Werk

Titel: Vorlesungen über Zahlentheorie
Autor: Dirichlet, Peter
Verlag: Vieweg
Ort: Braunschweig
Jahr: 1871
Kollektion: Mathematica
Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen
Werk Id: PPN30976923X
PURL: http://resolver.sub.uni-goettingen.de/purl?PPN30976923X
OPAC: http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X

LOG Id: LOG_0006
LOG Titel: Erster Abschnitt: Von der Theilbarkeit der Zahlen
LOG Typ: chapter

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

Erster Abschnitt.

Von der Theilbarkeit der Zahlen.

§. 1.

Wir behandeln in diesem Abschnitte einige arithmetische Sätze, welche man zwar in den meisten Lehrbüchern vorfindet, die aber für unsere Wissenschaft von so fundamentaler Bedeutung sind, dass eine strenge Begründung derselben hier durchaus nothwendig erscheint. Dahin gehört zuerst der Satz, dass das Product einer Reihe von ganzen positiven Zahlen unabhängig von der Anordnung ist, in welcher man die Multiplication ausführt. Indem wir uns zunächst auf den Fall beschränken, in welchem es sich um *drei* Zahlen a, b, c handelt, bilden wir das folgende Schema

$$\begin{array}{cccccc} c, & c, & c, & c & \ldots & c \\ c, & c, & c, & c & \ldots & c \\ c, & c, & c, & c & \ldots & c \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ c, & c, & c, & c & \ldots & c \end{array}$$

welches aus b Horizontalreihen besteht, deren jede die Zahl c gleich oft, nämlich $a$mal enthält, und stellen uns die Aufgabe, die Summe aller aufgeschriebenen Zahlen zu bestimmen. Zunächst können wir sagen: da die Zahl c in jeder Horizontalreihe $a$mal vorkommt, so ist nach dem Grundbegriff der Multiplication die

Summe aller in einer solchen Reihe befindlichen Zahlen gleich ca, indem wir den *Multiplicand* c durch die Stellung von dem *Multiplicator* a unterscheiden; da ferner b solche Horizontalreihen vorhanden sind, so ist die Summe sämmtlicher Zahlen gleich $(ca)b$, wo jetzt ca der Multiplicand, b der Multiplicator ist. Nun können wir aber dieselbe Summe auch auf anderm Wege durch die Bemerkung bestimmen, dass das obige Schema aus a Verticalreihen besteht, deren jede $b$mal die Zahl c enthält; es ist also die Summe aller in einer Verticalreihe befindlichen Zahlen gleich cb, und folglich die Totalsumme gleich $(cb)a$. Wir erhalten mithin das erste Resultat

$$(ca)b = (cb)a,$$

aus welchem wir, indem wir die bisher ganz willkürliche Zahl $c = 1$ setzen, die Folgerung ziehen, dass

$$ab = ba$$

ist, d. h.: *in einem Product aus zwei ganzen positiven Zahlen dürfen Multiplicand und Multiplicator mit einander vertauscht werden.* Man lässt deshalb auch in der Benennung den Unterschied zwischen Multiplicand und Multiplicator ganz fallen, indem man beide unter dem gemeinschaftlichen Namen *Factoren* zusammenfasst.

Wir können nun dieselbe Totalsumme sämmtlicher in dem obigen Schema befindlichen Zahlen noch auf eine dritte Art bestimmen, indem wir abzählen, wie oft der Summand c im Ganzen vorkommt. Zunächst ist a die Anzahl der in einer jeden Horizontalreihe befindlichen Zahlen c, und folglich ist, da b solche Horizontalreihen vorhanden sind, die Anzahl aller aufgeschriebenen Zahlen gleich ab. Hieraus folgt, dass die Totalsumme den Werth $c(ab)$ hat, dass also

$$(ca)b = (cb)a = c(ab)$$

ist. Verbindet man hiermit den schon oben betrachteten speciellen Fall $ab = ba$, so kann man das Bisherige in folgendem Satze zusammenfassen:

Wenn man von drei positiven ganzen Zahlen zwei nach Belieben auswählt und als Factoren zu ihrem Producte vereinigt, sodann dieses Product und die dritte jener drei Zahlen mit einander multiplicirt, so hat das so entstehende Product stets denselben Werth, wie man auch die ersten beiden Zahlen ausgewählt haben mag.

Da also dieses Product von der Anordnung der beiden successiven Multiplicationen ganz unabhängig ist, so bezeichnet man

dasselbe kurz als das Product aus jenen drei Zahlen und nennt diese letzteren ohne Unterschied die Factoren des Productes.

§. 2.

Es ist nun leicht zu zeigen, ohne ein neues Princip anzuwenden, dass ein ganz ähnlicher allgemeinerer Satz für jedes System S von beliebig vielen positiven ganzen Zahlen

$$a, b, c \ldots$$

gilt. Die allgemeinste Art, diese Zahlen durch wiederholte Anwendung einfacher, d. h. auf nur zwei Zahlen bezüglicher Multiplicationen zu einem Producte zu vereinigen, ist folgende. Man greife nach Belieben zwei Zahlen aus dem System S heraus und bilde ihr Product; der aus den übrigen Zahlen des Systems S und aus diesem Product bestehende Zahlencomplex S' enthält dann eine Zahl weniger als S; indem man wieder ganz nach Belieben zwei Zahlen aus S' zu ihrem Producte vereinigt und die anderen unverändert lässt, erhält man ein System S'' von Zahlen, deren Anzahl um zwei kleiner ist als die der ursprünglich gegebenen Zahlen. Fährt man so fort, so wird man zuletzt zu einer einzigen Zahl gelangen, und der zu beweisende Satz besteht darin, *dass diese am Ende des Processes resultirende Zahl immer dieselbe sein wird, auf welche Art man auch die einzelnen einfachen Multiplicationen anordnen mag.*

Um dies zu zeigen, wenden wir die vollständige Induction an, d. h. wir nehmen an, der Satz sei richtig, wenn die Anzahl der ursprünglich gegebenen Zahlen oder Factoren $= n$ ist, und beweisen, dass er dann auch für die nächst grössere Anzahl $n + 1$ von Factoren ebenfalls gültig sein muss. Es sei also ein System S von $n + 1$ Zahlen

$$a, b, c, d, e \ldots$$

gegeben, so wähle man irgend zwei derselben, z. B. a und b, und bilde ihr Product ab; der nun entstehende Zahlencomplex enthält nur noch die n Zahlen

$$ab, c, d, e \ldots$$

und folglich ist nach unserer Annahme das Endresultat von der weitern Anordnung des Processes ganz unabhängig. Bei einer andern Anordnung der ganzen Operation kann daher höchstens

dann ein anderes Endresultat zum Vorschein kommen, wenn das bei dem ersten Schritte ausgewählte Zahlenpaar von a, b verschieden ist, und zwar sind zwei Fälle zu unterscheiden.

Erstens kann es sein, dass bei der zweiten Anordnung zuerst *eine* der beiden Zahlen a, b, z. B. a, mit einer der übrigen c, d, e . . ., z. B. mit c, zu dem Producte ac vereinigt wird, so dass der nächste Complex aus den n Zahlen

$$ac,\ b,\ d,\ e\ \ldots$$

besteht; da nun sowohl bei der erstern wie bei der letztern Anordnung die auf den ersten Schritt folgenden Operationen keinen Einfluss auf das Endresultat ausüben können, so setze man die erste Anordnung so fort, dass zunächst die beiden Zahlen ab und c, die zweite so, dass zunächst die beiden Zahlen ac und b vereinigt werden. Auf diese Weise entsteht bei der ersten Anordnung zunächst der Complex

$$(ab)c,\ d,\ e\ \ldots$$

bei der zweiten der Complex

$$(ac)b,\ d,\ e\ \ldots$$

Da nun zufolge des vorhergehenden Paragraphen die beiden Producte $(ab)c$ und $(ac)b$ und folglich auch die beiden vorstehenden Complexe identisch sind, so wird, da jeder derselben nur noch $n-1$ Zahlen enthält, bei der ersten wie bei der zweiten Anordnung dasselbe Endresultat auftreten.

Zweitens kann es aber auch sein, dass bei dem ersten Schritt der zweiten Anordnung *keine* der beiden Zahlen a, b, sondern zwei von den übrigen, z. B. c, d, herausgegriffen werden, so dass zunächst der Complex

$$a,\ b,\ cd,\ e\ \ldots$$

entsteht. Auch jetzt kann man wieder die auf den ersten Schritt folgenden Operationen bei beiden Anordnungen nach Belieben ausführen; man vereinige daher zunächst bei der ersten Anordnung die Zahlen c, d, und bei der zweiten Anordnung die Zahlen a, b; dann besteht bei beiden Anordnungen der nächstfolgende Complex aus denselben $n-1$ Zahlen

$$ab,\ cd,\ e\ \ldots$$

und folglich wird abermals das Endresultat bei beiden dasselbe sein.

Hiermit ist die Allgemeingültigkeit des Satzes bewiesen; denn da er nach dem vorhergehenden Paragraphen für $n = 3$ gilt, so

gilt er nach dem Vorstehenden auch für alle Systeme von Zahlen, deren Anzahl = 4, 5, 6 u. s. w. ist. Das Endresultat heisst auch jetzt wieder das Product aus den gegebenen Zahlen, diese letzteren heissen die Factoren des Productes, und man bezeichnet das Product durch das Nebeneinanderschreiben sämmtlicher in beliebiger Ordnung folgenden Factoren.

Ein besonderer Fall dieses Satzes ist der, dass man bei der Bildung des Productes aus beliebig vielen Zahlen oder Factoren dieselben nach Belieben in Gruppen vertheilen und alle in einer Gruppe enthaltenen Factoren zu ihrem Product vereinigen darf; das Product aus diesen den einzelnen Gruppen entsprechenden Producten wird immer mit dem Producte aller gegebenen Zahlen übereinstimmen; denn offenbar ist diese Bildung selbst eine der verschiedenen möglichen Anordnungen des Processes. So ist z. B.

$$abcde = (ab)c(de) = (abcd)e = (abe)(cd).$$

Es ist nicht schwierig, dieselben Sätze auch für den Fall zu beweisen, dass unter den Factoren eines Productes beliebig viele *negative* sind; das Vorzeichen des Productes wird das positive oder negative sein, je nachdem die Anzahl der negativen Factoren gerade oder ungerade ist. Endlich mag noch daran erinnert werden, dass auch die ganze Zahl *Null* als Factor auftreten kann, in welchem Falle das Product stets = 0 sein wird.

§. 3.

Wenn die Zahl*) a das Product aus der Zahl b und einer zweiten ganzen Zahl m, also $a = mb$ ist, so nennt man a ein *Vielfaches* oder *Multiplum* von b; statt dessen sagt man auch: a ist *theilbar* durch b, oder: b ist ein *Theiler* oder *Divisor* von a, oder endlich: b *geht in* a *auf*. Alle diese Benennungen sind gleich gebräuchlich, und da es in der Zahlentheorie ausserordentlich oft vorkommt, diese Beziehung zwischen zwei Zahlen auszudrücken, so ist es angenehm, dafür eine Reihe verschiedener Ausdrücke zu besitzen. Aus der Definition des Vielfachen leuchten nun sogleich folgende Sätze ein, von denen später sehr häufig Gebrauch gemacht werden wird.

*) Unter *Zahlen* schlechthin sind hier und im Folgenden immer *ganze* Zahlen zu verstehen.

1. Ist a Multiplum von b, b wieder Multiplum von c, so ist auch a Multiplum von c. Denn der Annahme nach ist $a = mb$, $b = nc$, wo m und n irgend zwei ganze Zahlen bedeuten; hieraus folgt $a = m(nc) = (mn)c$, also ist a theilbar durch c.

Allgemein: hat man eine Reihe von Zahlen, in welcher jede ein Vielfaches der nächstfolgenden ist, so ist auch jede frühere Zahl ein Vielfaches von jeder spätern.

2. Ist die Zahl a sowohl als auch b ein Multiplum einer dritten Zahl c, so ist auch die Summe und die Differenz der beiden ersteren ein Multiplum der dritten. Denn aus $a = mc$, $b = nc$ folgt $a \pm b = (m \pm n)c$.

§. 4.

Von der grössten Wichtigkeit für die Lehre von der Theilbarkeit der Zahlen ist folgende Aufgabe *): *Wenn irgend zwei ganze positive Zahlen a, b gegeben sind, so sollen die gemeinschaftlichen Theiler derselben, d. h. diejenigen Zahlen δ gefunden werden, welche gleichzeitig in a und in b aufgehen.*

Wir können annehmen, es sei a grösser oder wenigstens nicht kleiner als b; dann wird die Division von a durch b einen Quotienten m und einen Rest c geben, welcher letztere jedenfalls kleiner als b ist. Betrachten wir nun die aus dieser Division resultirende Gleichung

$$a = mb + c$$

und nehmen wir an, es sei δ irgend eine sowohl in a als in b aufgehende Zahl, so ist δ jedenfalls auch ein Divisor des Restes c; denn da a und b Multipla von δ sind, so ist (nach §. 3) mb, und folglich auch die Differenz $a - mb = c$ ein Multiplum von δ. Wir können daher sagen: jeder gemeinschaftliche Theiler der beiden Zahlen a, b ist auch ein gemeinschaftlicher Theiler der beiden Zahlen b, c. Umgekehrt, ist δ ein gemeinschaftlicher Divisor der beiden Zahlen b, c, so ist, da δ dann auch in mb aufgeht, die Summe $mb + c = a$ der beiden Multipla mb und c von δ ebenfalls ein Multiplum von δ; also ist jeder gemeinschaftliche Divisor der Zahlen b, c auch gemeinschaftlicher Divisor der Zahlen a, b. Mithin stimmen die gemeinschaftlichen Divisoren der beiden Zahlen a, b

*) *Euclid's Elemente*, Buch VII, Satz 2.

vollständig mit denen der beiden Zahlen b, c überein; unsere Untersuchung ist daher von dem Paare a, b auf das Paar b, c reducirt, und da b nicht grösser als a, c aber jedenfalls kleiner als b ist, so können wir mit Recht sagen, dass das Problem auf ein einfacheres zurückgeführt sei.

Wenn nun c von Null verschieden ist, die erste Division also nicht aufgeht, so können wir, indem wir b durch die kleinere Zahl c dividiren, wieder eine Gleichung von der Form

$$b = nc + d$$

bilden, in welcher der Divisionsrest d kleiner als der vorhergehende c ist. Durch eine der obigen ganz ähnliche Betrachtung ergiebt sich dann, dass die gemeinschaftlichen Divisoren der beiden Zahlen c, d vollständig mit denen der Zahlen b, c und also auch mit denen der Zahlen a, b übereinstimmen.

So kann man fortfahren, bis einmal die Division aufgeht, was nach einer endlichen Anzahl von Operationen durchaus eintreten muss; denn die Zahlen $b, c, d \ldots$ bilden eine Reihe von beständig abnehmenden Zahlen, und da es nur eine endliche Anzahl von Zahlen giebt, welche kleiner sind als b, so muss unter ihnen endlich auch die Null erscheinen. Wir haben dann eine Kette von Gleichungen von der Form

$$\begin{aligned} a &= mb + c \\ b &= nc + d \\ c &= pd + e \\ &\cdots\cdots\cdots \\ &\cdots\cdots\cdots \\ f &= sg + h \\ g &= th. \end{aligned}$$

Jeder gemeinschaftliche Divisor δ von a, b ist auch Divisor der folgenden Zahlen $c, d \ldots$, endlich auch von h; umgekehrt, ist δ ein Divisor von h, so lehrt die letzte Gleichung, dass δ auch Divisor von g, also gemeinschaftlicher Divisor von g und h ist; folglich ist δ auch Divisor von f und ebenso von den vorhergehenden Zahlen, endlich auch von b und von a. Wir haben daher das Resultat:

Die gemeinschaftlichen Divisoren zweier Zahlen a und b stimmen überein mit den sämmtlichen Divisoren Einer bestimmten Zahl h, welche man durch den obigen Algorithmus stets finden kann. Da nun h selbst zu diesen Divisoren gehört und unter ihnen dem

Werth nach der grösste ist, so nennt man diese Zahl h den *grössten gemeinschaftlichen Divisor* der beiden Zahlen a und b.

Hiermit ist nun zwar unser Problem nicht vollständig gelöst, sondern nur auf das andere zurückgeführt, sämmtliche Divisoren einer gegebenen Zahl h zu finden, für welches wir noch keine directe Lösung haben; allein es wird sich im Folgenden hinreichend zeigen, dass der obige Algorithmus ein Fundament bildet, auf welchem sich die Grundprincipien der Zahlentheorie mit ebenso grosser Strenge wie Leichtigkeit aufbauen lassen. Nur einige Bemerkungen noch, um auch nicht den geringsten Zweifel gegen die Allgemeinheit der folgenden Sätze aufkommen zu lassen: wir haben die obige Kette von Gleichungen gebildet unter der Voraussetzung, dass a nicht kleiner als b sei; allein für den Fall, dass $a < b$ sein sollte, braucht man nur $m = 0$, also $c = a$ zu nehmen, um dieselbe Form auch dann zu wahren. Ebenso leicht erkennt man, dass das Vorzeichen der Zahlen a, b ganz unwesentlich ist; ja, es darf sogar eine von ihnen $= 0$ sein; nur, wenn beide $= 0$ sind, kann von einem grössten gemeinschaftlichen Divisor derselben keine Rede sein.

§. 5.

Besonders interessant ist der specielle Fall, in welchem der grösste gemeinschaftliche Divisor zweier Zahlen a, b die Einheit ist; man nennt zwei solche Zahlen *relative Primzahlen*, auch wohl *Zahlen ohne gemeinschaftlichen Divisor*, indem man absieht von dem allen Zahlen gemeinschaftlichen Divisor 1; oder man sagt auch: a ist relative Primzahl *gegen* oder *zu* b. Dieser Definition zufolge erkennt man also zwei Zahlen als relative Primzahlen daran, dass bei dem Algorithmus des grössten gemeinschaftlichen Divisors einmal der Rest $h = 1$ auftritt. Für solche Zahlen gilt nun der folgende

Hauptsatz: Sind a, b relative Primzahlen, und ist k eine beliebige dritte Zahl, so ist jeder gemeinschaftliche Theiler der beiden Zahlen ak, b auch gemeinschaftlicher Theiler der beiden Zahlen k, b.

Um sich hiervon zu überzeugen, braucht man nur sämmtliche Gleichungen, die bei dem Algorithmus des grössten gemeinschaftlichen Divisors der Zahlen a, b gebildet werden, und deren vorletzte, da $h = 1$ ist, in unserm Falle $f = sg + 1$ lautet, mit k zu multipliciren; man erhält dann

$$ak = mbk + ck$$
$$bk = nck + dk$$
$$ck = pdk + ek$$
$$\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots$$
$$fk = sgk + k.$$

Ist nun δ irgend ein gemeinschaftlicher Divisor von ak und b, so geht δ auch in mbk, also auch in $ak - mbk = ck$ auf; es geht daher δ auch in nck und folglich auch in $bk - nck = dk$ auf. Und indem man diese Schlussweise fortsetzt, gelangt man zu dem Resultat, dass δ auch in fk, in gk, folglich auch in $fk - sgk = k$ aufgehen muss, was zu beweisen war.

Im Folgenden werden wir vorzüglich zwei specielle Fälle dieses Satzes gebrauchen, nämlich:

1. *Das Product zweier Zahlen a und k, deren jede relative Primzahl gegen eine dritte b ist, ist gleichfalls relative Primzahl zu b;* denn unserm Satze nach haben ak und b dieselben gemeinschaftlichen Divisoren, wie k und b; da aber k und b relative Primzahlen sind, so haben sie nur den einzigen gemeinschaftlichen Divisor 1; dasselbe gilt daher von ak und b, also sind diese Zahlen relative Primzahlen.

2. *Sind a und b relative Primzahlen, und ist ak durch b theilbar, so ist auch k durch b theilbar;* denn da der Annahme zufolge ak und b den gemeinschaftlichen Divisor b haben, so muss dem Hauptsatze nach b auch gemeinschaftlicher Divisor von k und b, also jedenfalls Divisor von k sein.

3. Den ersten dieser beiden Sätze kann man leicht verallgemeinern. Ist jede der Zahlen $a, b, c, d \ldots$ relative Primzahl gegen eine Zahl α, so ist auch ab, folglich auch das Product abc aus ab und c, folglich auch das Product $abcd$ aus abc und d u.s.f., kurz das Product $abcd \ldots$ aller jener Zahlen ebenfalls relative Primzahl gegen α. Allgemeiner, *hat man zwei Reihen von Zahlen*

$$a, b, c, d \ldots$$

und

$$\alpha, \beta, \gamma \ldots$$

von der Beschaffenheit, dass jede Zahl der einen Reihe relative Primzahl gegen jede Zahl der andern Reihe ist, so ist auch das Product abcd ... aller Zahlen der einen Reihe relative Primzahl

gegen das Product $\alpha\beta\gamma \ldots$ aller Zahlen der andern Reihe. Denn soeben ist bewiesen, dass jede der Zahlen α, β, $\gamma \ldots$ relative Primzahl gegen das Product $abcd \ldots$ ist, woraus durch nochmalige Anwendung desselben Satzes auch folgt, dass ihr Product $\alpha\beta\gamma \ldots$ ebenfalls relative Primzahl gegen $abcd \ldots$ ist.

4. Hieraus können wir wieder einen speciellen Fall ableiten, indem wir annehmen, dass die Zahlen b, c, $d \ldots$ identisch mit a, ferner die Zahlen β, $\gamma \ldots$ identisch mit α sind; wir erhalten dann das Resultat: *ist a relative Primzahl gegen α, so ist auch jede Potenz der Zahl a relative Primzahl gegen jede Potenz der Zahl α.*

Eine Anwendung hiervon macht man bei dem Beweise des Satzes, dass die $m$te Wurzel aus einer ganzen Zahl A entweder irrational oder selbst eine ganze Zahl ist; denn wenn jene Wurzel rational, d. h. von der Form $r:s$ ist, wo r und s ganze Zahlen bedeuten, die man ohne gemeinschaftlichen Divisor annehmen kann, so ergiebt sich aus $r^m = A\,s^m$, dass r^m durch s^m theilbar ist; da nun r und s, folglich auch r^m und s^m relative Primzahlen sind, so muss $s^m = 1$, also auch $s = 1$ sein; mithin ist jene Wurzel eine ganze Zahl r.

§. 6.

Die Aufgabe des §. 4 in der Weise verallgemeinert, dass für eine ganze Reihe gegebener Zahlen a, b, c, $d \ldots$ alle gemeinschaftlichen Divisoren gesucht werden, führt zu einem ganz ähnlichen Resultate. Es sei h der grösste gemeinschaftliche Divisor von a und b, so ist, wie wir früher fanden, jeder gemeinschaftliche Divisor von a und b auch Divisor von h und umgekehrt; jeder gemeinschaftliche Divisor der drei Zahlen a, b, c ist daher auch gemeinschaftlicher Divisor von h, c und umgekehrt; bezeichnet man daher mit k den grössten gemeinschaftlichen Divisor von h und c, so ist jede gleichzeitig in a, b, c aufgehende Zahl Divisor von k, und umgekehrt wird jeder Divisor von k auch Divisor der drei Zahlen a, b, c sein. Bildet man ferner den grössten gemeinschaftlichen Divisor l der beiden Zahlen k und d, so stimmen die gemeinschaftlichen Divisoren der vier Zahlen a, b, c, d vollständig überein mit den sämmtlichen Divisoren der Zahl l u. s. f. Wir haben daher das Resultat: *ist irgend eine Reihe von Zahlen a, b, c, $d \ldots$ gegeben, so giebt es stets eine — und natürlich auch nur*

eine — Zahl m von der Beschaffenheit, dass jede gleichzeitig in a, in b, in c, in d u. s. w. aufgehende Zahl auch in m aufgeht, und umgekehrt jeder Divisor von m auch Divisor jeder einzelnen der Zahlen $a, b, c, d \ldots$ *ist.* Diese vollkommen bestimmte Zahl m heisst deshalb wieder der *grösste gemeinschaftliche Divisor* der gegebenen Zahlen. (Eine Ausnahme hiervon tritt nur dann ein, wenn die gegebenen Zahlen *alle* $= 0$ sind.) Setzt man ferner $a = ma'$, $b = mb'$, $c = mc'$, $d = md' \ldots$, so sind $a', b', c', d' \ldots$ ganze Zahlen, deren grösster gemeinschaftlicher Theiler $= 1$ ist, oder, wie man kurz sagt, *Zahlen ohne gemeinschaftlichen Theiler.* Umgekehrt, wenn $a', b', c', d' \ldots$ Zahlen ohne gemeinschaftlichen Theiler sind, so leuchtet ein, dass m der grösste gemeinschaftliche Theiler der Zahlen $ma', mb', mc', md' \ldots$ ist.

Dagegen bemerken wir an dieser Stelle ein- für allemal, dass, wenn Zahlen $a, b, c, d \ldots$ *relative Primzahlen* genannt werden, darunter stets zu verstehen ist, dass *je zwei* von ihnen relative Primzahlen sind; solche Zahlen sind daher stets zugleich Zahlen ohne gemeinschaftlichen Theiler; aber Zahlen ohne gemeinschaftlichen Theiler sind nicht nothwendig relative Primzahlen.

§. 7.

Gewissermaassen das Umgekehrte der vorhergehenden ist die folgende Aufgabe: *Wenn eine Reihe von Zahlen* $a, b, c, d \ldots$ *gegeben ist, so sollen alle gemeinschaftlichen Multipla derselben, d. h. alle Zahlen gefunden werden, welche durch jede einzelne der gegebenen Zahlen theilbar sind.* Da von den gesuchten Zahlen zuerst gefordert wird, dass sie durch a theilbar sein sollen, so sind sie jedenfalls in der Form sa enthalten, wo s irgend eine ganze Zahl bedeutet. Ist nun δ der grösste gemeinschaftliche Divisor der beiden Zahlen $a = \delta a'$ und $b = \delta b'$, so sind a' und b' relative Primzahlen; soll daher $sa = sa'\delta$ theilbar sein durch $b = b'\delta$, so muss sa' durch b' und folglich (§. 5, 2.) auch s durch b' theilbar, also von der Form $s'b'$ sein, wo s' wieder irgend eine ganze Zahl bedeutet. Sämmtliche sowohl durch a als durch b theilbare Zahlen sind daher von der Form $sa = s'.a'b'\delta$, und umgekehrt leuchtet ein, dass alle in dieser Form enthaltenen Zahlen sowohl durch $a = a'\delta$ als durch $b = b'\delta$ theilbar sind.

Es zeigt sich also, dass die sämmtlichen gemeinschaftlichen

Multipla der beiden Zahlen a, b übereinstimmen mit den sämmtlichen Vielfachen *einer* bestimmten Zahl

$$a'b'\delta = \frac{ab}{\delta} = \mu,$$

welche man deshalb das *kleinste gemeinschaftliche Vielfache* der beiden Zahlen a, b nennt.

Um diesen Satz für eine beliebige Anzahl gegebener Zahlen $a, b, c, d \ldots$ zu verallgemeinern, braucht man nur zu bemerken, dass jedes gemeinschaftliche Vielfache der Zahlen

$$a, b, c, d \ldots$$

nothwendig auch ein gemeinschaftliches Vielfaches der Zahlen

$$\mu, c, d \ldots$$

ist und umgekehrt. Man wird daher zunächst das kleinste gemeinschaftliche Multiplum ν der beiden Zahlen μ und c suchen, dann das kleinste gemeinschaftliche Vielfache ϱ von ν und d u. s. f. Auf diese Weise leuchtet ein, dass sämmtliche gemeinschaftliche Multipla der gegebenen Zahlen $a, b, c, d \ldots$ übereinstimmen mit den sämmtlichen Vielfachen einer einzigen vollständig bestimmten Zahl ω, welche man deshalb das *kleinste gemeinschaftliche Vielfache* der gegebenen Zahlen nennt.

Von besonderer Wichtigkeit ist der Fall, in welchem die Zahlen $a, b, c, d \ldots$ relative Primzahlen sind. In diesem Falle ist zunächst $\delta = 1$, also ist das kleinste gemeinschaftliche Vielfache der beiden relativen Primzahlen a und b ihr Product ab. Da nun c wieder relative Primzahl gegen a und gegen b, also (§. 5, 1.) auch gegen ab ist, so ist abc das kleinste gemeinschaftliche Multiplum der drei Zahlen a, b, c u. s. f. Kurz, man erhält das Resultat: *Sind $a, b, c, d \ldots$ relative Primzahlen, so ist jede Zahl, welche durch jede einzelne derselben theilbar ist, auch durch ihr Product $abcd \ldots$ theilbar.*

§. 8.

Da jede Zahl sowohl durch die Einheit, als auch durch sich selbst theilbar ist, so hat jede Zahl — die Einheit selbst ausgenommen — mindestens zwei (positive) Divisoren. Jede Zahl nun, welche keine anderen als diese beiden Divisoren besitzt, heisst eine *Primzahl (numerus primus)*; es ist zweckmässig, die Einheit nicht

zu den Primzahlen zu rechnen, weil manche Sätze über Primzahlen nicht für die Zahl 1 gültig bleiben.

Aus dieser Erklärung ergiebt sich der Satz: *Wenn p eine Primzahl und a irgend eine ganze Zahl ist, so geht entweder p in a auf, oder p ist relative Primzahl zu a.* Denn der grösste gemeinschaftliche Divisor von p und a ist entweder p selbst oder die Einheit.

Hieraus folgt weiter: *Wenn ein Product aus mehreren Zahlen $a, b, c, d \ldots$ durch eine Primzahl p theilbar ist, so geht p mindestens in einem der Factoren $a, b, c, d \ldots$ auf.* Denn wäre keine einzige dieser Zahlen durch p theilbar, so wäre p relative Primzahl gegen jede einzelne von ihnen und folglich auch gegen ihr Product, was gegen die Annahme streitet, dass dies Product durch p theilbar ist.

Jede Zahl, welche ausser sich selbst und der Einheit noch andere Divisoren hat, heisst *zusammengesetzt (numerus compositus).* Diese Benennung wird gerechtfertigt durch folgenden

Fundamentalsatz: Jede zusammengesetzte Zahl lässt sich stets und nur auf eine einzige Weise als Product aus einer endlichen Anzahl von Primzahlen darstellen.

Beweis. Da jede zusammengesetzte Zahl m ausser 1 und m noch andere Divisoren hat, so sei a ein solcher; ist nun a keine Primzahl, also eine zusammengesetzte Zahl, so besitzt a ausser 1 und a noch andere Divisoren, z. B. b; ist b noch keine Primzahl, also zusammengesetzt, so hat b wieder mindestens einen Divisor c, der von 1 und b verschieden ist. Fährt man so fort, so muss man endlich einmal zu einer Primzahl gelangen; denn die Reihe der Zahlen $m, a, b, c \ldots$ ist eine abnehmende, sie kann also, da es nur eine endliche Anzahl von Zahlen giebt, welche kleiner als m sind, nur eine endliche Anzahl von Gliedern enthalten; das letzte Glied derselben muss aber eine Primzahl sein, denn sonst könnte man ja die Reihe noch weiter fortsetzen. Bezeichnet man diese Primzahl mit p, so ist, da jedes Glied der Reihe ein Multiplum des folgenden ist, die erste Zahl m auch ein Multiplum von der letzten p. Man kann daher

$$m = pm'$$

setzen. Nun ist m' entweder eine Primzahl — dann ist m schon als Product von Primzahlen dargestellt — oder m' ist zusammengesetzt; im letztern Falle muss es wieder eine in m' aufgehende Primzahl p' geben, so dass

$$m' = p'm'', \quad \text{also} \quad m = pp'm''$$

wird. Ist nun m'' noch keine Primzahl, so kann man auf dieselbe Weise fortfahren, bis man m als Product von lauter Primzahlen dargestellt hat. Dass dies wirklich nach einer endlichen Anzahl von ähnlichen Zerlegungen geschehen muss, leuchtet daraus ein, dass die Reihe der Zahlen m, m', m'' ... ebenfalls eine abnehmende und folglich eine endliche ist.

Hiermit ist der eine Haupttheil des Satzes erwiesen, welcher die Möglichkeit der Zerlegung behauptet; offenbar ist aber diese successive Ablösung von Primzahl-Factoren in mancher Beziehung willkürlich, und es bleibt daher noch nachzuweisen übrig, dass, auf welche Weise dieselbe auch ausgeführt sein mag, das Endresultat doch stets dasselbe sein muss. Nehmen wir daher an, man habe durch zwei verschiedene Anordnungen einmal

$$m = pp'p'' \ldots$$

ein anderes Mal

$$m = qq'q'' \ldots$$

gefunden, wo p, p', p'' ... und q, q', q'' ... sämmtlich Primzahlen bedeuten. Da nun das Product $pp'p''$ ... durch die Primzahl q theilbar ist, so muss mindestens einer der Factoren, z. B. p, durch q theilbar sein; p besitzt aber als Primzahl nur die beiden Divisoren 1 und p, und folglich muss $q = p$ sein, da q nicht $= 1$ ist. Hieraus folgt nun

$$p'p'' \ldots = q'q'' \ldots$$

und man kann auf dieselbe Weise zeigen, dass q' mit einer der Primzahlen p', p'' ..., z. B. mit p', identisch sein muss, woraus dann wieder

$$p'' \ldots = q'' \ldots$$

folgt. Auf diese Weise überzeugt man sich davon, dass jede Primzahl, welche bei der zweiten Art der Zerlegung ein oder mehrere Male als Factor auftritt, mindestens ebenso oft auch bei der ersten Zerlegung vorkommt; da aber ferner auf dieselbe Weise gezeigt werden kann, dass sie bei der zweiten Zerlegung mindestens ebenso oft vorkommt wie bei der ersten, so muss jede Primzahl in beiden Zerlegungen gleich oft als Factor vorkommen, und folglich stimmt der Complex aller Primzahlen bei der einen Zerlegung vollständig mit dem bei der andern überein.

Nachdem so der Satz in allen seinen Theilen bewiesen ist,

können wir die Darstellung der zusammengesetzten Zahl m noch dadurch vereinfachen, dass wir jedesmal alle unter einander identischen Primzahl-Factoren zu einer Potenz vereinigen. Es sei nämlich a eine von den in m aufgehenden Primzahlen, und zwar mag dieselbe genau αmal als Factor in der Zerlegung vorkommen, so vereinigen wir diese α Factoren zu der Potenz a^α; sind hierdurch noch nicht alle Factoren erschöpft, und ist b eine der übrigen Primzahlen, so bilden wir, wenn sie genau βmal vorkommt, die Potenz b^β, und in derselben Weise fahren wir fort, wenn hierdurch noch nicht alle Primzahl-Factoren von m erschöpft sind. Auf diese Weise überzeugt man sich, dass man jeder zusammengesetzten Zahl m die Form

$$m = a^\alpha b^\beta c^\gamma \ldots$$

geben kann, in welcher a, b, c die sämmtlichen unter einander verschiedenen, in m aufgehenden Primzahlen, und α, β, γ . . . ganze positive Zahlen bedeuten. Dass aber in dieser Form nicht nur alle zusammengesetzten, sondern auch alle Primzahlen enthalten sind, leuchtet unmittelbar ein.

Die Primzahlen bilden daher gewissermaassen das Material, aus welchem alle anderen Zahlen sich zusammensetzen lassen. *Dass es unendlich viele Primzahlen giebt*, hat schon *Euclid**) bewiesen, und zwar in folgender Art. Gesetzt es gäbe nur eine endliche Anzahl von Primzahlen, so würde eine von ihnen, die wir mit p bezeichnen wollen, die letzte, d. h. die grösste sein. Denken wir uns nun alle diese Primzahlen aufgeschrieben

$$2, 3, 5, 7, 11 \ldots p,$$

so müsste jede Zahl, welche grösser als p ist, zusammengesetzt und folglich durch mindestens eine dieser Primzahlen theilbar sein. Allein es ist sehr leicht, eine Zahl zu bilden, welche erstens grösser als p und zweitens durch keine jener Primzahlen theilbar ist; dazu bilden wir das Product aller Primzahlen von 2 bis p und vergrössern dasselbe um eine Einheit. Diese Zahl

$$z = 2.\,3.\,5 \ldots p + 1$$

ist in der That grösser als p, da ja schon $2p$ grösser als p ist; sie ist aber durch keine der Primzahlen theilbar, da z, durch jede derselben dividirt, immer den Rest 1 lässt. Damit ist also unsere

*) *Elemente*, Buch IX, Satz 20.

Annahme im Widerspruch, und folglich giebt es unendlich viele Primzahlen.

Dieser Satz ist nur ein specieller Fall des andern, dass in jeder unbegrenzten arithmetischen Progression, deren allgemeines Glied $kx + m$ ist, und in welcher das Anfangsglied m und die Differenz k relative Primzahlen sind, unendlich viele Primzahlen enthalten sind; allein, so einfach der Beweis für den speciellen Fall war, in welchem $k = 1$, so schwierig war es, einen strengen Beweis für den allgemeinen Satz zu geben, und dies ist bis jetzt nur durch Zuziehung von Principien gelungen, welche der Infinitesimalrechnung angehören *).

§. 9.

Durch den soeben bewiesenen Fundamentalsatz haben wir nun ein einfaches Kriterium gewonnen, nach welchem stets beurtheilt werden kann, ob eine Zahl m durch eine andere n theilbar ist oder nicht, sobald wir voraussetzen dürfen, dass beide in ihre Primfactoren zerlegt sind. Nehmen wir nämlich an, dass m durch n theilbar, dass also $m = nq$ ist, so leuchtet ein, dass jede in n aufgehende Primzahl auch in m aufgehen muss; es kann daher n keine anderen Primfactoren enthalten als m, und ausserdem kann auch ein solcher Primfactor nicht öfter in n als in m vorkommen; und umgekehrt, wenn jeder Primfactor der Zahl n mindestens ebenso oft in m vorkommt wie in n, so ist auch m durch n theilbar.

Sind daher $a, b, c \ldots$ die sämmtlichen von einander verschiedenen, in m aufgehenden Primzahlen, so dass

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots,$$

so ist jeder Divisor n dieser Zahl in der Form

$$n = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$$

enthalten, in welcher

α' irgend eine der $\alpha + 1$ Zahlen $0, 1, 2 \ldots \alpha$
β' „ „ „ $\beta + 1$ „ $0, 1, 2 \ldots \beta$
γ' „ „ „ $\gamma + 1$ „ $0, 1, 2 \ldots \gamma$
u. s. w.

*) Siehe die Supplemente VI. §. 132 bis 137.

bedeutet; und alle diese Zahlen n sind wirklich Divisoren von m. Hieraus gehen sogleich einige interessante Folgerungen hervor.

Zunächst leuchtet ein, da jede Combination eines Werthes von α' mit einem von β', mit einem von γ' u. s. w. einen Divisor von m liefert, und da je zwei verschiedenen solchen Combinationen (nach §. 8) auch zwei ungleiche Divisoren von m entsprechen, dass die Anzahl aller Divisoren von m gleich

$$(\alpha+1)\,(\beta+1)\,(\gamma+1)\ldots$$

ist; diese Anzahl hängt daher nur von den Exponenten $\alpha, \beta, \gamma \ldots$ ab, nicht aber von der Natur der in m aufgehenden Primzahlen a, b, c u. s. w.

Bildet man ferner das Schema

$$1,\ a,\ a^2 \ldots a^\alpha$$
$$1,\ b,\ b^2 \ldots b^\beta$$
$$1,\ c,\ c^2 \ldots c^\gamma$$
$$\text{u. s. w.}$$

und bildet alle Producte $a^{\alpha'}\, b^{\beta'}\, c^{\gamma'} \ldots$, indem man aus jeder dieser Horizontalreihen ein Glied $a^{\alpha'}$, $b^{\beta'}$, $c^{\gamma'} \ldots$ auswählt, so erhält man alle Divisoren der Zahl m, und zwar jeden nur ein einziges Mal. Die Summe aller dieser Divisoren erhält man daher nach derselben Regel, nach welcher man die einzelnen Aggregate

$$1+a+a^2+\ldots+a^\alpha = \frac{a^{\alpha+1}-1}{a-1}$$
$$1+b+b^2+\ldots+b^\beta = \frac{b^{\beta+1}-1}{b-1}$$
$$1+c+c^2+\ldots+c^\gamma = \frac{c^{\gamma+1}-1}{c-1}$$
$$\text{u. s. w.}$$

mit einander zu multipliciren hat; folglich ist die Summe aller Divisoren der Zahl m gleich dem Product

$$\frac{a^{\alpha+1}-1}{a-1}\cdot\frac{b^{\beta+1}-1}{b-1}\cdot\frac{c^{\gamma+1}-1}{c-1}\cdots$$

Nehmen wir z. B. $m = 60 = 2^2 . 3 . 5$, so sind die sämmtlichen Divisoren folgende:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60;$$

ihre Anzahl ist

$$(2+1)\,(1+1)\,(1+1) = 12$$

und ihre Summe

$$\frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1}\cdot\frac{5^2-1}{5-1}=7.4.6=168.$$

§. 10.

Wir kehren nun zu einigen früheren Aufgaben zurück, zunächst zu derjenigen (§. 6), den grössten gemeinschaftlichen Divisor einer Reihe von Zahlen zu bilden, jetzt unter der Voraussetzung, dass ihre Zerlegungen in Primfactoren gegeben sind. Man betrachte alle Primzahlen, welche in diesen Zerlegungen vorkommen, und scheide zunächst diejenigen unter ihnen aus, welche in einer oder mehreren der gegebenen Zahlen gar nicht als Primfactoren enthalten sind. Bleibt auf diese Weise gar keine Primzahl übrig, so ist die Einheit der gesuchte grösste gemeinschaftliche Divisor. Im entgegengesetzten Fall sei a eine Primzahl, welche bei dieser vorläufigen Ausscheidung zurückgeblieben ist und also in jeder der gegebenen Zahlen mindestens einmal enthalten ist; man zähle, wie oft a als Primfactor in jeder einzelnen der gegebenen Zahlen vorkommt, und nehme die kleinste dieser Anzahlen, die wir mit α bezeichnen, so dass a in mindestens einer der gegebenen Zahlen genau α mal, in allen übrigen aber mindestens ebenso oft als Primfactor vorkommt. Aehnlich verfahre man mit den übrigen Primzahlen b, c . . ., sofern diese noch nicht erschöpft sind, und bilde für jede, für b die Anzahl β, für c die Anzahl γ u. s. w. nach derselben Regel, nach welcher für die Primzahl a die Anzahl α gebildet wurde. Dann ist

$$a^\alpha b^\beta c^\gamma \ldots$$

der gesuchte grösste gemeinschaftliche Divisor. Der Beweis für diese Regel leuchtet unmittelbar dadurch ein, dass der grösste gemeinschaftliche Divisor keine anderen Primfactoren enthalten kann, als solche, welche in jeder der gegebenen Zahlen enthalten sind, und dass er keinen Primfactor öfter enthalten kann, als irgend eine der gegebenen Zahlen.

Aehnlich gestaltet sich die Lösung der anderen Aufgabe, das kleinste gemeinschaftliche Multiplum einer Reihe von gegebenen Zahlen zu bilden (§. 7). Jetzt betrachte man *jede* Primzahl, die in irgend einer der gegebenen Zahlen als Factor enthalten ist, und sehe nach, in welcher sie am häufigsten vorkommt; ebenso oft

nehme man sie als Factor in das kleinste gemeinschaftliche Multiplum auf; sind aber a, b, c . . . die sämmtlichen Primzahlen, welche in den einzelnen Zerlegungen der gegebenen Zahlen vorkommen, so erhält man nach dieser Regel das gesuchte kleinste gemeinschaftliche Multiplum in der Form

$$a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots,$$

wo z. B. der Exponent α' dadurch bestimmt ist, dass die Primzahl a in mindestens einer der gegebenen Zahlen genau α' mal, in allen übrigen aber nicht öfter als Factor enthalten ist. Der Beweis liegt hier darin, dass die gesuchte Zahl jeden Primfactor enthalten muss, der in einer der gegebenen Zahlen enthalten ist, und zwar mindestens ebenso oft, als diese.

Endlich können wir aus den vorhergehenden Principien noch ein Kriterium ableiten, nach welchem zu erkennen ist, ob eine Zahl

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots$$

eine genaue $r$te Potenz einer ganzen Zahl k ist. Dazu ist offenbar erforderlich und hinreichend, dass alle Exponenten $\alpha, \beta, \gamma \ldots$ durch r theilbar sind, wie man sogleich aus der Annahme

$$m = k^r$$

erkennt.

§. 11.

Wir gehen nun zu einer Untersuchung über, welche an sich schon interessant und ausserdem für die Folge von der grössten Wichtigkeit ist. Denken wir uns einmal alle ganzen Zahlen

$$1, 2, 3, 4 \ldots m$$

bis zu einer beliebigen letzten m aufgeschrieben, und zählen wir ab, wie viele von ihnen relative Primzahlen gegen die letzte m sind. Diese Anzahl bezeichnet man in der Zahlentheorie durchgängig mit $\varphi(m)$, wo der Buchstabe φ die Rolle eines Functionszeichens spielt*). Da die Einheit relative Primzahl gegen sich selbst ist, so folgt zunächst

$$\varphi(1) = 1;$$

durch wirkliches Abzählen findet man ferner

*) *Gauss: Disquisitiones Arithmeticae* art. 38.

$$\varphi(2) = 1,\ \varphi(3) = 2,\ \varphi(4) = 2,\ \varphi(5) = 4$$

u. s. w. Allein es kommt darauf an, einen allgemeinen Ausdruck für die Function $\varphi(m)$ zu finden, und wir werden sehen, dass man zu diesem Zweck nur die sämmtlichen von einander verschiedenen Primzahlen $a, b, c \ldots$ zu kennen braucht, welche in m aufgehen. Unsere Aufgabe ist nämlich identisch mit dieser: die Anzahl der obigen Zahlen zu bestimmen, welche durch keine dieser Primzahlen $a, b, c \ldots$ theilbar sind; und diese ist wieder nur ein specieller Fall der folgenden:

Wenn $a, b, c \ldots$ relative Primzahlen sind und sämmtlich in einer Zahl m aufgehen, so soll die Anzahl derjenigen der Zahlen

$$1, 2, 3 \ldots m \qquad (M)$$

bestimmt werden, welche durch keine der Zahlen $a, b, c \ldots$ theilbar sind.

Es zeigt sich nun, wie es häufig geschieht, dass die allgemeinere Aufgabe leichter zu lösen ist, als der direct angegriffene specielle Fall. Zu diesem Zweck scheiden wir zunächst aus dem Zahlencomplex (M) alle diejenigen aus, welche durch die Zahl a theilbar sind; es sind dies offenbar die Zahlen

$$a, 2a, 3a \ldots \frac{m}{a} a;$$

die Anzahl derselben ist $m : a$; es bleiben daher, nachdem dieselben aus dem Complex (M) ausgeschieden sind, nur

$$m - \frac{m}{a} = m\left(1 - \frac{1}{a}\right) \qquad (1)$$

Zahlen übrig, welche nicht durch a theilbar sind, und deren Complex wir mit (A) bezeichnen wollen.

Aus diesem Complex (A) sind nun zunächst alle durch b theilbaren Zahlen auszuscheiden; es sind dies offenbar alle diejenigen Zahlen des Complexes (M), welche der doppelten Forderung genügen, erstens dass sie nicht durch a, zweitens dass sie durch b theilbar sind. Alle Zahlen nun, welche der zweiten Forderung genügen, sind die folgenden

$$b, 2b, 3b, \ldots \frac{m}{b} b;$$

damit aber eine dieser Zahlen, z. B. rb, auch der ersten Forderung genüge, ist erforderlich und hinreichend, dass der Coefficient r

nicht durch a theilbar sei; denn da der Annahme nach a und b relative Primzahlen sind, so ist rb theilbar oder nicht theilbar durch a, je nachdem r durch a theilbar ist oder nicht (§. 5, 2.). Die Anzahl der noch aus dem Complex (A) auszuscheidenden Zahlen stimmt daher überein mit der Anzahl derjenigen der Zahlen

$$1, 2, 3 \ldots \frac{m}{b},$$

welche nicht durch a theilbar sind. Da nun m durch a und b, folglich auch durch ab theilbar ist, so ist die letzte dieser Zahlen $m : b$ theilbar durch a; unsere Frage ist also dieselbe für die Zahl $m : b$ wie diejenige, welche wir durch den ersten Schritt für die Zahl m gelöst und durch die Formel (1) beantwortet haben. Die Anzahl der aus (A) auszuscheidenden Zahlen ist daher gleich

$$\frac{m}{b}\left(1-\frac{1}{a}\right)$$

und wir erhalten

$$m\left(1-\frac{1}{a}\right)-\frac{m}{b}\left(1-\frac{1}{a}\right)=m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right) \qquad (2)$$

als Anzahl derjenigen im Complex (A) enthaltenen Zahlen, welche nicht durch b theilbar sind, oder, was dasselbe ist, als Anzahl derjenigen in (M) enthaltenen Zahlen, welche weder durch a noch durch b theilbar sind.

Bezeichnen wir den Complex dieser Zahlen mit (B), so kann man in derselben Weise fortfahren und gelangt so durch Induction zu dem Resultat, dass die Anzahl derjenigen in (M) enthaltenen Zahlen (K), welche durch keine der Zahlen $a, b, c \ldots k$ theilbar sind, gleich

$$m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots\left(1-\frac{1}{k}\right) \qquad (3)$$

ist. Um die Allgemeingültigkeit dieses Gesetzes nachzuweisen, nehmen wir an, dass die Richtigkeit desselben für die Zahlen $a, b, c \ldots k$ schon bewiesen sei, und untersuchen, was geschieht, wenn zu denselben noch eine andere l hinzukommt, wobei natürlich wieder vorausgesetzt wird, erstens dass l in m aufgeht, zweitens dass l relative Primzahl gegen jede der vorhergehenden Zahlen $a, b, c \ldots k$ ist.

Um die Anzahl aller in (M) enthaltenen Zahlen zu bestimmen, welche durch keine der Zahlen $a, b, c \ldots k, l$ theilbar sind, haben

wir aus dem Complex (K) derjenigen Zahlen, welche durch keine der Zahlen $a, b, c \ldots k$ theilbar sind, und deren Anzahl durch die Formel (3) gegeben ist, nur noch die auszuscheiden, welche durch l theilbar sind; es sind dies alle diejenigen in (M) enthaltenen Zahlen, welche erstens nicht theilbar durch $a, b, c \ldots k$, zweitens theilbar durch l sind. Alle durch l theilbaren Zahlen des Complexes (M) sind diese

$$l, 2l, 3l \ldots \frac{m}{l} l,$$

und damit irgend eine derselben, z. B. rl, durch keine der Zahlen $a, b \ldots k$ theilbar sei, ist erforderlich und hinreichend, dass der Coefficient r dieselbe Eigenschaft habe. Die Anzahl der auszuscheidenden Zahlen stimmt daher überein mit der Anzahl derjenigen unter den Zahlen

$$1, 2, \ldots \frac{m}{l},$$

welche durch keine der Zahlen $a, b \ldots k$ theilbar sind; diese ist aber nach der als richtig vorausgesetzten Formel (3) gleich

$$\frac{m}{l}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right);$$

nach Ausscheidung derselben aus dem Complex (K) bleiben daher

$$\begin{aligned} &m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right) \\ &-\frac{m}{l}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right) \\ &=m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{l}\right) \end{aligned}$$

Zahlen übrig, nämlich diejenigen, welche durch keine der Zahlen $a, b, c \ldots k, l$ theilbar sind.

Hiermit ist die Allgemeingültigkeit unseres Satzes bewiesen; kehren wir nun zu unserer ursprünglichen Aufgabe zurück, so erhalten wir das Resultat*):

---

*) *Euler*: *Theoremata arithmetica nova methodo demonstrata*, Comm. nov. Ac. Petrop. VIII. p. 74. *Speculationes circa quasdam insignes proprietates numerorum*, Acta Petrop. IV, 2. p. 18. — Eine höchst werthvolle Sammlung der arithmetischen Abhandlungen *Euler's* ist von den Brüdern *Fuss* unter folgendem Titel herausgegeben: *Leonhardi Euleri Commentationes Arithmeticae Collectae*. Petropoli 1849. 2 tom.

Sind $a, b \ldots k, l$ die sämmtlichen von einander verschiedenen in m aufgehenden Primzahlen, so ist

$$\varphi(m) = m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\cdots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{l}\right)$$

die Anzahl aller derjenigen der Zahlen

$$1, 2 \ldots m,$$

welche relative Primzahlen gegen die letzte m sind.

Denn damit irgend eine Zahl relative Primzahl gegen m sei, ist erforderlich und hinreichend, dass sie durch keine der in m aufgehenden absoluten Primzahlen theilbar sei.

Wir können dem gefundenen Ausdruck eine andere Form geben, indem wir m als Product von Primzahl-Potenzen darstellen; da $a, b, c \ldots$ die sämmtlichen von einander verschiedenen in m aufgehenden Primzahlen sind, so hat m die Form

$$m = a^\alpha b^\beta c^\gamma \ldots,$$

und es wird

$$\varphi(m) = (a-1)\, a^{\alpha-1} \cdot (b-1)\, b^{\beta-1} \cdot (c-1)\, c^{\gamma-1} \ldots$$

Um unsern Satz an einem Beispiel zu prüfen, wählen wir $m = 60$; die sämmtlichen Zahlen, welche nicht grösser als 60 und relative Primzahlen gegen 60 sind, bilden die Reihe

1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59,

und ihre Anzahl ist $= 16$; in der That finden wir nach der obigen Formel, da 2, 3, 5 sämmtliche in 60 aufgehende Primzahlen sind,

$$\varphi(60) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16.$$

§. 12.

Aus der gefundenen Form der Function $\varphi(m)$ geht auch noch folgender Satz hervor: *Sind m und m' zwei relative Primzahlen, so ist*

$$\varphi(mm') = \varphi(m)\, \varphi(m').$$

Denn sind $a, b, c \ldots$ sämmtliche in m, und $a', b', c' \ldots$ sämmtliche in m' aufgehende Primzahlen, so stimmt, da m und m' relative Primzahlen sind, keine Primzahl der einen Reihe mit einer der andern überein, d. h. alle Primzahlen

$$a, b, c \ldots \quad a', b', c' \ldots$$

sind von einander verschieden. Sie gehen ferner sämmtlich in dem Product mm' auf, und umgekehrt muss jede in mm' aufgehende Primzahl, da sie in einem der beiden Factoren m, m' aufgehen muss, mit einer dieser Primzahlen übereinstimmen. Also sind dies die sämmtlichen von einander verschiedenen in mm' aufgehenden Primzahlen; hieraus folgt

$$\varphi(mm') = mm' \left\{ \begin{matrix} \left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots \\ \left(1-\frac{1}{a'}\right)\left(1-\frac{1}{b'}\right)\left(1-\frac{1}{c'}\right)\cdots \end{matrix} \right\}$$

Da nun andererseits

$$\varphi(m) = m\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\cdots$$

und

$$\varphi(m') = m'\left(1-\frac{1}{a'}\right)\left(1-\frac{1}{b'}\right)\left(1-\frac{1}{c'}\right)\cdots$$

ist, so ergiebt sich durch den unmittelbaren Anblick die Richtigkeit des zu beweisenden Satzes.

So ist z. B.

$$\varphi(60) = \varphi(4 \,.\, 15) = \varphi(4)\,\varphi(15) = 2 \,.\, 8 = 16.$$

Uebrigens leuchtet ein, dass der soeben bewiesene Satz ohne Weiteres auf ein Product aus beliebig vielen Zahlen m, m', m'' ... ausgedehnt werden kann, welche sämmtlich unter einander relative Primzahlen sind; denn es ist z. B.

$$\varphi(mm'm'') = \varphi(m)\ \varphi(m'm'') = \varphi(m)\ \varphi(m')\ \varphi(m'')$$

und ähnlich für eine grössere Anzahl von Factoren.

§. 13.

Die Aufgabe, den Werth der Function $\varphi(m)$ zu bestimmen, ist eigentlich nur ein specieller Fall von der folgenden:

Wenn δ irgend ein Divisor der Zahl $m = n\delta$ ist, so soll die Anzahl derjenigen der Zahlen

$$1,\ 2,\ 3 \ldots m$$

bestimmt werden, welche mit m den grössten gemeinschaftlichen Divisor δ haben.

Wir können dieselbe sogleich auf den frühern speciellen Fall

zurückführen. Zunächst leuchtet nämlich ein, dass die Zahlen, um welche es sich handelt, unter den Vielfachen von δ, also unter den Zahlen

$$\delta, 2\delta, 3\delta, \ldots n\delta$$

zu suchen sind. Damit nun δ der grösste gemeinschaftliche Divisor von $m = n\delta$ und einer Zahl von der Form $r\delta$ sei, ist erforderlich und hinreichend, dass der Coefficient r relative Primzahl gegen n sei; die gesuchte Anzahl ist daher zugleich die Anzahl derjenigen der Zahlen

$$1, 2, 3 \ldots n,$$

welche relative Primzahlen gegen die letzte n derselben sind; diese Anzahl ist folglich $= \varphi(n)$. Offenbar geht diese allgemeinere Aufgabe wieder in die frühere über, wenn der Divisor $\delta = 1$ ist.

Aus der Lösung dieser Aufgabe lässt sich nun ein schöner Satz über die Function $\varphi(m)$ ableiten, der in späteren Untersuchungen eine grosse Rolle spielt. Schreiben wir einmal alle Divisoren

$$\delta', \delta'', \delta''' \ldots$$

der Zahl

$$m = n'\delta' = n''\delta'' = n'''\delta''' = \ldots$$

auf, und theilen wir alle m Zahlen

$$1, 2, 3 \ldots m$$

in ebenso viele Gruppen ein, als es Divisoren δ von m giebt, indem wir alle die Zahlen, welche mit m den grössten gemeinschaftlichen Divisor δ' haben, und deren Anzahl nach dem Vorhergehenden $= \varphi(n')$ ist, in die erste Gruppe, ebenso alle die $\varphi(n'')$ Zahlen, welche mit m den grössten gemeinschaftlichen Divisor δ'' haben, in die zweite Gruppe aufnehmen u. s. f. So leuchtet ein, dass jede der m Zahlen in eine, aber auch nur in eine solche Gruppe aufgenommen wird, und es muss daher das Aggregat der Zahlen

$$\varphi(n'), \varphi(n''), \varphi(n''') \ldots$$

welche angeben, wie viele Zahlen der ersten, zweiten, dritten u. s. w. Gruppe angehören, mit der Anzahl m der sämmtlichen in diese Gruppen vertheilten Zahlen übereinstimmen. Da nun die Zahlen $n', n'', n''' \ldots$ die sämmtlichen Divisoren der Zahl m bilden, so erhalten wir folgenden Satz*):

*) *Gauss: D. A.* art. 39.

Durchläuft n alle Divisoren einer Zahl m, so ist die entsprechende Summe

$$\Sigma \varphi(n) = m.$$

Es wird gut sein, diesen Satz wieder an einem Beispiel zu prüfen. Nehmen wir $m = 60$, so sind die Zahlen

$$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$$

die sämmtlichen Divisoren n von 60. Nun ist

$$\begin{array}{llllllll} \varphi(1) & = 1, & \varphi(2) & = 1, & \varphi(3) & = 2, & \varphi(4) & = 2, \\ \varphi(5) & = 4, & \varphi(6) & = 2, & \varphi(10) & = 4, & \varphi(12) & = 4, \\ \varphi(15) & = 8, & \varphi(20) & = 8, & \varphi(30) & = 8, & \varphi(60) & = 16; \end{array}$$

uud die Summe aller dieser Zahlen ist in der That $= 60$.

§. 14.

Der soeben gegebene Beweis dieses wichtigen Satzes über die Function $\varphi(m)$ ergab sich unmittelbar aus dem Begriff dieser Function ohne Hülfe der vorher für dieselbe gefundenen Form und ohne alle Rechnung*); es wird aber gut sein, noch einen zweiten Beweis hinzuzufügen, welcher mehr rechnend zu Werke geht und die früher abgeleitete Form der Function und die daraus gezogenen Folgerungen voraussetzt.

Jeder Divisor n der Zahl

$$m = a^{\alpha} b^{\beta} c^{\gamma} \ldots$$

hat die Form

$$n = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$$

wo wie früher $a, b, c \ldots$ von einander verschiedene Primzahlen bedeuten. Da also $a^{\alpha'}, b^{\beta'}, c^{\gamma'} \ldots$ unter einander relative Primzahlen sind, so ist

$$\varphi(n) = \varphi(a^{\alpha'}) \cdot \varphi(b^{\beta'}) \, \varphi(c^{\gamma'}) \ldots$$

Um nun alle Divisoren n der Zahl m zu erhalten, muss man

*) Dieser Satz charakterisirt umgekehrt die Function $\varphi(m)$ vollständig, so dass aus ihm auch die (in §. 11 gefundene) Form derselben abgeleitet werden kann; siehe die Supplemente VII, §. 188.

α' die Zahlen $0, 1, 2 \ldots \alpha$
β' „ „ $0, 1, 2 \ldots \beta$
γ' „ „ $0, 1, 2 \ldots \gamma$
u. s. w.

durchlaufen lassen. Bildet man nun das Aggregat aller entsprechenden Werthe $\varphi(n)$, so leuchtet ein, dass dasselbe mit dem Product aus den folgenden Summen

$$\varphi(1) + \varphi(a) + \varphi(a^2) + \cdots + \varphi(a^\alpha)$$
$$\varphi(1) + \varphi(b) + \varphi(b^2) + \cdots + \varphi(b^\beta)$$
$$\varphi(1) + \varphi(c) + \varphi(c^2) + \cdots + \varphi(c^\gamma)$$
u. s. w.

übereinstimmt. Die erste dieser Summen ist aber gleich

$$1 + (a-1) + (a-1)\,a + \cdots + (a-1)\,a^{\alpha-1}$$
$$= 1 + (a^\alpha - 1) = a^\alpha;$$

ebenso ist b^β die zweite, c^γ die dritte Summe u. s. f. Es ergiebt sich daher, dass das Aggregat

$$\Sigma\,\varphi(n) = a^\alpha \cdot b^\beta \cdot c^\gamma \ldots = m$$

ist, was zu beweisen war.

§. 15.

Wir wenden uns nun noch zu einer Aufgabe, deren Lösung zu einem rein arithmetischen Beweise eines Satzes führt, welcher sonst gewöhnlich durch andere Betrachtungen erwiesen wird. Es handelt sich darum, wenn m eine beliebige ganze Zahl und p eine beliebige Primzahl ist, den Exponenten der höchsten Potenz von p zu bestimmen, welche in der Facultät

$$m! = 1 \cdot 2 \cdot 3 \ldots m$$

aufgeht. Bezeichnen wir mit m' die grösste in dem Bruch $m : p$ enthaltene ganze Zahl, so sind unter den m Factoren von $m!$ nur die folgenden m' durch p theilbar

$$p, 2p, 3p \ldots m'p;$$

und da die übrigen Factoren bei unserer Frage keine Rolle spielen, so stimmt der gesuchte Exponent mit dem Exponenten der höchsten Potenz von p überein, welche in dem Product

$$1 \cdot 2 \ldots m' \cdot p^{m'}$$

dieser Multipla von p aufgeht, und ist daher gleich der Summe aus m' und dem Exponenten der höchsten Potenz von p, welche in der Facultät

$$m'! = 1 \cdot 2 \ldots m'$$

aufgeht. Hieraus ergiebt sich unmittelbar, dass der gesuchte Exponent gleich

$$m' + m'' + m''' + \cdots$$

ist, wo m'', m''' ... die grössten in den Brüchen $m' : p$, $m'' : p$ ... enthaltenen ganzen Zahlen bedeuten. Offenbar ist die Reihe der Zahlen m', m'', m''' ... eine abnehmende und folglich eine endliche; der gesuchte Exponent wird $= 0$ sein, wenn $p > m$ ist; denn dann ist schon $m' = 0$. Es mag beiläufig noch bemerkt werden, dass die Zahlen m', m'', m''' ... auch die grössten resp. in den Brüchen $m : p$, $m : p^2$, $m : p^3$ ... enthaltenen ganzen Zahlen sind; ist nämlich r die grösste in $m : a$, und s die grösste in $r : b$ enthaltene ganze Zahl, so ist s auch stets die grösste in $m : ab$ enthaltene ganze Zahl.

Ist z. B. $m = 60$ und $p = 7$, so ist die grösste in

$$\frac{60}{7} \text{ enthaltene ganze Zahl } m' = 8$$

und die grösste in

$$\frac{8}{7} \text{ oder in } \frac{60}{49} \text{ enthaltene ganze Zahl } m'' = 1$$

und die grösste in

$$\frac{1}{7} \text{ oder in } \frac{60}{243} \text{ enthaltene ganze Zahl } m''' = 0;$$

also ist

$$7^{8+1} = 7^9$$

die höchste Potenz von 7, welche in der Facultät $60!$ aufgeht.

Durch das so gewonnene Resultat sind wir in den Stand gesetzt, folgenden Satz zu beweisen: *Ist*

$$m = f + g + h + \cdots,$$

so ist

$$\frac{m!}{f!\, g!\, h! \ldots}$$

eine ganze Zahl.

Denn wenn p irgend eine im Nenner aufgehende Primzahl ist, und wenn wir eine der frühern analoge Bezeichnung beibehalten, so sind

$$f' + f'' + f''' + \cdots$$
$$g' + g'' + g''' + \cdots$$
$$h' + h'' + h''' + \cdots$$
u. s. w.

die Exponenten der höchsten Potenzen von p, welche resp. in $f!$, in $g!$, in $h!$ u. s. w. aufgehen, und folglich ist

$$(f' + g' + h' + \cdots) + (f'' + g'' + h'' + \cdots) + (f''' + g''' + h''' + \cdots) + \cdots$$

der Exponent der höchsten Potenz von p, welche in dem ganzen Nenner aufgeht. Andererseits ist

$$m' + m'' + m''' + \cdots$$

der Exponent der höchsten im Zähler aufgehenden Potenz von p; es ist daher nur zu zeigen, dass die letztere Summe nicht kleiner ist als die erstere. Da nun

$$\frac{m}{p} = \frac{f}{p} + \frac{g}{p} + \frac{h}{p} + \cdots$$

ist, so leuchtet unmittelbar ein, dass

$$m' \geqq f' + g' + h' + \cdots$$

sein muss; hieraus folgt aber wieder

$$\frac{m'}{p} \geqq \frac{f'}{p} + \frac{g'}{p} + \frac{h'}{p} + \cdots$$

also *a fortiori*

$$m'' \geqq f'' + g'' + h'' + \cdots$$

u. s. f., woraus die Richtigkeit der obigen Behauptung erhellt. Da nun jede im Nenner aufgehende Primzahl mindestens ebenso oft im Zähler aufgeht, so ist der Zähler theilbar durch den Nenner, der Bruch selbst also wirklich eine ganze Zahl.

Hieraus folgt auch, dass jedes Product von m successiven ganzen Zahlen

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

stets durch das Product der ersten m ganzen Zahlen

$$m! = 1 \cdot 2 \cdot 3 \ldots (m-1)\,m$$

theilbar ist; denn der Quotient

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

ist gleich

$$\frac{(a+m)!}{a!\;m!}$$

und folglich eine ganze Zahl.

§. 16.

Hiermit beschliessen wir die Reihe der Sätze über die Theilbarkeit der Zahlen; aber es ist wohl der Mühe werth, an dieser Stelle noch einen Rückblick auf den Entwicklungsgang dieser unserer bisherigen Untersuchungen zu werfen. Da beobachten wir nun vor allen Dingen, dass das ganze Gebäude auf *einem* Fundament ruht, nämlich auf dem Algorithmus, welcher dazu dient, den grössten gemeinschaftlichen Theiler zweier Zahlen aufzufinden. Dass alle nachfolgenden Sätze, wenn sie sich auch zum Theil auf erst später eingeführte Begriffe, wie die der relativen und absoluten Primzahlen, beziehen, doch nur einfache Consequenzen aus dem Resultat jener ersten Untersuchung sind, ist so evident, dass man unmittelbar zu der Behauptung berechtigt wird: in jeder analogen Theorie, in welcher ein dem Algorithmus des grössten gemeinschaftlichen Divisors ähnlicher Algorithmus existirt, muss auch ein System von Folgerungen Statt finden, welches dem in unserer Theorie entwickelten ganz analog ist. In der That giebt es solche Theorieen; betrachtet man z. B. alle in der Form

$$t + u\sqrt{-a}$$

enthaltenen Zahlen, in welcher a eine bestimmte positive, t und u dagegen unbestimmte reelle ganze Zahlen bedeuten, und nennt dieselben ganze complexe Zahlen oder kurz ganze Zahlen, so kann man den Begriff des Vielfachen so fassen, dass eine solche Zahl ein Vielfaches von einer zweiten heisst, wenn die erste ein Product aus der zweiten und irgend einer dritten solchen Zahl ist. Aber nur für gewisse besondere Werthe von a, z. B. für $a = 1$, lässt sich die Frage nach den gemeinschaftlichen Divisoren zweier Zahlen durch einen endlich abschliessenden Algorithmus beantworten, der dem in unserer reellen Theorie ganz ähnlich ist; es findet daher in der Theorie der Zahlen von der Form $t + u\sqrt{-1}$ auch durchgängige Analogie mit unserer Theorie der reellen Zahlen Statt. Ganz anders verhält es sich, wenn z. B. $a = 11$ ist; in der Theorie der Zahlen von der Form $t + u\sqrt{-11}$ findet unter andern der Satz nicht mehr Statt, dass eine Zahl nur auf eine einzige Weise als Product von nicht weiter zerlegbaren Zahlen dargestellt werden kann; so z. B. lässt sich die Zahl 15 einmal als $3 \cdot 5$, ein

anderes Mal als $(2+\sqrt{-11})\,(2-\sqrt{-11})$ darstellen, obgleich jede der vier Zahlen

$$3,\quad 5,\quad 2+\sqrt{-11},\quad 2-\sqrt{-11}$$

nicht weiter in Factoren von der Form $t+u\sqrt{-11}$ zerlegbar ist. Der Grund dieser interessanten Erscheinung liegt allein darin, dass es bei den Zahlen dieser Form nicht mehr gelingt, einen nach einer endlichen Anzahl von Operationen abschliessenden Algorithmus zur Auffindung der gemeinschaftlichen Divisoren zweier Zahlen zu bilden*).

*) Die Einführung der ganzen complexen Zahlen von der Form $t+u\sqrt{-1}$ rührt von *Gauss* her; eine kurze Darstellung der Elemente dieser neuen Zahlentheorie findet man in seiner Abhandlung *Theoria residuorum biquadraticorum* II, oder in einer Abhandlung von *Dirichlet: Recherches sur les formes quadratiques à coëfficients et à indéterminées complexes* (Crelle's Journal XXIV). Das oben erwähnte abweichende Verhalten anderer Zahlformen hat *Kummer* zur Einführung der *idealen* Zahlen veranlasst (Crelle's Journal XXXV).