für $c > k$ gibt es ein $R < c$, nämlich k selbst. Falls $(c, k) > 1$ ist, so ist dies R kein r, also $s = 0 < \frac{q}{2}$. Falls $(c, k) = 1$ ist, so ist $s = 1$.

In diesem Fall ist entweder $s < \frac{q}{2}$ (für $q > 2$), oder $s = \frac{q}{2}$ (für $q = 2$), oder $s = q$ (für $q = 1$).

Wir bemerken im Voraus, dass jeder gemeinsame Teiler von c und n auch in $\frac{\varphi(cn)}{\varphi(n)} = q$ aufgeht.

1) $\frac{\varphi(cn)}{\varphi(n)} = q = 2.$

1, 1) $(c, n) = 1$. Also $\varphi(c) = 2$, $c = 3$, 4 oder 6. Wenn $s = \frac{q}{2}$ ist, ist also

$$\begin{array}{llll} c = 3, & n > 3, & (n, 3) = 1, & k = 1 \text{ oder } 2, \\ c = 4, & n > 4, & (n, 4) = 1, & k = 1 \text{ oder } 3, \\ c = 6, & n > 6, & (n, 6) = 1, & k = 1 \text{ oder } 5. \end{array}$$

Es muss übrigens $(k, n) = 1$ sein.

In diesen Fällen ist in der Tat stets $s = 1$, $q = 2$.

1, 2) $(c, n) = d > 1$. Es ist $d \mid q$, also $d = 2$. Es geht 4 nicht auf in c, sonst wäre auch 4 ein Teiler von q. Wir setzen $c = 2\gamma$, γ ungerade, $n = 2\nu$, $(\gamma, \nu) = 1$. Es ist:

$$2 = \frac{\varphi(4\gamma\nu)}{\varphi(2\nu)} = \varphi(\gamma)\frac{\varphi(4\nu)}{\varphi(2\nu)} = 2\varphi(\gamma),$$

also $\varphi(\gamma) = 1$, $\gamma = 1$, $c = 2$. Wenn $s = \frac{q}{2}$ ist, ist also $c = 2$, n gerade, $k = 1$.

Dann ist in der Tat stets $s = 1$, $q = 2$.

2) $\frac{\varphi(cn)}{\varphi(n)} = q = 1$. Es müssen c und n teilerfremd sein. Es ist also $\varphi(c) = 1$. Da nach Voraussetzung $c = 1$ ausgeschlossen ist, so ist $c = 2$, n ungerade, $k = 1$.

Hier ist in der Tat stets $s = 1$, $q = 1$.

B) $n = k$, also wegen (1): $n = k = 1$.

Hier ist offenbar für alle c:

$$s = q = \varphi(c).$$

Es ist also der folgende Satz bewiesen (wir ändern die Buchstaben):

SATZ I. — *Gegeben sind die Zahlen* $c' > 1$ *und* $n' \geq k' > 0$, $(k', n') = 1$. *Die Anzahl der positiven Zahlen* $r' \equiv k' \pmod{n'}$, $(r', c') = 1$, *die einerseits* $\leq c'n'$ *und anderseits* $< c'$ *sind, sei* Q *bezw.* S'.

Behauptung: es ist stets $S' < \frac{Q}{2}$, *ausser in folgenden Fällen:*

A) $n' > k' \geq 1$.

I) $c' > n'$. *Es ist* $S' = \frac{Q}{2}$ *für:*

$$\begin{array}{lll} n' = 2, & c' \text{ beliebig}, & k' = 1, \\ n' = 3, & c' = 4, 5, 8, 10, 20, & k' = 1, \\ n' = 4, & c' = 6, & k' = 1, \\ n' = 5, & c' = 6, 12, & k' = 1. \end{array}$$

II) $c' \leq n'$. *Es ist* $S' = \frac{Q}{2}$ *für:*

$$\begin{array}{lll} c' = 2, & n' \text{ gerade}, & k' = 1, \\ c' = 3, & (n', 3) = 1, & k' = 1, 2, \\ c' = 4, & (n', 4) = 1, & k' = 1, 3, \\ c' = 6, & (n', 6) = 1, & k' = 1, 5. \end{array}$$

Es ist $S' = Q = 1$ *für:*

$$c' = 2, \quad n' \text{ ungerade} > 1, \quad k' = 1.$$

B) $n' = k' = 1$. *Es ist für alle* c': $S' = Q = \varphi(c')$.

Corollar: aus $S' > \frac{Q}{2}$ folgt $S' = Q$.

5. SATZ II. — *Gegeben sind die Zahlen* $c' > 1$ *und* $n \geqq k > 0$, $(c', k, n) = 1$. *Die Anzahl der positiven Zahlen* $r \equiv k \pmod{n}$, $(r, c') = 1$, *die* $\leqq c'n$ *bezw.* $< c'$ *sind, sei* Q *bezw.* S.

Behauptung: es ist stets $S < \frac{Q}{2}$, *ausser in wenigen Fällen, die wir vollständig beherrschen.*

Beweis: Der Fall $(k, n) = d = 1$, wo $S = S'$ ist, ist durch Satz I erledigt.

Es sei also $(k, n) = d > 1$, $k = k'd$, $n = n'd$. Es ist $n' \geqq k' > 0$, $(k', n') = 1$, und auch $(d, c') = 1$. Wir bezeichnen mit r' die Zahlen $r' \equiv k' \pmod{n'}$, $(r', c') = 1$. Jedes $r'd$ ist ein r und jedes $\frac{r}{d}$ ist ein r'.

Es ist also Q bezw. S die Anzahl der $r' \leqq c'n'$ bezw. $< \frac{c'}{d}$. Es heisse S' die Anzahl der $r' < c'$. Es folgt: $S \leqq S'$.

Die Zahlen c', n', k', r', Q, S' erfüllen dieselben Bedingungen wie im letzten Satze: es ist also $S \leqq S' < \frac{Q}{2}$, mit folgenden Ausnahmen:

A) $n' > k' \geqq 1$ also $n > k \geqq d$.

I) $c' > n'$. Es ist $S \leqq S' = \frac{Q}{2}$, in den im Satz I genannten Fällen.

II) $c' \leqq n'$. Es ist entweder $S \leqq S' = \frac{Q}{2}$, in den im Satz I genannten Fällen, oder $S \leqq S' = Q = 1$, für $c' = 2$, n' ungerade, $k' = 1$. Aber $d > 1$, $(d, c') = 1$ ergibt $d > 2$, $k > c'$. Es ist folglich in diesem Falle $S = 0 < \frac{Q}{2}$.

B) $n' = k' = 1$ also $n = k = d$.

Es ist $S \leqq S' = Q = \varphi(c')$. Es ist S die Anzahl der Zahlen, die $< \frac{c'}{d}$ und zu c' teilerfremd sind. Aus $d \geqq 2$ folgt $S < Q$.

I) $d = 2$, also c' ungerade > 1:

$$S = \frac{\varphi(c')}{2} = \frac{Q}{2}$$

für alle c'.

II) $d \geqq 3$: es ist im Allgemeinen $S < \frac{Q}{2}$; es ist $S = \frac{Q}{2}$, höchstens falls es zwischen $\frac{c'}{d}$ incl. und $\frac{c'}{2}$ incl., a fortiori zwischen $\frac{c'}{3}$ incl. und $\frac{c'}{2}$ incl. keine zu c' teilerfremde Zahl gibt; und sicher nicht für $d > c'$, denn dann ist $S = 0$, wegen $k > c'$.

Für c' ungerade: $\frac{c' - 1}{2} < \frac{c'}{3}$ gibt $c' < 3$: unmöglich.

Für $c' \equiv 0 \pmod 4$: $\frac{c'}{2} - 1 < \frac{c'}{3}$ gibt $c' = 4$, $d = 3$. Hier ist in der Tat $S = \frac{Q}{2}$, da $r' = 1, 3$ ist.

Für $c' \equiv 2 \pmod 4$: $\frac{c'}{2} - 2 < \frac{c'}{3}$ gibt $c' = 6$, $d = 5$ oder $c' = 10$, $d = 3$, nicht $d = 7$ oder 9, sonst liegt die Zahl 3 zwischen $\frac{c'}{d}$ und $\frac{c'}{2}$. Hier ist in der Tat $S = \frac{Q}{2}$, da für $c' = 6$, $d = 5$, $r' = 1, 5$ und für $c' = 10$, $d = 3$, $r' = 1, 3, 7, 9$ ist.

Corollar: aus $S > \frac{Q}{2}$ folgt $S = Q$ in allen Fällen.

6. Wir wollen jetzt alle Fälle aufzählen, wo $S = \frac{Q}{2}$ ist. Dazu bilden wir aus den Sätzen I und II eine gemeinsame Tabelle. Hier ist also: entweder $S = S'$ für $d = 1$, oder $S \leqq S'$ für $d > 1$. Also für $d = 1$ brauchen wir die Fälle, wo $S = S' = \frac{Q}{2}$ ist, und für $d > 1$ die Fälle, wo $S = S' = \frac{Q}{2}$ oder $S = \frac{S'}{2} = \frac{Q}{2}$ ist. Aber zunächst erhalten wir nur für $d = 1$: $S = S' = \frac{Q}{2}$; und für $d > 1$: entweder $S \leqq S' = \frac{Q}{2}$, oder $S = \frac{S'}{2} = \frac{Q}{2}$. Dann wird eine genauere Discussion zeigen, wann wirklich für $d > 1$, $S = S' = \frac{Q}{2}$ ist.

TABELLE I *für* $S \leqq S' = \frac{Q}{2}$ *und* $S = \frac{S'}{2} = \frac{Q}{2}$.

I) $n' > 1$, $c' > n'$. Es ist $S \leqq S' = \frac{Q}{2}$ für:

α)	$n' = 2$,	c' beliebig > 2,	$k' = 1$,
β)	$n' = 3$,	$c' = 4, 5, 8, 10, 20$,	$k' = 1$,
γ)	$n' = 4$,	$c' = 6$,	$k' = 1$,
δ)	$n' = 5$,	$c' = 6, 12$,	$k' = 1$.

II) $n' > 1$, $c' \leqq n'$. Es ist $S \leqq S' = \frac{Q}{2}$ für:

α)	n' gerade,	$c' = 2$,	$k' = 1$,
β)	$(n', 3) = 1$,	$c' = 3$,	$k' = 1, 2$,
γ)	$(n', 4) = 1$,	$c' = 4$,	$k' = 1, 3$,
δ)	$(n', 6) = 1$,	$c' = 6$,	$k' = 1, 5$.

III) $n' = k' = 1$. Es ist $S = \frac{S'}{2} = \frac{Q}{2}$ für:

α)	$n = k = d = 2$,	c' ungerade > 1,
β)	$n = k = d = 3$,	$c' = 4, 10$,
γ)	$n = k = d = 5$,	$c' = 6$.

Es sollen übrigens in der ganzen Tabelle $(d, c') = 1$, $(k', n') = 1$ genommen werden.

Es bleibt in der Wahl von d eine grosse Willkür. Diese wollen wir jetzt untersuchen, indem wir die Bedingung $S = \frac{Q}{2}$ ins Auge fassen.

Wir haben $k \leqq n$, $r \equiv k \pmod{n}$, $r > 0$, also $k \leqq r$, und $S = \frac{Q}{2} \neq 0$, also $S \geqq 1$. Es soll also mindestens ein $r < c'$ geben; also muss $k < c'$ sein, also $d < \frac{c'}{k'}$. Ferner teilt d alle r, wegen $d \mid k$, $d \mid n$.

I)

α) $n' = 2$, c' beliebig > 2, $k' = 1$, d beliebig, $k = d$, $n = 2d$.

Es ist nach dem 1. Hilfssatze:

$$Q = \frac{\varphi(c'n)}{\varphi(n)} = \frac{\varphi(2dc')}{\varphi(2d)} = \frac{\varphi(2c')}{\varphi(2)} = \varphi(2c')$$

wegen $(d, c') = 1$.

Es sei c' ungerade > 2:

$$S = \frac{Q}{2} = \frac{\varphi(2c')}{2} = \frac{\varphi(c')}{2},$$

d. h.: es gibt $\frac{\varphi(c')}{2}$ Zahlen $\equiv k = d \pmod{2d}$, zu c' teilerfremd und $< c'$ oder: setzt man sie $= xd$, so gibt es $\frac{\varphi(c')}{2}$ Zahlen x, wo x ungerade ist, $(x, c') = 1$ und $x < \frac{c'}{d}$.

Es sei $d \geqq 2$, also $x < \frac{c'}{2}$. Da es überhaupt $\frac{\varphi(c')}{2}$ zu c' teilerfremde Zahlen unterhalb $\frac{c'}{2}$ gibt, so muss, weil $(2, c') = 1$ ist, die Zahl $2 > \frac{c'}{2}$ sein, also $c' \leqq 3$, $c' = 3$, $d < \frac{c'}{k'}$, also $d = 2$.

Es sei jetzt $d = 1$; c' ist in der Tat eine beliebige ungerade Zahl.

Es sei c' gerade > 2:

$$S = \frac{Q}{2} = \frac{\varphi(2c')}{2} = \varphi(c'),$$

d. h.: es gibt $\varphi(c')$ Zahlen $\equiv k = d \pmod{2d}$, zu c' teilerfremd und $< c'$, oder: setzt man sie $= xd$, so gibt es $\varphi(c')$ Zahlen x, x ungerade, $(x, c') = 1$ und $x < \frac{c'}{d}$. Für $d > 1$ ist das unmöglich. Für $d = 1$ ist dagegen c' eine beliebige gerade Zahl > 2.

Die Möglichkeiten reducieren sich auf:

$$n' = 2, \quad c' \text{ beliebig} > 2, \quad k' = 1, \quad d = 1$$

und

$$n' = 2, \quad c' = 3, \quad k' = 1, \quad d = 2.$$

β) $n' = 3$, $c' = 4$, $k' = 1$, d beliebig, $d < \frac{c'}{k'}$, $(d, c') = 1$, also $d = 1, 3$.

β) $n' = 3$, $c' = 5$, $k' = 1$, $d = 1, 2, 3, 4$ (nach denselben Bedingungen).

Folglich:

$$S = \frac{1}{2} Q = \frac{1}{2} \frac{\varphi(15d)}{\varphi(3d)} = \frac{1}{2} \varphi(5) = 2.$$

Es müssen also zwei r-Zahlen unter 5 liegen; wegen $d \mid r$ ist also $d \neq 3, 4$. Für $d = 2$ wäre $n = 6$, $k = 2$, $r = 2, 8$, u. s. w., also $S = 1$. Das lässt nur $d = 1$.

β) $\quad n' = 3, \quad c' = 8, \quad k' = 1, \quad d = 1, 3, 5, 7.$

$S = \frac{1}{2} \frac{\varphi(24d)}{\varphi(3d)} = \frac{1}{2} \varphi(8) = 2$. Es gibt zwei r-Zahlen < 8. Also $d \neq 5, 7$. Für $d = 3$ wäre $n = 9$, $k = 3$, $S = 1$. Es bleibt $d = 1$.

β) $\quad n' = 3, \quad c' = 10, \quad k' = 1, \quad d = 1, 3, 7, 9.$

$S = \frac{1}{2} \varphi(10) = 2$. Also $d \neq 7, 9$. Für $d = 3$ wäre $n = 9$, $k = 3$, $S = 1$. Es bleibt $d = 1$.

β) $\quad n' = 3, \quad c' = 20, \quad k' = 1, \quad d = 1, 3, 7, 9, 11, 13, 17, 19.$

$S = \frac{1}{2} \varphi(20) = 4$. Es gibt vier r-Zahlen < 20. Also $d \neq 7, 9, 11, 13, 17, 19$. Für $d = 3$ wäre $n = 9$, $k = 3$, r unter den Zahlen 3, 12, 21, ..., also $S = 1$. Es bleibt $d = 1$.

γ) $\quad n' = 4, \quad c' = 6, \quad k' = 1, \quad d = 1, 5.$

$S = \frac{1}{2} \frac{\varphi(24d)}{\varphi(4d)} = \frac{1}{2} \frac{\varphi(24)}{\varphi(4)} = 2$. Also $d \neq 5$, also $d = 1$.

δ) $\quad n' = 5, \quad c' = 6, \quad k' = 1, \quad d = 1, 5.$

δ) $\quad n' = 5, \quad c' = 12, \quad k' = 1, \quad d = 1, 5, 7, 11.$

$S = \frac{1}{2} \frac{\varphi(60d)}{\varphi(5d)} = \frac{1}{2} \varphi(12) = 2$, $d \neq 7, 11$. Für $d = 5$ wäre $n = 25$, $k = 5$, r unter den Zahlen 5, 30, ..., also $S = 1$. Also ist $d = 1$

II)

α) $\quad n'$ gerade, $\quad c' = 2, \quad k' = 1, \quad d < \frac{c'}{k'}$ also $d = 1$,

β) $\quad (n', 3) = 1, \quad c' = 3, \quad k' = 1, \quad$ also $d = 1, 2,$
$\qquad\qquad\qquad\qquad\qquad\quad k' = 2, \quad$ also $d = 1,$

γ) $\quad (n', 4) = 1, \quad c' = 4, \quad k' = 1, \quad$ also $d = 1, 3,$
$\qquad\qquad\qquad\qquad\qquad\quad k' = 3, \quad$ also $d = 1,$

δ) $\quad (n', 6) = 1, \quad c' = 6, \quad k' = 1, \quad$ also $d = 1, 5,$
$\qquad\qquad\qquad\qquad\qquad\quad k' = 5, \quad$ also $d = 1.$

Wir sind jetzt imstande, unsere Tabelle präcise darzustellen. So bilden wir die Tabelle II, die alle Fälle enthält, wo $S = \frac{Q}{2}$ ist, und nur diese [18]). Indessen benutzen wir die Bedingung: $(k', n') = 1$. Es ist $n = n' d$.

---

[18]) Der Leser braucht sich nicht zu überlegen, dass wir keine unnützen Systeme von Zahlen in der Tabelle haben: später würden wir sie doch finden und weglassen. In der Tat ist es aber so, vergl. [22]).

TABELLE II *für* $S = \frac{Q}{2}$.

I) $c' > n' > 1$.

$n'=2$	c' beliebig >2	$k'=1$		$d=1$	$n=2$
$n'=2$	$c'=3$	$k'=1$		$d=2$	$n=4$
$n'=3$	$c'=4$	$k'=1$		$d=1,3$	$n=3,9$
$n'=3$	$c'=5$	$k'=1$		$d=1$	$n=3$
$n'=3$	$c'=8$	$k'=1$		$d=1$	$n=3$
$n'=3$	$c'=10$	$k'=1$		$d=1$	$n=3$
$n'=3$	$c'=20$	$k'=1$		$d=1$	$n=3$
$n'=4$	$c'=6$	$k'=1$		$d=1$	$n=4$
$n'=5$	$c'=6$	$k'=1$		$d=1,5$	$n=5,25$
$n'=5$	$c'=12$	$k'=1$		$d=1$	$n=5$

II) $n' \geq c' > 1$.

n' gerade $n' \geq 2$	$c'=2$	$k'=1$		$d=1$	n gerade $n \geq 2$	
$(n', 3)=1$ $n' \geq 4$	$c'=3$	$k'=1$		$d=1$	$(n, 3)=1$ $n \geq 4$	
		$k'=1$		$d=2$	$(n, 3)=1$ $n \geq 8$	$n \equiv 0 \pmod 2$
		$k'=2$	also $n' \not\equiv 0 \pmod 2$	$d=1$	$(n, 3)=1$ $n \geq 4$	$n \not\equiv 0 \pmod 2$
$(n', 4)=1$ $n' \geq 5$	$c'=4$	$k'=1$		$d=1$	$(n, 4)=1$ $n \geq 5$	
		$k'=1$		$d=3$	$(n, 4)=1$ $n \geq 15$	$n \equiv 0 \pmod 3$
		$k'=3$	also $n' \not\equiv 0 \pmod 3$	$d=1$	$(n, 4)=1$ $n \geq 5$	$n \not\equiv 0 \pmod 3$
$(n', 6)=1$ $n' \geq 7$	$c'=6$	$k'=1$		$d=1$	$(n, 6)=1$ $n \geq 7$	
		$k'=1$		$d=5$	$(n, 6)=1$ $n \geq 35$	$n \equiv 0 \pmod 5$
		$k'=5$	also $n' \not\equiv 0 \pmod 5$	$d=1$	$(n, 6)=1$ $n \geq 7$	$n \not\equiv 0 \pmod 5$

III) $n' = k' = 1$

$n'=1$	c' ungerade >1	$k'=1$		$d=2$	$n=2$
$n'=1$	$c'=4$	$k'=1$		$d=3$	$n=3$
$n'=1$	$c'=10$	$k'=1$		$d=3$	$n=3$
$n'=1$	$c'=6$	$k'=1$		$d=5$	$n=5$.

Jetzt können wir eine Tabelle nach wachsenden n und abnehmenden $k = k'd$ bilden:

TABELLE III *für* $S = \frac{Q}{2}$.

$n = 2$	c' ungerade > 1	$k = 2$	aus III
	c' beliebig > 2	$k = 1$	aus I
	$c' = 2$	$k = 1$	aus II
$n = 3$	$c' = 4, 10$	$k = 3$	aus III
	$c' = 4, 5, 8, 10, 20$	$k = 1$	aus I
$n = 4$	$c' = 3$	$k = 2$	aus I
	$c' = 6$	$k = 1$	aus I
	$c' = 2$	$k = 1$	aus II
	$c' = 3$	$k = 1$	aus II
$n = 5$	$c' = 6$	$k = 5$	aus III
	$c' = 4$	$k = 3$	aus II
	$c' = 3$	$k = 2$	aus II
	$c' = 6, 12$	$k = 1$	aus I
	$c' = 3$	$k = 1$	aus II
	$c' = 4$	$k = 1$	aus II
oder $n > 5$:			
$n = 9$	$c' = 4$	$k = 3$	aus I
$n = 25$	$c' = 6$	$k = 5$	aus I

diese zwei Fälle brauchen aber nicht speciell erwähnt zu werden, da sie in den folgenden enthalten sind:

n gerade	$c' = 2$	$k = 1$	aus II
$n \equiv 1, 2 \pmod 3$	$c' = 3$	$k = 1, 2$ unabhängig von n	aus II
$n \equiv 1, 3 \pmod 4$	$c' = 4$	$k = 1, 3$ unabhängig von n	aus II [19])
$n \equiv 1, 5 \pmod 6$	$c' = 6$	$k = 1, 5$ unabhängig von n	aus II [19]).

Anmerkung: es ist überall

$$(c', k) = 1, \quad 1 \leqq k < c', \quad k \leqq n.$$

---

[19]) Hier könnten wir eventuell überflüssige Systeme erhalten, da wir, um soviele Unterfälle nicht unterscheiden zu müssen, gewisse Nebenbedingungen für n weggelassen haben. Diese überflüssigen Systeme sind:

$c' = 4, \quad k = 3, \quad n = 9$ (falls $3 \mid n$ war, musste ja $n \geqq 15$ sein)

$c' = 6, \quad k = 5, \quad n = 25$ (falls $5 \mid n$ war, musste ja $n \geqq 35$ sein).

Aber genau diese zwei Systeme kommen von I, und müssen hinzugefügt werden. Also ist unsere Tabelle notwendig und hinreichend. Vergl. [18]), [22]).

ANHANG ZU TABELLE III.

Jetzt zählen wir noch die Fälle, wo $S = Q$ ist, auf. Hier ist stets $d = 1$, wie aus Satz II hervorgeht. Also nach Satz I ($n' = n$, $k' = k$):

n ungerade > 1	$c' = 2$	$k = 1$
$n = 1$	c' beliebig	$k = 1$.

7. SATZ III. — *Gegeben sind* $c' \geqq 1$, $a' \geqq 1$, $n > 1$, *mit der Bedingung* $(c', a') = 1$. *Bezeichnen wir mit* ρ_1' *alle positiven Zahlen, die* $< c'n$, *zu* c' *teilerfremd, und* $\equiv 1 \pmod{n}$ *sind, mit* Q_a *die Anzahl der* ρ_1' *und mit* S_a *die Anzahl der* $\rho_1' a' < c' \pmod{c'n}$.

Es sei k *der kleinste positive Rest von* $a' \pmod{n}$; *es sei* Q *bezw.* S *die Anzahl der positiven Zahlen* $r \equiv k \pmod{n}$, $(r, c') = 1$, *die* $\leqq c'n$ *bezw.* $< c'$ *sind.*

Behauptung:

I. *Je zwei Werte von* $\rho_1' a'$ *sind incongruent* $\pmod{c'n}$.

II. *Jedes* $\rho_1' a'$ *ist congruent einem* $r \pmod{c'n}$ *und umgekehrt.*

III. *Es ist* $Q_a = Q$, $S_a = S$.

Beweis: Die Zahlen ρ_1' sind diejenigen unter den Zahlen:

$$1, \quad 1 + n, \quad 1 + 2n, \quad \ldots, \quad 1 + (c' - 1)n,$$

die zu c' teilerfremd sind. Nach dem 1. Hilfssatz ist also

$$Q_a = \frac{\varphi(c'n)}{\varphi(n)}.$$

Die Zahlen r sind diejenigen unter den Zahlen:

$$k, \quad k + n, \quad k + 2n, \quad \ldots, \quad k + (c' - 1)n,$$

die zu c' teilerfremd sind. Wegen $(n, k) = (n, a')$ und wegen $(c', a') = 1$ ist $(c', n, k) = 1$. Also ist ebenfalls $Q = \frac{\varphi(c'n)}{\varphi(n)}$. Also ist $Q_a = Q$.

Betrachten wir jetzt die Zahlen $\rho_1' a'$. Wären zwei von diesen congruent $\pmod{c'n}$, so gäbe es ein f und ein g, derart dass:

$(1 + fn)a' \equiv (1 + gn)a' \pmod{c'n}$, $\quad 0 \leqq f \leqq c' - 1$, $\quad 0 \leqq g \leqq c' - 1$

wäre. Also wäre $fa' \equiv ga' \pmod{c'}$, also $f \equiv g \pmod{c'}$, folglich $f = g$.

Die Zahlen $\rho_1' a'$ sind also paarweise incongruent $\pmod{c'n}$.

Ferner ist für alle ρ_1': $\rho_1' a' \equiv a' \equiv k \pmod{n}$. Es haben die positiven Reste der $\rho_1' a' \pmod{c'n}$ folgende Eigenschaften: sie sind alle $\equiv k \pmod{n}$, zu c' teilerfremd, $\leqq c'n$, untereinander verschieden, und ihre Anzahl ist Q_a. Also sind es genau die Zahlen r, jede einmal, womit der Satz bewiesen ist.

Corollar: ist $c' = 1$, so ist $S = 0$, also $S < \frac{Q}{2}$; ist $c' > 1$, so erfüllen, wegen $(c', n, k) = 1$, die Zahlen c', n, k, r, Q, S die Bedingungen des 2. Satzes.

8. SATZ IV. — *Gegeben sind* $c > 1$, $a \geqq 1$, $n > 1$. *Bezeichnen wir mit* ρ_1 *alle positiven Zahlen, die* $< cn$, *zu* c *teilerfremd und* $\equiv 1 \pmod{n}$ *sind, mit* q_a *die Anzahl*

der ρ_1 *und mit* s_a *die Anzahl der* $\rho_1 a$, *welche* $< c$ (mod. cn) *sind. Es werde* $(c, a) = e$, $c = c'e$, $a = a'e$ *gesetzt. Bezeichnen wir mit* ρ'_1 *alle positiven Zahlen, die* $< c'n$, *zu* c' *teilerfremd und* $\equiv 1$ (mod. n) *sind, mit* Q_a *die Anzahl der* ρ'_1 *und mit* S_a *die Anzahl der* $\rho'_1 a' < c'$ (mod. $c'n$).

Behauptung: es ist $\frac{s_a}{q_a} = \frac{S_a}{Q_a}$, *unabhängig von* e.

Beweis: Der Rest jedes ρ_1 (mod. $c'n$) ist selbstverständlich ein ρ'_1. Nach dem 1. Hilfssatze ist die Anzahl der zu e teilerfremden Glieder der Progression $\rho'_1 + x.c'n$, $0 \leqq x \leqq e-1$, dieselbe für alle ρ'_1, da stets $(e, c'n, \rho'_1) = 1$ ist, wegen der Definition von ρ'_1. Es entstehen in dieser Weise sämtliche ρ_1, wenn ρ'_1 alle seine Werte durchläuft.

Wir können also sagen, dass die ρ_1 in Q_a Classen von je $\frac{q_a}{Q_a}$ Zahlen zerfallen: zu jedem ρ'_1 gehören $\frac{q_a}{Q_a}$ verschiedene ρ_1, welche congruent dem ρ'_1 (mod. $c'n$) sind.

Zu jedem ρ'_1 gehören folglich $\frac{q_a}{Q_a}$ verschiedene $\rho_1 a$, für welche jedesmal $\rho_1 \equiv \rho'_1$ (mod. $c'n$) ist. Damit sind die $\rho_1 a$ erschöpft.

Also: zu jedem $\rho'_1 a'$ gehören $\frac{q_a}{Q_a}$ verschiedene $\rho_1 a$, für welche $\rho_1 \equiv \rho'_1$ (mod. $c'n$) ist.

Also, zu den S_a Zahlen $\rho'_1 a' < c'$ (mod. $c'n$) gehören $\frac{q_a}{Q_a} S_a$ Zahlen $\rho_1 a$. Aber es ist $\rho_1 a' \equiv \rho'_1 a' < c'$ (mod. $c'n$), und daher $\rho_1 a < c$ (mod. cn). Umgekehrt: ist $\rho_1 a < c$ (mod. cn), so ist auch $\rho'_1 a' \equiv \rho_1 a' < c'$ (mod. $c'n$).

Hieraus folgt unmittelbar:

$$s_a = \frac{q_a}{Q_a} S_a, \quad \text{also} \quad \frac{s_a}{q_a} = \frac{S_a}{Q_a}.$$

9. Sätze IV und III und dessen Corollar wollen wir zusammenfassen:

SATZ V. — *Gegeben sind* $c > 1$, $a \geqq 1$, $n > 1$. *Bezeichnen wir mit* ρ_1 *alle positiven Zahlen, die* $< cn$, *zu* c *teilerfremd und* $\equiv 1$ (mod. n) *sind, mit* q_a *die Anzahl der* ρ_1, *mit* s_a *die Anzahl der* $\rho_1 a$, *welche* $< c$ (mod. cn) *sind.*

Es werde $(c, a) = e$, $c = c'e$, $a = a'e$ *gesetzt. Es sei* k *der kleinste positive Rest von* a' (mod. n); *es sei* Q *bezw.* S *die Anzahl der positiven Zahlen* $r \equiv k$ (mod. n), $(r, c') = 1$, *die* $\leqq c'n$ *bezw.* $< c'$ *sind.*

Behauptung:

I. *Es ist* $\frac{s_a}{q_a} = \frac{S}{Q}$, *unabhängig von* e.

II. *Wenn* $s_a > \frac{q_a}{2}$ *ist, so ist* $s_a = q_a$.

III. *Tabelle* III *und deren Anhang gibt alle Fälle, wo* $s_a = \frac{q_a}{2}$ *und* $s_a = q_a$ *ist.*

Beweis: Definieren wir wie im Satze IV die Zahlen ρ'_1, S_a und Q_a, so folgt I aus

Satz IV und Satz III, III; denn es ist:

$$\frac{s_a}{q_a} = \frac{S_a}{Q_a} = \frac{S}{Q},$$

unabhängig von e.

Also, wenn $s_a > \frac{q_a}{2}$ ist, so ist $S > \frac{Q}{2}$. Also nach dem Corollar zum Satze III, ist $c' > 1$ und dürfen wir den 2. Satz und sein Corollar anwenden; also ist $S = Q$, also auch $s_a = q_a$; ferner sind die Fälle, wo $s_a = \frac{q_a}{2}$ und die, wo $s_a = q_a$ ist, identisch mit den Fällen, die wir in Tabelle III nebst Anhang aufgezählt haben.

§ 3.

10. Gegeben sind vier Zahlen a, b, c, m mit den Bedingungen:

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

Es heissen ϱ-Zahlen alle positiven Zahlen, die zu m teilerfremd sind. (Specielle ϱ-Zahlen werden wir auch mit ϱ', ϱ_1 u. s. w. bezeichnen).

Wir sagen, dass die Zahlen a, b, c, m ein System bilden, in Zeichen:

$$\{a, b, c\} \quad \text{oder} \quad m\{a, b, c\},$$

dann und nur dann, falls die $\varphi(m)$ folgenden Bedingungen erfüllt sind: *für jedes* $\varrho < m$ *ist*

(6) *entweder* $\varrho a < \varrho c < \varrho b \pmod m$ *oder* $\varrho a > \varrho c > \varrho b \pmod m$.

[Wegen der Symmetrie dieser Bedingungen in a und b wollen wir auch sagen, dass b, a, c, m ein System bilden; und wegen ihrer Invarianz gegenüber einer Änderung einer der Zahlen a, b, c (mod. m) wollen wir sagen, dass irgend vier Zahlen A, B, C, m ein System bilden, wenn es die Reste von A, B, C (mod. m) und m tun].

Das Ziel dieser Arbeit ist, alle solchen Systeme aufzusuchen. Diese sind nach Gruppen eingeteilt: mit $m\{a, b, c\}$ ist $m\{\varrho a, \varrho b, \varrho c\}$ ein System. Es würde genügen aus jeder Gruppe ein System aufzuzählen: mit Bezugnahme auf den 2. Hilfssatz werden wir alle Systeme aufzählen, wo c in m aufgeht.

Wir stellen also die Frage folgendermassen: Was sind alle Systeme

$$m\{a, b, c\}, \quad 0 < a < c < b < m, \quad (a, b, c, m) = 1, \quad c \mid m?$$

Oder, indem wir $m = cn$ setzen: *Was sind alle Systeme*

$$cn\{a, b, c\}, \quad 0 < a < c < b < cn, \quad (a, b, c) = 1,$$

für welche die $\varphi(m)$ *Bedingungen* (6) *erfüllt sind?*

Es sollen ϱ_1 die Zahlen ϱ heissen, die $< m$ und $\equiv 1 \pmod n$ sind. Es ist z. B. stets 1 ein ϱ_1.

Einige notwendige Bedingungen [20]) sind die folgenden: für jedes ϱ_1 ist

entweder $\varrho_1 a < \varrho_1 c < \varrho_1 b \pmod{cn}$ oder $\varrho_1 a > \varrho_1 c > \varrho_1 b \pmod{cn}$.

[20]) Dass sie nicht hinreichen, zeigt das Beispiel: $a = 2$, $c = 6$, $b = 11$, $n = 5$, also $m = 30$. Es ist wohl (6) für alle ϱ_1, d. h. für $\varrho_1 = 1$ und 11 erfüllt, nicht aber für $\varrho = 7$.

Wir bemerken, dass $\rho_1 c \equiv c \pmod{cn}$ ist für alle ρ_1. Wir werden zunächst folgendes Problem betrachten:

Was sind alle Systeme von vier Zahlen $0 < a < c < b < m = cn$, $(a, b, c) = 1$, *für welche folgende Bedingungen erfüllt sind:*

(7) *entweder* $\rho_1 a < c < \rho_1 b \pmod{m}$ *oder* $\rho_1 a > c > \rho_1 b \pmod{m}$,

für jede Zahl ρ_1, *die zu* m *teilerfremd,* $< m$ *und* $\equiv 1 \pmod{n}$ *ist?*

Ist diese Frage gelöst, so verificieren wir, für welche Systeme unter den gefundenen auch (6) erfüllt ist.

11. Jetzt wollen wir das eben genannte speciellere Problem ins Auge fassen.

Aus den Voraussetzungen folgt, dass in jedem System, das unsere Bedingungen erfüllt, $1 < c < m$, $1 < n < m$, $m \geq 4$ ist.

Wir wissen, dass die Zahlen $\rho < m$ eine Gruppe bilden, d. h., dass der kleinste positive Rest (mod. m) des Productes zweier ρ-Zahlen, die $< m$ sind, auch ein $\rho < m$ ist; ebenso bilden die ρ_1 eine Gruppe; denn, wegen $n \mid m$, ist auch der Rest (mod. m) des Productes zweier ρ_1-Zahlen zu 1 congruent (mod. n).

Gegeben sei ein beliebiges System, das unsere Bedingungen erfüllt. Wir nennen q die Anzahl der ρ_1. Es ist $q > 0$, da 1 stets ein ρ_1 ist. Es haben also $\rho_1 a$ und $\rho_1 b$ je q Werte. Wir setzen $q = q_a = q_b$.

Unter den q Zahlen $\rho_1 a$ sei s_a die Anzahl der $\rho_1 a$, die $< c \pmod{m}$ sind; ebenso s_b die Anzahl der $\rho_1 b$, die $< c \pmod{m}$ sind.

Da a, b, c, m die Bedingungen (7) erfüllen, so ist:

$$q = s_a + s_b.$$

Für $\rho_1 = 1$ ist $1 \cdot a < c \pmod{m}$. Also ist stets $s_a \geq 1$. Wir behaupten, dass $s_a \geq \frac{q}{2}$ ist. Wäre $s_a < \frac{q}{2}$, so wäre $s_b > \frac{q}{2}$, also, nach Satz V, II, wo wir b statt a setzen, $s_b = q_b = q$, also $s_a = 0$, ein Widerspruch zu $s_a \geq 1$.

Also ist $s_a \geq \frac{q}{2}$. Also ist entweder $s_a = \frac{q}{2}$ oder, nach Satz V, II, $s_a = q$.

Wir unterscheiden zwei Fälle:

I) $s_a = \frac{q}{2}$ also $s_b = \frac{q}{2}$.

II) $s_a = q$ also $s_b = 0$.

12. ERSTER HAUPTFALL:

$$s_a = \frac{q}{2}, \qquad s_b = \frac{q}{2}.$$

Die Hälfte aller $\rho_1 a$ ist $< c \pmod{cn}$, ebenso die Hälfte aller $\rho_1 b$. Wir stellen also die Nebenfrage, alle Zahlen $c > a > 0$, $n > 1$ zu finden, derart dass genau die Hälfte der $\rho_1 a < c \pmod{cn}$ ist, wobei ρ_1 alle positiven Zahlen durchläuft, die $< cn$, zu c teilerfremd und $\equiv 1 \pmod{n}$ sind.

13. *Lösung der Nebenfrage.* — Gegeben die Zahlen c, a, n, die die Bedingungen der Nebenfrage erfüllen. Damit sind auch ρ_1, q und s_a festgelegt; und es ist $s_a = \frac{q}{2}$.

Wir definieren wie im Satze V und in dessen Beweis die Zahlen q_a, e, c', a', k, r, ϱ_1'. Es ist $a' < c'$ und $q = q_a$. Nach unseren Voraussetzungen folgt nach Satz V, III, dass n, c', k der Tabelle III angehören müssen.

Also haben wir alle [21]) zulässigen n, c', k. Wir suchen jetzt alle n, c', r.

Betrachten wir irgend ein Zahlentripel n, c', k aus der Tabelle. Die Zahl k erfüllt alle Bedingungen, die die Zahl a' im Satze III erfüllt, nämlich: es ist $k \geqq 1$ und $(k, c') = 1$, nach der Anmerkung zur Tabelle. Da auch $k \leqq n$ ist, so ist k sein eigener Rest. Also ist nach Satze III, II jedes r congruent einem $\varrho_1' k$ (mod. $c'n$). Also, indem wir für alle n, c' die Reste aller $\varrho_1' k$ (mod. $c'n$) betrachten, so bekommen wir unter diesen Zahlen alle zulässigen r.

Es seien n, c', k fest. So muss jedes zugehörige a' folgende Bedingungen erfüllen: $a' \equiv k$ (mod. n), $(a', c') = 1$, $a' \leqq c'n$, wegen $a' < c'$. Also ist a' ein r, und zwar ein $r < c'$.

Also für alle n, c' gehören alle a' zu den Resten aller $\varrho_1' k$, die $< c'$ (mod. $c'n$) sind.

Aus der Gruppeneigenschaft der ϱ_1' folgt, dass wenn wir ein a' haben, die Reste aller $\varrho_1' a'$, die $< c'$ (mod. $c'n$) sind, ebenfalls a' sind. Also, da in der Tabelle $k < c'$ ist, so ist entweder k ein a' oder es ist kein $\varrho_1' k \equiv$ einem a'.

Wir brauchen also nur noch für jedes n, c', k der Tabelle III zu verificieren, ob es auch ein n, c', a' ist.

Es müssen n, $c = c'e$, $a = a'e$ so beschaffen sein, dass $a < c$ und $\frac{s_a}{q_a} = \frac{1}{2}$ ist. Da nach Satz V, I der Bruch $\frac{s_a}{q_a}$ von e unabhängig ist, so ist notwendig und hinreichend, indem man $e = 1$ setzt, dass $a' < c'$ ist und dass genau die Hälfte der $\varrho_1' a' < c'$ (mod. $c'n$) ist. Das werden wir also verificieren. Dass $k < c'$ ist, wissen wir schon.

Wir müssen auch nachher alle Zahlen $b > c > 0$, $n > 1$, $b < cn$ finden, derart dass die Hälfte der $\varrho_1 b < c$ (mod. cn) ist.

Im Satze V schreiben wir b statt a, E statt e, b' statt a'. Nach Satz V, I ist notwendig und hinreichend, dass $c' < b' < c'n$ ist und dass genau die Hälfte der $\varrho_1' b' > c'$ (mod. $c'n$) ist. Nimmt man aber den Rest eines $\varrho_1' b'$, das $< c'$ (mod. $c'n$) ist, so erfüllt es alle Bedingungen eines a'. Nimmt man den Rest eines $\varrho_1' a' > c'$ (mod. $c'n$), so ist es ein b'.

Also brauchen wir nur noch aus Tabelle III jedes n, c', k zu betrachten: ist genau die Hälfte der Reste der $\varrho_1' k$ (mod. $c'n$) auch $< c'$, so setzen wir sie $= a'$, und die anderen $= b'$.

Das gibt uns zwei neue Tabellen, die eine für n, c', a', die andere für n, c'', b'' (indem wir aus späteren Gründen ϱ_1'', c'', b'' statt ϱ_1', c', b' setzen). Diese zwei Ta-

---

[21]) Dass wir nur zulässige Systeme von Zahlen haben, brauchen wir uns wiederum nicht zu überlegen; vergl. [18]), [19]), [22]).

bellen wollen wir in eine gemeinsame vereinigen [22]). Wir wollen $c'n = m'$, $c''n = m''$ setzen. Wir lassen $n = 2$ ganz aus der nächsten Betrachtung weg und nehmen also an: $n \geqq 3$. Tabelle IV ordnen wir nach wachsenden n und $c' = c''$.

Nach dem Vorangehenden sind also $a = a'e$, $c = c'e$, $m = m'e$, $b = b''E$, $c = c''E$, $m = m''E$ zu setzen, wo e und E willkürliche positive Zahlen sind. Dann müssen wir paarweise je ein a und ein b, die zu denselben n und c gehören, combinieren, und sehen, ob wir ein System erhalten, das (7) erfüllt.

Tabelle IV.

	n	$c' = c''$	$m' = m''$	$\rho_1' = \rho_1''$	a'	b''
	$n = 3$					
α)		4	12	1, 7	1, 3	7, 9
β)		5	15	1, 4, 7, 13	1, 4	7, 13
γ)		8	24	1, 7, 13, 19	1, 7	13, 19
δ)		10	30	1, 7, 13, 19	1, 3, 7, 9	13, 19, 21, 27
ε)		20	60	1, 7, 13, 19, 31, 37, 43, 49	1, 7, 13, 19	31, 37, 43, 49
	$n = 4$					
α)		2	8	1, 5	1	5
β)		3	12	1, 5	1, 2	5, 10
γ)		6	24	1, 5, 13, 17	1, 5	13, 17
	$n = 5$					
α)		3	15	1, 11	1, 2	7, 11
β)		4	20	1, 11	1, 3	11, 13
γ)		6	30	1, 11	1, 5	11, 25
δ)		12	60	1, 11, 31, 41	1, 11	31, 41
	$n > 5$, gerade					
α)	n beliebig	2	$2n$	$1, n+1$	1	$n+1$
β)	$n \equiv 2 \pmod 6$	3	$3n$	$1, 2n+1$	1, 2	$2n+1, n+2$
	$n \equiv 4 \pmod 6$	3	$3n$	$1, n+1$	1, 2	$n+1, 2n+2$
	$n > 5$, ungerade					
α)	$n \equiv 1 \pmod 6$	3	$3n$	$1, n+1$	1, 2	$n+1, 2n+2$
	$n \equiv 5 \pmod 6$	3	$3n$	$1, 2n+1$	1, 2	$2n+1, n+2$
β)	$n \equiv 1 \pmod 4$	4	$4n$	$1, 2n+1$	1, 3	$2n+1, 2n+3$
	$n \equiv 3 \pmod 4$	4	$4n$	$1, 2n+1$	1, 3	$2n+1, 2n+3$
γ)	$n \equiv 1 \pmod 6$	6	$6n$	$1, 4n+1$	1, 5	$4n+1, 2n+5$
	$n \equiv 5 \pmod 6$	6	$6n$	$1, 2n+1$	1, 5	$2n+1, 4n+5$.

[22]) Die Bildung der Tabelle IV enthält also jetzt die Verification, dass wir bisher keine unnützen Systeme von Zahlen haben: da wirklich jedes k ein zulässiges a' ist, so musste in Tabellen II und III überall $S = \frac{Q}{2}$ sein.

14. Gegeben ein m und ein c, also ein $n = \frac{m}{c}$, so haben wir für e gewisse Möglichkeiten, also auch für $\frac{m}{e} = m'$, $\frac{c}{e} = c'$; die Tabelle gibt dann die zugehörigen a', also die $a = a'e$. Ebenso für E, also auch für $\frac{m}{E} = m''$, $\frac{c}{E} = c''$; die Tabelle gibt die b'', also die $b = b''E$. Wenn also ein m und ein c gegeben sind, so haben wir alle a und alle b.

Aus $(a, b, c) = 1$ folgt die notwendige Bedingung $(e, E) = 1$.

Jetzt wollen wir bei festen n, c, m untersuchen, für welche Paare a, b die Bedingung (7) erfüllt ist; denn, wir wissen nicht ob $\rho_1 a < c \pmod m$ für genau dieselben ρ_1 wird, für welche auch $\rho_1 b > c \pmod m$ wird.

Bei den folgenden Versuchen schreiben wir näturlich nur die Reste (mod. m).

Es wird folgende Betrachtung unsere Versuche etwas vereinfachen.

Wir müssen $m'e$, $a'e$, $c'e$ mit $m''E$, $c''E$, $b''E$ folgendermassen combinieren: es wird $m'e = m''E = m$ gesetzt, also $c'e = c''E = c$; dann $a'e = a$, $b''E = b$; dann müssen wir sehen, ob m, a, b, c für alle ρ_1 die Bedingung (7) erfüllen. Es kann unter Umständen eintreten, dass für ein gewisses ρ_1, es heisse P_1, welches $\equiv 1 \pmod{m'}$ ist, $c'' > P_1 b'' \pmod{m''}$ ist. Wegen $P_1 a' \equiv a' < c' \pmod{m'}$ und $c'' > P_1 b'' \pmod{m''}$ ist also

$$P_1 a < c \pmod m \qquad \text{und} \qquad c > P_1 b \pmod m.$$

Dann liefern m, a, b, c kein System.

Dies tritt natürlich nicht ein in Combinationen wie α) mit α), β) mit β), u. s. w.; denn, in solchen Fällen ist $m' = m''$; daher $e = E$; wegen $(e, E) = 1$ ist $e = E = 1$, $m' = m'' = m$; die Zahl 1 ist das einzige ρ_1, welches $\equiv 1 \pmod{m'}$ ist; und $\rho_1 = 1$ ist natürlich kein P_1, da stets $1.b'' > c'' \pmod{m''}$ ist.

Es kann also nur bei Combinationen wie α) mit β) u. s. w. ein P_1 existieren.

Es sei schon für zwei Zeilen, z. B. α) und β), gezeigt, dass sie in der Combination α) mit β) kein System liefern. Wir behaupten, dass auch β) mit α) kein System gibt. Die Voraussetzung lautet folgendermassen: es sei irgend ein a' von α) und irgend ein b'' von β); dann ist $m = nc'e = nc''E$, $a = a'e$, $b = b''E$, $c = c'e = c''E$ kein System. Es soll sich ein Widerspruch ergeben, falls für ein a' von β), es heisse a'', und ein b'' von α), es heisse b', die Zahlen, m, $a''E$, $b'e$, c ein System bilden.

Aus der Annahme, dass m, $a''E$, $b'e$, c ein System des ersten Hauptfalles bilden, folgt $\rho_1 a''E > c > \rho_1 b'e \pmod m$ für die Hälfte der ρ_1, also, wegen $q > 0$, für mindestens ein ρ_1. Der Rest von $\rho_1 a'' \pmod{m''}$ ist ein b'' von β) und der Rest von $\rho_1 b' \pmod{m'}$ ist ein a' von α). Dies widerspricht der Voraussetzung.

Wir wollen jetzt für jede Combination ein P_1 suchen:

$n = 3$:

α) mit β) $m = 12\, e = 15\, E$; $e = 5$, $E = 4$; $m = 60$. Für $P_1 = 13$ ist $5 > 13.7 \equiv 1$ und $5 > 13.13 \equiv 4 \pmod{15}$.

α) mit γ) $e=2$, $E=1$; $m=24$. Für $P_1=13$ ist $8>13.13\equiv 1$ und $8>13.19\equiv 7$ (mod. 24).

α) mit δ) $e=5$, $E=2$; $m=60$. Für $P_1=49$ ist $10>49.13\equiv 7$; $10>49.19\equiv 1$; $10>49.21\equiv 9$ und $10>49.27\equiv 3$ (mod. 30).

α) mit ε) $e=5$, $E=1$; $m=60$. Für $P_1=49$ ist $20>49.31\equiv 19$; $20>49.37\equiv 13$; $20>49.43\equiv 7$ und $20>49.49\equiv 1$ (mod. 60).

β) mit γ) $e=8$, $E=5$; $m=120$. Für $P_1=61$ ist $8>61.13\equiv 1$ und $8>61.19\equiv 7$ (mod. 24).

β) mit δ) $e=2$, $E=1$; $m=30$. Es gibt kein P_1.

β) mit ε) $e=4$, $E=1$; $m=60$. Für $P_1=31$ ist $20>31.31\equiv 1$; $20>31.37\equiv 7$; $20>31.43\equiv 13$ und $20>31.49\equiv 19$ (mod. 60).

γ) mit δ) $e=5$, $E=4$; $m=120$. Für $P_1=49$ ist $10>49.13\equiv 7$; $10>49.19\equiv 1$; $10>49.21\equiv 9$ und $10>49.27\equiv 3$ (mod. 30).

γ) mit ε) $e=5$, $E=2$; $m=120$. Für $P_1=49$ ist $20>49.31\equiv 19$; $20>49.37\equiv 13$; $20>49.43\equiv 7$ und $20>49.49\equiv 1$ (mod. 60).

δ) mit ε) $e=2$, $E=1$; $m=60$. Für $P_1=31$ ist $20>31.31\equiv 1$; $20>31.37\equiv 7$; $20>31.43\equiv 13$ und $20>31.49\equiv 19$ (mod. 60).

$n=4$:

α) mit β) $e=3$, $E=2$; $m=24$. Für $P_1=17$ ist $3>17.5\equiv 1$ und $3>17.10\equiv 2$ (mod. 12).

α) mit γ) $e=3$, $E=1$; $m=24$. Für $P_1=17$ ist $6>17.13\equiv 5$ und $6>17.17\equiv 1$ (mod. 24).

β) mit γ) $e=2$, $E=1$; $m=24$. Für $P_1=13$ ist $6>13.13\equiv 1$ und $6>13.17\equiv 5$ (mod. 24).

$n=5$:

α) mit β) $e=4$, $E=3$; $m=60$. Für $P_1=31$ ist $4>31.11\equiv 1$ und $4>31.13\equiv 3$ (mod. 20).

α) mit γ) $e=2$, $E=1$; $m=30$. Es gibt kein P_1.

α) mit δ) $e=4$, $E=1$; $m=60$. Für $P_1=31$ ist $12>31.31\equiv 1$ und $12>31.41\equiv 11$ (mod. 60).

β) mit γ) $e=3$, $E=2$; $m=60$. Für $P_1=41$ ist $6>41.11\equiv 1$ und $6>41.25\equiv 5$ (mod. 30).

β) mit δ) $e=3$, $E=1$; $m=60$. Für $P_1=41$ ist $12>41.31\equiv 11$ und $12>41.41\equiv 1$ (mod. 60).

γ) mit δ) $e=2$, $E=1$; $m=60$. Für $P_1=31$ ist $12>31.31\equiv 1$ und $12>31.41\equiv 11$ (mod. 60)

$n>5$, gerade:

α) mit β) $e=3$, $E=2$; $m=6n$.

Es sei $n\equiv 2$ (mod. 6). Für $P_1=2n+1$ ist $3>(2n+1)(2n+1)\equiv 1$ und $3>(2n+1)(n+2)\equiv 2$ (mod. $3n$).

Es sei $n\equiv 4$ (mod. 6). Für $P_1=4n+1$ ist $3>(4n+1)(n+1)\equiv 1$ und $3>(4n+1)(2n+2)\equiv 2$ (mod. $3n$).

$n > 5$, ungerade:

α) mit β) $e = 4$, $E = 3$; $m = 12n$. In allen Fällen: für $P_1 = 6n + 1$ ist $4 > (6n + 1)(2n + 1) \equiv 1$ und $4 > (6n + 1)(2n + 3) \equiv 3 \pmod{4n}$.

α) mit γ) $e = 2$, $E = 1$; $m = 6n$. Es gibt kein P_1.

β) mit γ) $e = 3$, $E = 2$; $m = 12n$.

Es sei $n \equiv 1 \pmod 6$. Für $P_1 = 4n + 1$ ist $6 > (4n + 1)(4n + 1) \equiv 1$ und $6 > (4n + 1)(2n + 5) \equiv 5 \pmod{6n}$.

Es sei $n \equiv 5 \pmod 6$. Für $P_1 = 8n + 1$ ist $6 > (8n + 1)(2n + 1) \equiv 1$ und $6 > (8n + 1)(4n + 5) \equiv 5 \pmod{6n}$.

Den Fall $n = 3$, β) mit δ) werden wir ganz anders widerlegen: es ist $e = 2$, $E = 1$; $m = 30$; $a = 2$ oder 8; $b = 13$ oder 19 oder 21 oder 27; $c = 10$. Für $\rho_1 = 19$ ist $\rho_1 c \equiv 19.10 \equiv 10 > 19.2 \equiv 8$; $10 > 19.8 \equiv 2$; $10 > 19.13 \equiv 7$; $10 > 19.19 \equiv 1$; $10 > 19.21 \equiv 9$ und $10 > 19.27 \equiv 3 \pmod{30}$.

In den Fällen $n = 5$, α) mit γ), γ) mit α) und $n > 5$, ungerade, α) mit γ), γ) mit α) ist (7) erfüllt [23]).

Es bleiben jetzt solche Combinationen wie α) mit α) u. s. w. zu untersuchen, wo $e = E = 1$ ist. In allen Fällen (also $n = 3, 4, 5$ oder $n > 5$) ist (7) erfüllt [23]), ausser für:

$n = 3$, δ) mit δ); $m = 30$, in folgenden Combinationen:

$a = 1$ oder 9; $b = 13$ oder 27; $c = 10$. Für $\rho_1 = 13$ ist $13.10 \equiv 10 < 13.1 \equiv 13$; $10 < 13.9 \equiv 27$; $10 < 13.13 \equiv 19$ und $10 < 13.27 \equiv 21 \pmod{30}$;

$a = 3$ oder 7; $b = 19$ oder 21; $c = 10$. Für $\rho_1 = 13$ ist $10 > 13.3 \equiv 9$; $10 > 13.7 \equiv 1$; $10 > 13.19 \equiv 7$ und $10 > 13.21 \equiv 3 \pmod{30}$.

$n = 3$, ε) mit ε); $m = 60$, in folgenden Combinationen:

$a = 1$ oder 19; $b = 37$ oder 43; $c = 20$. Für $\rho_1 = 13$ ist $13.20 \equiv 20 > 13.1 \equiv 13$; $20 > 13.19 \equiv 7$; $20 > 13.37 \equiv 1$ und $20 > 13.43 \equiv 19 \pmod{60}$;

$a = 7$ oder 13; $b = 31$ oder 49; $c = 20$. Für $\rho_1 = 13$ ist $20 < 13.7 \equiv 31$; $20 < 13.13 \equiv 49$; $20 < 13.31 \equiv 43$ und $20 < 13.49 \equiv 37 \pmod{60}$.

Wir haben jetzt überhaupt alle Fälle, wo $n > 2$ und $s_a = s_b = \frac{q}{2}$ ist, aufgezählt, die die Bedingung (7) erfüllen.

15. ZWEITER HAUPTFALL:

$$s_a = q, \quad s_b = 0.$$

Wir stellen die Nebenfrage, alle $c > a > 0$, $n > 1$ zu finden, derart dass alle $\rho_1 a < c \pmod{cn}$ sind. Die Lösung ist ganz analog der vorigen (Nr. 13).

Gegeben drei Zahlen c, a, n, die die Bedingungen der Nebenfrage erfüllen. Damit sind auch ρ_1, q und s_a festgelegt; und es ist $s_a = q$. Wir definieren wie im Satze V und in dessen Beweis die Zahlen q_a, e, c', a', k, r, ρ_1'. Es ist $a' < c'$ und $q = q_a$.

---

[23]) Das Erfülltsein braucht nicht im Texte verificiert zu werden: unzulässige Systeme würden wir doch in Nr. 17 entdecken.

Nach unseren Voraussetzungen folgt nach Satz V, III, dass n, c', k dem Anhang der Tabelle III angehören müssen.

Wegen $n > 1$ ist also n ungerade > 1, $c' = 2$, $k = 1$. Daher ist $r = 1$.

Es seien n, c', k fest. So muss jedes zugehörige a' folgende Bedingungen erfüllen: $a' \equiv k \pmod{n}$, $(a', c') = 1$, $a' \leqq c'n$, wegen $a' < c'$. Also ist a' ein r; also kann nur $a' = 1$ sein.

Die Verification ist leicht gemacht: ϱ'_1 hat nur den Wert 1. Also sind alle $\varrho'_1 a' < c' \pmod{c'n}$.

Also ist jedes System von Zahlen: n ungerade > 1, $c' = 2$, $a' = 1$ zulässig; also, indem wir mit einem beliebigen e multiplicieren, ist n eine beliebige ungerade Zahl > 1, $c = 2e$, $a = e$.

Wir wissen wegen $(a, b, c) = 1$, dass $(e, b) = 1$ ist; ausserdem ist bisher über b und e nur festgestellt worden, dass $s_b = 0$ ist.

In diesem Fall ist von selbst $n \neq 2$.

16. Jetzt müssen wir untersuchen, ob die Bedingung (6), die mehr [24]) besagt als (7), erfüllt ist. Im ersten Hauptfall ist dies schliesslich nur eine kurze Verification. Im zweiten dagegen werden wir b, e bestimmen müssen; das gibt zu einer ganz anderen Methode Anlass.

17. Erster Hauptfall. — Die Verification wird in vielen Fällen dadurch erleichtert, dass die Landausche Arbeit [25]) in einer Tabelle alle ihm bekannten Systeme $m\{a, b, c\}$ angibt, ausser den unendlich vielen, die er als Nr. I bezeichnet [26]) (ein solches ist $8\{1, 5, 2\}$).

Uns sind also bisher die folgenden Systeme des ersten Hauptfalls begegnet:

$n = 3$:

$12\{1$ oder $3, 7$ oder $9, 4\}$ [27]); $15\{1$ oder $4, 7$ oder $13, 5\}$;
$24\{1$ oder $7, 13$ oder $19, 8\}$; $30\{1$ oder $9, 19$ oder $21, 10\}$;
$30\{3$ oder $7, 13$ oder $27, 10\}$; $60\{1$ oder $19, 31$ oder $49, 20\}$;
$60\{7$ oder $13, 37$ oder $43, 20\}$.

$n = 4$:

$8\{1, 5, 2\}$; $12\{1$ oder $2, 5$ oder $10, 3\}$; $24\{1$ oder $5, 13$ oder $17, 6\}$.

$n = 5$:

$15\{1$ oder $2, 7$ oder $11, 3\}$; $20\{1$ oder $3, 11$ oder $13, 4\}$;
$30\{1$ oder $5, 11$ oder $25, 6\}$; $60\{1$ oder $11, 31$ oder $41, 12\}$.

Dagegen gibt die Combination von α) mit γ) kein System:

---

[24]) Vergl. [20]).

[25]) Op. cit. [8]), p. 35 sqq.

[26]) Op. cit. [8]), p. 33.

[27]) Die Alternativen für b sind überall unabhängig von den Alternativen für a.

$m=30$; $a=2$ oder 4; $b=11$ oder 25; $c=6$. Für $\rho=13$ ist $13.6\equiv 18<13.2\equiv 26$; $18<13.4\equiv 22$; $18<13.11\equiv 23$ und $18<13.25\equiv 25 \pmod{30}$.

Damit ist auch die Combination von γ) mit α) widerlegt.

$n>5$, gerade:

$$2n\{1,\ n+1,\ 2\}\ \text{[Fall I von LANDAU [28])]}.$$

Es gibt sonst kein System:

$m=3n$; $n\equiv 2 \pmod 6$, also $n\geq 8$; $a=1,\ 2$; $b=2n+1,\ n+2$; $c=3$. Für $\rho=n+3$ ist $\rho c\equiv 9<\rho a\equiv n+3,\ 2n+6$; $9<\rho b\equiv 2n+3,\ n+6 \pmod{3n}$.

$m=3n$; $n\equiv 4 \pmod 6$, also $n\geq 10$; $a=1,\ 2$; $b=n+1,\ 2n+2$; $c=3$. Für $\rho=n+3$ ist $\rho c\equiv 9<\rho a\equiv n+3,\ 2n+6$; $9<\rho b\equiv 2n+3,\ n+6 \pmod{3n}$.

$n>5$, ungerade:

$m=3n$; $n\equiv 1 \pmod 6$, also $n\geq 7$; $a=1,\ 2$; $b=n+1,\ 2n+2$; $c=3$. Für $\rho=n+3$ ist $\rho c\equiv 9<\rho a\equiv n+3,\ 2n+6$; $9<\rho b\equiv 2n+3,\ n+6 \pmod{3n}$.

$m=3n$; $n\equiv 5 \pmod 6$, also $n\geq 11$; $a=1,\ 2$; $b=2n+1,\ n+2$; $c=3$. Für $\rho=n+3$ ist $\rho c\equiv 9<\rho a\equiv n+3,\ 2n+6$; $9<\rho b\equiv 2n+3,\ n+6 \pmod{3n}$.

$m=4n$; $n\geq 7$; $a=1,\ 3$; $b=2n+1,\ 2n+3$; $c=4$. Für $\rho=n+2$ ist $\rho c\equiv 8<\rho a\equiv n+2,\ 3n+6$; $8<\rho b\equiv 3n+2,\ n+6 \pmod{4n}$.

$m=6n$; $n\equiv 1 \pmod 6$, also $n\geq 7$; $a=1,\ 5$; $b=4n+1,\ 2n+5$; $c=6$. Für $\rho=3n+2$ ist $\rho c\equiv 12<\rho a\equiv 3n+2,\ 3n+10$; $12<\rho b\equiv 5n+2,\ n+10 \pmod{6n}$.

$m=6n$; $n\equiv 5 \pmod 6$, also $n\geq 11$; $a=1,\ 5$; $b=2n+1,\ 4n+5$; $c=6$. Für $\rho=3n+2$ ist $\rho c\equiv 12<\rho a\equiv 3n+2,\ 3n+10$; $12<\rho b\equiv n+2,\ 5n+10 \pmod{6n}$.

Ebenso gibt die Combination von α) mit γ) kein System:

$m=6n$, $n\equiv 1 \pmod 6$, also $n\geq 7$; $a=2,\ 4$; $b=4n+1,\ 2n+5$; $c=6$. Für $\rho=n-2$ ist $\rho c\equiv 6n-12>\rho a\equiv 2n-4,\ 4n-8$; $6n-12>\rho b\equiv 3n-2,\ 3n-10 \pmod{6n}$.

$m=6n$, $n\equiv 5 \pmod 6$, also $n\geq 11$; $a=2,\ 4$; $b=2n+1,\ 4n+5$; $c=6$. Für $\rho=n+2$ ist $\rho c\equiv 12<\rho a\equiv 2n+4,\ 4n+8$; $12<\rho b\equiv 3n+2,\ 3n+10 \pmod{6n}$.

Die Combination von γ) mit α) ist also auch unzulässig.

Damit ist diese Discussion fertig.

18. ZWEITER HAUPTFALL.

Es ist $m=2en$, n ungerade >1, $a=e$, $c=2e$, $(e,\ b)=1$, also $c=2a$.

Vorbemerkung: Zunächst ist klar, dass wir im ersten Hauptfalle schon alle Systeme, wo $c\,|\,m$ ist, aufgezählt haben, für welche zugleich $c\neq\frac{m}{2}$ und $c\neq 2a$ ist. $\left(c\neq\frac{m}{2}\right.$ heisst in unserer Bezeichnung $\left.n\neq 2\right)$.

---

[28]) Op. cit. [8]), p. 33.

Was sind alle Systeme $2en\{e, b, 2e\}$, $(e, b) = 1$, n ungerade > 1?

Wir wollen zunächst zwei Specialfälle erledigen:

1) $b = 3e$, also wegen $(e, b) = 1$, $e = 1$. Wann ist $2n\{1, 3, 2\}$, n ungerade > 1, ein System? Für $\rho = n - 2$ ist $\rho.1 < \rho.2 \pmod{2n}$. Es muss also sein $\rho.2 < \rho.3 \pmod{2n}$ oder $2n - 4 < 3n - 6 \equiv n - 6 \pmod{2n}$, also $n = 3$ oder 5. Das gibt also nur die Systeme: $6\{1, 3, 2\}$, $10\{1, 3, 2\}$.

2) $b = en + e$, also wegen $(e, b) = 1$, $e = 1$. Wann ist $2n\{1, n + 1, 2\}$, n ungerade > 1, ein System? Offenbar immer.

Wir stellen jetzt die Frage: was sind alle Systeme $2en\{e, b, 2e\}$, $(e, b) = 1$, n ungerade > 1, $b \neq 3e$, $b \neq en + e$?

Mit $m\{\rho a, \rho b, \rho c\}$ ist stets auch $m\{\rho c - \rho a, m - \rho a, \rho b - \rho a\}$ ein System und umgekehrt, wie man leicht sieht [vergl. op. cit. [8]), p. 25]. Wir brauchen also nur alle Systeme $2en\{\rho e, 2en - \rho e, \rho b - \rho e\}$ aufzusuchen, oder sogar nur eins aus jeder Gruppe, mit den Nebenbedingungen $(e, b - e) = 1$, n ungerade > 1, $b \neq 3e$, $b \neq en + e$; nach Hilfssatz II können wir ρ so bestimmen, dass der Rest von $\rho b - \rho e \pmod{2en}$ in $2en$ aufgeht; das zugehörige $m\{\rho a, \rho b, \rho c\}$ ist ein System der Gruppe $2en\{\rho e, \rho b, \rho.2e\}$, womit wir auch das System für $\rho = 1$ leicht erhalten.

Was sind also alle Systeme $M\{A, B, C\}$, mit den Nebenbedingungen: $\frac{M}{2(M, A)}$ ungerade > 1, $B = M - A$, $(M, A, C) = 1$, $C \mid M$ also $(A, C) = 1$, $C \neq 2A$ wegen $\rho(b - e) \not\equiv \rho.2e \pmod{m}$, und $C \neq \frac{M}{2}$ wegen $\rho(b - e) \not\equiv \rho.en \pmod{m}$?

Es sei $A < B$. Nach der Vorbemerkung haben wir schon alle solchen Systeme im ersten Hauptfalle aufgezählt. Es sind:

$$30\{9, 21, 10\}, \quad 30\{3, 27, 10\}, \quad 12\{2, 10, 3\}, \quad 30\{5, 25, 6\}.$$

Es ist: $\rho e = A$, $\rho b = \rho e + C = A + C$. Das gibt:

$$30\{9, 19, 18\}, \quad 30\{3, 13, 6\}, \quad 12\{2, 5, 4\}, \quad 30\{5, 11, 10\}.$$

Das sind die Systeme $2en\{\rho e, \rho b, \rho.2e\}$ [29]). Jetzt brauchen wir nur mit allen ρ' zu multiplicieren, die so beschaffen sind, dass $\rho'.\rho.2e$ congruent ist einem Factor von m, also sicher dem Factor $2e$, in Zeichen: $\rho'\rho 2e \equiv 2e \pmod{2en}$:

$30\{9, 19, 18\}$ für $\rho' = 7$ und 17 gibt $30\{3, 13, 6\}$ und $30\{3, 23, 6\}$;

$30\{3, 13, 6\}$ für $\rho' = 1$ und 11 gibt dasselbe;

$12\{2, 5, 4\}$ für $\rho' = 1$ und 7 gibt $12\{2, 5, 4\}$ und $12\{2, 11, 4\}$;

$30\{5, 11, 10\}$ für $\rho' = 1$, 7, 13 und 19 gibt $30\{5, 11, 10\}$, $30\{5, 17, 10\}$, $30\{5, 23, 10\}$ und $30\{5, 29, 10\}$.

Es sei jetzt $B < A$, $C \neq 2B$. Das gibt dieselben vier Systeme aus dem ersten Hauptfall, wo aber A und B ihre Rollen vertauscht haben. Das gibt aber für den

---

[29]) Wir haben schon jetzt mindestens ein System jeder Gruppe und dürften den Fall $A < B$ schliessen; aber es ist noch nicht $m = cn$.

zweiten Hauptfall nichts neues; denn:

$$30\{21, 9, 10\}, \quad 30\{27, 3, 10\}, \quad 12\{10, 2, 3\} \text{ und } 30\{25, 5, 6\}$$

werden

$$30\{9, 21, 10\}, \quad 30\{3, 27, 10\}, \quad 12\{2, 10, 3\} \text{ und } 30\{5, 25, 6\},$$

für $\rho = 19, 19, 5$ und 11.

Es sei endlich $B < A$, $C = 2B$, also $2M - 2A = C$. Wegen $(A, C) = 1$ ist $(A, M) = 1$, $\frac{M}{2}$ ungerade > 1. Es gibt aber ein ρ, sodass: $\rho . A \equiv \frac{M}{2} + 2$ ist; also $\rho . B \equiv \frac{M}{2} - 2$, $\rho . C \equiv M - 4 \pmod{M}$ ist. Es ist also $M - 4 < \frac{M}{2} + 2$, $M = 6$ oder 10. Das gibt für $M\{A, B, C\}$: $6\{5, 1, 2\}$, $10\{9, 1, 2\}$.

Es ist $\rho e = A$, $\rho b = \rho e + C = A + C$. Das gibt: $6\{5, 1, 4\}$, $10\{9, 1, 8\}$.

Jetzt multiplicieren wir mit ρ' wie vorhin:

$$6\{5, 1, 4\} \text{ für } \rho' = 5 \text{ gibt } 6\{1, 5, 2\};$$
$$10\{9, 1, 8\} \text{ für } \rho' = 9 \text{ gibt } 10\{1, 9, 2\}.$$

Somit haben wir alle Systeme überhaupt, wo $c \mid m$, $c \neq \frac{m}{2}$ ist.

19. Der Fall $n = 2$, also $c = \frac{m}{2}$.

Es ist klar, dass für alle a, b, c, $m = 2c$, die Hälfte der $\rho a < c$ und die Hälfte der $\rho b > c \pmod{m}$ ist. Daher konnte uns die Methode des ersten Hauptfalls nichts liefern.

Wir bemerken zunächst, dass für alle geraden m und alle $a < \frac{m}{2}$, die folgenden Zahlen ein System bilden: $m\left\{a, \frac{m}{2} + a, \frac{m}{2}\right\}$.

Was sind jetzt alle Systeme $m\left\{a, b, \frac{m}{2}\right\}$, $b \neq a + \frac{m}{2}$, m gerade?

Es genügt sogar ein System aus jeder Gruppe $m\left\{\rho a, \rho b, \frac{m}{2}\right\}$ aufzuzählen, z. B. dasjenige, für welches der Rest von $\rho(b - a) \pmod{m}$ in m aufgeht; natürlich ist für jedes ρ: $\rho(b - a) \not\equiv \frac{m}{2} \pmod{m}$.

Setzen wir a für den Rest von ρa und b für den Rest von ρb, so stellen wir die Frage: was sind alle Systeme $m\left\{a, b, \frac{m}{2}\right\}$, m gerade, $b - a \not\equiv \frac{m}{2}$, für welche der Rest von $b - a$ in m aufgeht?

Mit $m\left\{a, b, \frac{m}{2}\right\}$ ist stets $m\left\{\frac{m}{2} - a, m - a, b - a\right\}$ ein System [vergl. op. cit. [8]), p. 25]. Was sind also alle Systeme $M\{A, B, C\}$, M gerade, $B \equiv \frac{M}{2} + A$, $C \mid M$, $C \neq \frac{M}{2}$?

Es sei $A < B$, also $B = \frac{M}{2} + A$. Die Systeme sind:

$12\{1, 7, 4\}$, $12\{3, 9, 4\}$, $24\{1, 13, 8\}$, $24\{7, 19, 8\}$,
$60\{1, 31, 20\}$, $60\{19, 49, 20\}$, $60\{7, 37, 20\}$, $60\{13, 43, 20\}$,
$24\{1, 13, 6\}$, $24\{5, 17, 6\}$, $20\{1, 11, 4\}$, $20\{3, 13, 4\}$,
$60\{1, 31, 12\}$, $60\{11, 41, 12\}$ und $2n\{1, n+1, 2\}$, $n \geq 3$, beliebig [30].

Dazu gehören die folgenden Systeme $m\{a, b, \frac{m}{2}\}$:

$12\{5, 9, 6\}$, $12\{3, 7, 6\}$, $24\{11, 19, 12\}$, $24\{5, 13, 12\}$,
$60\{29, 49, 30\}$, $60\{11, 31, 30\}$, $60\{23, 43, 30\}$, $60\{17, 37, 30\}$,
$24\{11, 17, 12\}$, $24\{7, 13, 12\}$, $20\{9, 13, 10\}$, $20\{7, 11, 10\}$,
$60\{29, 41, 30\}$, $60\{19, 31, 30\}$ und $2n\{n-1, n+1, n\}$, $n \geq 3$.

Es sei jetzt $A > B$, also $A = \frac{M}{2} + B$. Wir erhalten dieselben Systeme, wo A und B ihre Rollen vertauscht haben. Ausser einem sind diese Systeme aber keine neuen; denn in allen Systemen, wo $M \equiv 0 \pmod 4$ ist, ist $\frac{M}{2} + 1$ ein ρ; und dieses ρ bewirkt eben die Umtauschung, wie man leicht verificieren kann: z. B. $12\{1, 7, 4\}$ wird $12\{7, 1, 4\}$ durch $\rho = 7$, u. s. w. Also liefern uns die neuen $M\{A, B, C\}$ nur Systeme in den schon erhaltenen Gruppen, ausser das letzte, falls $M \equiv 2 \pmod 4$ ist, nämlich $2n\{n+1, 1, 2\}$, n ungerade > 1. Dies gibt in der Tat das neue System: $2n\{2n-1, 1, n\}$ oder, was dasselbe ist, $2n\{1, 2n-1, n\}$ für alle ungeraden $n > 1$.

Durch Multiplication mit allen ρ-Zahlen erhalten wir alle Systeme, wo $c = \frac{m}{2}$ ist.

20. SCHLUSSWORT: Jetzt haben wir alle Systeme, wo c ein Teiler von m ist. Durch Multiplication mit allen ρ-Zahlen erhalten wir alle Systeme überhaupt. Ein Vergleich mit Herrn LANDAUS Tabelle [31] zeigt, dass Herr SCHWARZ alle Möglichkeiten erschöpft hatte. Also folgt, was schon in der Einleitung erwähnt wurde, dass die ρ-Bedingung auch hinreichend ist dafür, dass die hypergeometrische Reihe algebraisch ist.

Göttingen, den 22. Juli 1912.

ALFRED ERRERA.

---

[30]) Dieser Fall kommt von verschiedenen Seiten her: für $n = 4$: $8\{1, 5, 2\}$ und für n gerade > 5: s. Nr. 17; für n ungerade > 1 s. Nr. 18, 2). $n = 2$ ist wegen $c \neq \frac{M}{2}$ auszuschliessen.

[31]) L. c. [8]), p. 33 und pp. 35-37; vergl. [11]).