$= 49$, $\sqrt[4]{2401} = 7 = \mathfrak{A}$, $A^2 + \mathfrak{A}^2 = 162$, $\frac{A + \mathfrak{A}^2}{8} = \frac{81}{4}$, $\sqrt{\frac{A + \mathfrak{A}^2}{8}} = \frac{9}{2}$. Also

$$\sqrt[4]{(113 + 72\sqrt{2})} = \sqrt{(\tfrac{9}{2} + \tfrac{7}{2})} + \sqrt{(\tfrac{9}{2} - \tfrac{7}{2})} = 1 + \sqrt{8} = 1 + 2\sqrt{2}.$$

12. Für $\sqrt[3]{(A \pm \sqrt{B})}$ müßte man nach (8.) die Gleichungen

$$A = x^3 + 3xy,\ y = x^2 - \tfrac{1}{3}\sqrt[3]{(A^2 - B)},$$

d. i. nach der Elimination von y die Gleichung des dritten Grades

$$4x^3 - 3x\sqrt[3]{(A^2 - B)} - A = 0$$

auflösen, und y aus obiger Formel bestimmen. Die Wurzeln höherer Grade führen eben so auf die Auflösung höherer Gleichungen, in welchem Verhältnisse natürlich auch die Schwierigkeit wächst.

M. s. über diesen Gegenstand Neutoni Arithmetica universalis. §. 84. und Castillons Commentar p. 78. Eulers Algebra. Thl. I. Cap. 8.; besonders einen Aufsatz von Hennert in Hindenburgs Archiv der reinen und angew. Math. Neuntes Heft. S. 50.

Wurzelgrößen, s. Wurzel (6.).

Wurzelzeichen, s. Wurzel und Zeichen, mathematische.

Z.

Zähler eines Bruchs, s. Bruch.

Zahl (Numerus). Der Begriff der Zahl entsteht überhaupt durch die Vorstellung des Neben- oder Beieinanderseyns mehrerer Dinge, welche entweder wirklich völlig gleich und gleichartig sind, oder auf deren Verschiedenheit, insofern sie zu einer Zahl vereinigt werden sollen, wenigstens keine Rücksicht genommen wird; also auch, was dasselbe ist, durch die Vorstellung der Wiederholung oder Vervielfachung eines und desselben Dinges, welches im Allge-

meinen durch A bezeichnet werden soll. Nun kann man sich aber entweder die durch Wiederholung des A entstandene Größe selbst, oder auch bloß die Menge der Wiederholungen vorstellen. Das Erste heißt eine benannte, concrete oder auch unreine Zahl, und A ihre Einheit; das Zweite wird eine unbenannte, abstracte oder reine Zahl genannt. In jeder benannten Zahl ist folglich eine unbenannte enthalten, und man kann also, wenn jene durch N, diese durch n, die Einheit durch A bezeichnet wird, jede benannte Zahl durch $N = nA$ darstellen, indem durch das bloße Nebeneinandersetzen der Symbole n und A bekanntlich die nmalige Wiederholung oder Vervielfachung der Größe A angedeutet wird. Umgekehrt kann jede unbenannte Zahl als eine benannte betrachtet werden, wenn sie auf eine bestimmte Größe als Einheit bezogen wird.

1. Daß jede benannte Zahl eine Größe (Quantum) ist, und ihr auch eine bestimmte Größe als Eigenschaft zukommt, unterliegt keinem Zweifel. Eben so klar ist es, daß auch jede unbenannte Zahl, in Bezug auf mehr oder minder oftmalige Wiederholung irgend einer willkührlich gedachten Einheit, eine Größe ist, und also auch unbenannte Zahlen rücksichtlich der Größe auf jede Art mit einander verbunden und verglichen werden können. Die Größe einer benannten Zahl $N = nA$ hängt sowohl von der Größe der Einheit A, auf welche sie sich bezieht, als auch von der Größe der in ihr enthaltenen unbenannten Zahl n ab. Ueberhaupt können aber benannte Zahlen nur dann mit einander verglichen werden, wenn die Einheiten, auf welche sie sich beziehen, wenn auch nicht gleich, aber doch gleichartig sind. Zwischen 12 Pfund und 6 Thlr. ist keine Vergleichung möglich; aber wohl zwischen 12 Pfund und 6 Lth. Sollen nun überhaupt, Gleichartigkeit der Einheiten vorausgesetzt, irgend zwei benannte Zahlen $N = nA$, $N' = n'A'$ mit einander verglichen werden; so suche man ein gemeinschaftliches Maaß der Einheiten A und A', welches durch M bezeichnet werden mag. Ist dieses gemeinschaftliche Maaß in A und A' respective m und m' Mal enthalten, so daß $A = mM$, $A' = m'M$ ist; so ist

$N = nmM$, $N' = n'm'M$, und die Größe der Zahlen N und N' hängt nun bloß von den unbenannten Zahlen nm und n'm' ab. Man kann also diese statt jener setzen, und mit ihnen alle Rechnungen ausführen, welche mit den benannten Zahlen vorgenommen werden sollten, wenn nur dem ebenfalls als unbenannte Zahl erscheinenden Resultate wieder M als Einheit untergelegt wird. Dieß ist auch der Grund, daß die Arithmetik bei allen ihren Operationen bloß unbenannte Zahlen zum Grunde legt, weil, um mit benannten Zahlen rechnen zu können, bloß noch specielle Regeln zur Reduction der verschiedenen Einheiten auf einander, oder zur Auffindung ihres gemeinschaftlichen Maaßes erforderlich sind, welche aber immer von der besondern Beschaffenheit der in Rechnung genommenen Größen abhängen, und eben deshalb der reinen Arithmetik fremd sind, sich aber immer aus der Natur dieser Größen leicht ergeben, wie schon aus den ersten Elementen des Rechnens bekannt ist.

2. Man pflegt zwischen ganzen und gebrochenen Zahlen oder Brüchen zu unterscheiden. Jene entstehen durch unmittelbare Vervielfachung der Einheit, und sind völlig einerlei mit dem, was wir so eben eine Zahl schlechthin genannt haben. Brüche entstehen durch Theilung der Einheit in gleiche Theile, und Vervielfachung eines der erhaltenen Theile. Liegt hierbei eine bestimmte Einheit zum Grunde, so ist der Bruch benannt, sonst unbenannt. Dieser Unterschied zwischen ganzen Zahlen und Brüchen ist aber durchaus nicht wesentlich, da jeder Bruch, wenn er nur auf eine andere Einheit bezogen wird, auch als ganze Zahl betrachtet werden kann, und umgekehrt. Der Bruch $\frac{n}{m}A$ ist die ganze Zahl n, auf $\frac{1}{m}A = A'$ als Einheit bezogen; die ganze Zahl nA ist der Bruch $\frac{1}{n}$, für $nnA = A''$ als Einheit. In diesem Artikel werden wir von nun an unter dem Worte Zahl immer die ganze Zahl verstehen.

Vorzüglich bei den ältern Mathematikern findet man sehr viele verschiedene Formen der Zahlen, von denen in einzelnen Artikeln dieses Wörterbuchs besonders gehandelt

worden ist, wie z. B. die geraden und ungeraden Zahlen, die Primzahlen, die vollständigen und unvollständigen Zahlen, die befreundeten Zahlen, die figurirten Zahlen, die Polygonal-, Pyramidal- und Pyrgoidal-Zahlen, die Pronikzahlen, u. dergl.

Ueber die Bezeichnung der Zahlen s. m. die Artikel Zahlensystem, Zahlzeichen und Ziffer.

3. Immer hat der abergläubische, dem Wunderbaren gern sich hinneigende Mensch, in gewissen Zahlen geheime übermenschliche Kräfte zu finden geglaubt. Schon bei den ägyptischen Priestern treffen wir die ersten Spuren der Zahlensymbolik. Die Zahl sieben war ihnen heilig, weil der Nil mit sieben Mündungen in's Meer strömt. Pythagoras mag sie auf seinen Reisen von den Aegyptiern gelernt haben, und die Zahlensymbolik ward ein charakteristisches Merkmal seiner Schule. Schon bei den Hebräern heißt schwören siebenen, d. h. bei der Zahl sieben betheuern. Zahlen, die in den Büchern der heiligen Schrift oft vorkommen, sind bei den Völkern der christlichen Zeitrechnung immer für heilig gehalten worden, wie z. B. die Zahl sechs, weil die Genesis lehrt, daß Gott in eben so vielen Tagen die Erschaffung der Welt vollendete. Heilbronner hat manches hierher gehörende in einem besondern Kapitel: De arcanis numerorum qualitatibus, a quibusdam ingeniose, interdum vero superstitiose inventis, seiner Historia Matheseos (p. 746—758.) gesammelt. Er führt z. B. zehn Sprachen an, in denen der Name des höchsten Wesens mit vier Buchstaben geschrieben wird. Von den hierher gehörenden Schriften des Virgilius (Salzburgensis), Clichtoveus, Paulinus, Lindenberg, Petrus Bungus handelt Kästner ausführlich in der Gesch. d. Math. Thl. I. S. 205 ff. Auch gehören hierher des Athanasius Kircher Arithmologia, sive de occultis numerorum mysteriis. Romae. 1665. 4.; Meursius de denario pythagorico; auch ein zwar kurzer, aber nicht uninteressanter Aufsatz in den Blättern für literarische Unterhal-

tung. Lpzg. 1827. Nr. 148. 149. Geschichte des Glaubens an die Heiligkeit der Zahl Sieben in F. Gedikes vermischten Schriften. Berlin. 1801. S. 32 — 60. Durch die Ueberschrift des hierher gehörenden Kapitels in Kästners Geschichte der Mathematik: „Gelehrter Tand von Zahlen" mag Zweck und Werth vorstehender Bemerkungen angedeutet seyn.

4. Die ganze Zahlenwissenschaft nennt man gewöhnlich die Arithmetik. In neuerer Zeit sind jedoch zwei wesentlich von einander verschiedene Theile derselben von einander geschieden worden. Den einen größern, am meisten bearbeiteten, könnte man den rechnenden oder calculatorischen nennen, weil der eigentliche Calcul nach allen möglichen Richtungen Hauptzweck desselben ist, seinen Hauptinhalt ausmacht. Unter der Arithmetik im engern Sinne wird namentlich dieser Theil verstanden. Er zerfällt wieder in mehrere einzelne große Wissenschaften, über welche besondere Artikel dieses Wörterbuchs hinreichende Belehrung ertheilen. Der andere Theil der Zahlenwissenschaft dagegen beschäftigt sich, so wie die Geometrie die Eigenschaften der verschiedenen Formen der ausgedehnten Größe untersucht, mit der Aufsuchung der Eigenschaften der Zahlen, d. i. immer der ganzen Zahlen, deren es viele höchst merkwürdige, zum Theil sehr versteckte, giebt. Man nennt diesen Zweig der Arithmetik die Zahlenlehre im engern Sinne, oder auch sehr passend, nach Legendre's Vorgange, die Theorie der Zahlen. Von dieser wichtigen und hohes Interesse habenden Disciplin einen Abriß zu geben, ist der Zweck dieses Artikels. Vollständigkeit ist auf so geringem Raume unerreichbar. Die Sätze ohne Beweise zu geben, möchte wenigen Nutzen haben, und nur höchst unvollständige Belehrung gewähren. Wir geben daher einige der wichtigsten, einflußreichsten und interessantesten Theoreme vollständig mit ihren Beweisen, wodurch der Leser in den Geist der Wissenschaft eingeführt, und zum Studium größerer Werke vorbereitet werden wird.

I. Satz des Euclides von den Primzahlen.

1. Wenn jede der beiden Zahlen P, Q kleiner als die Primzahl p ist; so ist das Product PQ nicht durch p theilbar.

Sey, indem man $P, r, r', r'', r''', \ldots$ als Divisoren, und $r, r', r'', r''', r'''', \ldots$ als die entsprechenden Reste betrachtet,

$$\begin{aligned} p &= Pq + r, \\ P &= rq' + r', \\ r &= r'q'' + r'', \\ r' &= r''q''' + r''', \\ &\text{ꝛc.} \qquad \text{ꝛc.} \end{aligned}$$

wobei zu bemerken, daß r, weil p eine Primzahl und $> P$ ist, positiv und nicht $= 0$ ist. Durch Substitution erhält man leicht nach und nach:

$$\begin{aligned} p &= Pq + r \\ &= rqq' + r'q + r \\ &= r'qq'q'' + r''qq' + r'q + r \\ &= r''qq'q''q''' + r'''qq'q'' + r''qq' + r'q + r \\ &\quad \text{ꝛc} \qquad\qquad \text{ꝛc.} \end{aligned}$$

Würde nie ein Glied der Reihe $r, r', r'', r''', \ldots$ $= 0$, so würden diese Ausdrücke in's Unendliche fortgehen, und folglich p durch eine unendliche Reihe positiver ganzer Zahlen ausgedrückt werden, welches ungereimt ist. Also muß man irgend ein Mal auf einen Rest $= 0$ kommen. Dieser Rest sey $= r^{(n+1)}$; so ist die Reihe der ersten Gleichungen begrenzt und folgende:

$$\begin{aligned} p &= Pq + r \\ P &= rq' + r' \\ r &= r'q'' + r'' \\ &\ldots\ldots\ldots \\ r^{(n-2)} &= r^{(n-1)}q^{(n)} + r^{(n)} \\ r^{(n-1)} &= r^{(n)}q^{(n+1)}. \end{aligned}$$

Also geht $r^{(n)}$ in $r^{(n-1)}$, folglich auch in $r^{(n-2)}$, folglich auch in $r^{(n-3)}$, also endlich auch in p auf. Da nun p eine Primzahl und $r^{(n)}$ offenbar $< p$ ist; so ist $r^{(n)} = 1$.

Folglich vorstehende Gleichungen, wenn man sie zugleich alle mit Q vervielfältigt:

$$\begin{aligned} pQ &= PQq + rQ \\ PQ &= rQq' + r'Q \\ rQ &= r'Qq'' + r''Q \\ &\ldots\ldots\ldots \\ r^{(n-2)}Q &= r^{(n-1)}Qq^{(n)} + Q\,. \end{aligned}$$

Ginge nun p in PQ auf, so müßte es, wegen der ersten Gleichung, da es in pQ aufgeht, offenbar auch in rQ, folglich eben so, wegen der zweiten, in r′Q, und, wegen der dritten, in r″Q aufgehen, u. s. f. Setzt man diesen Schluß fort, so erhellet, daß p in Q aufgehen müßte, welches ungereimt ist, da nach der Voraussetzung $p \nmid Q$. Also kann p nicht in PQ aufgehen.

2. Geht die Primzahl p weder in P, noch in Q auf; so geht sie auch in PQ nicht auf.

Sey

$$P = pp' + r,\ Q = pq' + r'\,;$$

wo $r < p$, $r' < p$ ist; so ist

$$PQ = p^2p'q' + pq'r + pp'r' + rr'\,.$$

Ginge nun p in PQ auf; so müßte es offenbar auch in rr′ aufgehen, welches gegen (1.) ist.

3. Geht also die Primzahl p in PQ auf; so muß sie entweder in P oder in Q aufgehen.

Diesen Satz, welcher in der Zahlenlehre sehr geschätzt wird, hat schon Euclides (VII. 32.). Andere Beweise geben Legendre (Théorie des nombres. Séc. édit. p. 3.), und Gauß (Disquisitiones arithmeticae. p. 8. 9.).

4. Geht die Primzahl p in keiner der Zahlen P, Q, R, S, ... auf; so kann sie auch in PQRS .... nicht aufgehen.

p geht in PQ nicht auf (2.); also auch in PQR nicht (2.); also auch in PQRS nicht (2.); u. s. f.

5. Geht also die Primzahl p in dem Producte PQRS .... auf; so muß sie in einem seiner Factoren aufgehen. Geht

sie also in Q, R, S, ... nicht auf; so muß sie in P aufgehen.

6. Ist p mit P, Q, R, S, ... relative Primzahl; so geht p in PQRS .... nicht auf.

Ist p absolute Primzahl; so folgt der Satz aus (4.). Ist dies aber nicht der Fall; so sey $p = p'q$, wo p' eine Primzahl ist. Ginge nun p in PQRS .... auf; so sey

$$\frac{PQRS\ldots.}{p} = N = \frac{PQRS\ldots.}{p'q};$$

also $PQRS\ldots = p'qN$, und es müßte folglich die Primzahl p' in PQRS ... aufgehen, ohne, weil $p = p'q$ mit P, Q, R, S, ... relative Primzahl ist, in einer dieser Zahlen aufzugehen; gegen (4.).

7. Geht p, welches mit P, Q, R, S, ... relative Primzahl ist, in dem Producte $PQRS\ldots \times N$ auf; so muß p in N aufgehen.

Sey wieder $p = p'q$ und p' eine Primzahl;

$$\frac{PQRS\ldots\times N}{p} = N' = \frac{PQRS\ldots\times N}{p'q},$$

$$\frac{PQRS\ldots\times N}{p'} = qN'.$$

Also geht die Primzahl p', welche, weil $p = p'q$ mit P, Q, R, S, ... relative Primzahl ist, in keiner dieser Zahlen aufgehen kann, in $PQRS\ldots \times N$ auf, und muß folglich in N aufgehen (5.). Sey daher $N = p'N_1$, $q = p''q'$, wo p'' wieder eine Primzahl ist; so ist

$$\frac{PQRS\ldots\times N}{p'q} = N' = \frac{PQRS\ldots\times N_1}{p''q'},$$

$$\frac{PQRS\ldots\times N_1}{p''} = q'N',$$

woraus wie vorher folgt, daß p'' in N_1 aufgehen muß. Sey daher $N_1 = p''N_2$, und jetzt q' selbst eine Primzahl, also nicht weiter zerlegbar; so ist

$$\frac{PQRS\ldots\times N_1}{p''q'} = N' = \frac{PQRS\ldots\times N_2}{q'};$$

folglich, wie vorher, auch N_2 durch q' theilbar, und daher $N_2 = q'N_3$. Aber $N = p'p''q'N_3$, und $p = p'p''q'$; also N durch p theilbar. Daß dieser Beweis allgemein ist, fällt in die Augen.

8. Sind p, p' relative Primzahlen, deren jede in P aufgeht; so geht auch pp' in P auf.

Sey $P = pq$, so geht p' in pq, und folglich (7.), weil es mit p relative Primzahl ist, in q auf. Ist also $q = p'q'$; so ist $P = pp'q'$, so daß also pp' in P aufgeht.

9. Sind p, p', p'', p''', ... relative Primzahlen, deren jede in P aufgeht; so geht $pp'p''p'''$ ... in P auf.

Nach (8.) geht pp' in P auf; pp' und p'' sind relative Primzahlen, weil, wenn dies nicht der Fall wäre, pp' und p'' einen gemeinschaftlichen Primfactor haben müßten, welcher, weil er in pp' aufginge, in p oder p' aufgehen müßte (3.), so daß also p'' und p oder p' nicht relative Primzahlen wären, gegen die Voraussetzung; also geht $pp'p''$ in P auf (8.). Wie man weiter gehen kann, fällt in die Augen.

10. Ist der Bruch $\frac{x}{y}$ auf seine kleinste Benennung gebracht, so sind x, y relative Primzahlen; also ist $\frac{xxx\ldots x}{y} = \frac{x^n}{y}$ keine ganze Zahl (6). Folglich ist auch $\frac{x^n}{y^n} = \left(\frac{x}{y}\right)^n$ keine ganze Zahl, weil, wenn dies der Fall, und $\frac{x^n}{y^n} = z$ wäre, $\frac{x^n}{y} = zy^{n-1}$, d. i. eine ganze Zahl, seyn würde, gegen das so eben Bewiesene.

11. Die Potenz a^n hat keinen andern Primfactor als a, weil jede Primzahl, die in a nicht aufgeht, auch in a^n nicht aufgeht (4.). Geht daher die Primzahl x in a^n auf; so muß x auch in a aufgehen.

12. Giebt es keine Zahl x, welche $= \sqrt[n]{a}$ ist; so giebt es auch keinen dieser Wurzel gleichen rationalen Bruch. Wäre nämlich $\sqrt[n]{a} = \frac{y}{z}$, und dieser Bruch, wie immer angenommen werden kann, auf seine kleinste Benennung gebracht, aber auch nach der Voraussetzung keiner ganzen Zahl gleich; so wäre $\left(\frac{y}{z}\right)^n = a$ doch eine ganze Zahl, gegen (10.). Dieser Satz ist für die strenge Theorie der Irrationalzahlen sehr wichtig.

13. Aus den bisherigen Sätzen läßt sich auch mit aller Strenge beweisen, daß jede Zahl nur auf eine einzige Art in Primfactoren zerlegt werden kann.

Sey nämlich $N = a^{\alpha} b^{\beta} c^{\gamma} \ldots$, wo a, b, c, ... lauter unter einander ungleiche Primzahlen sind. Könnte nun N noch auf eine andere Art in Primfactoren zerlegt werden, so ist zunächst klar, daß unter derselben keine andern als a, b, c, ... vorkommen können, weil sonst N von einer Primzahl getheilt werden müßte, welche weder in a, noch in b, noch in c, u. s. f. aufginge, welches mit (4.) streitet. Auch kann in dem zweiten Systeme keiner der Primfactoren a, b, c, ... fehlen, weil sonst ebenfalls nach (4.) der fehlende Primfactor nicht in N aufgehen könnte. Demnach könnte der Unterschied der beiden Systeme bloß darin liegen, daß ein Primfactor, z. B. p, in dem einen öfter vorkäme, als in dem andern. Käme nun p in dem einen μ, in dem andern ν Mal vor; so schaffe man, vorausgesetzt, daß $\mu > \nu$, diesen Primfactor aus jedem Systeme ν Mal durch Division weg, wodurch er aus dem einen ganz verschwinden, in dem andern dagegen noch $\mu - \nu$ Mal vorkommen wird. Es würde also die Zahl $\frac{N}{p^{\nu}}$ sowohl durch p theilbar, als auch (4.) durch p nicht theilbar seyn, welches offenbar ungereimt ist. S. Gauß a. a. O. p. 10.

II. Die Congruenz der Zahlen.

1. Begriff und Zeichen der Congruenz sind von Gauß in die Zahlenlehre eingeführt worden, und für diese Wissenschaft in jeder Beziehung so wichtig, daß die Hauptsätze darüber hier nicht fehlen dürfen.

Wenn die Differenz zweier Zahlen b, c von der Zahl a gemessen wird, so heißen die Zahlen b, c nach dem Modulus a einander congruent, und jede ein Rest der andern. Wird dagegen die Differenz dieser Zahlen von a nicht gemessen, so heißen sie nach dem Modulus a nicht congruent, und jede ein Nichtrest der andern. Diese Begriffe gelten, b und c mögen positiv oder negativ seyn.

Der Modulus wird aber immer als positiv angenommen. Die Beziehung der Congruenz zwischen zwei Zahlen wird nach Gauß durch $b \equiv c$ (Mod. a) bezeichnet, wie z. B. $-16 \equiv 9$ (Mod. 5), $-7 \equiv 15$ (Mod. 11), da $(-16-9):5 = -5$, $(-7-15):11 = -2$, oder auch $(9-(-16)):5 = 5$, $(15-(-7)):11 = 2$, d. i. immer eine ganze Zahl ist. 9 heißt ein Rest von -16 für den Modulus 11, 15 ein Nichtrest von -7 für den Modulus 3. Jeder Rest der Zahl a für den Modulus m ist unter der Form $a + km$, wo k irgend eine unbestimmte Zahl bezeichnet, enthalten. Jede Zahl ist sich selbst in Bezug auf einen willkührlichen Modulus congruent, da Null durch jede Zahl theilbar ist.

2. Für irgend eine Zahl a oder $-a$ sey

$$a = mk + r, \quad a = m(k+1) - \varrho;$$
$$-a = -mk - r, \quad -a = -m(k+1) + \varrho;$$

so daß $r < m$, $\varrho < m$ ist. Dann ist

$$a - r = mk, \quad a - (-\varrho) = m(k+1);$$
$$-a - (-r) = -mk, \quad -a - \varrho = -m(k+1).$$

Folglich hat jede Zahl a einen in den Reihen

$$0, 1, 2, 3, 4, \ldots (m-1);$$
$$0, -1, -2, -3, -4, \ldots (m-1);$$

enthaltenen positiven und negativen Rest. Diese beiden Reste reduciren sich aber auf den einen Rest o, wenn a selbst durch den Modulus m theilbar ist. Aus den obigen Gleichungen folgt durch Subtraction leicht

$$o = -m + r + \varrho, \quad r + \varrho = m.$$

Also ist, wenn die Reste r, ϱ ungleich sind, immer einer $< \frac{1}{2}m$, wenn sie aber gleich sind, jeder $= \frac{1}{2}m$. Zugleich erhellet aber auch, daß in jeder der beiden obigen Reihen nicht mehr als ein Rest der Zahl a enthalten seyn kann, indem für den positiven Rest r, da der Bruch $\frac{a-r}{m}$ eine ganze Zahl ist, offenbar keiner der Brüche

$$\frac{a-1}{m} = \frac{a-r+(r-1)}{m},$$
$$\frac{a-2}{m} = \frac{a-r+(r-2)}{m},$$
$$\ldots\ldots\ldots\ldots$$

$$\frac{a-(r-1)}{m} = \frac{a-r+1}{m},$$
$$\frac{a-(r+1)}{m} = \frac{a-r-1}{m},$$
$$\frac{a-(r+2)}{m} = \frac{a-r-2}{m},$$
$$\cdots\cdots\cdots$$
$$\frac{a-(m-1)}{m} = \frac{a-r-(m-1-r)}{m}$$

eine ganze Zahl seyn kann, weil alle zu $a-r$ addirten, oder davon abgezogenen, Größen $< m$ sind. Für den negativen Rest $-\varrho$ ist der Bruch $\frac{a+\varrho}{m}$ eine ganze Zahl, und folglich auf ähnliche Art wie vorher keiner der Brüche

$$\frac{a+1}{m} = \frac{a+\varrho-(\varrho-1)}{m},$$
$$\frac{a+2}{m} = \frac{a+\varrho-(\varrho-2)}{m},$$
$$\cdots\cdots\cdots$$
$$\frac{a+(\varrho-1)}{m} = \frac{a+\varrho-1}{m},$$
$$\frac{a+(\varrho+1)}{m} = \frac{a+\varrho+1}{m},$$
$$\frac{a+(\varrho+2)}{m} = \frac{a+\varrho+2}{m},$$
$$\cdots\cdots\cdots$$
$$\frac{a+(m-1)}{m} = \frac{a+\varrho+(m-1-\varrho)}{m}$$

eine ganze Zahl.

Die beiden Reste der Zahl a, welche $< m$ sind, sollen die kleinsten Reste derselben genannt werden. Wie sie in jedem Falle leicht gefunden werden können, erhellet aus dem Obigen. Von -13 sind für den Modulus 5 die beiden kleinsten Reste -3 und $+2$, da $-13 = -5.2-3$, $-13 = -5.3+2$ ist.

Bei allen folgenden Sätzen über die Congruenz der Zahlen soll immer Identität des Modulus vorausgesetzt werden.

3. Wenn $a \equiv c$, $b \equiv c$; so ist auch $a \equiv b$.

Bezeichnen wir immer den Modulus durch m; so ist

$a - c = mk$, $b - c = mk'$, $(a - c) - (b - c) = a - b = m(k - k')$; also $a \equiv b$.

4. Wenn $a \equiv b$, $a' \equiv b'$, $a'' \equiv b''$, $a''' \equiv b'''$,... ist; so ist auch

$$a + a' + a'' + a''' + \ldots \equiv b + b' + b'' + b''' + \ldots.$$

Denn es ist nach der Voraussetzung

$$a - b = mk,\ a' - b' = mk',\ a'' - b'' = mk'',\ a''' - b''' = mk''', \ldots;$$

also

$$(a - b) + (a' - b') + (a'' - b'') + (a''' - b''') + \ldots. = m(k + k' + k'' + k''' + \ldots.),$$

$$(a + a' + a'' + a''' + \ldots) - (b + b' + b'' + b''' + \ldots) = m(k + k' + k'' + k''' + \ldots),$$

$$a + a' + a'' + a''' + \ldots. \equiv b + b' + b'' + b''' + \ldots$$

5. Ist $a \equiv b$, $a' \equiv b'$; so ist auch $a - a' \equiv b - b'$.

Denn $a - b = mk$, $a' - b' = mk'$; also $(a - b) - (a' - b') = (a - a') - (b - b') = m(k - k')$, d. i. $a - a' \equiv b - b'$.

6. Ist $a \equiv b$, $a' \equiv b'$, $a'' \equiv b''$, $a''' \equiv b'''$,....; so ist auch

$$aa'a''a'''\ldots. \equiv bb'b''b'''\ldots.$$

Betrachten wir nur den Fall, wenn fünf Congruenzen gegeben sind, weil daran der Beweis schon in seiner Allgemeinheit völlig deutlich werden wird; so erhellet leicht, daß

$$(a - b)a'a''a'''a'''' = aa'a''a'''a'''' - ba'a''a'''a'''',$$
$$b(a' - b')a''a'''a'''' = ba'a''a'''a'''' - bb'a''a'''a'''',$$
$$bb'(a'' - b'')a'''a'''' = bb'a''a'''a'''' - bb'b''a'''a'''',$$
$$bb'b''(a''' - b''')a'''' = bb'b''a'''a'''' - bb'b''b'''a'''',$$
$$bb'b''b'''(a'''' - b'''') = bb'b''b'''a'''' - bb'b''b'''b''''.$$

Wird nun, indem man wieder $a - b = mk$, $a' - b' = mk'$, $a'' - b'' = mk''$, ... setzt, auf beiden Seiten addirt; so erhält man leicht

$$aa'a''a'''a'''' - bb'b''b'''b'''' = m\left\{\begin{array}{l} ka'a''a'''a'''' + bk'a''a'''a'''' + bb'k''a'''a'''' \\ + bb'b''k'''a'''' + bb'b''b'''k'''' \end{array}\right\},$$

woraus die behauptete Congruenz unmittelbar folgt.

7. Da für jedes α immer $\alpha \equiv \alpha$ ist (1.); so ist, wenn $a \equiv b$ ist, nach dem vorigen Satze immer auch $\alpha a \equiv \alpha b$.

8. Eben so leicht folgt auch aus (6.), daß für jedes positive ganze α, wenn $a \equiv b$ ist, immer auch $a^\alpha \equiv b^\alpha$ seyn muß.

Aus den vorhergehenden Sätzen folgt unmittelbar, daß mit den Congruenzen ähnliche Veränderungen, wie mit den Gleichungen vorgenommen werden können; nämlich durch Addition, Subtraction und Multiplication.

9. Bezeichnen a, b, c, d, ... positive ganze, A, B, C, D, ... ganze Zahlen, so sind, wenn für x in dem Polynom

$$Ax^a + Bx^b + Cx^c + Dx^d + \ldots.$$

irgend zwei congruente Werthe gesetzt werden, die entsprechenden Werthe des Polynoms einander ebenfalls congruent, in Bezug auf denselben Modulus.

Sey $p \equiv q$, so ist $p^a \equiv q^a$, $p^b \equiv q^b$, $p^c \equiv q^c$, $p^d \equiv q^d$, ... (8.), $Ap^a \equiv Aq^a$, $Bp^b \equiv Bq^b$, $Cp^c \equiv Cq^c$, $Dp^d \equiv Dq^d$, ... (7.);

$$Ap^a + Bp^b + Cp^c + Dp^d + \ldots.$$
$$\equiv Aq^a + Bq^b + Cq^c + Dq^d + \ldots. \quad (4.).$$

10. Ist $a \equiv b$ (Mod. mn); so ist immer auch $a \equiv b$ (Mod. n). Denn $a - b = mnk$, $a - b = n \cdot mk$, also $a \equiv b$ (Mod. n).

11. Ist $a \equiv b$ (Mod. m), $a \equiv b$ (Mod. n), $a \equiv b$ (Mod. p), ...; so ist, wenn m, n, p, ... relative Primzahlen sind, auch $a \equiv b$ (Mod. mnp...).

Da nämlich m, n, p, ... in $a - b$ aufgehen, und relative Primzahlen sind; so muß auch mnp.... in $a - b$ aufgehen (I. 9.), d. h. $a \equiv b$ (Mod. mnp ...) seyn.

12. Wenn a, b durch n theilbar, und in Bezug auf den Modulus m congruent sind; so ist, wenn m und n relative Primzahlen sind, immer $\frac{a}{n} \equiv \frac{b}{n}$ (Mod. m).

Da nämlich sowohl m, als auch n in $a - b$ aufgeht; so geht, weil m und n relative Primzahlen sind, auch mn in $a - b$ auf (I. 9.), und es ist folglich $a - b = mnk$, $\frac{a}{n} - \frac{b}{n} = mk$, also $\frac{a}{n} \equiv \frac{b}{n}$ (Mod. m).

13. Ist $a \equiv b$ (Mod. m); so ist, wenn n in a, b, m aufgeht, immer auch $\frac{a}{n} \equiv \frac{b}{n}$ (Mod. $\frac{m}{n}$).

Denn es ist $a - b = mk$. Ist nun $a = na'$, $b = nb'$, $m = nm'$; so ist $n(a' - b') = nm'k$, $a' - b' = m'k$, $a' \equiv b'$ (Mod. m'), d. i. $\frac{a}{n} \equiv \frac{b}{n}$ (Mod. $\frac{m}{n}$).

14. Sind m, n nicht relative Primzahlen, sondern haben das größte gemeinschaftliche Maaß e; so ist, wenn a, b durch n theilbar, und in Bezug auf m als Modulus congruent sind, immer $\frac{a}{n} \equiv \frac{b}{n}$ (Mod. $\frac{m}{e}$).

Sey $m = ee'$, $n = ee''$; so ist nach der Voraussetzung $a \equiv b$ (Mod. ee'), $a \equiv b$ (Mod. ee''), da a und b, also auch $a - b$, durch n theilbar ist. Folglich $\frac{a}{e} \equiv \frac{b}{e}$ (Mod. e'), $\frac{a}{e} \equiv \frac{b}{e}$ (Mod. e'') (13.); folglich, weil e', e'' relative Primzahlen sind, $\frac{a}{e} \equiv \frac{b}{e}$ (Mod. $e'e''$) (11.). Da aber $ee'' = n$ in a und b aufgeht, so geht auch e'' in $\frac{a}{e}$ und $\frac{b}{e}$ auf, so daß also

$$\frac{a}{ee''} \equiv \frac{b}{ee''} \text{ (Mod. } e') \text{ (13.), d. i. } \frac{a}{n} \equiv \frac{b}{n} \left(\text{Mod. } \frac{m}{e}\right).$$

15. Ist a mit m relative Primzahl, und p, q sind in Bezug auf m als Modulus nicht congruent; so sind auch ap und aq in Bezug auf diesen Modulus nicht congruent.

Wäre $ap \equiv aq$ (Mod. m); so wäre, da a und m relative Primzahlen sind, auch $\frac{ap}{a} \equiv \frac{aq}{a}$ (Mod. m) (12.), d. i. $p \equiv q$ (Mod. m); gegen die Voraussetzung.

16. Einen Ausdruck wie $ax \equiv b$ (Mod. m) nennt man nach Gauß eine Congruenz des ersten Grades. Ein solcher Ausdruck verlangt nämlich, x so zu bestimmen, daß ax mit b in Bezug auf den Modulus m congruent, oder $ax - b$ durch m theilbar wird, woraus man sogleich übersieht, daß dies ein Problem der unbestimmten Analytik, und mit der Auflösung der unbestimmten Gleichungen

des ersten Grades einerlei ist, indem sich aus den Bedingungen der Aufgabe unmittelbar die unbestimmte Gleichung des ersten Grades:

$$\frac{ax - b}{m} = y, \; ax - my = b$$

ergiebt, deren Auflösung in dem Artikel Unbestimmte Analytik ausführlich gelehrt worden ist, so daß wir also dabei hier nicht länger verweilen. Eben so würde bei mehrern unbekannten Größen die Congruenz

$$ax + by \equiv c \, (\text{Mod. } m)$$

auf die unbestimmte Gleichung

$$\frac{ax + by - c}{m} = z, \; ax + by - mz = c$$

führen, u. s. f. Uebersteigen die Potenzen der unbekannten Größen den ersten Grad, so kann man auf ähnliche Art, wie bei den Gleichungen, Congruenzen verschiedener Grade unterscheiden. Immer wird aber das Problem auf eine Aufgabe der unbestimmten Analytik zurückkommen, woraus zugleich die innige Verwandschaft dieses Theiles der Algebra mit der Theorie der Zahlen erhellet.

17. Soll die Congruenz des ersten Grades

$$Ax + B \equiv C \, (\text{Mod. } p)$$

im Allgemeinen auflösbar seyn, so dürfen A und p kein gemeinschaftliches Maaß haben. Da nämlich $C \equiv C$ ist (1.), so folgt aus der obigen Congruenz leicht durch Subtraction

$$Ax + B - C \equiv o \, (\text{Mod. } p) \quad (5.),$$

d. h. $Ax + B - C$ durch p theilbar. Also läßt sich setzen

$$Ax + B - C = pq.$$

Hätten nun A und p ein gemeinschaftliches Maaß e, so daß $A = eA'$, $p = ep'$ wäre; so wäre

$$eA'x + B - C = ep'q,$$

$$A'x + \frac{B - C}{e} = p'q,$$

und folglich auch $B - C$ durch e theilbar. Hätten also A und p ein gemeinschaftliches Maaß, so würde unsere Congruenz nur in dem besondern Falle in ganzen Zahlen auflösbar seyn, wenn auch $B - C$ durch dasselbe Maaß theilbar wäre. Soll unsere Congruenz also im Allgemeinen

auflösbar seyn, so dürfen A und p kein gemeinschaftliches Maaß haben.

18. Ist nun p eine nicht in A aufgehende Primzahl, so läßt sich zeigen, daß alle die Congruenz

$$Ax + B \equiv C \text{ (Mod. p)}$$

auflösenden Zahlen, nach demselben Modulus unter einander congruent sind.

Seyen α, β irgend zwei Auflösungen unserer Congruenz, also

$$A\alpha + B \equiv C \text{ (Mod. p)}, \; A\beta + B \equiv C \text{ (Mod. p)};$$

so folgt durch Subtraction leicht

$$A(\alpha - \beta) \equiv 0 \text{ (Mod. p) (5.)}.$$

Also geht die Primzahl p in $A(\alpha - \beta)$, und folglich, weil sie in A nicht aufgeht, in $\alpha - \beta$ auf (I. β.), so daß also

$$\alpha \equiv \beta \text{ (Mod. p)}.$$

Für jede Congruenz des ersten Grades giebt es also, wenn p eine in A nicht aufgehende Primzahl ist, insofern immer nur eine Auflösung, als alle übrigen dieser congruent sind. Es ist merkwürdig, daß dieser Satz sich auf die Congruenzen aller Grade ausdehnen läßt, wie wir jetzt beweisen wollen.

19. Es ist bekanntlich

$$\frac{\alpha^n - \beta^n}{\alpha - \beta} = \alpha^{n-1} + \alpha^{n-2}\beta + \ldots + \alpha\beta^{n-2} + \beta_{n-1},$$

und folglich immer $\alpha^n - \beta^n$ durch $\alpha - \beta$ theilbar. Bezeichnen wir nun die Function $\frac{\alpha^n - \beta^n}{\alpha - \beta}$ überhaupt durch $\varphi(n-1)$; so läßt sich leicht zeigen, daß aus der Congruenz

$$A(\alpha^n - \beta^n) + B(\alpha^{n-1} - \beta^{n-1}) + \ldots + M(\alpha^2 - \beta^2) + N(\alpha - \beta) \equiv 0$$

für die Primzahl p als Modulus, wenn α und β nicht congruent sind, immer die Congruenz

$$A\varphi(n-1) + B\varphi(n-2) + \ldots + M\varphi(1) + N \equiv 0$$

folgt. Die gegebene Congruenz läßt sich nämlich offenbar so darstellen:

$$\{A\varphi(n-1) + B\varphi(n-2) + \ldots + M\varphi(1) + N\}(\alpha - \beta) \equiv 0,$$

so daß also p in dem Producte

$$\{A\varphi(n-1) + B\varphi(n-2) + \ldots + M\varphi(1) + N\}(\alpha - \beta)$$

aufgehen muß. Da nun α und β nicht congruent sind, so ist $\alpha - \beta$ durch p nicht, und folglich, weil p eine Primzahl ist, nach (I. 3.) der andere Factor durch p theilbar, d. i. in Bezug auf p als Modulus

$$A\varphi(n-1) + B\varphi(n-2) + \ldots + M\varphi(1) + N \equiv 0 .$$

20. Sey nun, wenn p eine in A nicht aufgehende Primzahl ist, in Bezug auf p als Modulus

$$Ax^n + Bx^{n-1} + Cx^{n-2} + \ldots + Mx + N \equiv 0 .$$

so läßt sich zeigen, daß es nicht mehr als n Auflösungen dieser Congruenz geben kann, welche, in Bezug auf p als Modulus, nicht unter einander congruent sind.

Es gebe $n + 1$ nicht unter einander congruente Auflösungen

$$x = \alpha, \beta, \gamma, \delta, \ldots \mu, \nu$$

der gegebenen Congruenz, so daß also

$$\begin{aligned}
&A\alpha^n + B\alpha^{n-1} + C\alpha^{n-2} + \ldots + M\alpha + N \equiv 0 ,\\
&A\beta^n + B\beta^{n-1} + C\beta^{n-2} + \ldots + M\beta + N \equiv 0 ,\\
&A\gamma^n + B\gamma^{n-1} + C\gamma^{n-2} + \ldots + M\gamma + N \equiv 0 ,\\
&\ldots\ldots\ldots\ldots\\
&A\mu^n + B\mu^{n-1} + C\mu^{n-2} + \ldots + M\mu + N \equiv 0 ,\\
&A\nu^n + B\nu^{n-1} + C\nu^{n-2} + \ldots + M\nu + N \equiv 0 .
\end{aligned}$$

Aus diesen $n + 1$ Congruenzen erhält man nach (5.) durch Subtraction unmittelbar die folgenden n neuen Congruenzen:

$$\begin{aligned}
&A(\alpha^n - \beta^n) + B(\alpha^{n-1} - \beta^{n-1}) + \ldots + M(\alpha - \beta) \equiv 0 ,\\
&A(\alpha^n - \gamma^n) + B(\alpha^{n-1} - \gamma^{n-1}) + \ldots + M(\alpha - \gamma) \equiv 0 ,\\
&\ldots\ldots\ldots\ldots\\
&A(\alpha^n - \mu^n) + B(\alpha^{n-1} - \mu^{n-1}) + \ldots + M(\alpha - \mu) \equiv 0 ,\\
&A(\alpha^n - \nu^n) + B(\alpha^{n-1} - \nu^{n-1}) + \ldots + M(\alpha - \nu) \equiv 0 ,
\end{aligned}$$

und hieraus ferner noch (19.)

$$\begin{aligned}
&A\frac{\alpha^n - \beta^n}{\alpha - \beta} + B\frac{\alpha^{n-1} - \beta^{n-1}}{\alpha - \beta} + \ldots + M \equiv 0 ,\\
&A\frac{\alpha^n - \gamma^n}{\alpha - \gamma} + B\frac{\alpha^{n-1} - \gamma^{n-1}}{\alpha - \gamma} + \ldots + M \equiv 0 ,\\
&\ldots\ldots\ldots\ldots\\
&A\frac{\alpha^n - \mu^n}{\alpha - \mu} + B\frac{\alpha^{n-1} - \mu^{n-1}}{\alpha - \mu} + \ldots + M \equiv 0 ,\\
&A\frac{\alpha^n - \nu^n}{\alpha - \nu} + B\frac{\alpha^{n-1} - \nu^{n-1}}{\alpha - \nu} + \ldots + M \equiv 0 .
\end{aligned}$$

Setzen wir nun

$$B' = A\alpha + B,$$
$$C' = A\alpha^2 + B\alpha + C,$$
$$D' = A\alpha^3 + B\alpha^2 + C\alpha + D,$$
$$\cdots\cdots\cdots$$
$$L' = A\alpha^{n-2} + B\alpha^{n-3} + C\alpha^{n-4} + \ldots + L,$$
$$M' = A\alpha^{n-1} + B\alpha^{n-2} + C\alpha^{n-3} + \ldots + L\alpha + M;$$

so verwandeln sich durch Entwickelung der Brüche obige Congruenzen in folgende:

$$A\beta^{n-1} + B'\beta^{n-2} + C'\beta^{n-3} + \ldots + L'\beta + M' \equiv o,$$
$$A\gamma^{n-1} + B'\gamma^{n-2} + C'\gamma^{n-3} + \ldots + L'\gamma + M' \equiv o,$$
$$\cdots\cdots\cdots\cdots$$
$$A\mu^{n-1} + B'\mu^{n-2} + C'\mu^{n-3} + \ldots + L'\mu + M' \equiv o,$$
$$A\nu^{n-1} + B'\nu^{n-2} + C'\nu^{n-3} + \ldots + L'\nu + M' \equiv o,$$

und es würde also auch für die Congruenz

$$Ax^{n-1} + B'x^{n-2} + C'^{n-3} + \ldots + L'x + M' \equiv o,$$

wo p eine nicht in A aufgehende Primzahl ist, n nicht unter einander congruente Auflösungen $\beta, \gamma, \delta, \ldots \mu, \nu$ geben. Gebe es also unter den Voraussetzungen des Satzes für eine Congruenz des nten Gerades $n+1$ nicht unter einander congruente Auflösungen, so würde es auch für eine Congruenz des $(n-1)$ten Grades n, also für eine Congruenz des $(n-2)$ten Grades $n-1$, u. s. f., für eine Congruenz des ersten Grades zwei untereinander nicht congruente Auflösungen geben, welches mit (8.) streitet. Unser Satz ist also bewiesen.

Ginge p in dem Coeficienten des ersten Gliedes, vielleicht auch noch in denen einiger folgenden Glieder, auf; so könnte man offenbar alle diese Glieder weglassen, wodurch die Congruenz auf einen niedrigern Grad reducirt würde, wo nun p nicht mehr in dem Coeficienten des ersten Gliedes aufgeht. Ginge p in den Coeficienten aller Glieder auf, so wäre die Congruenz identisch.

Einen andern Beweis dieses merkwürdigen und wichtigen Satzes giebt Gauß a. a. O. p. 38., Lagrange in den Mém. de Berlin. 1768. p. 192., Euler in den Nov. Comm. Petrop. XVIII. p. 93. für den besondern Fall $x^n - 1 \equiv o$, Legendre in den Mém. de l'Acad. de Paris. 1785. p. 466.

Sind q und q′ zwei zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ liegende Auflösungen unserer Congruenz; so ist offenbar immer, q und q′ mögen positiv oder negativ seyn, dem absoluten Werthe nach, $q-q' < p$, so daß also p nie in $q-q'$ aufgeht, d. h. nie $q \equiv q'$ ist. Also sind alle Auflösungen unserer Congruenz, welche zwischen den angegebenen Grenzen liegen, unter einander nicht congruent, und ihre Anzahl folglich nie $> n$. Legendre (Théorie des nombres. p. 169.) nennt daher vorzugsweise die zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ liegenden Auflösungen unserer Congruenz Wurzeln derselben, oder, wenn das gegebene Polynom durch P bezeichnet wird, und e überhaupt eine ganze Zahl bedeutet, Auflösungen oder Wurzeln der unbestimmten Gleichung $\frac{P}{p} = e$. Hat man eine dieser Wurzeln k gefunden, so genügt offenbar auch jede Zahl von der Form $x = k + pz$ dieser unbestimmten Gleichung, oder, was Dasselbe ist, obiger Congruenz, wovon man sich augenblicklich überzeugt, wenn man sich nur diesen Werth von x für x gesetzt, und die Potenzen nach dem binomischen Lehrsatze entwickelt denkt, indem dadurch augenscheinlich eine ebenfalls durch p theilbare Größe erhalten wird.

Sind q und q′ beide positiv, und $< p$, so ist auch immer $q-q' < p$, folglich $q-q'$ nicht durch p theilbar, d. i. nicht $q \equiv q'$. Also auch die Anzahl aller positiven Wurzeln unserer Congruenz, welche $< p$ sind, nie $> n$.

III. Fermat's und Wilsons Sätze von den Primzahlen.

1. Seyen a und p relative Primzahlen, und

$$(1), (2), (3), (4), \ldots (q)$$

alle Zahlen, welche mit p relative Primzahlen, und $< p$ sind; so können nie zwei Glieder der Reihe

$$(1)a, (2)a, (3)a, (4)a, \ldots (q)a;$$

in Bezug auf p als Modulus einander congruent seyn.

Wäre $(k)a \equiv (k')a$ (Mod. p), so wäre auch $\{(k) - (k')\}a \equiv o$ (Mod. p) (II. 5.); also

$\{(k) - (k')\}a$ durch p theilbar. Es ist aber a mit p relative Primzahl. Folglich muß $(k) - (k')$ durch p theilbar seyn (I. 7.). Dies ist aber unmöglich, da, wegen der Voraussetzung, offenbar $(k) - (k') < p$ ist.

Jeder bei der Division der Glieder obiger Reihe durch p bleibende Rest ist mit p relative Primzahl.

Sey z. B. $(k)a = pp' + r$, so ist r mit p relative Primzahl, weil, wenn p und r durch die Primzahl $\Theta > 1$ theilbar wären, diese Primzahl auch in $(k)a$, folglich entweder in (k) oder in a aufgehen müßte (I. 3.), also entweder (k) oder a, gegen die Voraussetzung, mit p nicht relative Primzahl wäre.

Da nun nicht zwei Glieder obiger Reihe in Bezug auf p einander congruent, also alle bei der Division derselben durch p bleibenden Reste ungleich, alle diese Reste aber $< p$ und mit p relative Primzahlen sind, ihre Anzahl aber $= q$ ist; so können diese Reste keine andern, als die Zahlen

$$(1), (2), (3), (4), \ldots (q)$$

seyn, ohne Rücksicht auf deren Ordnung in Bezug auf die obige Reihe.

Also sind immer zwei und zwei Glieder der Reihen

$$(1)a, (2)a, (3)a, (4)a, \ldots (q)a;$$
$$(1), (2), (3), (4), \ldots (q);$$

einander congruent, ohne Rücksicht auf die Ordnung, aber auch immer nur je zwei, da nach dem Obigen nie zwei Glieder der ersten Reihe einander congruent sind.

Folglich (II. 6.) ist auch

$$(1)(2)(3)\ldots(q).a^q \equiv (1)(2)(3)\ldots(q) \text{ (Mod. p)},$$
$$(1)(2)(3)\ldots(q).a^q - (1)(2)(3)\ldots(q) \equiv o \text{ (Mod. p)},$$
$$(1)(2)(3)\ldots(q)\{a^q - 1\} \equiv o \text{ (Mod. p)}.$$

Es ist aber p mit jedem Gliede der Reihe

$$(1), (2), (3), (4), \ldots (q)$$

relative Primzahl, und muß folglich, da es in

$$(1)(2)(3)\ldots(q)\{a^q - 1\}$$

aufgeht, in $a^q - 1$ aufgehen (I. 7.). In Worten läßt sich dieser Satz so aussprechen:

Wenn a und p relative Primzahlen sind, und q die Anzahl der Zahlen bezeichnet, welche $< p$ und mit p relative Primzahlen sind; so ist immer $a^q - 1$ durch p theilbar, oder $a^q \equiv 1$ (Mod. p).

Zerlegt man p in seine Primfactoren, so daß $p = \alpha^m \beta^n \gamma^h \ldots$ ist; so ist die Anzahl der Zahlen, welche $<$ p, und mit p relative Primzahlen sind, d. i. q,

$$= p\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right)\left(1 - \frac{1}{\gamma}\right) \ldots$$

$$= \alpha^{m-1}(\alpha - 1)\, \beta^{n-1}(\beta - 1)\, \gamma^{h-1}(\gamma - 1) \ldots$$

(Theiler einer Zahl. 14.); also immer

$$a^{\alpha^{m-1}(\alpha-1)\, \beta^{n-1}(\beta-1)\, \gamma^{h-1}(\gamma-1) \ldots} - 1$$

durch p theilbar.

Ist p selbst eine in a nicht aufgehende Primzahl, so sind offenbar

$$1, 2, 3, 4, 5, \ldots p - 1$$

Primzahlen zu p, und alle $< p$; in diesem Falle also $q = p - 1$, und folglich $a^{p-1} - 1$ durch p theilbar, oder $a^{p-1} \equiv 1$ (Mod. p), wenn, wie gesagt, p eine in a nicht aufgehende Primzahl ist.

Ist z. B. $p = 7$, $a = 12$; so ist $12^6 - 1 = 2985983$, $(12^6 - 1) : 7 = 426569$.

Diesen merkwürdigen, für die Zahlenlehre überaus wichtigen, Satz hat Fermat gefunden (Fermatii Opp. math. Tolosae. 1679. fol. p. 163.), aber einen Beweis nicht gegeben. Den ersten Beweis gab Euler (Comm. Petrop. T. VIII.), einen zweiten in den Comm. nov. Petrop. T. VII. p. 70. Mit letzterem stimmt der von Gauß (Disq. arithm. p. 50.) gegebene dem Wesentlichen nach überein; ersterer, welcher sich auf den binomischen Lehrsatz gründet, findet sich auch in der Théorie des nombres. p. 166. von Legendre. Auch Lambert hat einen ähnlichen Beweis gegeben (Act. Erud. 1769. p. 109.), und ein Beweis von Laplace wird gelegentlich mitgetheilt in Lacroix Traité du calc. diff. et int. T. III. p. 722. Zwei Beweise von Lejeune Dirichlet findet man in Crelles Journal. T. III.

S. 390. Mit dem zweiten, von Lejeune Dirichlet geführten, Beweise stimmt der hier gegebene dem Wesentlichen nach überein; es ist aber hier das Theorem zugleich zu größerer Allgemeinheit erhoben worden (Gauß a. a. O. p. 80.), wodurch seine Anwendung sehr erweitert wird. Auch Leibnitz soll einen Beweis gegeben haben, hat denselben aber nirgends bekannt gemacht; s. Gauß a. a. O. p. 46. in der Note. Mit dem Wilson'schen Theorem zugleich hat endlich auch Lagrange (Mém. de Berlin. 1771. p. 125—137.) den Satz bewiesen, wovon nachher weiter die Rede seyn wird.

Um eine Anwendung des erweiterten Fermat'schen Satzes zu geben, wählen wir eine Aufgabe aus den Annales de Math. T. XIX. p. 256.

Eine aus lauter Neunen und angehängten Nullen bestehende decadische Zahl zu finden, welche durch irgend eine gegebene Zahl theilbar ist.

Die gesuchte Zahl sey

$$\begin{aligned} Z &= \overset{(x)}{9}\ \overset{(x-1)}{9}\ \overset{(x-2)}{9} \ldots \overset{(1)}{9}\ \overset{(0)}{9}\ \overset{(1)}{0}\ \overset{(2)}{0} \ldots \overset{(y)}{0} \\ &= 9\{1 + 10 + 10^2 + \ldots + 10^x\}.10^y \\ &= 9.\frac{10^{x+1} - 1}{10 - 1}.10^y = (10^{x+1} - 1).10^y . \end{aligned}$$

Sey $p = 2^\mu . 5^\nu . \alpha^m \beta^n \gamma^h \ldots$, wo $\alpha, \beta, \gamma, \ldots$ ungleiche Primzahlen sind, welche weder $= 2$, noch $= 5$.

Setzen wir nun

$$x + 1 = \alpha^{m-1}(\alpha - 1)\ \beta^{n-1}(\beta - 1)\ \gamma^{h-1}(\gamma - 1) \ldots$$

so ist nach dem erweiterten Satze von Fermat, da 10 mit $\alpha^m \beta^n \gamma^h \ldots$ relative Primzahl ist, $10^{x+1} - 1$ durch $\alpha^m \beta^n \gamma^h \ldots$ theilbar. Ferner setze man,

1) wenn $\nu > \mu$, $\nu = \mu + \lambda$, also $2^\mu . 5^\nu = 10^\mu . 5^\lambda$ ist, $10^y = 10^\mu . 5^\lambda . 2^\lambda = 10^\mu . 10^\lambda = 10^{\mu+\lambda} = 10^\nu$, also $y = \nu$; so ist auch 10^y durch $10^\mu . 5^\lambda = 2^\mu . 5^\nu$ theilbar. Ist aber

2) $\mu > \nu$, $\mu = \nu + \lambda'$, $2^\mu . 5^\nu = 2^{\nu+\lambda'} . 5^\nu = 10^\nu . 2^{\lambda'}$; so setze man $10^y = 10^\nu . 2^{\lambda'} . 5^{\lambda'} = 10^\nu . 10^{\lambda'} = 10^{\nu+\lambda'} = 10^\mu$; so ist wieder 10^y durch $10^\nu . 2^{\lambda'} = 2^\mu . 5^\nu$ theilbar.

Bezeichnen wir also überhaupt die größere der beiden Zahlen μ, ν durch $M(\mu, \nu)$, so muß man $y = M(\mu, \nu)$ setzen, damit 10^y durch $2^\mu . 5^\nu$ theilbar werde.

Es ist also für

$$x = \alpha^{m-1}(\alpha-1)\,\beta^{n-1}(\beta-1)\,\gamma^{h-1}(\gamma-1) - 1\,,$$
$$y = M(\mu, \nu)\,,$$

immer Z durch $p = 2^\mu . 5^\nu . \alpha^m \beta^n \gamma^h \ldots$ theilbar, und es läßt sich also immer eine aus lauter Neunen und angehängten Nullen bestehende decadische Zahl finden, welche durch die willkührliche Zahl p theilbar ist.

Für $p = 2^2 . 5 . 7^3 . 11$ ist $x = 7^2 . 6 . 11^0 . 10 - 1 = 49 . 60 - 1 = 2940 - 1 = 2939$, $y = M(2, 1) = 2$, also Z bestimmt. Freilich ist in diesem Falle die Anzahl der Neunen sehr groß; aber auch p ist schon von beträchtlicher Größe.

2. Wenn p eine Primzahl ist; so ist immer

$$1 . 2 . 3 . 4 \ldots (p-1) \equiv -1 \ (\text{Mod. } p)\,;$$

oder

$$1 . 2 . 3 . 4 \ldots (p-1) + 1$$

durch p theilbar.

Gewöhnlich wird der Beweis dieses wichtigen Satzes aus dem Fermat'schen Satze mittelst eines Satzes aus der Differenzenrechnung abgeleitet, wovon nachher weiter die Rede seyn wird, oder es werden dabei Sätze von der Zahl der Auflösungen der unbestimmten Gleichungen oder der Congruenzen des zweiten Grades vorausgesetzt. Der Einmischung der Differenzenrechnung scheint die Zahlenlehre durchaus abhold zu seyn. Ich werde daher hier einen Beweis entwickeln, welcher, mit dem zweiten von Gauß a. a. O. p. 75. gegebenen zwar auf gleiches Princip sich stützend, doch von den dort angewandten Sätzen aus der unbestimmten Analytik, so wie von dem Fermat'schen Satze, völlig unabhängig ist, und bloß auf den einfachsten Sätzen von der Congruenz der Zahlen beruhet, die sich auch leicht in die gewöhnliche arithmetische Sprache übersetzen lassen würden. Wir schicken Alles voraus, was bei dem Beweise nöthig seyn dürfte.

1) p ist nach der Voraussetzung eine Primzahl, und liegt bei allen folgenden Congruenzen als Modulus zum Grunde.

2) Ist $q^2 \equiv 1$, so ist $q \equiv \pm 1$. Denn $q^2 - 1 \equiv 0$, $(q-1)(q+1) \equiv 0$ (II. 5.); also geht p in $(q-1)(q+1)$, und folglich, da es eine Primzahl ist, entweder in $q-1$, oder in $q+1$ (I. 3.) auf, so daß also $q \mp 1 \equiv 0$, $q \equiv \pm 1$ ist, immer für p als Modulus.

3) Ist also nicht $q \equiv \pm 1$, so kann auch nicht $q^2 \equiv 1$ seyn.

4) Wenn p' nicht $= 0$ ist; so können nie zwei Glieder der Reihe

$$p-p',\ 2(p-p'),\ 3(p-p'),\ \ldots\ (p-1)(p-p')$$

für p als Modulus einander congruent seyn.

Wäre $k(p-p') \equiv k'(p-p')$, wo $k < p$, $k' < p$ ist; so wäre auch $(k-k')(p-p') \equiv 0$, und folglich $(k-k')(p-p')$, also $k-k'$ oder $p-p'$, durch die Primzahl p theilbar (I. 3.), welches ungereimt ist, da $k-k' < p$, $p-p' < p$ ist.

5) Dividirt man folglich alle Glieder obiger Reihe durch p; so müssen die bleibenden Reste alle verschieden, und können also, da offenbar keiner $= 0$, ihre Anzahl $= p-1$ ist, alle aber $< p$ sind, keine andern als

$$1,\ 2,\ 3,\ 4,\ \ldots\ p-1$$

seyn, wenn nur von der Ordnung der Glieder dieser Reihe, in Bezug auf die vorhergehende, abstrahirt wird.

6) Also muß es in der Reihe

$$p-p',\ 2(p-p'),\ 3(p-p'),\ \ldots\ (p-1)(p-p')$$

immer ein Glied geben, welches $\equiv 1$ ist, aber auch nur eins, da nie zwei Glieder dieser Reihe einander congruent sind (4.).

7) Dieses Glied kann nicht $(p-p')(p-p') = (p-p')^2$ seyn, wenn nicht $p-p' \equiv \pm 1$ (2,), d. i., da p' immer $< p$, p' entweder $= p-1$, oder $= 1$ ist.

8) Auch kann dieses Glied, wenn p' weder $= p-1$, noch $= 1$ ist, weder $p-p'$, noch $(p-1)(p-p')$

seyn, weil im ersten Falle $p - p' \equiv 1$, $p \equiv p' + 1$, also $p' + 1$ durch p theilbar, und folglich $p' + 1 \equiv 0$, $p' \equiv -1$, $p' = p - 1$; im andern aber $(p - 1) . (p - p') \equiv 1$, $p(p - p') - (p - p') \equiv 1$, $p(p - p') \equiv p - p' + 1$, d. i. $p - p' + 1$ durch p theilbar, oder $p - p' + 1 \equiv 0$, $p \equiv p' - 1$, $p' - 1 \equiv 0$, $p' \equiv 1$, also $p' = 1$ seyn müßte. Man hat bei diesem Beweise nie zu vergessen, daß immer $p' < p$ ist.

9) Ist folglich p' irgend eine Zahl $< p$, nur nicht $= 1$, oder $= p - 1$; so ist in der Reihe

$$2(p-p'),\ 3(p-p'),\ \ldots.\ (p-2)(p-p')$$

immer ein Glied, welches $\equiv 1$, aber auch nur eins (6, 4,).

10) Auch kann, wenn p' und p'' ungleich sind, etwa $p'' > p'$ ist, nie $k(p - p') \equiv k(p - p'')$ seyn, weil sonst $k(p - p' - p + p'') \equiv 0$, d. i. $k(p'' - p') \equiv 0$, folglich $k(p'' - p)$, also entweder k oder $p'' - p$, durch die Primzahl p theilbar seyn müßte (I. 3.), welches ungereimt ist, da $k < p$, $p'' - p < p$ ist.

11) Aus allem Vorhergehenden erhellet nun deutlich, daß, wenn man der Zahl p' alle möglichen Werthe von 2 bis $p - 2$ giebt, oder überhaupt die Glieder der Reihe

$$2, 3, 4, 5, \ldots.\ p-2$$

betrachtet, es in dieser Reihe, deren Gliederzahl $= p - 3$, d. i. eine gerade Zahl ist, immer je zwei zusammengehörende Glieder geben muß, deren Product $\equiv 1$ ist, oder, wenn man mit Euler und Gauß überhaupt zwei solche Zahlen, deren Product der Einheit congruent ist, Socii oder Gefährten nennt, daß jedes Glied in obiger Reihe immer einen Socius in derselben haben muß, aber, wie sich aus den vorher bewiesenen Sätzen unmittelbar ergiebt, auch nur einen. Denkt man sich nun die $\frac{1}{2}(p - 3)$ Producte, deren jedes $\equiv 1$ ist, in einander multiplicirt; so erhält man offenbar das Product aller Glieder der Reihe

$$2, 3, 4, 5, \ldots.\ p-2;$$

und es ist folglich, da die einzelnen Producte alle $\equiv 1$ sind, nach (II. 6.), auch

$$2.3.4.5.6 \ldots (p-2) \equiv 1.$$

Da aber offenbar p in p aufgeht; so ist

$$1.(p-1)+1 \equiv 0,\ 1.(p-1) \equiv -1 \text{ (II. 5.)};$$

also, wenn man multiplicirt,

$$2.3.4.5 \ldots (p-2).1.(p-1) \equiv 1.(-1) \text{ (II. 6.)};$$

$$\text{d. i. } 1.2.3.4.5 \ldots (p-1) \equiv -1,$$

oder $1.2.3.4.5 \ldots (p-1)+1$ durch p theilbar, w. z. b. w.

3. Unter Voraussetzung des Fermat'schen Satzes und der Differenzenrechnung, oder der Lehre von den arithmetischen Reihen höherer Ordnungen, die aber der Zahlenlehre gewiß eben so fremd sind, wie das Binomialtheorem, läßt sich unser Satz auch auf folgende Art beweisen. Für $p-1=q$ ist

$$1.2.3.4 \ldots q =$$

$$q^q - \frac{q}{1}(q-1)^q + \frac{q(q-1)}{1.2}(q-2)^q - \frac{q(q-1)(q-2)}{1.2.3}(q-3)^q + \cdots$$

(Arithmetische Reihen höherer Ordnungen. 18. 23.). Diese Reihe bricht mit dem qten Gliede ab, da das (q+1)te

$$\frac{q(q-1)(q-2)\ldots 3.2.1}{1.2.3.4\ldots q}(q-q)^q.(-1)^q$$

schon $=0$ ist. Nach dem binomischen Lehrsatze ist

$$(1-1)^q = 1 - \frac{q}{1} + \frac{q(q-1)}{1.2} - \frac{q(q-1)(q-2)}{1.2.3} + \ldots,$$

eine Reihe mit $q+1$ Gliedern, deren letztes, da p eine Primzahl, also $q+1=p$, ungerade ist, vorausgesetzt, daß $p>2$ ist, $=+1$ ist. Zieht man nun die Reihe $(1-1)^q-1=-1$ von der ersten Reihe ab; so erhält man

$$1.2.3.4 \ldots q+1$$

$$= q^q - 1 - \frac{q}{1}\left\{(q-1)^q - 1\right\}$$

$$+ \frac{q(q-1)}{1.2}\left\{(q-2)^q - 1\right\}$$

$$- \frac{q(q-1)(q-2)}{1.2.3}\left\{(q-3)^q - 1\right\}$$

$$+ \ldots\ldots$$

Alle Binomialcoefficienten sind, da q eine positive ganze Zahl ist, positive ganze Zahlen, wie aus der Entstehung jeder Potenz eines Binomiums mit positivem ganzen Expo-

nenten augenblicklich erhellet; und nach dem Fermat'schen Satze ist $q + 1$ ein Theiler von

$$q^q - 1, (q-1)^q - 1, (q-2)^q - 1, (q-3)^q - 1, \ldots;$$

da $q + 1$ eine Primzahl, und keine der Zahlen q, $q-1$, $q-2$, $q-3$, ... durch $q + 1$ theilbar ist. Folglich ist offenbar auch

$$1.2.3 \ldots q+1 = 1.2.3 \ldots (p-1) + 1$$

durch $q + 1 = p$ theilbar, w. z. b. w. Für $p = 2$, $p = 1$ erhellet die Richtigkeit des Satzes von selbst, da $1.1 + 1$ und $1.0 + 1$ durch 2 und 1 theilbar ist.

Dieser in der Zahlenlehre sehr geschätzte Satz kommt zuerst in Waring Meditt. algebr. Ed. 3. p. 380., aber ohne Beweis, vor, und seine Erfindung wird einem gewissen John Wilson zugeschrieben. Zwei Beweise gab Lagrange in den Mém. de Berlin. 1771. p. 125 — 137. Der zweite, auch von Legendre aufgenommene (Théorie des nombres. p. 167.), ist im Wesentlichen mit dem oben zuletzt geführten einerlei, obgleich Lacroix (Traité du calc. diff. et int. T. III. p. 722.) seine Erfindung auch Laplace zuschreibt. Noch einen Beweis hat Euler gegeben (Opuscula analytica. T. I. p. 329.), mit welchem der erste bei Gauß (Disq. arithm. p. 74.) übereinkommt. Auch s. m. Crelles Journal a. a. O.

Der erste von Lagrange gegebene Beweis hat nicht nur manches Eigenthümliche, sondern macht den Satz zugleich auch allgemeiner, und verdient daher in seinen Grundzügen hier noch mitgetheilt zu werden.

Entwickelt man das Product

$$(x+1)(x+2)(x+3) \ldots (x+p-1)$$

nach Potenzen von x; so erhält man offenbar eine Reihe von der Form

$$x^{p-1} + A'x^{p-2} + A''x^{p-3} + \ldots + A^{(p-2)}x + A^{(p-1)},$$

wo alle Coefficienten ganze Zahlen sind, und offenbar

$$A^{(p-1)} = 1.2.3.4 \ldots (p-1)$$

ist. Setzt man nun $x + 1$ für x; so wird leicht die Richtigkeit folgender Gleichung erhellen:

$$(x+p)\{x^{p-1} + A'x^{p-2} + A''x^{p-3} + \ldots + A^{(p-1)}\}$$
$$= (x+1)\{(x+1)^{p-1} + A'(x+1)^{p-2} + A''(x+1)^{p-3} + \ldots + A^{(p-1)}\},$$

da offenbar jedes dieser beiden Producte

$$= (x+1)(x+2)(x+3) \ldots (x+p)$$

ist.

Entwickelt man nun diese beiden Producte nach Potenzen von x, und setzt die Coefficienten gleicher Potenzen von x einander gleich; so erhält man nach einigen leichten Reductionen, mit Anwendung der im Art. Wahrscheinlichkeitsrechnung (29.) gebrauchten Bezeichnung der Binomialcoefficienten, folgende Gleichungen:

$$A' = \left[\frac{p}{2}\right],$$
$$2A'' = \left[\frac{p}{3}\right] + \left[\frac{p-1}{2}\right]A',$$
$$3A''' = \left[\frac{p}{4}\right] + \left[\frac{p-1}{3}\right]A' + \left[\frac{p-2}{2}\right]A'',$$
$$\ldots\ldots\ldots\ldots$$
$$(p-1)A^{(p-1)} = \left[\frac{p}{p}\right] + \left[\frac{p-1}{p-1}\right]A' + \left[\frac{p-2}{p-2}\right]A'' + \ldots + \left[\frac{2}{2}\right]A^{(p-2)}.$$

Alle Binomialcoefficienten sind ganze Zahlen, und, weil p eine Primzahl ist, alle Binomial-Coefficienten der pten Potenz durch p theilbar. Denn es ist, vorausgesetzt, daß q nicht $= o$ ist,

$$\left[\frac{p}{p-q}\right] = \frac{p(p-1)(p-2)\ldots(q+1)}{1.2.3\ldots(p-q)} = e$$

eine ganze Zahl; also

$$(p-1)(p-2)\ldots(q+1) = \frac{1.2.3\ldots(p-q).e}{p}$$

eine ganze Zahl, so daß folglich die Primzahl p in $1.2.3\ldots(p-q).e$, und folglich, weil p offenbar in keinem Factor von $1.2.3\ldots(p-q)$ aufgeht, in e aufgehen muß, so daß also $\left[\frac{p}{p-q}\right]$ durch p theilbar, wenn q nicht $= o$ ist (I. 5.).

Also geht p in A', folglich auch in $2A''$, und demnach, weil $2 < p$ ist, auch in A'' auf (I. 5.); also, wegen der obigen Gleichungen, auch in $3A'''$, und folglich, weil $3 < p$, in A''', u. s. f., so daß also p in

$$A', A'', A''', A'''', \ldots A^{(p-2)}$$

aufgehen wird. Die Formel für $(p-1)A^{(p-1)}$ enthält aber das durch p nicht theilbare Glied $\left[\frac{p}{p}\right] = 1$, so daß also p in $(p-1)A^{(p-1)}$ nicht aufgeht. Es ist aber

$$pA^{(p-1)} - A^{(p-1)} = 1 + A' + A'' + A''' + \ldots + A^{(p-2)},$$
$$A^{(p-1)} + 1 = pA^{(p-1)} - A' - A'' - A''' - \ldots - A^{(p-2)},$$

woraus mittelst des Obigen folgt, daß p immer in $A^{(p-1)} + 1$ aufgehen muß. Es ist aber nach dem Obigen

$$A^{(p-1)} = 1.2.3.4 \ldots (p-1);$$

also geht p in $1.2.3.4 \ldots (p-1) + 1$ auf, welches der Wilsonsche Satz ist. Da aber

$$(x+1)(x+2)(x+3) \ldots (x+p-1) =$$
$$x^{p-1} + A'x^{p-2} + A''x^{p-3} + \ldots + A^{(p-2)}x + A^{(p-1)},$$
$$(x+1)(x+2)(x+3) \ldots (x+p-1) - x^{p-1} + 1 =$$
$$A'x^{p-2} + A''x^{p-3} + \ldots + A^{(p-2)}x + A^{(p-1)} + 1$$

ist; so erhellet aus dem Vorigen, daß die Primzahl p in

$$(x+1)(x+2)(x+3) \ldots (x+p-1) - x^{p-1} + 1$$

aufgeht, oder

$$(x+1)(x+2)(x+3) \ldots (x+p-1) - x^{p-1} + 1 \equiv 0$$

ist, welches der von Lagrange gefundene allgemeinere Satz ist.

Dies gilt für jedes x. Ist aber x weder $= 0$, noch durch p theilbar; so wird sich unter den Factoren des Products

$$(x+1)(x+2)(x+3) \ldots (x+p-1)$$

gewiß immer ein durch p theilbarer finden. Sey $x = py + \varrho$, wo ϱ, da p in x nicht aufgeht, nicht $= 0$ und $< p$ ist; ist nun $\varrho = p - p'$, wo $p' > 0$ und $< p$ ist, so ist $x = py + p - p'$, $x + p' = p(y+1)$, und folglich $x + p'$ ein durch p theilbarer Factor obigen Products. Ist also x nicht durch die Primzahl p theilbar; so ist das Product

$$(x+1)(x+2)(x+3) \ldots (x+p-1),$$

folglich, wegen obiger Congruenz, auch $-x^{p-1} + 1$ oder $x^{p-1} - 1$ durch p theilbar, welches der Fermat'sche Satz ist, so daß also durch diesen schönen Beweis nicht bloß der

Wilson'sche und Fermat'sche Satz, sondern auch noch ein allgemeinerer Satz, zugleich gerechtfertigt sind.

4. Ist p keine Primzahl, so ist

$$1.2.3.4 \ldots (p-1) + 1$$

nicht durch p theilbar. Sey $p = qq'$, wo weder q noch $q' = 1$, aber jeder dieser Factoren $< p$ ist, und sey obige Summe durch p theilbar, oder

$$\frac{1.2.3.4 \ldots (p-1) + 1}{qq'} = e,$$

eine ganze Zahl; so wäre auch

$$\frac{1.2.3.4 \ldots (p-1) + 1}{q} = eq'$$

eine ganze Zahl. Da aber $q < p$ ist, so kommt q unter den Factoren des Products

$$1.2.3.4 \ldots (p-1)$$

nothwendig vor, so daß also auch

$$\frac{1.2.3.4 \ldots (p-1)}{p} = e'$$

eine ganze Zahl, und folglich auch

$$\frac{1}{q} = eq' - e'$$

eine ganze Zahl, also $q = 1$ seyn müßte, welches gegen die Annahme.

5. Hieraus ergiebt sich eine allgemeine Methode, zu prüfen, ob irgend eine Zahl p eine Primzahl ist, oder nicht. Man bilde nämlich die Größe

$$1.2.3.4 \ldots (p-1) + 1;$$

so ist p eine Primzahl oder keine, jenachdem diese Größe durch p theilbar ist, oder nicht. In der Ausübung wird aber diese Methode, wenn p auch nur einigermaßen groß ist, sehr weitläufig. Durch eine weit fortgesetzte Tafel der Permutationszahlen (s. Versetzungen. 2.) würde sich aber, wie hieraus erhellet, leicht eine Tafel der Primzahlen bilden lassen.

6. Durch einfache Rechnung überzeugt man sich von der Richtigkeit folgender Gleichungen:

$$\frac{1^2.2.3\ldots(p-2)-1}{p}=1.2.3\ldots(p-2)-\frac{1.2.3\ldots(p-1)+1}{p},$$

$$\frac{1^2.2^2.3\ldots(p-3)-1}{p}=1^2.2.3\ldots(p-3)-\frac{1^2.2.3\ldots(p-2)-1}{p},$$

$$\frac{1^2.2^2.3^2.4\ldots(p-4)-1}{p}=1^2.2^2 3\ldots(p-4)-\frac{1^2.2^2.3\ldots(p-3)+1}{p},$$

$$\frac{1^2.2^2.3^2.4^2.5\ldots(p-5)+1}{p}=1^2.2^2.3^2.4\ldots(p-5)-\frac{1^2.2^2.3^2.4\ldots(p-4)-1}{p},$$

2c. 2c.

Hieraus folgt, von dem Wilson'schen Satze ausgehend, durch eine successive Schlußweise, daß die Primzahl p in jeder der folgenden Formeln, deren Gesetz in die Augen fällt, aufgehen muß:

$$1.2.3.4\ldots.(p-1)+1,$$
$$1^2.2.3.4\ldots.(p-2)-1,$$
$$1^2.2^2.3.4\ldots.(p-3)+1,$$
$$1^2.2^2.3^2.4\ldots.(p-4)-1,$$
$$1^2.2^2.3^2.4^2.5\ldots.(p-5)+1,$$
$$1^2.2^2.3^2.4^2.5^2.6\ldots.(p-6)-1,$$

2c. 2c.

Hierdurch kann die Prüfung, ob eine willkührliche Zahl p eine Primzahl ist, oder nicht, abgekürzt werden, indem sich mittelst (5.) leicht zeigen läßt, daß p, wenn es keine Primzahl ist, in keiner dieser Formeln aufgehen kann.

7. Für jedes q ist

$$1.2.3.4\ldots(p-q)=$$
$$1.2.3..(p-q-1).p-1.2.3\ldots(p-q-1).q;$$
$$1.2.3\ldots(p-q-1).p=$$
$$1.2.3.4\ldots(p-q)-\{-q.1.2.3..(p-q-1)\};$$

folglich, wenn wir das Product $1.2.3.4\ldots p$ überhaupt durch $\{p\}$ bezeichnen, immer in Bezug auf p als Modulus

$$\{p-q\}\equiv-q\{p-q-1\}.$$

Folglich, wenn man für q nach und nach $q, q+1, q+2, \ldots p-3, p-2$ setzt:

$$\{p-q\}\equiv\quad -q\{p-q-1\}$$
$$\{p-q-1\}\equiv-(q+1)\{p-q-2\}$$
$$\{p-q-2\}\equiv-(q+2)\{p-q-2\}$$
$$\ldots\ldots\ldots\ldots$$
$$\{2\}\equiv-(p-2)\{1\}$$
$$\{1\}\equiv-(p-1).$$

Die letzte Congruenz erhellet von selbst. Also durch Multiplication (II. 6.)

$$\{1\}\{2\}\ldots\{p-q-1\}\{p-q\}$$
$$\equiv q(q+1)(q+2)\ldots(p-1)\{1\}\{2\}\ldots\{p-q-1\}.(-1)^{p-q},$$

wo diese Potenz der negativen Einheit nur wegen des Vorzeichens beigefügt worden. Ist nun p eine Primzahl, so geht es in dem Producte

$$\{1\}\{2\}\{3\}\ldots\{p-q-1\},$$

wie leicht erhellet, nicht auf (I. 4.), und es ist folglich (II. 12.)

$$\{p-q\}\equiv q(q+1)(q+2)\ldots(p-1).(-1)^{p-q};$$

also auch, wenn man mit

$$1.2.3.4\ldots(q-1)=\{q-1\}$$

multiplicirt (II. 6.),

$$\{q-1\}\{p-q\}\equiv\{p-1\}.(-1)^{p-q}.$$

Setzen wir nun

$$q-1=\frac{p-1}{p},\ p-q=p-\frac{p-1}{2}-1=\frac{p-1}{2};$$

so erhält man sogleich

$$\left\{\frac{p-1}{2}\right\}^2\equiv\{p-1\}.(-1)^{\frac{p-1}{2}}.$$

Nach dem Wilson'schen Satze ist aber immer

$$\{p-1\}\equiv-1,\ \{p-1\}.(-1)^{\frac{p-1}{2}}\equiv-(-1)^{\frac{p-1}{2}}\ \text{(II. 6.)}.$$

Also auch (II. 3.)

$$\left\{\frac{p-1}{2}\right\}^2\equiv-(-1)^{\frac{p-1}{2}};$$

d. i. $\left\{\frac{p-1}{2}\right\}^2\equiv-1$, wenn $\frac{p-1}{2}$ eine gerade Zahl, oder p von der Form $4n+1$, und $\left\{\frac{p-1}{2}\right\}^2\equiv1$, wenn $\frac{p-1}{2}$ eine ungerade Zahl, oder von der Form $4n+3$ ist. In letztern Falle also auch immer (2.2,)

$$\left\{\frac{p-1}{2}\right\}\equiv\pm1;$$

d. h., wenn p eine Primzahl von der Form $4n+3$ ist, so ist immer

$$\text{entweder } \left\{\frac{p-1}{2}\right\} - 1 \text{ oder } \left\{\frac{p-1}{2}\right\} + 1$$

durch p theilbar.

Wenn p eine Primzahl von der Form $4n+3$ ist, so ist also immer

$$\left\{\frac{p-1}{2}\right\}^2 - 1^2$$

durch p theilbar, und man kann folglich in diesem Falle immer leicht zwei Quadrate angeben, deren Differenz durch p theilbar ist.

8. Wenn p eine Primzahl, Q ein Polynom von einem niedrigern Grade als p, und P irgend ein Polynom des nten Grades ist, welches in

$$x^{p-1} + pQ - 1$$

aufgeht; so giebt es immer n Werthe von x zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$, welche die Congruenz

$$P \equiv o \text{ (Mod. } p)$$

auflösen, oder das Polynom P durch p theilbar machen. Alle Coefficienten der beiden Polynomien sind, wie immer, ganze Zahlen.

Sey $x^{p-1} + pQ - 1 = PP'$; so ist P' ein Polynom vom Grade $p-n-1$. Nach dem Fermat'schen Satze ist $x^{p-1} - 1$, also auch $x^{p-1} + pQ - 1$ für folgende zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ liegende Werthe von x durch p theilbar:

$$\pm 1, \pm 2, \pm 3, \pm 4, \ldots \pm \frac{p-1}{2},$$

da p in keinem dieser Werthe aufgeht. Daß man diese Werthe auch negativ nehmen kann, fällt in die Augen. Ist nämlich $p > 2$, so ist $p-1$ eine gerade Zahl, und folglich x^{p-1} immer positiv. Für $p = 2$ gilt der Satz überhaupt nur dann, wenn man ± 1 als zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ liegende Werthe von x annimmt, indem für diese beiden Werthe entweder $x^{p-1} - 1 = o$, oder $x^{p-1} - 1 = -2$, also immer durch $p = 2$ theilbar ist. Die Anzahl der obigen Werthe ist im Allgemeinen $= p-1$, für $p = 2$ wenigsten nicht kleiner. Für alle diese Werthe von x geht also p in PP' auf, d. i., weil p eine Primzahl

ist, entweder in P, oder in P'. Nach (II. 20.) ist die Anzahl der Werthe von x zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$, welche die Congruenz $P \equiv o$ auflösen, oder P durch p theilbar machen, nicht $> n$. Wäre nun ihre Anzahl $< n$, z. B. $= n - m$, so würde es nach dem so eben Bewiesenen $p - 1 - (n - m) = p - n - 1 + m$ Werthe von x zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ geben, welche die Congruenz $P' \equiv o$ auflößen. Dies ist aber nicht möglich, da P' nur ein Polynom vom Grade $p - n - 1$ ist, und demnach nicht mehr als $p - n - 1$ Auflösungen der Congruenz $P' \equiv o$ zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ zulassen kann (II. 20.). Also ist unter den obigen Voraussetzungen die Anzahl der zwischen $-\frac{1}{2}p$ und $+\frac{1}{2}p$ liegenden Werthe von x, welche die Congruenz $P \equiv o$ auflösen, oder P durch p theilbar machen, weder $> n$, noch $< n$, d. i. $= n$, w. z. b. w.

9. Wenn p eine Primzahl ist, welche > 2 ist, und in a nicht aufgeht, für irgend einen Werth von x aber $x^2 \equiv a$ (Mod. p) ist; so ist immer

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p)}.$$

Nach der Voraussetzung ist

$$x^2 \equiv a, \text{ also } (x^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \text{ (Mod. p) (II. 8.)},$$

d. i.

$$x^{p-1} \equiv a^{\frac{p-1}{2}} \text{ (Mod. p)}.$$

Folglich auch

$$x^{p-1} - 1 \equiv a^{\frac{p-1}{2}} - 1 \text{ (Mod. p) (II. 5.)}.$$

Da nun p in a nicht aufgeht; so kann es, wegen der Congruenz $x^2 \equiv a$, immer für p als Modulus, auch in x^2 nicht aufgehen, weil, wegen dieser Congruenz, bei der Division von x^2 durch p, und a durch p, gleiche Reste bleiben müssen. Also geht auch offenbar p in x nicht auf, so daß also nach dem Fermat'schen Satze

$$x^{p-1} - 1 \equiv o \text{ (Mod. p)}.$$

Also nach dem Obigen auch

$$a^{\frac{p-1}{2}} - 1 \equiv 0 \text{ (Mod. p)}, \quad a^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p)}.$$

Es ist klar, daß a hier positiv und negativ seyn kann, da der Beweis offenbar für beide Fälle ohne Einschränkung gilt.

10. Ist p eine in a nicht aufgehende Primzahl > 2, und

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p)};$$

so muß es immer einen Werth von $x < \frac{1}{2}p$ geben, für welchen

$$x^2 \equiv a \text{ (Mod. p)}.$$

Da $a^{\frac{p-1}{2}} \equiv 1$ (Mod. p), so ist $a^{\frac{p-1}{2}} - 1$ durch p theilbar, und man kann folglich

$$a^{\frac{p-1}{2}} - 1 = \alpha p, \quad a^{\frac{p-1}{2}} = \alpha p + 1$$

setzen, wo α eine ganze Zahl bezeichnet. Da nach der Voraussetzung $p > 2$, also $p - 1$ eine gerade Zahl ist, und folglich $= 2q$ gesetzt werden kann; so ist

$$x^{p-1} - a^{\frac{p-1}{2}} = x^{p-1} - \alpha p - 1 = x^{2q} - a^q.$$

Aber

$$x^{2q} - a^q = (x^2 - a)\left\{x^{2q-2} + x^{2q-4}a + \ldots + x^2 a^{q-2} + a^{q-1}\right\}.$$

Also geht $x^2 - a$ in $x^{2q} - a^q$ auf, und es giebt folglich, da $x^2 - a$ vom zweiten Grade ist, und in $x^{p-1} - \alpha p - 1$ aufgeht, zwei Werthe von x, welche $< \frac{1}{2}p$ sind, für welche $x^2 - a \equiv 0$ (Mod. p), $x^2 \equiv a$ (Mod. p) (8.). Da diese beiden Werthe von x sich jedoch nur rücksichtlich des Zeichens unterscheiden (8.), und x^2 immer positiv ist; so fallen sie in einen zusammen.

11. Ist also, wenn p eine in a nicht aufgehende Primzahl > 2 ist, für keinen Werth von x die Größe $x^2 - a$ durch p theilbar, oder $x^2 \equiv a$ (Mod. p); so kann auch nicht

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p)},$$

oder $a^{\frac{p-1}{2}} - 1$ durch p theilbar seyn (10.). Nun ist aber

$$a^{p-1} - 1 = \left\{a^{\frac{p-1}{2}} - 1\right\}\left\{a^{\frac{p-1}{2}} + 1\right\},$$

und nach dem Fermat'schen Satze $a^{p-1} - 1$ durch p, nach dem so eben Bewiesenen aber $a^{\frac{p-1}{2}} - 1$ nicht durch p theilbar; also muß in diesem Falle $a^{\frac{p-1}{2}} + 1$ durch p theilbar, oder

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p)}$$

seyn (I. 3.).

12. Ist umgekehrt

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p)},$$

und p wie immer eine nicht in a aufgehende Primzahl > 2; so kann es keinen Werth von x geben, für welchen $x^2 - a$ durch p theilbar, oder

$$x^2 \equiv a \text{ (Mod. p)}$$

ist.

Wäre nämlich, für irgend einen Werth von x,

$$x^2 \equiv a \text{ (Mod. p)};$$

so wäre

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p) (9.)},$$

oder $a^{\frac{p-1}{2}} - 1$ durch p theilbar. Folglich könnte, da $p > 2$ ist, nicht $a^{\frac{p-1}{2}} - 1 + 2 = a^{\frac{p-1}{2}} + 1$ durch p theilbar, d. i. nicht

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p)}$$

seyn, wie doch angenommen wurde.

13. Ist demnach p eine nicht in a aufgehende Primzahl > 2, so geht p in $a^{\frac{p-1}{2}} - 1$ auf, oder es ist

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p)};$$

wenn es einen Werth von x giebt, für welchen p in $x^2 - a$ aufgeht, oder

$$x^2 \equiv a \text{ (Mod. p)}$$

ist (9.). Dagegen geht p in $a^{\frac{p-1}{2}} + 1$ auf, oder es ist

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p)},$$

wenn es keinen Werth von x giebt, für welchen $x^2 - a$ durch p theilbar, oder

$$x^2 \equiv a \text{ (Mod. p)}$$

ist (11.).

Nennen wir nun mit Gauß alle Zahlen, welche in Bezug auf eine gewisse Zahl als Modulus irgend einem Quadrate congruent werden können, wo sich also immer ein Quadrat finden läßt, welches, durch den Modulus dividirt, denselben Rest giebt, wie die Zahl selbst, durch den Modulus dividirt, quadratische Reste des Modulus; alle die Zahlen dagegen, bei denen es keine solche Beziehung giebt, nicht quadratische Reste des Modulus (residua quadratica und non residua quadratica); so läßt sich vorstehender höchst merkwürdiger Satz auch so ausdrücken:

Wenn p eine in a nicht aufgehende Primzahl > 2 ist; so ist immer

$$a^{\frac{p-1}{2}} \equiv \pm 1 \text{ (Mod. p)},$$

und das obere oder untere Zeichen zu nehmen, je nachdem a quadratischer Rest, oder nicht quadratischer Rest von p ist.

Auch erhellet aus dem Vorhergehenden unmittelbar die Richtigkeit folgender Sätze:

Ist p eine in a nicht aufgehende Primzahl > 2, so ist a quadratischer Rest oder nicht quadratischer Rest von p, je nachdem

$$a^{\frac{p-1}{2}} \equiv +1 \text{ Mod. p } (10.),$$

oder

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p) } (12.)$$

ist.

Um noch ein Beispiel zu der vorhergehenden wichtigen Theorie zu geben, so sey $p = 5$, $a = 9$. Dann ist

$$a^{\frac{p-1}{2}} = 9^2 = 81, \; a^{\frac{p-1}{2}} - 1 = 80;$$

also durch 5 theilbar, oder

$$a^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. 5)}.$$

Es ist aber auch, für $x = 3$, $x^2 - a = 9 - 9 = 0$ durch 5 theilbar. Für $a = 8$ dagegen wäre

$$a^{\frac{p-1}{2}} = 8^2 = 64, \; a^{\frac{p-1}{2}} + 1 = 65,$$

also durch 5 theilbar, oder

$$a^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. 5)}.$$

Also kann es keinen Werth von x geben, für welchen $x^2 - 8$ durch 5 theilbar, oder $x^2 \equiv 8$ (Mod. 5) ist. Ist a selbst ein Quadrat, so folgt aus dem Fermat'schen Satze leicht, daß immer $a^{\frac{p-1}{2}} \equiv 1$ (Mod. p), oder $a^{\frac{p-1}{2}} - 1$ durch p theilbar ist.

Nach dem Wilson'schen Theorem ist immer

$$1.2.3.4 \ldots (p-1) \equiv -1 \text{ (Mod. p)},$$

Also

$$1.2.3.4 \ldots (p-1) \equiv \mp a^{\frac{p-1}{2}} \text{ (Mod. p)},$$

und das obere oder untere Zeichen zu nehmen, je nachdem a quadratischer oder nicht quadratischer Rest von p ist.

Hier schließen wir nun einen der wichtigsten und merkwürdigsten Sätze der ganzen Zahlenlehre an.

IV. Der Satz von der Reciprocität, oder der Fundamentalsatz in der Lehre von den quadratischen Resten von Gauß und Legendre.

1. Wenn p eine Primzahl, a eine durch p nicht theilbare Zahl ist; so bezeichnet Legendre den bei der Division von $a^{\frac{p-1}{2}}$ durch p bleibenden Rest durch $\left(\frac{a}{p}\right)$. Mit Hülfe dieser Bezeichnung läßt der Satz von der Reciprocität sich so ausdrücken:

Wenn p, q zwei ungleiche ungerade Primzahlen sind; so sind, wenn p, q nicht beide von der Form $4n+3$ sind, die Reste $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$ entweder beide $= +1$, oder beide $= -1$; sind aber p, q beide von der Form $4n+3$; so ist immer der eine dieser beiden Reste $= +1$, der andere $= -1$. Im ersten Falle ist also immer $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, im andern $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Mittelst des Zeichens der Congruenz läßt sich dieser wichtige Satz so ausdrücken:

Wenn p, q zwei ungleiche ungerade Primzahlen sind; so ist, wenn nicht beide von der Form $4n+3$ sind, immer

$$p^{\frac{q-1}{2}} \equiv \pm 1 \text{ (Mod. q)}, \quad q^{\frac{p-1}{2}} \equiv \pm 1 \text{ (Mod. p)};$$

wenn aber beide von der Form $4n+3$ sind,

$$p^{\frac{q-1}{2}} \equiv \pm 1 \text{ (Mod. q)}, \quad q^{\frac{p-1}{2}} \equiv \mp 1 \text{ (Mod. p)}.$$

Daß beide Ausdrücke des Satzes einerlei sind, fällt in die Augen. Zum Beweise schicken wir folgendes Lemma voraus.

2. Wenn p irgend eine ungerade in a nicht aufgehende Primzahl ist; so wird ein Theil der bei der Division von

$$a,\ 2a,\ 3a,\ 4a,\ \ldots\ \frac{p-1}{2}a$$

durch p bleibenden Reste, deren jeder natürlich $< p$ ist, $< \frac{1}{2}p$, ein Theil dagegen $> \frac{1}{2}p$ seyn. Bezeichnen wir nun die Reste der ersten Art durch

$$\alpha_1, \alpha_2, \alpha_3\ \alpha_4, \ldots \alpha_\lambda;$$

die der andern durch

$$\beta_1, \beta_2, \beta_3, \beta_4, \ldots \beta_\mu;$$

so ist nach Legendre's Bezeichnung,

$$\left(\frac{a}{p}\right) = (-1)^\mu,$$

dieser Rest nämlich $= +1$, oder $= -1$, jenachdem μ gerade oder ungerade ist; oder, was dasselbe ist,

$$a^{\frac{p-1}{2}} \equiv (-1)^\mu \ (\text{Mod. } p).$$

Zuerst erhellet, daß die obigen Reste alle unter einander ungleich sind. Wären nämlich irgend zwei einander gleich, und folglich die entsprechenden Glieder der gegebenen Reihe, welche wir durch ka und k'a bezeichnen wollen, einander congruent, so daß

$$ka \equiv k'a \ (\text{Mod. } p)$$

wäre; so wäre auch

$$(k-k')\,a \equiv o \ (\text{Mod. } p);$$

folglich $(k-k')a$ durch die Primzahl p theilbar, welches aber nicht möglich ist, da sowohl a nach der Voraussetzung durch p nicht theilbar, als auch $k < \frac{1}{2}p$, $k' < \frac{1}{2}p$, $k - k' < \frac{1}{2}p$, und demnach ebenfalls durch p nicht theilbar ist (I. 2.).

Folglich sind auch die Differenzen

$$p-\beta_1, p-\beta_2, p-\beta_3, \ldots p-\beta_\mu$$

alle untereinander ungleich, und jede $< \frac{1}{2}p$, da die Reste

$$\beta_1, \beta_2, \beta_3, \beta_4, \ldots \beta_\mu$$

alle $> \frac{1}{2}p$ sind. Auch läßt sich leicht zeigen, daß keine dieser Differenzen einem der Reste

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots \alpha_\lambda$$

gleich ist. Seyen nämlich α und β zwei allgemeine Glieder der beiden in Rede stehenden Reihen von Resten, welche

respective den Gliedern ka und k'a der gegebenen Reihe entsprechen mögen; so erhellet leicht, daß

$$ka \equiv \alpha \text{ (Mod. p)}, \; k'a \equiv \beta \text{ (Mod. p)}.$$

Also

$$(k+k')a \equiv \alpha + \beta \text{ (Mod. p) (II. 4.)}.$$

Könnte nun $p - \beta = \alpha$, $p = \alpha + \beta$ seyen; so wäre

$$(k+k')a \equiv p \text{ (Mod. p)},$$

und folglich $(k+k')a$ durch p theilbar, welches unmöglich ist, da

$$k < \tfrac{1}{2}p, \; k' < \tfrac{1}{2}p, \; k + k' < p,$$

also, so wie nach der Voraussetzung auch a, durch die Primzahl p nicht theilbar ist. Also kann nie $p - \beta = \alpha$ seyn.

Da folglich alle Glieder der beiden Reihen

$$\alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots \alpha_\lambda;$$

$$p-\beta_1, p-\beta_2, p-\beta_3, p-\beta_4, \ldots p-\beta_\mu;$$

unter einander ungleich sind, jedes $< \frac{1}{2}p$, und ihre Anzahl überhaupt $= \lambda + \mu = \frac{1}{2}(p-1)$ ist; so können diese Größen keine andern, als

$$1, 2, 3, 4, 5, \ldots \frac{p-1}{2}$$

seyn, wenn nur von der Ordnung der einzelnen Glieder abstrahirt wird. Also ist

$$\alpha_1 \alpha_2 \alpha_3 \alpha_4 \ldots \alpha_\lambda (p-\beta_1)(p-\beta_2)(p-\beta_3)\ldots(p-\beta_\mu)$$
$$= 1.2.3.4.5 \ldots \left(\frac{p-1}{2}\right).$$

Denkt man sich das erste Product entwickelt; so erhält man, wenn x eine ganze Zahl bezeichnet, offenbar eine Gleichung von folgender Form:

$$px + \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_\lambda \beta_1 \beta_2 \beta_3 \ldots \beta_\mu . (-1)^\mu$$
$$= 1.2.3.4.5 \ldots \left(\frac{p-1}{2}\right),$$

woraus sich unmittelbar

$$1.2.3.4.5 \ldots \left(\frac{p-1}{2}\right)$$
$$\equiv \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_\lambda \beta_1 \beta_2 \beta_3 \ldots \beta_\mu . (-1)^\mu$$

ergiebt, immer für p als Modulus. Da aber die Differenzen zwischen den Größen

$$a, 2a, 3a, 4a, \ldots \frac{p-1}{2} a$$

und ihren entsprechenden Resten offenbar durch p theilbar, folglich diese Größen den entsprechenden Resten congruent sind; so ist (II. 6. 7.)

$$a.2a.3a.4a \ldots \frac{p-1}{2} a$$
$$\equiv \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_\lambda \beta_1 \beta_2 \beta_3 \ldots \beta_\mu,$$
$$a.2a.3a.4a \ldots \frac{p-1}{2} a.(-1)^\mu$$
$$\equiv \alpha_1 \alpha_2 \alpha_3 \ldots \alpha_\lambda \beta_1 \beta_2 \beta_3 \ldots \beta_\mu.(-1)^\mu;$$

also auch (II. 3.) nach dem Obigen

$$a.2a.3a.4a \ldots \frac{p-1}{2} a.(-1)^\mu \equiv 1.2.3.4 \ldots \left(\frac{p-1}{2}\right),$$

d. i. $1.2.3.4 \ldots \frac{p-1}{2}.a^{\frac{p-1}{2}}.(-1)^\mu \equiv 1.2.3.4 \ldots \left(\frac{p-1}{2}\right)$.

Da nun aber der Modulus p eine offenbar in

$$1.2.3.4 \ldots \left(\frac{p-1}{2}\right)$$

nicht aufgehende Primzahl ist; so ist, wenn man auf beiden Seiten mit diesem Producte dividirt nach (II. 12.)

$$a^{\frac{p-1}{2}}.(-1)^\mu \equiv 1,\ a^{\frac{p-1}{2}} (-1)^{2\mu} \equiv 1.(-1)^\mu \quad \text{(II. 7.)}$$

d. i., weil $(-1)^{2\mu}$ immer $= 1$ ist, $a^{\frac{p-1}{2}} \equiv (-1)^\mu$ (Mod. p), oder, nach Legendre's Bezeichnung, $\left(\frac{a}{p}\right) = (-1)^\mu$, d. h. der bei der Division von $a^{\frac{p-1}{2}}$ durch p bleibende Rest $= (-1)^\mu$, w. z. b. w.

3. Fermats Satz ist aus diesem Satze eine unmittelbare Folge. Da nämlich μ gerade und ungerade seyn kann, so wird nach dem Bewiesenen p immer entweder in

$$a^{\frac{p-1}{2}} + 1 \text{ oder in } a^{\frac{p-1}{2}} - 1,$$

folglich immer in

$$(a^{\frac{p-1}{2}}+1)(a^{\frac{p-1}{2}}-1)=a^{p-1}-1$$

aufgehen, welches der Fermat'sche Satz. Daß dieser Satz auch für $p=2$ gilt, erhellet leicht, da in diesem Falle $a^{p-1}-1=a-1$, also, da $p=2$ in a nach der Voraussetzung nicht aufgeht, $a^{p-1}-1$ eine gerade Zahl, und folglich durch $p=2$ theilbar ist.

4. Man bezeichne nun, wie schon im Artikel Theiler einer Zahl (17.), die größte in x enthaltene ganze Zahl durch $G(x)$, so daß also immer $x-G(x)$ ein positiver echter Bruch ist, welcher nur dann $=0$ wird, wenn x selbst eine ganze Zahl ist. ka und k'a seyen zwei beliebige Vielfache von a, und α, β die entsprechenden Reste, wobei übrigens Alles wie in (2.) bleibt; so ist nach dieser Bezeichnung

$$\frac{ka}{p}-G\left(\frac{ka}{p}\right)=\frac{\alpha}{p},\ \frac{k'a}{p}-G\left(\frac{k'a}{p}\right)=\frac{\beta}{p}.$$

Aber $\alpha<\frac{1}{2}p$, $\beta>\frac{1}{2}p$, jedoch $\beta<p$; also

$$\frac{ka}{p}-G\left(\frac{ka}{p}\right)<\tfrac{1}{2},\ \frac{k'a}{p}-G\left(\frac{k'a}{p}\right)\begin{matrix}>\frac{1}{2}\\<1\end{matrix};$$

$$\frac{2ka}{p}<2G\left(\frac{ka}{p}\right)+1,\ \frac{2k'a}{p}>2G\left(\frac{k'a}{p}\right)+1$$

$$<2G\left(\frac{k'a}{p}\right)+2.$$

Folglich, wie leicht erhellet,

$$G\left(\frac{2ka}{p}\right)=2G\left(\frac{ka}{p}\right),\ G\left(\frac{2k'a}{p}\right)=2G\left(\frac{k'a}{p}\right)+1;$$

$$G\left(\frac{2ka}{p}\right)-2G\left(\frac{ka}{p}\right)=0,\ G\left(\frac{2k'a}{p}\right)-2G\left(\frac{k'a}{p}\right)=1.$$

Eine Gleichung von der Art dieser beiden kann nun in Bezug auf jedes Vielfache von a in der Reihe in (2.) gebildet werden. Die Anzahl aller dieser Gleichungen ist $=\lambda+\mu$. Unter ihnen kommen λ vor, deren rechte Seite $=0$, dagegen μ, deren rechte Seite $=1$ ist, und durch Addition aller dieser Gleichungen erhält man also:

$$\left.\begin{matrix}G\left(\frac{2a}{p}\right)+G\left(\frac{4a}{p}\right)+G\left(\frac{6a}{p}\right)+\ldots+G\left(\frac{(p-1)a}{p}\right)\\-2G\left(\frac{a}{p}\right)-2G\left(\frac{2a}{p}\right)-2G\left(\frac{3a}{p}\right)-\ldots-2G\left(\frac{\frac{1}{2}(p-1)a}{p}\right)\end{matrix}\right\}=\mu.$$

Es kommt aber, wie auch schon aus (2.) erhellet, hier nicht sowohl auf den absoluten Werth von μ, sondern bloß darauf an, ob μ gerade oder ungerade ist, so daß man also in dieser Beziehung kürzer

$$G\left(\frac{2a}{p}\right) + G\left(\frac{4a}{p}\right) + G\left(\frac{6a}{p}\right) + \ldots + G\left(\frac{(p-1)a}{p}\right) = \mu$$

setzen kann, wodurch der Zweck, den wir hier im Auge haben, völlig erreicht wird. Um den wirklichen Werth von μ zu erhalten, müßte man sich freilich der unverkürzten Formel bedienen. Hat man μ, so ist auch λ gefunden, weil $\lambda + \mu = \frac{1}{2}(p-1)$ ist.

5. Unsere Formel ist aber noch einiger Abkürzungen fähig. Zu dem Ende ist zunächst zu bemerken, daß immer

$$G\left(\frac{(2k+1)a}{p}\right) + G\left(\frac{(p-2k-1)a}{p}\right) = a - 1$$

ist. Sey nämlich $a = mp + \Theta$; so erhält man leicht

$$\frac{(p-2k-1)a}{p} = mp + \Theta - (2k+1)m - \frac{(2k+1)\Theta}{p}$$

$$= a - (2k+1)m - \frac{(2k+1)\Theta}{p}$$

$$\frac{(2k+1)a}{p} = (2k+1)m + \frac{(2k+1)\Theta}{p}.$$

Setzt man nun

$$\frac{(2k+1)\Theta}{p} = G\left(\frac{(2k+1)\Theta}{p}\right) + \frac{\varrho}{p};$$

so wird

$$\frac{(p-2k-1)a}{p} = a - (2k+1)m - G\left(\frac{(2k+1)\Theta}{p}\right) - \frac{\varrho}{p}$$

$$= a - (2k+1)m - G\left(\frac{(2k+1)\Theta}{p}\right) - 1 + \frac{p-\varrho}{p},$$

$$\frac{(2k+1)a}{p} = (2k+1)m + G\left(\frac{(2k+1)\Theta}{p}\right) + \frac{\varrho}{p}.$$

Also, weil $\varrho < p$, $p - \varrho < p$ ist,

$$G\left(\frac{(p-2k-1)a}{p}\right) = a - 1 - (2k+1)m - G\left(\frac{(2k+1)\Theta}{p}\right),$$

$$\left(\frac{(2k+1)a}{p}\right) = (2k+1)m + G\left(\frac{(2k+1)\Theta}{p}\right),$$

woraus, wenn man addirt, die zu beweisende Formel augenblicklich folgt.

6. p kann, als eine ungerade Primzahl, nur von einer der beiden Formen $4n+1$, $4n+3$ seyn. Wir unterscheiden daher folgende zwei Fälle:

$$1)\ p = 4n + 1.$$

Die abgekürzte Reihe für μ in (4.) hat $\frac{1}{2}(p-1) = 2n$ Glieder. Die n ersten Glieder sind:

$$G\left(\frac{2a}{p}\right) + G\left(\frac{4a}{p}\right) + G\left(\frac{6a}{p}\right) + \ldots + G\left(\frac{2na}{p}\right);$$

die n letzten Glieder

$$\begin{aligned} G\left(\frac{(2n+2)a}{p}\right) + G\left(\frac{(2n+4)a}{p}\right) + G\left(\frac{(2n+6)a}{p}\right) \\ + \ldots + G\left(\frac{(p-1)a}{p}\right) \\ = \quad a - 1 - G\left(\frac{(2n-1)a}{p}\right) \\ + a - 1 - G\left(\frac{(2n-3)a}{p}\right) \\ + a - 1 - G\left(\frac{(2n-5)a}{p}\right) \\ \ldots\ldots\ldots\ldots \\ + a - 1 - G\left(\frac{a}{p}\right) \quad (\text{s. } 5.) \\ = n(a-1) - G\left(\frac{a}{p}\right) - G\left(\frac{3a}{p}\right) - G\left(\frac{5a}{p}\right) - \ldots \\ \ldots - G\left(\frac{(2n-1)a}{p}\right). \end{aligned}$$

Folglich, da $n = \frac{1}{4}.4n = \frac{1}{4}(p-1)$ ist,

$$\mu = \tfrac{1}{4}(p-1)(a-1) + G\left(\frac{2a}{p}\right) + G\left(\frac{4a}{p}\right) + G\left(\frac{6a}{p}\right) + \ldots + G\left(\frac{2na}{p}\right)$$
$$- G\left(\frac{a}{p}\right) - G\left(\frac{3a}{p}\right) - G\left(\frac{5a}{p}\right) - \ldots - G\left(\frac{(2n-1)a}{p}\right).$$

Da es aber, wie schon erinnert, bloß darauf ankommt, ob μ gerade oder ungerade ist; so kann man zu diesem Ausdrucke auch

$$2G\left(\frac{a}{p}\right) + 2G\left(\frac{3a}{p}\right) + 2G\left(\frac{5a}{p}\right) + \ldots + 2G\left(\frac{(2n-1)a}{p}\right)$$

addiren, wodurch man erhält:

$$\mu = \tfrac{1}{4}(p-1)(a-1) + G\left(\frac{a}{p}\right) + G\left(\frac{2a}{p}\right) + G\left(\frac{3a}{p}\right) + \ldots$$
$$\ldots + G\left(\frac{(2n-1)a}{p}\right) + G\left(\frac{2na}{p}\right),$$

ohne Rücksicht auf den wirklichen Werth von μ, immer nur in der Beziehung, ob μ gerade oder ungerade ist, worauf es hier allein ankommt.

2) $p = 4n + 3$.

Die abgekürzte Reihe für μ in (4.) hat $\frac{1}{2}(p-1) = 2n+1$ Glieder, also in diesem Falle immer ein Mittelglied. Die n ersten Glieder sind:

$$G\left(\frac{2a}{p}\right) + G\left(\frac{4a}{p}\right) + G\left(\frac{6a}{p}\right) + \ldots + G\left(\frac{2na}{p}\right);$$

das Mittelglied ist:

$$G\left(\frac{(2n+2)a}{p}\right);$$

die n letzten Glieder sind:

$$G\left(\frac{(2n+4)a}{p}\right) + G\left(\frac{(2n+6)a}{p}\right) + G\left(\frac{(2n+8)a}{p}\right) + \ldots + G\left(\frac{(p-1)a}{p}\right)$$
$$= a - 1 - G\left(\frac{(2n-1)a}{p}\right)$$
$$+ a - 1 - G\left(\frac{(2n-3)a}{p}\right)$$
$$+ a - 1 - G\left(\frac{(2n-5)a}{p}\right)$$
$$\ldots\ldots\ldots\ldots$$
$$+ a - 1 - G\left(\frac{a}{p}\right) \quad (\text{s. } 5.).$$

Transformirt man nun das Mittelglied auf ähnliche Art; so erhält man

$$G\left(\frac{(2n+2)a}{p}\right) = a - 1 - G\left(\frac{(2n+1)a}{p}\right);$$

und folglich, da die Anzahl der letzten Glieder, vom Mittelgliede an, $= n + 1 = \frac{1}{4}(p+1)$ ist:

$$\mu = \tfrac{1}{4}(p+1)(a-1) + G\left(\frac{2a}{p}\right) + G\left(\frac{4a}{p}\right) + G\left(\frac{6a}{p}\right) + \ldots + G\left(\frac{2na}{p}\right)$$
$$- G\left(\frac{a}{p}\right) - G\left(\frac{3a}{p}\right) - G\left(\frac{5a}{p}\right) - G\left(\frac{7a}{p}\right) - \ldots - G\left(\frac{(2n+1)a}{p}\right),$$

oder, wenn man wieder das doppelte der abgezogenen Reihe addirt, indem es bloß darauf ankommt, ob μ gerade oder ungerade ist,

$$\mu = \tfrac{1}{4}(lp+1)(a-1) + G\left(\frac{a}{p}\right) + G\left(\frac{2a}{p}\right) + G\left(\frac{3a}{p}\right) + \ldots$$
$$\ldots + G\left(\frac{2na}{p}\right) + G\left(\frac{(2n+1)a}{p}\right).$$

Ist a ungerade; so ist $a-1$, also auch, da $\frac{1}{4}(p-1)$ und $\frac{1}{4}(p+1)$ ganze Zahlen sind, $\frac{1}{4}(p\mp 1)(a-1)$ eine gerade Zahl, so daß also beide eben gefundenen Formeln auf

$$\mu = G\left(\frac{a}{p}\right) + G\left(\frac{2a}{p}\right) + G\left(\frac{3a}{p}\right) + \ldots + G\left(\frac{\frac{1}{2}(p-1)a}{p}\right)$$

reducirt werden können, weil für $p = 4n+1$, $p-1 = 4n$, $\frac{1}{2}(p-1) = 2n$, dagegen für $p = 4n+3$, $p-1 = 4n+2$, $\frac{1}{2}(p-1) = 2n+1$ ist. Ist a gerade, also $a-1$ ungerade; so ist $\frac{1}{4}(p\mp 1)(a-1)$ gerade oder ungerade, je nachdem $\frac{1}{4}(p\mp 1)$ gerade oder ungerade ist. Daher kann man in diesem Falle

$$\mu = \tfrac{1}{4}(p\mp 1) + G\left(\frac{a}{p}\right) + G\left(\frac{2a}{p}\right) + G\left(\frac{3a}{p}\right) + \ldots + G\left(\frac{\frac{1}{2}(p-1)a}{p}\right)$$

setzen, und das Zeichen ist immer so zu nehmen, daß $\frac{1}{4}(p\mp 1)$ eine ganze Zahl ist.

7. Sind nun p, q zwei ungleiche ungerade Primzahlen, die Einheit ausgeschlossen; so geht natürlich keine in der andern auf, und es ist folglich, wenn ν eine ähnliche Bedeutung hat, wie bisher μ, nach (2.) immer

$$q^{\frac{p-1}{p}} \equiv (-1)^{\mu} \text{ (Mod. p)}, \quad p^{\frac{q-1}{2}} \equiv (-1)^{\nu} \text{ (Mod. q)}.$$

Da p und q beide ungerade sind, so ist nach dem Vorhergehenden

$$\mu = G\left(\frac{q}{p}\right) + G\left(\frac{2q}{p}\right) + G\left(\frac{3q}{p}\right) + \ldots + G\left(\frac{\frac{1}{2}(p-1)q}{p}\right),$$

$$\nu = G\left(\frac{p}{q}\right) + G\left(\frac{2p}{q}\right) + G\left(\frac{3p}{q}\right) + \ldots + G\left(\frac{\frac{1}{2}(q-1)p}{q}\right),$$

$$\mu + \nu = G\left(\frac{q}{p}\right) + G\left(\frac{2q}{p}\right) + G\left(\frac{3q}{p}\right) + \ldots + G\left(\frac{\frac{1}{2}(p-1)q}{p}\right)$$
$$+ G\left(\frac{p}{q}\right) + G\left(\frac{2p}{q}\right) + G\left(\frac{3p}{q}\right) + \ldots + G\left(\frac{\frac{1}{2}(q-1)p}{q}\right),$$

d. h. nach dem Vorhergehenden nichts anders, als $\mu + \nu$ ist eine gerade oder ungerade Zahl, jenachdem die Größe auf der rechten Seite des Gleichheitszeichens gerade oder ungerade ist, indem es hier immer nur auf ein solches Kriterium ankommt.

Setzen wir nun

$$\frac{q}{p} = x,\ p = 2p' + 1,\ q = 2q' + 1,\ \frac{p}{q} = \frac{1}{x};$$

so erhält obige Formel folgende Gestalt:

$$\mu + \nu = G(x) + G(2x) + G(3x) + \ldots + G(p'x)$$
$$+ G\left(\frac{1}{x}\right) + G\left(\frac{2}{x}\right) + G\left(\frac{3}{x}\right) + \ldots + G\left(\frac{q'}{x}\right).$$

Zugleich wollen wir, welches offenbar, ohne der Allgemeinheit zu schaden, verstattet ist, annehmen, daß q die kleinere der beiden gegebenen Primzahlen p, q ist; so ist also x immer ein echter Bruch, und folglich $G(x) = 0$.

Ferner ist

$$p'x = \frac{p'q}{p} = \frac{\frac{1}{2}(p-1)(2q'+1)}{p} = \frac{2pq' - 2q' + p - 1}{2p}$$
$$= q' + \frac{p - (q-1) - 1}{2p} = q' + \frac{p-q}{2p}.$$

Folglich ist, weil nach der Annahme $p - q$ positiv und $< p$ ist, $G(p'x) = q'$. Hieraus, und aus dem Obigen sieht man nun, daß die Glieder der Reihe

$$Z = G(x) + G(2x) + G(3x) + \ldots + G(p'x)$$

von 0 bis q' wachsen. Um aber diese Glieder noch näher zu bestimmen, nehme man die Größen

$$m_1, m_2, m_3, m_4, \ldots m_{q'},$$

so an, daß

$$m_1 x = 1,\ m_2 x = 2,\ m_3 x = 3, \ldots m_{q'} x = q'$$

wird, welches offenbar immer möglich ist; so erhellet leicht, daß keiner dieser Factoren eine ganze Zahl seyn kann. Sey überhaupt

$$m_z x = z,\ m_z = \frac{z}{x} = z.\frac{1}{x} = \frac{pz}{q};$$

so geht, weil p eine Primzahl, und nach dem Vorhergehenden z höchstens $= q'$, also $< q$ ist, die Primzahl q weder in p, noch in z, also auch nicht in pz auf (I. 2.), so

daß also mz nie eine ganze Zahl seyn kann. Sey nun allgemein

$$G(m_z) = M_z; \text{ so ist}$$
$$m_z > M_z,\ m_z < M_z + 1;$$
$$m_z x > M_z x,\ m_z x < (M_z + 1)x;$$

d. i., da allgemein

$$m_z x = z$$

ist,

$$z > M_z x,\ z < (M_z + 1)x.$$

Also können die Glieder der Reihe

$$G(x),\ G(2x),\ G(3x),\ \ldots\ G(M_z x)$$

höchstens den Werth z — 1 haben. Dagegen erhellet auch leicht, daß

$$G((M_z + 1)x) = z$$

ist. Denn es ist

$$z > M_z x,\ z < (M_z + 1)x;$$

aber x ein echter Bruch; also $1 > x$, und folglich

$$z + 1 > M_z x + x,\ z + 1 > (M_z + 1)x.$$

Demnach

$$z < (M_z + 1)x,\ z + 1 > (M_z + 1)x;$$

also offenbar

$$G((M_z + 1)x) = z.$$

Aus dem Bisherigen ergiebt sich nun unmittelbar die Richtigkeit folgender Gleichungen:

$$G(x) = G(2x) = G(3x) = \ldots = G(M_1 x) = 0,$$
$$G((M_1 + 1)x) = G((M_1 + 2)x) = \ldots = G(M_2 x) = 1,$$
$$G((M_2 + 1)x) = G((M_2 + 2)x) = \ldots = G(M_3 x) = 2,$$
$$\ldots\ldots\ldots\ldots$$
$$G((M_{q'-1} + 1)x) = G((M_{q'-1} + 2)x) = \ldots = G(M_{q'} x) = q' - 1,$$
$$G((M_{q'} + 1)x) = G((M_{q'} + 2)) = \ldots = G(M_{q'+1} x) = q'.$$

Es ist aber

$$m_{q'+1} x = q' + 1,\ M_{q'+1} = G(m_{q'+1}).$$

Also

$$m_{q'+1} > M_{q'+1},\ m_{q'+1} < M_{q'+1} + 1;$$
$$m_{q'+1} x > M_{q'+1} x,\ m_{q'+1} x < (M_{q'+1} + 1)x;$$
$$q' + 1 > M_{q'+1} x,\ q' + 1 < (M_{q'+1} + 1)x;$$
$$M_{q'+1} < \frac{q' + 1}{x},\ M_{q'+1} + 1 > \frac{q' + 1}{x};$$
$$M_{q'+1} = G\left(\frac{q' + 1}{x}\right).$$

Aber

$$\frac{q'+1}{x} = p' + \frac{p+q}{2q},$$

wie leicht erhellen wird; und, da $p > q$, $p + q > 2q$ ist, $\frac{p+q}{2q}$ ein unechter Bruch; also

$$G\left(\frac{q'+1}{x}\right) > p', \; M_{q'+1} > p'.$$

Setzt man nun q' für $q' + 1$, so erhält man wie vorher

$$M_{q'} = G\left(\frac{q'}{x}\right).$$

Aber

$$\frac{q'}{x} = p' - \frac{p-q}{2q},$$

folglich, weil $p > q$, also $\frac{p-q}{2q}$ ein positiver Bruch ist,

$$G\left(\frac{q'}{x}\right) < p', \; M_{q'} < p'.$$

Also ist auch

$$M_{q'} + 1 \text{ nicht} > p'.$$

In der Reihe

$$M_{q'}+1, \; M_{q'}+2, \; M_{q'}+3, \; \ldots \; M_{q'+1}$$

ist also das niedrigste Glied nicht $> p'$, das höchste dagegen $> p'$; folglich muß in dieser Reihe immer ein Glied vorkommen, welches $= p'$ ist, so daß man also die letzte der obigen Reihen mit diesem Gliede abgebrochen denken, und statt jener Reihe kürzer

$$G((M_{q'}+1)x) = G((M_{q'}+2)x) = \ldots = G(p'x) = q'$$

schreiben kann. Dies vorausgesetzt, so ist die Anzahl der Glieder der obigen Reihen für jede einzeln nach der Ordnung

$$M_1, \; M_2 - M_1, \; M_3 - M_2, \; \ldots \; M_{q'} - M_{q'-1}, \; p' - M_{q'}.$$

Folglich, wenn man die obigen Reihen zu einander addirt, da

$$Z = G(x) + G(2x) + G(3x) + \ldots + G(p'x)$$

gesetzt worden ist,

$$\begin{aligned} Z = 0.M_1 &+ 1.(M_2 - M_1) \\ &+ 2.(M_3 - M_2) \\ &+ 3.(M_4 - M_3) \\ &\ldots\ldots\ldots \\ &+ (q'-1)\,(M_{q'} - M_{q'-1}) \\ &+ q'(p' - Mq') \\ = p'q' - M_1 - M_2 - M_3 &- \ldots - M_{q'-1} - M_{q'}. \end{aligned}$$

Aber überhaupt

$$M_z = G(mz) = G\left(\frac{z}{x}\right);$$

also

$$\begin{aligned} Z &= p'q' - G\left(\frac{1}{x}\right) - G\left(\frac{2}{x}\right) - G\left(\frac{3}{x}\right) - \ldots - G\left(\frac{q'}{x}\right) \\ &= G(x) + G(2x) + G(3x) + \ldots + G(p'x); \end{aligned}$$

$$\begin{aligned} p'q' = \; & G(x) + G(2x) + G(3x) + \ldots + G(p'x) \\ & + G\left(\frac{1}{x}\right) + G\left(\frac{2}{x}\right) + G\left(\frac{3}{x}\right) + \ldots + G\left(\frac{q'}{x}\right). \end{aligned}$$

Oben ist aber gefunden

$$\begin{aligned} \mu + \nu = \; & G(x) + G(2x) + G(3x) + \ldots + G(p'x) \\ & + G\left(\frac{1}{x}\right) + G\left(\frac{2}{x}\right) + G\left(\frac{3}{x}\right) + \ldots + G\left(\frac{q'}{x}\right); \end{aligned}$$

also ist, insofern es bloß darauf ankommt, ob $\mu + \nu$ gerade oder ungerade ist,

$$\mu + \nu = p'q' = \tfrac{1}{2}(p-1).\tfrac{1}{2}(q-1) = \tfrac{1}{4}(p-1)(q-1),$$

so daß also $\mu + \nu$ gleichzeitig mit $\frac{1}{4}(p-1)(q-1)$ gerade und ungerade ist.

8. Hieraus, in Verbindung mit dem bewiesenen Lemma, folgt unmittelbar der Satz von der Reciprocität. Nach diesem Lemma ist nämlich

$$p^{\frac{q-1}{2}} \equiv (-1)^{\nu} \text{ (Mod. } q), \quad q^{\frac{p-1}{2}} \equiv (-1)^{\mu} \text{ (Mod. } p).$$

Sind nun p, q beide von der Form $4n+1$, oder nur eine dieser beiden Primzahlen; so ist, da $\frac{1}{2}(4n+1-1) = 2n$ eine gerade Zahl ist, immer auch das Product

$$\tfrac{1}{2}(p-1).\tfrac{1}{2}(q-1) = \tfrac{1}{4}(p-1)(q-1),$$

d. i. nach dem Obigen $\mu + \nu$, eine gerade Zahl, so daß also μ und ν entweder beide gerade, oder beide ungerade, die Potenzen $(-1)^{\nu}$, $(-1)^{\mu}$ also entweder beide $= +1$, oder beide $= -1$ sind; also

$$p^{\frac{q-1}{2}} \equiv \pm 1 \text{ (Mod. } q), \; q^{\frac{p-1}{2}} \equiv \pm 1 \text{ (Mod. } p);$$

welches der erste Theil des Satzes von der Reciprocität ist.

Sind aber p, q beide von der Form

$$4n+3; \text{ so ist } \tfrac{1}{2}(4n+3-1) = 2n+1,$$

d. i. eine ungerade Zahl. Folglich ist auch

$$\tfrac{1}{2}(p-1)\tfrac{1}{2}(q-1) = \tfrac{1}{4}(p-1)(q-1),$$

da beide Factoren ungerade sind, eine ungerade Zahl, und folglich auch $\mu+\nu$ ungerade, d. i. immer eine der beiden Zahlen μ, ν gerade, die andere ungerade, folglich die Potenzen $(-1)^{\nu}$, $(-1)^{\mu}$ immer einander entgegengesetzt, und daher

$$p^{\frac{q-1}{2}} \equiv \pm 1 \text{ (Mod. } q), \; q^{\frac{p-1}{2}} \equiv \mp 1 \text{ (Mod. } p);$$

welches der zweite Theil des Satzes von der Reciprocität ist.

Da das Erste statt findet, wenn $\mu+\nu$ gerade, das Zweite, wenn $\mu+\nu$ ungerade ist; so lassen sich mit Anwendung der von Legendre gebrauchten Bezeichnung beide Fälle auf folgende Art zusammenfassen:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

9. Gauß hat in den Disq. arithm. p. 132. den Satz auf folgenden merkwürdigen Ausdruck gebracht:

Wenn p eine Primzahl von der Form $4n+1$ ist, so ist p; wenn aber p eine Primzahl von der Form $4n+3$ ist, so ist $-p$ quadratischer Rest oder nicht quadratischer Rest einer jeden Primzahl q, welche, positiv genommen, quadratischer Rest, oder nicht quadratischer Rest von p ist.

Sey zuerst p von der Form $4n+1$. Ist nun q eine Primzahl, welche quadratischer Rest von p ist; so muß es ein gewisses Quadrat geben, welches, für p als Modulus, $\equiv q$ ist, nach dem oben mitgetheilten Begriffe des quadratischen Restes. Folglich ist $q^{\frac{p-1}{2}} \equiv 1$ (Mod. p) (III. 9.). Also bei obiger Form von p nach dem Satze von der Re-

ciprocität $p^{\frac{q-1}{2}} \equiv 1$ (Mod. q). Folglich giebt es ein Quadrat, welchem p in Bezug auf q als Modulus congruent ist (III. 10.), d. i. p ist quadratischer Rest von q. Ist aber q nicht quadratischer Rest von p; so ist $q^{\frac{p-1}{2}} \equiv -1$ (Mod. p) (III. 11.); also nach dem Satze von der Reciprocität im vorliegenden Falle auch $p^{\frac{q-1}{2}} \equiv -1$ (Mod. q). Folglich p nicht quadratischer Rest von q (III. 12.).

Ferner sey p von der Form $4n+3$, und zuerst q von der Form $4n+1$. Ist q quadratischer Rest von p; so ist $q^{\frac{p-1}{2}} \equiv 1$ (Mod. p) (III. 9.). Also nach dem Satze von der Reciprocität in diesem Falle auch $p^{\frac{q-1}{2}} \equiv 1$ (Mod. q). Da aber $\frac{q-1}{2} = 2n$ eine gerade Zahl ist; so ist $p^{\frac{q-1}{2}} = (-p)^{\frac{q-1}{2}}$; also auch $(-p)^{\frac{q-1}{2}} \equiv 1$ (Mod. q). Folglich $-p$ quadratischer Rest von q (III. 10.). Ist q nicht quadratischer Rest von p; so ist $q^{\frac{p-1}{2}} \equiv -1$ (Mod. p) (III. 11.) Folglich nach dem Satze von der Reciprocität $p^{\frac{q-1}{2}} \equiv -1$ (Mod. q), und demnach, wie vorher, auch $(-p)^{\frac{q-1}{2}} \equiv -1$ (Mod. q). Also $-p$ nicht quadratischer Rest von q (III. 12.). Ist aber auch q von der Form $4n+3$, und zuerst quadratischer Rest von p; so ist $q^{\frac{p-1}{2}} \equiv 1$ (Mod. p) (III. 9.). Also in diesem Falle nach dem Satze von der Reciprocität $p^{\frac{q-1}{2}} \equiv -1$ (Mod. q). Da nun aber $\frac{q-1}{2} = 2n+1$ eine ungerade Zahl ist; so ist $(-p)^{\frac{q-1}{2}} = -p^{\frac{q-1}{2}}$; also eben so, wie $p^{\frac{q-1}{2}} + 1$ durch q theilbar ist, natürlich auch

$(-p)^{\frac{q-1}{2}} - 1$ durch q theilbar, d. i. $(-p)^{\frac{q-1}{2}} \equiv 1$ (Mod. q). Folglich $-p$ quadratischer Rest von q (III. 10.). Ist endlich q nicht quadratischer Rest von p; so ist $q^{\frac{p-1}{2}} \equiv -1$ (Mod. p) (III. 11.), und folglich nach dem Satze von der Reciprocität in diesem Falle $p^{\frac{q-1}{2}} \equiv 1$ (Mod. q). Also, ganz wie vorher, $(-p)^{\frac{q-1}{2}} \equiv -1$ (Mod. q), d. i. $-p$ nicht quadratischer Rest von q (III. 12.).

10. Unter vorstehender Gestalt macht der Satz die Grundlage der für die Zahlenlehre so wichtigen Theorie der quadratischen Reste. Unter der ersten Gestalt kommt er zuerst in Legendre Recherches d'Analyse indeterminée. Hist. de l'Ac. des Sc. 1785. p. 465. sqq. vor, aber nur mit einem unvollständigen Beweise versehen. Legendre nennt ihn den Satz von der Reciprocität. Unter der zweiten Form hat ihn Gauß in die Zahlenlehre eingeführt, und (a. a. O. Sect. IV. V.) auf doppelte Art streng bewiesen. Gauß nennt den Satz den Fundamentalsatz in der Lehre von den quadratischen Resten, und hat noch vier andere Beweise gegeben in den Abhandlungen: Summatio quarundam serierum singularium. Comm. Soc. Gotting. recent. Vol. I. und Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae. Gotting. 1818. In letzterer Abhandlung (p. 4.) führt Gauß als Grund seiner vielfältigen Bemühungen um diesen Satz auch den an, daß er dadurch zu einer zur Untersuchung der cubischen und biquadratischen Reste geschickten Methode zu gelangen geglaubt habe, welches ihm auch endlich gelungen sey. Die Resultate dieser für die Zahlenlehre höchst wichtigen Arbeit hat Gauß der Göttingischen Akademie der Wissenschaften vorgelegt, und in einer besondern Abhandlung bekannt gemacht. M. s. auch einige Bemerkungen von Jacobi über diesen wichtigen Gegenstand in Crelles Journal. II. 1. S. 66. Legendre hat den Satz in der Théorie des nombres. p. 198—

207; p. 386—393 auf doppelte Art bewiesen. Der erste Beweis ist, wie der Vf. selbst gesteht, nicht völlig genügend; der zweite gehört Gauß, und ist mit dem hier mitgetheilten im Ganzen übereinstimmend. Ich habe mich aber bemüht, diesen, des Scharfsinnes seines berühmten Erfinders völlig würdigen, Beweis so deutlich als möglich darzustellen, weshalb er nicht selten erläuternde Zusätze erhalten hat. Die Formeln, auf denen der Beweis vorzüglich beruht, gestatten auch noch manche andere wichtige Anwendungen, worüber wir nun noch Einiges mittheilen. Neuerlich hat auch Cauchy einen schönen Beweis dieses merkwürdigen Satzes gegeben, mit vielen wichtigen Anwendungen. M. s. Férussac Bulletin des sc. math. Septembre. 1829. p. 205.

11. -1 ist quadratischer Rest jeder Primzahl von der Form $4n+1$, nicht quadratischer Rest jeder Primzahl von der Form $4n+3$.

Sey $p = 4n+1$, $\frac{p-1}{2} = 2n$; so ist $(-1)^{2n}$; positiv, folglich $(-1)^{\frac{p-1}{2}} \equiv 1$ (Mod. p). Also -1 quadratischer Rest von $p = 4n+1$ (III. 10.). Ist aber $p = 4n+3$, $\frac{p-1}{2} = 2n+1$; so ist $(-1)^{2n+1}$ negativ, also $(-1)^{\frac{p-1}{2}} \equiv -1$ (Mod. p), und folglich -1 nicht quadratischer Rest von $p = 4n+3$ (III. 12.).

Man kann diesen Satz auch so ausdrücken: Wenn p eine Primzahl von der Form $4n+1$ ist; so giebt es immer ein Quadrat x^2, für welches x^2+1 durch p theilbar ist; ist aber p eine Primzahl von der Form $4n+3$; so giebt es kein Quadrat x^2, für welches x^2+1 durch p theilbar ist. Unter dieser Form haben Euler und Lagrange den Satz auf verschiedene Arten bewiesen; s. Gauß a. a. O. pp. 61. 108.

12. Setzen wir in (2.) $a = 2$; so ist a gerade; folglich, wenn in (6.) die Primzahl $p > 2$ angenommen wird, $\mu = \frac{1}{4}(p \mp 1)$, da

$$G\left(\frac{a}{p}\right) + G\left(\frac{2a}{p}\right) + \dots + G\left(\frac{\frac{1}{2}(p-1)a}{p}\right) =$$
$$= G\left(\frac{a}{p}\right) + G\left(\frac{2a}{p}\right) + \dots + G\left(\frac{p-1}{p}\right) = 0$$

ist. Es ist also μ mit $\frac{1}{4}(p \mp 1)$ gleichzeitig gerade und ungerade. Das zweideutige Zeichen muß wie in (6.) bestimmt werden. Sey nun

$$1,\ p = 8n + 1;\ \text{so ist}\ \tfrac{1}{4}(p-1) = 2n,$$

also auch μ, eine gerade Zahl. Folglich

$$2^{\frac{p-1}{2}} \equiv 1\ (\text{Mod. } p)\ (2.).$$

Aber auch $\frac{p-1}{2} = 4n$, eine gerade Zahl. Also auch

$$(-2)^{\frac{p-1}{2}} \equiv 1\ (\text{Mod. } p).$$

Demnach sowohl $+2$, als auch -2 ein quadratischer Rest von p (III. 10.).

$$2,\ p = 8n + 3,\ \tfrac{1}{4}(p+1) = 2n + 1,$$

μ ungerade; also

$$2^{\frac{p-1}{2}} \equiv -1\ (\text{Mod. } p)\ (2.).$$

Aber $\frac{p-1}{2} = 4n + 1$, ungerade; also $(-2)^{\frac{p-1}{2}} = -2^{\frac{p-1}{2}}$, und folglich, so wie $2^{\frac{p-1}{2}} + 1$ durch p theilbar ist, auch $(-2)^{\frac{p-1}{2}} - 1$ durch p theilbar, d. i.

$$(-2)^{\frac{p-1}{2}} \equiv 1\ (\text{Mod. } p).$$

Folglich $+2$ nicht quadratischer Rest von p (III. 12.); aber -2 quadratischer Rest von p (III. 10.).

$$3,\ p = 8n + 5,\ \tfrac{1}{4}(p-1) = 2n + 1,$$

μ ungerade, folglich

$$2^{\frac{p-1}{2}} \equiv -1\ (\text{Mod. } p)\ (2.).$$

Aber $\frac{p-1}{2} = 4n + 2$, gerade; also auch

$$(-2)^{\frac{p-1}{2}} \equiv -1\ (\text{Mod. } p).$$

Folglich sowohl $+2$, als auch -2, nicht quadratischer Rest von p.

$$4)\ p = 8n + 7,\ \tfrac{1}{4}(p+1) = 2n + 2,$$

μ gerade; also

$$2^{\frac{p-1}{2}} \equiv 1\ (\text{Mod. } p)\ (2.).$$

Aber $\frac{p-1}{2} = 4n + 3$, ungerade; also $(-2)^{\frac{p-1}{2}} = -2^{\frac{p-1}{2}}$, und folglich, so wie $2^{\frac{p-1}{2}} - 1$ durch p theilbar ist, auch $(-2)^{\frac{p-1}{2}} + 1$ durch p theilbar, d. i.

$$(-2)^{\frac{p-1}{2}} \equiv -1\ (\text{Mod. } p).$$

Folglich $+2$ quadratischer Rest von p (III. 10.), -2 nicht quadratischer Rest von p (III. 12.).

13. Setzen wir ferner $a = 3$; so ist, weil nun a ungerade, in (6.)

$$\mu = G\left(\frac{a}{p}\right) + G\left(\frac{2a}{p}\right) + G\left(\frac{3a}{p}\right) + \ldots + G\left(\frac{\frac{1}{2}(p-1)a}{p}\right)$$

zu setzen. Aber für $a = 3$

$$\frac{\frac{1}{2}(p-1)a}{p} = 1 + \frac{p-3}{2p},$$

$$\frac{(\frac{1}{2}(p-1)-1)a}{p} = 1 + \frac{p-9}{2p},$$

$$\frac{(\frac{1}{2}(p-1)-2)a}{p} = 1 + \frac{p-15}{2p},$$

$$\cdots\cdots\cdots$$

$$\frac{(\frac{1}{2}(p-1)-q)a}{p} = 1 + \frac{p-3-6q}{2p}.$$

Denkt man sich nun q so bestimmt, daß $p - 3 > 6q$, $p - 3 < 6(q+1)$ ist; so werden die zu der Einheit addirten Brüche in den folgenden Gliedern alle negativ, so daß also alle in diesen Gliedern enthaltenen Ganze $= 0$ sind, und folglich $\mu = q + 1$ ist. Sey nun p eine Primzahl, und

1) $p = 12n + 1$, $p - 3 = 12n - 2 = 6.(2n-1) + 4$. Also $q = 2n - 1$, $q + 1 = 2n$, und folglich μ eine gerade Zahl. Also

$$3^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p) (2.)}.$$

Aber $\frac{p-1}{2} = 6n$, eine gerade Zahl. Also auch

$$(-3)^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p)}.$$

Folglich sowohl $+3$ als -3 ein quadratischer Rest von p (III. 10.).

2) $p = 12n + 7$, $p - 3 = 12n + 4 = 6.2n + 4$, $q = 2n$, $q + 1 = 2n + 1$. Also μ eine ungerade Zahl. Folglich

$$3^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p) (2.)}.$$

Auch ist $\frac{p-1}{2} = 6n + 3$, eine ungerade Zahl, $(-3)^{\frac{p-1}{2}} = -3^{\frac{p-1}{2}}$. So wie nun $3^{\frac{p-1}{2}} + 1$ durch p theilbar, ist, so ist auch $(-3)^{\frac{p-1}{2}} - 1$ durch p theilbar, d. i.

$$(-3)^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p)}.$$

Demnach ist 3 nicht quadratischer Rest von p (III. 12.), aber -3 ist quadratischer Rest von p (III. 10.).

3) $p = 12n + 5$, $p - 3 = 12n + 2 = 6.2n + 2$, $q = 2n$, $q + 1 = 2n + 1$; also μ ungerade. Folglich

$$3^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p) (2.)}.$$

Aber $\frac{p-1}{2} = 6n + 2$, gerade. Also auch

$$(-3)^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p)}.$$

Folglich sowohl $+3$, als -3, nicht quadratischer Rest von p (III. 12.).

4) $p = 12n + 11$, $p - 3 = 12n + 8 = 6.(2n + 1) + 2$, $q = 2n + 1$, $q + 1 = 2n + 2$, μ gerade. Folglich

$$3^{\frac{p-1}{2}} \equiv 1 \text{ (Mod. p) (2.)}.$$

Aber $\frac{p-1}{2} = 6n + 5$, ungerade; also $(-3)^{\frac{p-1}{2}} = -3^{\frac{p-1}{2}}$. So wie nun $3^{\frac{p-1}{2}} - 1$ durch p theilbar ist, so ist auch $(-3)^{\frac{p-1}{2}} + 1$ durch p theilbar, d. i.

$$(-3)^{\frac{p-1}{2}} \equiv -1 \text{ (Mod. p)}.$$

Folglich + 3 quadratischer Rest von p (III. 10.), — 3 nicht quadratischer Rest von p (III. 12.).

14. Bei größeren Primzahlen wird die Untersuchung natürlich weitläufiger, läßt sich jedoch immer ausführen. Sey z. B. a = 5; so ist

$$\frac{\frac{1}{2}(p-1)a}{p} = 2 + \frac{p-5}{2p},$$
$$\frac{(\frac{1}{2}(p-1)-1)a}{p} = 2 + \frac{p-15}{2p},$$
$$\frac{(\frac{1}{2}(p-1)-2)a}{p} = 2 + \frac{p-25}{2p},$$
$$\cdots\cdots\cdots\cdots$$
$$\frac{(\frac{1}{2}(p-1)-q)a}{p} = 2 + \frac{p-5-10q}{2p},$$
$$\frac{(\frac{1}{2}(p-1)-(q+1))a}{p} = 1 + \frac{3p-5-10(q+1)}{2p},$$
$$\frac{(\frac{1}{2}(p-1)-(q+2))a}{p} = 1 + \frac{3p-5-10(q+2)}{2p},$$
$$\cdots\cdots\cdots\cdots$$
$$\frac{(\frac{1}{2}(p-1)-(q+q'))a}{p} = 1 + \frac{3p-5-10(q+q')}{2p}.$$

Nehmen wir also q und q′ so, daß

$$p-5 > 10q,\ p-5 < 10(q+1);$$
$$3p-5 > 10(q+q'),\ 3p-5 < 10(q+q'+1);$$
$$3p-5-10q > 10q',\ 3p-5-10q < 10(q'+1);$$

ist; so werden alle folgenden zu der Einheit addirten Brüche negativ, und folglich $\mu = 2(q+1) + q'$ (6.), also, da es bloß auf ein Kriterium ankommt, ob μ gerade oder ungerade ist, $\mu = q'$.

Sey nun z. B. die Primzahl p von der Form $20n + 11$; so ist $p - 5 = 20n + 6 = 10.2n + 6$, $q = 2n$, $3p - 5 = 60n + 28$, $3p - 5 - 10q = 40n + 28 = 10.(4n + 2) + 8$, $q' = 4n + 2$; also μ gerade, und folglich

$$5^{\frac{p-1}{2}} \equiv 1\ (2.).$$

Aber $\frac{p-1}{2} = 10n + 5$. Also $(-5)^{\frac{p-1}{2}} = -5^{\frac{p-1}{2}}$, und es ist folglich, so wie $5^{\frac{p-1}{2}} - 1$ durch p theilbar ist, auch $(-5)^{\frac{p-1}{2}} + 1$ durch p theilbar, d. i.

$$(-5)^{\frac{p-1}{2}} \equiv -1.$$

Folglich $+5$ quadratischer Rest, -5 nicht quadratischer Rest von $p = 20n + 11$.

Für $p = 20n + 17$ ist $p - 5 = 20n + 12 = 10.(2n + 1) + 2$, $q = 2n + 1$, $3p - 5 = 60n + 46$, $3p - 5 - 10q = 40n + 36 = 10.(4n + 3) + 6$, $q' = 4n + 3$, μ ungerade. Also

$$5^{\frac{p-1}{2}} \equiv -1\ (2.).$$

$\frac{p-1}{2} = 10n + 8$ ist gerade. Also

$$(-5)^{\frac{p-1}{2}} \equiv -1.$$

Folglich weder $+5$ noch -5 quadratischer Rest von $p = 20n + 17$.

Für $p = 20n + 1$ ist $p - 5 = 20n - 4 = 10.(2n - 1) + 6$, $q = 2n - 1$, $3p - 5 = 60n - 2$, $3p - 5 - 10q = 40n + 8 = 10.4n + 8$, $q' = 4n$, $\frac{p-1}{2} = 10n$. Also sowohl μ als $\frac{p-1}{2}$ gerade. Folglich

$$5^{\frac{p-1}{2}} \equiv 1\ (2.),\quad (-5)^{\frac{p-1}{2}} \equiv 1.$$

Demnach $+5$ und -5 quadratischer Rest von $p = 20n + 1$.

Ganz auf ähnliche Weise kann man alle Formen

$$p = 20n + 1, +3, +7, +9, +11, +13, +17, +19;$$

untersuchen.

15. Sowohl ± 3, als auch ± 5, so wie überhaupt jede Primzahl p ist quadratischer Rest von 2, da offenbar $1^2 \mp p$ durch 2 theilbar ist. Eben so ist jede Zahl $\pm x$ quadratischer Rest von sich selbst, da offenbar $x^2 \mp x$ durch x theilbar ist. Also ist ± 3 quadratischer Rest von 3, ± 5 quadratischer Rest von 5.

In Bezug auf die quadratischen Reste der zusammengesetzten Zahlen beweisen wir noch folgende Sätze.

16. Wenn p eine Primzahl > 2 ist, die in a nicht aufgeht; so ist a quadratischer Rest, oder nicht quadratischer Rest von p^n, jenachdem a quadratischer Rest oder nicht quadratischer Rest von p ist.

Ist a quadratischer Rest von p; so giebt es ein Quadrat α^2, für welches $\alpha^2 - a$ durch p theilbar, oder $\alpha^2 \equiv a$ (Mod. p) ist. Um ein Quadrat zu finden, welches $\equiv a$ (Mod. p^n) ist, wollen wir überhaupt $\alpha^2 \equiv a$ (Mod. p^m) setzen, wobei wir annehmen, daß $n > m$, aber nicht $> 2m$. Die Wurzel des gesuchten Quadrats sey $\pm \alpha + p^m x$, so daß also

$$\alpha^2 \pm 2\alpha p^m x + p^{2m} x^2 \equiv a \text{ (Mod. } p^n),$$

oder, weil n nicht $> 2m$, also $p^{2m} x^2$ durch p^n theilbar ist, offenbar

$$\alpha^2 \pm 2\alpha p^m x \equiv a \text{ (Mod. } p^n);$$
$$a - \alpha^2 \equiv \pm 2\alpha p^m x \text{ (Mod. } p^n).$$

Da nun $\alpha^2 \equiv a$ (Mod. p^m); so ist $a - \alpha^2$ durch p^m theilbar, und man kann also $a - \alpha^2 = p^m q$ setzen, woraus

$$p^m q \equiv \pm 2\alpha p^m x \text{ (Mod. } p^n).$$

Also auch, da p^m und p^n das größte gemeinschaftliche Maaß p^m haben, nach (II. 14.)

$$q \equiv \pm 2\alpha x \text{ (Mod. } p^{n-m}).$$

Man muß also x so bestimmen, daß $q \mp 2\alpha x$ durch p^{n-m} theilbar wird, und hat folglich die unbestimmte Gleichung des ersten Grades

$$q \mp 2\alpha x = p^{n-m} y, \; q = p^{n-m} y \pm 2\alpha x$$

aufzulösen. Die Auflösung dieser Gleichung in ganzen Zahlen ist aber jederzeit möglich. Denn nach der Voraussetzung ist die Primzahl $p > 2$, und geht in $\alpha^2 - a$ auf, müßte also, wenn sie in α oder α^2 aufginge, auch in a aufgehen, welches gegen die Voraussetzung ist, so daß also p und 2α offenbar relative Primzahlen sind. Die Größe x kann also immer bestimmt werden (M. v. d. Art. Unbestimmte Analytik. 1.). So wie man hier von p^m zu p^n überging, wo n nicht $> 2m$; so kann man von p zu p^2, von p^2 zu p^4, von p^4 zu p^8 übergehen, u. s. f., so daß also überhaupt a quadratischer Rest von p^n ist, wenn a quadratischer Rest von p ist. Ist aber α nicht quadratischer Rest von p, so kann auch a nicht quadratischer Rest von p^n seyn, weil, wenn p^n in $z^2 - a$ aufginge, offenbar auch p in $z^2 - a$ aufgehen, und folglich a quadratischer Rest von p seyn würde.

17. Geht p in a auf, so daß $a = p^\alpha a'$, wo a' nicht mehr durch p theilbar ist; so muß man drei Fälle unterscheiden:

1) Wenn $\alpha =$ oder $> n$ ist; so ist offenbar a durch p^n theilbar; also $a \equiv o^2$ (Mod. p^n), d. i. a quadratischer Rest von p^n.

2) Ist $\alpha < n$ und ungerade, $= 2\gamma + 1$; so ist a nicht quadratischer Rest von p^n.

Wäre nämlich $x^2 \equiv a \equiv p^{2\gamma+1} a'$ (Mod. p^n); so wäre $x^2 - p^{2\gamma+1} a'$ durch p^n, also auch, da $2\gamma + 1 < n$ ist, durch $p^{2\gamma+1}$ theilbar. Folglich wäre auch x^2 durch $p^{2\gamma+1}$, und also x durch $p^{\gamma+1}$ theilbar, weil, wenn x bloß durch die Potenz $p^{\gamma+1-\delta}$ theilbar wäre, auch x^2 bloß durch die Potenz $p^{2\gamma+1-(2\delta-1)}$ theilbar seyn würde. Demnach müßte also auch x^2 durch $p^{2\gamma+2}$, und, da $2\gamma + 2$ nicht $> n$ ist, auch $p^{2\gamma+1} a'$ durch $p^{2\gamma+2}$, d. i. a' durch p theilbar seyn, welches gegen die Annahme. Also ist a nicht quadratischer Rest von p^n.

3) Ist $\alpha < n$ und gerade; so ist a quadratischer Rest, oder nicht quadratischer Rest von p^n, jenachdem a' quadratischer Rest, oder nicht quadratischer Rest von p ist.

Ist nämlich a' quadratischer Rest von p; so ist es auch quadratischer Rest von $p^{n-\alpha}$ (16.). Setzen wir nun $x^2 \equiv a'$ (Mod. $p^{n-\alpha}$); so geht $p^{n-\alpha}$ in $x^2 - a'$, also auch p^n in $p^\alpha x^2 - p^\alpha a'$ auf, oder es ist $p^\alpha x^2 \equiv p^\alpha a' \equiv a$ (Mod. p^n), d. i., weil $p^\alpha x^2$ ein Quadrat ist, a quadratischer Rest von p^n. Ist aber a' nicht quadratischer Rest von p, so kann auch $a = p^\alpha a'$ nicht quadratischer Rest von p^n seyn. Wäre nämlich $x^2 \equiv p^\alpha a'$ (Mod. p^n); so ist, weil $\alpha < n$, $x^2 - p^\alpha a'$, also auch x^2 durch p^α theilbar, und folglich, für $\alpha = 2\gamma$, $\left(\frac{x}{p^\gamma}\right)^2$ eine ganze Zahl. Da nun $x^2 - p^{2\gamma} a'$ durch p^n theilbar ist; so ist offenbar auch $\left(\frac{x}{p^\gamma}\right)^2 - a'$ durch $p^{n-2\gamma}$, also um so mehr $\left(\frac{x}{p^\gamma}\right)^2 - a'$ durch p theilbar, d. i. $\left(\frac{x}{p^\gamma}\right)^2 \equiv a'$ (Mod. p), oder a' quadratischer Rest von p, gegen die Voraussetzung. Folglich ist a nicht quadratischer Rest von p^n.

18. Der Werth $p = 2$ ist vorher ausgeschlossen worden. Wir müssen also für denselben noch einige Bestimmungen beifügen.

1) Jede Zahl ist ein quadratischer Rest von 2. Denn es erhellet leicht, daß $(2x)^2 \mp 2\alpha$, $(2x+1)^2 \mp (2\alpha+1)$ durch 2 theilbar, also

$$(2x)^2 \equiv \pm 2\alpha \text{ (Mod. 2)}, \quad (2x+1)^2 \equiv \pm (2\alpha+1) \text{ (Mod. 2)};$$

d. i. $\pm 2\alpha$ und $\pm (2\alpha+1)$ ein quadratischer Rest von 2 ist.

2) Jede ungerade Zahl von der Form $4\alpha + 1$ ist quadratischer Rest, jede ungerade Zahl von der Form $4\alpha + 3$ nicht quadratischer Rest von $2^2 = 4$.

Denn $(2x+1)^2$ ist von der Form $4y + 1$, also offenbar $(2x+1)^2 \equiv 4\alpha + 1$ (Mod. 4), oder $4\alpha + 1$ quadratischer Rest von 4. Daß $4\alpha + 3$ keinem geraden Quadrate in Bezug auf den Modulus 4 congruent seyn kann, versteht sich von selbst. Eben so wenig kann aber auch $(2x+1)^2 \equiv 4\alpha + 3$ (Mod. 4) seyn, da $(2x+1)^2 - (4\alpha+3)$ offenbar von der Form $4(y-\alpha) - 2$, also nicht durch 4 theilbar ist. Folglich ist $4\alpha + 3$ nicht quadratischer Rest von 4.

3) $8\alpha + 1$ ist immer ein quadratischer Rest von $2^3 = 8$. Denn $(4x + 1)^2$ ist von der Form $8y + 1$, also offenbar $(4x + 1)^2 - (8\alpha + 1)$ durch 8 theilbar, d. i. $(4x + 1)^2 \equiv 8\alpha + 1$ (Mod. 8), oder $8\alpha + 1$ quadratischer Rest von 8.

4) Sey $a^2 \equiv 8\alpha + 1$ (Mod. 2^m) und $m > 2$; so kann man sich n so genommen denken, daß $n > m$, aber nicht $> 2m - 2$ ist, welches für $m = 2$ nicht möglich wäre, da dann $2m - 2$ auch $= 2$. Ich behaupte nun, daß es ein Quadrat giebt, welches $\equiv 8\alpha + 1$ (Mod. 2^n). Man setze die Wurzel dieses Quadrats $= \pm a + 2^{m-1}x$; so ist also

$$a^2 \pm 2^m ax + 2^{2m-2}x^2 \equiv 8\alpha + 1 \text{ (Mod. } 2^n\text{)}.$$

Also, da n nicht $> 2m - 2$, auch

$$a^2 \pm 2^m . ax \equiv 8\alpha + 1 \text{ (Mod. } 2^n\text{)}.$$

Aber nach der Voraussetzung

$$(8\alpha + 1) - a^2 = 2^m . q;$$

also $\pm 2^m . ax \equiv 2^m . q$ (Mod. 2^n), und folglich, da $n > m$, offenbar auch

$$\pm ax \equiv q \text{ (Mod. } 2^{n-m}\text{)}.$$

Man muß also x so bestimmen, daß $q \mp ax$ durch 2^{n-m} theilbar ist, d. h. die unbestimmte Gleichung des ersten Grades

$$q \mp ax = 2^{n-m} . y, \; q = 2^{n-m} . y \pm ax$$

auflösen. Diese Auflösung ist aber möglich, da 2^{n-m} und a relative Primzahlen sind. Denn, ginge 2 in a auf, so müßte es, da dann auch 2 in a^2 aufginge, und nach der Voraussetzung 2^m in $a^2 - (8\alpha + 1)$ aufgeht, auch in $8\alpha + 1$ aufgehen, welches unmöglich ist. Also ist $8\alpha + 1$ quadratischer Rest von 2^n. Da nun $8\alpha + 1$ wirklich quadratischer Rest von 2^3 ist, wo $3 > 2$; so ist $8\alpha + 1$ quadratischer Rest aller höhern Potenzen bis $2^{6-2} = 2^4$, folglich wieder alle Potenzen bis $2^{8-2} = 2^6$, $2^{12-2} = 2^{10}$, $2^{20-2} = 2^{18}$, $2^{36-2} = 2^{34}$, u. s. f. überhaupt von jeder höhern Potenz als 2^3.

5) Die ungeraden Zahlen von der Form $8\alpha + 3$, $8\alpha + 5$, $8\alpha + 7$ sind dagegen nicht quadratische Reste von

2^3, oder einer höhern Potenz der 2, welches augenblicklich daraus erhellet, daß das Quadrat jeder ungeraden Zahl von der Form $4x + 1$ oder $4x + 3 = 4(x+1) - 1 = 4y - 1$ von der Form $8x + 1$ ist, und demnach offenbar nie ein ungerades Quadrat einer der Zahlen $8\alpha + 3$, $8\alpha + 5$, $8\alpha + 7$ in Bezug auf den Modulus 8 congruent werden kann, eben so wenig, wie ein gerades Quadrat.

6) Für die durch 2 theilbaren Zahlen finden die in (17.) gegebenen Bestimmungen ihre Anwendung.

19. Ist nun der Modulus m eine zusammengesetzte Zahl, $= pqrs \ldots$, wo p, q, r, ... ungleiche Primzahlen, oder Potenzen ungleicher Primzahlen sind; so fällt sogleich in die Augen, daß, wenn a ein quadratischer Rest von m ist, a auch ein quadratischer Rest von p, q, r, ... seyn wird; und daß folglich umgekehrt, wenn a nicht quadratischer Rest von einer der Größen p, q, r, ... ist, a auch nicht quadratischer Rest von m seyn kann. Auch läßt sich behaupten, daß a quadratischer Rest von m ist, wenn a quadratischer Rest von p, q, r, ... ist. Um dies zu beweisen, nehmen wir zuerst an, daß m bloß zwei Factoren, p, q habe, und nach der Annahme

$$\alpha^2 \equiv a \text{ (Mod. p)}, \quad \beta^2 \equiv a \text{ (Mod. q)}$$

sey. Man bestimme nun x so, daß

$$x \equiv \alpha \text{ (Mod. p)}, \quad x \equiv \beta \text{ (Mod. q)},$$

eine Bestimmung, welche immer möglich ist, indem nämlich obige Congruenzen auf die unbestimmten Gleichungen des ersten Grades

$$x - \alpha = py, \quad x - \beta = qz;$$

und diese wieder auf

$$\alpha - \beta = qz - py,$$

deren Auflösung, da p, q, relative Primzahlen sind, immer möglich ist (Unbestimmte Analytik. 1.), führen. Ist nun x den obigen Bedingungen gemäß bestimmt; so führen die gegebenen und gefundenen Congruenzen leicht auf

$$x^2 \equiv \alpha^2 \equiv a \text{ (Mod. p)}, \quad x^2 \equiv \beta^2 \equiv a \text{ (Mod. q)}$$

(II. 8.), so daß also $x^2 - a$ sowohl durch p, als durch q, folglich, weil p, q relative Primzahlen sind, auch

durch pq theilbar, und demnach $x^2 \equiv a$ (Mod. pq), oder $x^2 \equiv a$ (Mod. m), d. i. a quadratischer Rest von m ist. Von zwei Factoren schließt man nun leicht auf drei, u. s. f., woraus die Allgemeinheit des Satzes folgt.

20. Mit Hülfe der bisher bewiesenen Sätze ist man im Stande, in allen Fällen über die quadratischen Reste der einfachen und zusammengesetzten Zahlen mit Sicherheit zu urtheilen, obgleich wir wegen weiterer Ausführung dieser wichtigen Lehre auf die Disq. arithm. Sect. IV. von Gauß verweisen müssen. Wir schließen mit folgenden merkwürdigen Sätzen:

$+2$ ist quadratischer Rest jeder Zahl, welche weder durch 4, noch durch Primzahlen von der Form $8n+3$, $8n+5$ theilbar ist; von allen andern nicht quadratischer Rest.

Denkt man sich eine Zahl m von der angegebenen Beschaffenheit in ihre Primfactoren zerlegt; so ist das Product von der Form $2.(8n+1)^\alpha.(8n+7)^\beta$. Nun ist 2 quadratischer Rest von 2 (15.), von $8n+1$ und $8n+7$ (12.), also, da 2 durch $8n+1$ und $8n+7$ nicht theilbar ist, auch von $(8n+1)^\alpha$, $(8n+7)^\beta$ (16.), folglich auch von $2.(8n+1)^\alpha.(8n+7)^\beta$, d. i. von m (19.). Ist aber m z. B. durch $8n+3$ theilbar; so ist, weil 2 nicht quadratischer Rest von $8n+3$ ist (12.), 2 auch nicht quadratischer Rest von m (16. 19.). Eben so in andern Fällen.

Auf ähnliche Art überzeugt man sich von der Richtigkeit des folgenden Theorems:

-2 ist quadratischer Rest jeder Zahl, welche weder durch 4, noch durch eine Primzahl von der Form $8n+5$ oder $8n+7$ theilbar ist; von jeder andern nicht quadratischer Rest.

Von 4 ist weder $+2$, noch -2, quadratischer Rest, da, x mag gerade oder ungerade seyn, offenbar weder x^2-2, noch x^2+2 durch 4 theilbar seyn kann.

$+3$ ist quadratischer Rest aller Zahlen, welche weder durch 4, noch durch 9, noch durch eine Primzahl von der

Form $12n + 5$ oder $12n + 7$ theilbar ist; von allen andern nicht quadratischer Rest.

Ist m von der angegebenen Beschaffenheit, so ist es, in seine Primfactoren zerlegt, von der Form $2.3.(12n+1)^{\alpha}.(12n+11)^{\beta}$. Es ist aber 3 quadratischer Rest von 2 (18. 1.), von 3 (15.), von $12n + 1$, $12n + 11$ (13.), von $(12n+1)^{\alpha}$, $(12n+11)^{\beta}$ (16.); also von dem obigen Product (19.), d. i. von m. Ist aber z. B. m durch 9 theilbar; so ist, weil offenbar 3 nicht quadratischer Rest von 9 ist, wie leicht aus (17. 2.) erhellet, auch 3 nicht quadratischer Rest von m (19.); und eben so in andern Fällen.

— 3 ist quadratischer Rest aller Zahlen, welche weder durch 8, noch durch 9, noch durch eine Primzahl von der Form $12n + 5$ oder $12n + 11$, d. i. von der Form $6n + 5$, theilbar ist; von allen übrigen Zahlen ist — 3 nicht quadratischer Rest.

Die Richtigkeit dieses Satzes erhellet auf ähnliche Art, wie vorher.

Der Erfinder dieser merkwürdigen Sätze ist Fermat (Opp. mathem. T. II. p. 857.). Lagrange und Euler haben zuerst Beweise derselben gegeben, in den Mém. de Berlin. 1775. p. 349. 351. 352. und den Nov. Comm. Petrop. T. VIII. p. 105. Auch s. m. Euleri Opuscula analytica. T. I. p. 259.

V. Form der Divisoren der Formel $t^2 + au^2$.

1. Die Form der Divisoren dieser Formel ist an sich so merkwürdig, und für viele Untersuchungen in der Zahlehre so wichtig, daß die hierher gehörenden Grundsätze hier nicht fehlen dürfen.

2. a bezeichnet jede gegebene positive oder negative Zahl, und t, u sind zwei unbestimmte Größen, denen alle positiven und negativen ganzen Zahlen als Werthe beigelegt werden können, nur mit der Bedingung, daß t

und u relative Primzahlen sind. Wären nämlich t und u nicht relative Primzahlen, sondern z. B. $t = \Theta t'$, $u = \Theta u'$; so wäre

$$t^2 + au^2 = \Theta(\Theta t'^2 + a\Theta u'^2),$$

also $t^2 + au^2$ durch Θ theilbar, so daß man also, da Θ jede Zahl bezeichnen kann, t und u immer so bestimmen könnte, daß $t^2 + au^2$ durch jede willkührliche Zahl theilbar wäre, folglich, ohne die Beschränkung, daß t und u relative Primzahlen sind, von gar keiner besondern Form der Divisoren der Formel $t^2 + au^2$ die Rede seyn könnte.

3. Zwei zusammengehörende Divisoren unserer Formel seyen p und p_1, so daß also

$$t^2 + au^2 = pp_1$$

ist. Zunächst erhellet, daß p (und eben so natürlich auch p_1) mit u relative Primzahl ist. Wäre nämlich die Primzahl Θ ein gemeinschaftlicher Divisor von p und u, so wäre auch

$$t^2 = pp_1 - au^2,$$

also, da Θ eine Primzahl ist, auch t durch Θ theilbar (I. 3.), und t und u wären folglich, gegen die vorher festgesetzte Bedingung, nicht relative Primzahlen. Also ist die Auflösung der unbestimmten Gleichung des ersten Grades

$$t = px + uq$$

in ganzen Zahlen jederzeit möglich (Unbestimmte Analytik. 1.). Man kann also

$$t = px + uq$$

setzen, welches, in die Gleichung

$$t^2 + au^2 = pp_1$$

für t gesetzt,

$$px^2 + 2uxq + \frac{(q^2+a)u^2}{p} = p_1$$

giebt. Also muß

$$\frac{(q^2+a)u^2}{p}$$

eine ganze Zahl seyn, oder p in $(q^2 + a)u^2$, folglich auch, weil p und u nach dem Obigen relative Primzahlen sind, in $q^2 + a$ aufgehen (I. 7.), so daß man also

$$\frac{q^2 + a}{p} = r, \; px^2 + 2uxq + ru^2 = p_1$$

setzen kann. Von dieser Form sind also, da p_1 jeden Factor von $t^2 + au^2$ bedeuten kann, alle Divisoren dieser Formel. Zugleich erhellet, daß x und u immer relative Primzahlen. Wäre nämlich, wenn Θ wieder eine Primzahl bezeichnet, x und u durch Θ theilbar, so würde Θ auch in p_1, folglich auch in

$$t^2 + au^2 = pp_1,$$

also, da Θ in u aufgeht, auch in t^2, und folglich auch in t (I. 3.) aufgehen, so daß also t und u gegen die Voraussetzung nicht relative Primzahlen wären. Die beiden zusammengehörenden Divisoren p und p_1 unserer Formel sind also immer von der Form

$$p_1 = px^2 + 2uxq + ru^2,$$
$$p = p_1x_1^2 + 2ux_1q_1 + r_1u^2.$$

Auch folgt aus der obigen Darstellung unmittelbar, daß jeder Factor von $t^2 + au^2$ immer auch ein Divisor der einfachern Formel $q^2 + a$ oder $t^2 + a$ ist, welche aus der vorhergehenden entspringt, wenn man $u = 1$ setzt, so daß man also den Factoren der Formel $t^2 + au^2$ auch die einfachere Form

$$px^2 + 2xq + r$$

geben kann.

4. Eben so kann man auch umgekehrt leicht zeigen, daß, wenn p und q so bestimmt sind, daß $\frac{q^2 + a}{p} = r$, eine ganze Zahl ist, immer p und

$$p_1 = px^2 + 2uxq + ru^2$$

zusammengehörende Divisoren der Formel $t^2 + au^2$ sind. Denn es ist

$$pp_1 = p^2x^2 + 2uxpq + pru^2;$$

aber $q^2 + a = rp$; also

$$pp_1 = p^2x^2 + 2uxpq + q^2u^2 + au^2 = (px + qu)^2 + au^2,$$

d. i. wenn

$$px + qu = t$$

gesetzt wird,

$$pp_1 = t^2 + au^2.$$

Folglich p und p_1 zusammengehörende Divisoren von $t^2 + au^2$.

Kann man überhaupt p, q so bestimmen, daß $\frac{q^2 + a}{p}$ eine ganze Zahl ist; so kann man zugleich q immer so bestimmen, daß es $\frac{1}{2}p$ nicht übersteigt. Ist nämlich $q^2 + a$ durch p theilbar; so ist auch für jedes z

$$\frac{(q - pz)^2 + a}{p} = \frac{q^2 + a}{p} + pz^2 - 2qz$$

eine ganze Zahl. Nimmt man nun für z die ganze Zahl, welche dem Bruche $\frac{q}{p}$ am nächsten kommt; so ist, wie leicht erhellet, immer entweder $\frac{q}{p} - z \lesseqgtr \frac{1}{2}$, oder $z - \frac{q}{p} \lesseqgtr \frac{1}{2}$, jenachdem $z \lesseqgtr \frac{q}{p}$ ist. Also $q - pz \lesseqgtr \frac{1}{2}p$ oder $pz - q \lesseqgtr \frac{1}{2}p$, folglich der positive Werth von $q - pz \lesseqgtr \frac{1}{2}p$, so daß also $q - pz = q'$ immer so bestimmt werden kann, daß $q'^2 + a$ durch p theilbar, und q' nicht $> \frac{1}{2}p$ ist.

5. Lagrange (Mém. de Berlin. 1773.) hat gezeigt, daß überhaupt die Formel

$$py^2 + 2qxy + rx^2$$

immer so transformirt werden kann, daß der mittlere Coefficient 2q keinen der beiden äußern p, r übersteigt.

Wir wollen annehmen, daß 2q einen der beiden äußern, z. B. p, welches willkührlich ist, da obige Formel in Bezug auf p, r eine ganz symmetrische Form hat, übersteige, und daß p, wenn 2q beide äußere Coefficienten übersteigt, der kleinere von beiden sey. Die ganze Zahl, welche dem Bruche $\frac{q}{p}$ am nächsten kommt, sey $= n$; so können folgende Fälle eintreten:

$$n - \frac{q}{p} = 0,\ 2np - 2q = 0;$$

$$n - \frac{q}{p} \lesseqgtr \frac{1}{2},\ 2np - 2q \lesseqgtr p;$$

$$\frac{q}{p} - n \lesseqgtr \frac{1}{2},\ 2q - 2np \lesseqgtr p;$$

und der absolute Werth von $2np - 2q$ übersteigt also den Werth des Coefficienten p nicht. Auch ist zu bemerken, daß, für $2q > p$, n nicht $= 0$ seyn kann, weil $\frac{q}{p} > \frac{1}{2}$, und

folglich die dem Bruche $\frac{q}{p}$ am nächsten kommende ganze Zahl nothwendig $> o$ ist. Ist aber $2q \overset{=}{<} p$, also $\frac{q}{p} \overset{=}{<} \frac{1}{2}$, so ist $n = o$ zu setzen, wie leicht erhellet.

Man setze nun $y = y' - nx$; so wird die gegebene Größe

$$= p(y'^2 - 2ny'x + n^2x^2) + 2q(y' - nx)x + rx^2$$
$$= py'^2 - 2(pn - q)xy' + (pn^2 - 2nq + r)x^2$$
$$= py'^2 - 2q'xy' + r'x^2,$$

für $q' = pn - q$, $r' = pn^2 - 2nq + r$; und es ist in dieser transformirten Formel nach dem Obigen $2q'$ nicht $> p$.

Zugleich erhellet, daß immer

$$pr' - q'^2 = pr - q^2$$

ist. Denn es ist

$$pr' - q'^2 = p(pn^2 - 2nq + r) - (pn - q)^2$$
$$= pr - q^2 + p^2n^2 - p^2n^2 - 2npq + 2npq.$$

Auch ist $q' < q$. Denn $2q > p$, $p \overset{=}{<} 2q'$, $2q > 2q'$, $q > q'$.

So lange also in einer Formel der obigen Form der mittlere Coefficient größer als einer der beiden äußern ist, kann man diese Formel immer in eine andere transformiren, in welcher der mittlere Coefficient diesen äußern Coefficienten nicht mehr übersteigt, und in jeden zwei solchen Formeln ist allgemein

$$p_{n-1}r_n - q_n^2 = p_{n-1}r_{n-1} - q^2_{n-1},$$

und $q_n < q_{n-1}$, wenn $2q_{n-1}$, $2q_n$ die mittlern Coefficienten sind, und $2q_{n-1} > p_{n-1}$ ist.

Wendet man nun die so eben gelehrte Transformation an, so lange der mittlere Coefficient noch größer als einer der beiden äußern ist, und bezeichnet die successiven mittlern Coefficienten durch $2q$, $2q'$, $2q''$, $2q'''$, ...; so ist

$$q, q', q'', q''', q'''', \ldots.$$

eine abnehmende Reihe. Käme man nie auf eine transformirte Formel, in welcher der mittlere Coefficient keinen der beiden äußern übersteigt; so würde obige Reihe in's Unendliche fortlaufen, welches ungereimt ist, da alle Glie-

der derselben endliche ganze Zahlen sind. Man muß folglich immer irgend einmal auf eine transformirte Formel kommen, in welcher der mittlere Coefficient keinen der beiden äußern übersteigt. In diesem Falle wird dann, wie schon oben erwähnt, die ganze Zahl $n = o$, und q, r behalten ihre absoluten Werthe, wie aus den für q' und r' gefundenen Ausdrücken unmittelbar folgt.

Die gegebene Formel sey z. B.

$$35y^2 + 172xy + 210x^2 ;$$

so ist $172 > 35$, $p = 35$, $2q = 172$, $q = 86$, $\frac{q}{p} = \frac{86}{35}$, $n = 2$, $q' = 70 - 86 = -16$, $r' = 140 - 344 + 210 = 6$. Also die transformirte Formel:

$$35y'^2 + 32xy' + 6x^2 .$$

Hier ist noch $32 > 6$. Also $p = 6$, $2q = 32$, $q = 16$, $r = 35$, $\frac{q}{p} = \frac{16}{6} = \frac{8}{3}$, $n = 3$, $q' = 18 - 16 = 2$, $r' = 54 - 96 + 35 = -7$, und demnach die transformirte Formel:

$$6x'^2 - 4y'x' - 7y'^2 ,$$

wo nun $4 < 6$, $4 < 7$, wie verlangt wurde.

6. In der Formel

$$px^2 + 2uxq + ru^2$$

in (3.) sind x und u relative Primzahlen (3.). Verwandelt man nach (5.) diese Formel in

$$px'^2 + 2ux'q + r'u^2 ,$$

wo also $x = x' - nu$ gesetzt werden muß; so erhellet leicht, daß auch in der transformirten Formel x' und u relative Primzahlen sind, weil, wenn dies nicht der Fall wäre, der gemeinschaftliche Factor auch in x aufgehen müßte, so daß also x und u nicht relative Primzahlen wären. Auch ist nach dem Vorigen immer

$$pr' - q'^2 = pr - q^2 , \text{ und } q' < q .$$

Folglich sind offenbar auch bei öfterer Anwendung voriger Transformation in der endlich resultirenden Formel die unbestimmten Größen relative Primzahlen, wovon man sich durch einen leichten Schluß überzeugt.

7. Man unterscheide nun zwei Fälle, jenachdem a in

der Formel $t^2 + au^2$ positiv oder negativ ist. Die beiden Formen seyen, indem man c immer als positiv annimmt,

$$t^2 + cu^2 \text{ und } t^2 - cu^2 .$$

Die Formen der Divisoren dieser beiden Formeln sind

$$px^2 + 2qxu + \left(\frac{c+q^2}{p}\right)u^2 ,$$

$$px^2 + 2qxu - \left(\frac{c-q^2}{p}\right)u^2 ;$$

oder

$$px^2 + 2qxu + ru^2 ,$$

für $r = \frac{c+q^2}{p}$, $pr - q^2 = c$; und

$$px^2 + 2qxu - ru^2 ,$$

für $r = \frac{c-q^2}{p}$, $pr + q^2 = c$. Denkt man sich nun diese Factoren nach (5.) transformirt; so ist in beiden

$$2q \gtreqless p, \; 2q \gtreqless r .$$

Also $4q^2 \gtreqless pr$, $q^2 \gtreqless \frac{1}{4}pr$. Aber im ersten Falle $pr = c + q^2$; also

$$q^2 \gtreqless \tfrac{1}{4}(c+q^2), \; 3q^2 \leqq c, \; q \gtreqless \sqrt{\tfrac{1}{3}c}.$$

Im zweiten Falle ist $q^2 \gtreqless \frac{1}{4}(c-q^2)$, $5q^2 \gtreqless c$, $q \gtreqless \sqrt{\frac{1}{5}c}$. Die Größen x und u sind immer relative Primzahlen.

Die Divisoren der Formel $t^2 + au^2$, unter der Voraussetzung, daß t und u relative Primzahlen sind, heißen wegen ihrer hier bewiesenen Form quadratische Divisoren. Alle Factoren obiger Formel, und folglich auch der einfachen Formel $t^2 + a$, haben die quadratische Form.

VI. Einige Sätze von den Primzahlen, als Folgerungen aus dem Vorhergehenden.

1. Jeder Divisor der Formel $t^2 + u^2$ ist, wenn t und u relative Primzahlen sind, die Summe zweier Quadrate, oder von der Form $x^2 + y^2$, so daß auch x und y relative Primzahlen sind.

Die vorher (V. 5.) gelehrte Transformation schon aus-

geführt gedacht, sind alle Divisoren der Formel $t^2 + u^2$ von der Form

$$px^2 + 2qxy + ry^2,$$

und es ist, da hier $c = 1$ (V. 7.),

$$pr - q^2 = 1, q < r^{\frac{1}{2}} \text{ (V. 7.)}.$$

Folglich, da q eine ganze Zahl ist, offenbar $q = o$; also $pr = 1$, und folglich $p = 1$, $r = 1$, da p und r ebenfalls ganze Zahlen sind. Dadurch verwandelt sich die obige Form der Divisoren hier in $x^2 + y^2$, und x, y sind relative Primzahlen, wie schon vorher (V. 6.) allgemein bewiesen worden.

2. Jede Primzahl von der Form $4n + 1$ ist die Summe zweier Quadrate.

Sey $4n + 1 = \gamma$; so ist

$$x^{\gamma-1} - 1 = x^{4n} - 1 = (x^{2n} - 1)(x^{2n} + 1).$$

Da nun $x^{2n} + 1$ in $x^{\gamma-1} - 1$ aufgeht; so giebt es immer 2n Werthe von x zwischen $-\frac{1}{2}\gamma$ und $+\frac{1}{2}\gamma$, welche die Congruenz

$$x^{2n} + 1 \equiv o \text{ (Mod. } \gamma)$$

auflösen (III. 8.), oder für welche $x^{2n} + 1$ durch $\gamma = 4n + 1$ theilbar wird. Es ist aber $x^{2n} + 1 = (x^n)^2 + 1^2$ die Summe zweier Quadrate, oder von der Form $t^2 + u^2$. Also ist auch jeder Theiler von $x^{2n} + 1$, d. i. auch die Primzahl $4n + 1$, von der Form $x^2 + y^2$ (1.), oder die Summe zweier Quadrate.

So ist z. B. $13 = 4.3 + 1 = 9 + 4$, $29 = 4.7 + 1 = 25 + 4$, $37 = 4.9 + 1 = 36 + 1$, $73 = 4.18 + 1 = 64 + 9$.

Da $8n + 1 = 4.2n + 1$, $8n + 5 = 4.(2n+1) + 1$ ist; so ist auch jede Primzahl von der Form $8n + 1$ oder $8n + 5$ die Summe zweier Quadrate.

Diesen Satz hat Fermat gefunden, s. Primzahl (13.).

3. Jede Primzahl von der Form $8n + 1$ hat zu gleicher Zeit die Formen

$$x^2 + y^2, x^2 + 2y^2, x^2 - 2y^2.$$

Sey $8n + 1 = \gamma$. Aus dem so eben Bewiesenen

wissen wir schon, daß $8n + 1$ immer von der Form $x^2 + y^2$ ist (2.). Nun ist

$$x^{\gamma-1} - 1 = x^{8n} - 1 = (x^{4n} - 1)(x^{4n} + 1),$$

d. i. $x^{\gamma-1} - 1$ durch $x^{4n} + 1$ theilbar. Folglich giebt es zwischen $-\frac{1}{2}\gamma$ und $+\frac{1}{2}\gamma$ nach (III. 8.) $4n$ Werthe von x, für welche $x^{4n} + 1$ durch γ theilbar wird. Aber

$$x^{4n} + 1 = (x^{2n} - 1)^2 + 2.(x^n)^2,$$

wo x^n und $x^{2n} - 1$ relative Primzahlen sind, weil ein gemeinschaftlicher Theiler derselben offenbar auch in x^{2n}, folglich auch in 1 aufgehen müßte, und demnach nur die Einheit selbst seyn könnte. Also ist $x^{4n} + 1$ unter der Form $t^2 + cu^2$, für $c = 2$, enthalten, und der Factor $\gamma = 8n + 1$ demnach von der Form

$$px^2 + 2qxy + ry^2,$$

wo $q < \sqrt{\frac{2}{3}}$, d. i., weil q eine ganze Zahl ist, $q = o$, $pr = q^2 + c$, $pr = 2$ (V. 7.); also immer entweder $p = 1$, $r = 2$, oder $p = 2$, $r = 1$, und folglich $8n + 1$ immer von der Form $x^2 + 2y^2$. Es ist aber auch

$$x^{4n} + 1 = (x^{2n} + 1)^2 - 2(x^n)^2,$$

wo auf ähnliche Art wie vorher erhellet, daß x^n und $x^{2n} + 1$ relative Primzahlen sind, also $x^{4n} + 1$ auch unter der Form $t^2 - cu^2$, für $c = 2$, enthalten ist. Folglich $q < \sqrt{\frac{2}{3}}$, d. i. $q = o$, $pr = 2$ (V. 7.). Folglich ist entweder $p = 1$, $r = 2$, oder $p = 2$, $r = 1$. Da nun alle Divisoren der Formel $t^2 - cu^2$ von der Form

$$px^2 + 2qxy - ry^2$$

sind; so ist auch $8n + 1$ von dieser Form, oder, wenn man für p, q, r ihre Werthe setzt, von der Form $x^2 - 2y^2$ oder $2x^2 - y^2$. Diese beiden Formen reduciren sich aber auf e i n e, da immer

$$2x^2 - y^2 = (2x - y)^2 - 2(x - y)^2,$$

folglich eine Zahl von der zweiten Form immer auch von der ersten Form ist.

Es ist z. B. $73 = 8^2 + 3^2 = 1^2 + 2.6^2 = 9^2 - 2.2^2 = 2.7^2 - 5^2$, $17 = 1^2 + 4^2 = 3^2 + 2.2^2 = 5^2 - 2.2^2 = 2.3^2 - 1^2$, $41 = 4^2 + 5^2 = 3^2 + 2.4^2 = 7^2 - 2.2^2 = 2.5^2 - 3^2$.

4. Jede Primzahl von der Form $8n + 3$ ist von der Form $x^2 + 2y^2$.

Sey wieder $8n + 3 = \gamma$; also

$$x^{\gamma-1} - 1 = x^{8n+2} - 1 = (x^{4n+1} - 1)(x^{4n+1} + 1).$$

Setzt man nun $x = 2$; so wird,

$$2^{\gamma-1} - 1 = \{2.(2^{2n})^2 - 1\}\{2^{4n+1} + 1\}.$$

Da nun $2^{\gamma-1} - 1$ immer durch γ theilbar ist (III. 1.); so muß entweder $2.(2^{2n})^2 - 1$, oder $2^{4n+1} - 1$ durch γ theilbar seyn (I. 3.). Fände das Erste statt, so müßte natürlich auch $1 - 2.(2^{2n})^2$ durch γ theilbar seyn, und γ müßte folglich ganz wie in (3.) von der Form $x^2 - 2y^2$ oder $2x^2 - y^2$, oder, weil diese beiden Formen nur eine bilden (3.), überhaupt z. B. von der Form $x^2 - 2y^2$ seyn. Daß dies aber nicht möglich ist, läßt sich so zeigen. Wäre nämlich $\gamma = 8n + 3 = x^2 - 2y^2$; so ist, da $2y^2$ gerade, aber $8n + 3$ ungerade ist, auch x^2 ungerade. Sey daher $x = 2z + 1$; so ist

$$x^2 = 4z^2 + 4z + 1 = 4z(z+1) + 1$$
$$= 8.\frac{z(z+1)}{2} + 1 = 8\nu + 1,$$

wenn wir $\frac{z(z+1)}{2}$, welches offenbar eine ganze Zahl ist, $= \nu$ setzen. Jedes ungerade Quadrat ist also von der Form $8\nu + 1$, jedes gerade von der Form 4ν. Also ist auch y^2 entweder von der Form $4\nu'$ oder $8\nu' + 1$. Im ersten Falle ist

$$x^2 - 2y^2 = 8\nu + 1 - 8\nu'$$
$$= 8(\nu - \nu') + 1;$$

im andern dagegen

$$x^2 - 2y^2 = 8\nu + 1 - 2(8\nu' + 1)$$
$$= 8(\nu - 2\nu' - 1) + 7;$$

in keinem Falle also von der Form $8n + 3$. Also kann auch $8n + 3$ nicht von der Form $x^2 - 2y^2$, also auch nicht von der Form $2x^2 - y^2$ (3.), und demnach auch $2.(2^{2n})^2 - 1$ nicht durch γ theilbar seyn. Also ist $2^{4n+1} + 1 = 1 + 2.(2^{2n})^2$ durch $\nu = 8n + 3$ theilbar, woraus ganz wie in (3.) folgt, daß jede Primzahl von der Form $8n + 3$ von der Form $x^2 + 2y^2$ ist.

Z. B. $11 = 3^2 + 2.1^2$, $19 = 1^2 + 2.3^2$.

5. Jede Primzahl von der Form $8n + 7$ ist von der Form $x^2 - 2y^2$.

Sey $\gamma = 8n + 7$; so ist

$$2^{\gamma-1} - 1 = 2^{8n+6} - 1 = (2^{4n+3} - 1)(2^{4n+3} + 1),$$

immer durch γ theilbar (III. 1.). Da nun

$$2^{4n+3} + 1 = 1^2 + 2.(2^{2n+1})^2$$

ist; so würde γ, wenn $2^{4n+3} + 1$ durch γ theilbar wäre, ganz auf ähnliche Art wie in (3.) bei einem ähnlichen Falle von der Form $x^2 + 2y^2$ seyn. Da aber $2y^2$ gerade und $8n + 7$ ungerade ist; so ist auch x^2 ungerade, folglich von der Form $8\nu + 1$ (4.). Also entweder

$$x^2 + 2y^2 = 8\nu + 1 + 8\nu' = 8(\nu + \nu') + 1,$$

oder

$$x^2 + 2y^2 = 8\nu + 1 + 2(8\nu' + 1) = 8(\nu + 2\nu') + 3;$$

folglich in keinem Fall von der Form $8n + 7$. Demnach kann γ in $2^{4n+3} + 1$ nicht aufgehen, und muß also in $2^{4n+3} - 1$ oder $1 - 2^{4n+3} = 1 - 2.(2^{2n+1})^2$ aufgehen. Hieraus folgt ganz wie in (3.), daß jede Primzahl von der Form $8n + 7$ von der Form $x^2 - 2y^2$ oder $2x^2 - y^2$ ist, welche zwei Formen sich aber auf die eine $x^2 - 2y^2$ reduciren (3.). Z. B. $23 = 5^2 - 2.1^2 = 2.4^2 - 3^2$, $47 = 7^2 - 2.1^2 = 2.6^2 - 5^2$.

6. Es sind also

1) die Primzahlen von den Formen $8n + 1$, $8n + 5$ ausschließlich von der Form $x^2 + y^2$;

2) die Primzahlen von den Formen $8n + 1$, $8n + 3$ ausschließlich von der Form $x^2 + 2y^2$; und

3) die Primzahlen von den Formen $8n + 1$, $8n + 7$ ausschließlich von der Form $x^2 - 2y^2$.

Die Primzahlen von der Form $8n + 1$ vereinigen alle drei Formen in sich.

Die Erfindung aller dieser Sätze verdanken wir Fermat, worüber der Art. Primzahl (13. 14. 16.) zu vergleichen. Beweise haben aber zuerst Euler (s. a. a. O.) und Lagrange (Mém. de Berlin. 1774.) gegeben.

7. Sey a eine Primzahl von der Form $4n + 1$, und

A irgend eine ungerade Zahl, aber Divisor der Formel $t^2 + au^2$, oder, was Dasselbe ist (V. 3.), der Formel $x^2 + a$; so ist immer $A^{\frac{a-1}{2}} \equiv 1$ (Mod. a), wenn A von der Form $4n + 1$, dagegen $A^{\frac{a-1}{2}} \equiv -1$ (Mod. a), wenn A von der Form $4n + 3$ ist.

Seyen α, β irgend zwei Primzahlen, die erste von der Form $4n + 1$, die andern von der Form $4n + 3$, aber beide Divisoren von $x^2 + a$; so ist also

$$x^2 \equiv -a \text{ (Mod. } \alpha), \; x^2 \equiv -a \text{ (Mod. } \beta).$$

Folglich, da α, β in der Primzahl a natürlich nicht aufgehen, nach (III. 9.)

$$(-a)^{\frac{\alpha-1}{2}} \equiv 1 \text{ (Mod. } \alpha), \; (-a)^{\frac{\beta-1}{2}} \equiv 1 \text{ (Mod. } \beta).$$

Da aber $\frac{\alpha-1}{2}$ gerade, $\frac{\beta-1}{2}$ ungerade ist; so ergiebt sich hieraus leicht

$$a^{\frac{\alpha-1}{2}} \equiv 1 \text{ (Mod. } \alpha), \; a^{\frac{\beta-1}{2}} \equiv -1 \text{ (Mod. } \beta).$$

Folglich, weil weder a, α noch a, β beide von der Form $4n + 3$ sind, nach dem Satze von der Reciprocität (IV. 1.)

$$a^{\frac{\alpha-1}{2}} \equiv 1 \text{ (Mod. } \alpha), \; \alpha^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)};$$

$$a^{\frac{\beta-1}{2}} \equiv -1 \text{ (Mod. } \beta), \; \beta^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)}.$$

Sey nun A in seine Primfactoren zerlegt, so daß

$$A = \alpha\alpha'\alpha'' \ldots \beta\beta'\beta'' \ldots,$$

wo α, α', α'', ... lauter Primzahlen von der Form $4n + 1$; β, β', β'', ... lauter Primzahlen von der Form $4n + 3$ bezeichnen. Ist nun A von der Form $4n + 1$, so ist die Anzahl der Primfactoren der letztern Gattung immer gerade. Wäre diese Anzahl nämlich ungerade, z. B. $= 2m + 1$; so wäre der von den durch 4 nicht theilbaren Theilen der einzelnen Primfactoren herührende Theil von A offenbar

$$= 3^{2m+1} = (4-1)^{2m+1} = 4e + \frac{2m+1}{1}.4 - 1$$
$$= 4(e + 2m) + 3,$$

wenn e eine ganze Zahl bezeichnet, und man sich nur die Potenz des Binomiums $4 - 1$ nach dem binomischen Lehrsatze entwickelt denkt. Also wäre A offenbar von der Form $4n + 3$, da es doch von der Form $4n + 1$ seyn soll. Ist dagegen A von der Form $4n + 3$; so ist die Anzahl der durch β bezeichneten Primfactoren ungerade, weil, wenn sie $= 2m$ wäre, der oben bezeichnete Theil des Products aller Primfactoren offenbar

$$= 3^{2m} = (4-1)^{2m} = 4e - \frac{2m}{1}.4 + 1$$
$$= 4(e - 2m) + 1,$$

und daher A selbst von der Form $4n + 1$ seyn würde. Dies vorausgesetzt, haben wir nun nach dem Obigen

$$\alpha^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}, \quad \beta^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)};$$
$$\alpha'^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}, \quad \beta'^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)};$$
$$\alpha''^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}, \quad \beta''^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)};$$
$$\text{\&c.} \quad \text{\&c.} \quad \text{\&c.} \quad \text{\&c.}$$

Also, wenn man multiplicirt, nach (II. 6.)

$$\alpha^{\frac{a-1}{2}}.\alpha'^{\frac{a-1}{2}}.\alpha''^{\frac{a-1}{2}}\ldots\beta^{\frac{a-1}{2}}.\beta'^{\frac{a-1}{2}}.\beta''^{\frac{a-1}{2}}\ldots$$
$$\equiv (-1).(-1).(-1).(-1)\ldots \text{ (Mod. a)}$$

d. i.

$$A^{\frac{a-1}{2}} \equiv (-1).(-1).(-1).(-1)\ldots \text{ (Mod. a)}.$$

Ist nun A von der Form $4n + 1$; so ist die Anzahl der Factoren des Products auf der rechten Seite gerade, und folglich in diesem Falle

$$A^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)};$$

ist aber A von der Form $4n + 3$; so ist die Anzahl dieser Factoren ungerade, und folglich

$$A^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)};$$

w. z. b. w.

8. Wenn a eine Primzahl von der Form $4n+3$, und A irgend ein ungerader Divisor der Formel t^2+au^2 oder x^2+a ist; so ist immer $A^{\frac{a-1}{2}} \equiv 1$ (Mod. a).

Seyen wieder α, β zwei Primzahlen, respective von der Form $4n+1$ und $4n+3$, beide Divisoren von x^2+a; so ist, wie vorher,

$$(-a)^{\frac{\alpha-1}{2}} \equiv 1 \text{ (Mod. } \alpha), \quad (-a)^{\frac{\beta-1}{2}} \equiv 1 \text{ (Mod. } \beta);$$

$$a^{\frac{\alpha-1}{2}} \equiv 1 \text{ (Mod. } \alpha), \quad a^{\frac{\beta-1}{2}} \equiv -1 \text{ (Mod. } \beta).$$

Da aber hier a, α nicht beide von der Form $4n+3$, dagegen a, β beide von der Form $4n+3$ sind, so ist nach dem Satze von der Reciprocität

$$a^{\frac{\alpha-1}{2}} \equiv 1 \text{ (Mod. } \alpha), \quad \alpha^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)};$$

$$a^{\frac{\beta-1}{2}} \equiv -1 \text{ (Mod. } \beta), \quad \beta^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}.$$

Sey nun wieder

$$A = \alpha\alpha'\alpha'' \ldots\ldots \beta\beta'\beta'' \ldots\ldots,$$

wo aber, weil A nach der Voraussetzung ungerade ist, kein Primfactor $= 2$ ist, welches wegen der Anwendung des Satzes von der Reciprocität nothwendig ist (IV. 1.); so ist

$$A^{\frac{a-1}{2}} = \alpha^{\frac{a-1}{2}} . \alpha'^{\frac{a-1}{2}} . \alpha''^{\frac{a-1}{2}} \ldots \beta^{\frac{a-1}{2}} . \beta'^{\frac{a-1}{2}} . \beta''^{\frac{a-1}{2}} \ldots\ldots$$
$$\equiv 1 \text{ (Mod. a) (II. 6.)}.$$

9. Sey jetzt a eine Primzahl von der Form $4n+1$, und α, α', α'', α''' seyen Primzahlen respective von der Form $8n+1$, $8n+3$, $8n+5$, $8n+7$, alle aber Divisoren von t^2+2au^2 oder x^2+2a; so ist nach (III. 9.)

$$(-2a)^{\frac{\alpha-1}{2}} \equiv 1 \text{ (Mod. } \alpha), \quad (-2a)^{\frac{\alpha'-1}{2}} \equiv 1 \text{ (Mod. } \alpha'),$$

$$(-2a)^{\frac{\alpha''-1}{2}} \equiv 1 \text{ (Mod. } \alpha''), \quad (-2a)^{\frac{\alpha'''-1}{2}} \equiv 1 \text{ (Mod. } \alpha''');$$

oder, weil die Exponenten der Potenzen nach der Ordnung gerade, ungerade, gerade, ungerade sind,

$$(2a)^{\frac{\alpha-1}{2}} \equiv 1 \ (\text{Mod. } \alpha), \ (2a)^{\frac{\alpha'-1}{2}} \equiv -1 \ (\text{Mod. } \alpha'),$$
$$(2a)^{\frac{\alpha''-1}{2}} \equiv 1 \ (\text{Mod. } \alpha''), \ (2a)^{\frac{\alpha'''-1}{2}} \equiv -1 \ (\text{Mod. } \alpha''');$$

Aber (IV. 12.)

$$2^{\frac{\alpha-1}{2}} \equiv 1 \ (\text{Mod. } \alpha), \ 2^{\frac{\alpha'-1}{2}} \equiv -1 \ (\text{Mod. } \alpha'),$$
$$2^{\frac{\alpha''-1}{2}} \equiv -1 \ (\text{Mod. } \alpha''), \ 2^{\frac{\alpha'''-1}{2}} \equiv 1 \ (\text{Mod. } \alpha''').$$

Folglich offenbar

$$a^{\frac{\alpha-1}{2}} \equiv 1 \ (\text{Mod. } \alpha), \ a^{\frac{\alpha'-1}{2}} \equiv 1 \ (\text{Mod. } \alpha'),$$
$$a^{\frac{\alpha''-1}{2}} \equiv -1 \ (\text{Mod. } \alpha'), \ a^{\frac{\alpha'''-1}{2}} \equiv -1 \ (\text{Mod. } \alpha''');$$

wovon man sich mittelst (II. 6.) und der vorigen Congruenzen leicht durch einen indirecten Schluß überzeugt.

Folglich nach dem Satze von der Reciprocität

$$\alpha^{\frac{a-1}{2}} \equiv 1 \ (\text{Mod. } a), \ \alpha'^{\frac{a-1}{2}} \equiv 1 \ (\text{Mod. } a),$$
$$\alpha''^{\frac{a-1}{2}} \equiv -1 \ (\text{Mod. } a), \ \alpha'''^{\frac{a-1}{2}} \equiv -1 \ (\text{Mod. } a).$$

Ist nun A irgend eine Zahl von den Formen $8n+1$, $8n+3$, dagegen B eine Zahl von den Formen $8n+5$, $8n+7$, beide aber Divisoren von $t^2 + 2au^2$ oder $x^2 + 2a$; so ist, wenn A in seine Primfactoren zerlegt wird, die Anzahl der Primfactoren von den Formen $8n+5$, $8n+7$ gerade, bei B dagegen die Anzahl der Primfactoren von diesen Formen ungerade, wovon man sich leicht auf folgende Art überzeugt.

Jede Potenz der 3 ist entweder von der Form $8n+1$ oder von der Form $8n+3$, welches offenbar von den ersten Potenzen der 3 gilt, da $3 = 8.0+3$, $9 = 8.1+1$, $27 = 8.3+3$, $81 = 8.10+1$ ist. Dieses Gesetz gelte nun überhaupt für 3^k, so daß $3^k = 8n+1 = 8n'+3$ ist; so ist $3^{k+1} = 24n+3 = 24n'+9 =$

$8.3n + 3 = 8.(3n + 1) + 1$. Folglich das Gesetz allgemein.

Jede Potenz der 5 ist entweder von der Form $8n + 1$ oder $8n + 5$, wie z. B. $5 = 8.0 + 5$, $25 = 8.3 + 1$, $125 = 8.15 + 5$, $625 = 8.78 + 1$. Sey $5^k = 8n + 1 = 8n' + 5$; so ist $5^{k+1} = 40n + 5 = 40n' + 25 = 8.5n + 5 = 8.(5n' + 3) + 1$, und das Gesetz also allgemein. Eben so überzeugt man sich leicht, daß jede Potenz der 7 entweder von der Form $8n + 1$, oder von der Form $8n + 7$ ist. Zugleich erhellet auch, daß die ungeraden Potenzen von 3, 5, 7, respective von der Form $8n + 3$, $8n + 5$, $8n + 7$, die geraden dagegen von der Form $8n + 1$ sind.

Wäre nun die Anzahl der in A enthaltenen Primfactoren von den Formen $8n + 5$, $8n + 7$ ungerade; so wäre, wegen des Vorigen, das Product dieser Factoren offenbar entweder von der Form $8n + 5$ oder $8n + 7$. Das Product der Primfactoren von den Formen $8n + 1$, $8n + 3$ ist entweder von der Form $8n + 1$ oder $8n + 3$. Also das Product aller Primfactoren von A, d. i. A, entweder von den Formen $8n + 5$, $8n + 7$, oder $8n + 15 = 8n' + 7$, $8n + 21 = 8n' + 5$, also nicht von der Form $8n + 1$ oder $8n + 3$, von welchen Formen A doch nur seyn soll. Also ist die Anzahl der Primfactoren von den Formen $8n + 5$, $8n + 7$ gerade, und demnach, wegen obiger Congruenzen nach (II. 6.)

$$A^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}.$$

Wäre in B die Anzahl der Primfactoren von den Formen $8n + 5$, $8n + 7$ gerade, so wäre das Product dieser Primfactoren entweder von der Form $8n + 1$, oder von der Form $8n + 35 = 8n' + 3$. Das Product der Primfactoren von der Form $8n + 1$, $8n + 3$ hat dieselben Formen. Folglich ist offenbar auch das Product aller Primfactoren entweder von der Form $8n + 1$ oder $8n + 3$, da doch B nur von den Formen $8n + 5$ oder $8n + 7$ seyn soll. Also ist die Anzahl der Primfactoren von den Formen $8n + 5$,

$8n+7$ in diesem Falle ungerade, und demnach wegen obiger Congruenzen nach (II. 6.)

$$B^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)}.$$

10. Alles Vorhergehende bleibe unverändert, a aber sey eine Primzahl von der Form $4n+3$; so folgt nun aus den ersten Congruenzen in (9.) nach dem Satze von der Reciprocität

$$\alpha^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}, \quad \alpha'^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)},$$

$$\alpha''^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)}, \quad \alpha'''^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}.$$

Sey nun A von den Formen $8n+1$, $8n+7$, B von den Formen $8n+3$, $8n+5$; so ist in Bezug auf A die Anzahl der Primfactoren von der Form $8n+3$, $8n+5$, gerade, in Bezug auf B dagegen ungerade, wovon man sich leicht auf ähnliche Art wie vorher überzeugt. Also in diesem Falle wieder

$$A^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}, \quad B^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)}.$$

11. Aus (9.) und (10.) ergiebt sich nun folgender Lehrsatz:

Ist a eine Primzahl von der Form $4n+1$ und A ein Divisor der Formel t^2+2au^2 von der Form $8n+1$, $8n+3$, B dagegen ein Divisor dieser Formel von der Form $8n+5$, $8n+7$; so ist

$$A^{\frac{a-1}{2}} \equiv 1 \text{ (Mod. a)}, \quad B^{\frac{a-1}{2}} \equiv -1 \text{ (Mod. a)};$$

und dieselben Congruenzen finden statt, wenn a eine Primzahl von der Form $4n+3$, die Divisoren A, B der Formel t^2+2au^2 dagegen von den Formen $8n+1$, $8n+7$, und $8n+3$, $8n+5$ sind.

VII. Ueber die Auflösung der Congruenzen $x^{\frac{a-1}{2}} \equiv 1$ (Mod. a), $x^{\frac{a-1}{2}} \equiv -1$ (Mod. a), wenn a eine ungerade Primzahl ist.

1. In Bezug auf die erste Congruenz kann man für x jedes y^2 setzen, wenn a nicht darin aufgeht, indem unter dieser Voraussetzung nach dem Fermat'schen Satze (III. 1.) $x^{\frac{a-1}{2}} = y^{a-1} \equiv 1$ ist. Also sind

$$1, 4, 9, 16, 25, \ldots \left(\frac{a-1}{2}\right)^2$$

Werthe von x. Ist nun überhaupt $y^2 = ap + r$, wo $r < a$, ein Glied dieser Reihe; so erhellet, wenn e überhaupt eine ganze Zahl bezeichnet, mittelst des binomischen Lehrsatzes leicht, daß $x^{\frac{a-1}{2}} = (ap + r)^{\frac{a-1}{2}} = ae + r^{\frac{a-1}{2}}$, also $x^{\frac{a-1}{2}} \equiv r^{\frac{a-1}{2}}$ ist; aber $x^{\frac{a-1}{2}} \equiv 1$; also auch $r^{\frac{a-1}{2}} \equiv 1$. Bezeichnen wir nun den bei der Division von y^2 durch a bleibenden Rest überhaupt durch ϱy^2; so haben wir folgende $\frac{a-1}{2}$ Wurzeln unserer Congruenz:

$$\varrho 1, \varrho 4, \varrho 9, \varrho 16, \varrho 25, \ldots \varrho \left(\frac{a-1}{2}\right)^2,$$

deren jede $< a$ und positiv ist. Auch überzeugt man sich leicht, daß alle diese Wurzeln ungleich sind. Wäre nämlich, wenn y^2 und z^2 irgend zwei Glieder der erstern Reihe bezeichnen,

$$y^2 = ap + r, \quad z^2 = aq + r,$$

so daß nämlich die bei der Division von y^2 und z^2 durch a bleibenden Reste einander gleich wären; so wäre

$$y^2 - z^2 = a(p - q) = (y - z)(y + z),$$

und folglich dieses Product, also auch, da a eine Primzahl ist, entweder $y - z$, oder $y + z$ durch a theilbar (I. 3.), welches nicht möglich ist, da $y < \frac{1}{2}a$, $z < \frac{1}{2}a$, also immer $y - z$ sowohl, als auch $y + z < a$ ist. Die obigen $\frac{a-1}{2}$ Wurzeln sind also alle positiven Wurzeln unserer Congruenz, die $< a$ sind (II. 20.).

Wollte man nur ungerade Werthe von x haben, so behalte man in obiger Reihe die ungeraden Werthe bei, und addire zu den geraden a; so erhält man $\frac{a-1}{2}$ ungerade Wurzeln unserer Congruenz, deren jede offenbar nicht $> 2a-1$ ist, da die ursprünglichen Wurzeln alle $<$ a sind. Ist überhaupt α eine Wurzel unserer Congruenz; so ist auch $az+\alpha$ für jedes z eine Wurzel, da

$$(az+\alpha)^{\frac{a-1}{2}} = eaz + \alpha^{\frac{a-1}{2}},$$

$$(az+\alpha)^{\frac{a-1}{2}} \equiv \alpha^{\frac{a-1}{2}}; \text{ aber } \alpha^{\frac{a-1}{2}} \equiv 1;$$

also auch $(az+\alpha)^{\frac{a-1}{2}} \equiv 1$. Ist α eine ungerade Wurzel, so ist auch überhaupt $2az+\alpha$ eine ungerade Wurzel.

Sey z. B. $a = 13$, $\frac{a-1}{2} = 6$; so erhält man leicht:

Quadrate: 1, 4, 9, 16, 25, 36;
Reste: 1, 4, 9, 3, 12, 10;
Ungerade Wurzeln: 1, 17, 9, 3, 25, 23.

Also die Wurzeln überhaupt:

$$x = 13z + \{1, 4, 9, 3, 12, 10;$$

die ungeraden Wurzeln:

$$x = 26z + \{1, 17, 9, 3, 25, 23.$$

2. Alle Zahlen, welche $<$ a sind, und die Congruenz $x^{\frac{a-1}{2}} \equiv 1$ nicht auflösen, lösen die Congruenz $x^{\frac{a-1}{2}} \equiv -1$ auf. Ist nämlich a eine Primzahl, welche in x nicht aufgeht; so ist immer entweder $x^{\frac{a-1}{2}} \equiv 1$, oder $x^{\frac{a-1}{2}} \equiv -1$ (III. 9. 11.). Da nun a in keiner Zahl, welche $<$ a ist, aufgeht; so erhellet die Richtigkeit obiger Behauptung. Da die Anzahl der Auflösungen der Congruenz $x^{\frac{a-1}{2}} \equiv 1$, welche $<$ a sind, $= \frac{a-1}{2}$ ist (1,); so ist auch die Anzahl der Auflösungen der Congruenz $x^{\frac{a-1}{2}} \equiv -1$, welche $<$ a sind, $= a - 1 - \frac{a-1}{2} = \frac{a-1}{2}$.

Eben so leicht erhellet auch, daß jede ungerade Zahl, welche $< 2a$ ist, ausgenommen a, und die Congruenz $x^{\frac{a-1}{2}} \equiv 1$ nicht auflöset, eine Wurzel der Congruenz $x^{\frac{a-1}{2}} \equiv -1$ ist. a geht nämlich in keiner der Zahlen von 1 bis $2a - 1$ auf, ausgenommen in a; denn, ginge a in $2a - k$, wo $k < 2a$ und nicht $= o$ ist, auf, so wäre $\frac{2a-k}{a} = e$, $2a = ea + k$; also, weil $k < 2a$ und nicht $= o$ ist, e weder $= o$, noch $= 2$ oder > 2; also $e = 1$, $2a = a + k$, $a = k$, so daß also a nun in $2a - a = a$ aufgeht, wie schon oben erwähnt. Da nun für jede Primzahl a, welche in x nicht aufgeht, immer entweder $x^{\frac{a-1}{2}} \equiv 1$, oder $x^{\frac{a-1}{2}} \equiv -1$ ist; so ist jede Zahl in der Reihe der ungeraden Zahlen 1, 3, 5, 7, ... $2a - 1$, welche die Congruenz $x^{\frac{a-1}{2}} \equiv 1$ nicht auflöset, eine Auflösung der Congruenz $x^{\frac{a-1}{2}} \equiv -1$, ausgenommen a, welches weder die eine, noch die andere Congruenz auflöset, da a in $a^{\frac{a-1}{2}}$ aufgeht, und folglich offenbar weder in $a^{\frac{a-1}{2}} - 1$, noch in $a^{\frac{a-1}{2}} + 1$ aufgehen kann. Die Anzahl der Glieder der Reihe 1, 3, 5, 7, ... $2a - 1$ ist, wegen des Ausfalls von a, $= a - 1$; die Anzahl der ungeraden Auflösungen von $x^{\frac{a-1}{2}} \equiv 1$, von 1 bis $2a - 1$, $= \frac{a-1}{2}$ (1.); also die Anzahl der ungeraden Auflösungen von $x^{\frac{a-1}{2}} \equiv -1$, von 1 bis $2a - 1$, $= a - 1 - \frac{a-1}{2} = \frac{a-1}{2}$.

Für $a = 13$ ist demnach nach (1.) überhaupt in Bezug auf die Congruenz $x^{\frac{a-1}{2}} \equiv -1$:

$$x = 13z + \{2, 5, 6, 7, 8, 11$$

und für die ungeraden Auflösungen:

$$x = 26z + \{5, 7, 11, 15, 19, 21,$$

da 13 ausfällt.

So ist z. B. $5^{\frac{13-1}{2}} = 5^6 = 15625$, $5^6 + 1 = 15626 = 13.1202$.

3. Wenn a, a′ zwei ungleiche Primzahlen sind; so kann den Congruenzen

$$x^{\frac{a-1}{2}} \equiv \pm 1 \text{ (Mod. a)}, \quad x^{\frac{a'-1}{2}} \equiv \pm 1 \text{ (Mod. a')};$$

ohne daß die obern und untern Zeichen sich auf einander beziehen, immer zu gleicher Zeit in ungeraden Zahlen genügt werden.

Soll jeder der vorhergehenden Congruenzen einzeln in ungeraden Zahlen genügt werden; so ist nach dem Vorigen

$$x = 2az + \alpha \text{ und } x = 2a'z' + \alpha'$$

zu setzen. Da nun beiden Congruenzen zugleich genügt werden soll, so setze man

$$2az + \alpha = 2a'z' + \alpha', \; az - a'z' = \frac{\alpha' - \alpha}{2}.$$

Da α, α' nach dem Vorigen ungerade Zahlen sind, so ist $\frac{\alpha'-\alpha}{2}$ eine ganze Zahl, und die gefundene unbestimmte Gleichung des ersten Grades kann also, weil auch a und a′ relative Primzahlen sind, in ganzen Zahlen aufgelöset werden. Dadurch erhält man, für $\frac{\alpha'-\alpha}{2} = \gamma$:

$$z = a'z'' \pm a'_0\gamma, \; z' = az'' \pm a_0\gamma.$$

Also, um beiden Congruenzen zugleich zu genügen,

$$\begin{aligned} x &= 2a(a'z'' \pm a'_0\gamma) + \alpha \\ &= 2a'(az'' \pm a_0\gamma) + \alpha' \\ &= 2aa'z'' + \alpha \pm 2aa'_0\gamma \\ &= 2aa'z'' + \alpha' \pm 2a'a_0\gamma \end{aligned}$$

wo $\alpha \pm 2aa'_0\gamma = \alpha' \pm 2a'a_0\gamma$ eine ungerade Zahl, und der Coefficient von $z'' = 2aa'$ ist.

Kommt nun noch eine dritte Congruenz

$$x^{\frac{a''-1}{2}} \equiv \pm 1 \text{ (Mod. a'')}$$

hinzu; so erhellet leicht, daß, weil aa′ und a″ relative

Primzahlen sind, auf ähnliche Art allen drei Congruenzen in ungeraden Zahlen genügt werden kann. Die Ausdehnung dieser Schlußart auf noch mehrere Congruenzen ist leicht.

VIII. Einige merkwürdige Sätze von den Potenzen.

1. Die unbestimmte Gleichung

$$x^2 + y^2 = z^2$$

läßt sich immer in ganzen Zahlen auflösen; d. h. man kann immer zwei Quadrate finden, deren Summe wieder ein vollkommenes Quadrat ist. Man braucht nämlich bloß zu setzen:

$$x = p^2 - q^2,\ y = 2pq,\ z = p^2 + q^2;$$

weil, wie leicht erhellet, immer

$$(p^2 - q^2)^2 + (2pq)^2 = p^2 + q^2$$

ist. Drei Zahlen, welche den obigen unbestimmten Gleichung genügen, bilden ein rechtwinkliges Dreieck. Eine schöne Reihe von Aufgaben über solche Dreiecke enthält Diophant's sechstes Buch.

2. Man kann aber auch umgekehrt zeigen, daß jede drei Zahlen, welche der Gleichung

$$x^2 + y^2 = z^2$$

genügen, von den Formen

$$p^2 - q^2,\ 2pq,\ p^2 + q^2$$

seyn müssen.

Zunächst ist klar, daß man immer annehmen kann, daß x, y, z kein gemeinschaftliches Maaß haben, weil ein solches offenbar immer durch Division weggeschafft werden könnte. Eben so leicht überzeugt man sich aber auch, daß je zwei der Zahlen x, y, z kein gemeinschaftliches Maaß haben können. Ginge nämlich z. B. die Primzal Θ in x und y auf, so müßte, wegen obiger Gleichung, Θ auch in z^2, folglich (I. 3.) auch in z aufgehen, so daß also Θ ein Maaß von x, y, z wäre, gegen das Obige. Also können x, y nicht beide gerade seyn. Es können aber auch

x, y nicht beide ungerade seyn. Wäre nämlich $x = 2n + 1$, $y = 2m + 1$, so wäre

$$x^2 + y^2 = 4n^2 + 4m^2 + 4n + 4m + 2 = z^2,$$

also z^2 durch 2, aber nicht durch 4 theilbar, welches ungereimt ist, da 2, welches in z^2 aufgeht, als Primzahl auch in z aufgehen muß (I. 3.), so daß also, wenn 2 in z^2 aufgeht, nothwendig auch 4 darin aufgehen muß. Demnach ist immer eine der Zahlen x, y, gerade, die andere ungerade. Sey nun x gerade, also y ungerade. Aus der Gleichung folgt

$$1 + \left(\frac{y}{x}\right)^2 = \left(\frac{z}{x}\right)^2.$$

Man setze

$$\sqrt{1 + \left(\frac{y}{x}\right)^2} = \frac{y}{x} + P,$$

$$1 + \left(\frac{y}{x}\right)^2 = \left(\frac{y}{x}\right)^2 + 2P\frac{y}{x} + P^2,$$

$$\frac{y}{x} = \frac{1 - P^2}{2P}.$$

Setzen wir nun allgemeiner

$$P = \frac{q}{p},$$

wo offenbar immer angenommen werden kann, daß p, q relative Primzahlen sind; so wird

$$\frac{y}{x} = \frac{p^2 - q^2}{2pq}.$$

$p^2 - q^2$ und $2pq$ sind relative Primzahlen. Ginge nämlich die Primzahl Θ, welche wir zuerst > 2 annehmen wollen, in $p^2 - q^2$ und in $2pq$ auf; so müßte Θ, da es in $2pq$ aufgeht, und > 2 ist, entweder in p, oder in q aufgehen (I. 3.). Ginge es nun z. B. in p, also auch in p^2 auf, so müßte es, da es in $p^2 - q^2$ aufgeht, auch in q^2, folglich, als Primzahl, auch in q aufgehen (I. 3.), so daß also, gegen die Voraussetzung, p und q nicht relative Primzahlen wären. Ginge ferner 2 in $p^2 - q^2$ und $2pq$ auf, so müßten p, q, da sie nicht beide gerade seyn können, beide ungerade seyn, so daß also auch pq eine ungerade Zahl, und folglich, zugleich nach dem Vorhergehenden, offenbar der Bruch

$$\frac{(p^2-q^2):2}{pq},$$

so wie der ihm gleiche Bruch $\frac{y}{x}$, auf seine kleinste Benennung gebracht wäre. Also wäre

$$y = \frac{p^2-q^2}{2},\ x = pq,$$

d. i. x eine ungerade Zahl, gegen die Voraussetzung. Demnach haben p^2-q^2 und $2pq$ nie ein gemeinschaftliches Maaß, und der Bruch

$$\frac{p^2-q^2}{2pq}$$

ist also, so wie der ihm gleiche Bruch $\frac{y}{x}$, auf die kleinste Benennung gebracht, woraus unmittelbar folgt:

$$y = p^2 - q^2,\ x = 2pq.$$

Also

$$\begin{aligned} z^2 &= x^2 + y^2 = (2pq)^2 + (p^2-q^2)^2 \\ &= p^4 + 2p^2q^2 + q^4 = (p^2+q^2)^2, \\ z &= p^2 + q^2. \end{aligned}$$

Folglich sind x, y, z immer von der angegebenen Form, w. z. b. w.

Es ist z. B.

$$3^2 + 4^2 = 5^2,\ 3 = 2^2 - 1,\ 4 = 2.2.1,\ 5 = 2^2 + 1;$$
$$5^2 + 12^2 = 13^2,\ 5 = 3^2 - 2^2,\ 12 = 2.3.2,\ 13 = 3^2 + 2^2.$$

Der Beweis des obigen Satzes hätte sich auch aus Sätzen der unbestimmten Analytik kürzer ableiten lassen; ich hielt es aber für besser, ihn hier unabhängig von diesen Sätzen zu beweisen, weil er für das Folgende von besonderer Wichtigkeit ist.

3. Die Summe zweier Biquadrate kann nie ein Quadrat seyn, wenn nicht eins derselben gleich Null ist. Sey

$$a^4 + b^4 = c^2,$$

wo man offenbar annehmen kann, daß a, b relative Primzahlen sind; so ist (2.)

$$a^2 = p^2 - q^2,\ b^2 = 2pq,\ c = p^2 + q^2,$$

und p, q sind relative Primzahlen, weil, wenn p, q den gemeinschaftlichen Primfactor Θ hätten, auch a^2, b^2, folglich auch a, b (I. 3.), diesen gemeinschaftlichen Prim-

factor haben, also nicht relative Primzahlen seyn würden. Auch können p, q nicht beide ungerade seyn, weil sonst offenbar a^2, b^2, also auch a, b, beide gerade, folglich wieder nicht relative Primzahlen wären. Endlich kann auch nicht p gerade, q ungerade seyn, weil sonst $p^2 - q^2$ von der Form $4k - 1 = 4(k-1) + 3 = 4n + 3$ seyn würde, diese Form aber offenbar nicht dem vollkommenen Quadrate $p^2 - q^2 = a^2$ zukommen kann. Also ist p ungerade, q gerade. Setzt man nun

$$p = \gamma^2,\ q = 2\lambda^2\ ,$$

wo γ, λ, wie p, q, relative Primzahlen sind; so folgt aus der Gleichung $p^2 - q^2 = a^2$ sogleich:

$$\gamma^4 - 4\lambda^4 = a^2,\ a^2 + (2\lambda^2)^2 = (\gamma^2)^2\ .$$

Also (2.)

$$a = f^2 - g^2,\ 2\lambda^2 = 2fg,\ \gamma^2 = f^2 + g^2\ ,$$

wo wieder f, g, wie γ, λ, relative Primzahlen sind. Daher kann wegen der Gleichung $\lambda^2 = fg$ offenbar bloß

$$f = \alpha^2,\ g = \beta^2$$

seyn, wo α, β ebenfalls relative Primzahlen sind. Also, wegen der Gleichung $f^2 + g^2 = \gamma^2$:

$$\alpha^4 + \beta^4 = \gamma^2\ .$$

Da nun

$$a = f^2 - g^2 = \alpha^4 - \beta^4\ ,$$
$$b = \sqrt{2pq} = 2\gamma\lambda = 2\sqrt{fg(f^2+g^2)} = 2\alpha\beta\sqrt{\alpha^4+\beta^4}\ ;$$

so erhellet zunächst, daß weder α, noch β, $= 0$ seyn kann, weil sonst, gegen die Voraussetzung, auch $b = 0$ seyn würde. Ferner ist

$$f^2 + g^2 = \alpha^4 + \beta^4 = \gamma^2 = \sqrt{a^2 + 4\lambda^4} = \sqrt{a^2 + q^2}\ ;$$
$$p^2 = a^2 + q^2,\ 4p^2q^2 = b^4,\ 4(a^2+q^2)q^2 = b^4\ ;$$
$$q^4 + a^2q^2 = \tfrac{1}{4}b^4\ .$$

Die Auflösung dieser quadratischen Gleichung giebt

$$q^2 = -\tfrac{1}{2}a^2 \pm \tfrac{1}{2}\sqrt{a^4+b^4}\ ,$$

wo, da q^2 immer positiv ist, bloß das obere Zeichen gelten kann. Also

$$\alpha^4 + \beta^4 = \sqrt{(\tfrac{1}{2}a^2 + \tfrac{1}{2}\sqrt{a^4+b^4})}\ .$$

Da nun offenbar

$$a^2 < \sqrt{a^4+b^4},\ \tfrac{1}{2}a^2 < \tfrac{1}{2}\sqrt{a^4+b^4}$$

ist, weil b nicht $= 0$; so ist

$$\tfrac{1}{2}a^2 + \tfrac{1}{2}\sqrt{a^4 + b^4} < \sqrt{a^4 + b^4},$$
$$\alpha^4 + \beta^4 < \sqrt{\sqrt{a^4 + b^4}},$$
$$\alpha^4 + \beta^4 < \sqrt[4]{a^4 + b^4}, \gamma^2 < \sqrt[4]{c^2},$$
$$\gamma^2 < \sqrt{c}, \gamma < \sqrt[4]{c}.$$

Da weder α, noch β, $= 0$; so ist auch γ nicht $= 0$.

Aus diesem allgemeinen Beweise ergiebt sich nun, daß, wenn $a^4 + b^4 = c^2$ seyn könnte, wo a, b relative Primzahlen sind, und keine $= 0$ ist, aus dieser Gleichung eine Reihe Gleichungen von der Form

$$a^4 + b^4 = c^2,$$
$$a'^4 + b'^4 = c'^2,$$
$$a''^4 + b''^4 = c''^2,$$
$$a'''^4 + b'''^4 = c'''^2,$$
$$\text{ꝛc.} \qquad \text{ꝛc.}$$

abgeleitet werden könnte, in denen alle durch a, b bezeichneten Größen relative Primzahlen sind, und keine $= 0$ ist, die Größen

$$c, c', c'', c''', c'''', \ldots\ldots$$

aber eine abnehmende Reihe bilden würden, ohne daß man jemals auf ein Glied $= 0$ käme, so daß also diese Reihe in's Unendliche abnehmen würde, welches ungereimt ist, da c eine endliche ganze Zahl bezeichnet. Also kann die Gleichung $a^4 + b^4 = c^2$ nicht Statt finden, und unser Satz ist folglich bewiesen.

Aus diesem Satze folgt unmittelbar, daß auch die Summe zweier Biquadrate nie ein Biquadrat seyn kann.

Könnte $a^4 - b^4 = c^4$ seyn, so wäre $a^4 = b^4 + c^4$, welches nach dem so eben Bewiesenen nicht möglich ist. Also kann auch die Differenz zweier Biquadrate nie ein Biquadrat seyn. Uebrigens kann auch auf eine der vorigen ähnliche Art gezeigt werden, daß die Differenz zweier Biquadrate nie ein Quadrat seyn kann (Legendre a. a. O. p. 343. Élémens d'Algèbre par L. Euler. Nouv. éd. Paris. 1807. II. p. 179.).

4. Wir haben den vorigen Satz vorzüglich der Beweisart wegen hier mitgetheilt, da dieselbe bei Untersu-

chungen in der Zahlenlehre oft mit Vortheil angewandt werden kann. Fermat behauptet in seinen Noten zu Diophant (p. 61.), daß überhaupt die unbestimmte Gleichung

$$x^n + y^n = z^n$$

unmöglich, d. h. in ganzen Zahlen nicht auflösbar ist, wenn n den zweiten Grad übersteigt. Der Beweis dieses Satzes ist jedoch noch nicht gegeben. Für $n = 3$ hat ihn Euler bewiesen (a. a. O. p. 262. ff. Legendre a. a. O. p. 345.). Die Methode des Beweises ist dieselbe wie vorher; jedoch erfordert derselbe mehrere Entwickelungen, die sich hier, der Beschränktheit des Raumes wegen, nicht mittheilen ließen. Für $n = 5$ hat Lejeune Dirichlet mehrere Sätze bewiesen in der Abhandlung: Mém. sur l'impossibilité de quelques équations indéterminées du cinquième degré (Crelles Journal. III. 4. S. 354.).

Auch folgende von Fermat gefundene, u. A. von Legendre (a. a. O. p. 340. sqq.) bewiesene, Sätze gehören hierher:

Die Formel $x^4 + 2y^4$ kann nie ein vollkommenes Quadrat werden, außer wenn $y = 0$ ist.

Keine Trigonalzahl, die Einheit ausgenommen, kann ein Biquadrat seyn.

Weder die Summe, noch die Differenz zweier Cubikzahlen kann das Doppelte eines vollkommenen Cubus seyn.

Keine Trigonalzahl, die Einheit ausgenommen, kann ein vollkommener Cubus seyn.

Noch mehrere Sätze dieser Art s. m. a. a. O.

IX. Einige Sätze von den arithmetischen Progressionen.

1. Sey

$$A - C,\ 2A - C,\ 3A - C,\ \ldots\ nA - C$$

irgend eine arithmetische Progression, und Θ eine Zahl, welche mit A relative Primzahl ist. Man soll die Anzahl der durch Θ theilbaren Gliedern obiger Progression finden.

Da A und Θ relative Primzahlen sind, so läßt sich die unbestimmte Gleichung des ersten Grades

$$Ax - \Theta y = - C$$

immer in ganzen Zahlen auflösen (Unbestimmte Analysis.), und sich folglich auch immer ein Werth von x finden, für welchen $Ax + C$ durch Θ theilbar wird. Ist dieser Werth $= \alpha$, so erhellet leicht, daß überhaupt $\alpha \pm \Theta z$ ein solcher Werth von x seyn wird, da offenbar dann auch $A(\alpha \pm \Theta z) + C = A\alpha + C \pm \Theta z$ durch Θ theilbar ist. Folglich kann man für x auch immer einen positiven Werth finden, welcher zugleich $< \Theta$ ist. Ist nämlich α positiv, so sey $\alpha = \Theta z + \varrho$, wo $\varrho < \Theta$, und folglich ein Werth von $x = \Theta z + \varrho - \Theta z = \varrho$. Ist aber α negativ, so sey $- \alpha = \Theta z - \varrho$, wo wieder $\varrho < \Theta$; dann ist $x = - \Theta z + \varrho + \Theta z = \varrho$ wieder ein Werth von der gesuchten Beschaffenheit. Auch erhellet leicht, daß es immer nur einen Werth von x geben kann, welcher positiv und $< \Theta$ ist. Wären ϱ und ϱ' zwei solche Werthe, und $\varrho' < \varrho$; so wäre

$$A\varrho + C = \Theta y, \; A\varrho' + C = \Theta y' ;$$

also $A(\varrho - \varrho') = \Theta(y - y')$, und folglich $A(\varrho - \varrho')$, also, weil A und Θ relative Primzahlen sind, auch $\varrho - \varrho'$ durch Θ theilbar (I. 7.), welches unmöglich ist, da $\varrho - \varrho'$ offenbar $< \Theta$ ist.

Bezeichnen wir nun den Werth von x, welcher positiv und $< \Theta$ ist, für welchen aber $Ax + C$ durch Θ theilbar ist, durch Θ^0, so sind die durch Θ theilbaren Glieder obiger arithmetischen Progression:

$$A(\Theta - \Theta^0) - C, \; A(2\Theta - \Theta^0) - C, \; A(3\Theta - \Theta^0) - C, \; \ldots.$$

Daß alle diese Glieder durch Θ theilbar sind, fällt in die Augen. Daß es aber außer diesen Gliedern auch keine andern durch Θ theilbaren Glieder geben kann, läßt sich so zeigen. Seyen

$$A\{\mu\Theta - \Theta^0\} - C, \; A\{(\mu + 1)\Theta - \Theta^0\} - C$$

überhaupt zwei auf einander folgende Glieder vorstehender Reihe. Läge zwischen denselben noch irgend ein Glied $Ax - C$, so daß

$$x > \mu\Theta - \Theta^0, x < (\mu+1)\Theta - \Theta^0,$$

welches durch Θ theilbar wäre; so wären auch die Differenzen

$$A\{x - \mu\Theta + \Theta^0\}, A\{(\mu+1)\Theta - \Theta^0 - x\},$$

und folglich, weil A und Θ relative Primzahlen sind, auch

$$x - \mu\Theta + \Theta^0, (\mu+1)\Theta - x - \Theta^0,$$

also auch $x + \Theta^0$ durch Θ theilbar. Es ist aber

$$x + \Theta^0 > \mu\Theta, x + \Theta^0 < (\mu+1)\Theta;$$
$$\frac{x+\Theta^0}{\Theta} > \mu, \frac{x+\Theta^0}{\Theta} < \mu+1;$$

also offenbar $\frac{x+\Theta^0}{\Theta} = \mu +$ einem ächten Bruche, und folglich keine ganze Zahl. Also kann es außer den obigen keine durch Θ theilbaren Glieder geben. Wegen der vor dem ersten Gliede $A(\Theta - \Theta^0) - C$ vorhergehenden Glieder bemerke man nur, daß auch $- A\Theta^0 - C$ nach dem Obigen durch Θ theilbar ist, und folglich wie vorher geschlossen werden kann.

Die Reihe der durch Θ theilbaren Glieder ist so weit fortzusetzen, als die Größen $\Theta - \Theta^0, 2\Theta - \Theta^0, 3\Theta - \Theta^0, \ldots$ die Gliederzahl n der gegebenen Reihe nicht übersteigen. Sey nun

$$k\Theta - \Theta^0 \leqq n, (k+1)\Theta - \Theta^0 > n;$$

so ist

$$k \leqq \frac{n+\Theta^0}{\Theta}, k+1 > \frac{n+\Theta^0}{\Theta};$$

und folglich, wenn die größte in $\frac{n+\Theta^0}{\Theta}$ enthaltene ganze Zahl durch $G\left(\frac{n+\Theta^0}{\Theta}\right)$ bezeichnet wird, k, oder die Anzahl der durch Θ theilbaren Glieder unserer arithmetischen Progression, $= G\left(\frac{n+\Theta^0}{\Theta}\right)$.

2. Ist also jetzt Θ eine in A nicht aufgehende Primzahl, so ist die Anzahl der durch Θ nicht theilbaren Glieder obiger arithmethischen Progression, wenn wir dieselbe durch y bezeichnen, $=$

$$y = n - G\left(\frac{n+\Theta^0}{\Theta}\right).$$

3. Sind Θ, λ zwei in A nicht aufgehende Primzahlen; so ist die Anzahl der durch Θ theilbaren Glieder $= G\left(\frac{n+\Theta^0}{\Theta}\right)$, die Anzahl der durch λ theilbaren Glieder $= G\left(\frac{n+\lambda^0}{\Theta}\right)$, und weil auch A und $\Theta\lambda$ relative Primzahlen sind, die Anzahl durch $\Theta\lambda$ theilbaren Glieder $= G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right)$ (1).

Folglich offenbar die Anzahl der durch Θ und λ nicht theilbaren Glieder =

$$y = n - G\left(\frac{n+\Theta^0}{\Theta}\right) + G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right) - G\left(\frac{n+\lambda^0}{\lambda}\right)$$

$$= n - \int G\left(\frac{n+\Theta^0}{\Theta}\right) + G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right),$$

wo das Summenzeichen bloß die Bedeutung hat, daß für Θ sowohl Θ, als auch λ zu setzen ist. Daß $G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right)$ addirt werden muß, fällt sogleich in die Augen, wenn man überlegt, daß mit $G\left(\frac{n+\Theta^0}{\Theta}\right)$ und $G\left(\frac{n+\lambda^0}{\lambda}\right)$ die durch $\Theta\lambda$ theilbaren Glieder offenbar einmal zu viel abgezogen sind.

4. Seyen ferner Θ, λ, μ drei nicht in A aufgehende Primzahlen; so ist die Anzahl der durch Θ, λ nicht theilbaren Glieder, nach dem Vorhergehenden

$$= n - G\left(\frac{n+\Theta^0}{\Theta}\right) + G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right) - G\left(\frac{n+\lambda^0}{\lambda}\right).$$

Die Anzahl der durch μ theilbaren Glieder, in denen aber zugleich weder Θ, noch λ, aufgeht, ist

$$= G\left(\frac{n+\mu^0}{\mu}\right) - G\left(\frac{n+(\Theta\mu)^0}{\Theta\mu}\right) + G\left(\frac{n+(\Theta\lambda\mu)^0}{\Theta\lambda\mu}\right) - G\left(\frac{n+(\lambda\mu)^0}{\lambda\mu}\right)$$

wovon man sich leicht auf ähnliche Art, wie vorher, überzeugt. Diese Anzahl muß, um die Anzahl der durch Θ,

λ, μ nicht theilbaren Glieder zu finden, von dem vorigen Resultat noch abgezogen werden, wodurch man

$$y = n - G\left(\frac{n+\Theta^0}{\Theta}\right) + G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right) - G\left(\frac{n+(\Theta\lambda\mu)^0}{\Theta\lambda\mu}\right)$$
$$- G\left(\frac{n+\lambda^0}{\lambda}\right) + G\left(\frac{n+(\Theta\mu)^0}{\Theta\mu}\right)$$
$$- G\left(\frac{n+\mu^0}{\mu}\right) + G\left(\frac{n+(\lambda\mu)^0}{\lambda\mu}\right)$$
$$= n - \int G\left(\frac{n+\Theta^0}{\Theta}\right) + \int G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right) - G\left(\frac{n+(\Theta\lambda\mu)^0}{\Theta\lambda\mu}\right)$$

erhält. Die Bedeutung der Summenzeichen wird leicht erhellen.

5. Kommt noch eine vierte in A nicht aufgehende Primzahl ν hinzu; so ist ganz auf dieselbe Weise die Anzahl der durch ν theilbaren Glieder, in denen aber Θ, λ, μ nicht aufgehen,

$$= G\left(\frac{n+\nu^0}{\nu}\right) - G\left(\frac{n+(\Theta\nu)^0}{\Theta\nu}\right) + G\left(\frac{n+(\Theta\lambda\nu)^0}{\Theta\lambda\nu}\right) - G\left(\frac{n+(\Theta\lambda\mu\nu)^0}{\Theta\lambda\mu\nu}\right)$$
$$- G\left(\frac{n+(\lambda\nu)^0}{\lambda\nu}\right) + G\left(\frac{n+(\Theta\mu\nu)^0}{\Theta\mu\nu}\right)$$
$$- G\left(\frac{n+(\mu\nu)^0}{\mu\nu}\right) + G\left(\frac{n+(\lambda\mu\nu)^0}{\lambda\mu\nu}\right).$$

Diese Größe muß, um die Anzahl der durch Θ, λ, μ, ν nicht theilbaren Glieder zu finden, von dem vorigen Resultat noch abgezogen werden, wodurch man für die gesuchte Größe erhält:

$$y = n - \int G\left(\frac{n+\Theta^0}{\Theta}\right) + \int G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right)$$
$$- \int G\left(\frac{n+(\Theta\lambda\mu)^0}{\Theta\lambda\mu}\right) + G\left(\frac{n+(\Theta\lambda\mu\nu)^0}{\Theta\lambda\mu\nu}\right).$$

6. Also kann man allgemein setzen:

$$y = n - \int G\left(\frac{n+\Theta^0}{\Theta}\right) + \int G\left(\frac{n+(\Theta\lambda)^0}{\Theta\lambda}\right) - \int G\left(\frac{n+(\Theta\lambda\mu)^0}{\Theta\lambda\mu}\right) + \ldots$$

die Reihe so weit fortgesetzt, bis sie von selbst abbricht.

Für die Reihe der ungeraden Zahlen ist $A = 2$, $C = 1$, und, wenn k eine nicht durch 2 theilbare Zahl ist, der Werth von k^0, für welchen $2k^0 + 1$ durch k theilbar wird, $= \frac{1}{2}(k-1)$, welcher Werth positiv und $< k$ ist.

Dadurch erhält man für die ersten 100 Glieder der Reihe der ungeraden Zahlen die Anzahl der durch 3, 5, 7, 11 nicht theilbaren Zahlen =

$$\begin{aligned} y = 100 &- G\left(\frac{101}{3}\right) + G\left(\frac{107}{15}\right) - G\left(\frac{152}{105}\right) + G\left(\frac{677}{1155}\right) \\ &- G\left(\frac{102}{5}\right) + G\left(\frac{110}{21}\right) - G\left(\frac{182}{165}\right) \\ &- G\left(\frac{103}{7}\right) + G\left(\frac{116}{33}\right) - G\left(\frac{215}{231}\right) \\ &- G\left(\frac{105}{11}\right) + G\left(\frac{117}{35}\right) - G\left(\frac{292}{385}\right) \\ &+ G\left(\frac{127}{55}\right) \\ &+ G\left(\frac{138}{77}\right) \end{aligned}$$

wo aber

$$G\left(\frac{215}{231}\right) = G\left(\frac{292}{385}\right) = G\left(\frac{677}{1155}\right) = 0$$

ist, und diese Glieder daher weggelassen werden können. Nach gehöriger Reduction findet man $y = 43$.

7. Ist n durch das Product aller gegebenen Primzahlen theilbar, so ist, da $\Theta^0 < \Theta$, für eine Primzahl offenbar $G\left(\frac{n + \Theta^0}{\Theta}\right) = \frac{n}{\Theta}$, und folglich

$$y = n - \frac{n}{\Theta} = n\left(1 - \frac{1}{\Theta}\right).$$

Eben so erhält man, wenn zwei Primzahlen gegeben sind, in diesem Falle

$$\begin{aligned} y = n - \frac{n}{\Theta} + \frac{n}{\Theta\lambda} &= n\left(1 - \frac{1}{\Theta}\right)\left(1 - \frac{1}{\lambda}\right) \\ &- \frac{n}{\lambda}. \end{aligned}$$

Sind drei Primzahlen gegeben, so wird

$$\begin{aligned} y = n &- \frac{n}{\Theta} + \frac{n}{\Theta\lambda} - \frac{n}{\Theta\lambda\mu} \\ &- \frac{n}{\lambda} + \frac{n}{\Theta\mu} \\ &- \frac{n}{\mu} + \frac{n}{\lambda\mu} \\ = n&\left(1 - \frac{1}{\Theta}\right)\left(1 - \frac{1}{\lambda}\right)\left(1 - \frac{1}{\mu}\right). \end{aligned}$$

Die Allgemeinheit des hier schon leicht zu bemerkenden Gesetzes wird aus den obigen combinatorischen Formeln mittelst des bekannten Productensatzes aus der combinatorischen Analysis oder der Theorie der Gleichungen (Gleichung. 144. 165.) leicht geschlossen.

Ist z. B. $A = 6$, $C = 4$, und 2, 8, 14, 20, 26, 32, 38, 44, 50, 56, 62, 68, 74, 80, 86 die gegebenen Progression, also $n = 15$, $\Theta = 5$; so ist $y = 15.(1 - \frac{1}{5}) = 12$, so wie denn in der That auch die Anzahl der durch 5 nicht theilbaren Glieder obiger Reihe $= 12$ ist.

Mehrere Anwendungen der hier entwickelten merkwürdigen Formeln, namentlich auch auf die Bestimmung der Anzahl der Primzahlen innerhalb gewisser Gränzen giebt Legendre (Théorie des nombres. IV. Part. §. XI.).

X. Fermat's Satz von der Zerlegung jeder Zahl in vier Quadratzahlen.

1. Wenn n eine Primzahl ist, welche in A nicht aufgeht, so lassen sich x und y immer in ganzen Zahlen so bestimmen, daß, A und B mögen positive oder negative ganze Zahlen seyn,

$$x^2 - Ay^2 - B$$

durch B theilbar ist.

Ginge n in B auf, so brauchte man bloß für x und y Vielfache von n zu setzen, wodurch das Verlangte augenblicklich erreicht würde. Man kann also im Folgenden annehmen, daß n in B nicht aufgeht.

Für $n = 1$ ist der Satz klar. Für $n = 2$ nehme man für y irgend eine gerade Zahl. Dann geht $n = 2$ in Ay^2 auf. Nimmt man nun für x eine ungerade Zahl, so ist x^2 ungerade; aber, da n in B nicht aufgehen soll, auch B ungerade; also $x^2 - B$ gerade. Folglich geht $n = 2$ in

$$x^2 - Ay^2 - B$$

auf.

Für $n > 2$ sey $n = 2a + 1$, und man unterscheide nun folgende Fälle.

1) Giebt es für y einen Werth, für welchen $Ay^2 + B$ durch n theilbar wird, so nehme man für x ein Vielfaches von n; dann ist offenbar

$$x^2 - Ay^2 - B$$

durch n theibar.

2) Giebt es aber keinen Werth von y, für welchen n in $Ay^2 + B$ aufgeht, so setze man

$$Ay^2 + B = V,\ x^2 - Ay^2 - B = x^2 - V.$$

Nun ist, wie leicht erhellet

$$\frac{x^{2a} - V^a}{x^2 - V} = P =$$

$$x^{2a-2} + x^{2a-4}V + \ldots + x^2V^{a-2} + V^{a-1};$$

also P eine ganze Zahl. Folglich

$$x^{2a} - V^a = (x^2 - V)P = x^{2a} - 1 - (V^a - 1);$$

$$(x^2 - V)PQ = (x^{2a} - 1)Q - (V^{2a} - 1),$$

für $Q = V^a + 1$. Nach der Fermat'schen Satze (III. 1.) geht die Primzahl $n = 2a + 1$ in $x^{2a} - 1$ auf, wenn sie in x nicht aufgeht, und eben so in $V^{2a} - 1$, wenn sie in V nicht aufgeht. Also geht, wenn n weder in x, noch in V aufgeht, n in $(x^2 - V)PQ$, folglich, wenn es weder in P, noch in Q aufgeht, in

$$x^2 - V = x^2 - Ay^2 - B$$

auf (I. 5.). Hieraus erhellet nun, daß x und y, wenn n in

$$x^2 - Ay^2 - B$$

aufgehen soll, so bestimmt werden müssen, daß folgenden Bedingungen genügt wird:

n darf in V nicht aufgehen;
n darf in Q nicht aufgehen;
n darf in P nicht aufgehen;
n darf in x nicht aufgehen.

Es fragt sich nun, ob die gleichzeitige Erfüllung dieser Bedingungen immer möglich ist.

Die erste ist als erfüllt anzusehen, da es nach der

Voraussetzung keinen Werth von y giebt, für welchen $Ay^2 + B = V$ durch n theilbar ist.

In Bezug auf die zweite Bedingung ist nach dem Binomialtheorem

$$Q = V^a + 1 = (Ay^2 + B)^a + 1$$
$$= A^a y^{2a} + \frac{a}{1} A^{a-1} B y^{2a-2} + \frac{a(a-1)}{1.2} A^{a-2} B^2 y^{2a-4} + \ldots$$
$$\ldots + \frac{a(a-1)}{1.2} A^2 B^{a-2} y^4 + \frac{a}{1} A B^{a-1} y^2 + B^a + 1 .$$

Ist nun

α) $B^a + 1$ durch n nicht theilbar, so setze man $y = o$, und die zweite Bedingung wird erfüllt seyn.

β) Ist aber $B^a + 1$ durch n theilbar, so sey

$$Q' = A^a y^{2a-2} + \frac{a}{1} A^{a-1} B y^{2a-4} + \frac{a(a-1)}{1.2} A^{a-2} B^2 y^{2a-6} + \ldots$$
$$\ldots + \frac{a(a-1)}{1.2} A^2 B^{a-2} y^2 + \frac{a}{1} A B^{a-1} .$$

Dies ist ein Polynom vom Grade $2a - 2$, wo nach der Voraussetzung n in A, also auch in A^a (I. 4.) nicht aufgeht. Folglich giebt es (II. 20.) höchstens $2a - 2$ Werthe von y zwischen $-\frac{1}{2}n$ und $+\frac{1}{2}n$, für welche Q' durch n theilbar wird. Da aber $\frac{1}{2}n = a + \frac{1}{2}$ ist; so giebt es zwischen den angegebenen Gränzen, die Null mit gerechnet, überhaupt $2a + 1 = n$ Werthe, welche für y gesetzt werden können. Aber nur höchstens für $2a - 2$ Werthe wird Q' durch n theilbar. Also giebt es zwischen den angegebenen Gränzen immer gewiß wenigstens $2a + 1 - (2a - 2) = 3$ Werthe von y, für welche Q' nicht durch n theilbar wird. Alle diese Werthe sind $< n$, und es geht also, wenn einer derselben dem y beigelegt wird, n in y, also auch in y^2, so wie in $Q'y^2$ nicht auf (I. 4.). Nach der Voraussetzung ging aber n in $B^a + 1$ auf; also nicht in $Q'y^2 + B^a + 1 = Q$, wodurch folglich die zweite Bedingung erfüllt ist.

Nachdem nun y, folglich V, auf diese Weise bestimmt ist; so ist in

$$P = x^{2a-2} + x^{2a-4} V + \ldots + x^2 V^{a-2} + V^{a-1}$$

nur x noch unbekannt. Der Coefficient des höchsten Glie-

des dieses Polynoms vom Grade $2a - 2$ ist $= 1$, und folglich durch $n > 2$ nicht theilbar. Also giebt es zwischen $-\frac{1}{2}n$ und $+\frac{1}{2}n$ höchstens $2a - 2$ Werthe von x, für welche P durch n theilbar ist (II. 20.); die Anzahl aller Werthe von n zwischen diesen Gränzen, die Null mit gerechnet, ist wie vorher $= 2a + 1$, so daß es also zwischen diesen Gränzen wenigstens $2a + 1 - (2a - 2) = 3$ Werthe von x giebt, für welche P durch n nicht theilbar ist, wodurch ferner die dritte Bedingung erfüllt ist. Mit ihr ist aber auch zugleich die vierte erfüllt, weil die in Rede stehenden 3 Werthe von x alle $< n$ sind, und demnach keiner derselben, wenn man ihn für x setzt, durch n, also auch x nicht durch n theilbar ist.

Also lassen sich x, y immer so bestimmen, daß die obigen vier Bedingungen gleichzeitig erfüllt werden, und man kann folglich x, y immer so bestimmen, daß die in A nicht aufgehende Primzahl n in

$$x^2 - Ay^2 - B$$

aufgeht. Dieser Satz gilt also auch von den speciellern Formeln

$$x^2 + y^2 + 1 \text{ und } x^2 + y^2 - 1,$$

wenn man $A = -1, B = -1$, oder $A = -1, B = 1$ setzt.

Der Erfinder dieses merkwürdigen Satzes ist Lagrange (Mém. de Berlin. 1770.). Die zuletzt erwähnten speciellen Fälle hatte schon Euler gefunden (Nov. Comm. Petrop. T. V.). M. s. auch Legendre. a. a. O. p. 182.

2. Das Quadrat jeder viertheiligen Größe $a + b + c + d$ besteht aus den Quadraten der einzelnen Theile, und den doppelten Producten von je zwei Theilen in einander. Denn es ist

$$(a + b + c + d)^2$$
$$= a^2 + b^2 + c^2 + d^2$$
$$+ 2ab + 2ac + 2ad + 2bc + 2bd + 2cd.$$

3. Das Product zweier Summen von vier Quadraten in einander ist wieder eine Summe von vier Quadraten. Denn es ist, wovon man sich durch wirkliche Entwicke-

lung der Quadrate der viertheiligen Größen sogleich überzeugt,

$$\begin{aligned}&(p^2 + q^2 + r^2 + s^2)(p'^2 + q'^2 + r'^2 + s'^2)\\ = \;&(pp' + qq' + rr' + ss')^2 + (pq' - qp' + rs' - sr')^2\\ &+ (pr' - qs' - rp' + sq')^2 + (ps' + qr' - rq' - sp')^2 .\end{aligned}$$

Multiplicirt man also mehrere Summen von vier Quadraten in einander, so erhält man immer wieder eine Summe von vier Quadraten.

4. Jede Primzahl n kann in vier Quadraten zerlegt werden, und ist also von der Form

$$p^2 + q^2 + r^2 + s^2 .$$

Da n eine Primzahl ist, so kann man p und q so bestimmen, daß n in $p^2 + q^2 + 1$ aufgeht (1.). Eben so lassen sich für r und s zwei Werthe finden, so daß n in $r^2 + s^2 - 1$ aufgeht (1.). Also lassen sich p, q, r, s so bestimmen, daß n in

$$(p^2 + q^2 + 1) + (r^2 + s^2 - 1) = p^2 + q^2 + r^2 + s^2$$

aufgeht, so daß man also

$$p^2 + q^2 + r^2 + s^2 = nn' ,$$

wo n' eine ganze Zahl ist, setzen kann. Setzt man aber

$$p - \alpha n , q - \beta n , r - \gamma n , s - \delta n$$

respective für p, q, r, s; so erhält man

$$\begin{aligned}&(p - \alpha n)^2 + (q - \beta n)^2 + (r - \gamma n)^2 + (s - \delta n)^2\\ &= p^2 + q^2 + r^2 + s^2\\ &\quad - 2p\alpha n - 2q\beta n - 2r\gamma n - 2s\delta n\\ &\quad + \alpha^2 n^2 + \beta^2 n^2 + \gamma^2 n^2 + \delta^2 n^2\end{aligned}$$

welches offenbar auch durch n theilbar ist, da $p^2 + q^2 + r^2 + s^2$ es ist. Da αn, βn, γn, δn ganz willkührliche Vielfache von n sind, so kann man offenbar α, β, γ, δ immer so annehmen, daß jede der Größen $p - \alpha n$, $q - \beta n$, $r - \gamma n$, $s - \delta n < \frac{1}{2}n$ ist. Folglich ist die Annahme verstattet, das in der Gleichung

$$p'^2 + q'^2 + r'^2 + s'^2 = nn''$$

jede der Größen p, q, r, s $< \frac{1}{2}n$, also jedes der Quadrate p^2, q^2, r^2, $s^2 < \frac{1}{4}n^2$, folglich $nn'' < 4 . \frac{1}{4}n^2$, $nn'' < n^2$, $n'' < n$ ist. Wäre nun $n'' = 1$, so wäre der Satz bewiesen. Ist aber $n'' > 1$, so geht doch n'' in

$$p'^2 + q'^2 + r'^2 + s'^2$$

auf, da diese Quadratensumme $= nn''$ ist.

Wie vorher schließt man also hieraus ferner, daß

$$p''^2 + q''^2 + r''^2 + s''^2 = n''n'''$$

seyn wird, wo jede der Größen p'', q'', r'', $s'' < \frac{1}{2}n''$, und $n''' < n''$ ist.

Entwickelt man nun das Product

$$nn''.n''n''' = (p'^2 + q'^2 + r'^2 + s'^2)(p''^2 + q''^2 + r''^2 + s''^2)$$
$$= (p'^2 + q'^2 + r'^2 + s'^2)$$
$$\times \{(p' - \alpha' n'')^2 + (q' - \beta' n'')^2 + (r' - \gamma' n'')^2 + (s' - \delta' n'')^2\}$$

nach (3.), so findet man, wenn in der Entwickelung nur

$$p'^2 + q'^2 + r'^2 + s'^2 = nn''$$

gesetzt wird, daß dieses Product wieder eine Summe von vier Quadraten ist, deren jedes durch n''^2 theilbar ist. Also ist auch nn''' die Summe von vier Quadraten, und folglich

$$p'''^2 + q'''^2 + r'''^2 + s'''^2 = nn'''.$$

Wäre nun $n''' = 1$, so wäre der Satz bewiesen. Wäre aber $n''' > n$, so könnte man, ganz wie vorher wieder eine Zahl $n^{iv} < n'''$ finden, für welche nn^{iv} die Summe von vier Quadraten ist, und der Satz würde bewiesen seyn, wenn $n^{iv} = 1$ wäre. In jedem Falle erhellet aber, daß man nach dem hier gelehrten Verfahren eine Reihe von Producten

$$nn'', nn''', nn^{iv}, nn^{v}, \ldots.$$

finden kann, deren jedes eine Summe von vier Quadraten ist, und daß die Factoren

$$n'', n''', n^{iv}, n^{v}, \ldots.$$

eine abnehmende Reihe bilden. Da nun aber diese Reihe nicht in's Unendliche fortlaufen kann, welches der Fall seyn würde, wenn man nie auf ein Glied $= 1$ käme, so erhellet, daß man immer endlich einmal auf ein solches Glied kommen muß, also jede Primzahl n die Summe von vier Quadraten ist.

5. Jede Zahl läßt sich in vier Quadrate zerlegen.

Jede Zahl läßt sich in Primfactoren zerlegen (Theiler einer Zahl. 1.). Jeder Primfactor ist die Summe

von vier Quadraten (4.), also auch das Product aller (3.), d. i. die gegebene Zahl.

Zu bemerken ist jedoch, daß auch eins oder einige dieser Quadrate = o seyn können, und die Zahl folglich entweder selbst ein Quadrat, oder die Summe von zwei, drei oder vier Quadraten ist. Betrachtet man aber Null selbst als ein Quadrat, so läßt sich in dieser Beziehung in der That jede Zahl in vier Quadrate zerlegen. So ist z. B. $10 = 4 + 4 + 1 + 1$, $11 = 9 + 1 + 1 + 0$, $20 = 16 + 4 + 0 + 0$, $25 = 25 + 0 + 0 + 0$.

Den ersten Beweis des hier bewiesenen merkwürdigen Satzes gab Euler in den Nov. Comm. Petrop. T. V., erklärte denselben aber nachher selbst für nicht ganz genügend. Darauf gab Lagrange einen sehr scharfsinnigen Beweis in den Mém. de Berlin. 1770., welcher nachher von Euler noch vereinfacht wurde. Act. Petrop. T. I. P. II. 1777. Mit diesem Beweise stimmt der hier mitgetheilte dem Wesentlichen nach überein. Der Erfinder des Satzes ist Fermat, und es ist derselbe eigentlich nur ein besonderer Fall seines allgemeinen Satzes von der Zerlegung jeder Zahl in Polygonalzahlen, worüber der Art. Fermat's Lehrsätze zu vergleichen. Der Satz von der Zerlegung jeder Zahl in drei Triagonalzahlen ist von Legendre (Théorie des nombres. p. 347. p. 188.) bewiesen worden. Der Beweis hängt mit der Theorie der sogenannten reciproken Divisoren der Formel $t^2 + au^2$ unmittelbar zusammen, so daß derselbe, ohne diese ganze Theorie aufzunehmen, hier nicht füglich mitgetheilt werden konnte. Gewiß wird aber Jeder, wer diesen Artikel studirt hat, Legendre's großes Werk im Zusammenhange zu lesen sich gedrungen fühlen, wozu namentlich derselbe eine Vorbereitung seyn soll. Einen andern Beweis hat Gauß gegeben (Disq. arithm. p. 495. 406., welcher aber eben so innig mit dem ganzen Inhalte des scharfsinnigen Werkes verknüpft ist, daß er hier ohne zu große Weitläufigkeit ebenfalls nicht aufgenommen werden konnte. Verbindet man mit dem Studium dieser beiden Werke noch das Studium der von Legendre (Supplément à

l'essai sur la théorie des nombres. Février. 1816.) und Cauchy (Exercices de Mathematiques par A. L. Cauchy. 10. Livraison. Paris. 1826. p. 265.) gegebenen Beweise des allgemeinen Satzes von Fermat über die Zerlegung jeder Zahl in Polygonalzahlen; so wird man sich dadurch die vollständigste Kenntniß dieser überaus merkwürdigen Folge von Sätzen verschaffen.

XI. Historische Bemerkungen.

Im Vorhergehenden sind bereits die Namen der Geometer, welche sich vor Andern um die Zahlenlehre verdient gemacht haben, und ihre Schriften, so oft genannt worden, daß hier nur noch eine ganz kurze Uebersicht im Zusammenhange nöthig ist.

Die arithmetischen Bücher des Euclides sind als die erste Schrift anzusehen, in welcher Untersuchungen aus der Zahlenlehre vorkommen. Außer vielen andern merkwürdigen Sätzen enthalten sie vorzüglich eine Reihe von Sätzen über die Primzahlen, unter denen das oben in I. bewiesene wichtige Theorem als die Grundlage der ganzen Zahlenlehre anzusehen ist, da fast keine Untersuchung über die Zahlen desselben entbehren kann. Von dem großen arithmetischen Werke des Diophantus ist in dem Artikel: Unbestimmte Analytik, ausführlich die Rede gewesen, worauf wir also hier, so wie überhaupt auf die dort mitgetheilte Geschichte der unbestimmten Analytik verweisen. Dieses Werk gehört indeß mehr zur unbestimmten Analytik, als zur Theorie der Zahlen im eigentlichen Sinne, insofern wir darunter vorzugsweise die Lehre von den Eigenschaften der Zahlen, und zwar immer der ganzen Zahlen, verstehen. Die meisten Entdeckungen verdankt diese Wissenschaft Fermat, Parlamentsrath zu Toulouse. Von dem größten Theile der vielen von ihm entdeckten merkwürdigen Sätze ist in dem Obigen ausführlich die Rede gewesen. Er hat kein eignes Werk über die Zahlenlehre hinterlassen, sondern seine wichtigen Entdeckungen sind bloß als Randbemerkungen in der von seinem Sohne S.

Fermat veranstalteten neuen Ausgabe von Bachets Diophant mitgetheilt. Diophanti Alexandrini Arithmeticorum libri sex, et de numeris multangulis liber unus. Cum Commentariis C. G. Bacheti V. Cl. et observationibus D. P. de Fermat Senatoris Tolosani. Tolosae. 1670. fol. Am meisten ist zu beklagen, daß Fermat alle Sätze ohne Beweise mittheilt, obgleich er ohne Zweifel, wenn er auch gewiß die meisten Sätze nur durch Versuche gefunden hat, im Besitz derselben gewesen ist, wie bei einem so großen Geometer sich schon von selbst versteht, und auch aus der Anmerkung zur 31sten Aufgabe des IV. Buches erhellet. Aus derselben Anmerkung geht auch hervor, daß Fermat allerdings die Absicht hatte, seine Untersuchungen in einem ausführlichen Werke, welches aber nie erschienen ist, bekannt zu machen. Die größten Mathematiker der neuern Zeit haben die Aufsuchung dieser Beweise zu einer besondern Aufgabe ihres Scharfsinns gemacht. An der Spitze steht auch hier wieder Euler. Er und Lagrange haben nicht bloß viele Fermat'sche Sätze mit bündigen Beweisen versehen, sondern auch die Zahlenlehre mit eignen Entdeckungen bereichert. Die hierher gehörenden Abhandlungen sind in den Schriften der gelehrten Gesellschaften zerstreu't. Man findet ein ziemlich vollständiges Verzeichniß derselben in Reuss Repertorium Commentationum a Societatibus litter. editorum. T. VII. Gott. 1808. p. 7—13, worauf ich hier der Kürze wegen verweise. Mehreres ist schon oben angeführt worden. Ein besonderes Verdienst um unsere Wissenschaft erwarb sich Legendre, indem er in seinem Essai sur la théorie des nombres. Sec. édit. Paris. 1808. einen vortrefflichen und sehr vollständigen Lehrbegriff der Zahlenlehre lieferte, der auch reich an eigenthümlichen Untersuchungen ist. Die erste Ausgabe erschien Paris. a VI. Und mit wem könnte ich diese Bemerkungen würdiger schließen, als mit unserm tiefdenkenden Gauß. Seine Disquisitiones arithmeticae. Lipsiae. 1801., sind ein Werk des größten Scharfsinns, voll der schönsten Entdeckungen. Die Einführung des Be-

griffs und des Zeichens der Congruenz der Zahlen, wodurch die Beweise vieler wichtigen Sätze von den Zahlen in hohem Grade vereinfacht werden, der Fundamentalsatz in der Lehre von den quadratischen Resten, welcher zwar einerlei mit Legendre's Satze von der Reciprocität, aber von Gauß zuerst auf mehrere ganz verschiedene Arten völlig streng und höchst scharfsinnig bewiesen worden ist, die ganze Lehre von den quadratischen und den Resten höherer Grade, würden allein hinreichend seyn, den Namen ihres Erfinders unsterblich zu machen. Aus den beiden zuletzt genannten Werken von Legendre und Gauß werden jetzt alle tiefern Kenntnisse der Zahlenlehre auf dem leichtesten und sichersten Wege geschöpft. Die Namen mehrerer anderer Mathematiker, welche sich um diesen schönen Theil der Mathematik verdient gemacht haben, sind schon oben genannt worden. M. vergl. übrigens auch noch die Artikel Theiler einer Zahl, Theilung, Primzahlen, Fermat's Lehrsätze, Vollkommene Zahl und überhaupt die besonderen Formen der Zahlen, vorzüglich aber den Artikel Unbestimmte Analytik.

Zahlensystem. Seyen N und x irgend zwei ganze Zahlen, deren jede hier aber bloß als eine Anzahl von Einheiten betrachtet wird, ohne Rücksicht auf jeden symbolischen Ausdruck dieser Zahlen. Mittelst gewöhnlicher Division, welche hier durch wiederholte Subtraction verrichtet gedacht werden kann, lassen sich in folgenden Gleichungen:

$$N = ax + \alpha$$
$$a = bx + \beta$$
$$b = cx + \gamma$$
$$c = dx + \delta$$

u. s. f. u. s. f.

die Größen α, β, γ, δ,.... offenbar so bestimmen, daß sie alle kleiner als x sind. Zugleich erhellet auch, daß a, b, c, d,.... eine abnehmende Reihe bilden, und man folglich offenbar immer einmal auf ein Glied dieser Reihe kommen muß, welches = Null ist, weil alle Glieder dieser Reihe positive ganze Zahlen sind, und dieselbe demnach

sich nicht in's Unendliche erstrecken kann. Es werden also obige Gleichungen immer folgende Gestalt annehmen:

$$\begin{aligned} N &= ax + \alpha \\ a &= bx + \beta \\ b &= cx + \gamma \\ c &= dx + \delta \\ &\ldots\ldots \\ l &= mx + \mu \\ m &= \quad\;\; \nu . \end{aligned}$$

Durch successive Substitution erhält man hieraus augenblicklich:

$$\begin{aligned} N &= ax + \alpha \\ &= bx^2 + \beta x + \alpha \\ &= cx^3 + \gamma x^2 + \beta x + \alpha \\ &= dx^4 + \delta x^3 + \gamma x^2 + \beta x + \alpha \\ &\ldots\ldots\ldots\ldots \\ &= \nu x^p + \mu x^{p-1} + \ldots + \delta x^3 + \gamma x^2 + \beta x + \alpha \end{aligned}$$

oder auch

$$N = \alpha + \beta x + \gamma x^2 + \delta x^3 + \ldots + \mu x^{p-1} + \nu x^p$$

wo $\alpha, \beta, \gamma, \delta, \ldots \mu, \nu$ alle kleiner als x sind, und offenbar auch ein oder das andere Glied dieser Reihe = Null seyn kann.

Man sieht also, daß alle Zahlen durch Reihen dargestellt werden können, welche nach Potenzen einer gewissen Zahl x fortschreiten, so daß alle Coefficienten dieser Reihen $< x$ sind. Jede solche Anordnung aller Zahlen als Reihen nach den Potenzen einer bestimmten Zahl x, deren Coefficienten alle $< x$ sind, heißt ein Zahlensystem, und x dessen Grundzahl oder Basis.

Will man nun auf diese Weise alle Zahlen symbolisch ausdrücken, so ist klar, daß zur Bezeichnung der Coefficienten dieser Reihen nur so viele einfache Zeichen nöthig sind, als x Einheiten enthält, weil die Anzahl aller ganzen Zahlen, welche $< x$ sind, $= x - 1$ ist, wozu dann noch ein einfaches Symbol für Null kommt. Es ist klar, daß x alle Werthe außer Null und Eins haben kann. Die einfachen Zeichen für die Coefficienten der obigen Reihen heißen Zahlzeichen oder Ziffern. So lange man bei diesen Reihen selbst stehen bleibt, würde in jedem System noch ein einfa-

ches Symbol für die Grundzahl nöthig seyn, welches man aber vermeidet, wenn die obigen Reihen auf folgende viel einfachere Weise, in welcher jetzt alle gebildete Völker übereinkommen, geschrieben werden.

Jede Zahl

$$N = \alpha + \beta x + \gamma x^2 + \delta x^3 + \ldots + \mu x^{p-1} + \nu x^p$$

wird nämlich auf die Weise symbolisch dargestellt, daß man bloß die Coefficienten dieser Reihe, indem man mit α auf der rechten Seite anfängt, in ihrer natürlichen Ordnung neben einander schreibt, so daß also hiernach

$$N = \nu\mu \ldots \delta\gamma\beta\alpha$$

ist, wobei man sich aber immer zu erinnern hat, daß, wenn es auf die Bestimmung des wahren Werthes der Zahl N ankommt, α, β, γ, δ, ... nach der Reihe mit x^0, x^1, x^2, x^3, ... multiplicirt werden müssen.

Die erste, zweite, dritte, vierte Stelle u. s. f. von der rechten nach der linken Seite hin nennt man bei dieser Art die Zahlen zu schreiben auch die nullte, erste, zweite, dritte Ordnung u. s. f., welches sich, wie man sieht, bloß auf die Potenzen der Grundzahl bezieht, mit welchen die Ziffern in den genannten Stellen multiplicirt werden müssen, wenn der wahre Werth der Zahl N bestimmt werden soll. Da nun die Grundzahl x, wenn o, 1 die bekannten Zeichen der Null und Eins sind, immer $= o + 1.x$ ist, so ist klar, daß in jedem Zahlensystem die Grundzahl 10 geschrieben werden muß, und daß folglich, wie schon oben bemerkt wurde, für die Grundzahl kein einfaches Zeichen nöthig ist.

Nach dieser Methode kann man also in einem Zahlensystem, dessen Grundzahl x ist, alle Zahlen mit x einfachen Zeichen schreiben. Das Wesentliche bei derselben ist, wie man leicht sieht, daß jedem einfachen Zahlzeichen ein verschiedener Werth nach seiner Stelle beigelegt wird. Daß die niedrigste Ordnung auf der rechten Seite beginnt, deutet auf einen orientalischen Ursprung dieser Methode, worüber mit Mehrerem der Artikel Zahlzeichen zu vergleichen ist.

Alle gebildete Völker legen jetzt die Zahl zehn als Basis

ihren Zahlensystemen zum Grunde. Die zehn nöthigen einfachen Zeichen oder Ziffern sind bekanntlich

0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Wollte man zwölf als Basis zum Grunde legen, so wären noch für die zehn und die eilf einfache Zeichen nöthig. Ist zwei die Grundzahl, so kann man alle Zahlen bloß mit den einfachen Zeichen 0, 1 schreiben. Das System, dessen Grundzahl zehn ist, heißt bekanntlich das Decadische. Ueber die Dyadik, Dodekadik und die Tetraktys s. m. die besondern Artikel. In dem Artikel Variationen gegebener Dinge (10.) ist eine allgemeine Anleitung zum Schreiben aller Zahlen nach einem willkührlichen Zahlensysteme gegeben. Für die Dyadik und Dodekadik wäre der Anfang, wenn in letzterem Systeme zehn und eilf durch ♀ und ♂ bezeichnet werden, folgender:

1	1	(1)
10	2	(2)
11	3	(3)
100	4	(4)
101	5	(5)
110	6	(6)
111	7	(7)
1000	8	(8)
1001	9	(9)
1010	♀	(10)
1011	♂	(11)
1100	10	(12)
1101	11	(13)
1110	12	(14)
1111	13	(15)
10000	14	(16)
10001	15	(17)
10010	16	(18)
10011	17	(19)
10100	18	(20)
10101	19	(21)
10110	1♀	(22)
10111	1♂	(23)
11000	20	(24)
11001	21	(25)

Jede dekadisch ausgedrückte Zahl kann nach einem anderen Systeme sehr leicht mittelst successiver Division mit der Grundzahl des Systems ausgedrückt werden, wie folgendes Beispiel für die Grundzahl 7 zeigt. Die gegebene dekadische Zahl sey = 3465.

7)	7)	7)	7)	7)	
3465	495	70	10	1	0
3465	490	70	7	0	
0	5	0	3	1	

Man dividirt so lange, bis man auf einen Quotienten = 0 kommt, und schreibt die Reste verkehrt neben einander. Die dekadische Zahl 3465 nach dem Zahlensystem, dessen Grundzahl 7 ist, geschrieben, ist also = 13050.

In der That ist auch diese Zahl

$$= 0 + 5.7 + 0.7^2 + 3.7^3 + 1.7^4$$
$$= 35 + 1029 + 2401 = 3465 ,$$

woraus man zugleich sieht, wie man umgekehrt jede nach irgend einem andern Zahlensysteme geschriebene Zahl dekadisch ausdrücken kann. Der Grund der obigen Verfahrungsarten wird leicht in die Augen stellen.

Das Aussprechen der Zahlen gehört nicht in die Mathematik, sondern in die Grammatik, da die Regeln nicht in allen Sprachen einerlei sind. Eine dreiziffrige dekadische Zahl kann Jeder aussprechen. Vielziffrige Zahlen theile man, von der rechten nach der linken Hand zu gehend, in Klassen zu drei Ziffern, und scheide die Klassen abwechselnd durch Commata und die römischen Ziffern I, II, III, IV, u. s. f. von einander, jede einzelne Klasse spreche man für sich aus, jedes Komma durch Tausend, und I, II, III, IV, ... nach der Reihe durch Million, Billion, Trillion, Quadrillion, u. s. f. Z. B.

47'''639,426''785,043'760,285;

47 Trillionen 639 Tausend, 426 Billionen 785 Tausend, 43 Millionen 760 Tausend, 285. Am besten setzt man die römischen Ziffern oben zur Rechten der einzelnen Klassen, wie dieses Beispiel zeigt. Diese Regeln sind die einfachsten für die deutsche Sprache.

Verschiedene Sätze, welche sonst bloß in Bezug auf das dekadische Zahlensystem bewiesen werden, lassen sich leicht auf jedes Zahlensystem erweitern. Z. B. folgendes Kennzeichen der Theilbarkeit der willkührlichen Zahl

$$N = \alpha + \beta x + \gamma x^2 + \delta x^3 + \varepsilon x^4 + \cdots$$

durch die beliebige Zahl n. Sey

$$x = qn + \varrho,\ x^2 = q'n + \varrho',\ x^3 = q''n + \varrho'',\ \ldots;$$

so ist

$$N = (\beta q + \gamma q' + \delta q'' + \varepsilon q''' + \ldots)n$$
$$+ \alpha + \beta\varrho + \gamma\varrho' + \delta\varrho'' + \varepsilon\varrho''' + \cdots$$

Also ist N durch n theilbar, wenn

$$\alpha + \beta\varrho + \gamma\varrho' + \delta\varrho'' + \varepsilon\varrho''' + \cdots$$

durch n theilbar ist. Man setze also unter die einzelnen Ziffern der Zahl N die Reste, welche bei der Division von x^0, x^1, x^2, x^3,... durch n bleiben, von der rechten nach der linken Hand hin, multiplicire die übereinanderstehenden Zahlen in einander, und untersuche, ob die Summe dieser Producte durch n theilbar ist. Da

$$x^m - 1 = (x-1)(x^{m-1} + x^{m-2} + \ldots + x + 1)$$

ist; so ist, wenn p eine ganze Zahl bezeichnet,

$$x^m = (x-1)p + 1,$$

und folglich der Rest, welchen die Division x^m durch $x - 1$ läßt, für jedes m, $= 1$. Also nach dem Obigen

$$N = \alpha + \beta x + \gamma x^2 + \delta x^3 + \varepsilon x^4 = \cdots$$
$$= \ldots\ \varepsilon\delta\gamma\beta\alpha$$

durch $x - 1$ theilbar, wenn die Summe der Ziffern

$$\alpha + \beta + \gamma + \delta + \varepsilon + \ldots$$

durch $x - 1$ theilbar ist. Dies stimmt überein mit dem bekannten Kennzeichen der Theilbarkeit einer Zahl durch 9 im dekadischen Zahlensysteme (Theiler einer Zahl. 6.)

M. vergl. den Art. Zahlzeichen.

Zahlzeichen, Ziffern (Characteres; numéraux, chiffres; engl. figures) sind in jedem Zahlensysteme schriftliche Charaktere oder Bezeichnungen der Zahlen, welche kleiner als die Grundzahl des Systems sind, die Null mit eingeschlossen, wobei es aber, welches wir sogleich hier bemerken, nicht sowohl auf die Gestaltung

dieser Symbole selbst, als vielmehr auf die Methoden ankommt, nach welchen mit einigen wenigen einfachen Zahlzeichen alle Zahlen bezeichnet werden. Von der vollkommensten dieser Methoden, welche jetzt alle gebildete Völker des alten und des neuen Continents befolgen, ist in dem Artikel Zahlensystem ein Abriß gegeben worden. Gegenwärtiger Artikel ist bestimmt, so weit die uns zu Gebote stehenden Mittel und der beschränkte Raum es gestatten, die Geschichte dieser wichtigen Erfindung zu liefern, von welcher Laplace in der Exposition du système du monde. édit. p. 325. mit Recht sagt: „der Gedanke, alle Quantitäten durch neun Zeichen auszudrücken, indem man ihnen zugleich einen absoluten und einen Stellenwerth giebt, ist so einfach, daß man eben deshalb nicht genugsam erkennt, welche Bewunderung er verdient. Aber eben diese Einfachheit und Leichtigkeit, welche die Methode dem Calcul zusichert, erheben das arithmetische System der Indier zu dem Range der nützlichsten Erfindungen. Wie schwer es war, eine solche Methode aufzufinden, kann man daraus abnehmen, daß sie dem Genie des Archimedes und Apollonius von Perga, zweier der größten Geister des Alterthums, entgangen war."

1. Den Grund, daß fast alle Völker bis zehn zählen, hat schon Aristoteles (Probl. Sect. XV. Probl. III.) in der Gestalt unserer Hände und Füße, als fünfästiger Organe gefunden, und Alexander von Humboldt führt in dieser Beziehung in einer trefflichen akademischen Abhandlung über die bei verschiedenen Völkern üblichen Systeme von Zahlenzeichen und über den Ursprung des Stellenwerthes in den indischen Zahlen, welche man in Crelles Journal der reinen und angew. Math. IV. 3. S. 205. findet, verschiedene interessante Thatsachen an, wovon wir hier Einiges ausheben. In der Chibcha-Sprache der Muyskas heißt 10 Fuß (quihieha oder qhieha), weil man den Fuß nennt, wenn schon beide Hände durchgezählt sind; 11, 12, 13 heißen von den Zahlwörtern ata, bosa, mica (eins, zwei, drei) quihieha ata, quihieha bosa, qui

hieha mica, d. i. Fuß ein, Fuß zwei, Fuß drei. 20 heißt Fuß zehn oder ein Häuschen (gueta), vielleicht, sagt von Humboldt, weil man nach Maiskörnern zählte, und ein Häufchen Mais an die Maisscheuer erinnerte. In einer großen Anzahl von Sprachen heißen 5, 10 eine Hand, zwei Hände. In der Sprache der Yaruros, von denen v. Humboldt volkreiche Missionsdörfer am Apure-Fluß, welcher sich in den Orinocco einmündet, fand, heißt 40 noeni pume, von noeni zwei und pume Mensch, d. i. zwei Menschen, weil man den ganzen Menschen nannte, nachdem man an beiden Extremitäten die Finger abgezählt hatte. Im Persischen heißt pendj fünf, von pentscha die Faust, herstammend von dem Sanscrit-Worte pantscha, welches nach Bopp's Bemerkung auf das römische quinque, so wie das indische tschatur auf quatuor geführt haben soll.

Aristoteles erwähnt a. a. O. zugleich eines thracischen Volkes, welches nur bis 4 zähle. Dadurch ward Erhard Weigel veranlaßt, die Regeln der tetraktischen Arithmetik in besondern Schriften zu entwickeln, worüber der Artikel Tetraktik nachzusehen ist. Dies wäre also eine Ausnahme von der Regel, daß alle Völker bis 10 zählen. In dem Bulletin des sciences math. par Férussac. Juin. 1827. p. 345. werden als hierher gehörende Beispiele noch die Grönländer und ein ostiakischer Stamm, welche nur bis 5 zählen (s. Egedes grönländische Grammatik. 1760. und Klaproth Asia polyglotta. 171.) erwähnt, so wie nach der Voyage de F. Pyrard. 2. partie. Paris. 1619. in einem maldivischen Sprachidiom 12 die Basis der Numeration seyn soll.

2. Die Zahlenzeichen der meisten alten Völker, und die Methoden, mit einer geringeu Anzahl einfacher Zeichen alle Zahlen zu schreiben, waren höchst unbequem. Meistens bedienten sie sich dazu der Buchstaben ihrer Alphabete. Die Hebräer z. B. bezeichneten die Einer durch die 9 ersten Buchstaben ihres Alphabetes; die Zehner durch die 9 folgenden; 100, 200, 300, 400 wurden durch die

vier letzten Buchstaben, und 500 bis 900 durch Zusammensetzung von 400 mit 100, 200, 300, 400, 500, so daß erstere, nach orientalischer Art zu schreiben, voran steht, bezeichnet. Die Tausender werden wie die Einer mit zwei darüber gesetzten Punkten bezeichnet. Alle übrigen Zahlen erhielt man durch bloße Nebeneinanderstellung dieser Zeichen, so daß immer die größere Zahl voran steht. M. s. Gesenius Lehrgebäude der hebr. Sprache. Leipzig. S. 15. Im hebräischen Texte des alten Testaments sind die Zahlen mit Worten geschrieben. v. Humboldt hat in der angeführten trefflichen Abhandlung sehr viele Methoden, die Zahlen mit einer geringen Anzahl einfacher Zeichen zu schreiben, verglichen, und dieselben, mit Ausschluß der heutigen Zahlensysteme, in folgende vier Klassen gebracht.

Erste Methode. Durch bloße Nebeneinanderstellung (Juxtaposition) einiger einfachen Zeichen, wie bei Tuskern, Römern, Griechen bis zur Myriade, Mexikanern und Aegyptern. Wir wählen als Beispiel die römische Bezeichnungsart.

Einfache Zeichen:

1,	5,	10,	50,	100,	500,	1000
I,	V,	X,	L,	C,	IↃ oder D,	CIↃ oder M.

Ein einzelnes Stück wurde durch eine senkrechte Linie (I) bezeichnet, fünf Stück durch einen spitzigen Winkel (V), funfzig Stück durch einen rechten Winkel (L). Aus der Verbindung zweier V entstand X, so wie aus der Verbindung zweier übereinander gesetzten L eine Klammer, und durch deren Abrundung, um des Wortes centum willen, das C. 500 Stück wurden durch ein Quadrat bezeichnet, woraus nach und nach IↃ und D entstanden. Aus CIↃ entstand M, weil dieser Buchstabe der erste des Wortes mille war (Lateinische Grammatik von Grotefend. 3. Aufl. Bnd. II. Frankf. 1820. S. 163.). Gleiche nebeneinander stehende Zeichen bedeuteten eine Vervielfachung des einfachen Zeichens, wie z. B. XX (20), XXX (30), CC (200). Stehen zwei ungleiche Zeichen bei einander,

so sind zwei Fälle zu unterscheiden. Findet sich das Zeichen, welches den kleinern Zahlenwerth hat, zur Linken, so ist es in Bezug auf das andere Zeichen subtractiv, wie z. B. IV (4), IX (9), XL (40), XC (90). Findet sich dagegen das Zeichen, welches den kleinern Zahlenwerth hat, rechts, so ist es in Bezug auf das andere Zeichen additiv, wie z. B. XI (11), VI (6), LX (60). Nach diesen Gesetzen ist es leicht, alle Zahlen zu bilden. So bedeutet z. B. MDCCCXXXIV die Zahl 1834. So ist nun auch IↃ = 5000, CCIↃ = 10000, IↃↃ = 50000, CCCIↃↃ = 100000, CCCCIↃↃↃ = 1000000. Wie weitläufig diese Bezeichnungsart ausfallen muß, wenn die Zahlen auch nur einigermaßen groß werden, fällt in die Augen.

Zweite Methode. Vervielfachung und Verminderung des Werthes durch darüber und darunter gesetzte Zeichen.

Ein Beispiel liefern zunächst die griechischen Buchstabenzahlen in der Reihe der Tausender und der Myriaden. Folgendes enthält eine Uebersicht der griechischen Zahlen.

α	β	γ	δ	ε	ς	ζ	η	Θ
1	2	3	4	5	6	7	8	9
					(Βαῦ)			
ι	κ	λ	μ	ν	ξ	ο	π	ϙ
10	20	30	40	50	60	70	80	90
								(Κόππα)
ρ	σ	τ	υ	φ	χ	ψ	ω	ϡ
100	200	300	400	500	600	700	800	900
								(Σαμπῖ)
$\underset{,}{\alpha}$	$\underset{,}{\beta}$	$\underset{,}{\gamma}$	$\underset{,}{\delta}$	$\underset{,}{\varepsilon}$	$\underset{,}{\varsigma}$	$\underset{,}{\zeta}$	$\underset{,}{\eta}$	$\underset{,}{\Theta}$
1000	2000	3000	4000	5000	6000	7000	8000	9000
$\overset{\alpha}{M}$,	$\overset{\beta}{M}$,	$\overset{\gamma}{M}$,	$\overset{\delta}{M}$,	$\overset{\varepsilon}{M}$,	u. s. f.			
10000,	20000,	30000,	40000,	50000,	u. s. f.			

10000 bilden eine Myriade, die auch durch *Mυ* bezeichnet wird. Nach dieser Bezeichnungsart ist z. B.

$$\overset{\eta\upsilon\xi\beta}{\underset{,}{M}\zeta\upsilon\lambda\eta} = 84627438 .$$

Brüche, deren Zähler die Einheit ist, werden bloß durch den Nenner mit einem Acutus bezeichnet. Z. B. $\gamma' = \frac{1}{3}$, $\delta' = \frac{1}{4}$, $\xi\delta' = \frac{1}{64}$. Sonst werden Zähler und Nenner in eine Linie geschrieben, der erstere voran, und durch die Größe der Schrift unterschieden. M. s. Délambre Histoire de l'Astronomie ancienne. T. II. Chap. I. p. 6. Oeuvres d'Archimède par F. Peyrard. Paris. 1807. Ueber die Arithmetik der Griechen. A. d. Franz. des Herrn Delambre von J. J. J. Hoffmann. Mainz. 1817. A. Matthiä ausführl. griech. Gramm. 2. Aufl. Lpzg. 1825. I. S. 23. 509.

Vorzüglich wichtig sind die von Silvestre de Sacy in einem Manuscripte aus der Bibliothek der alten Abtey St. Germain du Près entdeckten arabischen Gobar-Ziffern. Silvestre de Sacy sagt: le gobar a un grand rapport avec le chiffre indien, mais il n'a pas de Zero (v. Humboldt a. a. O. S. 223.).

In dieser Gobar- oder Staubschrift werden die Zehner, Hunderter u. s. f. durch beigefügte Punkte angegeben, wie z. B. $3\cdot = 30$, $4\cdot\cdot = 400$, $6\cdot\cdot\cdot = 6000$.

S. auch in (3.) das Scholion des Mönchs Neophytos.

Dritte Methode. Vervielfachung des Werthes durch Coefficienten.

Diophantus und Pappus z. B. schreiben $\beta M\upsilon$ für $2 \times 10000 = 20000$, $\alpha M\upsilon\beta$ bedeutet einmal $10000 + 2 = 10002$.

Vierte Methode. Vervielfältigung und Verminderung, aufsteigend und absteigend, durch Abtheilung von Zahlschichten, deren Werth sich in geometrischer Progression vermindert. M. s. mit Mehrerem v. Humboldt a. a. O. S. 225.

3. Die Inder haben in uralter Zeit schon unsere gegenwärtige Bezeichnungsart der Zahlen gebraucht. Ihre jetzigen Zahlzeichen stimmen zwar nicht mit den unsrigen überein, allein auf die Figur kommt es, wie schon oben erinnert, hier nicht an, sondern auf die im Art. Zahlensy-

stem dargestellte Methode, mit einigen einfachen Zeichen alle Zahlen zu bezeichnen. Unsere Zahlzeichen werden zwar oft arabische genannt, aber die Araber haben sie von den Indern erhalten. Die Beweise für diese Behauptung liefern Wallis in seiner Mathesis universalis. Cap. IX., wie auch in seiner Algebra (Cap. III.), und Montucla in seiner Geschichte der Mathematik. T. I. p. 375., welcher das Meiste von jenem entlehnt hat. Erstlich findet man in mehreren Bibliotheken Manuscripte von arabischen Abhandlungen über die Arithmetik, welche den Titel haben: Die Kunst zu rechnen nach Indischer Art. In der Bibliothek zu Leiden ist ein Manuscript dieser Art, worin die Zahlzeichen den unsrigen sehr ähnlich sind. — Zweitens sagt ein arabischer Schriftsteller Alsephadi, daß die Indische Nation sich dreierlei Dinge rühme, eines Buches, das moralische Fabeln enthält, ihrer Rechnungsart, und des Schachspiels. Ferner sagt ein anderer arabischer Schriftsteller aus dem 13ten Jahrhundert in der Vorrede zu einer astronomischen Schrift, die sich in der Bibliothek zu Leiden befindet, daß die gedachte Rechnungsart von Indischen Philosophen erfunden sey. — Drittens ist von dem Mönch Planudes im 13ten Jahrhundert handschriftlich an mehreren Orten ein arithmetisches Werk vorhanden, welches den Titel hat: λογιστικη ινδικη, oder ψηφοφορια κατα Ινδους, d. i. Indische Rechenkunst, oder Rechnungsart zufolge der Inder. Die Bezeichnungsart der Zahlen ist völlig unsere jetzt übliche, nur die Charaktere oder Zahlfiguren sind von den unsrigen verschieden, kommen aber fast gänzlich mit denen überein, welche Alsephadi als die zu seiner Zeit üblichen angiebt. Planudes fügt ferner, nachdem er die Beschaffenheit der neun bedeutenden Ziffern erklärt hat, noch ausdrücklich hinzu: Diese neun Charaktere sind Indische. Zu diesen, fährt er fort, kommt noch das zehnte Zeichen, τζιφρα genannt, welches etwas nicht vorhandenes bedeutet. Das arabische Wort Tzaphar heißt leer seyn, welches ohne Zweifel der Ursprung der Wörter chiffre, cifera oder cifra, Ziffer und zero ist. — Viertens; als die

jetzt übliche Rechnungsart in Europa eingeführt ward, nahm man es als ausgemacht an, daß sie von den Indern herkomme. Johannes de Sacro Bosco im 13ten Jahrhundert bezeugt dieses in den Versen, womit sich seine in gebundener Rede geschriebene Arithmetik anfängt:

Haec Algorithmus arc praesens dicitur, in qua
Talibus Jndorum fruimur bis quinque figuris.

Die Zahlzeichen des Johannes de Sacro-Bosco sind mit den unsrigen größtentheils einerlei.

Von besonderer Wichtigkeit ist auch folgendes von v. Humboldt a. a. O. S. 227. aus einem Codex der Pariser Bibliothek mitgetheilte Scholion des Mönchs Neophytos:

Tzyphra est et vocatur id, quod cuivis litterae inde a decade et insequentibus numeris quasi *ομικρὸν* inscribitur. Significat autem hac Indica voce tale analogiam numerorum. Ubi igitur scriptum est simile primae litterae *ἄλφα*, pro unitate scriptae, atque superimpositum habet vel punctum vel quasi *ομικρὸν*, addita altera figura litterae Indicae, differentiam et augmentum numerorum declarat. E. g. pro primo graeco numero, *α* scripto, apud Indos sive linea recta perpendicularis, quando non habet superimpositum punctum vel *ομικρὸν*, ipsum hoc denotat unitatem, ubi vero superimpositum sit punctum atque altera littera adscripta sit, figura quidem similis priori, significat XI, propter additamentum similis litterae atque superimpositum unum punctum. Similiter etiam in reliquis litteris, quemadmodum adspectus docet. Si vero plura habet puncta, plura denotat. Quod intelligas, lector, et supputes unumquidque.

Die 9 Ziffern des Neophytos sind, außer der 4, ganz den persischen ähnlich. Nach dieser Bezeichnungsart wäre also z. B. $\overset{\circ}{2} = 20$, $\overset{\circ}{2}4 = 24$, $\overset{\circ\circ}{5} = 500$, $\overset{\circ\circ\circ}{6} = 6000$, $\overset{\circ}{3}\overset{\circ\circ}{4}\overset{\circ\circ\circ}{6}\overset{\circ}{7} = 3467$. Wie ähnlich, nur weitläufiger,

diese indische Bezeichnungsart der unsrigen ist, fällt auf den ersten Blick in die Augen. Die über die einzelnen Ziffern gesetzten Nullen erleichtern gleichsam nur das Aussprechen der Zahlen, und konnten ebenfalls weggelassen werden. M. s. mit Mehrerem v. Humboldt. a. a. O. S. 228.

4. Eine Stelle in der Geometrie des Boethius (im Anfange des 6ten Jahrh.) könnte wegen des Indischen Ursprungs unserer Numeration Zweifel erregen. Er sagt, daß einige Pythagoräer zur Bezeichnung der Zahlen gewisse Zeichen erfunden hätten, die er Apices oder Characteres nennt. Er erklärt darauf ihren Gebrauch, und, ungeachtet der Dunkelheit seiner Beschreibung, erkennt man doch daran die jetzt übliche Art zu rechnen. Ja sogar in einigen Handschriften des gedachten Werkes findet man Ziffern, die den unsrigen nahe kommen, zum Theil ganz ähnlich sind. Doch wird auch in alten Handschriften desselben Werks Alles mit römischen Zahlbuchstaben ausgedrückt. Wäre die dekadische Bezeichnungsart eine griechische Erfindung, so ist nicht zu begreifen, daß ein so sinnreiches Volk als die Griechen sie nicht benutzt haben sollte. Aber Eutocius, welcher um dieselbe Zeit mit dem Boethius lebte, bedient sich in seinem Commentar über des Archimedes Sandrechnung der Buchstaben aus dem Alphabete als Ziffern. Die Inder, welche so fest an ihren Gewohnheiten und Kenntnissen halten, haben ihre Rechnungsart, welche die unsrige ist, gewiß nicht von Ausländern angenommen. Vielmehr ist sie von ihnen durch die Araber und andere asiatische Völker in dem westlichen Asien bekannt geworden, woher Boethius, der in Italien lebte, Nachricht davon erhalten konnte. Er schrieb sie den Pythagoräern zu, die wegen ihrer arithmetischen Kenntnisse in Ruf standen, entweder zufolge einer Sage, oder nach seiner eigenen Muthmaßung. Man hatte aber keine rechte Vorstellung von der dekadischen Rechnung und ihren großen Vortheilen, und blieb daher immer bei der alten unbequemen Weise, wozu noch kam, daß die mathematischen Wissenschaften und alle übrigen in den Abendländern und in dem

griechischen Reiche immer mehr in Verfall geriethen. Die alte Rechnungsform hat sich noch lange weiter hin in dem westlichen Asien erhalten. Man sieht es daraus, daß der Kaliph Waled (um 700) verboten hat, die griechische Sprache und Bezeichnung der Zahlen bei den Rechnungen der Staatskassen zu gebrauchen (Gibbon's history of the decline and fall of the Roman empire. Vol. V. p. 321.). M. vergl. Weidleri Spicilegium observationum ad Historiam notarum numeralium pertinentium. Wittenbergae. 1755. Mannert de numerorum quos arabicos vocant vera origine pythagorica. Norimb. 1801.

5. Nach einer Bemerkung Sedillots, welche v. Humboldt a. a. O. S. 229. anführt, hat die indische Rechnungsart ihren Weg in die Abendländer durch den gelehrten Astronomen Rihan Muhammed ebn Ahmet Albiruni, welcher sich in Indien aufhielt, gefunden, vielleicht auch durch maurische Zollbeamte an der nordafrikanischen Küste und den Verkehr derselben mit italiänischen Kaufleuten. Nach der gewöhnlichen Meinung brachten sie die Araber, welche sie von den Indern angenommen hatten, nach Spanien, wo wahrscheinlich schon im zehnten Jahrhundert der wegen seiner Gelehrsamkeit berühmte Gerbert, aus Frankreich gebürtig, welcher unter dem Namen Sylvester II. im Jahre 999 die päbstliche Würde erhielt, sie von ihnen lernte. In einem seiner Briefe sagt er, daß dieselbe Zahl modo simplex, modo compositus, nunc digitus, nunc constituatur ut articulus. In einem Rechenbuche aus dem 14ten Jahrhundert heißen 10, 20, 30 numerus articulus, und 11, 12 bis 19 numerus compositus. (Kästners G. d. M. II. S. 699.). Ein Chronikenschreiber Wilhelm von Malmesbury, der ungefähr 150 Jahre nach Gerbert lebte, sagt von ihm: Abacum certe primus a Saracenis rapiens regulas dedit, quae a sudantibus Abacistis vix intelligantur. In einem geometrischen Werke Gerberts, das in eine Sammlung verschiedener Schriften: Thesaurus Anecdo-

torum. T. III. Augustae Videl. 1721. eingerückt ist, sind Ausrechnungen der Figuren mit dekadischen Zahlen dargestellt. Das Manuscript, woraus es abgedruckt worden, schätzt der Herausgeber 600 Jahre alt. Es ist nicht ausdrücklich angeführt, daß es dekadische Ziffern enthalte; doch aber zu vermuthen, weil sonst die Veränderung der Zahlbuchstaben in dekadische Zeichen wohl vom Herausgeber angezeigt worden wäre.

6. Die dekadischen Ziffern sind langsam in Gebrauch gekommen, wie es in jenem Zeitalter nicht anders seyn konnte. Man sieht es aus einer arithmetischen Schrift des Leonardus Pisanus, die im J. 1202 verfaßt ist. Von dieser findet man eine ausführliche Nachricht in des Targioni Tozzetti Relazioni d'alcuni viaggi fatti in Toscana. T. II. p. 59. der zweiten Ausgabe zu Florenz. 1768. Die Schrift des Leonardo ist auf der Magliabecchischen Bibliothek zu Florenz handschriftlich vorhanden. Der Verfasser erzählt, daß sein Vater, ein Handelsmann, ihn in dem studio abaci unterrichtet habe; der vortreffliche Unterricht, mit den neun Figuren der Inder zu rechnen, habe ihm ganz vorzüglich gefallen; er habe daraus begriffen, was er auf seinen weiten, wegen der Handlung unternommenen Reisen in und außer Europa mit vieler Mühe gelernt hätte; das Alles aber und andere Rechnungsarten halte er gleichsam für fehlerhaft (quasi errorem) in Vergleichung mit der Weise der Inder. Deswegen wolle er diese so deutlich als möglich vortragen. In dem ersten Kapitel zeigt er, wie mit den neun Figuren und dem Zeichen 0, welches arabisch Zephirum heiße, alle Zahlen geschrieben werden. Man sieht aus dieser Schrift, daß die indische Rechenkunst gegen Ende des 12ten Jahrhunderts selbst unter Kaufleuten noch nicht ausgebreitet gewesen ist. Schon Vossius (de Matheseos natura. p. 34.) war der Meinung, daß unsere Zahlzeichen nicht vor 1300 oder höchstens 1250 in Europa eingeführt seyen. Wallis glaubt, daß ihr Gebrauch älter sey, auch in England, wenn nicht im gemeinen Leben, doch in astronomischen Tafeln. Bei diesen habe man den Anfang ge-

macht, als sie aus den arabischen Originalen abgeschrieben und zugleich in's Lateinische übersetzt wurden; hernach habe man die dekadischen Ziffern auch zu andern Rechnungen angewandt. In der Bibliothek zu Oxford sind astronomische Tafeln von einem maurisch-spanischen Verfasser Arzachel, die etwa um 1080 verfertigt sind. In diesen sind dekadische Ziffern gebraucht. Die lateinische Abschrift scheint um 1200 oder doch vor 1250 gemacht zu seyn. Da die Alphonsinischen Tafeln um 1270 oder schon 1252 bekannt gemacht worden sind, so hat man sich gewiß nicht die Mühe gegeben, ältere von geringerem Werthe abzuschreiben. In einer andern Sammlung astronomischer Tafeln, die für den Anfang des Jahres 1150 berechnet sind, werden schon die dekadischen Ziffern angetroffen. Ein Paar Schriften über die Festrechnung aus der ersten Hälfte des 13ten Jahrhunderts zeigen sie auch in alten Exemplaren. Wie früh man sie im gemeinen Leben gebraucht habe, ist nicht zuverlässig auszumachen. Die älteste Spur glaubte Wallis auf einem Kamine zu Helmdon in Northamtonshire gefunden zu haben, folgendergestalt: A° DO' M° 133, d. i. 1133. Nach seiner Zeit meinte man noch frühere Jahreszahlen in England entdeckt zu haben, als 1090 in Colchester, auch M16 = 1016, ferner 1011, sogar 975. Dagegen hat Dr. Ward in den Philos. Transact. erinnert, daß es unwahrscheinlich sey, daß die neuen Zahlzeichen von Handwerksleuten so sehr früher gebraucht seyen, als von Gelehrten, da sie in keinem alten Manuscripte eher vorkämen als in einigen Abschriften von des Johannes de Sacro Bosco Werk, der 1256 gestorben ist. Er bemerkt, daß die Inschrift zu Helmdon 1233 gelesen werden müsse, daß die zu Colchester 1490 sey, daß M16 keine Zahl, sondern die Anfangsbuchstaben MIC eines Namens sey, und daß statt der Jahrzahl 975 die römische Zahl MXV gelesen werden müsse (Martyn's Abridg. Phil. Trans. Vol. 9. p. 420.). Die Zahl 1011 hat man nachgehends für Buchstaben aus dem Namen eines Schutzheiligen erkannt.

In öffentlichen Aufschriften erscheinen nach Gatterers

Versicherung die Ziffern erst vom 14ten Jahrhundert an; aber in Urkunden höchst selten vor dem 15ten. Auch wird häufig von einer Zahl ein Theil mit Worten, der andere mit römischen Zahlzeichen ausgedrückt. Ziffern sind ihm unter Tausenden von Urkunden, deren Originale er in Händen gehabt, erst 1527 vorgekommen.

Außer den schon angeführten Schriften s. m. noch:

Hutton's mathem. and philos. Dictionary. Art. Figures.

Kästners Gesch. d. Math. I. S. 36. II. S. 695.

Berlinische Blätter, herausgegeben von Biester. 1. Blatt. 1797. Darin Bemerkungen über die Observations on the introduction of arabic numerals into England by M. North. in der Archaeologia by the Society of Antiquaries at London. 1792.

Weidler de characteribus numerorum vulgaribus et eorum aetatibus. Vitemb. 1727.

Die einzelnen Abhandlungen von Ward findet man Philos. Transact. 1735. p. 120. 1735. p. 136. 1744. p. 79. 1745. p. 283. 1748. p. 603. Zwei Abhandlungen von Wallis ebendas. 1683. p. 399. 1700. p. 677. Von Luffkin und Barlow 1699. p. 287. 1741. p. 652.

Vom Ursprunge der üblichen Zahlziffern von Siegfrieden im Gothaischen Magazin. 1. Band. 1776. 2. Band. 1777.

Zauberquadrat, s. Quadrat, magisches.

Zehner, die Ziffern der ersten Ordnung im dekadischen Zahlensystem; s. Zahlensystem.

Zehneck, s. Vieleck (48. ff.).

Zeichen in der Mathematik sind willkührliche Bilder der Größen, ihrer Formen und Verbindungen.

Von den Zeichen bestimmter Zahlen s. Zahlensystem

und Zahlzeichen. Die Zeichen unbestimmter Größen sind Buchstaben, s. Bezeichnung und Buchstabenrechnung. In diesem Artikel soll nur eine Uebersicht der gewöhnlichen Zeichen gegeben werden (s. Thl. I. S. 307.).

Das Zeichen der Addition ist +, das Zeichen der Subtraction ist —. Beide Zeichen hat Hutton (Math. Dict. Art. Characters) zuerst bei Stifel gefunden. Cardan, Tartalea u. A. gebrauchten die Buchstaben p und m, d. i. plus oder piu und minus.

Auch bedeuten + und — vor dem Symbol einer Größe das Positive und Negative, wie z. B. + a oder — a (s. Entgegengesetzte Größen). Dieser doppelte Gebrauch der Zeichen + und — hat Einige veranlaßt, für die Beziehung des Entgegengesetzten andere Zeichen vorzuschlagen (s. z. B. H. A. Rothe Lehrb. der Arithm. Thl. I. Lpzg. 1804. Eilftes Kapitel), von denen aber keine allgemein in Gebrauch gekommen sind.

Das Zeichen der Multiplication ist ×, bei bestimmten Zahlen, bei Linien, die durch die beiden Buchstaben an ihren Endpunkten angedeutet werden, etwa bei gebrochenen Factoren, oder zur Absonderung einiger Factoren eines Products von den andern, wenn jene als ein einziger Factor betrachtet und ausgezeichnet werden sollen. Dieses Zeichen ist von Oughtred eingeführt. Werden die Factoren eines Products durch einzelne Buchstaben bezeichnet, so werden sie bloß neben einander geschrieben, wie abcde... Auch ein Punkt (.) zeigt bei numerischen Factoren eine Multiplication an. Z. B. 4.5 ist 20. Bei gebrochenen Factoren in bestimmten oder unbestimmten Größen wird ebenfalls noch oft ein Punkt zur Bezeichnung der Multiplication gebraucht.

Das Zeichen der Division ist entweder ein Strich mit dem Dividendus darüber und dem Divisor darunter, wie $\frac{a}{b}$, oder : , zwischen dem Dividendus und Divisor, so daß ersterer voran steht, wie a : b. Beides heißt a durch b dividirt. Wenn Dividendus und Divisor aus mehreren Theilen bestehen, so ist die erstere Bezeichnung

vorzuziehen. Letztere hat den Vortheil, daß die Zeilen nicht gesperrt werden. Pell hat nach Hutton a. a. O. das Zeichen ÷ zur Bezeichnung der Division gebraucht, welches aber in deutschen Rechenbüchern auch zur Bezeichnung der Subtraction angewandt wird.

Zusammengesetzte (complexe) Größen, welche wie eine einfache Größe betrachtet und behandelt werden sollen, werden in Parenthesen oder Klammern eingeschlossen, wie z. B. $(a+b-c)$. Nach dem Dict. math. der französischen Encyklopädie (Art. Caractère) hat Guido Grandi sich dieser Bezeichnung zuerst bedient. Wahrscheinlicher rührt dieselbe aber von Albert Girard her. Vieta zog einen Strich über die als einfach zu betrachtende complexe Größe, wie $\overline{a+b-c}$. In neuerer Zeit ist diese Bezeichnung, wie sie es, wenn mehrere Parenthesen hinter einander vorkommen, oder bei Wurzelgrößen, allerdings auch verdient, wieder mehr in Aufnahme gekommen. So ist z. B.

$$\sqrt[3]{\overline{a+b-c}} = \sqrt[3]{(a+b-c)}\,.$$

Anstatt der Klammern werden bei complexen Größen, wenn es keinen Mißverstand giebt, zuweilen auch Punkte gebraucht, wie z. B. bei der Multiplication mehrerer Factoren in einander, welche nach einem bestimmten Gesetze fortschreiten:

$$\frac{n(n-1)..(n-m+1)}{1.2.3...m} = \frac{n.n-1.n-2..n-m+1}{1.2.3...m}\,.$$

Die mte Potenz von a wird durch a^m, die nte Wurzel aus der mten Potenz von a durch $\sqrt[n]{a^m}$ oder $a^{\frac{m}{n}}$ bezeichnet, worüber, so wie über verschiedene ältere Bezeichnungen der Potenzen und Wurzeln, mit Mehrerem der Art. Potenz nachzusehen ist. Nur bei der Quadratwurzel wird der Wurzelexponent weggelassen. Eben so sind log, log nat, sin, cos, tang, cot, sec, cosec, sin vers, cos vers, Arc sin, Arc cos, Arc tang, u. s. f. leicht verständliche Bezeichnungen, über die man in den Artt. Logarithmus, Cyclometrie und Goniometrie weitere Belehrung suchen muß.

Das Zeichen der Gleichheit ist $=$. Robert Recorde hat es nach Hutton zuerst gebraucht. Descartes bediente sich des Zeichens ∞; eben so Hudde, Rolle, Ozanam nach Saverien Dict. Math. Durch Harriot ist das Zeichen $=$ zuerst allgemein geworden.

Das Zeichen der Ungleichheit ist $>$ und $<$. Nämlich $a > b$ heißt: a ist größer als b, und $b < a$ heißt: b ist kleiner als a. Oughtred, Barrow u. A. bedienten sich der Zeichen ⊐ (größer) und ⊏ (kleiner). Das Zeichen $\gtrless$ zeigt an, daß eine Größe größer, kleiner oder eben so groß als eine andere seyn könne (S. den Art. Verhältniß). Es ist ein neues, etwa in der deutschen Ausgabe des Euklides von Lorenz zuerst gebrauchtes, Zeichen.

Das Zeichen des arithmetischen Verhältnisses zweier Größen ist $a - b$, des geometrischen Verhältnisses $a : b$. Der Grund dieser Bezeichnungen durch das Subtractions- und Divisionszeichen erhellet leicht aus der Natur dieser Verhältnisse. Die arithmetische und geometrische Proportion bezeichnet man durch $a - b = c - d$ und $a : b = c : d$. Letztere Bezeichnung ist seit Wolf in Deutschland allgemein eingeführt, und entspricht ihrem Zwecke vollkommen. Englische und französische Schriftsteller bezeichnen die geometrische Proportion gewöhnlich durch $a : b :: c : d$. Das Zeichen (::) rührt von Oughtred her. Auch findet man $a . b = c . d$ als Bezeichnung einer geometrischen Proportion, nach Saverien a. a. O., aber selten. Ein Verhältniß, welches aus den Verhältnissen $a : b$, $c : d$, $e : f$, u. s. f. zusammengesetzt ist, bezeichnet man durch $(a : b) + (c : d) + (e : f) + \ldots$ Eine geometrische Progression wird auch bezeichnet durch ∺ 3, 6, 12, 24, 48, ...; eben so eine stetige arithmetische Proportion durch ÷ a . b . c, eine stetige geometrische Proportion durch ∺ a.b.c. Eine arithmetische Progression durch ÷ 2, 6, 10, 14, 18, 22, ...

∞ bedeutet bei einigen englischen und französischen Schriftstellern, wenn es zwischen zwei Größen steht, wie z. B. $a \infty b$, den Unterschied der beiden Größen a und b,

es mag die vorangesetzte a die größere oder die kleinere seyn. Dieses Zeichen scheint von Wallis zuerst gebraucht zu seyn. Es ist aber völlig unnöthig und unnütz, daher auch gar nicht in Gebrauch gekommen. Das Vorzeichen der Differenz liefert die nöthige Bestimmung von selbst.

Bei deutschen Schriftstellern ist ∞ das Zeichen der Aehnlichkeit, ein liegendes lateinisches S. Leibnitz und Wolf haben es zuerst angewandt. Oft gebraucht man das Wort ähnlich selbst. Vergl. Miscellan. Berolin. Part. III. p. 159.

Mit dem Begriffe hat auch Gauß das Zeichen $\equiv$ als Zeichen der Zahlen-Congruenz eingeführt (s. den Art. Zahl. II. 1.). $\sqrt{-1}$ wird oft, auch in diesem Wörterbuche, durch i bezeichnet.

Hat eine Größe mehrere Werthe, so wird nach Cauchy der Inbegriff aller Werthe durch Einschließung in doppelte Parenthesen, ein bestimmter Werth durch Einschließung in eine einfache Parenthese bezeichnet. So bezeichnet z. B. $\sqrt[n]{((a+x))}$ den Inbegriff aller Werthe, welche diese Wurzel haben kann, $\sqrt[n]{(a+x)}$ dagegen irgend einen bestimmten Werth dieser Wurzel. Bei allen mehrerer Werthe fähigen analytischen Ausdrücken ist diese Bezeichnung, welche allgemeiner eingeführt zu werden verdiente, anwendbar.

$*$ bedeutet ein fehlendes Glied in einer Reihe oder Gleichung, wie z. B. $ax^3 * + bx + c = o$, weil in dieser Gleichung das die Potenz x^2 enthaltende Glied fehlt.

Ist $y = f(x)$, eine Function einer veränderlichen Größe x (über die Bezeichnung der Functionen s. m. den Art. Function. 2.), so werden der erste, zweite, dritte, vierte Differentialquotient nach der Reihe durch $\frac{\partial y}{\partial x}, \frac{\partial^2 y}{\partial x^2}, \frac{\partial^3 y}{\partial x^3}, \frac{\partial^4 y}{\partial x^4}, \ldots$ bezeichnet. Lagrange's derivirte Functionen sind mit den Differentialquotienten einerlei, und wer-

den nach der Reihe durch $f'(x)$, $f''(x)$, $f'''(x)$, $f^{iv}(x)$, ... bezeichnet.

Die Engländer gebrauchen die von Newton eingeführte höchst unbequeme Bezeichnung der auf einander folgenden Differentialverhältnisse $\dot{x}:y$, $\ddot{x}:y$, $\dddot{x}:y$, u. s. f. Jetzt mag aber diese Bezeichnung wohl auch größtentheils abgekommen seyn. Ist y eine Function mehrerer veränderlichen Größen x, v, u, ..., so bedeutet $\left(\frac{\partial y}{\partial x}\right)$ den Differentialquotienten von y in Bezug auf x, wenn bloß diese Größe als veränderlich betrachtet wird, d. h. das partielle Differential von y in Bezug auf x. Eine ähnliche Bedeutung haben Symbole wie $\frac{\partial^4 y}{\partial v \partial x^3}$, $\frac{\partial^6 y}{\partial u \partial v^2 \partial x^3}$, u. s. f.

Das unbestimmte Integral eines Differentials Xdx wird durch $\int Xdx$ bezeichnet. Soll dieses Integral aber zwischen den Gränzen a, b, d. i. von a bis b, genommen werden, so erhält man ein bestimmtes Integral, und bezeichnet es nach den neuesten französischen Schriftstellern durch $\int_a^b Xdx$.

Die nte Variation einer Function V wird durch $\delta^n V$ bezeichnet; s. Variationsrechnung.

Ueber die vielen combinatorischen Zeichen s. m. den Art. Combinatorische Analysis und Localzeichen. Eben so den Art. Facultät über die bei dieser Größenform gewöhnlichen Bezeichnungen, u. s. f.

Von geometrischen Zeichen bemerke man nur noch folgende:

△ ein Dreieck.

□ ein Quadrat.

▭ ein Rechteck, oder Parallelogramm überhaupt.

AB × BC das unter den Linien AB und BC als zusammenstoßenden Seiten enthaltene Rechteck.

AB^2 oder AB^q das Quadrat der Linie AB; auch □AB.

○ ein Kreis.

∠ ein Winkel.

∟ oder R, auch ℜ, ein rechter Winkel.

⊥ eine senkrechte Linie, wenig üblich.

|| Parallelen.

⋕ Gleiche und parallele Linien.

Französische Schriftsteller setzen über die Bezeichnung einer geraden Linie durch die beiden Buchstaben A und B an ihren Endpunkten gewöhnlich einen Strich, wie $\overline{AB}$.

Bei Winkelmessungen bedeuten die Zeichen, °, ′, ″, ‴, ... Grade, Minuten, Secunden, Tertien, Quarten u. s. f., wie z. B. 25° 17′ 32″ 45‴.

Bei Messungen gerader Linien bedeuten dieselben Zeichen Ruthen, Fuße, Zolle, Linien, Scrupel u. s. f. Um Zweideutigkeiten zu verhüten, mag man in diesem Falle einen kleinen Bogen unter jedes Zeichen setzen, wie z. B. 16° 9′ 8″ 7‴.

Die hier aufgeführten werden die am meisten vorkommenden Zeichen seyn.

Zens nebst seinen Zusammensetzungen, s. Potenz (8.).

Zerlegung der Zahlen (Partitio numerorum) s. Theilung (2.).

Zerstreute Proportion, s. Verhältniß (13.).

Zero, Null, s. Zahlzeichen (3.).

Zetetice, ein bei den ältern Algebraisten, z. B. Harriot und Vieta, gebräuchliches Kunstwort, welches die Erfindung oder Aufstellung der Gleichungen bei einer Aufgabe bezeichnet. Pars prior Analytices, quae in constitutione aequationum versatur.

Ziffern, s. Zahlzeichen.

Zone nennt man jedes von zwei parallelen Kreisen eingeschlossene Stück der Oberfläche eines durch Umdrehung

einer Curve entstandenen Körpers. Im Art. Sphäroid. (35. ff.) ist von dem Flächeninhalte der Zonen des elliptischen Sphäroids ausführlich gehandelt, weshalb wir hier nur noch einige Bemerkungen über Kugelzonen beibringen wollen.

1. Man bezeichne den Halbmesser der Kugel durch r, und rechne die Abscissen vom Mittelpunkte; so ist die Gleichung des erzeugenden Kreises $x^2 + y^2 = r^2$. Entsprechen nun die Parallelkreise, welche die Zone Z begränzen, den Abscissen α, a; so ist nach Thl. I. S. 514.

$$Z = 2\pi \int_\alpha^a y\partial x \sqrt{1 + \left(\frac{\partial y}{\partial x}\right)^2}.$$

Aber

$$x\partial x + y\partial y = 0, \frac{\partial y}{\partial x} = -\frac{x}{y};$$

$$\int y\partial x \sqrt{1 + \left(\frac{\partial y}{\partial x}\right)^2} = \int y\partial x \sqrt{\frac{r^2}{y^2}} = \int r\partial x = rx.$$

Also $Z = 2\pi r(a - \alpha)$. Da nun offenbar $a - \alpha$ die Höhe der Zone, und $2r\pi$ die Peripherie eines größten Kugelkreises ist; so findet man den Inhalt einer sphärischen Zone, wenn man mit ihrer Höhe die Peripherie eines größten Kugelkreises multiplicirt. Einen elementaren Beweis s. m. in Legendre Elém. de Géom. Livre VIII. Prop. XI. Auch ist, wie schon Archimedes (De Sphaera et Cylindro I. 50. Coroll. 4.) gefunden hat, der Flächeninhalt einer sphärischen Zone der Seitenfläche eines geraden Cylinders gleich, welcher mit der Zone einerlei Höhe und mit der Kugel einerlei Halbmesser hat.

2. Der Inhalt des der Zone entsprechenden Körpers ist nach Thl. I. S. 580., wenn wir denselben durch Z′ bezeichnen, =

$$Z' = \pi \int_\alpha^a y^2 \partial x.$$

Aber

$$\int y^2 \partial x = \int (r^2 - x^2)\partial x = r^2 x - \tfrac{1}{3}x^3.$$

Folglich

$$\begin{aligned} Z' &= \pi r^2 (a - \alpha) - \tfrac{1}{3}\pi (a^3 - \alpha^3) \\ &= \pi r^2 (a - \alpha) - \tfrac{1}{3}\pi (a - \alpha)(a^2 + a\alpha + \alpha^2) \\ &= \pi r^2 (a - \alpha) - \tfrac{1}{3}\pi (a - \alpha) a^2 - \tfrac{1}{3}\pi (a - \alpha) \alpha^2 \\ &\quad - \tfrac{1}{3}\pi (a - \alpha) a\alpha. \end{aligned}$$

$$= \tfrac{1}{2}(a-\alpha)(r^2-a^2)\pi + \tfrac{1}{6}\pi(a-\alpha)a^2$$
$$+ \tfrac{1}{2}(a-\alpha)(r^2-\alpha^2)\pi + \tfrac{1}{6}\pi(a-\alpha)\alpha^2$$
$$- \tfrac{1}{3}\pi(a-\alpha)a\alpha$$
$$= (a-\alpha).\frac{(r^2-a^2)\pi+(r^2-\alpha^2)\pi}{2} + \tfrac{1}{6}\pi(a-\alpha)^3 .$$

$r^2 - a^2$ und $r^2 - \alpha^2$ sind offenbar die Quadrate der Halbmesser der Grundkreise der Zone. Man erhält also den Inhalt des entsprechenden Körpers, wenn man die Höhe der Zone mit der halben Summe der Flächenräume der Grundkreise multiplicirt, und den Inhalt einer Kugel addirt, deren Durchmesser die Höhe der Zone ist. Einen andern Beweis s. bei Legendre a. a. O. L. VIII. P. XVIII.

Für einen bloßen sphärischen Abschnitt ist die eine Grundfläche $= 0$, oder $a = r$. Also der Flächeninhalt $= 2\pi r(r-\alpha)$ (1.), und der cubische Inhalt

$$= \frac{(r-\alpha)(r^2-\alpha^2)\pi}{2} + \tfrac{1}{6}\pi(r-\alpha)^3 .$$

M. s. Archimedes l. c. Coroll. 1.

3. Sind die geographischen Breiten der Parallelkreise einer Zone H, H′; so ist, wenn beide Breiten nördlich, oder beide südlich sind, die Höhe der Zone offenbar

$$= r\cos(90^\circ - H') - r\cos(90^\circ - H)$$
$$= r\{\sin H' - \sin H\} .$$

Wäre die Breite H′ nördlich, H dagegen südlich, oder umgekehrt; so erhellet leicht, daß man H negativ nehmen muß, wodurch das Minuszeichen in obigem Ausdruck in ein Pluszeichen verwandelt wird. Folglich die Oberfläche der Zone nach (1.)

$$= 2\pi r^2\{\sin H' - \sin H\}$$
$$= 4r^2\pi\sin\left(\frac{H'-H}{2}\right)\cos\left(\frac{H'+H}{2}\right)$$

(Goniometrie. 28.).

Für eine südliche Breite H, wenn H′ nördlich, wird dieser Ausdruck

$$= 4r^2\pi\sin\left(\frac{H'+H}{2}\right)\cos\left(\frac{H'-H}{2}\right) .$$

Für die gemäßigten Zonen der Erde ist $H = 23^\circ 28'$,

$H' = 66^0\ 32'$; für die kalten $H = 66^0\ 32'$, $H' = 90^0$; für die heiße Zone $H = -23^0\ 28'$, $H' = +23^0\ 28'$; woraus man mittelst vorstehender Formel und des bekannten mittlern Halbmessers der Erde leicht die Flächenräume der einzelnen Zonen berechnen kann.

4. Sey nun der Flächeninhalt eines sphärischen Vierecks, welches von zwei bekannten Meridianen und zwei bekannten Parallelkreisen eingeschlossen wird, $= V$. Die Längen und Breiten seiner Spitzen seyen L, L' und H, H'. Der zwischen den beiden Meridianen enthaltene Bogen des Aequators ist $= L' - L$. Ist nun, wie oben, die Area der ganzen Zone $= Z$; so erhellet leicht die Richtigkeit folgender Proportion:

$$360^0 : L' - L = Z : V.$$

Also

$$V = Z \cdot \frac{L' - L}{360^0},$$

d. i. nach (3.)

$$V = 4r^2\pi\left(\frac{L' - L}{360^0}\right)\sin\left(\frac{H' - H}{2}\right)\cos\left(\frac{H' + H}{2}\right)$$

$$= r^2\pi\left(\frac{L' - L}{90^0}\right)\sin\left(\frac{H' - H}{2}\right)\cos\left(\frac{H' + H}{2}\right).$$

$L' - L$ muß, so wie 90^0, in Graden ausgedrückt seyn. Wäre $L' - L$ in Secunden gegeben, so müßte man auch 90^0 auf Secunden bringen.

Zufälliger Punkt, s. Perspectiv (9.).

Zufällige Wurzeln, s. Gleichung (171.).

Zugeordneter oder conjugirter Punkt, s. Conjugirt. III. und Vielfacher Punkt.

Zuglinie, s. Tractoria.

Zusammengesetzte Gleichung, s. Gleichung (4.).

Zusammengesetztes Verhältniß, s. Verhältniß (14.).

Zusammengesetzte Zahl, s. Primzahl (1.), Theiler einer Zahl (1.).

Zusammenlaufende Linien (lineae convergentes) sind solche gerade Linien, welche, verlängert, einander schneiden.

Zusatz, s. Corollarium.

Zweig einer krummen Linie, s. Krumme Linie (26.).

Zwerchaxe heißt zuweilen die bestimmte oder Hauptaxe der Hyperbel, welche zwischen ihren beiden Scheiteln liegt.

Zweitheilige Größe, s. Binomium.