

Werk

Titel: Encyklopädie und elementare Darstellung der Theorie der Zahlen. (Fortsetzung).

Autor: Crelle, A.L.

Jahr: 1844

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0027|log15

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

✉ info@digizeitschriften.de

10. Encyklopädische und elementare Darstellung der Theorie der Zahlen.

(Vom Herausgeber dieses Journals.)

(Fortsetzung der Abhandlung No. 2. im vorigen Heft.)

§. 21.

Erläuterung.

Jede theilbare ganze Zahl z kann z. B. durch

$$z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu$$

ausgedrückt werden, wo die Factoren $a, b, c, d \dots n$ von z entweder theilbare, unter einander theilerverwandte, oder theilerfremde, oder auch untheilbare ganze Zahlen sein *können*, die Exponenten $\alpha, \beta, \gamma, \dots \nu$ aber *nothwendig* ganze *positive* Zahlen sind.

Denn eine theilbare ganze Zahl z ist nichts anderes als das *Product* anderer ganzen Zahlen, die selbst wiederum theilbar, unter einander theilerverwandt, oder theilerfremd, oder auch untheilbar sein können. Diejenigen unter diesen Factoren, welche einander *gleich sind*, wie z. B. alle die, welche gleich a sind, geben für sich, in einander multiplicirt, eine *Potenz* mit ganzzahligen positiven Exponenten. Z. B. wenn a α mal als Factor vorkommt, so entsteht daraus die Potenz a^α ; b , wenn es β mal vorkommt, giebt die Potenz b^β u. s. w., und das Product aller dieser Potenzen macht die Zahl z aus.

§. 22.

Lehrsatz.

I. Wenn von einer ganzen Zahl z , die nach (§. 21.) immer durch

$$1. \quad z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu$$

ausgedrückt werden kann, keiner der Factoren $a, b, c, d, \dots n$ mit einer andern beliebigen ganzen Zahl u theilerverwandt ist, so ist auch z selbst mit u nicht theilerverwandt, sondern zu u theilerfremd.

II. Wenn von einer ganzen Zahl

$$2. \quad z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu$$

keiner der Factoren $a, b, c, d, \dots n$ mit irgend einem der Factoren $a_1, b_1, c_1, \dots k_1$ einer andern ganzen Zahl

$$3. \quad u = a_1^{\alpha_1} b_1^{\beta_1} c_1^{\gamma_1} \dots k_1^{\nu_1}$$

theilerverwandt ist, so sind auch z und u selbst nicht theilerverwandt, sondern zu einander theilerfremd.

III. *Wenn die Factoren $a, b, c, \dots n$ und $a_1, b_1, c_1, \dots k_1$ der beiden Zahlen z und u (2. u. 3.) sämtlich Stammzahlen sind, und keiner der Factoren $a, b, c, \dots n$ ist irgend einem der Factoren $a_1, b_1, c_1, \dots k_1$ gleich, so sind z und u zu einander theilerfremd.*

Beweis von I. *A.* Da nach der Voraussetzung a in (1.) zu u theilerfremd ist, so ist es nach (§. 20. I.) auch das **Product** $a.a$ oder a^2 . Folglich sind a und a^2 beide zu u theilerfremd. Also ist es nach (§. 20. I.) auch ihr **Product** $a.a^2$ oder a^3 . Also sind a und a^3 beide zu u theilerfremd, und folglich ist es auch ihr **Product** $a.a^3 = a^4$. Und so weiter. Also ist zuletzt a^α zu u theilerfremd.

B. Aus gleichen Gründen sind, da $b, c, d, \dots n$ sämtlich der Voraussetzung nach zu u theilerfremd sind, auch $b^\beta, c^\gamma, d^\delta, \dots n^\nu$ zu u theilerfremd. U. s. w.

C. Da weiter z. B. a^α und b^β beide zu u theilerfremd sind, so ist es nach (§. 20. I.) auch ihr **Product** $a^\alpha b^\beta$. Und da demzufolge $a^\alpha b^\beta$ und c^γ (*B.*) beide zu u theilerfremd sind, so ist es nach (§. 20. I.) auch ihr **Product** $a^\alpha b^\beta c^\gamma$. So ist weiter, aus gleichen Gründen, $a^\alpha b^\beta c^\gamma d^\delta$ u. s. w. und folglich zuletzt $z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu$ nothwendig zu u theilerfremd; wie es (I.) behauptet.

Beweis von II. *D.* Da nach der Voraussetzung in (II.) keiner der Factoren $a_1, b_1, c_1, \dots k_1$ von u z. B. mit dem Factor a von z theilerverwandt ist, so ist nach (I.) auch u selbst mit a nicht theilerverwandt. Aus demselben Grunde ist u auch mit keinem andern der Factoren von z theilerverwandt. Also ist kein Factor von z mit u theilerverwandt und folglich nach (I.) auch z selbst nicht; gemäß (II.).

Beweis von III. Nur *einander gleiche* Stammzahlen sind theilerverwandt; denn keine Stammzahl hat einen andern Theiler >1 , als sich selbst. Nun soll in (III.) keiner der Stammfactoren von z irgend einem der Stammfactoren von u *gleich sein*: also ist keiner der Factoren von z irgend einem der Factoren von u theilerverwandt, und folglich sind nach (II.) z und u selbst einander *nicht* theilerverwandt, sondern theilerfremd.

Anm. Der Beweis von (I.) beruht auf der wiederholten Anwendung des Lehrsatzes (§. 20. I.). Der Beweis von (II.) beruht auf der Anwendung von (I.) zunächst auf die einzelnen Factoren von z ; der Beweis von (III.)

beruht darauf, daß hier die Factoren von u und z von selbst in dem in (II.) vorausgesetzten Falle sind.

§. 23.

Lehrsatz.

Der größte Gemeintheiler zweier ganzen Zahlen z und u ist das Product aller derjenigen Stammfactoren, welche z und u gemein haben.

Beispiel. Der größte Gemeintheiler von

$$1. \quad z = 3^5 \cdot 7^4 \cdot 11 \cdot 13^3 \cdot 17^2 \quad \text{und} \quad u = 3^7 \cdot 7^2 \cdot 17^3 \cdot 19^2$$

ist

$$2. \quad 3^5 \cdot 7^2 \cdot 17^2.$$

Nur die Stammfactoren von (2.) kommen in z und u zugleich vor.

Beweis. *A.* Man bezeichne das Product *aller* Stammfactoren, welche z und u gemein haben, durch v , die Producte der übrigen Stammfactoren in z und in u durch z_1 und u_1 , so daß also

$$3. \quad \frac{z}{u} = \frac{v \cdot z_1}{v \cdot u_1}$$

ist. Hier ist $\frac{v \cdot z_1}{v \cdot u_1}$ nichts anderes als der Bruch $\frac{z_1}{u_1}$ im Zähler und Nenner durch die gleiche Zahl v multiplicirt. Also ist nach (§. 13. I. 8.)

$$4. \quad \frac{z}{u} = \frac{z_1}{u_1}.$$

B. Nach der Voraussetzung sind in v alle diejenigen Stammfactoren von u enthalten, die zugleich in z vorkommen. Also sind alle Stammfactoren, die u_1 noch sonst enthält, von allen, die noch in z_1 vorkommen, verschieden. Deshalb sind denn zufolge (§. 22. III.) z_1 und u_1 in (4.) theilerfremd; das heißt, sie haben keinen Factor > 1 weiter gemein. Folglich ist v , nemlich das Product *aller* Stammfactoren, welche z und u gemein haben, der größte Gemeintheiler von z und u ; wie es der Lehrsatz behauptet.

§. 24.

Lehrsatz.

Wenn eine ganze Zahl z mit einer andern ganzen Zahl u aufgeht, so müssen unter den Stammfactoren von z nothwendig alle Stammfactoren von u ohne Ausnahme vorkommen.

Beweis. *A.* Es sei

$$1. \quad z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu,$$

wo $a, b, c, \dots n$ Stammzahlen sind. Käme in u irgend ein Stammfactor

v vor, der keinem der Stammfactoren $a, b, c, \dots n$ gleich wäre, so ginge v in *keinen* dieser Factoren auf, also zuerst in a nicht. Deshalb geht denn v nach (§. 20. II.) auch in $a.a = a^2$ nicht auf; folglich auch nicht in $a.a^2 = a^3$ u. s. w., und folglich nicht in a^a . Auch in b geht v nicht auf, folglich aus gleichen Gründen auch in b^b nicht. Eben so nicht in $c^c, d^d, \dots n^n$, also auch gemäß (§. 20. II.) in $a^a b^b$ nicht, und auch nicht in $a^a b^b . c^c = a^a b^b c^c$ u. s. w., mithin auch in z selbst nicht.

B. Wenn nun aber z mit dem **Factor** v von u nicht aufgeht, so geht auch nach (§. 15. I.) u selbst in z nicht auf. Es ist also, wenn u in z aufgeht, nicht möglich, dafs u irgend einen Factor v habe, der von allen Stammfactoren von z verschieden wäre.

§. 25.

Lehrsatz.

I. Wenn eine ganze Zahl u in das Product $z_1 z_2$ zweier ganzen Zahlen z_1 und z_2 aufgeht, und sie ist zu einer derselben, z. B. zu z_1 , theilerfremd, so mufs sie nothwendig in die andere z_2 aufgehen.

II. Ist dagegen u zu keiner der beiden Zahlen z_1 und z_2 theilerfremd, so kann u in das Product $z_1 z_2$ aufgehen, obgleich weder in z_1 noch in z_2 .

Beispiele. No. 1. zu I. $u = 16$ geht in $z_1 z_2 = 75.144 = 10800$ auf und ist zu $z_1 = 75$ theilerfremd. Deshalb mufs $u = 16$ in $z_2 = 144$ aufgehen.

No. 2. zu II. $u = 120$ ist weder zu $z_1 = 75$ noch zu $z_2 = 144$ theilerfremd und geht in $z_1 z_2 = 75.144 = 10800$ auf, obgleich weder in 75, noch in 144.

Beweis von I. **A.** Da u in das Product $z_1 z_2$ aufgehen soll, so müssen nach (§. 24.) in diesem Product *alle* Stammfactoren von u ohne Ausnahme vorkommen. Nun sollen z_1 und u theilerfremd sein, das heifst, es soll in z_1 *keiner* der Stammfactoren von u vorkommen. Also müssen *alle* Stammfactoren von u ohne Ausnahme in z_2 allein vorhanden sein, und folglich mufs u selbst, welches das Product seiner Stammfactoren ist, nothwendig in z_2 aufgehen.

Beweis von II. **B.** Sind u und z_1 nicht theilerfremd, so hat z_1 mit u Stammfactoren gemein; angenommen *nicht alle*. Enthält nun das Product $z_1 z_2$ die verschiedenen Stammfactoren von u zusammen nur gerade so oft, als sie in u vorkommen, welches schon hinreicht, damit u in $z_1 z_2$ auf-

gehe, so enthält z_2 nicht mehr *alle* Stammfactoren von u , indem z_1 schon einige davon wegnimmt. Also geht in diesem Falle nach (§. 24.) u nicht mehr in z_2 auf, eben so wenig wie in z_1 , obschon gleichwohl in $z_1 z_2$.

§. 26.

Lehrsatz.

Wenn eine ganze Zahl z mit jeder der verschiedenen Zahlen $v_1, v_2, v_3, \dots v_n$ aufgeht, so geht sie auch mit ihrem Product

$$1. \quad u = v_1 v_2 v_3 \dots v_n$$

auf, jedoch nothwendig nur dann, wenn keine der Zahlen v einen Stammfactor mit der andern gemein hat.

Beispiel 1. Die Zahl $z = 75600$ geht mit jeder der drei Zahlen 8, 21 und 25 auf, deren keine einen Stammfactor mit der andern gemein hat. Deshalb geht sie *nothwendig* auch mit ihrem *Product* $8 \cdot 21 \cdot 25 = 4200$ auf.

2. Die Zahl $z = 75600$ geht mit jeder der drei Zahlen 12, 36 und 105 auf, welche Stammfactoren mit einander gemein haben, nicht aber mit ihrem Product $12 \cdot 36 \cdot 105 = 45360$.

Beweis. *A.* Da nach der Voraussetzung z mit $v_1, v_2, v_3, \dots v_n$ aufgehen soll, so müssen nach (§. 24.) unter den Stammfactoren von z *alle* Stammfactoren von $v_1, v_2, v_3, \dots v_n$ ohne Ausnahme, also *alle* Stammfactoren von u sein.

B. Es geht also nothwendig z eben sowohl z. B. mit v_1 auf, als u . Setzt man daher

$$2. \quad z = v_1 z_1,$$

so ist z_1 eine *ganze* Zahl.

C. Sind nun alle Stammfactoren jedes der Factoren v von denen der übrigen *verschieden*, so wird durch die Division von z durch v_1 *keiner* der Stammfactoren von $v_2, v_3, \dots v_n$ weggenommen; mithin enthält z_1 in (2.) noch alle diese letzteren Stammfactoren vollständig.

D. Nun ist zufolge (2.)

$$3. \quad \frac{z}{u} = \frac{v_1 z_1}{v_1 v_2 v_3 \dots v_n} = \frac{z_1}{v_2 v_3 v_4 \dots v_n} \quad (\S. 13. I. 8.)$$

und es kann z_1 , da es noch alle Stammfactoren von $v_2, v_3, \dots v_n$ enthält, durch v_2 dividirt werden, so dafs, wenn man

$$4. \quad z_1 = v_2 z_2$$

setzt, z_2 eine *ganze* Zahl ist. Und zwar enthält wieder z_2 noch alle Stammfactoren von $v_3, v_4, \dots v_n$ vollständig.

E. Vermöge (3. u. 4) ist weiter

$$5. \quad \frac{z}{u} = \frac{v_2 z_2}{v_2 v_3 v_4 \dots v_n} = \frac{z_2}{v_3 v_4 \dots v_n},$$

wo wiederum z_2 mit v_3 aufgeht.

F. Fährt man so fort, so findet sich zuletzt

$$6. \quad \frac{z}{u} = \frac{z_{n-1}}{v_n},$$

wo z_{n-1} noch alle Stammzahlen von v_n enthalten muß und folglich mit v aufgeht.

Also ist $\frac{z}{u}$ nothwendig eine *ganze* Zahl; das heißt, z geht nothwendig mit dem Product $u = v_1 v_2 v_3 \dots v_n$ auf; wie es der Lehrsatz behauptet.

G. Sind dagegen nicht alle Stammfactoren jedes v von dem jedes anderen v verschieden, so kann es sein, daß z. B. schon bei der Division von z durch v_1 in (**B.**) Factoren von z weggenommen werden, die auch noch für ein anderes v , z. B. für v_2 nöthig sind, und folglich sind dann in (4.) *nicht* mehr nothwendig alle Stammfactoren von $v_2, v_3, v_4, \dots v_n$ in z_1 enthalten. Mithin geht dann in diesem Fall z_1 schon nicht mehr nothwendig mit v_2 auf, und folglich auch z nicht mit u .

§. 27.

Lehrsatz.

Zwei ganze Zahlen z und y können einander nicht anders gleich sein, als wenn die eine alle die Stammfactoren der andern ohne Ausnahme enthält, und auch keine mehr; so daß also eine ganze Zahl nur auf eine einzige Art durch die Multiplication aus Stammfactoren zusammengesetzt werden kann.

Beweis. Wenn $z = y$ sein soll, so muß y in z und z in y *aufgehen*. Damit y in z *aufgehe*, muß vermöge (§. 24.) z *alle* Stammfactoren von y enthalten; also keinen *weniger* als y . Und damit z in y *aufgehe*, muß y *alle* Stammfactoren von z enthalten; also y keinen *weniger* als z ; folglich z keinen *mehr* als y . Es muß also z alle Stammfactoren von y enthalten, keinen *weniger* und keinen *mehr* als y , und umgekehrt. Folglich kann eine ganze Zahl nur auf eine einzige Weise ein Product von Stammfactoren sein. Andere Stammfactoren geben Zahlen, die nicht mehr in die vorige *aufgehen* und folglich auch nicht ihr gleich sein können.

§. 28.

Lehrsatz.

I. *Eine ganze Zahl ist immer gerade, das heißt, sie geht mit 2 auf, wenn entweder nur einer oder wenn mehrere ihrer Factoren gerade*

sind. Die Zahl kann nur dann ungerade sein, das heisst, nicht mit 2 aufgehen, wenn kein einziger ihrer Factoren gerade ist. In diesem Falle aber ist z nothwendig ungerade.

II. Alle Stammzahlen, ausser der einzigen Stammzahl 2, sind ungerade Zahlen.

III. Jede gerade Zahl kann durch

$$1. \quad 2mn \pm 0 \pm 2, \pm 4, \pm 6, \dots \pm m, \text{ oder auch}$$

$$2. \quad 2mn \pm 0 \pm 2, \pm 4, \pm 6, \dots \pm (m-1)$$

ausgedrückt werden, wo n jede beliebige Zahl und m in (1.) jede gerade, in (2.) jede ungerade Zahl sein kann. In (1.) wird durch $2mn \pm m$ eine und dieselbe Zahl doppelt ausgedrückt; in (2.) nicht.

IV. Jede ungerade Zahl, also auch jede Stammzahl > 2 , kann durch

$$3. \quad 2mn \pm 1, \pm 3, \pm 5, \dots \pm (m-1), \text{ oder durch}$$

$$4. \quad 2mn \pm 1, \pm 3, \pm 5, \dots \pm m$$

ausgedrückt werden, wo n jede beliebige Zahl und m in (3.) jede gerade, in (4.) jede ungerade Zahl sein kann. In (4.) wird durch $2mn \pm m$ eine und dieselbe Zahl doppelt ausgedrückt; in (3.) nicht.

Beweis von I. **A.** Wenn einer oder mehrere Factoren der Zahl z gerade sind, also mit 2 aufgehen, so müssen diese Factoren unter ihren Stammfactoren nothwendig die Stammzahl 2 haben. Also kommt 2 unter den Stammfactoren von z ein- oder mehreremale vor. Kommt aber der Stammfactor 2 auch nur einmal vor, so geht z mit 2 auf. Also ist die Zahl z immer gerade, sobald nur einer oder auch mehrere ihrer Factoren gerade sind.

B. Ist kein einziger Factor von z gerade, das heisst, geht keiner derselben mit 2 auf, so kommt in keinem, und folglich auch in z selbst nicht, der Stammfactor 2 vor. Mithin geht dann, und nur dann, z mit 2 nicht auf und ist folglich nothwendig ungerade.

Beweis von II. **C.** Eine Stammzahl > 2 kann deshalb keine gerade Zahl sein, weil sie sonst mit 2 aufgehen, folglich einen Theiler > 1 haben müfste, und mithin keine Stammzahl sein würde.

Beweis von III. **D.** Dafs alle die durch (1. u. 2.) ausgedrückten Zahlen gerade sind, ist offenbar; denn sie gehen alle mit 2 auf.

Dafs es keine andern geraden Zahlen weiter gebe, als die, welche durch (1. u. 2.) ausgedrückt werden, läfst sich am kürzesten an bestimmten Werthen von m zeigen.

a. Es sei zuerst für *gerade* m , z. B. $m = 6$, also $2m = 12$, so werden *alle* gerade Zahlen 0, 2, 4, 6, 8 etc. der Reihe nach wie folgt ausgedrückt:

$$5. \left\{ \begin{array}{l} 0.12, 0.12+2, 0.12+4, 0.12+6, \\ 1.12-6, 1.12-4, 1.12-2, 1.12, 1.12+2, 1.12+4, 1.12+6, \\ 2.12-6, 2.12-4, 2.12-2, 2.12, 2.12+2, 2.12+4, 2.12+6, \\ 3.12-6, 3.12-4, 3.12-2, 3.12, 3.12+2, 3.12+4, 3.12+6, \\ \dots \end{array} \right.$$

Für die erste horizontale Reihe ist $n=0$, und die Zahlen, welche in dieser Reihe stehen, werden durch $2m \cdot 0 + 0, 2, 4, 6 (=m)$ ausgedrückt. Für die zweite horizontale Reihe ist $n=1$, und die Zahlen, welche in dieser Reihe stehen, werden durch $2m \cdot 1 \pm 0, \pm 2, \pm 4, \pm 6 (=m)$ ausgedrückt. Für die dritte horizontale Reihe ist $n=2$; die Zahlen, welche in dieser Zeile stehen, werden durch $2m \cdot 2 \pm 0, \pm 2, \pm 4, \pm 6 (=m)$ ausgedrückt; u. s. w. Allgemein also drückt, für *irgend ein* n , $2mn \pm 0, \pm 2, \pm 4, \dots \pm m$ *jede mögliche gerade* Zahl aus. Dabei ist die *letzte* Zahl jeder Reihe *dieselbe*, wie die erste der nächstfolgenden Reihe: also drückt $2mn \pm m$ eine und dieselbe Zahl *doppelt* aus.

b. Es sei für *ungerade* m , z. B. $m = 5$, also $2m = 10$, so werden *alle* geraden Zahlen 0, 2, 4, 6, 8, etc. der Reihe nach wie folgt ausgedrückt:

$$6. \left\{ \begin{array}{l} 0.10, 0.10+2, 0.10+4, \\ 1.10-4, 1.10-2, 1.10, 1.10+2, 1.10+4, \\ 2.10-4, 2.10-2, 2.10, 2.10+2, 2.10+4, \\ 3.10-4, 3.10-2, 3.10, 3.10+2, 3.10+4, \\ \dots \end{array} \right.$$

Hier ist der Ausdruck der Zahlen in der ersten Zeile $0.10 + 0, 2, 4 (=m-1)$, derer in der zweiten Reihe $1.10 \pm 0, \pm 2, \pm 4 (=m-1)$, derer in der dritten Reihe $2.10 \pm 0, \pm 2, \pm 4 (=m-1)$; und so weiter. Allgemein also drückt $2mn \pm 0, \pm 2, \pm 4, \dots \pm (m-1)$, mit irgend einem Werth von n , jede mögliche *gerade* Zahl aus. Dabei aber kommt, in dem gegenwärtigen Fall eines *ungeraden* m , anders wie in (5.) für ein *gerades* m , *keine* Zahl *zweimal* vor, und *keine* wird also doppelt ausgedrückt.

Dieses ist zusammen, was (III.) behauptet.

E. Auf eine ähnliche Weise läßt sich zeigen, dafs die durch (3. u. 4.) ausgedrückten Zahlen, welche offenbar alle *ungerade* sind, weil keine mit 2 aufgeht, *alle ungleichen ungeraden* Zahlen sind.

a. Es sei zuerst für *gerade* m , z. B. wieder $m=6$, also $2m=12$, so werden *alle* ungeraden Zahlen 1, 3, 5, 7, 9, der Reihe nach wie folgt ausgedrückt:

$$7. \quad \left\{ \begin{array}{l} 0.12+1, 0.12+3, 0.12+5, \\ 1.12-5, 1.12-3, 1.12-1, 1.12+1, 1.12+3, 1.12+5, \\ 2.12-5, 2.12-3, 2.12-1, 2.12+1, 2.12+3, 2.12+5, \\ 3.12-5, 3.12-3, 3.12-1, 3.12+1, 3.12+3, 3.12+5, \\ \dots \end{array} \right.$$

Die Zahlen in der ersten horizontalen Reihe werden durch $0m+0, 1, 3, 5 (=m-1)$ ausgedrückt; also ist für sie $n=0$. Die Zahlen der zweiten Reihe werden durch $2m.1 \pm 1, \pm 3, \pm 5 (=m-1)$ ausgedrückt; also ist für sie $n=1$. Die der dritten Reihe werden durch $2m.2 \pm 1, \pm 3, \pm 5 (=m-1)$ ausgedrückt; also ist für sie $n=2$; und so weiter. Für *irgend einen* Werth von n drückt also $2mn \pm 1, \pm 3, \pm 5, \dots \pm (m-1)$ *jede mögliche* ungerade Zahl aus, und zwar keine zweimal; denn in (7.) ist keine der Zahlen dieselbe.

b. Für *ungerade* m sei wieder $m=5$, also $2m=10$, so werden *alle* ungerade Zahlen 1, 3, 5, 7, 9 wie folgt ausgedrückt:

$$8. \quad \left\{ \begin{array}{l} 0.10+1, 0.10+3, 0.10+5, \\ 1.10-5, 1.10-3, 1.10-1, 1.10+1, 1.10+3, 1.10+5, \\ 2.10-5, 2.10-3, 2.10-1, 2.10+1, 2.10+3, 2.10+5, \\ 3.10-5, 3.10-3, 3.10-1, 3.10+1, 3.10+3, 3.10+5, \\ \dots \end{array} \right.$$

Die Zahlen der ersten horizontalen Reihe werden durch $2m.0+1, 3, 5 (=m)$ ausgedrückt, und es ist für sie $n=0$. Die Zahlen der zweiten Zeile werden durch $2m.1 \pm 1, \pm 3, \pm 5 (=m)$ ausgedrückt, und es ist für sie $n=1$. Die Zahlen der dritten Reihe werden durch $2m.2 \pm 1, \pm 3, \pm 5 (=m)$ ausgedrückt, und es ist für sie $n=2$; u. s. w. Also drückt allgemein $2mn \pm 1, \pm 3, \pm 5, \dots \pm m$ für *irgend ein* n *jede mögliche* ungerade Zahl aus; und zwar je die letzte in den verschiedenen Reihen *zweimal*, denn je die erste in den nächstfolgenden Reihe sind dieselben.

Dieses ist zusammen was (IV.) behauptet.

Anm. *F.* Für die *ungeraden Stammzahlen* setzt man am gewöhnlichsten $m=2$ und drückt sie also nach (3.) durch

$$9. \quad 4n \pm 1$$

aus; denn mehrere Eigenschaften der durch $4n+1$ bezeichneten Stammzahlen sind, wie sich weiter unten ergeben wird, von denen der Stammzahlen $4n-1$ wesentlich verschieden.

§. 29.

Lehrsatz.

Es werde die beliebige ganze Zahl z durch ihre Stammfactoren $a, b, c, d, \dots n$ ausgedrückt, nemlich nach (§. 21.) durch

$$1. \quad z = a^\alpha b^\beta c^\gamma d^\delta \dots n^\nu,$$

wo $\alpha, \beta, \gamma, \delta, \dots \nu$ ganze positive Zahlen sind. Alsdann geht

I. Jedes Glied der Reihe, welche das Product

$$2. \quad P = (1+a+a^2+\dots+a^\alpha)(1+b+b^2+\dots+b^\beta)(1+c+c^2+\dots+c^\gamma)\dots \\ \dots (1+n+n^2+\dots+n^\nu)$$

entwickelt giebt, in z auf. Auch hat z keine andern Theiler aufer diesen Gliedern.

II. Die Anzahl der Theiler von z ist, die Einheit und z mit eingeschlossen,

$$3. \quad \tau = (\alpha+1)(\beta+1)(\gamma+1)\dots(\nu+1).$$

III. Ist τ (3.) eine gerade Zahl, so sind $\frac{1}{2}\tau$ Theiler von z kleiner und $\frac{1}{2}\tau$ Theiler größer als die Quadratwurzel aus z . Ist τ ungerade, so sind $\frac{1}{2}(\tau-1)$ Theiler von z kleiner und $\frac{1}{2}(\tau-1)$ Theiler größer als die Quadratwurzel von z . Die Zahl z ist in diesem Falle eine Quadratzahl; alle die Zeiger $\alpha, \beta, \gamma, \dots \nu$ sind dann nothwendig gerade, und der eine noch übrige Theiler von z , der durch

$$4. \quad \sqrt{z} = a^{\frac{1}{2}\alpha} b^{\frac{1}{2}\beta} c^{\frac{1}{2}\gamma} \dots n^{\frac{1}{2}\nu}$$

ausgedrückt wird, ist die Quadratwurzel von z .

IV. Die Summe aller Theiler von z ist

$$5. \quad s = \frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \dots \frac{n^{\nu+1}-1}{n-1}.$$

Beispiel 1. Es sei

$$6. \quad z = 2^2 \cdot 3^2 \cdot 5 = 360,$$

also

$$7. \quad a = 2, \quad b = 3, \quad c = 5, \quad \alpha = 2, \quad \beta = 2, \quad \gamma = 1.$$

Alsdann ist nach (1.)

$$8. \quad P = (1+2+4+8)(1+3+9)(1+5),$$

und dieses giebt, entwickelt:

$$9. \quad P = 1+2+4+8+3+6+12+24+9+18+36+72+5+10+20 \\ +40+15+30+60+120+45+90+180+360.$$

Jedes Glied dieses entwickelten Products geht in $z = 360$ auf und es giebt

keinen andern Theiler von z aufser diesen Gliedern. Die Anzahl τ der Theiler ist 24, und (3.) giebt, wie gehörig,

$$10. \quad \tau = (3+1)(2+1)(1+1) = 4.3.2 = 24.$$

τ ist hier also *gerade*. Die $\frac{1}{2}\tau = 12$ Theiler 1, 2, 4, 8, 3, 6, 12, 9, 18, 5, 10, 15 sind *kleiner* als die Quadratwurzel von z , welche zwischen 18 und 19 liegt; die übrigen $\frac{1}{2}\tau = 12$ Theiler sind *größer* als $\sqrt{z}$. Die *Summe* s der Theiler beträgt 1170, und wie gehörig giebt (5.)

$$11. \quad s = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{5^2-1}{5-1} = \frac{15}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} = 15.13.6 = 1170.$$

2. Es sei

$$12. \quad z = 2^4.3^2 = 144,$$

so dafs

$$13. \quad a = 2, \quad b = 3, \quad \alpha = 4, \quad \beta = 2$$

ist, so ist in (1.)

$$14. \quad P = (1+2+4+8+16)(1+3+9),$$

und dieses giebt, entwickelt:

15. $P = 1+2+4+8+16+3+6+12+24+48+9+18+36+72+144$. *Alle* Glieder dieses entwickelten Products sind aufgehende Theiler von $z=144$, und es giebt keine andern. Die Anzahl τ dieser Theiler ist 15, und (3.) giebt, wie gehörig,

$$16. \quad \tau = (4+1)(2+1) = 5.3 = 15.$$

τ ist *hier ungerade*. Die $\frac{1}{2}(\tau-1)=7$ Theiler, 1, 2, 4, 8, 3, 6, 9 sind kleiner als die Quadratwurzel von z , welche 12 ist; die $\frac{1}{2}(\tau-1)=7$ Theiler 16, 24, 48, 18, 36, 72 und 144 sind *größer* als die Quadratwurzel aus z . Der letzte, 15te Theiler ist 12, nemlich

$$17. \quad \sqrt{z} = 2^{\frac{4}{2}}.3^{\frac{2}{2}} = 2^2.3 = 4.3 = 12.$$

z ist hier eine *Quadratzahl*. Die *Summe* der Theiler ist 403, und wie gehörig giebt (5.)

$$18. \quad s = \frac{2^5-1}{2-1} \cdot \frac{3^3-1}{3-1} = \frac{31}{1} \cdot \frac{26}{2} = 31.13 = 403.$$

Beweis von I. *A.* z kann nicht mit *andern* Stammzahlen als $a, b, c, d, \dots n$ aufgehen (§. 14. II. u. §. 24.). Es geht aber nach (§. 14. I.) mit $a, b, c, \dots n$ und mit allen *Potenzen* von $a, b, c, \dots n$ auf, deren *Zeiger* nicht höher sind als $\alpha, \beta, \gamma, \dots \nu$, und mit keinen andern; so wie mit allen *Producten* dieser Potenzen; denn alle diese sind *Factoren* von z . Es kommt daher nur darauf an, die verschiedenen möglichen Producte jener Potenzen zu finden.

B. Wäre zuerst bloß

$$19. \quad z = a^\alpha b^\beta,$$

so wären die sämtlichen möglichen Theiler von z die Potenzen $a^0 = 1, a^1, a^2, a^3, \dots, a^\alpha$ von a , und $b^0 = 1, b^1, b^2, b^3, \dots, b^\beta$ von b , nebst allen möglichen Producten derselben. Man findet dieselben *alle*, nemlich die *Producte* und die *Potenzen selbst*, wenn man $1 + a + a^2 + \dots + a^\alpha$ mit $1 + b + b^2 + \dots + b^\beta$ multiplicirt. Denn zuerst 1mal $1 + a + a^2 + \dots + a^\alpha$ giebt alle Potenzen von a , welche vorkommen können. Darauf b mal $1 + a + a^2 + \dots + a^\alpha$ giebt alle möglichen Producte jener Potenzen mit b , so wie b selbst. b^2 mal $1 + a + a^2 + \dots + a^\alpha$ giebt alle möglichen Producte der vorkommenden Potenzen von a mit b^2 , so wie b^2 selbst. Und so weiter. Die Multiplication von $1 + a + a^2 + \dots + a^\alpha$ mit $1 + b + b^2 + \dots + b^\beta$ giebt also alle möglichen Producte der hier vorkommenden Potenzen von a , mit allen vorkommenden Potenzen von b , und zugleich die Potenzen von a und b selbst; also *Alles*, was gesucht wird. Mithin sind die verschiedenen Glieder des Productes $(1 + a + a^2 + \dots + a^\alpha)(1 + b + b^2 + \dots + b^\beta)$ sämtlich Theiler von $z = a^\alpha b^\beta$ (19.) und es giebt keine anderen.

C. Es sei ferner

$$20. \quad z = a^\alpha b^\beta c^\gamma,$$

so gehen offenbar in z zunächst alle Theiler von $a^\alpha b^\beta$ auf, und keine anderen mit nur a oder b zu Stammfactoren. Sie gehen aber alle auch dann noch in z (20.) auf, wenn man sie noch mit c , mit c^2 , mit c^3 u. s. w. bis c^γ multiplicirt; jedoch nicht mehr, wenn sie mit einer höheren Potenz von c als c^γ multiplicirt werden. Also findet man die sämtlichen Theiler von z (20.), wenn man diejenigen von z (19.) mit $1, c, c^2, \dots, c^\gamma$ multiplicirt. Die sämtlichen Theiler von z (19.) waren die Glieder des Productes $(1 + a + a^2 + \dots + a^\alpha)(1 + b + b^2 + \dots + b^\beta)$ (**B.**), also sind die Glieder des Productes $(1 + a + a^2 + \dots + a^\alpha)(1 + b + b^2 + \dots + b^\beta)(1 + c + c^2 + \dots + c^\gamma)$ sämtliche Theiler von z (20.), und es giebt keine andern; denn es können keine höheren Potenzen von c vorkommen als c^γ ; die Theiler $1, c, c^2, \dots, c^\gamma$ selbst aber, mit welchen z ebenfalls aufgeht, finden sich in dem Product durch das Glied 1 , welches in $(1 + a + a^2 + \dots + a^\alpha)(1 + b + b^2 + \dots + b^\beta)$ vorkommt, ebenfalls.

D. Ganz auf ähnliche Weise folgt, dafs man, im Fall

$$21. \quad z = a^\alpha b^\beta c^\gamma d^\delta$$

ist, alle möglichen Theiler von z findet, wenn man der Reihe nach alle Theiler von z (20.) mit $1, d, d^2, \dots, d^\delta$ multiplicirt, folglich, da jene Theiler nach (**C.**) die Glieder des Productes $(1 + a + a^2 + \dots + a^\alpha)(1 + b + b^2 + \dots + b^\beta)$

$(1 + c + c^2 + \dots + c^\gamma)$ sind, wenn man dieses Product noch mit $1 + d + d^2 + \dots + d^\delta$ multiplicirt; und so weiter; so dafs also zuletzt die Glieder des Products **P** (2.) alle möglichen Theiler von z (1.) sind; wie es (I.) behauptet.

Beweis von II. **E.** Die *Anzahl* der Glieder des ersten Factors $1 + a + a^2 + \dots + a^\alpha$ von **P** (2.) ist $\alpha + 1$. Multiplicirt man diese Glieder mit den $\beta + 1$ Gliedern des zweiten Factors $1 + b + b^2 + \dots + b^\beta$, so liefert *jedes* Glied dieses zweiten Factors $\alpha + 1$ Producte, also giebt die Multiplication der beiden Factoren überhaupt $(\alpha + 1)(\beta + 1)$ Glieder; und zwar sind alle diese Glieder unter sich *verschieden*. Denn die ersten unter sich verschiedenen $\alpha + 1$ Glieder, welche aus der Multiplication von $1 + a + a^2 + \dots + a^\alpha$ mit 1 entstehen, enthalten *kein* b ; die zweiten $\alpha + 1$ Glieder, welche aus der Multiplication von $1 + a + a^2 + \dots + a^\alpha$ mit b entstehen, enthalten *sämmtlich* b , aber keine *höhere* Potenz von b ; die dritten $\alpha + 1$ Glieder, welche aus der Multiplication von $1 + a + a^2 + \dots + a^\alpha$ mit b^2 entstehen, enthalten *sämmtlich* b^2 , und keine *höhere* Potenz von b u. s. w. Also sind die $(\alpha + 1)(\beta + 1)$ Glieder sämmtlich von einander *verschieden*.

F. Multiplicirt man weiter die sämmtlichen $(\alpha + 1)(\beta + 1)$ Glieder, welche das Product $(1 + a + a^2 + \dots + a^\alpha)(1 + b + b^2 + \dots + b^\beta)$ enthält, und welche sämmtlich Theiler von z sind, mit den $\gamma + 1$ Gliedern von $1 + c + c^2 + \dots + c^\gamma$, so entstehen, da jedes dieser Glieder $(\alpha + 1)(\beta + 1)$ Glieder liefert, zusammen $(\alpha + 1)(\beta + 1)(\gamma + 1)$ Glieder, die alle wieder von einander *verschieden* sind, weil die ersten unter sich verschiedenen $(\alpha + 1)(\beta + 1)$ Glieder gar kein c , die zweiten $(\alpha + 1)(\beta + 1)$ von c herkommenden Glieder sämmtlich c als Factor, die dritten $(\alpha + 1)(\beta + 1)$ von c^2 herkommenden Glieder sämmtlich c^2 als Factor enthalten, u. s. w.

So folgt dann, wenn man weiter mit der Multiplication der Factoren von **P** (2.) fortfährt, dafs die *Anzahl* der Glieder dieses Products gemäß (3.) $\tau = (\alpha + 1)(\beta + 1)(\gamma + 1) \dots (\nu + 1)$ ist; und alle diese Glieder sind von einander verschieden. Das ist was (II.) behauptet

Beweis von III. **G.** Da z (1.) mit allen Gliedern des Products **P** (2.) aufgeht, so ist, wenn z_1 *irgend eines* dieser Glieder und z_2 den *Quotienten* von z dividirt durch z_1 bezeichnet,

$$22. \quad z = z_1 z_2,$$

wo z_2 eine *ganze* Zahl ist. Hieraus folgt, dafs auch der Quotient z_2 in z aufgehen und folglich nothwendig *ebenfalls eins* von den Gliedern des Products **P** sein mufs. Zu *jedem* Gliede des Products **P** gehört also nothwendig ein

zweites, welches, mit ihm multiplicirt, z giebt. Aber die Glieder des Products P sind *alle* unter sich verschieden ($F.$): also können in (22.) z_1 und z_2 einander *nicht gleich* sein, es wäre denn, dafs z_1 mit *sich selbst* multiplicirt z gäbe und also z eine *Quadratzahl* wäre.

Ist dies nicht der Fall, so ist nothwendig z_1 entweder *kleiner* oder *größer* als $\sqrt{z}$. Zu jedem $z_1 < \sqrt{z}$ gehört aber, wegen $z_1 z_2 = z$ (22.), ein $z_2 > \sqrt{z}$. Also giebt es in solchem Falle *gerade eben so viele* Glieder $< \sqrt{z}$ als Glieder $> \sqrt{z}$, und folglich von jeder Art $\frac{1}{2}\tau$.

Ist dagegen *ein* Glied vorhanden, welches, mit sich selbst multiplicirt, z giebt, so bleiben noch $\tau - 1$ Glieder *übrig*, und diese sind dann alle, entweder $< \sqrt{z}$ oder $> \sqrt{z}$. Von *diesen* $\tau - 1$ Gliedern gilt wieder dasselbe wie vorhin; und folglich sind ihrer $\frac{1}{2}(\tau - 1)$ *kleiner* und $\frac{1}{2}(\tau - 1)$ *größer* als $\sqrt{z}$. Das übrig bleibende *eine* Glied ist $= \sqrt{z}$.

H. Aber die Zahl τ der Glieder selbst *entscheidet*, ob ein z_1 statt finden könne, welches, *mit sich selbst* multiplicirt, z giebt. Ist nemlich τ *gerade*, so ist $\frac{1}{2}\tau$ eine *ganze* Zahl und folglich bleibt, da nach ($G.$) $\frac{1}{2}\tau$ Glieder kleiner und $\frac{1}{2}\tau$ Glieder größer als $\sqrt{z}$ sein müssen, *kein* Glied *übrig*, welches *gleich* $\sqrt{z}$ sein könnte. Die Zahl τ (3.) ist aber nach (§. 28. I.) *immer gerade*, wenn auch nur ein einziger ihrer Factoren $\alpha + 1, \beta + 1, \gamma + 1, \dots \nu + 1$ *gerade*, also nur ein einziger der Exponenten $\alpha, \beta, \gamma, \dots \nu$ *ungerade* ist. In solchem Falle also giebt es keine Quadratwurzel aus z , die eine ganze Zahl wäre.

Ist dagegen τ *ungerade*, so ist $\frac{1}{2}(\tau - 1)$ eine *ganze* Zahl, und da alsdann $\frac{1}{2}(\tau - 1)$ Glieder *kleiner* und $\frac{1}{2}(\tau - 1)$ Glieder *größer* als $\sqrt{z}$ sind ($G.$), so bleibt *ein Glied* übrig, welches, mit sich selbst multiplicirt, z giebt. Es ist aber τ nach (§. 28. I.) nur dann *ungerade*, wenn *keiner* der Factoren $\alpha + 1, \beta + 1, \gamma + 1, \dots \nu + 1$ *gerade*, also wenn *keiner* der Exponenten $\alpha, \beta, \gamma, \dots \nu$ *ungerade* ist. Also *nur* in diesem Fall giebt es eine ganzzahlige Quadratwurzel von z . Dieses zusammen ist was (III.) behauptet.

Beweis von IV. **I.** Die Summe der sämtlichen Glieder des entwickelten Products P (2.) ist der *Werth* des Products selbst. Nun ist

$$23. \quad 1 + a + a^2 + a^3 \dots + a^\alpha = \frac{a^{\alpha+1} - 1}{a - 1};$$

denn multiplicirt man hier rechts und links mit $a - 1$, so ergibt sich

$$24. \quad \begin{cases} a + a^2 + a^3 + a^4 \dots + a^\alpha + a^{\alpha+1} = a^{\alpha+1} - 1, \\ -1 - a - a^2 - a^3 - a^4 \dots - a^\alpha \end{cases}$$

wie gehörig. Eben so ist $1 + b + b^2 + \dots + b^\beta = \frac{b^{\beta+1} - 1}{b - 1}$, $1 + c + c^2 + \dots + c^\gamma = \frac{c^{\gamma+1} - 1}{c - 1}$, u. s. w. Also läßt sich P , dessen *Werth* in (5.) durch s bezeichnet wurde, wie folgt ausdrücken:

$$25. \quad s = \frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \cdot \frac{c^{\gamma+1} - 1}{c - 1} \cdot \dots \cdot \frac{n^{\nu+1} - 1}{n - 1};$$

wie (IV.) es behauptet.

Anm. Die Hauptmomente in dem Beweise sind, daß der Ausdruck (1) von z mit keinen *höheren* Potenzen von $a, b, c, \dots, n$ aufgeht, als mit denen, deren Exponenten $\alpha, \beta, \gamma, \dots, \nu$ sind; sodann, daß alle diese Potenzen in den Gliedern des Products P (2.) vorkommen; und endlich, daß alle Glieder des Products P von einander *verschieden* sind.

§. 30.

Lehrsatz.

Jede Menge von Einheiten, also jede ganze Zahl z , kann, wenn a eine beliebige andere, kleinere Menge von Einheiten bezeichnet, durch

$$1. \quad z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + x_{m-3} a^{m-3} + \dots + x_1 a + x_0$$

ausgedrückt werden, wo die x sämmtlich ganze Zahlen und sämmtlich kleiner als a sind. m ist ebenfalls eine ganze Zahl, deren Gröfse sich nach z und a richtet. Die x können für ein- und dasselbe z und a jedes nur einen Werth haben. Bestimmt man für die verschiedenen Werthe, welche die x haben können, und deren $a - 1$ sind, ausschließliche, willkürliche Zeichen, und dann noch für Null ebenfalls ein Zeichen, so kann z durch diese Zeichen, blofs der Reihe nach hinter einander geschrieben, ausgedrückt werden, ohne a selbst zu schreiben. Dieses Mittel Mengen von Einheiten auszudrücken, giebt die Zahlensysteme. Die Zeichen für die verschiedenen möglichen Werthe von x sind die Ziffern, und die verschiedenen Potenzen von a werden als eben so viele verschiedene Einheiten betrachtet, deren Werthe die Stellen der Ziffern schon ausdrücken. In dem üblichen dekadischen Zahlensystem enthält a zehn Einheiten, und die $a - 1$ Ziffern 1, 2, 3, 4, 5, 6, 7, 8 und 9, nebst dem Zeichen 0 für Null, reichen hin, jede Menge z von Einheiten, also jede ganze Zahl auszudrücken.

Beweis. A. Welche Menge von Einheiten auch z enthalten mag: es wird immer durch wiederholte Multiplication von a mit sich selbst, sobald

a mehr als *eine* Einheit enthält, zu einer Zahl a^m zu gelangen sein, die, wenn man sie *noch einmal* mit a multiplicirt, eine Zahl giebt, welche *größer* ist als z . Denn durch wiederholte Multiplication mit a kann man die Menge der Einheiten in dem Product bis *in's Unendliche* vergrößern.

B. Ist nun a^m diejenige Potenz von a , welche noch *kleiner* als z ist, aber, noch einmal mit a multiplicirt, eine Zahl giebt, die *größer* ist als z , so wird sich z durch

$$2. \quad z = x_m a^m + r_1$$

ausdrücken lassen, wo $x_m < a$ und $r_1 < a^m$ ist. Denn wäre x_m gleich a oder $> a$, so wäre $x_m a^m + r_1$ gleich $a^{m+1} + r_1$, also *größer* als z , gegen die Voraussetzung; r_1 aber kann immer $< a^m$ gemacht werden, da man nur a^m so oft von z abziehen darf, als es möglich ist.

C. Da also $r_1 < a^m$ ist, aber möglicherweise $> a^{m-1}$ sein kann, so wird sich aus gleichen Gründen r_1 wieder wie folgt ausdrücken lassen:

$$3. \quad r_1 = x_{m-1} a^{m-1} + r_2,$$

wo wieder x_{m-1} nothwendig $< a$ und $r_2 < a^{m-1}$ ist. Eben so wird weiter

$$4. \quad \begin{cases} r_2 = x_{m-2} a^{m-2} + r_3, \\ r_3 = x_{m-3} a^{m-3} + r_4, \\ \dots \end{cases}$$

gesetzt werden können, bis man zuletzt auf ein r kommt, welches kleiner als a selbst ist und folglich in die Reihe der x gehört, die *alle* $< a$ sind.

D. Substituirt man die Ausdrücke (2., 3. u. 4.) in einander, so er giebt sich der Reihe nach

$$5. \quad \begin{cases} z = x_m a^m + r_1, \\ z = x_m a^m + x_{m-1} a^{m-1} + r_2, \\ z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + r_3, \\ \dots \\ z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} + x_{m-3} a^{m-3} + \dots + x_1 a + x_0. \end{cases}$$

Der letzte dieser Ausdrücke von z ist der (1.) des Lehrsatzes.

E. Bestimmt man nun für die $a-1$ verschiedenen Werthe, welche x haben kann, eben so viele ausschließliche, verschiedene Zeichen oder *Ziffern*, z. B. für das dekadische System die Ziffern 1, 2, 3, 4, 5, 6, 7, 8, und 9 und für Null das Zeichen 0, so kann zunächst a selbst bloß durch 10 bezeichnet werden; denn für $z = a$ sind in (1.) *alle* x , mit Ausnahme von x_1 , gleich Null; x_m aber ist $= 1$. Also ist z oder $x_1 a + x_0$ hier $1 \cdot x + 0 \cdot 1$, und wenn man nun x selbst als eine neue Einheit betrachtet, welche zehn

der einfachen Einheiten enthält, so kann man blofs schreiben $1.1 \vdash 0.1$, oder zusammengezogen 10, wo schon die *Stelle* der 1 ausdrückt, dafs die *nächst höhere* Einheit gemeint sei.

Eben so sind für $z = a^2$ alle x , mit Ausnahme von x_2 , gleich Null, und x_2 ist $= 1$. Also ist $z = x_{m-1}a^2 \vdash 0.1 \vdash 0 = 1.1 \vdash 0.1 \vdash 0$, wofür zusammengezogen blofs 100 geschrieben werden kann, da die Stelle der 1 schon anzeigt, welche Potenz von a gemeint sei. Und so weiter.

Sind nun die verschiedenen x *nicht* Null, so multipliciren sie der Reihe nach die verschiedenen Einheiten oder Potenzen von a , deren Exponenten schon von den Stellen der Ziffern angezeigt werden; denn keine Ziffer, da sie nur ein einziges Zeichen ist, nimmt mehr als eine Stelle ein.

Also läfst sich jede Menge z von Einheiten blofs durch die hinter einander geschriebenen Ziffern oder Mengen der verschiedenen Potenzen von a ausdrücken.

F. Um zu zeigen, dafs für ein- und dasselbe z und a , die x jedes *nur einen* Werth haben können, setze man, es könne ein- und dasselbe z , aufser wie in (1.), auch durch

6. $z = y_m a^m \vdash y_{m-1} a^{m-1} \vdash y_{m-2} a^{m-2} \dots \vdash y_1 a \vdash y_0$
ausgedrückt werden, wo die y von den x in (1.) *verschieden* sind.

Man ziehe (6.) von (1.) ab, so ergibt sich

$$7. \quad 0 = (x_m - y_m) a^m \vdash (x_{m-1} - y_{m-1}) a^{m-1} \vdash (x_{m-2} - y_{m-2}) a^{m-2} \dots \\ \dots \vdash (x_1 - y_1) a \vdash x_0 - y_0.$$

In diesem Ausdruck geht rechterhand Alles bis auf $x_0 - y_0$ mit a auf, also mufs nach (§. 18.) auch $x_0 - y_0$ mit a aufgehen. Dies aber ist nicht anders möglich, als wenn $x_0 - y_0$ gleich Null ist, da x_0 und y_0 beide nach der Voraussetzung $< a$ sind und also auch $x_0 - y_0 < a$ ist. Also mufs nothwendig y_0 *gleich* x_0 sein.

Läfst man $x_0 - y_0$, als Null, aus (7.) weg und dividirt was übrig bleibt durch a , so ergibt sich

$$8. \quad 0 = (x_m - y_m) a^{m-1} \vdash (x_{m-1} - y_{m-1}) a^{m-2} \vdash (x_{m-2} - y_{m-2}) a^{m-3} \dots \\ \dots \vdash (x_2 - y_2) a \vdash x_1 - y_1,$$

und hieraus folgt, ganz aus demselben Grunde wie vorhin, dafs auch y_1 *gleich* x_1 sein mufs.

Läfst man wieder $x_1 - y_1$, als Null, aus (8.) weg und dividirt was übrig bleibt durch a , so folgt ferner, dafs auch y_2 *gleich* x_2 sein mufs. Und so weiter für alle x und y bis zu $y_m = x_m$ selbst. Also können für ein- und dasselbe z und a die x in (1.) jedes *nur einen* Werth haben.

§. 31.

Lehrsatz.

I. *Jede ganze Zahl ist die Summe dieser oder jener Potenzen der Zahl 2; und zwar nur auf eine Art.*

II. *Jede ganze Zahl ist die Summe dieser oder jener Potenzen der Zahl 3, weniger der Summe dieser oder jener Potenzen derselben Zahl 3; und zwar wieder nur auf eine Art.*

Beispiel zu I. Es ist $83 = 64 + 16 + 2 + 1 = 2^6 + 2^4 + 2^1 + 2^0$;
 $74 = 64 + 8 + 2 = 2^6 + 2^3 + 2^1$; $181 = 128 + 32 + 16 + 4 + 1 = 2^7 + 2^5 + 2^4 + 2^2 + 2^0$
 u. s. w.

Zu II. Es ist $83 = 81 + 3 - 1 = 3^4 + 3^1 - 3^0$; $74 = 81 - 9 + 3 - 1 = 3^4 - 3^2 + 3^1 - 3^0$; $181 = 243 - 81 + 27 - 9 + 1 = 3^5 - 3^4 + 3^3 - 3^2 + 3^0$.

Beweis von I. **A.** Nach (§. 30.) kann jede ganze Zahl durch

1. $z = x_m a^m + x_{m-1} a^{m-1} + x_{m-2} a^{m-2} \dots + x_1 a + x_0$
 ausgedrückt werden, wo *a willkürlich* ist und *alle* $x < a$ sind.

Setzt man also das *willkürliche* $a = 2$, so können die x nur 1 oder 0 sein. Also wird jede Zahl z durch

2. $z = x_m 2^m + x_{m-1} 2^{m-1} + x_{m-2} 2^{m-2} \dots + x_1 2 + x_0$
 ausgedrückt, wo die x *nie größer* als 1, jedoch diese oder jene x auch Null sein können. Also wird jedes z blofs durch *einmal* genommene Potenzen von $a = 2$ ausgedrückt, unter welchen diese oder jene *fehlen* können. Jedes z ist also die Summe dieser oder jener Potenzen (nemlich derer, die *nicht* fehlen) von der Zahl $a = 2$.

B. Ferner können für ein- und dasselbe z und a die x (2.) nach (§. 30.) jedes *nur einen* Werth haben: also kann auch hier z *nur auf eine Art* aus diesen oder jenen Potenzen von 2 zusammengesetzt werden.

Beweis von II. **C.** Setzt man in (1.) $a = 3$, so können die x , weil sie $< a$ sein sollen, nur 0, 1 oder 2 sein. Diejenigen, welche 0 oder 1 sind, geben die Potenzen von $a = 3$ entweder gar nicht, oder blofs einmal. Für diejenigen, welche 2 sein müssen, setze man $2 = 3 - 1 = a - 1$. Dadurch geht das Glied, welches 2 zum Coëfficienten hat, mit einem seiner Theile in die nächst höhere Potenz von a , also zu dem nächstvorhandenen Gliede über, der andere Theil aber kommt dann nur einfach, und zwar negativ vor. Z. B. wenn zwei aufeinander folgende Glieder in (1.) $x_k 3^k + 2 \cdot 3^{k-1}$ wären, so verwandeln sie sich, wenn man $3 - 1$ statt 2 schreibt, in

$x_k \cdot 3^k + 3 \cdot 3^{k-1} - 3^{k-1} = x_k \cdot 3^k + 3^k - 3^{k-1} = (x_k + 1)3^k - 3^{k-1}$. Ist hier x_k nicht 0, sondern 1, so bekommt 3^k zum Coëfficienten 2 und man kann wie vorhin verfahren. Ist x_k schon 2, so kann man zuvor schon statt dessen $3 - 1$ statt 2 setzen, u. s. w., falls es nöthig ist, bis zum *ersten* Gliede $x_m a^m$ hinauf, welches, wenn $x_m = 2$ wäre, $3 \cdot a^m - a^m = a^{m+1} - a^m$ geben würde. Also lassen sich überall die Coëfficienten 2, wo sie vorkommen, wegschaffen, und es lassen sich die x blofs auf $+1$, -1 und 0 reduciren, also so, dafs z blofs durch eine Summe dieser oder jener Potenzen der Zahl 3, *weniger* der Summe dieser oder jener andern Potenzen derselben Zahl 3 ausgedrückt wird.

D. Dafs solches *nur auf eine Art* geschehen kann, folgt daraus, dafs in (2.) die x nach (§. 30.) allgemein für ein- und dasselbe a und z jedes *nur einen Werth* haben können.

§. 32.

Lehrsatz.

Wenn man eine beliebige gegebene ganze Zahl Z nach (§. 30. 1.) durch

$$1. \quad Z = x_m A^m + x_{m-1} A^{m-1} + x_{m-2} A^{m-2} \dots + x_2 A^2 + x_1 A + x_0$$

ausdrückt, und man setzt

$$2. \quad nA = \mathfrak{G}s + r,$$

wo s ebenfalls gegeben, n willkürlich aber zu s theilerfremd und $r < s$ ist, so geht Z (1.) mit der Zahl s auf, oder nicht auf, je nachdem

$$3. \quad z = x_m r^m + n x_{m-1} r^{m-1} + n^2 x_{m-2} r^{m-2} + n^3 x_{m-3} r^{m-3} \dots \\ \dots + n^{m-2} x_2 r^2 + n^{m-1} x_1 r + n^m x_0$$

mit s aufgeht, oder nicht aufgeht.

Beweis. A. Wenn man von (2.) z. B. die k te Potenz nimmt, so ist nach (§. 11. No. 5.)

$$4. \quad n^k A^k = \mathfrak{G}s + r^k;$$

also der Reihe nach

$$5. \quad \left\{ \begin{array}{l} nA = \mathfrak{G}s + r, \\ n^2 A^2 = \mathfrak{G}s + r^2, \\ n^3 A^3 = \mathfrak{G}s + r^3, \\ n^4 A^4 = \mathfrak{G}s + r^4, \\ \dots \dots \dots \dots \dots \dots \dots \\ n^m A^m = \mathfrak{G}s + r^m. \end{array} \right.$$

B. Nun multiplicire man (1.) mit n^m , so ergiebt sich

$$6. \quad n^m Z = x_m n^m A^m + x_{m-1} n^m A^{m-1} + x_{m-2} n^m A^{m-2} \dots \\ \dots + x_2 n^m A^2 + x_1 n^m A + x_0 n^m.$$

Setzt man hierin die Ausdrücke von nA , $n^2 A^2$, $n^3 A^3$, ..., so erhält man

$$7. \quad n^m Z = x_m (\mathfrak{G}s + r^m) \\ + x_{m-1} (\mathfrak{G}s + r^{m-1}) n \\ + x_{m-2} (\mathfrak{G}s + r^{m-2}) n^2 \\ + x_{m-3} (\mathfrak{G}s + r^{m-3}) n^3 \\ \dots \dots \dots \\ + x_2 (\mathfrak{G}s + r^2) n^{m-2} \\ + x_1 (\mathfrak{G}s + r) n^{m-1} \\ + x_0 \quad \quad \quad n^m,$$

oder, nach (§. 11.),

$$8. \quad n^m Z = \mathfrak{G}s + x_m r^m + n x_{m-1} r^{m-1} + n^2 x_{m-2} r^{m-2} \dots \\ \dots + n^{m-2} x_2 r^2 + n^{m-1} x_1 r + n^m x_0,$$

oder auch, durch (3.) ausgedrückt,

$$9. \quad n^m Z = \mathfrak{G}s + z.$$

C. Geht nun hier z mit s auf, so gehen die *beiden* Glieder $\mathfrak{G}s$ und z mit s auf. Also muß alsdann nach (§. 18.) auch das *dritte* Glied $n^m Z$ mit s aufgehen. Aber n ist nach der Voraussetzung zu s *theilerfremd*, also auch n^m . Mithin geht von den beiden Factoren n^m und Z der Factor n^m *nicht* mit s auf. Dieserhalb muß zufolge (§. 25. I.) nothwendig der *andere* Factor Z mit s aufgehen. Also folgt, daß, wenn z (3.) mit s *aufgeht*, auch Z (1.) mit s *aufgehen* muß.

D. Geht in (9.) z *nicht* mit s auf, so kann auch Z nicht mit s aufgehen, denn sonst wäre $\frac{n^m Z}{s}$, so wie $\frac{\mathfrak{G}s}{s} = \mathfrak{G}$, eine ganze Zahl, also auch in $\frac{n^m Z - \mathfrak{G}s}{s} = \frac{z}{s}$, $\frac{n^m Z - \mathfrak{G}s}{s}$ eine ganze Zahl, $\frac{z}{s}$ dagegen ein Bruch, und einer ganzen Zahl kann ein Bruch nicht gleich sein

Dieses zusammen ist was der Lehrsatz behauptet.

Anm. Der Beweis beruht auf (§. 11, 18. und 25. I.).

§. 33.

Aufgabe.

Ob eine gegebene ganze Zahl Z mit einer andern gegebenen Zahl s *aufgehe*, vermittels anderer, von Z und s abhängender Zahlen z zu finden,

die, während sie *kleiner* sind als $\mathbf{Z}$, die Eigenschaft haben, dafs, je nachdem sie mit s aufgehen oder nicht aufgehen, das Gleiche auch mit $\mathbf{Z}$ geschieht.

Auflösung. **A.** In (§. 32.) zeigte sich, dafs

1. $\mathbf{Z} = x_m A^m + x_{m-1} A^{m-1} + x_{m-2} A^{m-2} \dots + x_2 A^2 + x_1 A + x_0$
mit s *aufgeht*, oder nicht *aufgeht*, je nachdem die Zahl

$$2. \quad z = x_m r^m + x_{m-1} n r^{m-1} + x_{m-2} n^2 r^{m-2} + x_{m-3} n^3 r^{m-3} \dots \\ \dots + x_2 n^{m-2} r^2 + x_1 n^{m-1} r + x_0 n^m,$$

in deren Ausdruck

$$3. \quad nA = \mathfrak{G}s + r$$

n eine *willkürliche* zu s *theilerfremde* Zahl ist, mit s *aufgeht* oder *nicht aufgeht*.

B. Dieser Satz kann zur Auflösung der gegenwärtigen Aufgabe dienen. Denn da r in (3.), wenn man es den *echten* positiven oder negativen Rest zu s sein läßt, jedenfalls $< s$, und wenn man für r den *unbedingt echten* Rest zu s nimmt, sogar $< \frac{1}{2}s$ ist, und man von den Multiplicatoren der x in (2.) wiederum nur die echten Reste zu s zu nehmen braucht: so sind die Multiplicatoren der x in (2.) immer kleiner als in (1.), und folglich ist immer z kleiner als $\mathbf{Z}$. Der Ausdruck (1.) für $\mathbf{Z}$ aber drückt nach (§. 30.) jede beliebige Zahl aus, und es ist nicht nöthig, dafs man grade, wie im dekadischen System, $A=10$ setzt, sondern es kann für A willkürlich eben sowohl $10^2=100$, $10^3=1000$ und so weiter genommen werden. Setzt man $A=10$, so sind die x blofs einfache Ziffern < 10 . Setzt man $A=100$, so sind die x Zahlen von 2 Ziffern und < 100 . Überhaupt sind die x , wenn man $A=10^k$ setzt, Zahlen von k Ziffern, aber jedenfalls $< A$. Für das dekadische Zahlensystem heifst die Gleichung (3.) allgemein

$$4. \quad n \cdot 10^k = \mathfrak{G}s + r,$$

und in dieser Gleichung sind die *beiden* Zahlen k und n *willkürlich*.

C. Da nun z (2.) *um so kleiner* sein wird, je kleiner r und n sind, insofern nicht k wiederum die x sehr grofs macht, so wird man die willkürlichen n und k so anzunehmen suchen müssen, dafs die r und n möglichst klein sind. Am *vortheilhaftesten* ist es offenbar, wenn r und n beide $= 1$ sein können; und *gut*, wenn wenigstens eins von ihnen $= 1$ ist.

D. Wenn s eine *theilbare* Zahl ist, so darf man eigentlich nur untersuchen, ob diejenigen *Stammzahlen*, oder diejenigen Potenzen von *Stammzahlen*, welche die Factoren von s sind, in $\mathbf{Z}$ aufgehen oder nicht. Denn wenn alle diese Factoren in $\mathbf{Z}$ aufgehen, so geht auch s in $\mathbf{Z}$ auf (§. 26.). Doch hindert nichts, auch s *auf einmal* in Rechnung zu bringen, wenn man

nur für n Zahlen setzt, die mit s keinen Theiler gemein haben. Vor Allem kommt es indessen auf die *Stammzahlen* an.

E. Auch kann, wenn ja z noch eine sehr *große* Zahl ist, auf dieselbe das Verfahren *wiederholt angewendet werden*, um zu noch *kleineren* Zahlen zu gelangen, mit welchen *zugleich* Z mit s aufgehe oder nicht aufgehe.

Beispiele.

No. 1. Es sei

$$s = 3 \quad \text{und} \quad s = 3^2 = 9.$$

Für diese beiden Werthe von s ist schon

$$5. \quad 10 = \textcircled{3}.3 + 1 = \textcircled{3}.9 + 1;$$

also $n = 1$, $k = 1$, $r = 1$ und in (2.)

$$6. \quad z = x_0 + x_1 + x_2 + \dots + x_m,$$

wo, wegen $k = 1$, die x die *bloßen Ziffern* von Z sind. Also geht die Zahl Z mit 3 und 9 auf, wenn die *Summe ihrer Ziffern* mit 3 und 9 aufgeht; wie bekannt.

No. 2. Es sei

$$s = 27 = 3^3.$$

Hier ist

$$7. \quad 10^3 = 37.27 + 1 = \textcircled{37}.27 + 1;$$

also ist hier $n = 1$, $k = 3$ und $r = 1$, und folglich in (2.) wieder

$$8. \quad z = x_0 + x_1 + x_2 + \dots + x_m,$$

wo aber, wegen $k = 3$, die x die Zahlen sind, welche je *drei Ziffern* von Z von der Rechten zur Linken ausdrücken. Folglich geht Z mit 27 auf, wenn die *Summe jener Zahlen* x mit 27 aufgeht.

Wäre z. B.

$$9. \quad Z = 25084365147,$$

so wäre

$$10. \quad z = 147 + 365 + 84 + 25 = 621.$$

Dieses z geht mit 27 auf, also muß auch Z mit 27 aufgehen; was auch der Fall ist.

No. 3. Es sei

$$s = 81 = 3^4.$$

Hier ist

$$11. \quad 10^9 = 12345679.81 + 1 = \textcircled{12345679}.81 + 1,$$

also ist hier $n = 1$, $k = 9$, $r = 1$ und in (2.) wieder

$$12. \quad z = x_0 + x_1 + x_2 + \dots + x_m,$$

wo, wegen $k = 9$, die x die Zahlen sind, welche je *neun Ziffern* von Z

von der Rechten zur Linken ausdrücken, und $\mathbf{Z}$ geht mit 81 auf, wenn die *Summe* dieser Zahlen mit 81 aufgeht.

Da aber z hier schon wenigstens 9 Ziffern hat, und also sehr groß ist, so mag man (4.) anders anzuwenden versuchen.

Es ist

$$13. \quad 8.10 = \mathfrak{G}.81 - 1,$$

also $n=8$, $k=1$, $r=-1$. Dieses giebt zunächst in (2.)

14. $z = (-1)^m [x_m - n x_{m-1} + n^2 x_{m-2} - n^3 x_{m-3} \dots \pm n^{m-1} x_1 \mp n^m x_0]$.
Sodann ist (nach §. 11. Anm. gerechnet, nemlich die echten Reste ϱ der Multiplicatoren der x genommen):

$$15. \quad \left\{ \begin{array}{ll} n = 8, & \text{also } \varrho_m = + 8, \\ n^2 = \mathfrak{G}.81 - 17, & \text{also } \varrho_{m-1} = - 17, \\ n^3 = \mathfrak{G}.81 + 26, & \text{also } \varrho_{m-2} = + 26, \\ n^4 = \mathfrak{G}.81 - 35, & \text{also } \varrho_{m-3} = - 35, \\ n^5 = \mathfrak{G}.81 - 37, & \text{also } \varrho_{m-4} = - 37, \\ n^6 = \mathfrak{G}.81 + 28, & \text{also } \varrho_{m-5} = + 28, \\ n^7 = \mathfrak{G}.81 - 19, & \text{also } \varrho_{m-6} = - 19, \\ n^8 = \mathfrak{G}.81 + 10, & \text{also } \varrho_{m-7} = + 10, \\ n^9 = \mathfrak{G}.81 - 1, & \text{also } \varrho_{m-8} = - 1; \end{array} \right. \quad \begin{array}{l} \text{(Die folgenden } \varrho \text{ sind} \\ \text{wieder dieselben; nur ha-} \\ \text{ben sie entgegengesetzte} \\ \text{Zeichen.)} \end{array}$$

folglich ist in (14.)

$$16. \quad z = \pm [x_m - 8.x_{m-1} - 17.x_{m-2} - 26.x_{m-3} - 35.x_{m-4} + 37.x_{m-5} \\ + 28.x_{m-6} + 19.x_{m-7} + 10.x_{m-8} + \dots],$$

wo die x die bloßen Ziffern der Zahl $\mathbf{Z}$ von der Linken zur Rechten sind.

Wäre z. B.

$$17. \quad \mathbf{Z} = 7943949936972,$$

so wäre nach (16.)

$$z = \pm [7 - 8.9 - 17.4 - 26.3 - 35.9 + 37.4 + 28.9 + 19.9 + 10.3 \\ + 1.6 - 8.9 - 17.7 - 26.2] \text{ oder}$$

$$21. \quad z = \pm [7 - 72 - 68 - 78 - 315 + 148 + 252 + 171 + 30 + 6 - 72 - 119 - 52] \\ = \pm (614 - 776) = \mp 162.$$

Dieses z geht mit 81 auf, also muß auch $\mathbf{Z}$ (17.) mit 81 aufgehen; was auch der Fall ist.

No. 4. Es sei

$$s = 7.$$

Hier ist

$$19. \quad 10^3 = 143.7 - 1,$$

also $n=1$, $k=3$ und $r=1$ und in (2.)

$$20. \quad z = x_0 - x_1 + x_2 - x_3 \dots \pm x_m,$$

wo die x die 3ziffrigen Zahlen in $\mathbf{Z}$ von der Rechten zur Linken sind.

Wäre z. B.

$$21. \quad \mathbf{Z} = 80939417280533,$$

so wäre zufolge (20.)

$$22. \quad z = 533 - 280 + 417 - 939 + 80 = 1030 - 1219 = -189.$$

Dieses z geht mit 7 auf; also auch $\mathbf{Z}$.

Wollte man (4.) anwenden, so könnte man setzen

$$23. \quad 5.10 = \mathfrak{G}.7 + 1;$$

also wäre $n=5$, $k=1$ und $r=1$. Dieses giebt für z in (2.)

$$24. \quad z = x_m + n x_{m-1} + n^2 x_{m-2} + n^3 x_{m-3} \dots + n^m x_0.$$

Nun ist

$$25. \quad \begin{cases} n = \mathfrak{G}.7 - 2, & n^4 = \mathfrak{G}.7 + 2, & n^7 = \mathfrak{G}.7 - 2, \\ n^2 = \mathfrak{G}.7 - 3, & n^5 = \mathfrak{G}.7 + 3, & n^8 = \mathfrak{G}.7 - 3, \\ n^3 = \mathfrak{G}.7 - 1, & n^6 = \mathfrak{G}.7 + 1, & n^9 = \mathfrak{G}.7 - 1, \end{cases} \quad \text{u. s. w.}$$

also in (24.)

$$z = x_m - 2x_{m-1} - 3x_{m-2} - x_{m-3} + 2x_{m-4} + 3x_{m-5} + x_{m-6} \dots \text{ oder}$$

$$26. \quad z = x_m - x_{m-3} + x_{m-6} - x_{m-9} \dots - 2(x_{m-1} - x_{m-4} + x_{m-7} \dots) \\ - 3(x_{m-2} - x_{m-5} + x_{m-8} \dots),$$

wo die x die einfachen Ziffern von $\mathbf{Z}$ sind. Dieser Ausdruck giebt z. B. für die Zahl $\mathbf{Z}$ (21.)

$$z = 8 - 3 + 1 - 8 + 3 - 2(0 - 9 + 7 - 0 + 3) - 3(9 - 4 + 2 - 5) \text{ oder}$$

$$27. \quad z = +1 - 2(+1) - 3(+2) = +1 - 2 - 6 = -7.$$

Dieses z geht mit 7 auf; also auch $\mathbf{Z}$.

No. 5. Es sei

$$s = 11.$$

Hier ist

$$28. \quad 10 = \mathfrak{G}.11 - 1 \quad \text{und} \quad 10 = \mathfrak{G}.11 + 1,$$

also $n=1$ und $r=-1$ für $k=1$, $r=+1$ für $k=2$. Mithin giebt (2.)

$$29. \quad z = -x_m + x_{m-1} - x_{m-2} + x_{m-3} \dots,$$

wo die x die einfachen Ziffern von $\mathbf{Z}$ sind, und

$$30. \quad z = x_m + x_{m-1} + x_{m-2} + x_{m-3} \dots,$$

wo die x die zweiziffrigen Zahlen in $\mathbf{Z}$ von der Rechten zur Linken bedeuten.

Z. B. für

$$31. \quad \mathbf{Z} = 37201458690434819$$

gibt (29.)

$$32. \quad z = -3 + 7 - 2 + 0 - 1 + 4 - 5 + 8 - 6 + 9 - 0 + 4 - 3 + 4 - 8 + 1 - 9 \\ = -37 + 37 = 0$$

und (30.) gibt

$$33. \quad z = 19 + 48 + 43 + 90 + 86 + 45 + 1 + 72 + 3 = 407$$

und, *wiederholt* angewendet,

$$34. \quad z = 4 + 7 = 11.$$

Diese z gehen mit 11 auf; also geht auch Z (31.) mit 11 auf.

No. 6. Es sei

$$s = 13.$$

Hier ist

$$35. \quad 10^3 = 77.13 - 1 = \mathfrak{G}.13 - 1,$$

also $n = 1$, $k = 3$, $r = -1$, mithin nach (2.)

$$36. \quad z = x_0 - x_1 + x_2 - x_3 \dots \pm x_m,$$

wo die x die *dreiziffrigen* Zahlen in Z von der Rechten zur Linken sind; eben wie in No. 4. für $s = 7$.

Will man (4.) anwenden, so kann man setzen:

$$37. \quad 4.10 = \mathfrak{G}13 + 1,$$

also $n = 4$, $k = 1$, $r = +1$, folglich in (2.)

$$38. \quad z = x_m + 4x_{m-1} + 4^2x_{m-2} + 4^3x_{m-3} \dots,$$

und da

$$39. \quad \begin{cases} n = \mathfrak{G}s + 4, & n^4 = \mathfrak{G}s - 4, & n^7 = \mathfrak{G}s + 4, \\ n^2 = \mathfrak{G}s + 3, & n^5 = \mathfrak{G}s - 3, & n^8 = \mathfrak{G}s + 3, & \text{u. s. w.} \\ n^3 = \mathfrak{G}s - 1, & n^6 = \mathfrak{G}s + 1, & n^9 = \mathfrak{G}s - 1, \end{cases}$$

ist,

$$40. \quad z = x_m + 4x_{m-1} + 3x_{m-2} - x_{m-3} - 4x_{m-4} - 3x_{m-5} \dots \text{ oder} \\ z = (x_m - x_{m-3} + x_{m-6} - x_{m-9} \dots) + 4(x_{m-1} - x_{m-4} + x_{m-7} \dots) \\ + 3(x_{m-2} - x_{m-5} + x_{m-8} \dots),$$

wo die x die einfachen Ziffern von Z sind.

Wäre z. B.

$$41. \quad Z = 589147620\dot{1}146758014,$$

so würde (36.)

$$42. \quad z = 14 - 758 + 146 - 201 + 476 - 891 + 5 = 641 - 1850 = -1209$$

und, *wiederholt* angewendet,

$$43. \quad z = 209 - 1 = 208$$

geben. Hingegen (40.) würde geben:

$$z = 5 - 1 + 6 - 1 + 6 - 8 + 4 + 4(8 - 4 + 2 - 1 + 7 - 0) \\ + 3(9 - 7 + 0 - 4 + 5 - 1) \text{ oder}$$

$$44. \quad z = 21 - 10 + 4(17 - 5) + 3(14 - 12) = 11 + 48 + 6 = 65.$$

Die z (43. und 44.) gehen mit $s=13$ auf; also auch Z (41.).

No. 7. Es sei

$$s = 17.$$

Hier kann man setzen:

$$45. \quad 10^2 = \mathfrak{G}.17 - 2,$$

also

$$46. \quad n = 1, \quad k = 2, \quad r = -2.$$

Dieses giebt in (2.)

$$z = x_0 - 2x_1 + 2^2x_2 - 2^3x_3 + 2^4x_4 \dots \text{ oder}$$

$$z = x_0 - 2x_1 + 4x_2 - 8x_3 - x_4 + 2x_5 - 4x_6 + 8x_7 + x_8 \dots \text{ oder}$$

$$47. \quad z = (x_0 - x_4 + x_8 - x_{12} \dots) - 2(x_1 - x_5 + x_9 \dots) + 4(x_2 - x_6 + x_{10} \dots) \\ - 8(x_3 - x_7 + x_{11} \dots),$$

wo die x die *zweiziffrigen* Zahlen in Z von der Rechten zur Linken sind.

Setzt man dagegen in (4.) $n=5$, $k=1$, so erhält man

$$48. \quad 5.10 = \mathfrak{G}.17 - 1 \text{ also } r = -1.$$

Dieses giebt in (2.)

$$z = -x_m + 5x_{m-1} - 5^2x_{m-2} + 5^3x_{m-3} - 5^4x_{m-4} \dots \text{ oder}$$

$$49. \quad z = -x_m + 5x_{m-1} - 8x_{m-2} + 6x_{m-3} + 4x_{m-4} - 3x_{m-5} \\ - 7x_{m-6} - x_{m-7} + 5x_{m-8} \dots,$$

wo x die einfachen Ziffern von Z sind.

Es sei z. B.

$$50. \quad Z = 308791540229761043805,$$

so giebt (47.)

$$z = 5 - 2.38 + 4.4 - 8.61 - 97 + 2.22 - 4.40 + 8.15 + 79 - 2.8 + 4.3 \\ \text{oder}$$

$$z = 5 + 16 + 44 + 120 + 79 + 12 - (76 + 488 + 97 + 160 + 16) \text{ oder}$$

$$z = 276 - 837 = -561$$

und, wiederholt angewendet,

$$51. \quad z = 61 - 25 = 51.$$

Hingegen (49.) giebt

$$z = -3 + 0 - 64 + 42 + 36 - 3 + 10 - 28 - 0 + 10 - 16 + 54 + 28 - 18 \\ + 2 - 0 - 4 + 15 - 64 + 0 + 20 \text{ oder}$$

$$52. \quad z = 217 - 200 = 17.$$

Beide Z (51. u. 52.) gehen mit $s=17$ auf; also geht auch Z (50.) mit 17 auf

No. 8. Es sei

$$s = 19.$$

Hier kann man in (4.) $n=2$, $k=1$ setzen. Dieses giebt

$$53. \quad 2.10 = \mathfrak{G} 19 + 1, \text{ also } r = 1,$$

folglich in (2.)

$$z = x_m + 2x_{m-1} + 2^2x_{m-2} + 2^3x_{m-3} + 2^2x_{m-4} \dots \text{ oder}$$

$$54. \quad z = x_m + 2x_{m-1} + 4x_{m-2} + 8x_{m-3} - 3x_{m-4} - 6x_{m-5} + 7x_{m-5} - 5x_{m-6} \\ + 9x_{m-7} - x_{m-7} - 2x_{m-1} - 4x_{m-2} \dots$$

Es sei z. B.

$$55. \quad Z = 13413966072992,$$

so giebt (54.)

$$z = 1 + 6 + 16 + 8 - 9 - 54 + 42 - 30 + 0 - 7 - 4 - 36 - 72 + 6 \text{ oder}$$

$$z = 79 - 212 = -133$$

und, wiederholt angewendet,

$$56. \quad z = 1 + 6 + 12 = 19.$$

Dieses z geht mit 19 auf; also auch Z .

F. Es würde nützlich sein, nach dieser Art eine *Tafel*, wenigstens für alle Stammzahlen, etwa bis 1000, zu berechnen.

Für eine solche *Tafel* würde es immer am besten sein, in (4.) n *stets* $= 1$ zu setzen. Ein anderer Werth von n kann zwar, wie sich an den obigen Beispielen zeigt, in einzelnen Fällen nützlich sein, aber wenn man eine voraus berechnete *Tafel* der Multiplicatoren der x in (2.) hat, nemlich eine *Tafel* der *echten Reste* der Multiplicatoren r^m , nr^{m-1} , n^2r^{m-2} etc. zu s , so ist es gleichgültig, was r in (4.) für $n=1$ ist: immer sind die Reste $< \frac{1}{2}s$. Ausserdem aber hat man, wenn immer $n=1$ ist, noch den Vortheil, dafs, wenn Z *nicht* mit s aufgeht, z auch *denselben Rest* läfst wie Z , so dafs man also in solchem Falle *auch noch sogleich den Rest der Division von Z mit s findet*; was nicht unmittelbar geschieht, wenn n *nicht* gleich 1 ist. Für $n=1$ nemlich giebt (9. §. 32.) blofs

$$57. \quad Z = \mathfrak{G}s + z,$$

und es folgt daraus, dafs, wenn man $Z = \mathfrak{G}s + \varrho_1$ und $z = \mathfrak{G}s + \varrho_2$ setzt, wo ϱ_1 und ϱ_2 beides die *unbedingt echten* Reste bezeichnen,

$$58. \quad \mathfrak{G}s + \varrho_1 = \mathfrak{G}s + \mathfrak{G}s + \varrho_2 = \mathfrak{G}s + \varrho_2$$

sein mufs; was nicht anders sein kann, als wenn ϱ_1 *gleich* ϱ_2 ist, indem es *nur einen* unbedingt echten Rest zu s giebt.

Ferner wird es für die *Tafel* auch gut sein, in (4.) k *stets gleich 1* zu setzen: denn in (2.), welches sich für $n=1$ auf

$$59. \quad z = x_m r^m + x_{m-1} r^{m-1} + x_{m-2} r^{m-2} + x_{m-3} r^{m-3} \dots + x_1 r + x_0.$$

oder, wenn man die unbedingt echten Reste $r^m, r^{m-1}, r^{m-2}, \dots$ durch $q_m, q_{m-1}, q_{m-2}, \dots$ bezeichnet, auf

$$60. \quad z = x_m q_m + x_{m-1} q_{m-1} + x_{m-2} q_{m-2} \dots + x_1 q_1 + x_0$$

reducirt, sind die Multiplicatoren q der x *immer* $< \frac{1}{2}s$. Ist nun $k=1$, so sind die x in (1.) oder (60.) die *einzelnen Ziffern* der Zahl Z , und z (60.) hat so viele Glieder als die Zahl Z einzelne Ziffern. Es kann also von dem q *nur das 1 bis 9fache* zu nehmen vorkommen. Ist dagegen $k > 1$, so hat zwar z in (60.) *weniger Glieder*, aber die x sind nun *mehrziffrige* Zahlen; eben wie die q ; letzteres wenn s einigermaßen groß ist. Mehrziffrige Zahlen mit *einander* zu multipliciren, wird aber, selbst wenn es *weniger oft* vorkommt, doch immer schwieriger sein, als bloß die 1 bis 9fachen der mehrziffrigen Zahlen q zu nehmen. Für *eine Tafel* ist das letztere aber noch *um so mehr* passend, da sich auch recht gut die 1 bis 9fachen der q vorausberechnen lassen und sogleich in die *Tafel* aufgenommen werden können, nicht aber wohl die 1 bis 100 oder die 1 bis 1000fachen u. s. w. Enthält nun die *Tafel* auf diese Weise sogleich die 1 bis 9fachen der q , im Voraus berechnet, so ist für z (60.) *gar keine Multiplication* weiter nöthig, sondern man kann die einzelnen Glieder der Reihe rechts in (60.) aus der *Tafel* unmittelbar *ablesen* und braucht nur die positiven wie die negativen Glieder zusammen- und die beiden Summen von einander abzuziehen.

G. Für die *Tafel* also würde man $n=1$ und $k=1$, folglich in (4.) bloß

$$61. \quad 10 = \mathfrak{G}s + r$$

zu setzen haben, welches, wenn $s > 10$ ist, gradezu $r=10$ giebt. Also sind dann die q in (60.) nichts andres als die *unbedingt echten* Reste der verschiedenen Potenzen von 10 selbst, zu s .

Für die Urzahl $s=857$ z. B. wäre

$$62. \quad \left\{ \begin{array}{lll} 10 = \mathfrak{G}.857 + q_1 & \text{und} & q_1 = + 10, \\ 10^2 = \mathfrak{G}.857 + q_2 & - & q_2 = + 100, \\ 10^3 = \mathfrak{G}.857 + q_3 & - & q_3 = + 143, \\ 10^4 = \mathfrak{G}.857 + q_4 & - & q_4 = - 284, \\ 10^5 = \mathfrak{G}.857 + q_5 & - & q_5 = - 269, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & - & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \end{array} \right.$$

Es würde daher, um zu finden, ob eine gegebene Zahl Z mit 857 aufgehe oder nicht, und welcher *Rest* im letzten Fall bleibe, von den Ziffern der Zahl Z , von der Rechten nach der Linken zu, die *erste* mit $+10$, die *zweite* mit $+100$, die *dritte* mit $+143$, die *vierte* mit -284 , die *fünfte* mit -269 u. s. w. zu multipliciren sein, und die algebraische Summe dieser Producte würde z (60.) geben. Je nachdem dieses z mit 857 aufgeht, oder nicht, geht auch die gegebene Zahl Z mit 857 auf, oder nicht; und wenn z *nicht* mit 857 aufgeht, so ist der *unbedingt echte* Rest von z zu 857 *derselbe*, wie der von Z .

Aber auch die 1 bis 9fachen der ϱ (62.), die vorkommen können, braucht man nicht so wie sie sind zu nehmen, sondern auch von ihnen nur die *unbedingt echten Reste* zu $s=857$. So würde man z. B. für die Vielfachen von $\varrho_4 = -284$ nicht -284 , -568 , -852 , -1136 u. s. w., sondern vielmehr nur -284 , $+289$, $+5$, -279 u. s. w. zu nehmen haben. Findet man nun diese Vielfachen in der Tafel, so ist für z (60.) *gar keine Multiplication* weiter nöthig, sondern nur die *Addition* von Zahlen, die sich, ganz ausgerechnet, in der Tafel finden.

Die Tafel würde für die Stammzahl $s=857$ Folgendes geben.

	Nummer der Ziffern von der Rechten zur Linken.	Werth der Ziffern.								
		1	2	3	4	5	6	7	8	9
	1	...	+ 1	+ 2	+ 3	+ 4	+ 5	+ 6	+ 7	+ 8
	2	...	+ 10	+ 20	+ 30	+ 40	+ 50	+ 60	+ 70	+ 80
	3	...	+ 100	+ 200	+ 300	+ 400	- 357	- 257	- 157	- 57
	4	...	+ 143	+ 286	- 428	- 285	- 142	+ 1	+ 144	+ 287
	5	...	- 284	+ 289	+ 5	- 279	+ 294	+ 10	- 274	+ 299
	6	...	- 269	+ 319	+ 50	- 219	+ 369	+ 100	- 169	+ 419
	7	...	- 119	- 238	- 357	+ 381	+ 262	+ 143	+ 24	- 95
	8	...	- 333	+ 191	- 142	+ 382	+ 49	- 284	+ 240	- 93
	9	...	+ 98	+ 196	+ 294	+ 392	- 367	- 269	- 171	- 73
	10	...	+ 123	+ 246	+ 369	- 365	- 242	- 119	+ 4	+ 127
	11	...	+ 373	- 111	+ 262	- 222	+ 151	- 333	+ 40	+ 413
	12	...	+ 302	- 253	+ 49	+ 351	- 204	+ 98	+ 400	- 155
	13	...	- 408	+ 41	- 367	+ 82	- 326	+ 123	- 285	+ 164
	14	...	+ 205	+ 410	- 242	- 37	+ 168	+ 373	- 279	- 74
	15	...	+ 336	- 185	+ 151	- 370	+ 34	+ 302	- 219	+ 117
	16	...	- 68	- 136	- 204	- 272	- 340	- 408	+ 381	+ 313
	17	...	+ 177	+ 354	- 326	- 119	+ 28	+ 205	+ 382	- 298
	18	...	+ 56	+ 112	+ 168	+ 224	+ 280	+ 336	+ 392	- 409
	19	...	- 297	+ 263	- 34	- 331	+ 229	- 68	- 365	+ 195
	20	...	- 399	+ 59	- 340	+ 118	- 281	+ 177	- 222	+ 236
	21	...	+ 295	- 267	+ 28	+ 323	- 239	+ 56	+ 351	- 211
	22	...	+ 379	- 99	+ 280	- 198	+ 181	- 297	+ 82	- 396
	23	...	+ 362	- 133	+ 229	- 266	+ 96	- 399	- 37	+ 325
	24	...	+ 192	+ 384	- 281	- 89	+ 103	+ 295	- 370	- 178

Wenn nun z. B.

$$64. \quad Z = 804739885214799049628954$$

wäre, so hätte man wie folgt zu rechnen:

65.	{	Für die 1te Ziffer	4 . . . +	4	Für die 7te Ziffer	9 . . . —	214
		- - 2te	- 5 . . . +	50	- - 11te	- 9 . . . —	71
		- - 3te	- 9 . . . +	43	- - 15te	- 2 . . . —	185
		- - 4te	- 8 . . . +	287	- - 16te	- 5 . . . —	340
		- - 5te	- 2 . . . +	289	- - 17te	- 8 . . . —	298
		- - 6te	- 6 . . . +	100	- - 18te	- 8 . . . —	409
		- - 8te	- 4 . . . +	382	- - 19te	- 9 . . . —	102
		- - 10te	- 9 . . . +	250	- - 20te	- 3 . . . —	340
		- - 12te	- 7 . . . +	400	- - 22te	- 4 . . . —	198
		- - 13te	- 4 . . . +	82	- - 24te	- 8 . . . —	178
		- - 14te	- 1 . . . +	205	Thut zusammen — 2335		
		- - 21te	- 7 . . . +	351	+ 2443		
		Thut zusammen + 2443				Bleibt + 108	

Die Zahl Z (64.) kann also mit $s=857$ *nicht* aufgehen, sondern es muß der Rest $+108$ bleiben; und so verhält es sich auch.

§. 34.

Lehrsatz.

Es seien u und v zwei beliebige, zu einander theilerfremde positive ganze Zahlen.

I. Setzt man in der Gleichung

$$1. \quad mv = nu + r$$

der Reihe nach

$$2. \quad m = 0, 1, 2, 3, 4, \dots u-1$$

und nimmt für alle r die positiven oder die negativen echten Reste, deren zeichenfreie Werthe also alle $< u$ sind, so ist kein r dem andern gleich, und die zeichenfreien Werthe von r sind nothwendig alle die Zahlen

$$3. \quad r = 0, 1, 2, 3, 4, \dots u-1,$$

obwohl in anderer Aufeinanderfolge als die von m .

Zugleich sind alle $n < v$, wenn $v > u$ ist. Ist $v < u$, so ist für diejenigen negativen r , welche mit v aufgehen und die sich dann unter den Werthen (3.) von r befinden, $n = v$.

Zu dem Werth 0 von m gehört $r = 0$, und zu $r = 0$ gehört $m = 0$ und $n = 0$.

II. Für jedes beliebige positive oder negative r in (1.), auch $r=0$ nicht ausgenommen, so daß also r allgemein durch

$$4. \quad r = \varepsilon u + r_0$$

ausgedrückt werden kann, wo ε eine ganze positive oder negative Zahl und r_0 eine der Zahlen (3.) ist, giebt es immer unzählige zusammengehörige ganzzahlige Werthe von m und n , welche der Gleichung (1.) genuthun. Sie werden allgemein durch

$$5. \quad m = \lambda u + m_0 \quad \text{und}$$

$$6. \quad n = \lambda v + n_0 - \varepsilon$$

ausgedrückt, wo λ willkürlich ist, das zu r_0 in (1.) gehörige m_0 aber immer eine der Zahlen

$$7. \quad m_0 = 0, 1, 2, 3, \dots u-1$$

und das zu r_0 gehörige n_0 eine der Zahlen

$$8. \quad n_0 = 0, 1, 2, 3, \dots v-1$$

bezeichnet, mit Ausnahme von $r_0 = -v$ für $v < u$, wo $n_0 = v$ ist. Ausser den durch (5. u. 6.) ausgedrückten Werthen von m und n giebt es aber keine andern.

III. Unter den unzähligen Werthen von m und n (5. u. 6.), die mit r (4.) der Gleichung (1.) genuthun, giebt es für jedes r immer einen und nur den einen positiven Werth $m_0 < u$ von m und ein und nur das eine negative $m_0 - u$, dessen zeichenfreier Werth $u - m_0$ ebenfalls $< u$ ist, aber nicht zugleich immer ein zugehöriges positives oder negatives n , dessen zeichenfreier Werth seinerseits $< v$ wäre, sondern letzteres nur in dem Falle, wenn in dem Ausdruck (4.) von r , $\varepsilon = 0$, also der zeichenfreie Werth von r eine der Zahlen (3.) ist. In diesem einen Falle sind auch die zeichenfreien Werthe der zu m_0 und $m_0 - u$ gehörigen Werthe n_0 und $n_0 - v$ von n aus den Zahlen (8.), und wenn $v < u$ ist, so ist für $r =$ den Vielfachen von $-v$, die $< u$ sind, $n_0 = v$. Wir wollen die Werthe m_0 und $m_0 - u$ von m , nebst dem zugehörigen $n_0 - \varepsilon$ und $n_0 - \varepsilon - v$ von n kleinste Wurzeln der Gleichung (1.) nennen.

IV. Wenn man dasjenige positive $m < u$ und das zugehörige positive $n < v$, welche in (1.) zu dem Rest $r = +1$ gehören, und welche nach (III.) immer Statt finden, durch m_1 und n_1 bezeichnet, so daß also m_1 und n_1 zu dem Reste $+1$ die kleinsten positiven Wurzeln der Gleichung

$$9. \quad mv = nu + 1$$

sind, so werden die kleinsten positiven und negativen Wurzeln der Gleichung (1.) zu einem beliebigen Rest r durch

$$10. \quad m_0 = m_1 r - \tau u \quad \text{und} \quad m_1 r - (\tau + 1)u \quad \text{und}$$

$$11. \quad n_0 - \varepsilon = n_1 r - \tau v \quad \text{und} \quad n_1 r - (\tau + 1)v$$

ausgedrückt, wo τu in (10.) dasjenige Vielfache von u bedeutet, welches, von $m_0 r$ abgezogen, einen positiven Rest $m_1 < u$ läßt. In (11.) muß τ denselben Werth bekommen, wie in (10.), wenn auch $n_0 r - \tau v$ nicht eine positive Zahl $< v$ ist.

Beispiel. Es sei

$$12. \quad v = 15, \quad u = 22.$$

Setzt man hier der Reihe nach $m = 0, 1, 2, 3, \dots, 21$, so ergibt sich

$$13. \quad \left\{ \begin{array}{ll} 0.15 = 0.22 + 0 = 0.22 - 0 & 11.15 = 7.22 + 11 = 8.22 - 11 \\ 1.15 = 0.22 + 15 = 1.22 - 7 & 12.15 = 8.22 + 4 = 9.22 - 18 \\ 2.15 = 1.22 + 8 = 2.22 - 14 & 13.15 = 8.22 + 19 = 9.22 - 3 \\ 3.15 = 2.22 + 1 = 3.22 - 21 & 14.15 = 9.22 + 12 = 10.22 - 10 \\ 4.15 = 2.22 + 16 = 3.22 - 6 & 15.15 = 10.22 + 5 = 11.22 - 17 \\ 5.15 = 3.22 + 9 = 4.22 - 13 & 16.15 = 10.22 + 20 = 11.22 - 2 \\ 6.15 = 4.22 + 2 = 5.22 - 20 & 17.15 = 11.22 + 13 = 12.22 - 9 \\ 7.15 = 4.22 + 17 = 5.22 - 5 & 18.15 = 12.22 + 6 = 13.22 - 16 \\ 8.15 = 5.22 + 10 = 6.22 - 12 & 19.15 = 12.22 + 21 = 13.22 - 1 \\ 9.15 = 6.22 + 3 = 7.22 - 19 & 20.15 = 13.22 + 14 = 14.22 - 8 \\ 10.15 = 6.22 + 18 = 7.22 - 4 & 21.15 = 14.22 + 7 = 15.22 - 15 \end{array} \right.$$

Wäre dagegen

$$14. \quad v = 22, \quad u = 15,$$

so wäre

$$15. \quad \left\{ \begin{array}{ll} 0.22 = 0.15 + 0 = 0.15 - 0 & 8.22 = 11.15 + 11 = 12.15 - 4 \\ 1.22 = 1.15 + 7 = 2.15 - 8 & 9.22 = 13.15 + 3 = 14.15 - 12 \\ 2.22 = 2.15 + 14 = 3.15 - 1 & 10.22 = 14.15 + 10 = 15.15 - 5 \\ 3.22 = 4.15 + 6 = 5.15 - 9 & 11.22 = 16.15 + 2 = 17.15 - 13 \\ 4.22 = 5.15 + 13 = 6.15 - 2 & 12.22 = 17.15 + 9 = 18.15 - 6 \\ 5.22 = 7.15 + 5 = 8.15 - 10 & 13.22 = 19.15 + 1 = 20.15 - 14 \\ 6.22 = 8.15 + 12 = 9.15 - 3 & 14.22 = 20.15 + 8 = 21.15 - 7 \\ 7.22 = 10.15 + 4 = 11.15 - 11 & \end{array} \right.$$

a. Wie (13. u. 15.) zeigen, sind die positiven so wie die negativen Reste alle unter einander *verschieden*, und beide sind in (13.) die Zahlen 0, 1, 2, 3, ..., 21 ($= u - 1$) und in (15.) die Zahlen 0, 1, 2, 3, ..., 14

($=u-1$). Desgleichen sind in (15.), wo $v > u$ ist, alle n ohne Ausnahme $< v (=22)$. In (13.) dagegen, wo $v < u$, ist für den Rest $r = -u = -15$, $n = 15 = v$. Die übrigen n sind ebenfalls alle $< v$. Desgleichen gehört überall zu $m = 0$, $r = 0$, und zu $r = 0$ gehört $m = 0$ und $n = 0$. Dieses zusammen ist was (I.) behauptet.

b. Es sei für (12.)

$$16. \quad r = 141 = 6 \cdot u + 9, \text{ also in (4.) } \varepsilon = 6, r_0 = 9.$$

Die zu $r_0 = 9$ gehörigen m_0 und n_0 sind zufolge (13.) $= 5$ und 3 : also ist nach (5. u. 6.)

$$17. \quad \begin{cases} m = \pm(1, 2, 3, \dots)22 + 5 & \text{und} \\ n = \pm(1, 2, 3, \dots)15 + 3 - 6 & = (1, 2, 3, \dots)15 - 3. \end{cases}$$

Man setze z. B. das willkürliche λ in (4. u. 5.) $= 4$, so ist nach (17.)

$$18. \quad \begin{cases} m = 4 \cdot 22 + 5 = 93 & \text{und} \\ n = 4 \cdot 15 - 3 = 57. \end{cases}$$

Diese m und n müssen also der Gleichung (1.) zu $r = 141$ genugthun, das heißt, es muß

$$19. \quad 93 \cdot 15 = 57 \cdot 22 + 141$$

sein; was auch der Fall ist.

Die *kleinsten* von den Werthen von m und n (17.) sind diejenigen für $\lambda = 0$, also $m = 5 < u$ und $n = -3$, welches die Werthe $m_0 = 5$ und $n_0 - \varepsilon = 3 - 6 = -3$ selbst sind; desgleichen sind es diejenigen für $\lambda = -1$, also $m = -17$ und $n = -18$, wo der zeichenfreie Werth 17 von m ebenfalls $< u$ ist. Also müssen auch die Werthe 5 und -17 von m , und -3 und -18 von n der Gleichung (1.) zu dem Rest $r = 141$ genugthun, das heißt, es muß

$$20. \quad \begin{cases} + 5 \cdot 15 = - 3 \cdot 22 + 141 & \text{und} \\ - 17 \cdot 15 = - 18 \cdot 22 + 141 \end{cases}$$

sein; was auch der Fall ist.

c. Es sei für (14.)

$$21. \quad r = -55 = -4 \cdot u + 5, \text{ so dafs in (4.) } \varepsilon = -4, r_0 = 5.$$

Die zu $r_0 = 5$ gehörigen m_0 und n_0 sind zufolge (15.) $= 5$ und 7 , also ist nach (5. u. 6.)

$$22. \quad \begin{cases} m = \pm(1, 2, 3, \dots)15 + 5 & \text{und} \\ n = \pm(1, 2, 3, \dots)22 + 7 + 4. \end{cases}$$

Man setze das willkürliche λ in (4. u. 5.) $= -2$, so ist nach (22.)

$$23. \quad \begin{cases} m = -2.15 + 5 = -25 & \text{und} \\ n = -2.22 + 11 = -33 \end{cases}$$

Diese m und n müssen der Gleichung (1.) zu $r = -55$ genugthun, das heisst, es mufs

$$24. \quad -25.22 = -33.15 - 55$$

sein; was auch der Fall ist.

Die *kleinsten* von den Werthen von m und n (22.) sind wieder diejenigen für $\lambda = 0$, also $m = 5 < u$ und $n = 11$, welches die Werthe von $m_0 = 5$ und $n_0 - \varepsilon = 7 - (-4) = 11$ *selbst* sind; desgleichen sind es diejenigen für $\lambda = -1$, also $m = -10$ und $n = -11$, wo der zeichenfreie Werth 10 von m ebenfalls $< u$ ist. Also müssen auch die Werthe 5 und -10 von m und 11 und -11 von n der Gleichung (1.) zu dem Reste $r = -55$ genugthun, das heisst es mufs

$$25. \quad \begin{cases} + 5.22 = + 11.15 - 55 & \text{und} \\ -10.22 = -11.15 - 55 \end{cases}$$

sein; was auch der Fall ist.

Die Resultate in (b. u. c.) sind den Behauptungen in (II. u. III.) gemäß.

d. Für (12.) ist zufolge (13.) dasjenige m und n , welches dem Rest $+1$ entspricht, $= 3$ und 2 , so dafs also für (12.)

$$26. \quad m_1 = 3 \quad \text{und} \quad n_1 = 2$$

ist. Nun sei, wie in (16.),

$$27. \quad r = 141,$$

so giebt (10. u. 11.)

$$28. \quad \begin{cases} m_0 = 3.141 - 19.22 = +5, & \text{also } \tau = 19 \text{ und } m_0 = 3.141 - 20.22 = -17 \text{ und} \\ n_0 = 2.141 - 19.15 = -3 \text{ und} & n_0 = 2.141 - 20.15 = -18, \end{cases}$$

und diese m_0 und n_0 müssen der Gleichung (1.) für den Rest $r = 141$ genugthun; was auch zufolge (20.) der Fall ist.

e. Für (14.) ist zufolge (15.) dasjenige m und n , welches dem Rest $+1$ entspricht $= 13$ und 19 , so dafs also für (14.)

$$29. \quad m_1 = 13 \quad \text{und} \quad n_1 = 19$$

ist. Nun sei, wie in (21.),

$$30. \quad v = -55,$$

so giebt (10. und 11.)

$$31. \quad \begin{cases} m_0 = -13.55 + 48.15 = +5, & \text{also } \tau = -48 \text{ und } m_0 = -13.55 + 47.15 = -10 \text{ und} \\ n_0 = -19.55 + 48.22 = +11 \text{ und} & n_0 = -19.55 + 47.22 = -11, \end{cases}$$

und diese m_0 und n_0 müssen der Gleichung (1.) für den Rest $r = -55$ genugthun; was auch zufolge (25.) der Fall ist.

Die Resultate (d. u. e.) sind den Behauptungen in (IV.) gemäß.

Beweis. *A.* Gäben zwei verschiedene m , z. B. m_β und m_γ , beide $< u$, mit den dazu gehörigen n_β und n_γ *ein und dasselbe* r , so dafs also

$$32. \quad \begin{cases} m_\beta v = n_\beta u \pm r \text{ und} \\ m_\gamma v = n_\gamma u \pm r \end{cases}$$

wäre, so würde daraus

$$33. \quad (m_\beta - m_\gamma)v = (n_\beta - n_\gamma)u$$

folgen, und also müfste $m_\beta - m_\gamma$ mit u *aufgehen*, da v nach der Voraussetzung keinen Theiler mit u gemein hat (§. 25.) Dieses kann aber nicht sein, da m_β und m_γ beide $< u$ sind und folglich auch $m_\beta - m_\gamma < u$ ist. Also können keine zwei m , beide $< u$, *einen und denselben* Rest $\pm r$ lassen, und folglich sind *alle* zu $m = 1, 2, 3, \dots, u-1$ gehörigen r *von einander verschieden*.

Die *Anzahl* der r ist aber der der Werthe von m *gleich*, und folglich $= u$. Zugleich sollen die zeichenfreien Werthe aller $r < u$ sein. Also sind diese zeichenfreien Werthe der r nothwendig *alle* die u Zahlen $0, 1, 2, 3, \dots, u-1$ selbst; gemäß (3.)

B. Der *größte* Werth von n findet in (1.) offenbar für den *größten* Werth von m Statt, also für $m = u-1$. Man setze für $m = u-1$ in (1.)

$$34. \quad (u-1)v = xu \pm r.$$

Soll hier r *positiv* sein, so kann x nicht $= v$ sein, selbst nicht für $r = 0$; denn $x = v$ würde immer $xu = vu > (u-1)v$ geben. Folglich ist für *positive* r , x , also n , *immer* $< v$.

Soll r *negativ* sein, so folgt aus

$$35. \quad (u-1)v = v.u - v = (v \mp x)u - (xu \mp v),$$

dafs nur dann

$$36. \quad n = v \mp x$$

sein kann, wenn

$$37. \quad xu \mp v < u$$

ist; denn der absolute Werth $xu \mp v$ des Restes in (35.) soll *immer* $< u$ sein. Die Bedingung (37.) ist aber nur für $x = 0$ erfüllbar; denn für *jedes* größere x ist $xu \mp v$ nicht $< u$, sondern $> u$, was auch v sein mag. *Nie* also kann zufolge (36.) $n > v$ sein. Es kann höchstens $= v$ sein, und dieses zufolge (37.) nur dann wenn $v < u$ ist. Nun ist für ein *beliebiges* $u - \mu$ fache von v :

$$38. \quad (u - \mu)v = v.u - \mu v.$$

Ist nun $v < u$, so kann auch noch $\mu v < u$ sein. Also für alle die Reste $-v, -2v, -3v, \dots, -\mu v$, die auch *alle* vorkommen, ist $n = v$.

Zusammen also folgt, dafs n für $v > u$ *immer* $< v$ ist; desgleichen auch für $v < u$, ausgenommen wenn der *negative Rest* mit v aufgeht; wie solches der Lehrsatz in (1.) behauptet.

C. Ist $m = 0$, so giebt (1.)

$$39. \quad 0 = nu + r.$$

Also mufs r mit u *aufgehen* (§. 18.). Dieses geschieht nur dann, wenn $r = 0$ ist, indem r jedenfalls $< u$ sein soll. Also ist für $m = 0$, $r = 0$, und folglich vermöge (39.) auch $n = 0$.

Ist $r = 0$, so giebt (1.)

$$40. \quad mv = nu,$$

also mufs m mit u *aufgehen* (§. 25.). Dieses ist nur möglich, wenn $m = 0$ ist, indem $m < u$ sein soll. Also ist für $r = 0$, $m = 0$, und folglich vermöge (40.) auch $n = 0$.

So behauptet es (I.).

D. Setzt man (5., 6. und 4.) in (1.), so ergibt sich

$$(\lambda u + m_0)v = (\lambda v + n_0 - \varepsilon)u + \varepsilon u + r_0 \quad \text{oder}$$

$$41. \quad m_0 v = n_0 u + r_0.$$

Diese Gleichung entspricht der (1.) mit allen den Werthen (7.) von m_0 , (8.) von n_0 und (3.) von r_0 . Also thun alle die durch (5. u. 6.) ausgedrückten Werthe von m und n mit jedem *beliebigen* λ der Gleichung (1.) ein Genüge; wie es (II.) behauptet.

E. Gäbe es noch andere Werthe von m und n , als die, welche (5. u. 6.) ausdrückt, so könnten es nur solche sein, die durch

$$42. \quad m = \lambda u + m_0 + \mu \quad \text{und}$$

$$43. \quad n = \lambda v + n_0 - \varepsilon + \nu$$

ausgedrückt werden, wo μ eine Zahl ist, die *nicht* mit u , ν eine Zahl, die *nicht* mit v *aufgeht*; denn ginge μ mit u auf, so wäre (42.) schon in (5.) und (43.) schon in (6.) *mitbegriffen*, indem dort λ *willkürlich* ist. Setzt man nun (42. u. 43.) nebst (4.) in (1.), so ergibt sich

$$(\lambda u + m_0 + \mu)u = (\lambda v + n_0 - \varepsilon + \nu)u + \varepsilon u + r_0 \quad \text{oder}$$

$$44. \quad m_0 v + \mu v = n_0 u + \nu u + r_0.$$

Hiervon die Gleichung (41.), die nothwendig zugleich Statt findet, abgezogen, giebt

$$45. \quad \mu v = \nu u.$$

Dieses ist wieder nur möglich, wenn μ mit u und ν mit v *aufgeht* (§. 25.). Und da dies *nicht* sein *soll*, so finden die Ausdrücke (42. u. 43.) von m und

n nicht Statt: mithin giebt es aufser den Werthen von m und n , welche (5. u. 6.) ausdrückt, *keine andern*; wie es (II.) behauptet.

F. Da λ in (5. u. 6.) willkürlich ist, so kann es auch 0 und -1 sein. Dieses giebt

$$46. \quad m = m_0 \quad \text{und} \quad m = m_0 - u \quad \text{und}$$

$$47. \quad n = n_0 - \varepsilon \quad \text{und} \quad n = n_0 - \varepsilon - v.$$

Hier sind m_0 und $m_0 - u$ dieselben beiden m , (an zeichenfreien Werth beide $< u$) welche der Gleichung (1.) für Reste $< u$ genugthun. Also thun *dieselben beiden* m auch der Gleichung (1.) für *beliebige* Reste r (4.) genug. Dagegen sind die *zugehörigen* beiden Werthe $n_0 - \varepsilon$ und $n_0 - \varepsilon - v$ von n *nicht* nothwendig $< v$. Sie sind es nur, wenn $\varepsilon = 0$, also r eine der Zahlen (3.) ist.

Dieses ist, was (III.) behauptet.

G. Multiplicirt man die in (IV.) vorausgesetzte Gleichung

$$48. \quad m_1 v = n_1 u + 1$$

mit r , so ergiebt sich

$$49. \quad m_1 r v = n_1 r u + r.$$

Hiervon die Gleichung

$$50. \quad m_0 v = (n_0 - \varepsilon) u + r,$$

die sich ergiebt, wenn man (5. u. 6.) in (1.) und das willkürliche $\lambda = 0$ setzt, abgezogen, giebt

$$51. \quad (m_1 r - m_0) v = (n_1 r - (n_0 - \varepsilon)) u.$$

Dieser Gleichung gemäß muß $m_1 r - m_0$ mit u aufgehen (§. 25.) und also

$$52. \quad m_1 r - m_0 = \tau u$$

sein, wo τ irgend eine *ganze* Zahl ist. Ferner giebt (52.), in (51.) gesetzt,

$$\tau u v = (n_1 r - (n_0 - \varepsilon)) u, \text{ also}$$

$$53. \quad \tau v = n_1 r - (n_0 - \varepsilon).$$

Aus (52. u. 53.) folgt (10. u. 11.) zunächst für ein *positives* $m_0 < u$, und dann, wenn man noch u und v abzieht, also $\tau + 1$ statt τ schreibt, auch für ein negatives m_0 , dessen absoluter Werth $< u$ ist.

Dies ist, was (IV.) behauptet.

H. Anm. Ein Hauptpunct des Beweises ist das Mittel, durch welches in (A.) gezeigt wird, daß nicht zwei verschiedene Vielfachen von v zu u *gleiche* Reste lassen können. Es kommt sehr häufig zur Anwendung. Dann der Schlufs, daß die Reste, weil sie alle verschieden und $> v$ und $< u$ sind, die Zahlen 1, 2, 3, 4, $u - 1$ selbst sein müssen. Auch dieser Schlufs kommt öfter vor.

§. 35.

Lehrsatz.

Es seien u und v zwei beliebige zu einander theilerfremde positive ganze Zahlen.

Setzt man in der Gleichung

$$1. \quad mv = Gu + r$$

der Reihe nach

$$2. \quad m = 1, 2, 3, 4, \dots \frac{1}{2}(u-1), \text{ wenn } u \text{ ungerade, und}$$

$$3. \quad m = 1, 2, 3, 4, \dots \frac{1}{2}u, \text{ wenn } u \text{ gerade ist,}$$

und bezeichnet diejenigen Werthe von m , welche in (1.) positive Reste $r > \frac{1}{2}u$ geben, durch $m_1, m_2, m_3, \dots m_x$, die übrigen Werthe von m , welche positive Reste nicht $> \frac{1}{2}u$ geben, durch $\mu_1, \mu_2, \mu_3, \dots \mu_{\frac{1}{2}(u-1)-x}$ oder $\mu_{\frac{1}{2}u-x}$, setzt darauf für alle r , die $> \frac{1}{2}u$ sind,

$$4. \quad r = u - \varrho,$$

wo nun also auch alle ϱ , eben wie die übrigen r , nicht größer als $\frac{1}{2}u$ sind, so dafs zusammengekommen

Erstlich für ein ungerades u :

$$5. \quad \left\{ \begin{array}{l} m_1 v = Gu + r_1, \\ m_2 v = Gu + r_2, \\ m_3 v = Gu + r_3, \\ \dots \dots \dots \\ m_{\frac{1}{2}(u-1)-x} v = Gu + r_{\frac{1}{2}(u-1)-x} \end{array} \right. \quad \text{und} \quad 6. \quad \left\{ \begin{array}{l} \mu_1 v = Gu - \varrho_1, \\ \mu_2 v = Gu - \varrho_2, \\ \mu_3 v = Gu - \varrho_3, \\ \dots \dots \dots \\ \mu_x v = Gu - \varrho_x; \end{array} \right.$$

Zweitens für ein gerades u :

$$7. \quad \left\{ \begin{array}{l} m_1 v = Gu + r_1, \\ m_2 v = Gu + r_2, \\ m_3 v = Gu + r_3, \\ \dots \dots \dots \\ m_{\frac{1}{2}u-x} v = Gu + r_{\frac{1}{2}u-x} \end{array} \right. \quad \text{und} \quad 8. \quad \left\{ \begin{array}{l} \mu_1 v = Gu - \varrho_1, \\ \mu_2 v = Gu - \varrho_2, \\ \mu_3 v = Gu - \varrho_3, \\ \dots \dots \dots \\ \mu_x v = Gu - \varrho_x \end{array} \right.$$

ist, so sind die absoluten Werthe der r und ϱ zusammengekommen nothwendig

9. *Im ersten Falle (5. u. 6.) alle die Zahlen $1, 2, 3, 4, \dots \frac{1}{2}(u-1)$ und*

10. *Im zweiten Falle (7. u. 8.) alle die Zahlen $1, 2, 3, 4, \dots \frac{1}{2}u$.*

Beispiele. 1. Es sei

$$11. \quad u = 15, \quad v = 22,$$

so ist

$$12. \quad (1, 2, 3, 4, 5, 6, 7)v = \mathfrak{G}u + 7, 14, 6, 13, 5, 12 \text{ und } 4.$$

Von diesen Resten sind die $z=3$ Reste, 14, 13 und $12 > \frac{1}{2}u$, also ist in (5. u. 6.)

$$13. \quad (1, 2, 3, 4, 5, 6, 7)v = \mathfrak{G}u + 7, -1, +6, -2, +5, -3 \text{ und } +4.$$

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7; gemäß (9.).

2. Es sei

$$14. \quad u = 15, \quad v = 4,$$

so ist

$$15. \quad (1, 2, 3, 4, 5, 6, 7)v = Nu + 4, 8, 12, 1, 5, 9 \text{ und } 13.$$

Von diesen Resten sind die $z=4$ Reste 8, 12, 9 und $13 > \frac{1}{2}u$, also ist in (5. und 6.)

$$16. \quad (1, 2, 3, 4, 5, 6, 7)v = \mathfrak{G}u + 4, -7, -3, +1, +5, -6 \text{ und } -2.$$

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7; gemäß (9.).

3. Es sei

$$17. \quad u = 18, \quad v = 49,$$

so ist

$$18. \quad (1, 2, 3, 4, 5, 6, 7, 8, 9)v = \mathfrak{G}u + 13, 8, 3, 16, 11, 6, 1, 14 \text{ und } 9.$$

Von diesen Resten sind die $z=4$ Reste 13, 16, 11 und $14 > \frac{1}{2}u$, also ist in (7. u. 8.)

$$19. \quad (1, 2, 3, 4, 5, 6, 7, 8, 9)v = \mathfrak{G}u - 5, +8, +3, -2, -7, +6, \\ +1, -4 \text{ und } +9.$$

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7, 8, 9; gemäß (10.).

4. Es sei

$$20. \quad u = 22, \quad v = 15,$$

so ist

$$21. \quad (1, 2, 3, \dots, 11)v = \mathfrak{G}u + 15, 8, 1, 16, 9, 2, 17, 10, 3, 18, 11.$$

Von diesen Resten sind die $z=4$ Reste 15, 16, 17 und $18 > \frac{1}{2}u$, also ist in (7. u. 8.)

$$22. \quad (1, 2, 3, \dots, 11)v = \mathfrak{G}u - 7, +8, +1, -6, +9, +2, -5, \\ +10, +3, -4, +11.$$

Die zeichenfreien Werthe *dieser Reste* r und ϱ sind zusammen alle die Zahlen 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 und 11; gemäß (10.).

Beweis. *A.* Kein r in (1.) kann $=0$ sein. Denn für $r=0$ wäre in (1.) $mv = \mathfrak{G}u$, also müßte m mit u aufgehen, da v zu u *theilerfremd* sein soll (§. 25.). m geht aber nicht mit u auf, weil alle $m < u$ sind (2. u. 3.); also kann r nicht $=0$ sein.

B. Wäre in (5. oder 7.) irgend ein r einem andern gleich, also z. B.

$$23. \quad m_e v = \mathfrak{G}u + r \quad \text{und} \quad m_\lambda v = \mathfrak{G}u + r,$$

so würde daraus

$$24. \quad (m_e - m_\lambda) v = \mathfrak{G}u$$

folgen, und also müßte $m_e - m_\lambda$ mit u aufgehen (§. 25.). Dieses ist aber nicht der Fall, da m_e und m_λ beide $< u$ sind und also $m_e - m_\lambda$ noch um so mehr $< u$ ist. Daher kann *kein* r dem andern gleich sein.

C. Ganz aus gleichen Gründen kann in (6. oder 8.) kein ϱ dem andern gleich sein.

D. Wäre in (5. und 6.) oder in (7. und 8.) ein r einem ϱ gleich, also z. B.:

$$25. \quad m_e v = \mathfrak{G}u + r \quad \text{und} \quad \mu_\lambda v = \mathfrak{G}u + r$$

so würde daraus

$$26. \quad (m_e + \mu_\lambda) v = \mathfrak{G}u$$

folgen; also müßte $m_e + \mu_\lambda$ mit u aufgehen (§. 25.). Aber in (5. und 6.) sind *alle* m oder $\mu < \frac{1}{2}u$ (2.) und in (7. und 8.) kann *nur eines* der m oder $\mu = \frac{1}{2}u$ sein (3.), die andern sind nothwendig *kleiner*: folglich ist *immer* $m_e + \mu_\lambda < u$. Mithin kann $m_e + \mu_\lambda$ *nicht* mit u aufgehen, und folglich kann in (5. und 6.), eben wie (7. und 8.), *kein* r einem ϱ gleich sein. Die r und ϱ sind also *alle* unter einander verschieden, und keins ist 0.

E. Nun ist die *Anzahl* der r und ϱ zusammengenommen der der m *gleich*, also in (5. und 6.) $= \frac{1}{2}(u-1)$ (2.) und in (7. und 8.) $= \frac{1}{2}u$ (3.): keins ist größer als $\frac{1}{2}u$, und alle sind von einander verschieden (*B.*, *C.* und *D.*). Also sind die r und ϱ zusammengenommen in (5. und 6.) nothwendig die Zahlen $1, 2, 3, \dots, \frac{1}{2}(u-1)$, und in (7. und 8.) nothwendig die Zahlen $1, 2, 3, \dots, \frac{1}{2}u$ selbst; wie es der Lehrsatz in (9. und 10.) behauptet.

F. Anm. Die in der Anmerkung zum vorigen Parapgraph erwähnten Schlüsse sind auch hier die Hauptmomente des Beweises.

§. 36.

Lehrsatz.

Es seien u und v zwei beliebige ungerade und zu einander theilerfremde ganze Zahlen und z sei eine beliebige positive ganze Zahl

$$1. \quad z < \frac{1}{2}uv.$$

Alsdann können, wenn man für ein und dasselbe z ,

$$2. \quad z = m_1 u + r \quad \text{und}$$

$$3. \quad z = m_2 v + \varrho$$

setzt, wo r und ϱ die echten positiven Reste zu u und v bezeichnen, so daß immer

$$4. \quad r < u \quad \text{und} \quad \varrho < v$$

ist, folgende verschiedene Fälle stattfinden.

$$5. \quad \left\{ \begin{array}{l} \text{Erstlich, wenn } r > \frac{1}{2}u \text{ ist, kann} \\ \quad 1) \quad \varrho = 0, \\ \quad 2) \quad \varrho < \frac{1}{2}v > 0, \\ \quad 3) \quad \varrho > \frac{1}{2}v \text{ sein.} \\ \text{Zweitens, wenn } r < \frac{1}{2}u > 0 \text{ ist, kann} \\ \quad 1) \quad \varrho = 0, \\ \quad 2) \quad \varrho < \frac{1}{2}v > 0 \text{ und} \\ \quad 3) \quad \varrho > \frac{1}{2}v \text{ sein.} \\ \text{Drittens, wenn } r = 0 \text{ ist, kann} \\ \quad 1) \quad \varrho < \frac{1}{2}v > 0 \text{ und} \\ \quad 2) \quad \varrho > \frac{1}{2}v \text{ sein.} \end{array} \right.$$

Bezeichnet man für diese 8 Fälle die Anzahl der $z < \frac{1}{2}uv$,

$$6. \quad \left\{ \begin{array}{llll} 1) & \text{für welche } r > \frac{1}{2}u & \text{und } \varrho = 0 & \text{ist, durch } n_1, \\ 2) & - - - r > \frac{1}{2}u & - \varrho < \frac{1}{2}v > 0 & - - - n_2, \\ 3) & - - - r > \frac{1}{2}u & - \varrho > \frac{1}{2}v & - - - n_3, \\ 4) & - - - r < \frac{1}{2}u > 0 & - \varrho = 0 & - - - n_4, \\ 5) & - - - r < \frac{1}{2}u > 0 & - \varrho < \frac{1}{2}v > 0 & - - - n_5, \\ 6) & - - - r < \frac{1}{2}u > 0 & - \varrho > \frac{1}{2}v & - - - n_6, \\ 7) & - - - r = 0 & - \varrho < \frac{1}{2}v > 0 & - - - n_7, \\ 8) & - - - r = 0 & - \varrho > \frac{1}{2}v & - - - n_8, \end{array} \right.$$

so ist

Erstlich, die Gesamtheit aller dieser verschiedenen z ,

$$7. \quad n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 = \frac{1}{2}(uv - 1).$$

Zweitens, die Anzahl der $n_7 + n_8$ mit u aufgehenden z ist

$$8. \quad n_7 + n_8 = \frac{1}{2}(v - 1).$$

Drittens, die Anzahl der $n_1 + n_4$ mit v aufgehenden z ist

$$9. \quad n_1 + n_4 = \frac{1}{2}(u - 1);$$

Viertens, die Anzahl der $n_2 + n_5 + n_7$ verschiedenen z , welche, mit v dividirt, Reste $\varrho < \frac{1}{2}v > 0$ lassen, gleichviel welche Reste r sie mit u dividirt geben mögen, ist

$$10. \quad n_2 + n_5 + n_7 = \frac{1}{4}(u+1)(v-1).$$

Fünftens, die Anzahl der $n_4 + n_5 + n_6$ verschiedenen z , welche, mit u dividirt, Reste $r < \frac{1}{2}u > 0$ lassen, gleichviel welche Reste ϱ sie mit v dividirt geben mögen, ist

$$11. \quad n_4 + n_5 + n_6 = \frac{1}{4}(u-1)(v+1).$$

Sechstens, die Anzahl der $n_3 + n_6 + n_8$ verschiedenen z , welche, mit v dividirt, Reste $\varrho > \frac{1}{2}v$ lassen, gleichviel welche Reste r sie mit u dividirt geben mögen, ist

$$12. \quad n_3 + n_6 + n_8 = \frac{1}{4}(u-1)(v-1).$$

Siebtens, die Anzahl der $n_1 + n_2 + n_3$ verschiedenen z , welche mit u dividirt Reste $r > \frac{1}{2}u$ lassen, gleichviel welche Reste ϱ sie mit v dividirt geben mögen, ist

$$13. \quad n_1 + n_2 + n_3 = \frac{1}{4}(u-1)(v-1).$$

Achtens, die Anzahl der $n_3 + n_5$ verschiedenen z , welche mit u und mit v dividirt entweder zugleich Reste $r > \frac{1}{2}u$ und $\varrho > \frac{1}{2}v$, oder zugleich Reste $r < \frac{1}{2}u > 0$ und $\varrho < \frac{1}{2}v > 0$ lassen, ist

$$14. \quad n_3 + n_5 = \frac{1}{4}(u-1)(v-1).$$

Neuntens, die Anzahl der $n_2 + n_6$ verschiedenen z , welche mit u und mit v dividirt entweder zugleich Reste $r > \frac{1}{2}u$ und $\varrho < \frac{1}{2}v > 0$, oder zugleich Reste $r < \frac{1}{2}u > 0$ und $\varrho > \frac{1}{2}v$ lassen, ist

$$15. \quad n_2 + n_6 = \frac{1}{4}(u-1)(v-1).$$

Zehntens, die doppelte Anzahl $2n_5$ derjenigen z , welche mit u und mit v dividirt zugleich Reste $r < \frac{1}{2}u > 0$ und $\varrho < \frac{1}{2}v > 0$ lassen, weniger der Anzahl n_1 derjenigen mit v aufgehenden z , welche mit u dividirt Reste $> \frac{1}{2}u$ lassen, und der mit u aufgehenden n_8 Zahlen z , welche mit v dividirt Reste $> \frac{1}{2}v$ lassen, ist

$$16. \quad 2n_5 - n_1 - n_8 = \frac{1}{4}(u-1)(v-1).$$

Elftens, die Anzahl der mit v aufgehenden n_1 verschiedenen z , welche Reste $> \frac{1}{2}u$ lassen, zusammen mit der Anzahl der n_8 mit u aufgehenden z , welche Reste $> \frac{1}{2}v$ lassen, und der Anzahl n_3 der z , welche mit u und v dividirt zugleich Reste $r > \frac{1}{2}u$ und $\varrho > \frac{1}{2}v$ lassen, ist der Anzahl n_5 derjenigen z gleich, welche mit u und v dividirt zugleich Reste $r < \frac{1}{2}u > 0$ und $\varrho < \frac{1}{2}v > 0$ lassen,

das heißt, es ist

$$17. \quad n_1 + n_2 + n_3 = n_5.$$

Beispiel. Es sei

$$18. \quad u = 7, \quad v = 11, \quad \text{also} \quad uv = 77 \quad \text{und}$$

$$19. \quad z = 1, 2, 3, 4, \dots, 38 (= \tfrac{1}{2}(uv - 1)),$$

so geben die beiden Gleichungen (2. u. 3.) Folgendes:

$$20. \quad \left\{ \begin{array}{l} \text{Für } z = 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 11 \ 12 \ 13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19 \ 20 \ 21 \ 22 \ 23 \ 24 \ 25 \ 26 \ 27 \ 28 \ 29 \ 30 \ 31 \ 32 \ 33 \ 34 \ 35 \ 36 \ 37 \ 38 \\ \text{ist } m_1 = 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 3 \ 3 \ 3 \ 3 \ 3 \ 3 \ 4 \ 4 \ 4 \ 4 \ 4 \ 4 \ 5 \ 5 \ 5 \ 5 \\ \quad r = 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 0 \ 1 \ 2 \ 3 \\ \quad m_2 = 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 3 \ 3 \ 3 \ 3 \ 3 \ 3 \\ \quad q = 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9 \ 10 \ 0 \ 1 \ 2 \ 3 \ 4 \ 5 \end{array} \right.$$

$$21. \quad 5 \ 5 \ 5 \ 2 \ 2 \ 3 \ 8 \ 6 \ 6 \ 6 \ 1 \ 2 \ 2 \ 7 \ 5 \ 5 \ 6 \ 3 \ 3 \ 3 \ 8 \ 4 \ 5 \ 5 \ 2 \ 2 \ 2 \ 8 \ 6 \ 6 \ 6 \ 3 \ 1 \ 2 \ 7 \ 5 \ 5 \ 5$$

Die horizontale Zeile (21.) giebt die *Nummer* der 8 Classen (6.) an, in welche jedes z gehört. Z. B.: Für $z = 17$ ist $r = 3 < \tfrac{1}{2}u > 0$ und $q = 6 > \tfrac{1}{2}v$, also gehört $z = 17$ in die *sechste* Classe (6.); und so die andern. Zufolge (21.) gehören also

$$22. \quad \left\{ \begin{array}{l} \text{die 2 Zahlen 11 und 33 in die } \textit{erste} \text{ Classe, folglich ist hier } n_1 = 2; \\ \text{die 8 Zahlen 4, 5, 12, 13, 25, 26, 27 und 34 gehören in} \\ \quad \text{die } \textit{zweite} \text{ Classe, also ist } n_2 = 8; \\ \text{die 5 Zahlen 6, 18, 19, 20 und 32 gehören in die } \textit{dritte} \\ \quad \text{Classe, also ist } n_3 = 5; \\ \text{die 1 Zahl 22 gehört in die } \textit{vierte} \text{ Classe, also ist } n_4 = 1; \\ \text{die 10 Zahlen 1, 2, 3, 15, 16, 23, 24, 36, 37 und 38} \\ \quad \text{gehören in die } \textit{fünfte} \text{ Classe, also ist } n_5 = 10; \\ \text{die 7 Zahlen 8, 9, 10, 17, 29, 30, 31 gehören in die} \\ \quad \textit{sechste} \text{ Classe, also ist } n_6 = 7; \\ \text{die 2 Zahlen 14 und 35 gehören in die } \textit{siebente} \text{ Classe,} \\ \quad \text{also ist } n_7 = 2; \\ \text{die 3 Zahlen 7, 21 und 28 gehören in die } \textit{achte} \text{ Classe,} \\ \quad \text{also ist } n_8 = 3. \end{array} \right.$$

Diese Werthe der verschiedenen n thun nun wie folgt den Gleichungen (7. bis 17.) des Lehrsatzes Genüge. Nämlich

$$23. \quad \left\{ \begin{array}{l} \text{die Gleichung (7.) ist hier } 2 + 8 + 5 + 1 + 10 + 7 + 2 + 3 = 38 = \tfrac{1}{2}(uv - 1), \\ - \quad - \quad - \quad (8.) \quad - \quad - \quad 2 + 3 = 5 = \tfrac{1}{2}(v - 1), \\ - \quad - \quad - \quad (9.) \quad - \quad - \quad 2 + 1 = 3 = \tfrac{1}{2}(u - 1), \\ - \quad - \quad - \quad (10.) \quad - \quad - \quad 8 + 10 + 2 = 20 = \tfrac{1}{4}(u + 1)(v - 1) = \tfrac{1}{4} \cdot 8 \cdot 10, \end{array} \right.$$

$$23. \left\{ \begin{array}{l} \text{die Gleichung (11.) ist hier } 1+10+7=18=\frac{1}{4}(u-1)(v+1)=\frac{1}{4}.6.12, \\ - \quad - \quad - \quad (12.) \quad - \quad 5+7+3=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ - \quad - \quad - \quad (13.) \quad - \quad 2+8+5=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ - \quad - \quad - \quad (14.) \quad - \quad 5+10=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ - \quad - \quad - \quad (15.) \quad - \quad 8+7=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ - \quad - \quad - \quad (16.) \quad - \quad 2.10-2-3=15=\frac{1}{4}(u-1)(v-1)=\frac{1}{4}.6.10, \\ - \quad - \quad - \quad (17.) \quad - \quad 2+3+5=10; \end{array} \right.$$

Alles wie gehörig.

Beweis. **A.** Dafs alle die 8 verschiedenen Classen für die z stattfinden *können*, ist offenbar. Es ist nur zu bemerken, dafs nicht, wie es scheinen könnte, auch noch für (5. Drittens), eben wie (5. Erstlich und Zweitens), ein *dritter* Fall $r=0$ und *zugleich* $\varrho=0$, also keine *neunte* Classe möglich ist. Denn könnte ein z mit u und v *zugleich* *aufgehen*, so würde es, da u und v nach der Voraussetzung zu einander *theilerfremd* sind, zufolge (§. 26.) auch mit dem Product uv *aufgehen* müssen; was nicht möglich ist, da das *größte* der z erst $\frac{1}{2}(uv-1)$ ist und also *alle* $z < uv$ sind.

B. Dafs kein z in *mehr als einer* Classe *zugleich* vorkommen kann, ist ebenfalls offenbar; denn eine Zahl z kann zu einer andern u oder v nicht *verschiedene* Reste zugleich lassen. Da nun zugleich jedes z nothwendig in einer der 8 Classen vorkommen *mufs*, indem nicht mehr als die 8 Fälle möglich sind, so folgt, dafs die *Summe* der Mengen der z in den verschiedenen 8 Classen der Anzahl der z *selbst* gleich ist. Diese letztere ist $\frac{1}{2}(uv-1)$, also mufs

$$24. \quad n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 = \frac{1}{2}(uv-1)$$

sein. Dies ist die Gleichung (7.) des Lehrsatzes.

C. Die mit u *aufgehenden* z , $n_7 + n_8$ an der Zahl, sind offenbar die *Vielfachen*

$$25. \quad u, 2u, 3u, 4u, \dots \frac{1}{2}(v-1)u$$

von u , und keine mehr; denn das *nächste* Vielfache von u , nemlich $\frac{1}{2}(v+1)u$, ist schon *größer* als der *größte* Werth $\frac{1}{2}(uv-1)$ von z . Die Anzahl jener Vielfachen von u (25.) ist aber $\frac{1}{2}(v-1)$, also ist

$$26. \quad n_7 + n_8 = \frac{1}{2}(v-1).$$

Dieses ist die Gleichung (8.) des Lehrsatzes.

D. Die mit v *aufgehenden* z , $n_1 + n_4$ an der Zahl, sind die *Vielfachen*

$$27. \quad v, 2v, 3v, 4v, \dots \frac{1}{2}(u-1)v$$

von v , und keine mehr; denn das *nächste* Vielfache von v , nemlich $\frac{1}{2}(u+1)v$, ist schon *größer* als der *größte* Werth $\frac{1}{2}(uv-1)$ von z . Die Anzahl der

$$\begin{aligned} n_3 + n_6 + n_8 &= \frac{1}{2}(uv - 1) - \frac{1}{2}(u - 1) - \frac{1}{4}(u + 1)(v - 1) \text{ oder} \\ &= \frac{1}{2}uv - \frac{1}{2} - \frac{1}{2}u + \frac{1}{2} - \frac{1}{4}uv + \frac{1}{4}u - \frac{1}{4}v + \frac{1}{4} \text{ oder} \end{aligned}$$

$$33. \quad n_3 + n_6 + n_8 = \frac{1}{4}uv - \frac{1}{4}u - \frac{1}{4}v + \frac{1}{4} = \frac{1}{4}(u - 1)(v - 1).$$

Dies ist die Gleichung (12.) des Lehrsatzes.

H. Die $n_1 + n_2 + n_3$ Zahlen z in (6.) lassen sämmtlich nach u Reste $r > \frac{1}{2}u$. Zieht man $n_7 + n_8 = \frac{1}{2}(v - 1)$ (8.) und $n_4 + n_5 + n_6 = \frac{1}{4}(u - 1)(v + 1)$ (11.) von $n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 = \frac{1}{2}(uv - 1)$ (7.) ab, so ergibt sich

$$\begin{aligned} n_1 + n_2 + n_3 &= \frac{1}{2}(uv - 1) - \frac{1}{2}(v - 1) - \frac{1}{4}(u - 1)(v + 1) \text{ oder} \\ &= \frac{1}{2}uv - \frac{1}{2} - \frac{1}{2}v + \frac{1}{2} - \frac{1}{4}uv - \frac{1}{4}u + \frac{1}{4}v + \frac{1}{4} \text{ oder} \end{aligned}$$

$$34. \quad n_1 + n_2 + n_3 = \frac{1}{4}uv - \frac{1}{4}u - \frac{1}{4}v + \frac{1}{4} = \frac{1}{4}(u - 1)(v - 1).$$

Dies ist die Gleichung (13.) des Lehrsatzes.

I. a. So wie die $\frac{1}{2}(uv - 1)$ Zahlen

$$35. \quad 1, 2, 3, 4, \dots, \frac{1}{2}(uv - 1)$$

durch z bezeichnet wurden, so mögen die *weiter folgenden* $\frac{1}{2}(uv - 1)$ Zahlen

$$36. \quad \frac{1}{2}(uv + 1), \frac{1}{2}(uv + 3), \frac{1}{2}(uv + 5), \dots, uv - 1$$

durch w bezeichnet werden. Alsdann gehört zu *jedem* z ein w , und *nur ein* w , welches mit ihm zusammen uv ausmacht: nemlich 1 mit $uv - 1$, 2 mit $uv - 2$, 3 mit $uv - 3$, $\dots$ $\frac{1}{2}(uv - 1)$ mit $\frac{1}{2}(uv + 1)$ zusammen machen sämmtlich uv aus. Wenn man also in der Gleichung

$$37. \quad z + w = uv$$

dem z *alle* die $\frac{1}{2}(uv - 1)$ Werthe (35.), die es haben kann, giebt, so hat w seinerseits *alle* die $\frac{1}{2}(uv - 1)$ Werthe (36.), die ihm zukommen.

b. Nun sei für irgend ein z , welches weder mit u noch mit v *aufgeht*, nach (2. u. 3.)

$$38. \quad z = m_1 u + r = m_2 v + \varrho,$$

wo also weder r noch ϱ Null aber $r < u$, $\varrho < v$ ist. Für das *zugehörige* w sei

$$39. \quad w = \mu_1 u + r' = \mu_2 v + \varrho',$$

wo $r' < u$ und $\varrho' < v$ angenommen wird; alsdann kann auch weder r' noch ϱ' Null sein. Denn ginge w mit u oder mit v auf, so müßte zufolge (37.) auch z mit u oder mit v aufgehen, gegen die Voraussetzung. Zuzufolge (37.) ist aus (38. u. 39.)

$$40. \quad z + w = (m_1 + \mu_1)u + r + r' = (m_2 + \mu_2)v + \varrho + \varrho' = uv.$$

Dieses ist so viel als die *zwei* Gleichungen

$$41. \quad uv = (m_1 + \mu_1)u + r + r' \quad \text{und}$$

$$42. \quad uv = (m_2 + \mu_2)v + \varrho + \varrho'.$$

Aus (41. u. 42.) folgt, dafs $r + r'$ mit u und $\varrho + \varrho'$ mit v *aufgehen* mufs (§. 18.). Aber $r + r'$ ist > 0 und $< 2u$, weil $r > 0 < u$ und $r' > 0 < u$; also mufs nothwendig

$$43. \quad r + r' = u$$

sein; denn zwischen 0 und $2u$ liegt keine andere Zahl als u selbst, die mit u aufginge. Gleichmäfsig ist $\varrho + \varrho' > 0$ und $< 2v$, weil $\varrho > 0 < v$ und $\varrho' > 0 < v$ ist; also mufs auch nothwendig

$$44. \quad \varrho + \varrho' = v$$

sein; aus gleichen Gründen.

Aus (43. u. 44.) folgt nun weiter, dafs, wenn $r > \frac{1}{2}u$ ist, $r' < \frac{1}{2}u > 0$ sein mufs, und umgekehrt; desgleichen, dafs, wenn $\varrho > \frac{1}{2}v$ ist, $\varrho' < \frac{1}{2}v > 0$ sein mufs, und umgekehrt.

c. Nun sind n_3 Zahlen z vorhanden, für welche $r > \frac{1}{2}u$ und *zugleich* $\varrho > \frac{1}{2}v$ ist (6.), also mufs es *eben so viele* Zahlen w geben, für welche $r' < \frac{1}{2}u > 0$ und *zugleich* $\varrho' < \frac{1}{2}v > 0$ ist, denn zu jedem z gehört ein w , für welches $r' < \frac{1}{2}u > 0$ und $\varrho' < \frac{1}{2}v > 0$, wenn für das zugehörige z , $r > \frac{1}{2}u$ und $\varrho > \frac{1}{2}v$ ist (6.).

Desgleichen sind n_5 Zahlen z vorhanden, für welche $r < \frac{1}{2}u > 0$ und *zugleich* $\varrho < \frac{1}{2}v > 0$ ist (6.); also mufs es *eben so viele* Zahlen w geben, für welche $r' > \frac{1}{2}u$ und *zugleich* $\varrho' > \frac{1}{2}v$ ist; aus gleichen Gründen.

Es sind also unter den Zahlen z und w *zusammengenommen*, das heisst unter den Zahlen

$$45. \quad 1, 2, 3, 4, \dots, uv - 1$$

nothwendig überhaupt $n_3 + n_5$ Zahlen vorhanden, die, weder mit u noch mit v *aufgehend*, nach u Reste r oder $r' > \frac{1}{2}u$ und *zugleich* nach v Reste ϱ oder $\varrho' > \frac{1}{2}v$ lassen; und *eben so viele* Zahlen, welche, weder mit u noch mit v *aufgehend*, nach u Reste r oder $r' < \frac{1}{2}u > 0$ und *zugleich* nach v Reste ϱ oder $\varrho' < \frac{1}{2}v > 0$ lassen.

d. Um durch u und v ausgedrückt zu finden, wie viele solcher letztgenannten Zahlen unter den z und w *zusammengenommen* sich befinden, bezeichne x jede derjenigen Zahlen aus der *Gesammtheit* der z und w , also aus den Zahlen (45.), welche mit u dividirt einen Rest $\varepsilon < \frac{1}{2}u > 0$ und mit v dividirt einen Rest $\sigma < \frac{1}{2}v > 0$ läfst; so dafs also

$$46. \quad x = eu + \varepsilon = sv + \sigma$$

ist, wo $\varepsilon < \frac{1}{2}u > 0$, *zugleich* $\sigma < \frac{1}{2}v > 0$ und $x < uv$ also $e < v$, $s < u$ sein soll.

e. Aus (46.) folgt

$$47. \quad sv = eu + \varepsilon - \sigma.$$

In dieser Gleichung soll also ε alle die Werthe $1, 2, 3, \dots, \frac{1}{2}(u-1)$ und σ alle die Werthe $1, 2, 3, \dots, \frac{1}{2}(v-1)$ bekommen können, während $s < u$, $e < v$ ist. Was nun auch $\varepsilon - \sigma$ sein mag, positiv, oder negativ, oder Null: immer giebt es nach (§. 34. III.) einen Werth von $s < u$, welcher der Gleichung (47.) genug thut; also kann in (47.) und folglich in (46.) in der That $s < u$ und folglich, da σ nothwendig $< v$ ist, auch $x < uv$ sein. Also kann in (46.) ε wirklich alle die Werthe $1, 2, 3, \dots, \frac{1}{2}(u-1)$ und σ alle die Werthe $1, 2, 3, \dots, \frac{1}{2}(v-1)$ haben, für $x < uv$.

f. Nun kann zunächst in (46.) erst ε ohne Rücksicht auf $sv + \sigma$ offenbar alle die Werthe $1, 2, 3, 4, \dots, \frac{1}{2}(u-1)$ haben; denn *alle* die x , welche diese Werthe des Restes ε geben, sind *vorhanden*.

Aber giebt man dem ε irgend einen *bestimmten* Werth, z. B. 1, so kann zufolge (e.) für dieses *nemliche* $\varepsilon = 1$, σ jeden der $\frac{1}{2}(v-1)$ Werthe $1, 2, 3, \dots, \frac{1}{2}(v-1)$ haben, und zwar offenbar immer für ein *anderes* x , da ein und dasselbe x nicht verschiedene Reste σ lassen kann. Für $\varepsilon = 1$ findet sich also zu jedem $\sigma = 1, 2, 3, \dots, \frac{1}{2}(v-1)$ irgend ein x . Folglich giebt es in (46.) $\frac{1}{2}(v-1)$ *verschiedene* x , die alle den Rest $\varepsilon = 1$, aber die *verschiedenen* Reste $\sigma = 1, 2, 3, \dots, \frac{1}{2}(v-1)$ lassen.

Ganz gleich verhält es sich für *jeden* der $\frac{1}{2}(u-1)$ Werthe $1, 2, 3, \dots, \frac{1}{2}(u-1)$, welche ε haben kann.

Also giebt es überhaupt $\frac{1}{2}(u-1) \cdot \frac{1}{2}(v-1) = \frac{1}{4}(u-1)(v-1)$ verschiedene x unter den Zahlen (45.), welche nach u Reste $< \frac{1}{2}u > 0$ und *zugleich* nach v Reste $< \frac{1}{2}v > 0$ lassen. Die Anzahl dieser Zahlen war (c.) $= n_3 + n_5$, also ist

$$48. \quad n_3 + n_5 = \frac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (14.) des Lehrsatzes.

K. Zieht man $n_7 + n_8 = \frac{1}{2}(v-1)$ (8.), $n_1 + n_4 = \frac{1}{2}(u-1)$ (9.) und $n_3 + n_5 = \frac{1}{4}(u-1)(v-1)$ (14.) von $n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 = \frac{1}{2}(uv-1)$ (7.) ab, so ergiebt sich

$$n_2 + n_6 = \frac{1}{2}(uv-1) - \frac{1}{2}(v-1) - \frac{1}{2}(u-1) - \frac{1}{4}(u-1)(v-1) \text{ oder}$$

$$n_2 + n_6 = \frac{1}{2}uv - \frac{1}{2} - \frac{1}{2}v + \frac{1}{2} - \frac{1}{2}u + \frac{1}{2} - \frac{1}{4}uv + \frac{1}{4}u + \frac{1}{4}v - \frac{1}{4} \text{ oder}$$

$$49. \quad n_2 + n_6 = \frac{1}{4}uv - \frac{1}{2}u - \frac{1}{2}v + \frac{1}{4} = \frac{1}{4}(u-1)(v-1).$$

Dieses ist die Gleichung (15.) des Lehrsatzes.

L. Addirt man $n_2 + n_6 = \frac{1}{4}(u-1)(v-1)$ (15.) zu $2(n_3 + n_5) = \frac{1}{2}(u-1)(v-1)$ (14.) und zieht von der Summe $n_2 + n_6 + n_8 = \frac{1}{4}(u-1)(v-1)$ (12.) und $n_1 + n_2 + n_3 = \frac{1}{4}(u-1)(v-1)$ (13.) ab, so ergibt sich
 $2(n_3 + n_5) + n_2 + n_6 - n_3 - n_6 - n_8 - n_1 - n_2 - n_3 = (\frac{1}{2} + \frac{1}{4} - \frac{1}{4} - \frac{1}{4})(u-1)(v-1)$ oder
 50. $2n_5 - n_1 - n_8 = \frac{1}{4}(u-1)(v-1)$.

Dieses ist die Gleichung (16.) des Lehrsatzes.

M. Zieht man endlich $n_3 + n_5 = \frac{1}{4}(u-1)(v-1)$ (14.) von $2n_5 - n_1 - n_8 = \frac{1}{4}(u-1)(v-1)$ (16.) ab, so ergibt sich

$$2n_5 - n_1 - n_8 - n_3 - n_5 = 0 \text{ oder}$$

$$51. \quad n_1 + n_8 + n_3 = n_5.$$

Dieses ist die Gleichung (17.) des Lehrsatzes.

N. Anm. Der Theil des Beweises (**L.**) enthält eigenthümliche Erwägungen und bedarf wesentlich des Satzes (§. 34.), welcher auch weiterhin oft nöthig ist. Alles Übrige ist sehr einfach.

§. 37.

Lehrsatz.

I. *Es seien m und n zwei beliebige positive ganze Zahlen und es sei*

$$1. \quad n > m.$$

Setzt man

$$2. \quad \left\{ \begin{array}{l} m = \mu_1 n + r_1, \\ 2m = \mu_2 n + r_2, \\ 3m = \mu_3 n + r_3, \\ \dots \dots \dots \\ (n-1)m = \mu_{n-1} n + r_{n-1}, \\ nm = \mu_n n + r_n, \end{array} \right. \quad \text{und} \quad 3. \quad \left\{ \begin{array}{l} n = \nu_1 m + \varrho_1, \\ 2n = \nu_2 m + \varrho_2, \\ 3n = \nu_3 m + \varrho_3, \\ \dots \dots \dots \\ (m-1)n = \nu_{m-1} m + \varrho_{m-1}, \\ mn = \nu_m m + \varrho_m \end{array} \right.$$

unter der Bedingung, daß die sämtlichen r und q positiv sind und

4. *die r aus den Zahlen 1, 2, 3, 4, . . . n,*

5. *die q aus den Zahlen 0, 1, 2, 3, . . . m-1*

genommen werden, und bezeichnet die Summe der sämtlichen Quotienten μ , nemlich

$$6. \quad \mu_1 + \mu_2 + \mu_3 \dots + \mu_{n-1} + \mu_n \text{ durch } S\mu;$$

die Summe der sämtlichen Quotienten ν , nemlich

$$7. \quad \nu_1 + \nu_2 + \nu_3 \dots + \nu_{m-1} + \nu_m \text{ durch } S\nu;$$

die Summe der sämtlichen Reste r, nemlich

$$8. \quad r_1 + r_2 + r_3 \dots + r_{n-1} + r_n \text{ durch } Sr;$$

die Summe der sämtlichen Reste ϱ , nemlich

9. $\varrho_1 + \varrho_2 + \varrho_3 \dots + \varrho_{m-1} + \varrho_m$ durch $S\varrho$,
so ist

$$10. \quad r_n = n, \quad \varrho_m = 0,$$

$$11. \quad \mu_n = m-1 \text{ und } \nu_m = n,$$

$$12. \quad S\mu + S\nu = mn,$$

$$13. \quad mSr + nS\varrho = \frac{1}{2}mn(m+n).$$

II. Sind m und n zu einander theilerfremd, so ist

$$14. \quad Sr = \frac{1}{2}n(n+1),$$

$$15. \quad S\varrho = \frac{1}{2}m(m-1),$$

$$16. \quad S\mu = \frac{1}{2}(n+1)(m-1) \quad \left\{ \begin{array}{l} S\mu + S\nu = mn, \\ S\nu = \frac{1}{2}((n-1)m + n + 1) \end{array} \right.$$

$$17. \quad S\nu = \frac{1}{2}((n-1)m + n + 1)$$

$$18. \quad S\mu - \mu_n = S\nu - \nu_m = \frac{1}{2}(n-1)(m-1).$$

Beispiel 1. Es sei für beliebige m und n ,

$$19. \quad m = 8, \quad n = 20,$$

so ist in (2 u. 3.)

$$20. \quad \left\{ \begin{array}{l} 1, \quad 2m = 0n + 8, \quad 16, \\ 3, \quad 4, \quad 5m = 1n + 4, \quad 12, \quad 20, \\ 6, \quad 7m = 2n + 8, \quad 16, \\ 8, \quad 9, \quad 10m = 3n + 4, \quad 12, \quad 20, \\ 11, \quad 12m = 4n + 8, \quad 16, \\ 13, \quad 14, \quad 15m = 5n + 4, \quad 12, \quad 20, \\ 16, \quad 17m = 6n + 8, \quad 16, \\ 18, \quad 19, \quad 20m = 7n + 4, \quad 12, \quad 20, \end{array} \right. \quad \text{und} \quad 21. \quad \left\{ \begin{array}{l} 1n = 2m + 4, \\ 2n = 5m + 0, \\ 3n = 7m + 4, \\ 4n = 10m + 0, \\ 5n = 12m + 4, \\ 6n = 15m + 0, \\ 7n = 17m + 4, \\ 8n = 20m + 0. \end{array} \right.$$

Die Summe aller Quotienten μ und ν ist hier

$$S\mu + S\nu = 2.0 + 3.1 + 2.2 + 3.3 + 2.4 + 3.5 + 2.6 + 3.7 + 2.5 + 7.10 + 12.15 + 17.20, \text{ oder}$$

$$22. \quad S\mu + S\nu = 3 + 4 + 9 + 8 + 15 + 12 + 21 + 88 = 160 = 8.20 = mn; \text{ gemäß (12.). Ferner ist}$$

$$23. \quad \mu_n = 7 = m-1 \text{ und } \nu_m = 20 = n; \text{ gemäß (11.),}$$

$$24. \quad mSr + nS\varrho = 8(8 + 16 + 4 + 12 + 20)4 + 20.4.4 = 4.8.60 + 320 = 2240 = \frac{1}{2}.8.20(8+20) = \frac{1}{2}mn(m+n); \text{ gemäß (13.),}$$

$$25. \quad r_n = 20 = n \text{ und } \varrho_m = 0; \text{ gemäß (10.).}$$

Beispiel 2. Es sei für theilerfremde m und n ,

$$26. \quad m = 9, \quad n = 38,$$

so ist in (2 u. 3.)

$$\begin{array}{lcl}
27. \left\{ \begin{array}{l} 1, 2, 3, 4m = 0n + 9, 18, 27, 36, \\ 5, 6, 7, 8m = 1n + 7, 16, 25, 34, \\ 9, 10, 11, 12m = 2n + 5, 14, 23, 32, \\ 13, 14, 15, 16m = 3n + 3, 12, 21, 30, \\ 17, 18, 19, 20, 21m = 4n + 1, 10, 19, 28, 37, \\ 22, 23, 24, 25m = 5n + 8, 17, 26, 35, \\ 26, 27, 28, 29m = 6n + 6, 15, 24, 33, \\ 30, 31, 32, 33m = 7n + 4, 13, 22, 31, \\ 34, 35, 36, 37, 38m = 8n + 2, 11, 20, 29, 38, \end{array} \right. & & 28. \left\{ \begin{array}{l} 1n = 4m + 2, \\ 2n = 8m + 4, \\ 3n = 12m + 6, \\ 4n = 16m + 8, \\ 5n = 21m + 1, \\ 6n = 25m + 3, \\ 7n = 29m + 5, \\ 8n = 33m + 7, \\ 9n = 38m + 0. \end{array} \right.
\end{array}$$

Die Summe der Quotienten μ und ν ist hier

$$\begin{aligned}
S\mu &= 4.0 + 4.1 + 4.2 + 4.3 + 5.4 + 4.5 + 4.6 + 4.7 + 5.8 \quad \text{oder} \\
29. \quad S\mu &= 4 + 8 + 12 + 20 + 20 + 24 + 28 + 40 = 156 = \frac{1}{2}(38+1)(9-1) \\
&= \frac{1}{2}.39.8 = \frac{1}{2}(n+1)(m-1); \text{ gemäß (16.)}
\end{aligned}$$

Die Summe der Quotienten ν ist

$$\begin{aligned}
30. \quad S\nu &= 4 + 8 + 12 + 16 + 21 + 25 + 29 + 33 + 38 = 186 \\
&= \frac{1}{2}((38-1).9 + 38 + 1) = \frac{1}{2}(37.9 + 39) = 186 = \frac{1}{2}((n-1)m + n + 1); \\
&\text{gemäß (17.). Ferner ist}
\end{aligned}$$

$$\begin{aligned}
31. \quad S\mu - \mu_n &= 156 - 8 = S\nu - \nu_m = 186 - 38 = 148 = \frac{1}{2}.37.8 \\
&= \frac{1}{2}(n-1)(m-1); \text{ gemäß (18.),} \\
32. \quad Sr &= (1+2+3+\dots+38) = \frac{1}{2}.38.39 = \frac{1}{2}n(n+1); \text{ gemäß (14.),} \\
33. \quad Sq &= (1+2+3+\dots+8) = \frac{1}{2}.8.9 = \frac{1}{2}m(m-1); \text{ gemäß (15.).}
\end{aligned}$$

Beweis. A. Da $m < n$ sein soll und zufolge der *ersten* Gleichung (3.) $\nu_1 m$ noch um ϱ_1 kleiner als n ist, so ist in (2.) für $m, 2m, 3m, \dots, \nu_1 m$ nothwendig $\mu_1 = 0$. Also sind die *ersten* ν_1 Quotienten $\mu_1, \mu_2, \mu_3, \dots, \mu_{\nu_1}$ sämmtlich Null.

Das nächstfolgende Vielfache $(\nu_1 + 1)m$ von m ist schon $> n$; denn, noch einmal m zu der ersten Gleichung (3.) gethan, würde einen Rest $\varrho_1 + m$ geben, der $> m$ wäre; was nicht sein soll. Also ist der Quotient μ_{ν_1+1} in (2.) der *erste* derjenigen, welche *nicht Null*, sondern 1 sind. Aber $\nu_2 m$ ist nach der 2ten Gleichung in (3.) noch um ϱ_2 kleiner als $2n$. Also sind in (2.) auch alle folgenden Vielfachen $(\nu_1 + 2)m, (\nu_1 + 3)m, (\nu_1 + 4)m$ etc., von m bis zu $\nu_2 m$, noch kleiner als $2n$, und folglich sind alle die $\nu_2 - \nu_1$ Quotienten $\mu_{\nu_1+1}, \mu_{\nu_1+2}, \mu_{\nu_1+3}, \dots, \mu_{\nu_2}$ in (2.) sämmtlich = 1.

Auf dieselbe Weise folgt, daß die sämmtlichen $\nu_3 - \nu_2$ Quotienten $\mu_{\nu_2+1}, \mu_{\nu_2+2}, \mu_{\nu_2+3}, \dots, \mu_{\nu_3}$ in (2.) = 2 sind, die sämmtlichen $\nu_4 - \nu_3$ Quo-

$$\frac{1}{2}mn[m(n+1)+n(m+1)] = m^2n^2 + mSr + nSq \text{ oder}$$

$$41. \quad mSr + nSq = \frac{1}{2}mn(m+n);$$

welches die Gleichung (13.) des Lehrsatzes ist.

F. Sind m und n zu einander *theilerfremd*, so sind nach (§. 34.) in (2.) die r die sämtlichen Zahlen

$$42. \quad 1, 2, 3, 4, \dots, n-1, n.$$

Denn nach (§. 34. I.) würden in (2.) den Factoren $0, 1, 2, 3, \dots, n-1$ von m die Reste $0, 1, 2, 3, 4, \dots, n-1$ zukommen, und zu dem Reste 0 gehört der Factor 0 (§. 34. I.). Dieser Factor 0 findet hier nicht Statt, also auch nicht der Rest 0 . Dagegen kommt hier der Factor n noch hinzu, und für diesen ist der Rest r zufolge (10.) $= n$. Also sind die r in (2.) nothwendig alle die Zahlen (42.).

Eben so sind die q in (3.) die sämtlichen Zahlen

$$43. \quad 0, 1, 2, 3, 4, \dots, m-1.$$

Denn den Factoren $1, 2, 3, \dots, m-1$ in (3.) kommen nach (§. 34. I.) die Reste $1, 2, 3, \dots, n-1$ zu, und der zu dem letzten Factor m in (3.) gehörige Rest q_m ist nach (10.) $= 0$, so daß also zusammen die q die Zahlen (43.) sind.

G. Aus (42. und 43.) folgt nun unmittelbar, daß die Summe der Reste r , nemlich $Sr = \frac{1}{2}(n+1)n$ und die Summe der Reste q , nemlich $Sq = \frac{1}{2}m(m-1)$ ist; wie es (14. u. 15.) behaupten.

H. Setzt man (14. u. 15.) in die Gleichungen (38. u. 39.), welche hier in dem besonderen Fall ebenfalls stattfinden, da sie für *jedes* m und n allgemein gelten; so ergibt sich

$$44. \quad \frac{1}{2}(n+1)mn = nS\mu + \frac{1}{2}n(n+1) \text{ und}$$

$$45. \quad \frac{1}{2}(m+1)mn = mS\nu + \frac{1}{2}m(m+1)$$

oder

$$46. \quad \frac{1}{2}m(n+1) - \frac{1}{2}(n+1) = S\mu = \frac{1}{2}(n+1)(m-1) \text{ und}$$

$$47. \quad \frac{1}{2}n(m+1) - \frac{1}{2}(m+1) = S\nu = \frac{1}{2}((n-1)m + n+1);$$

welches die Gleichungen (16. u. 17.) des Lehrsatzes sind.

J. Aus (16, 17. u. 11.) ergibt sich

$$48. \quad S\mu - \mu_n = \frac{1}{2}(n+1)(m-1) - (m-1) = \frac{1}{2}(n-1)(m-1) \text{ und}$$

$$49. \quad S\nu - \nu_m = \frac{1}{2}(n-1)m + \frac{1}{2}(n+1) - n = \frac{1}{2}(n-1)(m-1);$$

wie es der Lehrsatz in (18.) behauptet.

K. Anm. Der Beweis erhält seine Entwicklung besonders durch die Summirung der Gleichungen (34. in **B.**), die ihrerseits aus einfachen Be-

trachtungen hervorgehen. In (E.) wird der bekannte Ausdruck der Summe einer sogenannten arithmetischen Reihe zu Hülfe genommen.

§. 38.

Lehrsatz.

Es seien m und n zwei beliebige positive ganze Zahlen und es sei

$$1. \quad n > m.$$

Man setze

$$2. \quad \left\{ \begin{array}{l} m = \mu_1 n + r_1, \\ 2m = \mu_2 n + r_2, \\ 3m = \mu_3 n + r_3, \\ \dots \dots \dots \\ \frac{1}{2}(n-1)m = \mu_{\frac{1}{2}(n-1)} n + r_{\frac{1}{2}(n-1)}, \\ \text{wenn } n \text{ ungerade und} \\ \frac{1}{2}nm = \mu_{\frac{1}{2}n} n + r_{\frac{1}{2}n}, \\ \text{wenn } n \text{ gerade ist,} \end{array} \right. \quad \text{und} \quad 3. \quad \left\{ \begin{array}{l} n = \nu_1 m + \varrho_1, \\ 2n = \nu_2 m + \varrho_2, \\ 3n = \nu_3 m + \varrho_3, \\ \dots \dots \dots \\ \frac{1}{2}(m-1)n = \nu_{\frac{1}{2}(m-1)} m + \varrho_{\frac{1}{2}(m-1)}, \\ \text{wenn } m \text{ ungerade und} \\ \frac{1}{2}mn = \nu_{\frac{1}{2}m} m + \varrho_{\frac{1}{2}m}, \\ \text{wenn } m \text{ gerade ist,} \end{array} \right.$$

unter der Bedingung, daß die sämtlichen r und q positiv sind und daß

4. *die r aus den Zahlen 1, 2, 3, 4, n und*

5. *die q aus den Zahlen 0, 1, 2, 3, m-1*

genommen werden. Ferner bezeichne man die Summe der sämtlichen Quotienten μ , nemlich

$$6. \quad \mu_1 + \mu_2 + \mu_3 \dots + \mu_{\frac{1}{2}(n-1)} \quad \text{oder} \quad \mu_{\frac{1}{2}n} \quad \text{durch } S\mu,$$

und die Summe der sämtlichen Quotienten ν , nemlich

$$7. \quad \nu_1 + \nu_2 + \nu_3 \dots + \nu_{\frac{1}{2}(m-1)} \quad \text{oder} \quad \nu_{\frac{1}{2}m} \quad \text{durch } S\nu.$$

Alsdann ist

$$\begin{array}{ll} 8. \quad \left\{ \begin{array}{l} 1. \quad S\mu + S\nu = \frac{1}{4}(m-1)(n-1), \\ 2. \quad \mu_{\frac{1}{2}(n-1)} = \frac{1}{2}(m-1) \quad \text{und} \quad r_{\frac{1}{2}(n-1)} = \frac{1}{2}(n-m); \end{array} \right\} & \left. \begin{array}{l} \text{wenn } m \text{ ungerade} \\ \text{und } n \text{ ungerade ist;} \end{array} \right\} \\ 9. \quad \left\{ \begin{array}{l} 1. \quad S\mu + S\nu = \frac{1}{4}(m-1)n, \\ 2. \quad \mu_{\frac{1}{2}(n-1)} = \frac{1}{2}(m-1) \quad \text{und} \quad r_{\frac{1}{2}n} = \frac{1}{2}n; \end{array} \right\} & \left. \begin{array}{l} \text{wenn } m \text{ ungerade} \\ \text{und } n \text{ gerade ist;} \end{array} \right\} \\ 10. \quad \left\{ \begin{array}{l} 1. \quad S\mu + S\nu = \frac{1}{4}m(n-1), \\ 2. \quad \left\{ \begin{array}{l} \mu_{\frac{1}{2}(n-1)} = \frac{1}{2}m-1 \quad \text{und} \quad r_{\frac{1}{2}(n-1)} = n - \frac{1}{2}m, \\ \nu_{\frac{1}{2}m} = \frac{1}{2}(n-1) \quad \text{und} \quad \varrho_{\frac{1}{2}m} = \frac{1}{2}m; \end{array} \right. \end{array} \right\} & \left. \begin{array}{l} \text{wenn } m \text{ gerade} \\ \text{und } n \text{ ungerade ist;} \end{array} \right\} \\ 11. \quad \left\{ \begin{array}{l} 1. \quad S\mu + S\nu = \frac{1}{4}mn, \\ 2. \quad \left\{ \begin{array}{l} \mu_{\frac{1}{2}n} = \frac{1}{2}m-1 \quad \text{und} \quad r_{\frac{1}{2}n} = n, \\ \nu_{\frac{1}{2}m} = \frac{1}{2}n \quad \text{und} \quad \varrho_{\frac{1}{2}m} = 0, \end{array} \right. \end{array} \right\} & \left. \begin{array}{l} \text{wenn } m \text{ gerade} \\ \text{und } n \text{ gerade ist.} \end{array} \right\} \end{array}$$

Beispiel 1. für (8.). Es sei

$$12. \quad m = 7, \quad n = 35,$$

so geben (2. u. 3.)

$$13. \quad \left\{ \begin{array}{l} 1, 2, 3, 4, 5m=0n+7, 14, 21, 28, 35, \\ 6, 7, 8, 9, 10m=1n+7, 14, 21, 28, 35, \\ 11, 12, 13, 14, 15m=2n+7, 14, 21, 28, 35, \\ 16, 17m=3n+7, 14; \end{array} \right. \text{ und } 14. \quad \left\{ \begin{array}{l} 1.35 = 5.7+0, \\ 2.35 = 10.7+0, \\ 3.35 = 15.7+0; \end{array} \right.$$

und die Summe sämtlicher Quotienten ist

$$14. \quad S\mu + S\nu = 5.0 + 5.1 + 5.2 + 2.3 + 5 + 10 + 15 = 51 = \frac{1}{4}(7-1)(35-1) \\ = \frac{6 \cdot 34}{4}; \text{ gemäß (8. 1.).}$$

Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 3 = \frac{1}{2}(m-1)$ und $r_{\frac{1}{2}(n-1)} = 14 = \frac{1}{2}(n-m)$; gemäß (8. 2.).

Beispiel 2. für (8.). Es sei

$$15. \quad m = 9, \quad n = 39,$$

so geben (2. u. 3.)

$$17. \quad \left\{ \begin{array}{l} 1, 2, 3, 4m=0n+9, 18, 27, 36, \\ 5, 6, 7, 8m=1n+6, 15, 24, 33, \\ 9, 10, 11, 12, 13m=2n+3, 12, 21, 30, 39, \\ 14, 15, 16, 17m=3n+9, 18, 27, 36, \\ 18, 19m=4n+6, 15; \end{array} \right. \quad 18. \quad \left\{ \begin{array}{l} 1.39 = 4.9+3, \\ 2.39 = 8.9+6, \\ 3.39 = 13.9+0, \\ 4.39 = 17.9+3; \end{array} \right.$$

also ist die Summe sämtlicher Quotienten hier

$$19. \quad S\mu + S\nu = 4.0 + 4.1 + 5.2 + 4.3 + 2.4 + 4 + 8 + 13 + 17 = 76 \\ = \frac{1}{4}(9-1)(39-1) = \frac{8 \cdot 38}{4}; \text{ gemäß (8. 1.).}$$

Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 4 = \frac{1}{2}(m-1)$ und $r_{\frac{1}{2}n} = 15 = \frac{1}{2}(n-m)$; gemäß (8. 2.).

Beispiel 3. für (9.). Es sei

$$20. \quad m = 21, \quad n = 24,$$

so ist

$$21. \left\{ \begin{array}{l} 1m = 0n + 21, \\ 2m = 1n + 18, \\ 3m = 2n + 15, \\ 4m = 3n + 12, \\ 5m = 4n + 9, \\ 6m = 5n + 6, \\ 7m = 6n + 3, \\ 8m = 6n + 24, \\ 9m = 7n + 21, \\ 10m = 8n + 18, \\ 11m = 9n + 15, \\ 12m = 10n + 12, \end{array} \right. \quad \text{und} \quad 22. \left\{ \begin{array}{l} 1n = 1m + 3, \\ 2n = 2m + 6, \\ 3n = 3m + 9, \\ 4n = 4m + 12, \\ 5n = 5m + 15, \\ 6n = 6m + 18, \\ 7n = 8m + 0, \\ 8n = 9m + 3, \\ 9n = 10m + 6, \\ 10n = 11m + 9, \end{array} \right.$$

also ist hier

$$23. \quad S\mu + S\nu = 61 + 59 = 120 = \frac{1}{4}(21-1)24 = \frac{20 \cdot 24}{4}; \text{ gemäß (9. 1.)}$$

Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 10 = \frac{1}{2}(m-1)$, $r_{\frac{1}{2}(n-1)} = 12 = \frac{1}{2}n$; gemäß (9. 2.).

Beispiel 4. für (10.). Es sei

$$24. \quad m = 6, \quad n = 15,$$

so ist

$$25. \left\{ \begin{array}{l} 1, 2m = 0n + 6, 12, \\ 3, 4, 5m = 1n + 3, 9, 15, \\ 6, 7m = 2n + 6, 12, \end{array} \right. \quad \text{und} \quad 26. \left\{ \begin{array}{l} 1n = 2m + 3, \\ 2n = 5m + 0, \\ 3n = 7m + 3, \end{array} \right.$$

also ist hier

$$27. \quad S\mu + S\nu = 2 \cdot 0 + 3 \cdot 1 + 2 \cdot 2 + 2 + 5 + 7 = 21 = \frac{1}{4}6(15-1) = \frac{6 \cdot 14}{4};$$

gemäß (10. 1.). Desgleichen ist $\mu_{\frac{1}{2}(n-1)} = 2 = \frac{1}{2}m - 1$, $r_{\frac{1}{2}(n-1)} = 12 = n - \frac{1}{2}m$, $\nu_{\frac{1}{2}m} = 7 = \frac{1}{2}(n-1)$, $\varrho_{\frac{1}{2}m} = 3 = \frac{1}{2}m$; gemäß (10. 2.).

Beispiel 5. für (11.). Es sei

$$28. \quad m = 8, \quad n = 34,$$

so ist

$$29. \left\{ \begin{array}{l} 1, 2, 3, 4m = 0n + 8, 16, 24, 32, \\ 5, 6, 7, 8m = 1n + 6, 14, 22, 30, \\ 9, 10, 11, 12m = 2n + 4, 12, 20, 28, \\ 13, 14, 15, 16, 17m = 3n + 2, 10, 18, 26, 34; \end{array} \right. \quad \text{und} \quad 30. \left\{ \begin{array}{l} 1n = 4m + 2, \\ 2n = 8m + 4, \\ 3n = 12m + 6, \\ 4n = 17m + 0, \end{array} \right.$$

also ist hier

$$31. \quad S\mu + S\nu = 4 \cdot 0 + 4 \cdot 1 + 4 \cdot 2 + 5 \cdot 3 + 4 + 8 + 12 + 17 = 68 = \frac{1}{4}8 \cdot 34;$$

gemäß (11. 1.). Desgleichen ist $\mu_{\frac{1}{2}n} = 3 = \frac{1}{2}m - 1$, $r_{\frac{1}{2}n} = 34 = n$, $\nu_{\frac{1}{2}m} = 17 = \frac{1}{2}n$ und $\varrho_{\frac{1}{2}m} = 0$; gemäß (11. 2.).

Beispiel 1. Es sei

$$7. \quad u = 4n - 1 = 11, \quad \text{also } n = 3, \quad \frac{1}{2}(u-1) = 5, \quad v = 15.$$

Alsdann giebt (2.)

$$8. \quad \begin{cases} v = 1u + 4, \\ 2v = 2u + 8, \\ 3v = 3u + 12, \\ 4v = 5u + 5, \\ 5v = 6u + 9; \end{cases}$$

also ist in (5.)

$$9. \quad s = 3 \cdot 14 + 1 + 2 + 3 + 5 + 6 = 59.$$

Die 3 Reste 8, 12 und 9 sind $> \frac{1}{2}u (= 5\frac{1}{2})$, also ist

$$10. \quad z = 3,$$

und s und z sind, gemäß (5.), beide *zugleich ungerade*.

Desgleichen sind gemäß (6.) hier, wo auch v *ungerade* ist, $z = 3$ und $S\mu = 1 + 2 + 3 + 5 + 6 = 17$ *beide zugleich ungerade*.

Beispiel 2. Es sei

$$11. \quad u = 4n + 1 = 13, \quad \text{also } n = 3, \quad \frac{1}{2}(u-1) = 6; \quad v = 18.$$

Alsdann giebt (2.)

$$12. \quad \begin{cases} v = 1u + 5, \\ 2v = 2u + 10, \\ 3v = 3u + 15, \\ 4v = 5u + 7, \\ 5v = 6u + 12, \\ 6v = 8u + 4; \end{cases}$$

also ist in (5.)

$$13. \quad s = 3 \cdot 17 + 1 + 2 + 3 + 5 + 6 + 8 = 76.$$

Die 4 Reste 10, 15, 7 und 12 sind $> \frac{1}{2}u (= 6\frac{1}{2})$, also ist

$$14. \quad z = 4;$$

und s und z sind, gemäß (5.), beide *zugleich gerade*.

Beweis A. Es sei für ein beliebiges ε fache von v :

$$15. \quad \varepsilon v = \mu_\varepsilon u + r_\varepsilon,$$

welche Gleichung, wenn man darin $\varepsilon = 1, 2, 3, \dots, \frac{1}{2}(u-1)$ setzt, die Gleichungen (2.) giebt. Die Gleichung (15.), mit 2 multiplicirt, giebt

$$16. \quad 2\varepsilon v = 2\mu_\varepsilon u + 2r_\varepsilon.$$

Setzt man nun in (16.) der Reihe nach $\varepsilon = 1, 2, 3, \dots, \frac{1}{2}(u-1)$ und in (15.) der Reihe nach $\varepsilon = 2, 4, 6, 8, \dots, u-1$, so erhält man folgende *zwiefachen* Ausdrücke von $2v, 4v, 6v, \dots, (u-1)v$, nemlich:

$$17. \quad \left\{ \begin{array}{l} 2v = 2\mu_1 u + 2r_1 = \mu_2 u + r_2, \\ 4v = 2\mu_2 u + 2r_2 = \mu_4 u + r_4, \\ 6v = 2\mu_3 u + 2r_3 = \mu_6 u + r_6, \\ 8v = 2\mu_4 u + 2r_4 = \mu_8 u + r_8, \\ . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ (u-1)v = 2\mu_{\frac{1}{2}(u-1)} u + 2r_{\frac{1}{2}(u-1)} = \mu_{u-1} u + r_{u-1}. \end{array} \right.$$

In den ersten dieser Ausdrücke von $2v, 4v, 6v, \dots (v-1)$ kommen alle die Reste $r_1, r_2, r_3, \dots r_{\frac{1}{2}(v-1)}$ vor, die sich in (2.) finden, und der *allgemeine* Ausdruck der Gleichungen (17.) ist

$$18. \quad 2\varepsilon v = 2\mu_\varepsilon u + 2r_\varepsilon = \mu_{2\varepsilon} u + r_{2\varepsilon};$$

wo $\varepsilon = 1, 2, 3, \dots, \frac{1}{2}(u-1)$ sein kann.

B. a. Ist in (18.) $r_\epsilon < \frac{1}{2}u$, so ist $2r_\epsilon < u$ und zugleich > 0 . Eben das ist $r_{2\epsilon}$, und es giebt nur einen positiven Rest > 0 und $< u$ für ein bestimmtes ϵ ; also ist nothwendig $r_{2\epsilon} = 2r_\epsilon$, und folglich auch

19. $2\mu_\varepsilon = \mu_{2\varepsilon}$, wenn $r_\varepsilon < \frac{1}{2}u$.

b. Ist hingegen in (18.) $r_\epsilon > \frac{1}{2}u$, so ist $2r_\epsilon > u$; also müßte der Quotient $2\mu_\epsilon$ um 1 *größer* genommen werden, wenn $2r_\epsilon = r_{2\epsilon}$ sein sollte. Mithin ist nothwendig

20. $2\mu_\varepsilon = \mu_{2\varepsilon} - 1$, wenn $r_\varepsilon > \frac{1}{2}u$.

c. Gleich $\frac{1}{2}u$ kann r nicht sein, weil nach der Voraussetzung u *ungerade* sein soll. Es kommen also in (17.) *nur* Reste $r < \frac{1}{2}u$ oder $r > \frac{1}{2}u$ vor.

C. Nun kommen in (17.), wie schon bemerkt, *alle* die Reste $r_1, r_2, r_3, \dots, r_{\frac{1}{2}(u-1)}$ vor, und z derselben sind nach der Voraussetzung $> \frac{1}{2}u$: also ist in jeder von z **Gleichungen** (17.) nach (B. b.) der Quotient μ *links* um **1 gröfser** als der Quotient μ *rechts*; in den *übrigen* $\frac{1}{2}(u-1) - z$ Gleichungen dagegen sind nach (B. a.) die Quotienten μ links und rechts einander *gleich*.

Nimmt man also links und rechts die *Summe* aller Quotienten μ , so ergibt sich

$$21. \quad 2\mu_1 + 2\mu_2 + 2\mu_3 + \dots + 2\mu_{i(u-1)} = \mu_2 + \mu_4 + \mu_6 + \dots + \mu_{u-1} - z,$$

oder, wenn man

22. $\mu_2 + \mu_4 + \mu_6 \dots + \mu_{u-1}$ durch $S_2\mu$

bezeichnet,

23. $z = S_2\mu - 2S_\mu$ (4.).

$$33. \left\{ \begin{array}{l} \text{für } u = 4n+1 \text{ ist } u-2n+1 = 2n+1, \text{ also folgt } \mu_{u-2n+1} = \mu_{2n+1} \\ \quad \text{in (31.) unmittelbar auf } u_{2n}, \text{ und} \\ \text{für } u = 4n+1 \text{ ist } u-2n+1 = 2n, \text{ also folgt } \mu_{u-2n+1} = \mu_{2n} \\ \quad \text{in (32.) unmittelbar auf } u_{2n-2}. \end{array} \right.$$

Setzt man nun in (31. u. 32.) für die *untere* Zeile ihre Werthe aus (30.), so ergibt sich

$$34. \quad S_2\mu = \mu_2 + \mu_4 + \mu_6 + \dots + \mu_{2n} + n(v-1) - (\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1})$$

für $u = 4n+1$ und

$$35. \quad S_2\mu = \mu_2 + \mu_4 + \mu_6 + \dots + \mu_{2n-2} + n(v-1) - (\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1})$$

für $u = 4n-1$.

G. Addirt man in (34. u. 35.) auf beiden Seiten noch

$$2(\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1}),$$

so ergibt sich

$$36. \quad S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1}) = \mu_2 + \mu_4 + \mu_6 + \dots + \mu_{2n} + n(v-1) \\ + \mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1} \\ = \mu_1 + \mu_2 + \mu_3 + \mu_4 + \dots + \mu_{2n} + n(v-1)$$

für $u = 4n+1$ und

$$37. \quad S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1}) = \mu_2 + \mu_4 + \mu_6 + \dots + \mu_{2n-2} + n(v-1) \\ + \mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-3} + \mu_{2n-1} \\ = \mu_1 + \mu_2 + \mu_3 + \mu_4 + \dots + \mu_{2n-1} + n(v-1)$$

für $u = 4n-1$.

Es ist aber in (36.) das letzte μ_{2n} rechts $= \mu_{\frac{1}{2}(u-1)}$, da $2n = \frac{1}{2}(u-1)$ ist für $u = 4n+1$, und in (37.) ist das letzte μ_{2n-1} rechts *ebenfalls* $= \mu_{\frac{1}{2}(u-1)}$, da $2n-1 = \frac{1}{2}(u-1)$ ist für $u = 4n-1$. Also geben (36. u. 37.) gleichmäfsig *Dasselbe*, nemlich

$$S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1}) = \mu_1 + \mu_2 + \mu_3 + \mu_4 + \dots + \mu_{\frac{1}{2}(u-1)} + n(v-1)$$

oder

$$38. \quad S_2\mu + 2(\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1}) = S\mu + n(v-1) \quad (4.).$$

Die hier zu $S_2\mu$ links addirte Zahl $2(\mu_1 + \mu_3 + \mu_5 + \dots + \mu_{2n-1})$, welche sie auch sein mag, ist aber *immer gerade*: also ist $S_2\mu$ *gerade* oder *ungerade*, je nachdem es $S\mu + n(v-1)$ ist. Nun war x *gerade* oder *ungerade*, je nachdem es $S_2\mu$ ist (C.): also ist x *gerade* oder *ungerade*, je nachdem es $S\mu + n(v-1)$ ist.

Dieses ist was der Lehrsatz in (5.) behauptet.

H. Ist auch v *ungerade*, gleichwie u , so ist $v-1$ *gerade*, also auch $n(v-1)$ *gerade*. Also ist x *gerade* oder *ungerade*, je nachdem es blofs $S\mu$ ist; gemäß (6.).

I. Anm. Der Beweis des Satzes entwickelt sich insbesondere aus den *zwiefachen* Ausdrücken (17.) der *geraden* Vielfachen $2v, 4v, 6v, \dots$ von v .

§. 40.

Lehrsatz.

Wenn p eine beliebige Stammzahl ist, so bleibt, wenn man die $p-1$ te Potenz jeder beliebigen positiven oder negativen Zahl z , die nicht mit p aufgeht, durch p dividirt, immer der Rest $+1$: das heisst, die Gleichung

$$1. \quad z^{p-1} \equiv \mathfrak{G}p + 1$$

findet für jede Stammzahl p und für jeden beliebigen positiven oder negativen Werth von z Statt, der nicht mit p aufgeht. Jedoch findet sie nicht nothwendig Statt, wenn p nicht eine Stammzahl ist, sondern Factoren >1 hat.

Diesen Satz nennt man gewöhnlich, nach seinem Erfinder, den Fermatschen Satz.

Auch ist immer

$$2. \quad z^{p-1} \equiv \mathfrak{G}(z^\delta - 1)p + 1,$$

wo δ einen beliebigen Theiler von $p-1$ bezeichnet.

Beispiele. 1. Es sei

$$3. \quad p = 13.$$

Ist hier z. B. $z = 11$, so ist $z^2 = 121 = \mathfrak{G}13 + 4$, $z^4 = \mathfrak{G}13 + 16 = \mathfrak{G}13 + 3$, $z^8 = \mathfrak{G}13 + 9$, $z^{12} = z^{p-1} = z^4 \cdot z^8 = (\mathfrak{G}13 + 3)(\mathfrak{G}13 + 9) = \mathfrak{G}13 + 27 = \mathfrak{G}13 + 1$; gemäß (1.).

Ist $z = 2$, so ist $z^3 = 8$, $z^6 = 64 = \mathfrak{G}p - 1$, $z^{12} = z^{p-1} = \mathfrak{G}p + 1$; ebenfalls gemäß (1.); und so giebt *jedes* andere, nicht durch p theilbare z , $z^{p-1} = \mathfrak{G}p + 1$. Ist $z > p$, so ist es so viel als $z = \mathfrak{G}p + z_1$, wo nun $z_1 < p$. Ist z *negativ*, so hat z^{p-1} gleichwohl denselben Rest $+1$, indem der Exponent $p-1$ von z für $p = 13$ und für jede andere *ungerade* Stammzahl *gerade* ist.

2. Es sei

$$4. \quad p = 2,$$

so ist $p-1 = 1$ und also $z^{p-1} = z$ selbst. Alle mit $p = 2$ nicht aufgehenden Zahlen, das heisst alle *ungeraden* positiven und negativen Zahlen lassen aber, durch 2 dividirt, offenbar den Rest $+1$. Z. B.: -15 ist gleich $-8 \cdot 2 + 1$. Also auch für die einzige *gerade* Stammzahl $p = 2$ findet der Satz Statt.

Beweis *A.* Es kann immer

$$5. \quad m\alpha = \mathfrak{G}p + r,$$

gesetzt werden, wo, wenn m eine beliebige ganze Zahl bedeutet,

$$6. \quad r \text{ eine der Zahlen } 1, 2, 3, 4, \dots, p-1$$

ist, aber nicht 0 sein kann, weil α nicht mit p aufgehen soll.

B. Giebt man nun dem beliebigen m der Reihe nach die Werthe $1, 2, 3, 4, \dots, p-1$, so durchläuft nach (§. 34. I.) auch r alle die Werthe $1, 2, 3, 4, \dots, p-1$, obwohl in verschiedener Ordnung. Es ergeben sich also die $p-1$ Gleichungen

$$7. \quad \begin{cases} 1\alpha = \mathfrak{G}p + r_1, \\ 2\alpha = \mathfrak{G}p + r_2, \\ 3\alpha = \mathfrak{G}p + r_3, \\ \dots\dots\dots \\ (p-1)\alpha = \mathfrak{G}p + r_{p-1}; \end{cases}$$

wo die r nun nothwendig alle die Zahlen $1, 2, 3, 4, \dots, p-1$ sind.

C. Multiplicirt man diese $p-1$ Gleichungen in einander, so ergibt sich

$$8. \quad 1.2.3.4 \dots (p-1). \alpha^{p-1} = \mathfrak{G}p + r_1 r_2 r_3 r_4 \dots r_{p-1},$$

und hieraus

$$9. \quad 1.2.3.4 \dots (p-1). \alpha^{p-1} = \mathfrak{G}p + 1.2.3.4 \dots (p-1).$$

D. Aus (9.) folgt

$$10. \quad 1.2.3.4 \dots (p-1) (\alpha^{p-1} - 1) = \mathfrak{G}p.$$

Hier geht die Stammzahl p in *keinen* der Factoren $1, 2, 3, 4, \dots, p-1$ auf; denn alle sind $< p$. Also geht p auch in dem Producte $1.2.3.4 \dots p-1$ nicht auf (§. 22.). Da nun aber nach (8.) p nothwendig in die gesammte Gröfse $1.2.3.4 \dots (p-1) (\alpha^{p-1} - 1)$ aufgehen *mufs*, so mufs es in den noch übrigen Factor $\alpha^{p-1} - 1$ aufgehen (§. 25.) und also

$$11. \quad \alpha^{p-1} - 1 = \mathfrak{G}p$$

sein; woraus die Gleichung (1.) des Lehrsatzes folgt.

E. Alles Vorige bleibt dasselbe, wie grofs oder klein auch die Zahl α sein und ob sie positiv oder negativ sein mag, wenn sie nur nicht mit p aufgeht. Aber in diesem, und nur in diesem einzigen Falle von α findet das Bewiesene *nicht* Statt, indem dann r nicht eine der Zahlen (5.), sondern für *jedes* m gleich *Null* ist. Mithin gilt die Gleichung (1.) für jeden beliebigen positiven oder negativen ganzzahligen Werth von α , der *nicht* mit p aufgeht.

F. Ist p *nicht* eine Stammzahl, so findet zwar noch für jedes zu p theilerfremde α zufolge (§. 34.) Alles Statt, was oben (*A.*, *B.*, *C.*) behaupten,

denn auch dann noch sind die r nothwendig alle die Zahlen 1, 2, 3, 4, $p-1$ (§. 34. I.), aber aus der Gleichung (10.) folgt nun nicht mehr, dafs nothwendig $x^{p-1}-1$ mit p aufgehen mufs, weil schon einzelne Factoren von p in 1, 2, 3, 4 $p-1$ aufgehen können.

G. Nach (1.) ist $x^{p-1}-1 = \mathfrak{G}p$. Aber $x^{p-1}-1$ geht für jedes x und $p-1$ mit $x^\delta-1$ auf, wenn δ in $p-1$ aufgeht, und giebt $x^{p-1-\delta} + x^{p-1-2\delta} + x^{p-1-3\delta} \dots + 1$ zum Quotienten. Also mufs auch $\mathfrak{G}p$ mit $x^\delta-1$ aufgehen. Aber die Stammzahl p geht *nicht* mit $x^\delta-1$ auf, also mufs $\mathfrak{G}$ mit $x^\delta-1$ aufgehen und folglich

$$12. \quad x^{p-1}-1 = \mathfrak{G}(x^\delta-1)p$$

sein; woraus die Gleichung (2.) folgt.

Anm. H. Der Beweis beruht insbesondere auf dem Umstande, dafs in (7.) die r nach (§. 34.) nothwendig alle die Zahlen 1, 2, 3, $p-1$ selbst sind.

Der *Fermatsche* Lehrsatz findet in der gesammten Theorie der Zahlen vielfache Anwendungen und ist also als einer der Hauptsätze derselben zu betrachten. Wie er sich ändert, wenn p *nicht* eine Stammzahl ist, wird weiter unten vorkommen

§. 41.

Lehrsatz.

Es sei p eine beliebige Stammzahl > 2 , z eine beliebige ganze Zahl, die nicht mit p aufgeht.

Man setze

$$1. \quad \left\{ \begin{array}{l} z = \mathfrak{G}p + r_1, \\ 2z = \mathfrak{G}p + r_2, \\ 3z = \mathfrak{G}p + r_3, \\ 4z = \mathfrak{G}p + r_4, \\ \dots \dots \dots \\ \frac{1}{2}(p-1)z = \mathfrak{G}p + r_{\frac{1}{2}(p-1)}, \end{array} \right.$$

und bezeichne

2. *die Anzahl der Reste r in (1.), welche $> \frac{1}{2}p$ sind, durch z .*

Alsdann ist

$$3. \quad z^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1, \text{ wenn } z \text{ gerade, und}$$

$$4. \quad z^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1, \text{ wenn } z \text{ ungerade ist.}$$

Das Eine und das Andere findet jedoch nothwendig nur dann Statt, wenn p eine Stammzahl ist; nicht nothwendig, wenn p Theiler > 1 hat.

Beispiel 1. Es sei

$$5. \quad p = 13, \quad z = 20,$$

so giebt (1.)

$$6. \quad 1, 2, 3, 4, 5, 6, z = \mathfrak{G}p + 7, 1, 8, 2, 9 \text{ und } 3.$$

Die 3 Reste 7, 8 und 9 sind $> \frac{1}{2}p$, also ist $z = 3$ und *ungerade*. $z^{\frac{1}{2}(p-1)}$ ist $20^6 = \mathfrak{G}p + 7^6 = \mathfrak{G}p + 49^3 = \mathfrak{G}p - 3^3 = \mathfrak{G}p - 27 = \mathfrak{G}p - 1$; wie es nach (4.) sein soll.

Beispiel 2. Es sei

$$7. \quad p = 19, \quad z = 42,$$

so giebt (1.)

$$8. \quad 1, 2, 3, 4, 5, 6, 7, 8, 9, z = \mathfrak{G}p + 4, 8, 12, 16, 1, 5, 9, 13 \text{ und } 17.$$

Die 4 Reste 12, 16, 13 und 17 sind $> \frac{1}{2}p$, also ist $z = 4$ und *gerade*. $z^{\frac{1}{2}(p-1)}$ ist $42^9 = \mathfrak{G}p + 4^9 = \mathfrak{G}p + 64^3 = \mathfrak{G}p + 7^3 = \mathfrak{G}p + 343 = \mathfrak{G}p + 1$; gemäß (4.).

Beweis. **A.** Man bezeichne diejenigen $\frac{1}{2}(p-1) - z$ Multiplicatoren von z in (1.), welche Reste $r < \frac{1}{2}p$ geben, durch m , die übrigen z Multiplicatoren, welche Reste $> \frac{1}{2}p$ geben, durch μ . Für die letzteren Vielfachen von z nehme man die Quotienten *um 1 größer*, also statt der *positiven* echten Reste r die *negativen echten* Reste, welche nun durch ϱ bezeichnet werden mögen, so daß also die Gleichungen (1.) zusammen folgende sind:

$$9. \quad \begin{cases} m_1 z = \mathfrak{G}p + r_1, \\ m_2 z = \mathfrak{G}p + r_2, \\ m_3 z = \mathfrak{G}p + r_3, \\ \dots \dots \dots \\ m_{\frac{1}{2}(p-1)-z} z = \mathfrak{G}p + r_{\frac{1}{2}(p-1)-z}; \end{cases} \quad 10. \quad \begin{cases} \mu_1 z = \mathfrak{G}p - \varrho_1, \\ \mu_2 z = \mathfrak{G}p - \varrho_2, \\ \mu_3 z = \mathfrak{G}p - \varrho_3, \\ \dots \dots \dots \\ \mu_x z = \mathfrak{G}p - \varrho_x. \end{cases}$$

Alsdann sind zufolge (§. 35. 9.), da die Stammzahl p ungerade sein soll und zu jedem z theilerfremd ist, die r und ϱ in (9. u. 10.) *zusammengenommen alle die Zahlen*

$$11. \quad 1, 2, 3, 4, \dots, \frac{1}{2}(p-1),$$

und z derselben sind *negativ*; während die m und μ *ebenfalls* alle die Zahlen (11.) sind.

B. Multiplicirt man also alle die $\frac{1}{2}(p-1)$ Gleichungen (9. u. 10.) in einander, so ergiebt sich

$$12. \quad 1.2.3.4 \dots \frac{1}{2}(p-1) z^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1.2.3.4 \dots \frac{1}{2}(p-1) (-1)^x,$$

und daraus folgt

$$13. \quad 1.2.3.4 \dots \frac{1}{2}(p-1) (z^{\frac{1}{2}(p-1)} - (-1)^x) = \mathfrak{G}p.$$

Zufolge dieser Gleichung muß das Product linkerhand mit p aufgehoben. Es geht aber keiner der Factoren $1, 2, 3, 4, \dots \frac{1}{2}(p-1)$ des Productes mit p auf, weil alle $< p$ sind, also muß der *letzte* Factor

$$14. \quad z^{\frac{1}{2}(p-1)} - (-1)^x = \mathfrak{G}p$$

sein (§. 25.), und daraus folgt

$$15. \quad z^{\frac{1}{2}(p-1)} = \mathfrak{G}p + (-1)^x;$$

welches für ein *gerades* z die Gleichung (3.) und für ein *ungerades* z die Gleichung (4.) des Lehrsatzes giebt.

C. Hätte p Factoren > 1 , so müßte wenigstens einer derselben $< \frac{1}{2}p$ sein, denn, alle $> \frac{1}{2}p$, würden eine Zahl $> p$ geben. Also geht dann in (13.) wenigstens ein Factor von p schon in $1.2.3.4 \dots \frac{1}{2}(p-1)$ auf, und die Gleichung (14.) folgt nicht mehr aus (13.). Der Lehrsatz gilt also nur *nothwendig*, wenn p eine *Stammzahl* ist.

Anm. **D.** Der Beweis beruht insbesondere auf dem Satze (§. 35.).

§. 42.

Lehrsatz.

Es seien p und q zwei beliebige Stammzahlen > 2 , die also immer durch

$$1. \quad p = 4n \pm 1 \quad \text{und} \quad q = 4m \pm 1$$

ausgedrückt werden können (§. 28. IV.).

Man setze

$$2. \quad \left\{ \begin{array}{l} q = \mu_1 p + r_1, \\ 2q = \mu_2 p + r_2, \\ 3q = \mu_3 p + r_3, \\ \dots \dots \dots \\ \frac{1}{2}(p-1)q = \mu_{\frac{1}{2}(p-1)} p + r_{\frac{1}{2}(p-1)}; \end{array} \right. \quad \text{und} \quad 3. \quad \left\{ \begin{array}{l} p = \nu_1 q + \varrho_1, \\ 2p = \nu_2 q + \varrho_2, \\ 3p = \nu_3 q + \varrho_3, \\ \dots \dots \dots \\ \frac{1}{2}(q-1)p = \nu_{\frac{1}{2}(q-1)} q + r_{\frac{1}{2}(q-1)}; \end{array} \right.$$

und

$$4. \quad \mu_1 + \mu_2 + \mu_3 \dots + \mu_{\frac{1}{2}(p-1)} = S\mu,$$

$$5. \quad \nu_1 + \nu_2 + \nu_3 \dots + \nu_{\frac{1}{2}(q-1)} = S\nu.$$

Desgleichen bezeichne man

6. *die Anzahl der $r > \frac{1}{2}p$ in (2.) durch k und*

7. *die Anzahl der $\varrho > \frac{1}{2}q$ in (3.) durch z .*

Alsdann findet folgendes Gesetz Statt:

Erstlich. Sind nicht p und q beide von der Form $4n-1$ oder $4m-1$, und ist also

$$8. \quad \begin{cases} 1. \text{ entweder } p = 4n + 1, & q = 4m + 1, \\ 2. \text{ oder } & p = 4n + 1, & q = 4m - 1, \\ 3. \text{ oder } & p = 4n - 1, & q = 4m + 1, \end{cases}$$

so ist

$$9. \quad \begin{cases} 1. \text{ zugleich } q^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1 \text{ und } p^{\frac{1}{2}(q-1)} = \mathfrak{G}q + 1, \text{ und zwar wenn } S_{\mu} \\ \text{oder wenn } k \text{ gerade, worauf zugleich } S_{\nu} \text{ oder } z \text{ gerade ist;} \\ 2. \text{ zugleich } q^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1 \text{ und } p^{\frac{1}{2}(q-1)} = \mathfrak{G}q - 1, \text{ und zwar wenn } S_{\mu} \\ \text{oder wenn } k \text{ ungerade, worauf zugleich } S_{\nu} \text{ oder } z \text{ ungerade ist.} \end{cases}$$

Zweitens. Sind p und q beide von der Form $4n - 1$ oder $4m - 1$, und ist also

$$10. \quad p = 4n - 1, \quad q = 4m - 1,$$

so ist

$$11. \quad \begin{cases} 1. \text{ zugleich } q^{\frac{1}{2}(p-1)} = \mathfrak{G}p + 1 \text{ und } p^{\frac{1}{2}(q-1)} = \mathfrak{G}q - 1, \text{ und zwar wenn } S_{\mu} \\ \text{oder wenn } k \text{ gerade, worauf zugleich } S_{\nu} \text{ oder } z \text{ ungerade ist;} \\ 2. \text{ zugleich } q^{\frac{1}{2}(p-1)} = \mathfrak{G}p - 1 \text{ und } p^{\frac{1}{2}(q-1)} = \mathfrak{G}q + 1, \text{ und zwar wenn } S_{\mu} \\ \text{oder wenn } k \text{ ungerade, worauf zugleich } S_{\nu} \text{ oder } z \text{ gerade ist.} \end{cases}$$

Dieses Gesetz wird *Reciprocitätsgesetz für Stammzahlen* genannt. Auf Deutsch wird es also *Gegenseitigkeitsgesetz für Stammzahlen* heißen müssen. Das Gesetz findet nur für Stammzahlen, nicht nothwendig für andere Zahlen Statt, welche Theiler > 1 mit einander gemein haben.

Man bezeichnet auch,

$$12. \quad \text{dafs z. B. } p^{\frac{1}{2}(q-1)} = \mathfrak{G}q \pm 1 \text{ sei, durch } \left(\frac{p}{q}\right) = \pm 1.$$

Nach dieser Bezeichnung ist zufolge (9. u. 11.)

$$13. \quad \left(\frac{p}{q}\right) = + \left(\frac{q}{p}\right), \text{ wenn } p \text{ und } q \text{ nicht beide von der Form } 4n - 1 \\ \text{oder } 4m - 1 \text{ sind, und}$$

$$14. \quad \left(\frac{p}{q}\right) = - \left(\frac{q}{p}\right), \text{ wenn } p \text{ und } q \text{ beide von der Form } 4n - 1 \\ \text{oder } 4m - 1 \text{ sind.}$$

Beispiel 1. Es sei

$$15. \quad p = 13, \quad q = 17, \quad \text{also } p = 4n + 1, \quad q = 4m + 1,$$

so ist in (2. u. 3.)

$$\begin{aligned}
 16. \left\{ \begin{array}{lll} q=1p+4, & p=0q+13, & \text{also } S\mu=24, \\ 2q=2p+8, & 2p=1q+9, & S\nu=24, \\ 3q=3p+12, & 3p=2q+5, & k=4, \\ 4q=5p+3, & 4p=3q+1, & \alpha=4; \\ 5q=6p+7, & 5p=3q+14, & q^6=q^{\frac{1}{2}(p-1)}=\mathfrak{G}p+27, \\ 6q=7p+11; & 6p=4q+10, & p^8=p^{\frac{1}{2}(q-1)}=\mathfrak{G}q+1. \\ & 7p=5q+7, & =\mathfrak{G}p+1; \\ & 8p=6q+2 & \end{array} \right.
 \end{aligned}$$

Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{G}p+1$ und zugleich $p^{\frac{1}{2}(q-1)}=\mathfrak{G}q+1$.
 Desgleichen sind $S\mu$ und $S\nu$ und k und α beide gerade.
 Gemäfs (9. 1.).

Beispiel 2. Es sei

$$17. \quad p=13, \quad q=19, \quad \text{also} \quad p=4n+1, \quad q=4m-1,$$

so ist

$$\begin{aligned}
 18. \left\{ \begin{array}{lll} q=1p+6, & p=0q+13, & \text{also } S\mu=27, \\ 2q=2p+12, & 2p=1q+7, & S\nu=27, \\ 3q=4p+5, & 3p=2q+1, & k=3, \\ 4q=5p+11, & 4p=2q+14, & \alpha=3; \\ 5q=7p+4, & 5p=3q+8, & q^8=q^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1; \\ 6q=8p+10; & 6p=4q+2, & p^8=p^{\frac{1}{2}(q-1)}=\mathfrak{G}q-1. \\ & 7p=4q+15, & \\ & 8p=5q+9, & \\ & 9p=6q+3; & \end{array} \right.
 \end{aligned}$$

Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1$ und zugleich $p^{\frac{1}{2}(q-1)}=\mathfrak{G}q-1$.
 Desgleichen sind $S\mu$ und $S\nu$ und k und α beide ungerade.
 Gemäfs (9. 2.)

Beispiel 3. Es sei

$$19. \quad p=11, \quad q=17, \quad \text{also} \quad p=4n-1, \quad q=4m+1,$$

so ist

$$\begin{aligned}
 20. \left\{ \begin{array}{lll} q=1p+6, & p=0q+11, & \text{also } S\mu=21, \\ 2q=3p+1, & 2p=1q+5, & S\nu=19, \\ 3q=4p+7, & 3p=1q+16, & k=3, \\ 4q=6p+2, & 4p=2q+10, & \alpha=4, \\ 5q=7p+8; & 5p=3q+4, & q^5=q^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1; \\ & 6p=3q+15, & p^8=p^{\frac{1}{2}(q-1)}=\mathfrak{G}q-1. \\ & 7p=4q+9, & \\ & 8p=5q+3; & \end{array} \right.
 \end{aligned}$$

Also ist $q^{\frac{1}{2}(p-1)}=\mathfrak{G}p-1$ und zugleich $p^{\frac{1}{2}(q-1)}=\mathfrak{G}q-1$.
 Desgleichen sind $S\mu$ und $S\nu$ und k und α beide ungerade.
 Gemäfs (9. 2.).

Beispiel 4. Es sei

$$21. \quad p=7, \quad q=19, \quad \text{also} \quad p=4n-1, \quad q=4m-1,$$

so ist

$$\begin{array}{l}
 22. \left\{ \begin{array}{lll}
 q = 2p + 5, & p = 0q + 7, & \text{also } S\mu = 15, \\
 2q = 5p + 3, & 2p = 0q + 14, & S\nu = 12, \\
 3q = 8p + 1; & 3p = 1q + 2, & k = 1, \quad q^3 = q^{k(p-1)} = \mathfrak{G}p - 1, \\
 & 4p = 1q + 9, & z = 4; \\
 & 5p = 1q + 16, & \\
 & 6p = 2q + 4, & \text{Also ist } q^{k(p-1)} = \mathfrak{G}p - 1 \text{ und zugleich } p^{k(q-1)} = \mathfrak{G}q + 1. \\
 & 7p = 2q + 11, & \text{Desgleichen sind } S\mu \text{ und } k \text{ ungerade und } S\nu \text{ und } z \text{ gerade.} \\
 & 8p = 2q + 18, & \text{Gemäfs (11. 2.)} \\
 & 9p = 3q + 6; &
 \end{array} \right.
 \end{array}$$

Erster Beweis. **A.** Zufolge (§. 38. 8.) ist für zwei beliebige ungerade Zahlen m und n , also auch hier für die ungeraden Stammzahlen p und q ,

$$23. \quad S\mu + S\nu = \frac{1}{4}(p-1)(q-1).$$

Dieses giebt für die 3 Fälle (*Erstlich.* 8.):

$$24. \left\{ \begin{array}{l}
 1. \quad S\mu + S\nu = \frac{1}{4}(4n)(4m) = 4mn = \text{einer geraden Zahl;} \\
 2. \quad S\mu + S\nu = \frac{1}{4}(4n)(4m-2) = 2n(m-1) = \text{einer geraden Zahl;} \\
 3. \quad S\mu + S\nu = \frac{1}{4}(4n-2)(4m) = 2m(n-1) = \text{einer geraden Zahl.}
 \end{array} \right.$$

Also ist in den Fällen (*Erstlich.*) des Lehrsatzes $S\mu + S\nu$ immer eine gerade Zahl, und folglich sind $S\mu$ und $S\nu$ immer zugleich gerade oder zugleich ungerade; wie es in (9.) behauptet wird.

Für den Fall (*Zweitens.* 10.) dagegen giebt (23.)

$$\begin{aligned}
 25. \quad S\mu + S\nu &= \frac{1}{4}(4n-2)(4m-2) = (2n-1)(2m-1) \\
 &= \text{einer ungeraden Zahl;}
 \end{aligned}$$

also ist in dem Falle (*Zweitens.*) des Lehrsatzes $S\nu$ gerade, wenn $S\mu$ ungerade ist, und $S\nu$ ungerade, wenn $S\mu$ gerade ist.

B. Sodann ist nach (§. 39. 6.) in (2.) k gerade oder ungerade, je nachdem es $S\mu$ ist; denn so ist es zufolge (§. 39. 6.) für beliebige ungerade Zahlen u und v , also auch hier für die ungeraden Stammzahlen p und q . Nach (§. 41. 3. u. 4.) aber ist für eine beliebige Zahl z , die nicht mit p aufgeht, also auch hier für die Stammzahl q , $q^{k(p-1)} = \mathfrak{G}p \pm 1$, je nachdem k gerade oder ungerade ist. Also ist hier

$$26. \quad \begin{cases} q^{k(p-1)} = \mathfrak{G}p + 1, & \text{wenn } S\mu \text{ gerade und} \\ q^{k(p-1)} = \mathfrak{G}p - 1, & \text{wenn } S\mu \text{ ungerade ist.} \end{cases}$$

So wird es in (9. u. 11.) behauptet.

C. Aber in den Fällen (*Erstlich.*) sind $S\mu$ und $S\nu$ zugleich gerade und zugleich ungerade (**A.**): also ist in diesen Fällen auch zugleich, weil

z und $S\nu$ eben so über $p^{\frac{1}{2}(q-1)}$, wie k und $S\mu$ über $q^{\frac{1}{2}(p-1)}$ entscheiden,

$$27. \quad \begin{cases} p^{\frac{1}{2}(q-1)} = \mathfrak{G}q + 1, & \text{wenn } S\mu \text{ oder } S\nu \text{ gerade, und} \\ p^{\frac{1}{2}(q-1)} = \mathfrak{G}q - 1, & \text{wenn } S\mu \text{ oder } S\nu \text{ ungerade ist.} \end{cases}$$

Dieses wird ferner in (9.) behauptet.

Dagegen ist in dem Falle (*Zweitens.*) $S\nu$ ungerade, wenn $S\mu$ gerade ist; und umgekehrt: also ist in diesem Falle

$$28. \quad \begin{cases} p^{\frac{1}{2}(q-1)} = \mathfrak{G}q - 1, & \text{wenn } S\mu \text{ gerade, also } S\nu \text{ ungerade und} \\ p^{\frac{1}{2}(q-1)} = \mathfrak{G}q + 1, & \text{wenn } S\mu \text{ ungerade, also } S\nu \text{ gerade ist.} \end{cases}$$

Dieses wird ferner in (11.) behauptet.

Zweiter Beweis. **D.** In (§. 36.) bezeichnet n_1 aus den mit v aufgehenden Zahlen $z < \frac{1}{2}uv$, also aus den Zahlen

$$29. \quad \begin{cases} v = \mathfrak{G}u + r_1, \\ 2v = \mathfrak{G}u + r_2, \\ 3v = \mathfrak{G}u + r_3, \\ \dots \dots \dots \\ \frac{1}{2}(u-1)v = \mathfrak{G}u + r_{\frac{1}{2}(u-1)}, \end{cases}$$

die Anzahl *derjenigen*, welche zu u Reste $r > \frac{1}{2}u$ lassen, und n_s , aus den mit u aufgehenden Zahlen $z < \frac{1}{2}uv$, also aus den Zahlen

$$30. \quad \begin{cases} u = \mathfrak{G}v + \varrho_1, \\ 2u = \mathfrak{G}v + \varrho_2, \\ 3u = \mathfrak{G}v + \varrho_3, \\ \dots \dots \dots \\ \frac{1}{2}(v-1)u = \mathfrak{G}v + \varrho_{\frac{1}{2}(v-1)}, \end{cases}$$

die Anzahl *derjenigen*, welche zu v Reste $\varrho > \frac{1}{2}v$ lassen.

Setzt man in (29. u. 30.) statt der dortigen, unter sich theilerfremden Zahlen u und v die gegenwärtigen, ebenfalls unter sich theilerfremden beiden Stammzahlen p und q , so sind die Gleichungen (29. u. 30.) diejenigen (2. u. 3.). Also ist für den gegenwärtigen Lehrsatz:

$$31. \quad n_1 = k \quad \text{und} \quad n_s = z.$$

E. Nun ist zufolge (36. 16.)

$$32. \quad 2n_s - n_1 - n_s = \frac{1}{4}(u-1)(v-1),$$

also ist *hier*

$$33. \quad 2n_s - (k + z) = \frac{1}{4}(p-1)(q-1).$$

Aber $\frac{1}{4}(p-1)(q-1)$ ist in den Fällen (*Erstlich.* 8.), wie aus (24.) erhellet, *immer gerade*; und nur in dem Falle (*Zweitens.* 10.) *ungerade*. Die Zahl $2n_s$, welche sie auch sein mag, ist *immer gerade*, also ist vermöge (33.)

34. $\begin{cases} k \nmid z \text{ in den Fällen (Erstlich. 8.) immer gerade, und} \\ k \mid z \text{ nur in dem Falle (Zweitens. 10.) ungerade;} \end{cases}$

woraus folgt, dafs

35. $\begin{cases} k \text{ und } z \text{ in den Fällen (Erstlich. 8.) beide zugleich gerade oder un-} \\ \text{gerade sind und dafs} \\ k \text{ und } z \text{ in dem Falle (Zweitens. 10.), das eine gerade, das andere} \\ \text{ungerade ist.} \end{cases}$

F. Zuzufolge (§. 41. 3. u. 4.) ist, da das dortige z für $z = q$ hier k und für $z = p$ und $p = q$ hier z ist,

36. $q^{k(p-1)} = \mathfrak{G}p + 1$, wenn k , und $p^{k(q-1)} = \mathfrak{G}q + 1$, wenn z gerade ist und

37. $q^{k(p-1)} = \mathfrak{G}p - 1$, wenn k , und $p^{k(q-1)} = \mathfrak{G}q - 1$, wenn z ungerade ist;

also finden in den Fällen (Erstlich. 8.) vermöge (35.) die Gleichungen (36.) oder die Gleichungen (37.) zugleich Statt, und in dem Falle (Zweitens. 10.) findet die erste Gleichung (36.) mit der zweiten (37.), oder die zweite (36.) mit der ersten (37.) zugleich Statt; und zwar auf die Weise, wie es (9. u. 11.) aussagen.

G. Dafs S_μ und k und S_ν und z zugleich gerade oder ungerade sind, wie es (9. u. 11.) noch behaupten, folgt bei diesem zweiten Beweise aus (§. 39. 6.).

H. Dafs der Lehrsatz nur für Stammzahlen p und q , nicht nothwendig für andere Zahlen, welche Theiler > 1 gemein haben, Statt findet, folgt daraus, dafs der Satz (§. 41.), auf welchem er mit beruht, nur für Stammzahlen nothwendig gilt.

Anm. **I.** Der erste Beweis beruft sich auf die Lehrsätze (§. 38. 39. und 41.), der zweite auf die Lehrsätze (§. 36., 39. und 41.); der erste also auf den Satz (§. 38.) von den *Quotienten* μ in den Gleichungen $((1, 2, 3, 4, \dots, \frac{1}{2}n \text{ oder } \frac{1}{2}(n-1))m = \mu n + r$, der zweite auf den Satz (§. 36.) von den *Resten* der Zahlen $1, 2, 3, 4, \dots, \frac{1}{2}(uv-1)$, dividirt durch u und v ; ausserdem auf *dieselben* Sätze (§. 39. u. 41.). Die Sätze (§. 36. 38., 39. u. 41.) bereiten das Reciprocitäts- oder Gegenseitigkeitsgesetz für Stammzahlen vor. Sie sind aber von ihm getrennt und besonders aufgestellt worden, theils um den Beweis des gegenwärtigen Satzes an sich zu verkürzen und dadurch übersichtlicher zu machen, theils weil die vorbereitenden Sätze auch für sich selbst noch andere Anwendungen finden.

Das Reciprocitäts- oder Gegenseitigkeitsgesetz findet wieder in der gesammten Theorie der Zahlen vielfache weitere Anwendungen und ist daher, gleich dem *Fermatschen* Satze (§. 40.), ebenfalls als einer der Hauptsätze der Zahlenlehre zu betrachten. (Die Fortsetzung folgt.)