Faksimile-Reprint der Auflage von 1889,
herausgegeben von H. Maser

Mit freundlicher Genehmigung des
Göttinger Digitalisierungszentrums (GDZ)
http://gdz.sub.uni-goettingen.de/

Verlag Kessel
Eifelweg 37
53424 Remagen-Oberwinter
Tel.: 02228-493
Fax: 03212-1024877
E-Mail: nkessel@web.de
www.verlagkessel.de

Druckerei Sieber
Rübenacher Str. 52
56220 Kaltenengers
www.business-copy.com

Auf der letzten Seite befindet sich eine Tabelle,
in der die im Original befindlichen handschriftlichen
Korrekturen bzw. Änderungen zusammengefasst sind.

ISBN: 978-3-941300-09-5

Carl Friedrich Gauss'

Untersuchungen über höhere Arithmetik.

(Disquisitiones arithmeticae. Theorematis arithmetici demonstratio nova. Summatio quarumdam serierum singularium. Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae. Theoria residuorum biquadraticorum, commentatio prima et secunda. Etc.)

Deutsch herausgegeben

von

H. Maser.



Berlin.

Verlag von Julius Springer.

1889.

EX
BIBLIOTHECA
REGIA ACADEM.
GEORGIAE
AUG.

Vorwort des Herausgebers.

Das Studium der herrlichen Geisteserzeugnisse unseres unsterblichen Gauss ist für jeden Mathematiker, der es ernsthaft mit seiner Wissenschaft meint, eine unabweisbare Pflicht. Grossen Dank ist man daher der Königlichen Gesellschaft der Wissenschaften zu Göttingen schuldig, dass sie durch Veranstaltung einer billigen in einzelnen Bänden erhältlichen Ausgabe der Gauss'schen Werke im Originaltext jedermann in den Stand gesetzt hat, sich dieselben anzuschaffen. Wenn nun trotz der leichten Erhältlichkeit des Originals hier noch der Versuch mit einer deutschen Ausgabe der *Disquisitiones arithmeticae* und der in lateinischer Sprache geschriebenen im zweiten Bande der Gesammelten Werke enthaltenen zahlentheoretischen Abhandlungen gewagt wird, so hat dies in der Erwägung seinen Grund, dass eben die sprachlichen Schwierigkeiten des Originals für viele Leser keine geringen sind und um so drückender empfunden werden, als das Verständnis des Inhaltes selbst, und zwar nicht bloss beim ersten Studium desselben, eine sehr bedeutende Geistesthätigkeit erfordert und alle Kräfte in Anspruch nimmt. Der des Faches kundige Gelehrte wird allerdings lieber zum Originale greifen. Denn wie in den Augen des Kenners ein Werk der Skulptur oder Malerei zwar durch die Gediegenheit und Bedeutung des behandelten Stoffes und durch die Feinheit in der Anordnung und Ausführung der einzelnen Teile Anerkennung findet, aber erst durch die Thatsache, dass es Original ist, seinen wahren Wert erhält, so auch ein Werk der schöngeistigen oder fachwissenschaftlichen Literatur. Nur das Originalwerk zeigt uns die Genialität seines Schöpfers im vollen Glanze und erfüllt uns mit jenem geistigen Vergnügen, welches die Bewunderung grosser Männer gewährt. Da nun die *Disquisitiones arithmeticae* ein durch seinen Inhalt wie durch seine Form hervorragendes klassisches Werk sind, so kann das Studium derselben im Originaltext nicht dringend genug empfohlen werden. Wem es aber zunächst nur darum zu thun ist, mit dem Inhalte selbst bekannt zu werden, der wird es jedenfalls dankbar annehmen, wenn es ihm durch Hinwegräumung äusserer Schwierigkeiten ermöglicht wird, seine ganze Aufmerksamkeit auf die Sache zu richten. Daher darf man sich immerhin der Hoffnung hingeben, dass die vorliegende deutsche Ausgabe vielen Lesern sehr willkommen sein wird.

Was nun diese Ausgabe selbst anlangt, so hätten in dieselbe von den kleineren Abhandlungen wohl nur die von Gauss selbst veröffentlichten aufgenommen werden sollen; ich habe aber auch die in seinem Nachlasse vorgefundenen, im zweiten Bande seiner Werke enthaltenen Fragmente nicht ausschliessen wollen, weil sie noch manches Goldkörnchen, manche wertvolle Bemerkungen und interessante Sätze enthalten, obwohl sie weder sachlich noch formell vollkommen druckfertig genannt werden können und daher wohl in der Gesamtausgabe seiner Werke aber nicht hier einen Platz beanspruchen durften. Um den Character und Geist der Gauss'schen Arbeiten möglichst rein und frei von jedem Beiwerk wiederzuspiegeln, habe ich mich aller eigenen Anmerkungen enthalten und nur die bereits sanctionierten, von Herrn Professor Dedekind herrührenden Bemerkungen zu einigen Abhandlungen mit gütiger Erlaubnis des Verfassers aus dem zweiten Bande der Göttinger Ausgabe übernommen.

Für diejenigen, denen dieser Band selbst nicht zur Hand ist, füge ich zur Orientierung hier noch einige daraus entnommene Notizen hinzu. An einigen Stellen der *Disqu. arithm.* wird auf einen achten Abschnitt verwiesen, obwohl ein solcher nicht vorhanden ist; ferner haben die hier mitgeteilten Artikel aus der „Lehre von den Resten" und die Abhandlung auf Seite 678 eine eigentümliche Numerierung. Es findet dies dadurch seine Erklärung, dass Gauss seine ursprünglichen Aufzeichnungen, welche den Titel *„Analysis residuorum"* tragen, einer gänzlichen Umarbeitung unterzog, aus welcher die *Disquisitiones arithmeticae* hervorgingen, deren achter Abschnitt die auf Seite 589 u. ff. mitgeteilten Untersuchungen zum Gegenstande haben sollte. Als zu umfangreich wurden diese Untersuchungen aber schliesslich von den *Disqu. arithm.* ausgeschlossen und der achte Abschnitt einer eingehenderen Betrachtung der Lehre von der Kreisteilung vorbehalten, daher das darauf bezügliche Fragment (Seite 678) sich in der Numerierung seiner Artikel unmittelbar an die *Disqu. arithm.* anschliesst. Die Artikel in den beiden Abschnitten aus der „Lehre von den Resten" tragen dieselben Nummern wie im ursprünglichen Manuskript.

Vor einigen Jahren ist von mir eine Ubersetzung des so überaus selten gewordenen Legendre'schen Werkes *„Théorie des nombres"* herausgegeben worden; es sei mir erlaubt, meiner Freude darüber Ausdruck zu geben, dass es mir vergönnt war, auch das zweite und bedeutendere klassische Werk über Zahlentheorie, die *Disquisitiones arithmeticae* von Gauss, dem mathematischen Publikum in deutscher Sprache zu überreichen. Ich hoffe damit der Wissenschaft auch einen kleinen Dienst erwiesen zu haben.

Berlin, im März 1889.

Der Herausgeber.

Vorrede des Verfassers zu den Arithmetischen Untersuchungen.

Die in diesem Werke enthaltenen Untersuchungen beziehen sich auf denjenigen Teil der Mathematik, der es mit den ganzen Zahlen zu thun hat, während die gebrochenen Zahlen meistenteils, die imaginären immer ausgeschlossen bleiben. Die sogenannte unbestimmte oder Diophantische Analysis, welche aus unendlich vielen dem unbestimmten Problem genügenden Lösungen diejenigen auszuwählen lehrt, welche ganzzahlig oder wenigstens rational sind (meistens auch noch unter der Bedingung, dass sie positiv seien), ist nicht jene Disziplin selbst, sondern vielmehr ein sehr specieller Teil derselben und verhält sich zu ihr ungefähr so, wie die Kunst, die Gleichungen zu reduzieren und aufzulösen (Algebra), zur gesamten Analysis. Wie nämlich in das Gebiet der Analysis alle Untersuchungen gehören, welche über die allgemeinen Eigenschaften und Beziehungen der Zahlgrössen angestellt werden können, so bilden die ganzen Zahlen (und die gebrochenen, insofern sie durch ganze bestimmt werden) den eigentlichen Gegenstand der Arithmetik. Da aber das, was gewöhnlich unter dem Namen Arithmetik gelehrt wird, kaum über die Kunst zu zählen und zu rechnen (d. h. die Zahlen durch geeignete Zeichen etwa nach dem dekadischen Systeme darzustellen und die arithmetischen Operationen auszuführen) hinausgeht, mit Hinzufügung noch einiger Sachen, die entweder gar nicht zur Arithmetik gehören (wie die Lehre von den Logarithmen) oder doch wenigstens nicht den ganzen Zahlen eigentümlich sind, sondern für alle Zahlgrössen gelten, so scheint es sachgemäss zu sein, zwei Teile der Arithmetik zu unterscheiden und das Erwähnte zur elementaren Arithmetik zu rechnen, dagegen alle allgemeinen Untersuchungen über die eigentlichen Beziehungen der ganzen Zahlen der höheren Arithmetik, von der hier allein die Rede sein wird, zu überweisen.

Zur höheren Arithmetik gehört das, was Euclid in den „*Elementen*“ Buch VII u. ff. mit der bei den Alten gewohnten Eleganz und Strenge gelehrt hat; doch beschränkt sich dies auf die ersten Anfänge dieser Wissenschaft. Das berühmte Werk des Diophant, welches ganz den Problemen aus der unbestimmten Analysis gewidmet ist, enthält viele Unter-

suchungen, welche wegen ihrer Schwierigkeit und der Feinheit der Kunstgriffe eine nicht geringe Meinung von dem Geiste und Scharfsinn ihres Verfassers erwecken, besonders wenn man die Geringfügigkeit der Hülfsmittel bedenkt, welche ihm zu Gebote standen. Da aber diese Aufgaben mehr eine gewisse Gewandtheit und geschickte Behandlung als tiefere Prinzipien erfordern und überdies zu speciell sind und selten zu allgemeineren Schlüssen führen, so dürfte dieses Buch mehr aus dem Grunde eine Epoche in der Geschichte der Mathematik bilden, weil es die ersten Spuren einer characteristischen Kunst und der Algebra in sich enthält, als weil es die höhere Arithmetik mit neuen Entdeckungen bereichert hat. Bei weitem das Meiste verdankt man den Neueren, von denen zwar nur wenige Männer, aber Männer von unvergänglichem Ruhme, wie P. de Fermat, L. Euler, L. Lagrange, A. M. Legendre, den Zugang zu dem Heiligtume dieser göttlichen Wissenschaft erschlossen und gezeigt haben, von wie grossen Reichtümern es überfüllt ist. Ich unterlasse es jedoch hier anzuführen, welche Entdeckungen von jedem einzelnen dieser Geometer ausgegangen sind, da man dies aus den Vorreden zu den Zusätzen, mit denen Lagrange Euler's Algebra bereichert hat, und zu dem bald zu erwähnenden erst kürzlich erschienenen Werke von Legendre erfahren kann und überdies die meisten an gehöriger Stelle in diesen Arithmetischen Untersuchungen Erwähnung finden werden.

Der Zweck dieses Werkes, dessen Herausgabe ich schon vor fünf Jahren versprochen hatte, war der, die Untersuchungen aus der höheren Arithmetik, die ich teils vor teils nach jener Zeit angestellt habe, zur allgemeineren Kenntnis zu bringen. Damit sich aber Niemand wundere, dass ich die Wissenschaft hier fast von ihren ersten Anfängen an wiederholt und viele Untersuchungen von Neuem aufgenommen habe, mit denen sich schon andere beschäftigt haben, glaube ich darauf hinweisen zu müssen, dass ich, als ich mich zuerst im Anfange des Jahres 1795 dieser Art von Untersuchungen zuwandte, von allem dem, was von Neueren auf diesem Gebiete geleistet worden war, nichts wusste und aller Hülfsmittel, durch welche ich mir davon hätte einige Kenntnis verschaffen können, baar war. Während ich nämlich damals mit einer andern Arbeit beschäftigt war, stiess ich zufällig auf eine ausgezeichnete arithmetische Wahrheit (wenn ich nicht irre, war es der Satz des Artikels 108), und da ich dieselbe nicht nur an und für sich für sehr schön hielt, sondern auch vermutete, dass sie mit anderen hervorragenderen Eigenschaften im Zusammenhang stehe, bemühte ich mich mit ganzer Kraft, die Prinzipien, auf denen sie beruhte, zu durchschauen und einen strengen Beweis dafür zu erhalten. Als mir dies endlich nach Wunsch gelungen war, hatten mich die Reize dieser Untersuchungen derart

umstrickt, dass ich sie nicht mehr verlassen konnte; so kam es, dass, während das Eine immer zu dem Andern den Weg bahnte, das in den vier ersten Abschnitten dieses Werkes Mitgeteilte grösstenteils erledigt war, ehe ich von ähnlichen Arbeiten anderer Geometer etwas zu Gesicht bekommen hatte. Als mir darauf Gelegenheit wurde, die Schriften dieser grossen Geister durchzusehen, erkannte ich zwar, dass der grössere Teil meiner Uberlegungen längst abgethanen Sachen gewidmet gewesen war, um so lebhafter aber bestrebte ich mich, den Fussstapfen jener folgend, die Arithmetik weiter auszubauen; so wurden verschiedene Untersuchungen angestellt, von denen die Abschnitte V, VI und VII einen Teil wiedergeben. Als ich nach einiger Zeit den Entschluss fasste, die Früchte meiner Anstrengungen zu veröffentlichen, liess ich mich, dem Wunsche vieler nachgebend, um so lieber überreden, auch von jenen früheren Untersuchungen nichts zu unterdrücken, weil es damals noch kein Buch gab, aus dem man die in den Denkschriften der Akademieen zerstreuten Arbeiten anderer Geometer über diese Gegenstände hätte kennen lernen können, sodann weil viele von ihnen vollständig neu und zum grossen Teil nach neuen Methoden behandelt waren, endlich weil sie alle sowohl unter einander als auch mit den späteren Untersuchungen durch ein so enges Band zusammenhingen, dass auch das Neue nicht bequem genug auseinandergesetzt werden konnte, ohne dass das andere von Anfang an wiederholt worden war.

Inzwischen erschien das ausgezeichnete Werk des schon vorher um die höhere Arithmetik hochverdienten Legendre, *Essai d'une théorie des nombres*, Paris a. VI, in welchem er nicht nur alles, was bis dahin in dieser Wissenschaft gearbeitet worden war, sorgfältig zusammentrug und in Ordnung brachte, sondern auch noch sehr viel Neues aus seinem Eigenen hinzuthat. Da mir dieses Buch zu spät in die Hände kam, nachdem bereits der grösste Teil meines Werkes gedruckt war, habe ich es nirgends, wo die Analogie des Gegenstandes Gelegenheit dazu gegeben hätte, erwähnen können; nur hinsichtlich einiger weniger Stellen hielt ich es für notwendig in den Zusätzen einige Bemerkungen hinzuzufügen, die der edeldenkende und aufgeklärte Mann, wie ich hoffe, nicht übeldeuten wird.

Während des Druckes dieses Werkes, welcher mehrere Male unterbrochen und durch mancherlei Hindernisse bis ins vierte Jahr hinausgezogen wurde, habe ich nicht nur diejenigen Untersuchungen, die ich zwar schon früher angefangen, deren Veröffentlichung aber ich auf eine andere Zeit zu verschieben beschlossen hatte, um nicht das Buch allzu umfangreich werden zu lassen, weiter fortgesetzt, sondern noch mehrere andere neue in Angriff genommen. Auch wurden mehrere, die ich aus demselben Grunde nur obenhin berührt habe, weil eine ausführlichere Behandlung weniger not-

wendig erschien (z. B. die, welche in den Artikeln 37, 82 u. ff. und andern Stellen angeführt sind), später wieder aufgenommen und haben dieselben zu allgemeineren Untersuchungen, die der Veröffentlichung wert erscheinen, Veranlassung gegeben (vgl. auch, was in den Zusätzen über Artikel 306 gesagt ist). Schliesslich habe ich, da das Buch besonders wegen der grossen Ausdehnung des fünften Abschnittes bei weitem umfangreicher geworden war, als ich erwartet hatte, mehreres, was anfänglich für dasselbe bestimmt war, und unter andern den ganzen achten Abschnitt (welcher in diesem Bande bereits an einigen Stellen erwähnt wird und eine allgemeine Abhandlung über die algebraischen Congruenzen jeden Grades enthält) weglassen müssen. Alles dieses, welches mit Leichtigkeit einen mit dem vorliegenden gleichstarken Band ausfüllen wird, werde ich veröffentlichen, sobald sich die Gelegenheit dazu bietet.

Dass ich bei mehreren schwierigen Untersuchungen mich synthetischer Beweise bedient und die Analysis, durch welche dieselben gefunden sind, unterdrückt habe, ist besonders durch das Streben nach Kürze veranlasst, der ich mich soviel wie möglich befleissigen musste.

Die Theorie der Kreisteilung oder der regulären Polygone, welche im siebenten Abschnitt behandelt wird, gehört zwar an und für sich nicht in die Arithmetik; doch müssen ihre Prinzipien einzig und allein aus der höheren Arithmetik geschöpft werden; dies wird vielleicht den Geometern ebenso überraschend sein, wie ihnen hoffentlich die neuen Wahrheiten, die man aus dieser Quelle schöpfen kann, angenehm sein werden.

Hierauf habe ich den Leser aufmerksam machen wollen. Über den Gegenstand selbst zu urteilen, ist nicht an mir. Ich wünsche nichts lebhafter, als dass sie denen, denen der Fortschritt der Wissenschaft am Herzen liegt, gefallen mögen, sei es nun, dass sie bisherige Lücken ausfüllen, sei es, dass sie den Zugang zu Neuem öffnen.

Inhaltsverzeichnis.

Arithmetische Untersuchungen.

Seite

Erster Abschnitt. Von der Congruenz der Zahlen im Allgemeinen . 1

Congruente Zahlen, Moduln, Reste und Nichtreste. Artikel 1—3. — Kleinste Reste. Artikel 4. — Elementare Sätze über die Congruenzen. Artikel 5—11. — Gewisse Anwendungen. Artikel 12.

Zweiter Abschnitt. Von den Congruenzen ersten Grades 6

Vorbereitende Sätze über Primzahlen, Factoren u. s. w. Artikel 13—25. — Auflösung der Congruenzen ersten Grades. Artikel 26—31. — Die Zahl zu finden, welche gegebenen Resten nach gegebenen Moduln congruent ist. Artikel 32—36. — Lineare Congruenzen mit mehreren Unbekannten. Artikel 37. — Verschiedene Sätze. Artikel 38—44.

Dritter Abschnitt. Von den Potenzresten 30

Die Reste der Glieder einer mit der Einheit anfangenden geometrischen Reihe bilden eine periodische Reihe. Artikel 45—48. — Es werden zunächst Moduln, welche Primzahlen sind, betrachtet. Artikel 49—81. — Ist der Modul gleich p, so ist die Anzahl der Glieder in der Periode ein Teiler der Zahl $p-1$. Artikel 49. — Der Fermat'sche Satz. — Artikel 50 u. 51. — Über die Anzahl der Zahlen, denen Perioden entsprechen, in welchen die Anzahl der Glieder ein gegebener Teiler von $p-1$ ist. Artikel 52—56. — Primitive Wurzeln, Grundzahlen, Indices. Artikel 57. — Algorithmus der Indices. Artikel 58 u. 59. — Über die Wurzeln der Congruenz $x^n \equiv A$. Artikel 60—68. — Zusammenhang zwischen den Indices in verschiedenen Systemen. Artikel 69—71. — Besonderen Zwecken dienende Grundzahlen. Artikel 72. — Methode zur Bestimmung der primitiven Wurzeln. Artikel 73 u. 74. — Verschiedene Sätze über Perioden und primitive Wurzeln. Artikel 75—81. — Über Moduln, welche Potenzen von Primzahlen sind. Artikel 82—89. — Moduln, welche Potenzen von 2 sind. Artikel 90 u. 91. — Aus mehreren Primzahlen zusammengesetzte Moduln. Artikel 92 u. 93.

Vierter Abschnitt. Von den Congruenzen zweiten Grades 65

Quadratische Reste und Nichtreste. Artikel 94 u. 95. — Sooft der Modul eine Primzahl ist, ist die Anzahl der Reste, welche kleiner als derselbe sind, gleich der Anzahl der Nichtreste. Artikel 96 u. 97. — Die Antwort auf die Frage, ob eine zusammengesetzte Zahl Rest oder Nichtrest einer

Seite

gegebenen Primzahl sei, hängt von der Natur der Factoren ab. Artikel 98 u. 99. — Über Moduln, welche zusammengesetzte Zahlen sind. Artikel 100—105. — Allgemeines Kriterium dafür, dass eine gegebene Zahl Rest oder Nichtrest einer gegebenen Primzahl ist. Artikel 106. — Untersuchungen über die Primzahlen, deren Reste oder Nichtreste gegebene Zahlen sind. Artikel 107—150. — Der Rest -1. Artikel 108—111. — Reste $+2$ und -2. Artikel 112—116. — Reste $+3$ und -3. Artikel 117—120. — Reste $+5$ und -5. Artikel 121—123. — Über ± 7. Artikel 124. — Vorbereituug auf die allgemeine Untersuchung. Artikel 125—129. — Durch Induction wird ein allgemeiner (fundamentaler) Satz begründet und daraus werden Schlüsse gezogen. Artikel 130—134. — Strenger Beweis des Fundamentalsatzes. Artikel 135—144. — Analoges Verfahren für den Beweis des Satzes im Artikel 114. Artikel 145. — Lösung des allgemeinen Problems. Artikel 146. — Über die linearen Formen, welche sämtliche Primzahlen enthalten, von denen eine beliebige gegebene Zahl Rest oder Nichtrest ist. Artikel 147—150. — Über die Arbeiten anderer bezüglich dieser Untersuchungen. Artikel 151. — Über die nichtreinen Congruenzen zweiten Grades. Artikel 152.

Fünfter Abschnitt. Von den Formen und unbestimmten Gleichungen zweiten Grades 111

Gegenstand der Untersuchung; Definition der Formen und Bezeichnung. Artikel 153. — Darstellung der Zahlen; die Determinante. Artikel 154. — Die Werte des Ausdrucks $\sqrt{b^2 - ac}$ (mod. M), zu welchen die Darstellung der Zahl M durch die Form (a, b, c) gehört. Artikel 155 u. 156. — Form, welche eine andere enthält oder unter einer anderen enthalten ist; Transformation, eigentliche und uneigentliche. Artikel 157. — Äquivalenz, eigentliche und uneigentliche. Artikel 158. — Entgegengesetzte Formen. Artikel 159. — Benachbarte Formen. Artikel 160. — Gemeinschaftliche Teiler der Coefficienten der Formen. Artikel 161. — Zusammenhang zwischen sämtlichen gleichartigen Transformationen einer gegebenen Form in eine gegebene Form. Artikel 162. — Ambige Formen. Artikel 163. — Satz betreffend den Fall, wo eine Form unter einer andern zugleich eigentlich und uneigentlich enthalten ist. Artikel 164 u. 165. — Allgemeines über die Darstellungen der Zahlen durch Formen und deren Zusammenhang mit den Transformationen. Artikel 166—170. — Über die Formen mit negativer Determinante. Artikel 171—182. — Specielle Anwendungen auf die Zerlegung der Zahlen in zwei Quadrate, in ein einfaches und ein doppeltes und in ein einfaches und ein dreifaches Quadrat. Artikel 182. — Von den Formen mit positiver nichtquadratischer Determinante. Artikel 183—205. — Von den Formen mit quadratischer Determinante. Artikel 206—212. — Formen, welche unter andern enthalten und trotzdem diesen nicht äquivalent sind. Artikel 213 u. 214. — Formen mit der Determinante 0. Artikel 215. — Allgemeine Auflösung aller unbestimmten Gleichungen zweiten Grades mit zwei Unbekannten durch ganze Zahlen. Artikel 216—221. — Geschichtliche Bemerkungen. Artikel 222. — **Weitere Untersuchungen über die Formen.** Artikel 223—265. — Einteilung der Formen mit gegebener

Seite

Determinante in Klassen. Artikel 223—225. — Einteilung der Klassen in Ordnungen. Artikel 226 u. 227. — Teilung der Ordnungen in Geschlechter. Artikel 228—233. — Von der Composition der Formen. Artikel 234—244. — Composition der Ordnungen. Artikel 245. — Composition der Geschlechter. Artikel 246—248. — Composition der Klassen. Artikel 249—251. — Für eine gegebene Determinante sind in den einzelnen Geschlechtern derselben Ordnung gleichviele Klassen enthalten. Artikel 252. — Die Anzahlen der in den einzelnen Geschlechtern verschiedener Ordnungen enthaltenen Klassen werden verglichen. Artikel 253—256. — Über die Anzahl der ambigen Klassen. Artikel 257—260. — Sicher der Hälfte aller für eine gegebene Determinante möglichen Charactere können eigentlich primitive (bei negativer Determinante, positive) Geschlechter nicht entsprechen. Artikel 261. — Zweiter Beweis des Fundamentalsatzes und der übrigen auf die Reste -1, $+2$, -2 sich beziehenden Sätze. Artikel 262. — Es wird diejenige Hälfte der Charactere, denen Geschlechter nicht entsprechen können, näher bestimmt. Artikel 263 u. 264. — Besondere Methode, Primzahlen in zwei Quadrate zu zerlegen. Artikel 265. — **Digression, enthaltend eine Untersuchung über ternäre Formen.** Artikel 266—285. — **Gewisse Anwendungen auf die Theorie der binären Formen.** Artikel 286—307. — Über die Ermittlung der Form, aus deren Duplikation eine gegebene binäre Form des Hauptgeschlechts entsteht. Artikel 286. — Allen Characteren mit Ausnahme derjenigen, welche in den Artikeln 263, 264 als unmöglich gefunden worden sind, entsprechen wirklich Geschlechter. Artikel 287. — Theorie der Zerlegung sowohl der Zahlen wie der binären Formen in drei Quadrate. Artikel 288—292. — Beweis der Fermat'schen Sätze, dass jede ganze Zahl in drei Trigonalzahlen oder in vier Quadrate zerlegt werden kann. Artikel 293. — Auflösung der Gleichung $ax^2 + by^2 + cz^2 = 0$. Artikel 294 u. 295. — Über die Methode, nach welcher Legendre das Fundamentaltheorem behandelt hat. Artikel 296—298. — Darstellung der Null durch beliebige ternäre Formen. Artikel 299. — Allgemeine Lösung der unbestimmten Gleichungen zweiten Grades mit zwei Unbekannten durch rationale Grössen. Artikel 300. — Über die mittlere Anzahl der Geschlechter. Artikel 301. — Über die mittlere Anzahl der Klassen. Artikel 302—304. — Eigentümlicher Algorithmus der eigentlich primitiven Klassen; reguläre und irreguläre Determinanten u. s. w. Artikel 305—307.

Sechster Abschnitt. Verschiedene Anwendungen der vorhergehenden Untersuchungen 364

Zerlegung der Brüche in einfachere. Artikel 309—311. — Verwandlung der gemeinen Brüche in Decimalbrüche. Artikel 312—318. — Auflösung der Congruenz $x^2 \equiv A$ durch die Methode der Ausschliessung. Artikel 319—322. — Lösung der unbestimmten Gleichung $mx^2 + ny^2 = A$ nach der Ausschliessungsmethode. Artikel 323—326. — Andere Methode, die Congruenz $x^2 \equiv A$ zu lösen für den Fall, in welchem A negativ ist. Artikel 327 u. 328. — Zwei Methoden, zusammengesetzte Zahlen von primen zu unterscheiden und ihre Factoren zu ermitteln. Artikel 329—334.

Seite

Siebenter Abschnitt. Über diejenigen Gleichungen, von denen die Teilung des Kreises abhängt 397

Die Untersuchung wird auf den einfachen Fall zurückgeführt, in welchem die Anzahl der Teile, in welche der Kreis geteilt werden soll, eine Primzahl ist. Artikel 336. — Gleichungen für die trigonometrischen Functionen der Bogen, welche ein Teil oder Teile der ganzen Peripherie sind; Reduction der trigonometrischen Functionen auf die Wurzeln der Gleichung $x^n - 1 = 0$. Artikel 337 u. 338. — Theorie der Wurzeln der Gleichung $x^n - 1 = 0$ (wo vorausgesetzt wird, dass n eine Primzahl sei). Lässt man die Wurzel 1 weg, so sind die übrigen (Ω) enthalten in der Gleichung $X = x^{n-1} + x^{n-2} + \cdots + x + 1 = 0$. Artikel 339 u. 340. — Die Function X lässt sich nicht in niedrigere Factoren zerlegen, in denen sämtliche Coefficienten rational sind. Artikel 341. — Das Ziel der folgenden Untersuchungen wird angegeben. Artikel 342. — Sämtliche Wurzeln Ω werden in gewisse Klassen (Perioden) eingeteilt. Artikel 343. — Verschiedene Sätze über die Perioden der Wurzeln Ω. Artikel 344—351. — Auf die vorstehenden Untersuchungen wird die Lösung der Gleichung $X = 0$ gegründet. Artikel 352—354. — Weitere Untersuchungen über die Perioden der Wurzeln. Die Aggregate, in denen die Anzahl der Glieder gerade ist, sind reelle Grössen. Artikel 355. — Über die Gleichung, durch welche die Verteilung der Wurzeln Ω in zwei Perioden bestimmt wird. Artikel 356. — Beweis eines im vierten Abschnitt erwähnten Satzes. Artikel 357. — Über die Gleichung für die Verteilung der Wurzeln Ω in drei Perioden. Artikel 358. — Zurückführung der Gleichungen, durch welche die Wurzeln Ω gefunden werden, auf reine Gleichungen. Artikel 359 u. 360. — Anwendung der vorstehenden Untersuchungen auf die trigonometrischen Functionen. Methode, die Winkel, welchen die einzelnen Wurzeln entsprechen, zu unterscheiden. Artikel 361. — Die Tangenten, Cotangenten, Sekanten und Cosekanten werden aus den Sinus und Cosinus ohne Division bestimmt. Artikel 362. — Methode, die Gleichungen für die trigonometrischen Functionen allmählig zu erniedrigen. Artikel 363 u. 364. — Die Teilungen des Kreises, welche man mittelst quadratischer Gleichungen oder durch geometrische Constructionen ausführen kann. Artikel 365 u. 366.

Zusätze 449

Tafeln 451

Abhandlungen.

Neuer Beweis eines arithmetischen Satzes 457

Summierung gewisser Reihen von besonderer Art 463

Neue Beweise und Erweiterungen des Fundamentalsatzes in der Lehre von den quadratischen Resten 496

Theorie der biquadratischen Reste. Erste Abhandlung 511

Theorie der biquadratischen Reste. Zweite Abhandlung 534

Einige Untersuchungen aus dem handschriftlichen Nachlasse von Gauss.

Seite

Die Lehre von den Resten 589

I. Lösung der Congruenz $X^m - 1 \equiv 0$ 589

II. Allgemeine Untersuchungen über die Congruenzen 602

Weitere Entwicklung der Untersuchungen über die reinen Gleichungen 630

Beweis einiger Sätze über die Perioden der Klassen der binären Formen zweiten Grades 653

Über den Zusammenhang zwischen der Anzahl der Klassen, in welche die binären Formen zweiten Grades zerfallen, und ihrer Determinante 655

Eingehendere Betrachtung gewisser auf die Kreisteilung bezüglicher Untersuchungen 678

Bemerkungen 683

Arithmetische Untersuchungen.

Erster Abschnitt.

Von der Congruenz der Zahlen im Allgemeinen.

Congruente Zahlen, Moduln, Reste und Nichtreste.

1.

Wenn die Zahl a in der Differenz der Zahlen b, c aufgeht, so werden b und c nach a **congruent**, im andern Falle **incongruent** genannt. Die Zahl a nennen wir den **Modul**. Jede der beiden Zahlen b, c heisst im ersteren Falle **Rest**, im letzteren aber **Nichtrest** der andern.

Diese Bezeichnungen gelten in Bezug auf alle **ganzen**, positiven sowohl wie negativen*), Zahlen, sie sind aber nicht auf gebrochene Zahlen auszudehnen. So sind z. B. -9 und $+16$ nach dem Modul 5 congruent; -7 ist nach dem Modul 11 Rest, nach dem Modul 3 aber Nichtrest von $+15$. Da übrigens die Null durch jede beliebige Zahl geteilt wird, so ist jede Zahl als nach jedem beliebigen Modul sich selbst congruent zu betrachten.

2.

Sämtliche Reste einer gegebenen Zahl a nach dem Modul m sind in der Formel $a + km$ enthalten, wo k eine unbestimmte ganze Zahl bezeichnet. Von den Sätzen, die wir später aufstellen werden, lassen sich die leichteren hieraus ohne Mühe beweisen; doch wird jeder die Richtigkeit derselben ebenso leicht durch den blossen Anblick erkennen können.

Die Congruenz der Zahlen werden wir im Folgenden durch das Zeichen $\equiv$ andeuten und den Modul da, wo es nötig sein wird, in Klammern hinzufügen: $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$.**)

*) Der Modul ist offenbar stets absolut, d. h. ohne jedes Vorzeichen, zu nehmen.

**) Dieses Zeichen habe ich wegen der grossen Analogie, die zwischen der Gleichheit und der Congruenz stattfindet, gewählt. Aus demselben Grunde hat Legendre in seinem unten öfter zu erwähnenden Werke geradezu das Gleichheitszeichen für die Congruenz beibehalten; doch habe ich Bedenken getragen, ihm darin zu folgen, um keine Zweideutigkeit entstehen zu lassen.

3.

Satz. Sind m aufeinanderfolgende ganze Zahlen

$$a,\ a+1,\ a+2,\ \ldots,\ a+m-1$$

und eine andere A gegeben, so wird eine und nur eine von jenen dieser letzteren nach dem Modul m congruent sein.

Ist nämlich $\frac{a-A}{m}$ eine ganze Zahl, so ist $a \equiv A$; ist es aber eine gebrochene Zahl, so sei die nächstgrössere ganze Zahl (oder wenn der Bruch negativ ist, die nächstkleinere, ohne Rücksicht auf das Vorzeichen) gleich k; dann wird $A+km$ zwischen a und $a+m$ liegen und daher die gesuchte Zahl sein. Offenbar aber liegen die Quotienten

$$\frac{a-A}{m},\ \frac{a+1-A}{m},\ \frac{a+2-A}{m},\ \ldots$$

sämtlich zwischen $k-1$ und $k+1$; daher kann nicht mehr als einer von ihnen eine ganze Zahl sein.

Kleinste Reste.

4.

Es wird demnach jede Zahl sowohl in der Reihe $0, 1, 2, \ldots, m-1$ wie in der Reihe $0, -1, -2, \ldots, -(m-1)$ einen Rest besitzen und zwar werden wir diese die **kleinsten Reste** nennen. Offenbar giebt es, falls nicht 0 der Rest ist, stets zwei solche, einen positiven und einen negativen. Sind dieselben der Grösse nach ungleich, so ist der eine kleiner als $\frac{m}{2}$, im andern Falle beide gleich $\frac{m}{2}$, abgesehen vom Vorzeichen. Hieraus geht hervor, dass eine jede Zahl einen Rest besitzt, der die Hälfte des Moduls nicht übersteigt und der **absolut kleinste Rest** genannt wird.

Die Zahl -13 besitzt z. B. nach dem Modul 5 den kleinsten positiven Rest 2, der zugleich der absolut kleinste Rest ist, dagegen den kleinsten negativen Rest -3. Die Zahl $+5$ ist nach dem Modul 7 ihr eigener kleinster positiver Rest, -2 dagegen der kleinste negative und zugleich absolut kleinste Rest derselben.

Elementare Sätze über die Congruenzen.

5.

Nachdem wir diese Bezeichnungen festgestellt haben, wollen wir diejenigen Eigenschaften congruenter Zahlen, die sich auf den ersten Blick darbieten, zusammenstellen.

Diejenigen Zahlen, welche nach einem zusammengesetzten Modul congruent sind, sind auch nach jedem Teiler desselben congruent.

Wenn mehrere Zahlen einer und derselben Zahl nach einem und demselben Modul congruent sind, so sind sie (nach demselben Modul) unter einander congruent.

Auch in den folgenden Sätzen wird vorausgesetzt, dass der Modul derselbe bleibt.

Congruente Zahlen haben dieselben, incongruente aber verschiedene kleinste Reste.

6.

Hat man beliebig viele Zahlen $A, B, C, \ldots$ und ebenso viele andere $a, b, c, \ldots$, welche jenen nach irgend welchem Modul congruent sind, also

$$A \equiv a,\ B \equiv b,\ \ldots,$$

so ist:

$$A + B + C + \cdots \equiv a + b + c + \cdots$$

Ist $A \equiv a,\ B \equiv b$, so ist: $A - B \equiv a - b$.

7.

Ist $A \equiv a$, so ist auch $kA \equiv ka$.

Ist k eine positive Zahl, so ist dieses nur ein besonderer Fall des Satzes im vorhergehenden Artikel, der entsteht, wenn man daselbst $A = B = C = \cdots$ und $a = b = c = \cdots$ setzt. Ist k negativ, so wird $-k$ positiv, daher $-kA \equiv -ka$ und hieraus $kA \equiv ka$.

Ist $A \equiv a,\ B \equiv b$, so ist auch $AB \equiv ab$.

Denn es ist $AB \equiv Ab \equiv ba$.

8.

Hat man beliebig viele Zahlen $A, B, C, \ldots$ und ebenso viele andere $a, b, c, \ldots$, welche jenen congruent sind, also $A \equiv a$, $B \equiv b, \ldots$, so sind auch die Producte aus den Zahlen jeder Reihe congruent, also $ABC\ldots \equiv abc\ldots$

Nach dem vorhergehenden Artikel ist $AB \equiv ab$ und aus demselben Grunde $ABC \equiv abc$; auf dieselbe Weise können beliebig viele andere Factoren hinzutreten.

Wenn alle Zahlen $A, B, C, \ldots$ gleich angenommen werden, ebenso die entsprechenden $a, b, c, \ldots$, so erhält man den **Satz:**

Ist $A \equiv a$ und k eine ganze positive Zahl, so ist $A^k \equiv a^k$.

9.

Es sei X eine algebraische Function der unbestimmten Grösse x von der Form:

$$Ax^a + Bx^b + Cx^c + \cdots,$$

wo $A, B, C, \ldots$ irgend welche ganze Zahlen, $a, b, c, \ldots$ aber ganze nicht negative Zahlen bezeichnen. Wenn alsdann der

Unbestimmten x Werte beigelegt werden, die nach einem beliebigen Modul congruent sind, so werden auch die daraus sich ergebenden Werte der Function X einander congruent sein.

Es seien f, g einander congruente Werte von x. Dann ergiebt sich aus dem vorhergehenden Artikel:

$$f^a \equiv g^a \text{ und } Af^a \equiv Ag^a; \text{ ebenso } Bf^b \equiv Bg^b \text{ u. s. w. Daher:}$$

$$Af^a + Bf^b + Cf^c + \cdots \equiv Ag^a + Bg^b + Cg^c + \cdots, \text{ w. z. b. w.}$$

Uebrigens sieht man leicht, wie sich dieser Satz auf Functionen von mehreren Unbestimmten ausdehnen lässt.

10.

Wenn demnach für x alle aufeinander folgenden ganzen Zahlen gesetzt und die Werte der Function X auf ihre kleinsten Reste gebracht werden, so werden diese eine Reihe bilden, in welcher nach einem Intervall von m Gliedern (wo m den Modul bezeichnet) immer dieselben Glieder wiederkehren, oder diese Reihe wird aus einer unendlichvielmal wiederholten **Periode** von m Gliedern gebildet sein. Ist z. B. $X = x^3 - 8x + 6$ und $m = 5$, so werden für $x = 0, 1, 2, 3 \ldots$ die Werte von X die folgenden kleinsten positiven Reste ergeben: 1, 4, 3, 4, 3, 1, 4, wo die fünf ersten 1, 4, 3, 4, 3 sich bis ins Unendliche hin wiederholen; und wenn die Reihe rückwärts fortgesetzt wird, d. h. wenn x negative Werte gegeben werden, so geht dieselbe Periode in umgekehrter Reihenfolge der Glieder hervor. Daraus ist offenbar, dass andere Glieder als die, welche diese Periode bilden, in der ganzen Reihe nicht statthaben können.

11.

In diesem Beispiel kann demnach X weder $\equiv 0$ noch $\equiv 2$ (mod. 5) und noch viel weniger $= 0$ oder $= 2$ werden. Daraus folgt, dass die Gleichungen $x^3 - 8x + 6 = 0$ und $x^3 - 8x + 4 = 0$ durch ganze Zahlen und infolge dessen, wie bekannt, durch rationale Zahlen nicht aufgelöst werden können. Allgemein ist ersichtlich, dass die Gleichung $X = 0$, wenn die Function X der Unbekannten x die Form

$$x^n + Ax^{n-1} + Bx^{n-2} + \cdots + N$$

hat, wo $A, B, C, \ldots$ ganze Zahlen sind und n eine ganze positive Zahl ist (auf welche Form bekanntlich alle algebraischen Gleichungen zurückgeführt werden können), keine rationale Wurzel hat, wenn man nicht der Congruenz $X \equiv 0$ nach irgend einem Modul Genüge leisten kann. Dieses Kriterium, welches sich uns hier unmittelbar darbot, soll im achten Abschnitt*) ausführlicher behandelt werden. Sicherlich wird man sich schon aus dieser Probe einen kleinen Begriff von dem Nutzen dieser Untersuchungen bilden können.

*) Vgl. das Vorwort des Herausgebers.

Gewisse Anwendungen.

12.

Auf die in diesem Kapitel angeführten Sätze gründet sich mehreres, was in der Arithmetik gelehrt zu werden pflegt, z. B. die Regeln zur Untersuchung der Teilbarkeit einer gegebenen Zahl durch 9, 11 oder durch andere Zahlen. Nach dem Modul 9 sind alle Zahlen, welche Potenzen von 10 sind, der Einheit congruent. Hat daher die gegebene Zahl die Form $a + 10b + 100c + \cdots$, so wird dieselbe denselben kleinsten Rest nach dem Modul 9 geben wie $a + b + c + \cdots$ Hieraus ist ersichtlich, dass, wenn die einzelnen Ziffern der dekadisch ausgedrückten Zahl ohne Rücksicht auf die Stelle, welche sie einnehmen, addirt werden, diese Summe und die gegebene Zahl dieselben kleinsten Reste darbieten und daher diese durch 9 geteilt werden kann, wenn jene durch 9 teilbar ist, und umgekehrt. Dasselbe gilt vom Teiler 3. Da ferner, nach dem Modul 11, $100 \equiv 1$ ist, so ist allgemein $10^{2k} \equiv 1$, $10^{2k+1} \equiv 10 \equiv -1$, und die Zahl von der Form $a + 10b + 100c + \cdots$ wird nach dem Modul 11 denselben kleinsten Rest geben wie $a - b + c - \cdots$, woraus sich sofort die bekannte Regel ergiebt. Aus demselben Prinzip lassen sich leicht alle ähnlichen Vorschriften ableiten.

Ebenso ist in dem Vorhergehenden der Grund für die Regeln zu suchen, welche man gewöhnlich zur Prüfung der Richtigkeit arithmetischer Rechnungen empfiehlt. Wenn nämlich aus gegebenen Zahlen andere durch Addition, Subtraction, Multiplikation oder Potenzerhebung abzuleiten sind, so werden an Stelle der gegebenen Zahlen die kleinsten Reste derselben nach einem willkürlichen Modul (gewöhnlich 9 oder 11, da sich in unserm dekadischen Systeme die Reste nach diesen, wie wir soeben gezeigt haben, so leicht finden lassen) gesetzt. Die aus diesen entstehenden Zahlen müssen denen, welche aus den gegebenen Zahlen abgeleitet worden waren, congruent sein. Ist dieses nicht der Fall, so folgt, dass sich ein Fehler in die Rechnung eingeschlichen habe.

Da jedoch dies und Ähnliches hinlänglich bekannt ist, so dürfte es überflüssig sein, länger dabei zu verweilen.

Zweiter Abschnitt.

Von den Congruenzen ersten Grades.

Vorbereitende Sätze über Primzahlen, Factoren u. s. w.

13.

Satz. Das Product aus zwei positiven Zahlen, welche kleiner als eine gegebene Primzahl sind, lässt sich nicht durch diese Primzahl teilen.

Es sei p eine Primzahl und a eine positive Zahl $< p$; dann wird behauptet, dass es keine positive Zahl $b < p$ von der Beschaffenheit giebt, dass $ab \equiv 0 \pmod{p}$ ist.

Beweis. Angenommen, es gäbe Zahlen $b, c, d, \ldots$, die sämtlich kleiner als p und von der Beschaffenheit sind, dass $ab \equiv 0$, $ac \equiv 0$, $ad \equiv 0, \ldots$, (mod. p) ist. Von allen diesen sei b die kleinste, so dass keine der Zahlen, die kleiner als b sind, jene Eigenschaft besitzt. Dann ist offenbar $b > 1$. Denn wäre $b = 1$, so würde $ab = a < p$ (nach Voraussetzung), also nicht durch p teilbar sein. Mithin lässt sich p, da es eine Primzahl ist, nicht durch b teilen, sondern wird zwischen zwei aufeinanderfolgende Vielfache von b, etwa zwischen mb und $(m+1)b$, fallen. Ist $p - mb = b'$, so wird b' eine positive Zahl und kleiner als b sein. Da nun nach unserer Annahme $ab \equiv 0 \pmod{p}$ ist, so hat man auch $mab \equiv 0$ (nach Artikel 7) und somit, wenn man dies von $ap \equiv 0$ subtrahiert: $a(p - mb) = ab' \equiv 0$, d. h. b' müsste zur Reihe der Zahlen $b, c, d, \ldots$ gerechnet werden, obwohl es kleiner als die kleinste b dieser Zahlen ist. Dies widerspricht aber unserer Annahme.

14.

Wenn weder a noch b durch die Primzahl p sich teilen lässt, so ist auch das Product ab durch p nicht teilbar.

Die kleinsten positiven Reste der Zahlen a, b nach dem Modul p seien α, β, von denen (nach Voraussetzung) keiner gleich 0 ist. Wäre nun $ab \equiv 0 \pmod{p}$, so würde auch, da $ab \equiv \alpha\beta$ ist, $\alpha\beta \equiv 0$ sein, was mit dem vorhergehenden Satze nicht verträglich ist.

Der Beweis dieses Satzes ist bereits von Euclid, *Elem. VII, 32,* gegeben worden. Wir haben ihn jedoch nicht weglassen wollen, einmal weil von den Neueren einige entweder nur nichtige Gründe für einen Beweis des Satzes ausgegeben oder ihn ganz und gar übergangen haben, sodann weil sich das Wesen der hier angewendeten Methode, deren wir uns später zur Aufsuchung viel versteckter liegender Wahrheiten bedienen werden, an einem einfacheren Beispiele leichter verstehen lässt.

15.

Wenn keine der Zahlen $a, b, c, d, \ldots$ durch die Primzahl p sich teilen lässt, so ist auch das Product $abcd \ldots$ durch p nicht teilbar.

Nach dem vorigen Artikel ist ab durch p nicht teilbar; daher auch nicht abc, daher auch nicht $abcd$ u. s. w.

16.

Satz. Jede zusammengesetzte Zahl lässt sich nur auf eine einzige Weise in Primfactoren zerlegen.

Beweis. Dass jede zusammengesetzte Zahl in Primfactoren zerlegt werden kann, ist aus den Anfangsgründen bekannt; dass dies aber nicht auf mehrere verschiedene Arten geschehen könne, wird mit Unrecht meistenteils stillschweigend angenommen. Denken wir uns, dass die zusammengesetzte Zahl A, welche gleich $a^\alpha b^\beta c^\gamma \ldots$ sei, wo $a, b, c, \ldots$ ungleiche Primzahlen bezeichnen, noch auf eine andere Weise in Primfactoren zerlegbar sei, so ist zunächst klar, dass in diesem zweiten System von Factoren andere Primzahlen als $a, b, c, \ldots$ nicht vorkommen können, da die aus letzteren zusammengesetzte Zahl A sich durch keine andere Primzahl teilen lässt. Andererseits darf aber auch in diesem zweiten System von Factoren keine der Primzahlen $a, b, c, \ldots$ fehlen, da sie ja sonst die Zahl A (nach vorigem Artikel) nicht teilen würde. Daher können sich diese beiden Zerlegungen in Factoren nur insoweit unterscheiden, dass in der einen irgend eine Primzahl öfter enthalten ist als in der andern. Es sei p eine solche Primzahl, welche in der einen Zerlegung m-mal, in der andern aber n-mal vorkommt, und es sei $m > n$. Hebt man dann den Factor p aus jedem der beiden Systeme n-mal weg, so wird er in dem einen noch $(m-n)$-mal übrig bleiben, in dem andern aber gar nicht mehr vorkommen, d. h. man erhält für die Zahl $\frac{A}{p^n}$ zwei Zerlegungen in Factoren, deren eine vom Factor p vollständig frei ist, während die andere ihn $(m-n)$-mal enthält. Dies steht aber im Widerspruch mit dem, was wir soeben bewiesen haben.

17.

Wenn daher die zusammengesetzte Zahl A das Product aus den Zahlen $B, C, D, \ldots$ ist, so ist klar, dass unter den Primfactoren der Zahlen $B, C, D, \ldots$ keine andern vorkommen können, als die, welche auch in