

Carl Friedrich Gauss‘

Untersuchungen über höhere Arithmetik.

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

Deutsch herausgegeben

von

H. Maser.

ehemals Julius Springer Verlag 1889

Reprint der Ausgabe von 1889

Verlag Kessel, Eifelweg 37, 53424 Remagen-Oberwinter

Tel.: 02228-493, Fax: 01212-512382426, E-Mail: nkessel@web.de

www.verlagkessel.de

< vorläufige Fassung >

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 mitgetheilten 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. mitgetheilten 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 Übersetzung 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 meistens, 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 charakteristischen 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 theils vor theils nach jener Zeit angestellt habe, zur allgemeineren Kenntniss 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 Kenntniss 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 Überlegungen 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 Akademien 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.

Inhalt

Arithmetische Untersuchungen XV

Erster Abschnitt.

Von der Congruenz der Zahlen im Allgemeinen.

Congruente Zahlen, Moduln, Reste und Nichtreste	1
Kleinste Reste	2
Elementare Sätze über die Congruenzen	2
Gewisse Anwendungen	5

Zweiter Abschnitt.

Von den Congruenzen ersten Grades.

Vorbereitende Sätze über Primzahlen, Factoren u. s. w.	6
Auflösung der Congruenzen ersten Grades	11
Die Zahl zu finden, welche gegebenen Resten nach gegebenen Moduln congruent ist	15
Lineare Congruenzen mit mehreren Unbekannten	19
Verschiedene Sätze	22

Dritter Abschnitt.

Von den Potenzresten.

Die Reste der Glieder einer mit der Einheit anfangenden geometrischen Reihe bilden eine periodische Reihe	30
Es werden zunächst Moduln, welche Primzahlen sind, betrachtet	31
Der Fermat'sche Satz	33
Über die Anzahl der Zahlen, denen Perioden entsprechen, in welchen die Anzahl der Glieder ein gegebener Teiler von $p - 1$ ist	34
Primitive Wurzeln, Grundzahlen, Indices	38
Algorithmus der Indices	39
Über die Wurzeln der Congruenz $x^n \equiv A$	40
Zusammenhang zwischen den Indices in verschiedenen Systemen	48
Besonderen Zwecken dienende Grundzahlen	50
Methode zur Bestimmung der primitiven Wurzeln	51
Verschiedene Sätze über Perioden und primitive Wurzeln	53
Über Moduln, welche Potenzen von Primzahlen sind	57
Moduln, welche Potenzen von 2 sind	62
Aus mehreren Primzahlen zusammengesetzte Moduln	63

Arithmetische Untersuchungen

—x—

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

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

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

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

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 $0, 1, 2, \dots, m - 1$ wie in der Reihe $0, -1, -2, -(m - 1)$ einen Rest besitzen und zwar werden wir diese die **kleinsten Reste** nennen. Offenbar gibt 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, \dots und ebenso viele andere a, b, c, \dots , welche jenen nach irgend welchem Modul congruent sind, also

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

so ist:

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

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

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, \dots gleich angenommen werden, ebenso die entsprechenden a, b, c, \dots , 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:

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

wo A, B, C, \dots irgend welche ganze Zahlen, a, b, c, \dots 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 ergibt sich aus dem vorhergehenden Artikel:

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

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

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 $x = 0, 1, 2, 3 \dots$ 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 $\equiv 2 \pmod{5}$ und noch viel weniger $\equiv 0$ oder $\equiv 2$ 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

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

hat, wo A, B, C, \dots 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 darbietet, 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 $a + 10b + 100c + \dots$, so wird dieselbe denselben kleinsten Rest nach dem Modul 9 geben wie $a + b + c + \dots$. 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 $a + 10b + 100c + \dots$ wird nach dem Modul 11 denselben kleinsten Rest geben wie $a - b + c - \dots$, woraus sich sofort die bekannte Regel ergibt. 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 Potenserhebung 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, \dots , die sämtlich kleiner als p und von der Beschaffenheit sind, dass $ab \equiv 0, ac \equiv 0, ad \equiv 0, \dots \pmod{p}$ 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: $a(p - mb) = ab'$. 0, d. h. b' müsste zur Reihe der Zahlen b, c, d, \dots 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, \dots durch die Primzahl p sich teilen lässt, so ist auch das Product $abcd \dots$ 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, meistens stillschweigend angenommen. Denken wir uns, dass die zusammengesetzte Zahl A , welche gleich $a^\alpha b^\beta c^\gamma \dots$ sei, wo a, b, c, \dots 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, \dots 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, \dots 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, \dots ist, so ist klar, dass unter den Primfactoren der Zahlen B, C, D, \dots keine andern vorkommen können, als die, welche auch in

den Factoren der Zahl A auftreten, und dass jeder dieser Primfactoren in B, C, D, \dots zusammen ebenso oft vorkommen muss wie in A . Hieraus ergibt sich ein Kriterium, nach welchem man entscheiden kann, ob eine Zahl B eine andere A teilt oder nicht. Jenes ist der Fall, wenn B weder andere Primfactoren, noch irgend einen öfter enthält als A . Ist irgend eine dieser Bedingungen nicht erfüllt, so ist B kein Teiler von A .

Hieraus kann man mit Hülfe der Combinationsrechnung leicht ableiten, dass, wenn

$$A = a^\alpha b^\beta c^\gamma \dots$$

ist, wo a, b, c, \dots wie oben verschiedene Primzahlen bezeichnen, die Anzahl der verschiedenen Teiler von A mit Einschluss von 1 und A gleich

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \dots$$

ist.

18.

Ist daher $A = a^\alpha b^\beta c^\gamma \dots$, $K = k^\lambda l^\mu m^\nu \dots$, und sind die Primzahlen $a, b, c, \dots, k, l, m, \dots$ sämtlich von einander verschieden, so haben offenbar A und K keinen gemeinschaftlichen Teiler ausser 1, oder sie sind zu einander prim.

Das mehreren gegebenen Zahlen A, B, C, \dots **gemeinschaftliche grösste Mass** bestimmt man folgendermassen: Man zerlege alle jene Zahlen in ihre Primfactoren und suche von diesen diejenigen heraus, welche allen Zahlen A, B, C, \dots gemeinschaftlich sind (gibt es keine solchen, so gibt es auch keinen allen gemeinschaftlichen Teiler). Sodann merke man sich, wie oft ein jeder dieser Primfactoren in den einzelnen Zahlen A, B, C, \dots enthalten ist, oder wie viel Dimensionen ein jeder in den einzelnen Zahlen A, B, C, \dots hat. Endlich gebe man jedem einzelnen Primfactor die kleinste von allen Dimensionen, welche er in A, B, C, \dots hat, und bilde aus den so erhaltenen Potenzen ein Product; dieses wird dann das gesuchte gemeinschaftliche Mass sein.

Wenn man aber das kleinste gemeinschaftliche Vielfache der Zahlen A, B, C, \dots haben will, so muss man folgendermassen verfahren. Man sammle alle Primzahlen, welche irgend eine der Zahlen A, B, C, \dots teilen, gebe jeder einzelnen die grösste von allen Dimensionen, welche sie in den Zahlen A, B, C, \dots hat, und bilde aus allen so erhaltenen Potenzen ein Product; dieses wird dann das gesuchte gemeinschaftliche Vielfache sein.

Beispiel. Es sei $A = 504 = 2^3 \cdot 3^2 \cdot 7$, $B = 2880 = 2^6 \cdot 3^2 \cdot 5$, $C = 864 = 2^5 \cdot 3^3$. Um den grössten gemeinschaftlichen Teiler zu finden, hat man die Primfactoren 2, 3, denen die Dimensionen 3, 2 zu geben sind, so dass derselbe gleich $2^3 \cdot 3^2 = 72$ wird. Das kleinste gemeinschaftliche Vielfache dagegen ist: $2^6 \cdot 3^3 \cdot 5 \cdot 7 = 60480$.

Die Beweise lassen wir ihrer Leichtigkeit wegen fort. Wie übrigens diese Aufgaben zu lösen sind, wenn die Zerlegung der Zahlen A, B, C, \dots in Factoren nicht gegeben ist, ist aus den Elementen bekannt.

19.

Wenn die Zahlen a, b, c, \dots zu einer andern k prim sind, so ist auch das Product aus jenen $abc \dots$ prim zu k .

Denn da keine der Zahlen a, b, c, \dots mit k einen Primfactor gemeinschaftlich hat und das Product $abc \dots$ nur die Primfactoren haben kann, welche Factoren irgend einer der Zahlen a, b, c, \dots sind, so hat auch das Product $abc \dots$ mit k keinen Primfactor gemeinschaftlich. Daher sind k und $abc \dots$ nach dem vorhergehenden Artikel prim zu einander.

Wenn die Zahlen a, b, c, \dots prim zu einander sind und einzeln eine andere Zahl k teilen, so ist auch das Product aus jenen ein Teiler der Zahl k .

Dies ergibt sich ebenso leicht aus den Artikeln 17 und 18. Denn ist p ein beliebiger Primteiler des Productes $abc \dots$, und ist derselbe π -mal darin enthalten, so muss offenbar irgend eine der Zahlen a, b, c, \dots denselben Teiler ebenfalls π -mal enthalten. Daher enthält auch k , welches durch jene Zahl geteilt wird, π -mal den Teiler p . Analoges gilt von den übrigen Teilern des Productes $abc \dots$.

Wenn daher zwei Zahlen m, n nach mehreren zu einander primen Moduln a, b, c, \dots congruent sind, so werden sie auch nach dem Producte aus diesen einander congruent sein.

Denn da $m-n$ durch jede einzelne der Zahlen a, b, c, \dots teilbar ist, so ist es auch durch das Product derselben teilbar.

Wenn endlich a zu b prim und ak durch b teilbar ist, so wird auch k durch b teilbar sein.

Denn da ak sowohl durch a als auch durch b teilbar ist, so ist es auch durch das Product ab teilbar, d. h. es ist $\frac{ak}{ab} = \frac{k}{b}$ eine ganze Zahl.

20.

Sobald die Zahl $A = a^\alpha b^\beta c^\gamma \dots$, wo a, b, c, \dots einander ungleiche Primzahlen bezeichnen, irgend eine Potenz ist, etwa $A = k^n$, so werden sämtliche Exponenten $\alpha, \beta, \gamma, \dots$ durch n teilbar sein.

Denn die Zahl k enthält keine andern Primfactoren als a, b, c, \dots , und zwar enthält sie alle diese. Kommt der Factor a darin α' -mal vor, so wird dieser Factor in k^n oder $A n\alpha'$ -mal vorkommen. Daher ist $n\alpha' = \alpha$ und $\frac{\alpha}{n}$ eine ganze Zahl. Ebenso beweist man, dass $\frac{\beta}{n}, \dots$ ganze Zahlen sind.

21.

Wenn a, b, c, \dots prim zu einander sind, und das Product $abc \dots$ irgend eine Potenz, etwa $abc \dots = k^n$, ist, so werden die einzelnen Zahlen a, b, c, \dots gleichfalls Potenzen sein.

Es sei $a = l^l m^m p^p \dots$, wo l, m, p, \dots von einander verschiedene Prim-

zahlen bezeichnen, von denen nach Voraussetzung keine ein Factor der Zahlen b, c, \dots ist. Daher wird das Product $abc \dots$ den Factor l λ -mal, den Factor m μ -mal u. s. w. enthalten. Somit sind (nach vorigem Artikel) λ, μ, π, \dots durch n teilbar, und daher ist

$$\sqrt[n]{a} = l^{\frac{\lambda}{n}} m^{\frac{\mu}{n}} p^{\frac{\pi}{n}}$$

eine ganze Zahl. Dasselbe gilt bezüglich der Zahlen b, c, \dots

Diese Sätze über die Primzahlen mussten wir zuerst vorausschicken. Jetzt wenden wir uns zu denen, die zu unserem Ziele in näherer Beziehung stehen.

22.

Wenn die Zahlen a, b durch eine andere k teilbar und nach dem zu k primen Modul m einander congruent sind, so sind auch $\frac{a}{k}$ und $\frac{b}{k}$ nach demselben Modul einander congruent.

Denn offenbar ist $a-b$ durch k und, nach Voraussetzung, auch durch m teilbar; daher ist (nach Artikel 19) $\frac{a-b}{k}$ durch m teilbar, d. h. es ist $\frac{a}{k} \equiv \frac{b}{k} \pmod{m}$.

Wenn aber, unter sonst gleichen Voraussetzungen, m und k den grössten gemeinschaftlichen Teiler e haben, so ist $\frac{a}{k} - \frac{b}{k} \pmod{\frac{m}{e}}$.

Denn $\frac{k}{e}$ und $\frac{m}{e}$ sind prim zu einander. Da, aber $a-b$ sowohl durch k als durch m

und daher auch $\frac{a-b}{e}$ sowohl durch $\frac{k}{e}$ als auch durch $\frac{m}{e}$ und somit durch $\frac{km}{e^2}$ teilbar

ist, so ist auch $\frac{a-b}{k}$ durch $\frac{m}{e}$ teilbar, oder $\frac{a}{k} \equiv \frac{b}{k} \pmod{\frac{m}{e}}$.

23.

Wenn a prim zu m ist, und e, f nach dem Modul m incongruente Zahlen sind, so werden auch ae und af nach dem Modul m incongruent sein.

Dieser Satz ist nur eine Umkehrung des Satzes im vorhergehenden Artikel.

Hieraus aber geht hervor, dass, wenn a mit sämtlichen ganzen Zahlen von 0 bis $m-1$ multipliciert wird und die Producte nach dem Modul m auf ihre kleinsten Reste gebracht werden, diese letzteren sämtlich von einander verschieden sind. Und da die Anzahl dieser Reste, von denen keiner grösser als m ist, gleich m ist, und es ebenso viele Zahlen von 0

bis $m-1$ giebt, so folgt, dass keine dieser Zahlen unter jenen Resten fehlen kann.

24.

Der Ausdruck $ax+b$, in welchem a, b gegebene Zahlen und x eine unbestimmte oder veränderliche Zahl bezeichnet, kann nach dem zu a primen Modul m jeder beliebigen gegebenen Zahl congruent werden.

Die Zahl, welcher jener Ausdruck congruent werden soll, sei c und der kleinste positive Rest von $c-b$ nach dem Modul m sei e . Dann giebt es nach dem vorhergehenden Artikel notwendig einen Wert von $x < m$ von solcher Beschaffenheit, dass der kleinste Rest des Products ax nach dem Modul m gleich e ist. Ist v dieser Wert, so hat man $av \equiv e \equiv c-b$, mithin $av + b \equiv c \pmod{m}$.

25.

Den Ausdruck, welcher zwei congruente Grössen nach Analogie einer Gleichung mit einander verbindet, nennen wir eine **Congruenz**. Enthält dieselbe eine Unbekannte, so heisst die Congruenz gelöst, wenn man für diese Unbekannte einen der Congruenz genügenden Wert (**Wurzel**) findet. Hieraus erkennt man ferner, was eine auflösbare und eine nicht auflösbare Congruenz ist. Endlich sieht man leicht, dass hier ähnliche Unterscheidungen stattfinden können, wie bei den Gleichungen. Von transcendenten Congruenzen werden weiter unten Beispiele vorkommen; die algebraischen aber werden je nach der höchsten in ihnen enthaltenen Potenz der Unbekannten in Congruenzen ersten, zweiten und höheren Grades eingeteilt. Ebenso können auch mehrere Congruenzen mit mehreren Unbekannten, über deren Elimination das Nähere mitzuteilen sein wird, gegeben sein.

Auflösung der Congruenzen ersten Grades.

26.

Die Congruenz ersten Grades $ax + b \equiv c$ ist nach Artikel 24 stets auflösbar, wenn der Modul zu a prim ist. Ist v ein passender Wert von x oder eine Wurzel der Congruenz, so werden offenbar alle Zahlen, welche v nach dem Modul der gegebenen Congruenz congruent sind, auch Wurzeln sein (Artikel 9). Ebenso leicht sieht man, dass alle Wurzeln v congruent sein müssen; denn ist t eine andere Wurzel, so ist $av + b \equiv at + b$, daher $av \equiv at$ und somit $v \equiv t$ (Artikel 22). Hieraus folgt, dass die Congruenz $x \equiv v \pmod{m}$ die vollständige Lösung der Congruenz $ax + b \equiv c$ darstellt.

Da die Lösungen der Congruenz durch Werte, welche x congruent sind, auf der Hand liegen und in dieser Hinsicht congruente Zahlen als äquivalent zu betrachten sind, so werden wir derartige Lösungen der Congruenz für eine und dieselbe halten. Wenn daher unsere Congruenz $ax + b \equiv c$ andere Lösungen nicht zulässt, so werden wir sagen, dass sie

nur auf eine einzige Weise lösbar sei oder nur eine einzige Wurzel habe. So besitzt z. B. die Congruenz $6x + 5 \equiv -13 \pmod{11}$ keine andern Wurzeln als die, welche $-5 \pmod{11}$ sind. Anders verhält sich die Sache bei Congruenzen höherer Grade oder bei Congruenzen ersten Grades, in denen die Unbekannte mit einer Zahl multipliciert ist, zu welcher der Modul nicht prim ist.

27.

Es bleibt uns noch übrig, über die Auffindung der Lösung einer derartigen Congruenz einiges hinzuzufügen.

Zunächst bemerken wir, dass die Congruenz $ax + t \equiv u$, deren Modul wir zu a prim voraussetzen, von der Congruenz $ax \equiv \pm 1$ abhängt. Denn wenn diese durch $x \equiv r$ befriedigt wird, so wird jener durch $x \equiv \pm(u - t)r$ genügt. Der Congruenz $ax \equiv \pm 1$ ist aber, wenn man den Modul mit b bezeichnet, die unbestimmte Gleichung $ax = by \pm 1$ äquivalent, und wie diese zu lösen sei, ist heutzutage hinreichend bekannt. Wir begnügen uns daher, hier den Algorithmus der Rechnung herzusetzen.

Wenn die Grössen A, B, C, D, E, \dots so von den Grössen $\alpha, \beta, \gamma, \delta, \dots$ abhängen, dass man hat:

$$A = \alpha, B = \beta A + 1, C = \gamma B + A, D = \delta C + B, E = \varepsilon D + C, \dots,$$

so bezeichnen wir sie der Kürze wegen in folgender Weise:

$$A = [\alpha], B = [\alpha, \beta], C = [\alpha, \beta, \gamma], D = [\alpha, \beta, \gamma, \delta], \dots^*)$$

Es sei nun die unbestimmte Gleichung $ax = by \pm 1$, in welcher a, b positiv sind, vorgelegt. Wir nehmen, was erlaubt ist, an, dass a nicht kleiner als b sei. Dann bilden wir nach Art des bekannten Algorithmus, durch welchen man den grössten gemeinschaftlichen Teiler zweier Zahlen sucht, mittelst gewöhnlicher Division die Gleichungen:

$$a = ab + c, b = \beta c + d, c = \gamma d + e, \dots,$$

so dass $\alpha, \beta, \gamma, \dots, c, d, e, \dots$ positive ganze Zahlen sind und b, c, d, e, \dots fortwährend abnehmen, bis wir zu einer Gleichung von der Form

$$m = \mu n + 1$$

gelangen, was bekanntlich einmal eintreten muss. Dann ist:

*) Diese Beziehung lässt sich noch viel allgemeiner betrachten, was wir vielleicht bei einer andern Gelegenheit thun werden. Hier fügen wir nur zwei Sätze bei, die bei der gegenwärtigen Untersuchung Anwendung finden, nämlich:

$$(1) [\alpha, \beta, \gamma, \dots, \lambda, \mu] \cdot [\beta, \gamma, \dots, \lambda] - [\alpha, \beta, \gamma, \dots, \lambda] \cdot [\beta, \gamma, \dots, \lambda, \mu] = \pm 1,$$

wo das obere oder untere Zeichen zu nehmen ist, je nachdem die Anzahl der Zahlen $\alpha, \beta, \gamma, \dots, \lambda, \mu$ gerade oder ungerade ist.

(2) Die Reihenfolge der Zahlen $\alpha, \beta, \gamma, \dots$ kann umgekehrt werden, also:

$$[\alpha, \beta, \gamma, \dots, \lambda, \mu] = [\mu, \lambda, \dots, \gamma, \beta, \alpha].$$

Die Beweise, welche nicht schwer sind, unterdrücken wir hier.

$$a = [n, \mu, \dots, \gamma, \beta, \alpha], \quad b = [n, \mu, \dots, \gamma, \beta].$$

Nimmt man sodann

$$x = [\mu, \dots, \gamma, \beta] \quad y = [\mu, \dots, \gamma, \beta, \alpha]$$

so wird $ax = by + 1$, wenn die Anzahl der Zahlen $\alpha, \beta, \gamma, \dots, \mu, n$ gerade, dagegen $ax = by - 1$, wenn sie ungerade ist.

28.

Die allgemeine Auflösung derartiger unbestimmter Gleichungen hat zuerst Euler gelehrt, *Comment. Petrop. T. VII p. 46.**) Die Methode, deren er sich bediente, besteht in der Substitution anderer Unbekannten an Stelle von x, y und ist heutzutage hinreichend bekannt. Lagrange griff die Sache ein wenig anders an: Aus der Theorie der Kettenbrüche nämlich ist bekannt, dass, wenn man den Bruch $\frac{a}{b}$ in einen Kettenbruch

$$\frac{1}{\alpha + \frac{1}{\beta + \frac{1}{\gamma + \dots + \frac{1}{\mu + \frac{1}{n}}}}}$$

verwandelt und diesen nach Weglassung seines letzten Gliedes $\frac{1}{n}$ wieder zu einem gewöhnlichen Bruche $\frac{x}{4}$ macht, $ax = by \pm 1$ ist, falls a prim zu b ist.

Uebrigens ergibt sich aus beiden Methoden derselbe Algorithmus. Die Untersuchungen von Lagrange finden sich in *Hist. de l'Ac. de Berlin Année 1767 p. 175* und nebst andern in den Zusätzen zur französischen Übersetzung von Euler's Algebra.

29.

Die Congruenz $ax + t \equiv u$, deren Modul nicht prim zu a ist, lässt sich leicht auf den vorhergehenden Fall zurückführen. Es sei m der Modul und e der grösste gemeinschaftliche Teiler der Zahlen a, m . Zunächst ist klar, dass jeder der Congruenz nach dem Modul m genügende Wert von x derselben auch nach dem Modul a genügt (Artikel 5). Es ist aber immer $ax \equiv 0 \pmod{\delta}$, da δ ein Teiler von a ist. Daher ist die vorgelegte Congruenz nur lösbar, wenn $t \equiv u \pmod{\delta}$, d. h. $t-u$ durch δ teilbar ist.

Setzen wir daher $a = \delta e, m = \delta f, t-u = \delta k$, so wird e zu f prim sein, und der gegebenen Congruenz $\delta ex + \delta k \equiv 0 \pmod{\delta f}$ wird die folgende $ex + k \equiv 0 \pmod{f}$ äquivalent sein, d. h. jeder Wert von x , welcher dieser genügt, wird auch jener genügen und umgekehrt. Denn offenbar lässt

*) Vgl. die Zusätze am Schlusse der Disquisitiones.

sich $ex+k$ durch f teilen, wenn sich $\delta ex + \delta k$ durch δf teilen lässt und umgekehrt. Die Congruenz $ex + k \equiv 0 \pmod{f}$ haben wir aber oben auflösen gelehrt, woraus zugleich folgt, dass, wenn v einer der Werte von x ist, $x \equiv v \pmod{f}$ die vollständige Lösung der gegebenen Congruenz darstellt.

30.

Wenn der Modul zusammengesetzt ist, ist es zuweilen besser, sich folgender Methode zu bedienen.

Es sei der Modul $=mn$ mit und die gegebene Congruenz $ax \equiv b$. Man löse zunächst diese Congruenz nach dem Modul m und nehme an, dass ihr genügt werde, wenn $x \equiv v \pmod{\frac{m}{\delta}}$ ist, wo δ den grössten gemeinschaftlichen Teiler der Zahlen m und a

bezeichnet. Nun ist klar, dass jeder der Congruenz $ax \equiv b$ nach dem Modul mn genügende Wert von x derselben auch nach dem Modul m genügen muss und daher in der Form $v + \frac{m}{\delta} x'$ enthalten ist, wo x' eine unbestimmte Zahl bezeichnet, obwohl nicht umgekehrt alle in der Form $v + \frac{m}{\delta} x'$ enthaltenen Zahlen der Congruenz nach dem Modul mn genügen.

Wie aber x' bestimmt werden muss, damit $v + \frac{m}{\delta} x'$ eine Wurzel der Congruenz $ax \equiv b \pmod{mn}$ werde, lässt sich aus der Lösung der Congruenz $\frac{am}{\delta} x' + av \equiv b \pmod{mn}$, welcher die folgende $\frac{a}{\delta} x' \equiv \frac{b - av}{m} \pmod{n}$ äquivalent ist, ersehen. Es folgt hieraus,

dass die Lösung jeder beliebigen Congruenz ersten Grades nach dem Modul mn zurückgeführt werden kann auf die Lösung zweier Congruenzen nach den Moduln m und n . Man erkennt leicht, dass, wenn n wiederum das Product aus zwei Factoren ist, die Lösung der Congruenz nach dem Modul n von der Lösung zweier Congruenzen abhängt, deren Moduln jene Factoren sind. Allgemein hängt die Lösung einer Congruenz nach irgend einem zusammengesetzten Modul von der Lösung anderer Congruenzen ab, deren Moduln Factoren jener Zahl sind. Diese letzteren können aber, wenn es zweckmässig erscheint, immer so angenommen werden, dass sie Primzahlen sind.

Beispiel. Ist die Congruenz $19x \equiv 1 \pmod{140}$ vorgelegt, so löse man sie zunächst nach dem Modul 2, wodurch sich ergibt $x \equiv 1 \pmod{2}$. Setzt man $x = 1 + 2x'$, so wird $38x' \equiv -18 \pmod{140}$, welcher die folgende: $19x' \equiv -9 \pmod{70}$ äquivalent ist. Löst man diese letztere wiederum nach dem Modul 2, so wird $x' \equiv 1 \pmod{2}$ und daher, wenn $x' = 1 + 2x''$ gesetzt wird: $38x'' \equiv -28 \pmod{70}$ oder $19x'' \equiv -14 \pmod{35}$. Diese nach dem Modul 5 gelöst giebt: $x'' \equiv -4 \pmod{5}$, und wenn man $x'' = 4 + 5x'''$ setzt, so wird: $95x''' \equiv -90 \pmod{35}$ oder: $19x''' \equiv -18 \pmod{7}$. Aus dieser endlich folgt: $x''' \equiv -2 \pmod{7}$, und wenn man

$x''' = 2 + 7x''''$ setzt, so findet man $x = 59 + 140x''''$. Daher ist $x \equiv 59 \pmod{140}$ die vollständige Lösung der vorgelegten Congruenz.

31.

In ähnlicher Weise, wie die Wurzel der Gleichung $ax = b$ durch $\frac{b}{a}$ ausgedrückt wird, werden wir auch irgend eine Wurzel der Congruenz $ax \equiv b \pmod{c}$ mit $\frac{b}{a}$ bezeichnen und den Modul der Congruenz der Deutlichkeit halber hinzusetzen. So^a bezeichnet z. B. $\frac{19}{17} \pmod{12}$ jede Zahl, welche $\equiv 11 \pmod{12}$ ist (was auch der Analogie nach durch $\frac{11}{1} \pmod{12}$ bezeichnet werden kann). Allgemein geht aus dem Vorhergehenden hervor, dass $\frac{b}{a} \pmod{c}$ keine reelle Bedeutung hat (oder, wenn man lieber will, ein imaginärer Ausdruck ist), wenn a und c einen gemeinschaftlichen Teiler haben, der nicht zugleich auch b teilt. Abgesehen von diesem Falle aber wird der Ausdruck $\frac{b}{a} \pmod{c}$ stets reelle Werte haben und zwar unendlich viele; letztere aber werden sämtlich nach dem Modul c congruent sein, wenn a prim zu c ist, oder nach dem Modul $\frac{c}{\delta}$, wenn δ der grösste gemeinschaftliche Teiler der Zahlen c und a ist.

Mit diesen Ausdrücken kann man fast ebenso rechnen, wie mit den gewöhnlichen Brüchen. Einige Eigenschaften, die sich leicht aus dem Vorhergehenden ableiten lassen, setzen wir hierher.

1. Wenn nach dem Modul c $a \equiv \alpha$, $b \equiv \beta$ ist, so sind die Ausdrücke $\frac{a}{b} \pmod{c}$ und $\frac{\alpha}{\beta} \pmod{c}$ äquivalent.
2. $\frac{a\delta}{b\delta} \pmod{c\delta}$ und $\frac{a}{b} \pmod{c}$ sind äquivalent.
3. $\frac{ak}{bk} \pmod{c}$ und $\frac{a}{b} \pmod{c}$ sind äquivalent, wenn k prim zu c ist.

Wir könnten noch viele andere ähnliche Sätze anführen; da dieselben aber keine Schwierigkeit bieten und für das Folgende nicht so nötig sind, gehen wir zu etwas anderem über.

Die Zahl zu finden, welche gegebenen Resten nach gegebenen Moduln congruent ist.

32.

Die Aufgabe, welche im Folgenden oft zur Anwendung kommen wird, nämlich: Alle Zahlen zu finden, welche nach beliebig vielen gegebenen Moduln gegebene Reste lassen, kann mit Hülfe des Vorhergehenden leicht gelöst werden. Es seien zunächst zwei Moduln A und B ge-

geben, nach denen eine gesuchte Zahl z den Zahlen a und b respective congruent sein soll. Es sind daher alle Werte von z unter der Form $Ax + a$ enthalten, wo x eine unbestimmte Zahl, aber von solcher Beschaffenheit ist, dass $Ax + a \equiv b \pmod{B}$ wird. Wenn nun δ der grösste gemeinschaftliche Teiler der Zahlen A und B ist, so wird die vollständige Lösung dieser Congruenz die folgende Form haben $x \equiv v \pmod{\frac{B}{\delta}}$, oder es wird, was auf dasselbe hinauskommt, $x = v + \frac{kB}{\delta}$ sein, wo k eine willkürliche ganze Zahl bezeichnet. Somit wird

die Formel $Av + a + \frac{kAB}{\delta}$ alle Werte von z umfassen, d. h. $z \equiv Av + a \pmod{\frac{AB}{\delta}}$ wird die

vollständige Lösung des Problems sein. – Kommt zu den Moduln A, B noch ein dritter C hinzu, nach welchem die gesuchte Zahl z congruent c sein soll, so muss man offenbar in derselben Weise weiter verfahren, da die beiden früheren Bedingungen bereits in eine einzige zusammengefasst sind. Ist also ε der grösste gemeinschaftliche Teiler der Zahlen $\frac{AB}{\delta}$ und C und $x \equiv w \pmod{\frac{C}{\varepsilon}}$ die Lösung der Congruenz $\frac{AB}{\delta}x + Av + a \equiv c \pmod{C}$, so

wird die Aufgabe durch die Congruenz $z \equiv \frac{ABw}{\delta} + Av + a \pmod{\frac{ABC}{\delta\varepsilon}}$ vollständig gelöst

sein. – In ähnlicher Weise hat man zu verfahren, wie viele Moduln auch immer gegeben sein mögen. Es mag bemerkt werden, dass $\frac{AB}{\delta}, \frac{ABC}{\delta\varepsilon}$ die kleinsten gemeinschaftlichen

Vielfachen resp. der Zahlen A, B und A, B, C sind; man erkennt hieraus leicht, dass, wie viele Moduln A, B, C, \dots auch vorhanden sein mögen, die vollständige Lösung die folgende Form haben wird: $z \equiv r \pmod{M}$, wo M der kleinste gemeinschaftliche Dividuum jener Zahlen ist. Ist ferner irgend eine der Hilfscongruenzen unlösbar, so folgt daraus, dass das Problem eine Unmöglichkeit in sich schliesst. Offenbar aber kann dies nicht der Fall sein, wenn alle Zahlen A, B, C, \dots unter einander prim sind.

Beispiel. Die Zahlen $A, B, C; a, b, c$ seien resp. 504, 35, 16; 17, -4, 33. Hier sind die beiden Bedingungen, dass $z \equiv 17 \pmod{504}$ und $\equiv -4 \pmod{35}$ sein solle, der einen: $z \equiv 521 \pmod{2520}$ äquivalent. Letztere, mit der folgenden: $z \equiv 33 \pmod{16}$ verbunden, liefert $z \equiv 3041 \pmod{5040}$.

33.

Sind alle Zahlen A, B, C, \dots zu einander prim, so ist bekanntlich das Product aller das kleinste gemeinschaftliche Vielfache derselben. In diesem Falle werden offenbar alle Congruenzen $z \equiv a \pmod{A}, z \equiv b \pmod{B}, \dots$ einer einzigen $z \equiv r \pmod{R}$, in welcher R das Product der

Zahlen A, B, C, \dots bezeichnet, vollkommen äquivalent sein. Hieraus folgt umgekehrt, dass die eine Bedingung $z \equiv r \pmod{R}$ in mehrere zerlegt werden kann. Wenn nämlich R auf irgend eine Weise in zu einander prime Factoren A, B, C, \dots zerlegt ist, so werden die Bedingungen $z \equiv r \pmod{A}, z \equiv r \pmod{B}, z \equiv r \pmod{C}, \dots$ die gegebene vollständig erschöpfen. Diese Bemerkung eröffnet uns einen Weg, nicht nur die Unmöglichkeit der Aufgabe, falls sich eine solche etwa aus den gegebenen Bedingungen ergeben sollte, sofort zu erkennen, sondern auch die Rechnung bequemer und kürzer durchzuführen.

34.

Die gegebenen Bedingungen seien wie oben: $z \equiv a \pmod{A}, z \equiv b \pmod{B}, z \equiv c \pmod{C}, \dots$ Man löse sämtliche Moduln in zu einander prime Factoren, A in $A'A''A''' \dots$, B in $B'B''B''' \dots$ u. s. w. und zwar derart auf, dass die Zahlen $A', A'', \dots, B', B'', \dots$ entweder Primzahlen oder Potenzen von Primzahlen sind. Ist daher eine der Zahlen A, B, C, \dots schon an sich eine Primzahl oder die Potenz einer solchen, so ist für diese eine Zerlegung in Factoren nicht nötig. Dann ergibt sich aus dem Vorhergehenden, dass man für die gegebenen Bedingungen die folgenden substituieren kann:

$$\begin{aligned} z &\equiv a \pmod{A'}, z \equiv a \pmod{A''}, z \equiv a \pmod{A'''}, \dots \\ z &\equiv b \pmod{B'}, z \equiv b \pmod{B''}, z \equiv b \pmod{B'''}, \dots \end{aligned}$$

u. s. w.

Wären nun nicht sämtliche Zahlen A, B, C, \dots zu einander prim, z. B. A nicht prim zu B , so könnten offenbar nicht alle Primteiler von A und B von einander verschieden sein, vielmehr müsste unter den Factoren A', A'', A''', \dots der eine oder der andere vorkommen, welcher unter den Factoren B', B'', B''', \dots einen sich gleichen oder ein Vielfaches oder einen genauen Teil von sich hätte. Wäre zuerst $A' = B'$, so müssten die Bedingungen $z \equiv a \pmod{A'}$ und $z \equiv b \pmod{B'}$ identisch oder also $a \equiv b \pmod{A'}$ oder B' sein, so dass eine von diesen beiden weggelassen werden könnte. Wäre aber a nicht $\equiv b \pmod{A'}$, so würde die Aufgabe etwas Unmögliches verlangen. Wenn zweitens B' ein Vielfaches von A' wäre, so müsste die Bedingung $z \equiv a \pmod{A'}$ in der folgenden $z \equiv b \pmod{B'}$ enthalten, oder es müsste die aus der letzteren folgende $z \equiv b \pmod{A'}$ mit der ersteren identisch sein. Hieraus folgt, dass die Bedingung $z \equiv a \pmod{A'}$, falls sie nicht mit den andern im Widerspruch steht (in welchem Falle das Problem unmöglich ist), weggelassen werden kann. Sind auf diese Weise alle überflüssigen Bedingungen weggelassen, so werden offenbar alle Moduln, welche von $A', A'', A''', \dots, B', B'', B''', \dots$ u. s. w. noch übrig bleiben, prim zu einander sein. Wir können alsdann hinsichtlich der Möglichkeit des Problems sicher sein und nach den vorher angegebenen Vorschriften verfahren.

35.

Beispiel. Soll wie oben $z \equiv 17 \pmod{504}$, $\equiv -4 \pmod{35}$ und $\equiv 33 \pmod{16}$ sein, so lassen sich diese Bedingungen in die folgenden zerlegen:

$$z \equiv 17 \pmod{8}, \equiv 17 \pmod{9}, \equiv 17 \pmod{7}$$

$$z \equiv -4 \pmod{5}, \equiv -4 \pmod{7}$$

$$z \equiv 33 \pmod{16}.$$

Von diesen können die Bedingungen: $z \equiv 17 \pmod{8}$ und $z \equiv 17 \pmod{7}$ weggelassen werden, da die erstere in der Bedingung $z \equiv 33 \pmod{16}$ enthalten, die letztere aber mit $z \equiv -4 \pmod{7}$ identisch ist. Es bleiben daher die folgenden Bedingungen:

$$z \equiv \begin{cases} 17 \pmod{9} \\ -4 \pmod{5} \\ -4 \pmod{7} \\ 33 \pmod{16}, \end{cases}$$

aus denen $z \equiv 3041 \pmod{5040}$ folgt.

Überdies ist klar, dass es meistens bequemer sein wird, wenn man von den übrig bleibenden Bedingungen diejenigen, welche aus einer und derselben Bedingung hervorgegangen waren, wieder für sich zusammennimmt. Sind z. B. von den Bedingungen $z \equiv a \pmod{A'}$, $z \equiv a \pmod{A''}$, ... einige weggelassen worden, so wird die aus den übrigen zusammengesetzte die folgende sein: $z \equiv a$ nach einem Modul, welcher das Product aller von A' , A'' , A''' , ... noch übrig gebliebenen Moduln ist. So wird in unserm Beispiel aus den Bedingungen $z \equiv -4 \pmod{5}$, $z \equiv -4 \pmod{7}$ gerade die, aus welcher sie entstanden waren, nämlich $z \equiv -4 \pmod{35}$, ohne Weiteres wieder hergestellt. Ferner folgt hieraus, dass es mit Rücksicht auf die Kürze der Rechnung nicht völlig gleichgültig ist, welche von den überflüssigen Bedingungen weggelassen wird; doch liegt es nicht in unserer Absicht, auf diese und andere practische Kunstgriffe, welche leichter durch Übung als durch besondere Vorschriften zu lernen sind, an dieser Stelle näher einzugehen.

36.

Wenn sämtliche Moduln A , B , C , D , ... unter sich prim sind, so ist es oft besser, sich der folgenden Methode zu bedienen. Man bestimme eine Zahl α , welche nach A der Einheit, nach dem Producte der übrigen Moduln aber der Null congruent ist, oder es sei α ein beliebiger (meistens ist es vorteilhaft den kleinsten zu nehmen) mit $BCD \dots$ multiplicirter Wort des Ausdrucks $\frac{1}{BCD \dots} \pmod{A}$ (siehe Artikel 32).

Ebenso sei $\beta \equiv 1 \pmod{B}$ und $\equiv 0 \pmod{ACD \dots}$, $\gamma \equiv 1 \pmod{C}$ und $\equiv 0 \pmod{ABD \dots}$ u. s. w. Wenn dann eine Zahl z gesucht wird, welche nach den Moduln A , B , C , D , ... respective den Zahlen a , b , c , d , ... congruent ist, so kann man setzen:

$$z \equiv \alpha a + \beta b + \gamma c + \delta d + \dots \pmod{ABCD \dots}$$

Augenscheinlich nämlich ist $aa \equiv a \pmod{A}$, während die übrigen Glieder $\beta b, \gamma c, \dots$ sämtlich $\equiv 0 \pmod{A}$ sind; daher ist $z \equiv a \pmod{A}$. Analog ist der Beweis bezüglich der übrigen Moduln. Diese Lösung ist der früheren vorzuziehen, wenn mehrere derartige Probleme zu lösen sind, für welche die Moduln A, B, C, \dots ihre Werte beibehalten; denn dann erhalten die Zahlen $\alpha, \beta, \gamma, \dots$ constante Werte. Dies ist der Fall bei einem Problem der Zeitrechnung, bei welchem gefragt wird, das wievielste Jahr in der Julianischen Periode eine gegebene Römer-Zinszahl, güldene Zahl und Sonnenzirkel besitze. Hierbei ist $A = 15$, $B = 19$, $C = 28$. Da nun der Wert des Ausdrucks $\frac{1}{19 \cdot 28} \pmod{15}$ oder $\frac{1}{532} \pmod{15}$ gleich 13 ist, so ist $\alpha = 6916$. Analog findet man $\beta = 4200$ und $\gamma = 4845$. Demnach ist die gesuchte Zahl der kleinste Rest der Zahl $6916a + 4200b + 4845c$, wo a die Römer-Zinszahl, b die güldene Zahl und c den Sonnenzirkel bezeichnet.

Lineare Congruenzen mit mehreren Unbekannten.

37.

Das Vorhergehende möge hinsichtlich der Congruenzen ersten Grades mit einer einzigen Unbekannten genügen. Wir haben aber noch über Congruenzen zu handeln, in denen mehrere Unbekannte vorkommen. Da aber dieser Abschnitt, falls wir die Einzelheiten mit aller Strenge auseinandersetzen wollten, nicht ohne Weitschweifigkeit durchgeführt werden kann, und es hier nicht in unserer Absicht liegt, eine erschöpfende Darstellung zu geben, wir vielmehr nur das anführen wollen, was der Aufmerksamkeit am würdigsten zu sein scheint, so werden wir unsere Untersuchung hier auf wenige Bemerkungen beschränken und uns eine eingehendere Darlegung dieses Gegenstandes für eine andere Gelegenheit vorbehalten.

1. In analoger Weise wie bei Gleichungen erkennt man, dass man auch hier ebensoviele Gleichungen haben muss, als Unbekannte zu bestimmen sind.

2. Es seien also ebensoviele Congruenzen

$$(A) \quad ax + by + cz + \dots \equiv f \pmod{m}$$

$$(A') \quad a'x + b'y + c'z + \dots \equiv f'$$

$$(A'') \quad a''x + b''y + c''z + \dots \equiv f''$$

gegeben, als Unbekannte x, y, z, \dots vorhanden sind.

Man bestimme nun Zahlen ξ, ξ', ξ'', \dots mittelst der Gleichungen

$$b\xi + b'\xi' + b''\xi'' + \dots = 0$$

$$c\xi + c'\xi' + c''\xi'' + \dots = 0$$

.....

und zwar so, dass sie sämtlich ganze Zahlen werden und keinen gemeinschaftlichen Factor haben, was, wie aus der Theorie der linearen Gleichungen

bekannt ist, immer möglich ist. In ähnlicher Weise bestimme man Zahlen $v, v', v'', \dots, \zeta, \zeta', \zeta'', \dots$ mittelst der Gleichungen:

$$\begin{aligned} av + a'v' + a''v'' + \dots &= 0 \\ cv + c'v' + c''v'' + \dots &= 0 \end{aligned}$$

$$\begin{aligned} a\zeta + a'\zeta' + a''\zeta'' + \dots &= 0 \\ b\zeta + b'\zeta' + b''\zeta'' + \dots &= 0 \end{aligned}$$

3. Werden die Congruenzen A, A', A'', \dots zuerst resp. mit ξ, ξ', ξ'', \dots , sodann mit v, v', v'', \dots u. s. w. multipliciert und sodann die Producte jedesmal addiert, so werden sich offenbar folgende Congruenzen ergeben:

$$\begin{aligned} (a\xi + a'\xi' + a''\xi'' + \dots)x &\equiv f\xi + f'\xi' + f''\xi'' + \dots \\ (bv + b'v' + b''v'' + \dots)y &\equiv fv + f'v' + f''v'' + \dots \\ (c\zeta + c'\zeta' + c''\zeta'' + \dots)z &\equiv f\zeta + f'\zeta' + f''\zeta'' + \dots \end{aligned}$$

die wir der Kürze wegen in folgender Weise darstellen wollen:

$$\Sigma(a\xi)x \equiv \Sigma(f\xi), \Sigma(bv)y \equiv \Sigma(fv), \Sigma(c\zeta)z \equiv \Sigma(f\zeta), \dots$$

4. Nunmehr sind mehrere Fälle zu unterscheiden.

Erstens, wenn sämtliche Coefficienten $\Sigma(a\xi), \Sigma(bv), \dots$ der Unbekannten zu dem Modul m der Congruenzen prim sind, so lassen sich diese Congruenzen nach den vorher angegebenen Regeln lösen, und die vollständige Lösung des Problems wird dargestellt werden durch Congruenzen von der Form: $x \equiv p \pmod{m}, y \equiv q \pmod{m}, \dots$ *).

Sind z. B. die Congruenzen gegeben:

$$x + 3y + z \equiv 1, 4x + y + 5z \equiv 7, 2x + 2y + z \equiv 3 \pmod{8},$$

so findet man $\xi = 9, \xi' = 1, \xi'' = -14$; hieraus wird $-15x \equiv -26$, daher $x \equiv 6 \pmod{8}$. Auf dieselbe Weise findet man $15y \equiv -4, 15z \equiv 1$ und hieraus $y \equiv 4, z \equiv 7 \pmod{8}$.

5. Zweitens, wenn nicht sämtliche Coefficienten $\Sigma(a\xi), \Sigma(bv), \dots$ zum Modul prim sind, so seien $\alpha, \beta, \gamma, \dots$ die grössten gemeinschaftlichen Teiler von m und $\Sigma(a\xi), \Sigma(bv), \Sigma(c\zeta), \dots$ respective. Offenbar ist dann die Aufgabe unmöglich, wofern nicht jene auch zugleich Teiler der Zahlen $\Sigma(f\xi), \Sigma(fv), \Sigma(f\zeta), \dots$ Wenn aber diese Bedingungen stattfinden, so werden die Congruenzen in (3) durch solche von den Formen $x \equiv p$

*) Es mag bemerkt werden, dass dieser Schluss eines Beweises bedarf, den wir aber hier unterdrücken. Denn eigentlich folgt aus unserer Deduction nichts weiter, als dass die gegebenen Congruenzen durch andere Werte der Unbekannten x, y, z, \dots nicht gelöst werden können; dass diese aber genügen, folgt nicht. Möglicherweise nämlich könnte es gar keine Lösung geben. Ein ähnlicher Paralogismus wird auch in der Theorie der linearen Gleichungen häufig begangen.