Verheltnis der Theilbarkeit unter den Zahlen

In: Bernard Bolzano (author); Karel Rychlík (other): Bernard Bolzano's Schriften. Band 2. Zahlentheorie. (German). Praha: Královská česká společnost nauk v Praze, 1931. pp. 3–57.

Persistent URL: http://dml.cz/dmlcz/400163

Terms of use:

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://dml.cz

VERHÄLTNISS DER THEILBARKEIT UNTER DEN ZAHLEN.

§. 1. Uibergang. Auch der Begriff der Division leitet auf viele sehr merkwürdige Verhältnisse zwischen den Zahlen, welche zum Vorschein kommen, sobald wir nur derselben mehrere vergleichen, wie das Nachfolgende zeigt.

§. 2. Erklärung. Wenn mehrere wirkliche Zahlen $a, b, c, d, \ldots$ sich als Factoren betrachten lassen, welche durch Multiplication mit gewissen anderen eine und eben dieselbe wirkliche Zahl M hervorbringen, oder was eben soviel heißt, wenn die Zahl M als theilbar durch die gesammten Zahlen $a, b, c, d, \ldots$ betrachtet werden kann: so sagen wir, M sey ein gemeinschaftliches Vielfache der Zahlen $a, b, c, d, \ldots$ So ist z. B. 60 ein gemeinschaftliches Vielfache der Zahlen 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60. Und wenn die Zahl M die kleinste Zahl ist, die sich als solch ein gemeinschaftliches Vielfache der gegebenen $a, b, c, d, \ldots$ betrachten läßt: d. h. wenn es keine kleinere Zahl gibt, die so beschaffen ist, daß sie durch jede der Zahlen $a, b, c, d, \ldots$ getheilt werden könnte; so nennen wir M das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, d, \ldots$ Wenn sich im Gegentheil mehrere wirkliche Zahlen $A, B, C, D, \ldots$ ansehen lassen als Producte, deren ein Factor die wirkliche Zahl m ist, oder was ebensoviel sagt, wenn die Zahl m die sämmtlichen Zahlen $A, B, C, D, \ldots$ theilt: so sagen wir, m sey ein gemeinschaftlicher Theiler oder auch ein gemeinschaftliches Maß der Zahlen $A, B, C, D, \ldots$ So ist z. B. 6 ein gemeinschaftlicher Theiler der Zahlen 6, 12, 18, 24. Und wenn die Zahl m die größte ist, die sich als ein gemeinschaftlicher Theiler der Zahlen $A, B, C, D, \ldots$ betrachten läßt, d. h. wenn es keine größere Zahl gibt, die als ein Factor jeder der Zahlen $A, B, C, D, \ldots$ angesehen werden kann: so sagen wir, m sey der größte gemeinschaftliche Theiler der Zahlen $A, B, C, D, \ldots$

§. 3. Lehrsatz. Keine wirkliche Zahl läßt sich als ein Product aus einer unendlichen Menge wirklicher Zahlen, die alle > 1 sind, betrachten.

Beweis. Schon früher (§.) wurde erwiesen, daß ein Product aus n wirklichen Zahlen, deren jede einzeln >1 ist, $>n$ sey. Wenn also die Menge der Factoren größer als eine jede gegebene Zahl seyn sollte: so müßte auch das Product größer als eine jede gegebene Zahl seyn.

§. 4. Zusatz. Also hat jede wirkliche Zahl nur eine endliche Menge von Theilern, die >1 sind.

§. 5. Lehrsatz. Zu jeder beliebigen nur immer doch endlichen Menge wirklicher Zahlen $a, b, c, d, \ldots$ gibt es auch eine wirkliche Zahl, die sich als ein gemeinschaftliches Vielfache derselben ansehen läßt.

Beweis. Wenn die Menge der wirklichen Zahlen $a, b, c, d \ldots$ endlich ist; so ist die Vorstellung einer Zahl, die das Product aus ihnen allen ist, eine gegenständliche Vorstellung (§.). Diese Zahl aber ist gewiß ein sie alle umfassendes Vielfache.

§. 6. Zusatz. Wäre die Menge der Zahlen $a, b, c, d, \ldots$ unendlich; so müßte es ein solches Vielfache derselben nicht nothwendig geben (§.).

§. 7. Lehrsatz. Auch ein kleinstes gemeinschaftliches Vielfache muß es zu jeder gegebenen endlichen Menge von Zahlen $a, b, c, d, \ldots$ geben.

Beweis. Denn es gibt irgend ein Vielfaches für alle diese Zahlen, nähmlich das aus ihnen allen gebildete Product. (§. 5.). Wohl mag es aber oft kleinere Vielfache als dieses geben. Nie jedoch kann es zu jedem gemeinschaftlichen Vielfachen derselben ein anderes noch kleineres geben, weil sonst die Menge dieser kleineren Vielfachen unendlich seyn müßte; während doch keine Reihe von wirklichen Zahlen, deren die folgende immer kleiner als die vorhergehende ist, in das Unendliche geht. (§.) Also muß eines dieser gemeinschaftlichen Vielfachen das kleinste seyn (§.).

§. 8. Lehrsatz. Zu jeder beliebigen endlichen oder selbst unendlichen Menge wirklicher Zahlen gibt es auch irgend einen gemeinschaftlichen Theiler, wenn man die Einheit selbst mit dazu rechnet.

Beweis. Denn die Einheit selbst ist als ein Theiler jeder Zahl (§.), auch der gemeinschaftliche Theiler jeder gegebenen Menge von Zahlen.

§. 9. Lehrsatz. Auch einen größten gemeinschaftlichen Theiler muß es zu jeder beliebigen endlichen oder unendlichen Menge von wirklichen Zahlen geben.

Beweis. Denn irgend einen gemeinschaftlichen Theiler für alle diese Zahlen gibt es nach §. 8., nähmlich die Einheit. Gibt es nun sonst keine andere, so ist dieser auch schon der größte zu nennen. Gibt es noch andere, so muß doch einer unter ihnen der größte seyn; denn größer als die kleinste unter den gegebenen Zahlen kann keiner seyn (§.).

§. 10. Lehrsatz. Wenn ein Paar Zahlen a und b bey der versuchten Division durch eine dritte m einerley Rest geben, so ist der Unterschied $a-b$ (wenn a die größere derselben heißt) theilbar durch diese dritte m.

Beweis. Wenn die versuchte Division von m in a den nächst kleineren Quotienten α und den Rest r gibt, so ist $a=\alpha m+r$. Und eben so, weil b denselben Rest geben soll, hat man $b=\beta m+r$. Daher wenn $a>b$, hat man $a-b=\alpha m-\beta m=$ $=(\alpha-\beta)m$. Folglich $\frac{a-b}{m}=\alpha-\beta$, eine wirkliche Zahl. So gibt die Zahl 34 bey der versuchten Division durch 5 den nächst kleineren Quotienten 6 und den Rest 4; die Zahl 19 gibt den nächst kleineren Quotienten 3 und denselben Rest 4; daher ist $34-19=15$ theilbar durch 5.

§. 11. Lehrsatz. Umgekehrt, wenn $a-b$ theilbar durch m, und a läßt bey der versuchten Theilung durch m einen Rest r; so muß auch b bey dieser Theilung den Rest r lassen. Und wenn bey b der Rest r bleibt, so muß auch a diesen Rest lassen.

Beweis. Es ist $\frac{a-b}{m}=$ einer wirklichen Zahl π. Wenn nun zuvörderst a bey der versuchten Division mit m den Rest $r<m$ läßt; so ist a von der Form $\alpha m+r$. Also hat man $a-b=m\pi$ und $b=a-m\pi=\alpha m+r-m\pi=(\alpha-\pi)m+r$. Da nun $r<m$, so gibt b bey der versuchten Division mit n den nächst kleineren Quotienten $\alpha-\pi$, und den Rest r.

2. Wenn aber b bey der versuchten Division mit m den Rest $r<m$ läßt; so ist b von der Form $b=\beta m+r$. Also hat man $a-b=m\pi$ und $a=b+m\pi=\beta m+r+m\pi=(\beta+\pi)m+r$. Weil nun $r<m$; so gibt a bey der versuchten Division mit m den nächst kleineren Quotienten $\beta+\pi$, und den Rest r.

Beyspiel. So ist $37-7$ theilbar durch 5, und $\frac{7}{5}$ gibt den Rest 2, also gibt auch $\frac{37}{5}$ den Rest 2. Eben so ist $37-7$ theilbar durch 6, und $\frac{37}{6}$ gibt den Rest 1, also gibt auch $\frac{7}{6}$ den Rest 1.

§. 12. Lehrsatz. Wenn die wirkliche Zahl $a>$ die wirkliche Zahl b und doch kein Vielfaches derselben ist; so gibt es

jederzeit eine Zahl n von der Art, daß Eines von Beiden, entweder der Rest $a-nb$ oder der Rest $(n+1)b-a$ eine Zahl darstellt, deren Doppeltes noch immer nicht b übersteigt.

Beweis. Weil die Zahl $a>b$, und doch kein Vielfaches von b ist: so gibt es (nach §.) jederzeit eine wirkliche Zahl n, von der Art, daß nb noch $<a$, $(n+1)b$, aber schon $>a$ ist. Wenn nun das Doppelte des Restes $a-nb$, d. h. wenn $2(a-nb)$ nicht $=$ oder $<$ ist: so muß es größer seyn, d. h. $2(a-nb)>b$. Wenn aber dieses ist, dann behaupte ich, daß das Doppelte des Restes $(n+1)b-a$ d. i. $2[(n+1)b-a]<b$ sey. Denn ist $2(a-nb)>b$: so ist $2nb+b<2a$: und wenn wir beiderseits b addiren: $2nb+2b<2a+b$: oder wenn wir $2a$ abziehen, $2nb+2b-2a<b$: d. i. $2[(n+1)b-a]<b$.

Beyspiel. Ist $b=7$ und $a=30$, so ist für $n=4$, $a-nb=2$ ein Rest, dessen Doppeltes <7. Ist $a=34$, so ist für $n=4$ $(n+1)b-a=1$ ein Rest, dessen Doppeltes <7.

§. 13. Lehrsatz. Wenn wir bey der versuchten Division einer Zahl b in eine größere a die Zahl α als den nächst kleineren Quotienten, und den Rest r finden: so daß also $a=\alpha b+r$ und $r<b$: wenn wir ferner bey der versuchten Division des Restes r in den vorigen Divisor b die Zahl β als den nächst kleineren Quotienten und den Rest r' finden, so daß also $b=\beta r+r'$; und $r'<r$: wenn wir so fortfahren mit dem gefundenen Reste immer in den nächst vorhergehenden Divisor zu dividiren: so müssen wir nach einer endlichen Menge von Wiederhohlungen dieses Verfahrens allemahl auf eine Division kommen, die aufgeht, d. h. bey welcher kein Rest verbleibt.

Beweis. Denn wenn wir die Reste, welche bey den versuchten Divisionen zum Vorschein kommen, der Ordnung nach durch $r, r', r'', \ldots$ bezeichnen; so muß $a>b$, $b>r>r'>r''>\ldots$ seyn. Da nun diese Zeichen insgesammt Zahlen bezeichnen: so kann die Menge derselben nicht unendlich seyn (§.).

Beyspiel. Ist $a=44$, $b=13$, so gibt die versuchte Division von 13 in 44 den nächst kleineren Quotienten 3, den Rest 5 und dieser bey der versuchten Division in 13 den nächst kleineren Quotienten 2 und den Rest 3 und dieser bey der versuchten Division in 5 den Quontienten 1 und den Rest 2, und dieser bey der versuchten Division in 3 den Quotienten 1 und den Rest 1, bey welchem die Division in 2 aufgehet.

§. 14. Lehrsatz. Wenn eine Zahl nb, welche ein Vielfaches einer anderen b ist, durch ihre versuchte Division in eine ge-

gebene Zahl a den nächst kleineren Quotienten c gibt: so gibt die versuchte Division des Factors b in a einen wirklichen nächst kleineren Quotienten, der gewiß nicht $< nc$ ist.

Beweis. Denn bezeichnen wir diesen wirklichen nächst kleineren Quotienten durch q, so ist $b(q+1) > a$. Aber $a > nb.c = b.nc$. Also $b(q+1) > b.nc$. Und somit $q+1 > nc$. Also gewiß q nicht $< nc$. So gibt, wenn $a = 40$, $b = 3$, $n = 2$ genommen wird, $nb = 6$ bey der versuchten Division in $a = 40$, den nächst kleineren Quotienten $c = 6$: $b = 3$ aber gibt bey der Division in $a = 40$ den nächst kleineren Quotienten $13 > (nc = 2.6)$.

§. 15. Lehrsatz. Wenn $a + \frac{m}{n} = b + \frac{p}{q}$ und a, b, m, n, p, q sind wirkliche Zahlen, ferner ist $m < n$ und $p < q$, so muß $a = b$ und $\frac{m}{n} = \frac{p}{q}$ seyn.

Beweis. Wäre $a \overset{n}{=} b$: so müßte Eine dieser Zahlen die größere seyn. Heiße dann (weil dieses gleichgültig ist), a diese größere. Also ist $a - b =$ einer wirklichen Zahl und da $a + \frac{m}{n} = b + \frac{p}{q}$ ist; so muß auch $a - b + \frac{m}{n}$ oder $c + \frac{m}{n}$ oder $\frac{nc+m}{n} = \frac{p}{q}$ seyn. Da aber $p < q$; so muß (nach §.) auch $cn + m < n$ seyn, welches ungereimt ist. Haben wir aber $a = b$: so folgt von selbst, daß auch $\frac{m}{n} = \frac{p}{q}$ seyn müsse, wenn von der Gleichung $a + \frac{m}{n} = b + \frac{p}{q}$ die Gleichung $a = b$ abgezogen wird.

§. 16. Lehrsatz. Wenn alle einzelnen in einer algebraischen Summe vorkommenden Summanden a, b, c, ... durch eine gewisse Zahl m theilbar sind. so ist auch die ganze Summe theilbar durch diese Zahl.

Beweis. Sind die Zahlen $a, b, c \ldots$ alle theilbar durch m, so ist $\frac{a}{m} =$ einer wirklichen Zahl α. $\frac{b}{m} =$ einer wirklichen Zahl β, $\frac{c}{m} =$ einer wirklichen Zahl γ u. s. w. Da nun (nach §.) $\frac{a+b+c+\ldots}{m} = \frac{a}{m} + \frac{b}{m} + \frac{c}{m} + \ldots$ so ist $\frac{a+b+c+\ldots}{m} = \alpha + \beta + \gamma + \ldots$, welches offenbar eine wirkliche Zahl oder Null ist; und zeigt, daß $a + b + c + \ldots$ theilbar durch m seyn müsse.

§. 17. Zusatz. Wenn also alle in einer Summe vorkommenden Summanden gerade sind, (d. h. sich durch zwey theilen lassen)

und ihre Menge ist endlich: so ist auch die Summe selbst gerade. Denn auch sie muß sich durch 2 theilen lassen. So ist z. B. $4+6+8=18$ gerade.

§. 18. Zusatz. Allein auch eine Summe von ungeraden Zahlen, wenn ihre Menge gerade ist, ist eine gerade Zahl. Denn ist die Menge der Zahlen $2n+1$, $2m+1$, $2p+1$, $2q+1$, ... gerade: so ist auch die Summe derselben

$$(2n+1)+(2m+1)+(2p+1)+(2q+1)+\ldots=$$
$$=(2n+2m+2p+2q+\ldots)+(1+1+1+1+\ldots).$$

Der erste Theil dieser Summe ist gerade, weil er aus lauter geraden Zahlen bestehet. Der zweyte Theil dieser Summe $(1+1+1+1+\ldots)$ bestehet aus ebenso vielen Einheiten als Zahlen summirt worden sind. Er ist also, wenn ihre Menge gerade war, abermahls gerade. Folglich ist auch die Summe beyder Theile gerade (§. 16.). So ist z. B. $5+3+11+7=26$ gerade.

§. 19. Zusatz. Dagegen eine Summe von ungeraden Zahlen, deren Menge ungerade ist, ist auch selbst ungerade. Denn ist eine dieser Zahlen $2n+1$, so ist die Summe der übrigen, weil ihre Menge gerade ist, eine gerade Zahl, und somit von der Form $2m$. Also die Summe aller, oder $2m+2n+1=2(m+n)+1$, welches die Form einer ungeraden Zahl ist. So ist z. B. $5+3+11=19$ ungerade.

§. 20. Zusatz. Der Satz des §. 16., daß eine algebraische Summe theilbar sey, wenn alle ihre Summanden es sind, läßt sich nicht umkehren, d. h. nicht immer müssen, wenn sich die Summe durch eine gewisse Zahl theilen läßt, auch ihre einzelnen Summanden durch eben diese Zahl sich theilen lassen. Denn diese können ja auch selbst kleiner als diese Zahl, wenn sie nicht 1 ist, angenommen werden. So ist z. B. zwar 4 theilbar durch 2, aber die einzelnen Summanden $1+1+1+1$, aus denen wir 4 zusammensetzen können, sind keiner theilbar durch 2. Wohl aber gilt folgender Satz.

§. 21. Lehrsatz. Wenn von zwey Zahlen a und b die Eine a, dann noch ihre Summe $a+b$ oder ihre Differenz $a-b$ oder $b-a$ (je nachdem a oder b die größere Zahl ist) theilbar durch eine und eben dieselbe Zahl m ist: so muß auch die andere Zahl b theilbar durch diese Zahl m seyn.

Beweis. 1. Wenn a und die Summe $a+b$ theilbar durch m ist: so hat man $\frac{a}{m}=$ einer wirklichen Zahl α, und $\frac{a+b}{m}=$

= einer wirklichen Zahl π. Also $a = m\alpha$, $a + b = m\pi$, und durch Abzug $b = m\pi - m\alpha$. Also ist letzterer Ausdruck eine wirkliche Zahl und mithin $= m(\pi - \alpha)$. Also $\pi - \alpha$ eine wirkliche Zahl, und mithin $\frac{b}{m} = \pi - \alpha$, also b theilbar durch m.

2. Wenn a und die Differenz $a - b$ theilbar durch m ist; so hat man $\frac{a}{m}$ = einer wirklichen Zahl α, und $\frac{a-b}{m}$ = einer wirklichen Zahl π. Also $a = m\alpha$, $a - b = m\pi$. Folglich die Zahl $b = a - m\pi = m\alpha - m\pi = m(\alpha - \pi)$. Also $\frac{b}{m} = \alpha - \pi$, einer wirklichen Zahl.

3. Wenn a und die Differenz $b - a$ theilbar durch m ist: so hat man $\frac{a}{m}$ = einer wirklichen Zahl α, $\frac{b-a}{m}$ = einer wirklichen Zahl π. Also $a = m\alpha$, $b - a = m\pi$, $b = m\pi + a = m\pi + m\alpha = m(\pi + \alpha)$. Daher $\frac{b}{m} = \pi + \alpha$, einer wirklichen Zahl.

Beyspiel. So ist 15 theilbar durch 5, ingleichen die Summe $15 + 30 = 45$, also muß es auch 30; ebenso ist 21 und die Differenz $182 - 21 = 161$ theilbar durch 7, also muß es auch 182 seyn.

§. 22. Lehrsatz. Ein Product aus lauter wirklichen Zahlen $a, b, c, \ldots, l$ ist theilbar durch eine Zahl m, sofern nur ein einziger Factor desselben z. B. a theilbar durch diese Zahl ist.

Beweis. Denn (nach §.) ist $\frac{a.b.c\ldots l}{m} = \frac{a}{m}.b.c\ldots l$. Ist nun a theilbar durch m, so ist $\frac{a}{m}$ = einer wirklichen Zahl, und somit $\frac{a.b.c\ldots l}{m}$ = einem Producte aus lauter wirklichen Zahlen, das also gewiß auch selbst eine wirkliche Zahl ist (§.).

So ist z. B. $434 = 31.14$ theilbar durch 7, weil es der Factor 14 ist.

§. 23. Zusatz. Auch dieser Satz läßt sich nicht umkehren: oder es muß nicht, so oft ein Product theilbar durch eine gewisse Zahl ist, auch irgend ein einzelner Factor desselben, der kleiner ist als das ganze Product, theilbar durch diese Zahl seyn. Denn jedes Product ist ja auch theilbar durch sich selbst; und doch ist gewiß keiner derjenigen Factoren, die kleiner als das Product sind, durch dieses theilbar.

§. 24. Lehrsatz. Wenn die (positiven oder negativen) Unterschiede $a_1 - b_1$, $a_2 - b_2$, $a_3 - b_3$, ..., $a_n - b_n$ der wirklichen Zahlen

a_1, b_1: a_2, b_2: a_3. b_3: ...: a_n, b_n insgesamt theilbar sind durch eine und eben dieselbe Zahl p: so ist auch der Unterschied der Producte $a_1 . a_2 . a_3 \ldots a_n - b_1 . b_2 . b_3 \ldots b_n$ theilbar durch p.

Beweis. Unter der angenommenen Voraussetzung bestehen die Gleichungen

$$\begin{aligned} a_1 &= b_1 + p . c_1 \\ a_2 &= b_2 + p . c_2 \\ a_3 &= b_3 + p . c_3 \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ a_n &= b_n + p . c_n, \end{aligned}$$

worin $c_1, c_2, \ldots . c_n$ gewisse entweder positive oder negative wirkliche Zahlen oder allenfalls (theilweise) auch Nullen bezeichnen. Daher ist dann auch, wenn wir diese Gleichungen mit einander multiplicieren (nach §.)

$$a_1 . a_2 . a_3 \ldots a_n = (b_1 + pc_1)(b_2 + pc_2)(b_3 + pc_3) \ldots (b_n + pc_n).$$

Ohne das angezeigte Product in dem rechten Gliede der Gleichung vollkommen zu entwickeln, sieht man doch, daß es aus dem Theilproducte $b_1 . b_2 . b_3 \ldots b_n$ und mehreren anderen Theilproducten bestehe, die insgesamt den Factor p ein oder mehrere Mahle enthalten. Nach §. 22. ist also jedes dieser Theilproducte, und mithin auch ihre algebraische Summe theilbar durch p. Daher dann auch (nach §.) $a_1 . a_2 . a_3 \ldots a_n - b_1 . b_2 . b_3 \ldots b_n$ theilbar durch p seyn muß.

Beyspiel. So sind die Unterschiede

$$\begin{aligned} 8 - 2 &= 6 \\ 5 - 26 &= -21 \\ 101 - 2 &= 99 \end{aligned}$$

alle theilbar durch 3; daher auch $8 . 5 . 101 - 2 . 26 . 2 = 3.936$ theilbar durch 3.

§. 23. Lehrsatz. Ein Product aus lauter wirklichen Zahlen, darin auch nur ein einziger Factor gerade, die Menge aller aber endlich ist, ist selbst gerade. Und wenn im Gegentheil auch nicht ein einziger Factor eines Productes gerade ist, so ist das Product selbst ungerade.

Beweis. Wenn auch nur ein Factor in einem Producte gerade ist, so ist es gerade: denn es ist dieser Eine Factor, und mithin nach §. 22. auch das ganze Product theilbar durch 2. Daß aber im Gegentheil ein Product, welches aus lauter ungeraden Factoren bestehet, ungerade seyn müsse, gilt wenig-

stens, wenn die Zahl dieser Factoren nur zwey ist. Denn das Product $(2n+1)(2m+1)$ läßt sich betrachten als eine Summe von lauter Summanden, die der Zahl $2n+1$ gleich sind und deren Menge $= 2m+1$ ist, d. h. es läßt sich betrachten als eine Summe von ungeraden Summanden, deren Anzahl abermahls ungerade ist. Eine solche Summe ist aber nach §. 14. ungerade. Gilt nun der Satz von irgend einer Anzahl Factoren $= n$, so gilt er auch von $n+1$ Factoren. Denn, ist das Product aus den ungeraden Factoren ungerade; so ist das Product aus den $n+1$ Factoren, weil es ein Product aus jenen, also aus einer ungeraden Zahl in den $(n+1)^{\text{ten}}$ Factor, d. h. in eine ungerade Zahl ist, abermahls ungerade. Also gilt der Satz allgemein.

Beyspiel. So ist das Product $3.7.4 = 84$ gerade, weil ein Factor 4 gerade; das Product $3.7.11 = 231$ ungerade, weil alle Factoren ungerade.

§. 26. Zusatz. So läßt eine Zahl, die ungerade ist, sich nur zerlegen in Factoren, die gleichfalls ungerade sind. So hat die ungerade Zahl 105 keine andere Factoren als 1, 3, 5, 7, 15, 21, 35 und 105, die alle ungerade sind.

§. 27. Lehrsatz. Es gibt auch Zahlen, die sonst keine andere Theiler als nur die Einheit und sich selbst haben.

Beweis. Eine solche Zahl ist z. B. die Zwey; denn diese hat sicher keinen anderen Theiler als die Einheit und sich selbst, weil jede andere Zahl >2 ist; also kein Theiler von ihr seyn kann (§.). Eine solche Zahl ist ferner auch die Zahl Drey; denn außer der Einheit und ihr selbst gibt es nur die Zahl Zwey, die nicht größer als sie selbst ist; durch 2 läßt sich aber 3 nicht theilen, weil $1.2 < 3$ und $2.2 = 4 > 3$ ist. U. s. w.

§. 28. Erklärung. Zahlen, die keinen anderen Theiler haben als die Einheit und sich selbst, werden einfache Zahlen oder Primzahlen genannt; alle anderen dagegen zusammengesetzte Zahlen. So sind z. B. 1, 2, 3 Primzahlen, 4 aber eine zusammengesetzte Zahl.

§. 29. Lehrsatz. Es gibt auch Inbegriffe von Zahlen, die keinen anderen gemeinschaftlichen Theiler als nur die Einheit haben.

Beweis. Wenn die in dem gegebenen Inbegriffe befindlichen Zahlen lauter Primzahlen sind; so haben sie gewiß keinen anderen gemeinschaftlichen Theiler als nur die Einheit. Denn jede derselben hat außer der Einheit nur noch sich selbst zum Theiler.

§. 30. Lehrsatz. Auch Zahlen, die keine Primzahlen sind, können doch so beschaffen seyn, daß sie ausser der Einheit sonst keinen anderen gemeinschaftlichen Theiler haben.

Beweis. So sind wohl 4 und 9 keine Primzahlen; denn jene ist durch 2, diese durch 3 theilbar, aber sie haben doch keinen anderen gemeinschaftlichen Theiler als die Einheit, weil 9 nicht durch 2 und 4, 4 aber nicht durch 3 und 9 theilbar ist.

§. 31. Erklärung. Wenn mehrere Zahlen $A, B, C, D, \ldots$ keinen anderen gemeinschaftlichen Theiler als die Einheit haben, so nennen wir sie beziehungsweise oder relativ einfache oder relative Primzahlen in der weiteren Bedeutung; im engeren Sinne aber heißen die Zahlen $A, B, C, D, \ldots$ nur dann relative Primzahlen untereinander, wenn auch nicht zwey derselben einen gemeinschaftlichen Theiler haben. Die Zahlen 4, 6, 9, 21 sind relative Primzahlen in der weiteren, die Zahlen 4, 9, 25, 49 relative Primzahlen in der engeren Bedeutung. Zur besseren Unterscheidung der relativen Primzahlen werden die Zahlen, die durchaus keine andere Theiler haben als nur die Einheit und sich selbst, auch Primzahlen an sich oder absolute Primzahlen genannt. Wenn künftig gesagt werden wird, daß gewisse Zahlen keinen gemeinschaftlichen Theiler haben: so soll immer verstanden werden, keinen außer der Einheit.

§. 32. Zusatz. Nach dieser Erklärung ist das Verhältniß, in welchem relative Primzahlen als solche unter einander stehen, ein gegenseitiges, d. h. wenn a eine relative Primzahl zu b ist, so ist es b auch zu a. Denn beydes heißt nur, daß a und b keinen gemeinschaftlichen Theiler haben, der > 1 ist.

§. 33. Zusatz. Nach dieser Erklärung stehet die Einheit zu jeder Zahl auch zu sich selbst in dem Verhältnisse einer relativen Primzahl: denn 1 und N, ingleichen 1 und 1 haben gewiß keinen anderen gemeinschaftlichen Theiler als die Einheit.

§. 34. Zusatz. Wenn es der Zahlen, die wir miteinander vergleichen, nur zwey gibt, und sie sind relative Primzahlen in der weiteren Bedeutung, so sind sie es auch in der engeren. Nur also, wenn der Zahlen mehr als zwey mit einander verbunden werden: muß man unterscheiden, ob wir sie für relative Primzahlen in der weiteren oder der engeren Bedeutung erklären: denn nicht immer werden sie, wenn sie das Erstere sind, auch das Letztere seyn. So sind die drey Zahlen 4, 6, 9 relative Primzahlen in der weiteren Bedeutung, nicht

aber in der engeren. Denn obgleich es außer der Einheit keine gemeinschaftlichen Theiler für diese drey Zahlen gibt, so haben doch je zwey und zwey derselben einen gemeinschaftlichen Theiler, 4 und 6 nähmlich den Theiler 2; 6 und 9 den Theiler 3.

§. 35. Zusatz. Sagen, daß in dem Inbegriffe der Zahlen $a, b, c, \ldots, l$ je zwey und zwey relative Primzahlen unter einander sind, heißt eben soviel als sagen, daß die Zahlen $a, b, c \ldots, l$ relative Primzahlen in der engeren Bedeutung sind.

§. 36. Lehrsatz. Wenn a und b unter einander, und a und c abermahls unter einander relative Primzahlen sind, so müssen darum nicht auch b und c unter einander relative Primzahlen seyn.

Beweis. Denn wenn z. B. a eine absolute Primzahl ist, so werden a und b, ingleichen a und c unter einander gewiß keinen gemeinschaftlichen Theiler haben, die Zahlen b und c selbst mögen wie immer gewählt werden, also auch so, daß sie einen gemeinschaftlichen Theiler haben. So haben 3 und 5 und eben so auch 3 und 10 keinen gemeinschaftlichen Theiler, 5 und 10 aber haben einen gemeinschaftlichen Theiler.

§. 37. Lehrsatz. Auch umgekehrt daraus, daß a und b unter einander, und a und c unter einander einen gemeinschaftlichen Theiler haben, folgt nicht, daß b und c unter einander einen gemeinschaftlichen Theiler haben.

Beweis. Denn der gemeinschaftliche Theiler, den a und b unter einander haben, könnte ein anderer seyn als der, den a und c unter einander haben. So können b und c Primzahlen, a aber ein Product von beyden seyn. Dann haben a und b, und a und c gewiß einen gemeinschaftlichen Theiler, je beyde unter einander: aber nicht b und c unter einander. So haben auch 6 und 14, ingleichen 6 und 9 einen gemeinschaftlichen Theiler, jene nähmlich die Zahl 2, diese die Zahl 3; 14 und 9 aber haben keinen gemeinschaftlichen Theiler.

§. 38. Lehrsatz. Daraus, daß die mehreren Zahlen $a, b, c, d, e, f, \ldots$ untereinander relative Primzahlen in der weiteren Bedeutung sind, folgt nicht, daß auch die wenigeren $a, b, c, \ldots$, deren Inbegriff nur ein Theil von dem Inbegriffe der vorigen ist, relative Primzahlen unter einander seyn müssen; wohl aber, wenn nicht einmahl die Zahlen $a, b, \ldots$ relative Primzahlen in der weiteren Bedeutung sind, so folgt, daß es um so weniger die mehreren $a, b, c, d, e, f, \ldots$ sind.

Beweis. 1. Denn c, $d, \ldots$ können einen gemeinschaftlichen Theiler haben, den aber nicht $a. b$ haben. So sind 4 und 6 keine relative Primzahlen, wohl aber 4, 6 und 7.

2. Wenn schon $a. b$ keinen gemeinschaftlichen Theiler haben: so haben um so weniger $a, b, c, d, \ldots$ einen gemeinschaftlichen Theiler.

§. 39. Lehrsatz. Daraus, daß die mehreren Zahlen $a, b. c. d, e, f, \ldots$ relative Primzahlen in der engeren Bedeutung sind, folgt, daß es auch die wenigeren $a, b, \ldots$ sind; allein nicht umgekehrt folgt daraus, weil die wenigeren Zahlen $a, b, \ldots$, relative Primzahlen in der engeren Bedeutung sind, daß es auch die mehreren $a. b. c, d, e, f, \ldots$ seyn werden.

Beweis. 1. Wenn unter den sämmtlichen Zahlen $a, b. c, d. e. f, \ldots$ auch nicht zwey einen gemeinschaftlichen Theiler haben, so haben auch nicht die wenigeren $a. b, \ldots$ einen gemeinschaftlichen Theiler.

2. Es kann sich treffen, daß auch nicht zwey der Zahlen $a, b, c, \ldots$ für sich, und eben so, daß auch nicht zwey der Zahlen $d, e. f$ für sich einen gemeinschaftlichen Theiler haben, und gleichwohl kann eine der Zahlen $a, b, c, \ldots$ mit einer der Zahlen $d, e, f, \ldots$ einen gemeinschaftlichen Theiler haben. Dann also sind die Zahlen $a, b, c, \ldots$ für sich, ingleichen auch die Zahlen $d. e, f$ für sich relative Primzahlen in der engeren Bedeutung, nicht aber die Zahlen $a. b. c, \ldots d, e. f$ zusammen. Z. B. 3, 4. 7 und 2, 9, 35.

§. 40. Lehrsatz. Wenn in einem Inbegriffe von Zahlen $a. b. c. d$ auch nur zwey, a und b relative Primzahlen sind; so sind sie alle unter einander relative Primzahlen in der weiteren Bedeutung.

Beweis. Denn wenn nur zwey derselben keinen gemeinschaftlichen Theiler haben, so gibt es umsoweniger eine Zahl, welche ein Theiler für alle diese Zahlen wäre.

§. 41. Zusatz. Wenn also ein gegebener Inbegriff von Zahlen $A. B. C, D \ldots$ auch nur zwey absolute Primzahlen in sich faßt, so ist er ein Inbegriff von Zahlen, die unter einander relative Primzahlen in der weiteren Bedeutung sind.

§. 42. Zusatz. Und wenn sich in einem Inbegriffe von Zahlen, die einen gemeinschaftlichen Theiler haben, eine absolute Primzahl befindet, so müssen die übrigen Zahlen insgesamt Vielfache von dieser einer seyn.

§. 43. Lehrsatz. Jede Zahl, die keine Primzahl ist, läßt sich als ein Product aus einer endlichen Menge von Primzahlen, die alle >1 sind, betrachten.

Beweis. Jede Zahl. die keine Primzahl ist, ist der Erklärung nach theilbar durch eine Zahl, die >1 und doch $<$ als sie selbst ist. Somit muß auch der Quotient, d. h. die andere Zahl, welche als Factor mit jener verbunden, die gegebene Zahl selbst darstellt, >1 und $<$ sie selbst seyn (§.). Also ist jede Zahl. die keine Primzahl ist, anzusehen als ein Product aus zwey Factoren. die beyde >1 und $<$ als sie selbst sind. Diese beyden Factoren P und Q können nun selbst entweder Primzahlen oder wieder Producte aus anderen Zahlen seyn. Sind sie Primzahlen, so ist der Fall beschaffen, wie ihn der Lehrsatz aussagt. Ist aber der eine oder der andere, oder sind beyde Factoren P und Q abermahls Producte aus anderen Zahlen: so müssen wir doch nach einer endlichen Menge von Wiederhohlungen dieser Schlüsse auf Zahlen kommen, die sich nicht weiter zerlegen lassen in Factoren, welche >1 wären. Denn im entgegengesetzten Falle, wenn diese Zerlegung ins Unendliche ginge, müßte es Zahlen geben, die eine unendliche Menge von Factoren, alle >1, enthielten (§. 3.).

§. 44. Zusatz. Nichts hindert, daß nicht einige oder auch alle Primzahlen, aus deren Multiplication eine gewisse Zahl, die selbst keine Primzahl ist, gebildet werden kann, unter einander gleich wären. So entsteht z. B. durch die Multiplication der zwey einander gleichen Primzahlen 3 und 3 die Zahl 9; durch Multiplicirung der drey einander gleichen Primzahlen 2, 2, 2 die Zahl 8; durch Multiplication der Zahlen 2, 2, 2, 3, 3 die Zahl 72 u. s. w.

§. 45. Erklärung. Factoren einer Zahl, welche Primzahlen sind, sollen einfache Factoren heißen; und ihre Angabe samt Bestimmung der Anzahl, wie viele gleiche es etwa von jeder Art gibt, soll die Zerlegung der Zahl in ihre einfachen Factoren heißen.

§. 46. Lehrsatz. Zu jeder Primzahl gibt es noch eine größere.

Beweis. Sey p eine Primzahl. so ist das Product aus p und aller der Zahl p vorhergehenden d. h. kleineren Primzahlen $1.2.3.5.7.11.13.17\ldots p$. wenn wir noch 1 hinzutun, oder die Summe $1.2.3.5.7.11.13.17\ldots p+1$ eine Zahl, die gewiß weder durch p, noch irgend eine kleinere Primzahl als p (die Eins nicht mitgerechnet) theilbar ist. Denn durch jede dieser Primzahlen ist das Product $1.2.3.5.7.11.13.17\ldots p$ theilbar, weil p und jede kleinere Primzahl darin als Factor erscheint. Die Zahl 1 aber ist durch keine dieser Primzahlen theilbar. Also auch nicht jene Summe (§. 17.). Folglich ist diese entweder eine Primzahl, die dann gewiß eine grössere ist als p,

oder sie ist ein Product aus Primzahlen (§. 43.), und zwar aus anderen als 2. 3, 5, 7, 11, 13, 17, ..., p. Also gibt es auf jeden Fall noch andere Primzahlen, als die soeben genannten, die mithin grösser sind als p.

§. 47. Zusatz. Also ist die Menge aller Primzahlen, die es nur überhaupt gibt, unendlich.

§. 48. Lehrsatz. Mit Ausnahme der zwey Primzahlen 2 und 3 ist jede andere Primzahl unter dem Ausdrucke $6n \pm 1$ enthalten, wenn n jede beliebige wirkliche Zahl vorstellen darf; nicht aber umgekehrt ist jede Zahl, die unter diesem Ausdrucke enthalten ist, eine Primzahl.

Beweis. Daß die zwey Primzahlen 2 und 3 unter dem Audrucke $6n \pm 1$ nicht enthalten sind, wenn n nicht Anderes als eine wirkliche Zahl vorstellen darf, erhellet von selbst. Denn für $n = 1$. ist $6n \pm 1$ entweder $= 7$ oder $= 5$. also $>$ als jede der beiden Zahlen 2 und 3. für jeden noch größeren Werth von n aber bekömmt $6n \pm 1$ einen noch größeren Werth. Daß aber jede Primzahl. die grösser als 2 oder 3 ist, unter jenem Ausdrucke allerdings begriffen werden könne, erweiset sich so. Die nächste Primzahl nach 3 ist die Zahl 5, und diese ist unter der Form $6n - 1$ enthalten, wenn $n = 1$ gesetzt wird. Die auf 5 folgende nächste Primzahl d. i. 7 und somit jede andere ist größer als die Zahl 6. Jede Zahl aber, die > 6 ist, muß, wenn wir eine Division derselben mit 6 versuchen, entweder aufgehen, oder einen Rest, der < 6 ist, also eine der Zahlen 1, 2, 3, 4, 5 zum Reste geben. Eine Zahl, bey welcher die Division mit 6 aufginge, wäre aber deßhalb keine Primzahl zu nennen. Ebenso auch keine Zahl, die 2 oder 4 zum Reste ließe. Denn eine solche wäre unter der Form $6n + 2$ oder $6n + 4$ enthalten, wenn wir den nächst kleineren Quotienten durch n bezeichnen. Aber $6n + 2$ und $6n + 4$ sind offenbar theilbar durch 2, wo sie die Quotienten $3n + 1$. $3n + 2$ geben. Endlich kann auch keine Zahl, welche bey dieser Division den Rest 3 läßt, eine Primzahl seyn. Denn sie wäre unter der Form $6n + 3$ enthalten, und somit theilbar durch 3, wo sie den Quotienten $2n + 1$ gäbe. Also muß jede Zahl, die eine Primzahl ist, bey der versuchten Division mit 6 nur Eines von Beydem, entweder 1 oder 5 zum Reste geben; mithin enthalten seyn unter der Form $6n + 1$ oder $6n + 5$. Allein eine Zahl, die unter der letzteren Form $6n + 5$ enthalten ist, kann auch unter der Form $6n - 1$ vorgestellt werden; weil $6n + 5 = 6(n + 1) - 1$ und $n + 1$ durch n vorgestellt werden kann.

wenn n jede beliebige Zahl bedeutet. Unter der letzten Form $6n-1$ ist aber auch die Primzahl 5 enthalten, wenn wir $n=1$ setzen. Also ist unter einer der Formen $6n\pm1$ jede Primzahl, die größer als 3 ist, enthalten. — Daß aber dieser Satz sich nicht umkehren lasse, oder daß nicht alle unter der Form $6n\pm1$ enthaltenen Zahlen Primzahlen seyn müssen, läßt sich durch viele Beyspiele beweisen. So wird, wenn wir $n=4$ setzen, $6n+1=25$, welches bekanntlich keine Primzahl, sondern $=5.5$ ist.

§. 49. Lehrsatz. Wenn die Zahl $a>b$. und die versuchte Division von b in a gibt entweder den genauen Quotienten q_1. oder sie gibt q_1 nur als nächst kleineren Quotienten und den Rest r_1; und wir versuchen nun wieder mit dem erhaltenen Reste r_1 in den vorhergehenden Divisor b zu dividieren, und erhalten entweder den genauen Quotienten q_2 oder die versuchte Division gibt q_2 nur als den nächst kleineren Quotienten und den Rest r_2; und wir versuchen mit diesem abermahls in den nächst vorhergehenden Divisor r_1, zu dividiren, und so immer fort, bis wir zu einem Divisor r_n gelangen, der genau aufgeht: so behaupte ich, dieser Divisor r_n sey ein gemeinschaftlicher, und zwar der größte gemeinschaftliche Theiler, den die beyden Zahlen a und b haben.

Beweis. Daß wir bey diesem Verfahren immer auf eine Division, die aufgehet, kommen müssen; wurde schon (§. 13.) bewiesen. Wenn nun schon die erste Division, nähmlich die von b in a, aufgeht, so ist kein Zweifel, daß b ein gemeinschaftlicher und zwar der größte gemeinschaftliche Theiler der Zahlen a und b sey; denn b theilt b und a, und es gibt sicher keine größere Zahl, die b theilt, als b selbst. Eben so gilt unser Satz, wenn erst die zweyte Division oder die von r_1 in b aufgeht. Dann nähmlich ist $a=q_1b+r_1$ und $b=q_2r_1$. Also $a=q_1q_2r_1+r_1$. Hieraus ist zuerst ersichtlich, daß r_1 ein gemeinschaftlicher Theiler von b sowohl als von a sey. Dann aber auch, daß r_1 der größte gemeinschaftliche Theiler dieser beyden Zahlen sey. Denn setzet, daß irgend ein gemeinschaftlicher Theiler dieser zwey Zahlen ϱ sey; so muß, weil $a=q_1b+r_1$ ist, auch q_1b+r_1 theilbar durch ϱ seyn. Da nun b, also muß auch q_1b theilbar durch ϱ seyn; so muß nach §. 21. auch r_1 theilbar durch ϱ seyn. Also kann ϱ auf keinen Fall $>r_1$ seyn. Unser Lehrsatz gilt also auch, wenn die Anzahl der Divisionen $=2$ ist. Daß er nun allgemein für eine jede Anzahl von Divisionen gelte, erhellet am deutlichsten so. Setzet, die Division gehe erst bey dem durch r_n bezeichneten Reste auf;

und dieser gebe durch seine Division in den vorhergehenden r_{n-1} den genauen Quotienten q_n: so bestehen folgende Gleichungen:

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ r_2 &= q_4 r_3 + r_4, \\ &\cdots\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} r_n. \end{aligned}$$

Aus der letzten Gleichung erhellet, daß r_{n-1} theilbar sey durch r_n. Daraus aber und aus dem vorletzten ergibt sich, weil sowohl r_{n-1} als auch r_n theilbär durch r_n sind, daß auch r_{n-2} theilbar durch r_n seyn müsse. Steigen wir nun in diesen Gleichungen anfangend von der letzten gliedweise bis zu der ersten auf: so erhellet, daß jede folgende (d. i. nächst höhere) in ihrem ersten Gliede zusammengesetzt sey aus zwey Summanden, deren der eine ein Product ist, davon der eine Factor bereits in der nächst vorhergehenden Gleichung (links) vorkam, der andere ebenfalls schon in dieser Gleichung (rechts) vorkam, die endlich beyde als theilbar durch r_n erkannt wurden. Daraus ergibt sich dann, daß auch das linke Glied in dieser nächst folgenden (oder höheren) Gleichung theilbar durch r_n seyn müsse. Und somit können wir nach einer endlichen Menge von Fortschreiten bis zu den Gleichungen $b = q_2 r_1 + r_2$ und $a = q_1 b + r_1$ gelangen, die darthun, daß auch b und a theilbar durch r_n seyn müssen, d. h. daß r_n ein gemeinschaftlicher Theiler der beyden Zahlen a und b sey. Daß aber dieses r_n zugleich auch der größte gemeinschaftliche Theiler für diese Zahlen sey; erhellet wieder so. Setzet, es sey ϱ irgend ein Theiler, den a und b gemeinschaftlich haben: so lehrt der Anblick der obersten Gleichung $a = q_1 b + r_1$, daß ϱ, weil es in a und b, also auch $q_1 b$ aufgeht, nach §. 21. auch in r_1 aufgehen müsse. Dann aber folgt auf gleiche Art aus der zweyten Gleichung $b = q_2 r_1 + r_2$, daß ϱ, weil es in b und r_1 oder $q_2 r_1$ aufgeht, auch in r_2 aufgehen müsse. Man sieht nun von selbst, daß wir durch eine endliche Menge von Wiederhohlungen dieser Schlüsse bis zu der vorletzten Gleichung $r_{n-2} = q_n r_{n-1} + r_n$ und zu der Folgerung gelangen können, daß ϱ, weil es in r_{n-2} und r_{n-1} aufgeht, auch in r_n aufgehen müsse. Hieraus erhellet aber, daß ϱ unmöglich $> r_n$ seyn könne; also, daß r_n der größte gemeinschaftliche Theiler der beyden Zahlen a und b sey.

Beyspiel. Ist $a=72$, $b=42$; so findet sich bey der ersten Division der Quotient $q=1$ und der Rest $r_1=30$; bey der Division von diesem in b, der Quotient $q_1=1$, der Rest $r_2=12$, bey der Division von diesem in r_1 der Quotient $q_2=2$ und der Rest $r_3=6$; bey der Division mit diesem in r_2 erscheint als vollkommener Quotient $q_3=2$. Also ist $r_3=6$ der größte gemeinschaftliche Theiler der beyden Zahlen 72 und 42.

§. 50. Zusatz. Wenn also r_n die Einheit ist, so sind die Zahlen a und b relative Primzahlen.

§. 51. Lehrsatz. Es lassen sich Vielfache von a sowohl als von b auffinden, die so beschaffen sind, daß ihre Unterschiede jedem der Reste $r_1, r_2, r_3, \ldots$ gleich werden.

Beweis. Ein Paar Vielfache von a und b, deren Unterschied dem ersten Reste r_1 gleich kommt, sind a und $q_1 b$; weil $a-q_1 b=r_1$. Da aber der zweyte Rest $r_2=b-q_2 r_1$ ist; so erhalten wir, wenn wir den Werth von r_1 aus der vorigen Gleichung substituiren: $r_2=b-q_2(a-q_1 b)=(q_1 q_2+1)b-q_2 a$, zwey Vielfache von a und b, deren Unterschied $=r_2$ ist. Aus der Natur der obigen Gleichungen ist nun leicht zu ersehen, daß man so immer weiter fortschließen könne. Denn gilt der Satz für zwey nächst kleinere Werthe von m, d. h. für r_{m-1} und r_{m-2}, so gilt er auch für r_m. Denn weil die Gleichung $r_m=r_{m-2}-q_m r_{m-1}$ bestehet; so muß, wenn r_{m-2} und r_{m-1} durch Unterschiede von gewissen Vielfachen der Zahlen a und b ausgedrückt werden können, auch für r_m eine Summe oder ein Unterschied gewisser Vielfachen von a und b zum Vorschein kommen, wenn wir die Werthe von r_{m-2} und r_{m-1} durch a und b ausgedrückt in jene Gleichung setzen. Aber eine Summe von Vielfachen der a und b kann r_m, da es $<b$ und $<a$ ist, unmöglich seyn. Es muß sich also durch einen Unterschied solcher Vielfachen ausdrücken lassen. So war z. B. einer der Reste bey den zwey Zahlen 72 und 42, $r_2=12$, also muß es auch gewisse Vielfache von 72 und 42 geben, deren Unterschied $=12$ ist. Dergleichen Vielfache sind 1.72 und $2.42=84$, denn $84-72=12$.

§. 52. Zusatz. Ist also einer der Reste $r_1, r_2, \ldots$, auf die man bey dem Verfahren des Lehrsatzes aus §. 49. kommt, $=1$; so gibt es gewisse Vielfache von a und b, deren Unterschied $=1$ ist. Ein solcher Rest zeigte sich (§. 13.) bey den Zahlen $a=54$ und $b=13$. Also muß es gewisse Vielfache von 54 und 13 geben, deren Unterschied $=1$ ist. In der That ist $25.13-6.54=1$.

§. 53. Lehrsatz. Wenn die zwey Zahlen a und b relative Primzahlen sind; so gibt es jederzeit gewisse Vielfache derselben

$ma.\,nb$, deren Unterschied $ma-nb$ oder $nb-ma$ (jenachdem $ma >$ oder $< nb) = 1$ ist.

Beweis. Wenn a und b relative Primzahlen sind; so wird man durch das Verfahren des §. 49., wenn man mit einer dieser Zahlen z. B. b in die andere a, und mit dem Reste in den vorigen Divisor u. s. f. dividirt, zuletzt auf einen Rest $r^{(n)}$, der $= 1$ ist, kommen. Denn der letzte Rest $r^{(n)}$ darf nicht > 1 seyn, weil er ein gemeinschaftlicher Theiler von a und b ist. Ist aber einer der Reste, auf welche man bey jenem Verfahren kommt, $= 1$; so gibt es auch gewisse Vielfache von a und b, ma und nb, deren Unterschied gleich diesem Reste, also $= 1$ ist. So sind 8 und 21 ein Paar relative Primzahlen, daher sind auch ein Paar Vielfache derselben, z. B. 8.8 und 3.21 angeblich, deren Unterschied $64-63 = 1$ ist.

§. 54. Lehrsatz. Wenn es erst Ein Vielfaches von a und Ein dazu gehöriges von b gibt, dabey der Unterschied $ma-nb$ einer gewissen Zahl p gleich wird; so gibt es auch unendlich viele Paare von Vielfachen, die eben denselben Unterschied p haben.

Beweis. Ist $ma-nb=p$; so ist, x sey was immer für eine wirkliche Zahl, auch $(xb+m)a-(xa+n)b=p$. Indem wir nun für x jeden beliebigen Wert annehmen können, erhalten wir auch unendlich viele verschiedene Vielfache von a und b, die der Bedingung, daß ihre Differenz $=p$ ist, entsprechen. Weil z. B 4.8 und 1.21 ein Paar Vielfache von 8 und 21 sind, welche den Unterschied 11 geben: so geben auch $(4+2.21)8$ und $(1+2.8)21$ d. i. 368 und 357, ingleichen $(4+5.21)8$ und $(1+5.8)21$ d. i. 536 und 525, u. s. w. den Unterschied 11.

§. 55. Lehrsatz. Wenn M ein gemeinschaftliches Vielfache der Zahlen $a, b, c\ldots$ und die Quotienten $\frac{M}{a}, \frac{M}{b}, \frac{M}{c}, \ldots$ sind nicht relative Primzahlen, sondern sie haben einen von 1 verschiedenen gemeinschaftlichen Theiler m: so ist $\frac{M}{m}$ ein kleineres gemeinschaftliches Vielfache der Zahlen $a, b, c, \ldots$

Beweis. Wenn die Quotienten $\frac{M}{a}, \frac{M}{b}, \frac{M}{c}, \ldots$ einen gemeinschaftlichen Theiler an der von 1 verschiedenen Zahl m haben; so ist $\frac{M}{a} : m =$ einer wirklichen Zahl α, $\frac{M}{b} : m =$ einer wirklichen Zahl β, $\frac{M}{c} : m =$ einer wirklichen Zahl γ u. s. w. Also ist auch

$\frac{M}{m} = a\alpha$, $\frac{M}{m} = b\beta$, $\frac{M}{m} = c\gamma$ u. s. w. Somit ist $\frac{M}{m}$ eine wirkliche Zahl, und dieß zwar eine solche, die $< M$ ist und theilbar durch $a, b, c, \ldots$. also ein gemeinschaftliches Vielfache von $a, b, c \ldots$., das kleiner ist als M. So haben die Zahlen 2, 3 und 7 ein gemeinschaftliches Vielfache an der Zahl 84; weil aber die Quotienten $\frac{84}{2} = 42$, $\frac{84}{3} = 28$, $\frac{84}{7} = 12$ noch einen gemeinschaftlichen Theiler 2 haben; so ist 84 nicht ihr kleinstes, sondern $\frac{84}{2} = 42$ ein kleineres gemeinschaftliches Vielfache derselben.

§. 56. Zusatz. Wenn also umgekehrt M das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots$ ist; so können die Quotienten $\frac{M}{a}, \frac{M}{b}, \frac{M}{c} \cdots$ keinen gemeinschaftlichen Theiler (der von Eins verschieden ist) haben, sondern sie müssen relative Primzahlen in der weiteren Bedeutung seyn.

§. 57. Lehrsatz. Jedes gemeinschaftliche Vielfache der Zahlen $a, b, c \ldots$. ist durch das kleinste Vielfache derselben theilbar.

Beweis. Seyen M und N ein Paar gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots$ Wenn nun N größer und doch nicht theilbar durch M ist; so gibt die versuchte Division von M in N eine Zahl μ zum nächst kleineren Quotienten und einen Rest R. Wir erhalten also $N = \mu M + R$. Weil nun M und N beyde gemeinschaftliche Vielfache der Zahlen $a, b, c \ldots$. sind: so geht jede derselben sowohl in N als auch in M auf; mithin (wegen der Gleichung $N = \mu M + R$). (nach §. 21.) auch in R. Und somit ist auch R ein gemeinschaftliches Vielfache der besagten Zahlen. R aber ist $< M$. also ist M nicht das kleinste gemeinschaftliche Vielfache derselben. Ist also irgend ein Vielfaches M das kleinste, so muß ein jedes andere N nicht nur größer, sondern auf die Art größer seyn. daß es durch M getheilt. keinen Rest gibt. d. h. es muß ein Vielfaches auch von M selbst seyn. So ist $42 = 3 \cdot 2 \cdot 7$ gewiß das kleinste gemeinschaftliche Vielfache der Zahlen 2, 3, 7; daher das größere 84 theilbar durch 42.

§. 58. Lehrsatz. Wenn die Quotienten $\frac{M}{a}, \frac{M}{b}, \frac{M}{c}, \cdots$ relative Primzahlen in der weiteren Bedeutung (§. 31.) sind; so ist M das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots$

Beweis. Bezeichnen wir das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots$ durch m; so muß M, wenn es von m verschieden ist. nach dem vorigen Satze theilbar durch

m seyn. Also muß $\frac{M}{m}$ = einer wirklichen Zahl μ, oder $M = m\mu$ seyn. Ferner müssen, wenn m ein Vielfaches der Zahlen $a, b, c, \ldots$ ist: $\frac{m}{a}, \frac{m}{b}, \frac{m}{c}, \ldots$ lauter wirkliche Zahlen seyn. Da nun $\frac{M}{a} = \mu\frac{m}{a}$, $\frac{M}{b} = \mu\frac{m}{b}$, $\frac{M}{c} = \mu\frac{m}{c}$ ....; so sieht man, daß die Quotienten $\frac{M}{a}, \frac{M}{b}, \frac{M}{c}, \ldots$ den gemeinschaftlichen Factor μ haben. Sollen sie gleichwohl, wie der Lehrsatz voraussetzt, relative Primzahlen seyn, so muß $\mu = 1$ und somit $M = m$ seyn, d. h. M ist das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots$. So sind die Quotienten $\frac{60}{4} = 15$, $\frac{60}{5} = 12$ und $\frac{60}{30} = 2$ relative Primzahlen in der weiteren Bedeutung: also ist 60 das kleinste gemeinschaftliche Vielfache der Zahlen 4. 5. 30.

§. 59. Lehrsatz. Wenn der Unterschied zweyer Producte $abcd\ldots$ und $\alpha\beta\gamma\ldots$ der Einheit gleicht; so ist jeder Factor des einen mit jedem Factor des anderen eine relative Primzahl.

Beweis. Setzet, daß Einer von den Factoren des Productes $abcd\ldots$ z. B. a und einer von den Factoren des Productes $\alpha\beta\gamma\ldots$ z. B. α den gemeinschaftlichen Theiler μ haben; so hat auch der Unterschied $abc\ldots - \alpha\beta\gamma\ldots$ (oder, falls $abc\ldots < \alpha\beta\gamma\ldots$ ist, der Unterschied $\alpha\beta\gamma\ldots - abc\ldots$) den Theiler μ. Da aber dieser Unterschied $abc\ldots - \alpha\beta\gamma\ldots$ (oder $\alpha\beta\gamma\ldots - abc\ldots$) $= 1$ seyn soll; so muß auch 1 theilbar durch μ seyn. Also muß $\mu = 1$ seyn, d. h. die Zahlen a und b haben keinen anderen gemeinschaftlichen Theiler als die Einheit, oder sie sind relative Primzahlen. So ist z. B. $15 - 14 = 1$, daher die Factoren von $15 = 3.5$ relative Primzahlen mit den Factoren von $14 = 2.7$.

§. 60. Lehrsatz. Wenn ein Paar Producte ab und $\alpha\beta$ einander gleich kommen; und es sind ein Factor a des ersten, und ein Factor α des zweyten relative Primzahlen untereinander: so muß der andere Factor β des zweyten durch a, und der andere Factor b des ersten durch α theilbar seyn.

Beweis. Weil $ab = \alpha\beta$, so ist $a = \frac{\alpha\beta}{b}$, und $\alpha = \frac{ab}{\beta}$. Da nun a und α relative Primzahlen sind; so müssen auch die Quotienten $\frac{\alpha\beta}{b}$ und $\frac{ab}{\beta}$ relative Primzahlen seyn. Folglich muß ihr gemeinschaftliches Vielfache $\alpha\beta = ab$ das kleinste gemeinschaftliche Vielfache der Zahlen b und β seyn (§. 58.). Allein auch das Product $b\beta$ ist ein gemeinschaftliches Vielfache der Zahlen b und β. Folglich

muß (nach §. 57.) $b\beta$ theilbar seyn durch $\alpha\beta = ab$. Also bezeichnen die Ausdrücke $\frac{b\beta}{\alpha\beta}$ und $\frac{b\beta}{ab}$ oder $\frac{b}{\alpha}$ und $\frac{\beta}{a}$ ein Paar wirkliche Zahlen. Also ist b theilbar durch α und β durch a. So ist $3.14 = 7.6$ und die Factoren 3 und 7 sind relative Primzahlen, daher der andere Factor 14 theilbar durch 7 und der andere Factor 6 theilbar durch 3.

§. 61. Zusatz. Wenn also umgekehrt ab und $\alpha\beta$ ein Paar Producte von solcher Art sind, daß jeder der beyden Factoren a und b des einen eine relative Primzahl ist zu jedem der beyden Factoren α und β des anderen: so können beyde Producte einander sicher nicht gleich seyn.

§. 62. Lehrsatz. Wenn ein Product ab theilbar ist durch eine Zahl α, die eine relative Primzahl mit dem Factor a ist: so ist der andere Factor b durch dieselbe theilbar.

Beweis. Ist ab theilbar durch α, so muß $\frac{ab}{\alpha}$ = einer wirklichen Zahl β seyn. und man hat $ab = \alpha\beta$, ein Paar Producte, die einander gleich kommen, und in dem einen ab ist ein Factor a eine relative Primzahl mit einem Factor α in dem anderen. Also muß nach dem vorigen Lehrsatze der andere Factor b theilbar durch α seyn. So ist das Product $56.11 = 616$ theilbar durch 7, eine Zahl, die eine relative Primzahl mit dem Factor 11 ist: also muß diese Zahl in dem anderen Factor aufgehen.

§. 63. Zusatz. Also auch, wenn ein Product $abcd\ldots l$, welches aus einer beliebigen, aber doch endlichen Menge Factoren zusammengesetzt ist, sich theilen läßt durch eine Zahl m, die eine relative Primzahl ist, mit allen Factoren $a, b, c, d, \ldots, k$ dieses Productes, bis auf den einen l; so muß l theilbar seyn durch m. Denn wenn wir dieses Product erst als zusammengesetzt nur aus den zwey Factoren a einerseits und dem Producte $b.cd\ldots kl$ andererseits betrachten; so folgt aus dem vorigen Lehrsatze, daß sofern $a.bcd\ldots kl$ theilbar durch m ist, und a und m gleichwohl relative Primzahlen sind, es nur der andere Factor $bcd\ldots kl$ seyn müsse, der durch m theilbar ist. Da nun $bcd\ldots kl$ ein Product ist, welches um Einen Factor weniger enthält, als das zuerst betrachtete $abcd\ldots kl$; so sieht man, daß wir durch eine endliche Menge von Wiederhohlungen dieses Schlusses endlich zu dem Producte kl, das nur aus zwey Factoren bestehet, gelangen; und indem wir auch von diesem behaupten, daß es durch m theilbar seyn müsse, daß aber der

eine Factor k eine relative Primzahl mit m ist, wird sich durch eine neue Anwendung des vorigen Lehrsatzes der Schluß, daß also l theilbar durch m seyn müsse, ergeben. So lehrt uns die Division, daß die Zahl 19950 theilbar durch 19 sey. Diese Zahl aber zerfällt in die Factoren $2 . 3 . 25 . 133$; da nun die ersteren drey: 2, 3, und 25 relative Primzahlen mit 19 sind; so folgt, daß der letzte Factor 133 theilbar durch 19 seyn müsse. Es ist nähmlich $\frac{1}{1}^{3}{}_{)}^{3} = 7$.

§. 64. Lehrsatz. Sind a und b relative Primzahlen; α aber ein Theiler von a; so sind auch α und b relative Primzahlen.

Beweis. Denn hätten α und b einen gemeinschaftlichen Theiler $= \mu$: so müßten um so gewisser auch a (weil es ein Vielfaches von α ist) und b diesen gemeinschaftlichen Theiler haben. So sind 133 und 6 relative Primzahlen; 19 aber ein Factor von 133. Also um so gewisser 19 und 6 relative Primzahlen.

§. 65. Lehrsatz. Wenn m und a relative Primzahlen, m und das Product ab aber nicht relative Primzahlen sind; so sind auch m und b nicht relative Primzahlen.

Beweis. Wenn m und ab nicht relative Primzahlen sind: so gibt es irgend eine absolute Primzahl μ, die beyde theilt. Theilt aber μ die m, so darf sie nicht theilen a, weil sonst m und a nicht relative Primzahlen wären. Wenn aber μ das Product ab, nicht aber den einen Factor a theilt, so folgt aus §. 62., daß μ den anderen Factor b theile. Also sind m und b beyde theilbar durch μ, folglich nicht relative Primzahlen untereinander. So sind 6 und 25 relative Primzahlen, 6 und $250 = 25 . 10$ aber nicht relative Primzahlen; also auch 6 und 10 nicht relative Primzahlen.

§. 66. Zusatz. Wenn also umgekehrt m und a, und eben so auch m und b relative Primzahlen sind; so sind auch m und das Product ab relative Primzahlen. So ist die Zahl 6 eine relative Primzahl mit 25 sowohl als auch mit 7; daher auch gewiß mit dem Producte $25 . 7 = 175$.

§. 67. Zusatz. Wenn m eine relative Primzahl ist mit jeder der Zahlen $a, b, c, d \ldots$. deren Menge endlich ist; so ist m auch eine relative Primzahl mit dem Producte aus allen diesen Zahlen $abcd \ldots$ Denn weil m eine relative Primzahl zu a und b ist; so ist m nach dem vorhergehenden Zusatze eine relative Primzahl zu der Zahl ab, also zu den zwey Zahlen ab und c, folglich auch zu der Zahl abc. Man sieht von selbst, daß sich diese Schlußart auf jede beliebige Menge von Zahlen, wenn sie nur endlich

ist, ausdehnen lasse, nach der Weise, die wir schon mehrmahl angegeben haben.

§. 68. Zusatz. Stehet daher jede der Zahlen $\alpha, \beta, \gamma, \ldots$, deren Menge beliebig, aber doch endlich ist, in dem Verhältnisse einer relativen Primzahl zu jeder der Zahlen $a, b, c, \ldots$, deren Menge abermahls beliebig, aber doch endlich ist: so steht auch das Product $\alpha\beta\gamma\ldots$ zu dem Producte $abc\ldots$ in dem Verhältnisse einer relativen Primzahl; und umgekehrt, wenn dieses ist, so ist auch jenes. Denn wenn jede der Zahlen $\alpha, \beta, \gamma\ldots$ zu jeder der Zahlen $a, b, c, \ldots$ eine relative Primzahl ist; so ist auch jede der Zahlen $\alpha, \beta, \gamma\ldots$ zu dem Producte $abc\ldots$ eine relative Primzahl. Also auch die Zahl $abc\ldots$ zu dem Producte $\alpha\beta\gamma\ldots$ eine relative Primzahl. Daß aber der Satz auch umgekehrt gelte, erhellet daraus, weil, wenn irgend einer der Factoren $\alpha, \beta, \gamma, \ldots$ einen gemeinschaftlichen Theiler mit einem der Factoren $a, b, c, \ldots$ hätte, dann auch das ganze Product $\alpha\beta\gamma\ldots$ diesen gemeinschaftlichen Theiler mit dem Producte $abc\ldots$ hätte.

§. 69. Zusatz. Wenn also jede der Zahlen $a, b, c, \ldots l$ eine relative Primzahl mit jeder der Zahlen $\alpha, \beta, \gamma, \ldots \lambda$ ist; so sind die Producte $a.b.c\ldots l$ und $\alpha.\beta.\gamma\ldots\lambda$ einander sicher nicht gleich. Denn zerlegen wir jedes dieser Producte nur in zwey Factoren, indem wir z. B. $b.c\ldots l = L$, und $\beta.\gamma\ldots\lambda = \Lambda$ als eine einzige Zahl betrachten; so ist jeder der beyden Factoren a und L des Productes $a.L$ eine relative Primzahl mit jedem der beyden Factoren α und Λ des Productes $\alpha\Lambda$ (§. 68.). Und nun folgt aus §. 61., daß diese Producte einander nicht gleich seyn können.

§. 70. Zusatz. Wenn α und a relative Primzahlen sind, so sind auch je zwey Potenzen von α und a wie α^m und a^n, wo m und n beliebige Zahlen seyn können, relative Primzahlen. Ebenso sind, wenn α und a, β und b, γ und $c\ldots$ relative Primzahlen sind, auch die Producte $\alpha^m.\beta^p.\gamma^r\ldots$ und $a^n.b^q.c^s\ldots$ relative Primzahlen, die Exponenten $m, p, r, \ldots n, q, s, \ldots$ seyen was immer für wirkliche Zahlen. Denn in allen diesen Fällen gilt, daß jeder einzelne Factor des einen Products mit jedem einzelnen Factor des anderen eine relative Primzahl ist. So sind die Zahlen 2 und 3 relative Primzahlen; daher auch jede Potenz von 2 z. B. $2^3 = 8$ und jede Potenz von 3 z. B. $3^4 = 81$ relative Primzahlen untereinander.

§. 71. Lehrsatz. Kein Product P aus einer endlichen Menge von absoluten Primzahlen, gleichviel ob sich darunter auch einige gleiche befinden oder nicht, gleicht einer Zahl, die eine Primzahl,

oder ein Product aus anderen als den aus P, oder zwar aus denselben, aber nicht in derselben Anzahl wie in P vorkommenden Primzahlen ist.

Beweis. Daß ein Product nicht einer einzigen Primzahl gleich seyn könne, ergibt sich schon aus dem bloßen Begriffe einer Primzahl. Daß aber ein Product P, welches aus einer gewissen endlichen Menge von Primzahlen zusammengesetzt ist, nicht gleich seyn könne einem Producte, welches aus anderen Primzahlen zusammengesetzt ist; erhellet daraus, weil absolute Primzahlen auch relative sind, und dargethan wurde, daß ein Paar Producte $\alpha\beta\gamma\ldots$ und $abcd\ldots$, wenn die Factoren des einen mit den Factoren des anderen relative Primzahlen sind, einander nicht gleich seyn können. Wenn endlich in beyden Producten zwar einige, aber nicht alle einfachen Factoren gleich sind, oder es sind wohl alle gleich, aber es ist nicht jeder in beyden Producten in derselben Anzahl vorhanden: so lasset uns wieder zwey Fälle unterscheiden: den einen, wo die einfachen Factoren des Productes P alle auch in dem anderen Q und diejenigen, die in P mehrmahls vorkommen, auch in Q eben so oft oder noch mehrmahl enthalten sind; den anderen, wo dieses nicht so ist. In dem ersten Falle können wir das Product Q in zwey Factoren zerlegen, deren der eine ganz aus denselben Factoren wie P und in derselben Anzahl zusammengesetzt ist, der andere die noch übrigen Factoren (deren es wenigstens einen gibt) in sich faßt. Nennen wir diesen q: so ist $Q = P \cdot q$ und folglich gewiß nicht $= P$, weil q nicht $= 1$ ist. In dem anderen Falle gibt es in P sowohl als in Q einige eigene einfache Factoren, die in dem anderen Producte entweder gar nicht, oder doch nicht sovielmahl vorkommen; es wird also möglich seyn, P sowohl als auch Q in zwey Factoren zu zerlegen, deren der eine die in P und Q gemeinschaftlich vorkommenden, von den anderen beyden aber ein jeder diejenigen einfachen Factoren enthält, die P oder Q eigenthümlich hat, oder die zwar auch in dem anderen Producte, aber dort nicht sovielmahl vorkommen. Bezeichnen wir diese letzteren durch p und q und den Factor, der aus denselben Primzahlen besteht, also auch beyderseits gleich seyn muß, durch m, so ist $P = mp$ und $Q = mq$. Sollte also $P = Q$ seyn, so müßte auch $p = q$ seyn. Aber p und q haben keinen gemeinschaftlichen einfachen Factor, und sind also sicher ungleich. Folglich auch P und Q.

§. 72. Lehrsatz. Wenn eine Zahl a sich theilen läßt durch eine andere b, so muß ein jeder einfache Factor, in welchen

sich b zerschlagen läßt, auch in a vorkommen, und jeder, den b mehrfach enthält, muß auch in a wenigstens eben so oft enthalten seyn.

Beweis. Wenn $\frac{a}{b}$ = einer wirklichen Zahl q ist: so ist $a = bq$. Also muß bq dieselben einfachen Factoren und einen jeden in derselben Anzahl wie a enthalten. Also darf nicht schon in b ein einfacher Factor, der in a fehlt, oder doch öfter als er in a erscheint, vorkommen. So läßt sich 180 theilen durch 60: 60 aber bestehet aus den einfachen Factoren $2^2 . 3 . 5$. und 180 aus $2^2 . 3^2 . 5$; woraus zu sehen, daß jeder einfache Factor, der in 60 vorkommt, auch in 180 und hier wenigstens eben so oft vorkomme.

§. 73. Zusatz. Wenn also unter den einfachen Factoren, in welche sich b zerschlagen läßt, einer vorkommt, der in a fehlt, oder hier wenigstens nicht so oft als in b vorkommt, so ist a nicht theilbar durch b. So ist z. B. $36 = 2^2 . 3^2$ nicht theilbar durch $24 = 2^3 . 3$, weil die letztere Zahl den einfachen Factor 2 dreymahl, die erstere aber nur zweymahl enthält.

§. 74. Lehrsatz. Wenn von den mehreren Zahlen $a, b, c, d, \ldots$ jede in ihre einfachen Factoren zerlegt ist, und wir bilden ein Product m aus allen in diesen Zahlen gemeinschaftlich vorkommenden Factoren, so zwar, daß wir denjenigen einfachen Factor, der in diesen Zahlen überall mehrfach erscheint, in das Product sovielmahl aufnehmen, als vielmahl er in derjenigen Zahl erscheint, in der er am seltensten vorkommt: so ist m der größte gemeinschaftliche Theiler der Zahlen $a, b, c, d, \ldots$

Beweis. Daß m ein Theiler dieser Zahlen ist, erhellet aus §. 72., daß es aber keinen größeren gemeinschaftlichen Theiler für diese Zahlen gebe, folgt daraus, weil jeder, also auch der größte gemeinschaftliche Theiler dieser Zahlen nach §. 73. aus keinen anderen einfachen Factoren zusammengesetzt seyn darf, als aus solchen, die auch in einer jeden der gegebenen Zahlen $a, b, c, d, \ldots$ vorkommen, und wenigstens eben so oft als in ihm vorkommen.

Beyspiel. Ist $a = 60 = 2^2 . 3 . 5$; $b = 240 = 2^4 . 3 . 5$, $c = 280 = 2^3 . 5 . 7$; so ist der größte gemeinschaftliche Theiler von $a . b . c$ die Zahl $2^2 . 5 = 20$.

§. 75. Lehrsatz. Wenn m der größte gemeinschaftliche Theiler der Zahlen $a, b, c, d, \ldots$ ist; so sind die Quotienten $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}, \cdots$ relative Primzahlen in der weiteren Bedeutung.

Beweis. Sey μ ein diesen Quotienten gemeinschaftlicher Theiler: so sind $\frac{a}{m}:\mu$, $\frac{b}{m}:\mu$. $\frac{c}{m}:\mu\ldots$ wirkliche Zahlen; folglich auch $\frac{a}{\mu m}, \frac{b}{\mu m}, \frac{c}{\mu m}, \cdots$ Also ist μm ein gemeinschaftlicher Theiler der Zahlen $a, b, c, \ldots$ Ist aber m der größte: so darf μm nicht $> m$ seyn. Also muß $\mu = 1$ seyn. d. h. die Quotienten $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}, \cdots$ haben keinen anderen gemeinschaftlichen Theiler als die Einheit. So haben z. B. die Zahlen $\frac{60}{20} = 3$, $\frac{240}{20} = 12$, $\frac{280}{20} = 14$ offenbar keinen gemeinschaftlichen Theiler untereinander.

§. 76. Zusatz. Wenn also umgekehrt die Quotienten $\frac{a}{m}, \frac{b}{m}, \frac{c}{m} \cdots$ nicht relative Primzahlen sind, sondern einen von der Einheit verschiedenen Theiler μ haben, so ist m nicht das größte gemeinschaftliche Maß der Zahlen $a, b, c, \ldots$, sondern μm ist ein größeres. So ist 8 nicht das größte gemeinschaftliche Maß der Zahlen 16, 32 und 48, weil die Quotienten $\frac{16}{8} = 2$, $\frac{32}{8} = 4$ und $\frac{48}{8} = 6$ noch den gemeinschaftlichen Theiler 2 haben. Daher ist $2.8 = 16$ ein größeres gemeinschaftliches Maß für jene Zahlen.

§. 77. Lehrsatz. Der größte gemeinschaftliche Theiler der Zahlen $a, b, c, \ldots$ ist durch jeden kleineren gemeinschaftlichen Theiler derselben Zahlen theilbar.

Beweis. Der größte gemeinschaftliche Theiler der Zahlen $a, b, c, \ldots$ ist derjenige, der alle ihre gemeinschaftlich zukommenden einfachen Factoren, und denjenigen, der etwa mehrfach in einer jeden erscheint, soviehmahl enthält, als er dort vorkommt, wo er am Seltensten vorkommt. Gibt es nebst diesem größten gemeinschaftlichen Theiler noch einen anderen kleineren: so muß derselbe nur einen Theil der in den Zahlen $a, b, c, \ldots$ vorkommenden einfachen Factoren oder wenn alle, doch nicht jeden soviehmahl enthalten, als er selbst in derjenigen Zahl vorkommt, in der er am Seltensten vorkommt. Daraus ergibt sich aber, daß dieser kleinere Theiler in dem größten aufgehen müsse. So haben z. B. die Zahlen 60, 140 und 280 die gemeinschaftlichen Theiler 2, 5, 10 und 20: und jeder kleinere derselben gehet in den größten 20 auf.

§. 78. Lehrsatz. Wenn ein gewisser Theiler μ nicht der größte gemeinschaftliche Theiler der Zahlen $a, b, c, \ldots$ ist: so

sind die Quotienten $\frac{a}{\mu}, \frac{b}{\mu}, \frac{c}{\mu}, \cdots$ nicht relative Primzahlen untereinander.

Beweis. Weil μ nicht der größte gemeinschaftliche Theiler der Zahlen $a, b, c, \ldots$ ist: so gibt es noch einen größeren und einen größten (§.). Sey dieser m: so ist m theilbar durch μ so zwar, daß $\frac{m}{\mu}$ = einer wirklichen Zahl. die > 1 ist. Bezeichnen wir diese durch π; so ist $\mu = \frac{m}{\pi}$ und die wirklichen Zahlen $\frac{a}{\mu}, \frac{b}{\mu}, \frac{c}{\mu} \cdots$ lassen sich auch so ausdrücken $\left(\frac{a}{m}\right)\pi, \left(\frac{b}{m}\right)\pi, \left(\frac{c}{m}\right)\pi, \ldots$. wo $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}, \cdots$ lauter wirkliche Zahlen sind. Hieraus ist denn ersichtlich, daß $\frac{a}{\mu}, \frac{b}{\mu}, \frac{c}{\mu}, \cdots$ alle den gemeinschaftlichen Factor π haben, der > 1 ist. Und somit ist erwiesen, daß diese Zahlen keine relative Primzahlen sind. So ist 5 nicht der größte gemeinschaftliche Theiler der Zahlen 15. 30 und 45; daher die Quotienten $\frac{15}{5} = 3$. $\frac{30}{5} = 6$ und $\frac{45}{5} = 9$ nicht relative Primzahlen untereinander sind. sondern noch den gemeinschaftlichen Theiler 5 haben.

§. 79. Zusatz. Wenn also umgekehrt die Quotienten $\frac{a}{m}, \frac{b}{m}, \frac{c}{m}, \cdots$ relative Primzahlen auch nur in der weiteren Bedeutung des §. 31. sind; so ist m das größte gemeinschaftliche Maß der Zahlen $a, b, c, \ldots$ So sind z. B. die Quotienten $\frac{30}{15} = 2$. $\frac{45}{15} = 3$ und $\frac{60}{15} = 4$ relative Primzahlen in der weiteren Bedeutung; also 15 der größte gemeinschaftliche Theiler der Zahlen 30, 45 und 60.

§. 80. Lehrsatz. Wenn eine Zahl m ein Vielfaches seyn soll der Zahlen $a, b, c, \ldots$. so muß sie alle in diesen Zahlen vorkommenden von einander verschiedenen einfachen Factoren, und diejenigen, welche in einer dieser Zahlen mehrfach vorkommen, so oft enthalten, als sie dort vorkommen, wo sie am Oeftesten vorkommen.

Beweis. Enthält m einen einfachen Factor einer der Zahlen $a, b, c, \ldots$ nicht, oder nicht sovielmahl. als er in dieser Zahl vorkommt. so ist m auch nicht theilbar durch diese Zahl (§. 73). Also kein Vielfaches der sämmtlichen $a, b, c, \ldots$ So ist 36 ein Vielfaches von 4, 12 und 18: allein auch jeder einfache Factor, der in den Zahlen $4 = 2^2$, $12 = 2^2 . 3$, $18 = 2 . 3^2$ vorkommt. erscheint

auch in $36 = 2^2 . 3^2$, und zwar so oft als in derjenigen der Zahlen 4. 12. 18, die ihn am Oeftesten enthält.

§. 81. Lehrsatz. Wenn eine Zahl m keine andere Factoren enthält als nur diejenigen, die in den Zahlen $a, b, c, \ldots$ vorkommen, und jeden, der in einer dieser Zahlen mehrfach erscheint, so oft als in derjenigen, in der er am Oeftesten vorkommt: so ist sie das kleinste Vielfache, das diese Zahlen haben.

Beweis. Denn eine Zahl, die kleiner ist, enthält entweder nicht alle diese Factoren, oder nicht jeden so oft als es hier angegeben wurde, und ist eben darum kein Vielfaches von allen diesen Zahlen. So wäre z. B. das kleinste Vielfache der Zahlen $9 = 3 . 3$, $18 = 2 . 3 . 3$, $20 = 2 . 2 . 5$ und $35 = 5 . 7$, kein anderes als $2 . 2 . 3 . 3 . 5 . 7 = 1260$.

§. 82. Zusatz. Wenn je zwey von den Zahlen $a, b, c, d, \ldots$ relative Primzahlen sind; so ist das kleinste gemeinschaftliche Vielfache derselben das Product $abcd\ldots$ aus ihnen allen. Denn unter der angenommenen Voraussetzung gibt es nicht einen einzigen von der Einheit verschiedenen Factor, welchen zwey oder mehrere der Zahlen $a, b, c, d, \ldots$ gemeinschaftlich haben. Um also alle in diesen Zahlen vorkommenden einfachen Factoren zu vereinigen, müssen wir diese Zahlen alle zusammen multipliziren. So ist das kleinste gemeinschaftliche Vielfache der Zahlen: 2, 3, 35 (= 5 . 7) und 11, kein anderes als $2 . 3 . 5 . 7 . 11 = 2310$.

§. 83. Lehrsatz. Wenn m der größte gemeinschaftliche Theiler der beyden Zahlen a und b ist; so ist $\frac{ab}{m}$ das kleinste gemeinschaftliche Vielfache derselben.

Beweis. Wenn m der größte gemeinschaftliche Theiler der beyden Zahlen a und b; so sind $\frac{a}{m}$ und $\frac{b}{m}$ relative Primzahlen untereinander. In dem Producte $\frac{a}{m} \cdot \frac{b}{m}$ erscheinen also nur diejenigen Factoren der beyden Zahlen a und b, die jede besonders hat. Multipliziren wir aber dieses Product mit m; so kommen in der Zahl $\frac{a}{m} \cdot \frac{b}{m} \cdot m = \frac{ab}{m}$ auch noch diejenigen hiezu, welche beyden Zahlen a und b gemein sind. Also enthält $\frac{ab}{m}$ die sämmtlichen in den Zahlen a und b vorkommenden einfachen Factoren und jeden so oft als er dort vorkommt, wo er

am Oeftesten vorkommt. So ist z. B. 6 der größte gemeinschaftliche Theiler der beyden Zahlen 72 und 42. daher $\frac{72 \cdot 42}{6} = 504$ das kleinste gemeinschaftliche Vielfache derselben; wie daraus zu ersehen, daß $\frac{504}{72} = 7$ und $\frac{504}{42} = 12$ relative Primzahlen sind.

§. 84. Lehrsatz. Wenn die durch a bezeichneten Zahlen, die ich die ursprünglich gegebenen nennen will, und zwar die Zahlen

$a_1, a_2, a_3, \ldots$ den größten gemeinschaftlichen Theiler b_1:
die $a_4, a_5, \ldots$ den größten gemeinschaftlichen Theiler b_2;
die $a_6, a_7, \ldots$ den größten gemeinschaftlichen Theiler b_3:
die $a_8, a_9, \ldots$ den größten gemeinschaftlichen Theiler b_4;

haben u. s. w. Wenn ferner die durch b bezeichneten Zahlen, die ich die ersten Theiler nennen will, und zwar die $b_1, b_2, \ldots$ den größten gemeinschaftlichen Theiler c u. s. w. haben: wenn ferner die durch c bezeichneten Zahlen, die ich die zweyten Theiler nennen will, und zwar

die $c_1, c_2, \ldots$ den größten gemeinschaftlichen Theiler d_1.
die $c_3, c_4, \ldots$ den größten gemeinschaftlichen Theiler d_2

u. s. w. haben: wenn endlich die n^{ten} Theiler $y_1, y_2, y_3, \ldots$ den größten gemeinschaftlichen Theiler z haben: so behaupte ich, z sey auch der größte gemeinschaftliche Theiler der ursprünglich gegebenen Zahlen $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, \ldots$

Beweis. Nach §. 74. bestehet b_1 aus den sämmtlichen in $a_1, a_2, a_3, \ldots$ gemeinschaftlich vorkommenden; b_2 aus den sämmtlichen in $a_4, a_5, \ldots$ gemeinschaftlich vorkommenden Factoren u. s. w. Mithin sind die in $b_1, b_2, b_3, b_4, \ldots$ gemeinschaftlich vorkommenden Factoren zugleich diejenigen, die in den sämmtlichen $a_1, a_2, a_3, \ldots, a_9 \ldots$ gemeinschaftlich vorkommen. Ebenso sind die sämmtlichen in $c_1, c_2, c_3, \ldots$ gemeinschaftlich vorkommenden Factoren einerley mit den sämmtlichen in $b_1, b_2, b_3, b_4, \ldots$ gemeinschaftlich vorkommenden Factoren; also auch einerley mit den sämmtlichen in $a_1, a_2, a_3, a_4, \ldots, a_9 \ldots$ gemeinschaftlich vorkommenden Factoren. Somit erhellet nach einer Schlußart, die wir schon sehr oft angewandt haben, daß auch die in z vorkommenden Factoren einerley seyn müssen mit den Factoren, die den gesammten ursprünglich gegebenen Zahlen $a_1, a_2, a_3, \ldots, a_9 \ldots$ gemeinschaftlich sind. Also ist z ihr größter gemeinschaftlicher Theiler.

Beyspiel. So ist

der Zahlen 12 und 30 größte gemeinschaftliche Theiler 6,
der Zahlen 42 und 63 größte gemeinschaftliche Theiler 21.
der Zahlen 75 und 90 größte gemeinschaftliche Theiler 15,
der Zahlen 120 und 150 größte gemeinschaftliche Theiler 30.

Ferner ist

der Zahlen 6 und 21 größte gemeinschaftliche Theiler 3,
der Zahlen 15 und 30 größte gemeinschaftliche Theiler 15.

Endlich

der Zahlen 3 und 15 größte gemeinschaftliche Theiler 3.

Also ist 3 der größte gemeinschaftliche Theiler der Zahlen

12, 30, 42, 63, 75, 90, 120, 150.

§. 85. Lehrsatz. Wenn die durch a bezeichneten Zahlen, die ich die ursprünglich gegebenen nenne, und zwar die

$a_1, a_2, a_3, \ldots$ das kleinste gemeinschaftliche Vielfache b_1;
die $a_4, a_5, \ldots$ das kleinste gemeinschaftliche Vielfache b_2;
die $a_6, a_7, \ldots$ das kleinste gemeinschaftliche Vielfache b_3;
die $a_8, a_9, \ldots$ das kleinste gemeinschaftliche Vielfache b_4

u. s. w. haben: wenn ferner die durch b bezeichneten Zahlen, die ich die ersten Vielfachen nennen will, und zwar

die $b_1, b_2, \ldots$ das kleinste gemeinschaftliche Vielfache c_1;
die $b_3, b_4, \ldots$ das kleinste gemeinschaftliche Vielfache c_2,

u. s. w. haben: wenn ferner die durch c bezeichneten Zahlen, die ich die zweyten Vielfachen nennen will, und zwar

die $c_1, c_2, \ldots$ das kleinste gemeinschaftliche Vielfache d_1;
die $c_3, c_4, \ldots$ das kleinste gemeinschaftliche Vielfache d_2

u. s. w. haben: wenn endlich die n^{ten} gemeinschaftlichen Vielfachen

$y_1, y_2, \ldots$ das kleinste gemeinschaftliche Vielfache z

haben: so behaupte ich, z sey das kleinste gemeinschaftliche Vielfache der sämmtlichen ursprünglich gegebenen Zahlen

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, \ldots$$

Beweis. Nach §. 80. bestehet b_1 aus den sämmtlichen von einander verschiedenen Factoren in $a_1, a_2, a_3, \ldots$, jeder sovielmahl genommen, als er in derjenigen dieser Zahlen erscheint, darin er am Oeftesten erscheinet: b_2 ebenso aus den verschiedenen in $a_4, a_5, \ldots$

vorkommenden Factoren u. s. w. Also erscheinen in den sämmtlichen Zahlen $b_1, b_2, b_3, b_4, \ldots$ die sämmtlichen in den ursprünglich gegebenen Zahlen $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, \ldots$ vorkommenden von einander verschiedenen Factoren jeder sovielmahl, als er in derjenigen, die ihn am Oeftesten enthält, erscheinet. Dasselbe gilt von den Zahlen $c_1, c_2, c_3, \ldots$, also zuletzt auch von der Zahl z. Folglich ist diese das kleinste gemeinschaftliche Vielfache der Zahlen $a_1, a_2, a_3, a_4, \ldots, a_9, \ldots$

Beyspiel. So ist der Zahlen 2 und 3 kleinstes gemeinschaftliche Vielfache $=6$, der Zahlen 4 und $3=20$, der Zahlen 6 und $7=42$. der Zahlen 8 und $9=72$. Ferner der Zahlen 6 und $20=60$, der Zahlen 72 und $42=504$. Endlich der Zahlen 60 und $504=2520$. Also 2520 das kleinste gemeinschaftliche Vielfache der sämmtlichen Zahlen 2, 3, 4, 5, 6. 7, 8 und 9.

§. 86. Lehrsatz. Wenn ein Paar Zahlen M und N sich um ein Vielfaches einer Zahl m unterscheiden. welche selbst irgend ein gemeinschaftliches Vielfache gewisser Zahlen $a, b. c, \ldots$ ist: so lassen M und N bey einer versuchten Division mit den Zahlen $a. b, c. \ldots$ beziehlich einerley Reste.

Beweis. Wenn der Unterschied $M-N$ (vorausgesetzt. daß wir die größere von beyden mit M bezeichnen) irgend ein Vielfaches der Zahl m ist: so haben wir $M-N=\mu m$. wo μ eine wirkliche Zahl. Weil nun m ein gemeinschaftliches Vielfache der Zahlen $a. b, c. \ldots$ ist; so läßt sich m und folglich auch μm oder $M-N$ durch jede dieser Zahlen theilen; daher müssen nach §. 11. auch M und N entweder theilbar seyn durch m d. h. gar keinen Rest lassen, oder beyde denselben Rest lassen.

Beyspiel. Sey $a=2, b=3, c=5, m=60$ ein Vielfaches von 2, 3, 5. Ferner $M=133$. $N=13$ also $M-N=120$ ein Vielfaches von m. Daher ist $1\frac{3}{2}^3=66\frac{1}{2}$, $1\frac{3}{2}=6\frac{1}{2}$, $1\frac{3}{3}^3=44\frac{1}{3}$, $1\frac{3}{3}=4\frac{1}{3}$; $1\frac{3}{5}^3=26\frac{3}{5}$, $1\frac{3}{5}=2\frac{3}{5}$.

§. 87. Lehrsatz. Wenn umgekehrt die Zahlen M und N bey einer versuchten Division durch die gegebenen Zahlen $a. b. c, \ldots$ beziehlich einerley Reste geben. so ist ihr Unterschied ein gemeinschaftliches Vielfache von allen diesen Zahlen $a, b, c, \ldots$

Beweis. Denn nach §. 16. ist $M-N$ theilbar durch a, weil M und N bey der versuchten Theilung mit a einerley Rest geben. Aus demselben Grunde ist $M-N$ auch theilbar durch b, theilbar durch c u. s. w. Folglich auch ein gemeinschaftliches Vielfache von allen diesen Zahlen.

Beyspiel. $M=185$, $N=17$: $a=4$. $b=6$, $c=7$. Weyl $1^{8}_{4}{}^{5}=46\frac{1}{4}$. $1^{7}_{4}=4\frac{1}{4}$; $1^{8}_{6}{}^{5}=30\frac{5}{6}$, $1^{7}_{6}=2\frac{5}{6}$; $1^{8}_{7}{}^{5}=26\frac{3}{7}$, $1^{7}_{7}=2\frac{3}{7}$; so ist der Unterschied $M-N=185-17=168=4.6.7$ also gewiß ein Vielfaches der Zahlen 4, 6, 7.

§. 88. Lehrsatz. Wenn jede der Zahlen $M, N, R, \ldots$ bey der versuchten Division mit den gegebenen Zahlen $a, b, c, \ldots$ beziehlich dieselben Reste gibt; so geben diese Zahlen auch bey einer versuchten Division durch das kleinste gemeinschaftliche Vielfache m der Zahlen $a. b, c, \ldots$ alle denselben Rest.

Beweis. Weil M und N bey der versuchten Division mit den Zahlen $a. b. c, \ldots$ beziehlich dieselben Reste geben: so ist der Unterschied $M-N$ (oder $N-M$, je nach dem $M>$ oder $<N$) irgendein Vielfaches von allen diesen Zahlen, also gewiß theilbar durch ihr kleinstes gemeinschaftliche Vielfache. Folglich muß (§. 11) M bey der versuchten Theilung mit m denselben Rest geben wie N. Weil eben dasselbe, was so eben von M und N gesagt wurde, auch von N und R gilt; so muß auch R bey der versuchten Division mit m denselben Rest geben, u. s. w.

Beyspiel. Wenn $M=17$, $N=23$, $R=41$, $a=2$, $b=3$, so ist $1^{7}_{2}=8\frac{1}{2}$, $2^{3}_{2}=11\frac{1}{2}$, $4^{1}_{2}=20\frac{1}{2}$; $1^{7}_{3}=5\frac{2}{3}$, $2^{3}_{3}=7\frac{2}{3}$, $4^{1}_{3}=13\frac{2}{3}$. Also gibt auch das kleinste gemeinschaftliche Vielfache von a und b d. i. 6 gleiche Reste. nähmlich $1^{7}_{6}=2\frac{5}{6}$, $2^{3}_{6}=3\frac{5}{6}$. $4^{1}_{6}=6\frac{5}{6}$.

§. 89. Lehrsatz. Wenn eine Zahl M bey der versuchten Division durch die Zahl m. die irgend ein gemeinschaftliches Vielfache der Zahlen $a, b. c, \ldots$ ist. den Rest R läßt; so lassen M und R bey der versuchten Division durch jede der Zahlen $a, b. c, \ldots$ beziehlich einerley Reste.

Beweis. Wenn $m>M$. so wird der bey der versuchten Division von m in M entstehende Rest $R=M$ seyn, und dann versteht sich von selbst, daß M und R auch bey den Divisionen durch $a. b, c. \ldots$ einerley Reste geben müssen. Ist aber $m<R$, so ist $M=\alpha m+R$, wo α eine wirkliche Zahl. Mithin ist $M-R=\alpha m$ theilbar durch m; folglich auch durch jede der Zahlen $a, b, c. \ldots$ welche selbst Theile von m sind. Also geben M und R bey der versuchten Division durch $a, b, c, \ldots$ beziehlich einerley Reste. (§. 11.)

Beyspiel. So ist $m=60$ ein Vielfaches der Zahlen $a=2$. $b=3$, $c=5$. Nehmen wir nun $M=157$ an; so ist $1^{5}_{60}{}^{7}=2+\frac{37}{60}$ und $1^{5}_{2}{}^{7}=78\frac{1}{2}$, $3^{7}_{2}=18\frac{1}{2}$, $1^{5}_{3}{}^{7}=52\frac{1}{3}$, $3^{7}_{3}=12\frac{1}{3}$; $1^{5}_{5}{}^{7}=31\frac{2}{5}$, $3^{7}_{5}=7\frac{2}{5}$.

§. 90. Zusatz. Da nun R kleiner als M ist; so kann man auch sagen, daß es zu jeder Zahl M. die größer als das gemein-

schaftliche Vielfache m der Zahlen $a, b, c, \ldots$ ist und bey versuchter Division durch diese Zahlen beziehlich die Reste $\alpha, \beta, \gamma, \ldots$ läßt, eine andere Zahl $R < m$ gebe, die eben diese Reste liefert.

§. 91. Lehrsatz. Wenn die Zahl M bey der versuchten Division durch die Zahl m, welche das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots$ ist, den Rest R gibt; so ist R die kleinste Zahl, welche getheilt durch die Zahlen $a, b, c, \ldots$ beziehlich dieselben Reste gibt, welche die Zahl M bey diesen Divisionen gibt.

Beweis. Denn sey S eine andere Zahl, die eben dieselben Reste wie R gibt: so muß (nach §. 87) Eines von beyden, entweder $S-R$ oder $R-S$ eine Zahl seyn, die durch die sämmtlichen Zahlen $a, b, c, \ldots$ mithin (nach §. 5) auch durch ihr kleinstes gemeinschaftliche Vielfache m theilbar ist. Allein R ist $< m$, folglich kann S nicht noch $< R$ seyn; weil sonst $R-S$ um so kleiner wäre. Also kann nicht $R-S$, sondern $S-R$ muß durch m theilbar seyn. Mithin ist $S > R$.

Beyspiel. So gibt $\begin{smallmatrix}1&2&7\\1&2\end{smallmatrix}$ den Rest 7 und 12 ist das kleinste gemeinschaftliche Vielfache der Zahlen 2, 3, 4. Also ist 7 die kleinste Zahl, welche dividirt durch 2, 3, 4 dieselben Reste gibt wie 127, nähmlich 1, 1, 3.

§. 92. Lehrsatz. Wenn es eine Zahl R gibt, die kleiner als das kleinste gemeinschaftliche Vielfache m der Zahlen $a, b, c, \ldots$ ist und die, durch diese Zahlen getheilt, beziehlich die Reste $\alpha, \beta, \gamma, \ldots$ läßt; so gibt es immer doch nur eine einzige dergleichen Zahl.

Beweis. Daß die Voraussetzung, welche der Lehrsatz macht, nicht an sich selbst Unmögliches sey, erhellet daraus, weil wir ja nach Belieben eine Zahl $R < m$ annehmen und indem wir sie der Ordnung nach durch die Zahlen $a, b, c, \ldots$ zu dividiren versuchen, die erscheinenden Reste beziehlich mit $\alpha, \beta, \gamma, \ldots$ bezeichnen können. Dann ist nur darzutun, daß eine jede andere Zahl S, die durch die Zahlen $a, b, c, \ldots$ getheilt, beziehlich dieselben Reste $\alpha, \beta, \gamma, \ldots$ liefert, $> m$ seyn müsse. Wegen dergleichen Reste muß Eines von Beyden entweder $S-R$ oder $R-S$ eine Zahl seyn, die durch m theilbar ist. Weil nun $R < m$; so kann, wie wir so eben gesehen, nicht $R-S$, sondern es muß $S-R$ diese Zahl seyn, und somit $S > R$. Ferner muß, weil $S-R =$ oder $> m$ seyn muß, S gewiß $> m$ seyn. Also ist jede von R verschiedene Zahl, welche die besagte Beschaffenheit hat, $> m$. Und es gibt somit nur eine einzige Zahl,

nähmlich die R. welche die Eigenschaft hat, jene Reste zu liefern und zugleich kleiner zu seyn als m.

Beyspiel. So ist $33 < 60$, das kleinste gemeinschaftliche Vielfache der Zahlen 12. 15 und 30. Daher gibt es auch keine einzige andere Zahl < 60, welche getheilt durch 12. 15. 30 beziehlich dieselben Reste wie 33 gibt, nähmlich 9, 3 und 3. So gibt z. B. 34 die Reste 10, 4 und 4; 30 die Reste 2. 3, 20; 59 die Reste 11. 14. 29; u. s. w.

§. 93. Lehrsatz. Wenn die Zahlen $a, b, c \ldots . l$ je zwey und zwey relative Primzahlen sind; so gibt es jederzeit eine Zahl R kleiner als das Product $a \,.\, b \,.\, c \ldots . l$, die so beschaffen ist, daß sie getheilt durch $a, b, c \ldots . l$ beziehlich die beliebig gegebenen Reste $\alpha . \beta . \gamma \ldots . \lambda$ liefert, wofern nur $\alpha < a$, $\beta < b$, $\gamma < c$. u. s. w.

Beweis. Wenn die Zahlen $a. b, c \ldots . k. l$ je zwey und zwey relative Primzahlen sind; wenn also auch nicht ein einziger Factor (die Einheit ausgenommen) zwey oder mehreren dieser Zahlen gemeinschaftlich ist; so bilden auch

$$\begin{aligned} &abc \ldots k \text{ und } l, \\ &abc \ldots il \text{ und } k, \\ &abd \ldots k \text{ und } c, \\ &acd \ldots l \text{ und } b. \\ &bcd \ldots l \text{ und } a \end{aligned}$$

eben so viele Paare relativer Primzahlen. Mithin gibt es (nach §. 33.) auch für ein jedes dieser Paare z. B. $abc \ldots k$ und l ein Paar andere Zahlen m_1 und r_1, die so beschaffen sind, daß der Unterschied der Producte $m_1 \,.\, abc \ldots - n_1 l = 1$ wird. Wir erhalten also

$$\begin{aligned} m_1 \,.\, abc \ldots k - n_1 l &= 1, \\ m_2 \,.\, abc \ldots il - n_2 k &= 1, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ m_{\mu-2} \,.\, abd \ldots l - n_{\mu-2} c &= 1, \\ m_{\mu-1} \,.\, acd \ldots l - n_{\mu-1} b &= 1, \\ m_\mu \,.\, bc \ldots l - n_\mu a &= 1. \end{aligned}$$

Betrachten wir nun folgenden Ausdruck, dessen Bildungsgesetz von selbst einleuchtet:

$$\begin{aligned} m_1 \,.\, abc \ldots k\lambda + m_2 \,.\, abc \ldots il \varkappa + \ldots + m_{\mu-2} \,.\, abd \ldots b\gamma + \\ + m_{\mu-1} \,.\, acd \ldots l\beta + m_\mu \,.\, bc \ldots l\alpha \end{aligned}$$

so werden wir bald gewahr, daß der Factor a in allen Gliedern desselben vorkomme, bis auf das letzte $m_\mu \,.\, bc \ldots l\alpha$. Hieraus er-

gibt sich, daß eine versuchte Division dieses Ausdruckes durch a überall aufgehe, bis bey dem letzten Gliede. Aus der letzten der früheren Gleichungen aber zeigt sich, daß $m_\mu . bc \ldots l = n_\mu a + 1$, also $m_\mu . bc \ldots l\alpha = n_\mu . a\alpha + \alpha$ sey. Die Division mit a in den Theil $n_\mu . a\alpha$ geht abermahls auf; und somit gibt unser obige Ausdruck durch die Division mit a keinen anderen Rest als α, wenn $\alpha < a$. Auf ähnliche Weise erhellet, daß unser Ausdruck bey der versuchten Division durch b den Rest β gebe. Denn der Factor b erscheint in allen Gliedern desselben bis auf das einzige $m_{\mu-1} . acd \ldots l\beta$, welches wie aus der vorletzten der obigen Gleichungen ersichtlich, $= n_\mu . a\beta + \beta$ und somit offenbar den Rest β gibt. So läßt sich dann überhaupt darthun, daß der besagte Ausdruck getheilt durch alle Zahlen $a, b, c, \ldots, l$ die beziehlichen Reste $\alpha, \beta, \gamma, \ldots, \lambda$ liefere. Nach §. 82. ist aber das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots, l = abc \ldots l$. Ist nun der Werth des obigen Ausdruckes schon für sich selbst $< abc \ldots l$; so ist er bereits so beschaffen, wie die Zahl R seyn soll, deren Vorhandenseyn der Lehrsatz aussagt. Wenn nicht, so läßt sich doch (nach §. 90) immer ein R finden, das kleiner als das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots, l$, also $< abc \ldots l$ ist und dieselben Reste liefert.

Beyspiel. So sind die Zahlen $a = 3$, $b = 4$, $c = 5$, $d = 7$ je zwey und zwey relative Primzahlen untereinander. Setzen wir nun $\alpha = 1 < 3$, $\beta = 2 < 4$, $\gamma = 4 < 5$, $\delta = 5 < 7$; so gibt es allerdings eine Zahl, nahmentlich $334 < 3 . 4 . 5 . 7$, welche durch Division mit 3, 4, 5, 7 beziehlich die Reste 1, 2, 4, 5 liefert. Hätten wir $\alpha = 1$, $\beta = 1$, $\gamma = 1$, $\delta = 1$ angenommen; so fände sich $R = 1$; nähmlich 1 dividirt durch 3, 4, 5, 7 gibt offenbar überall den Rest 1.

§. 94. Zusatz. Wenn nicht je zwey und zwey der Zahlen $a, b, c, \ldots, l$ relative Primzahlen sind; so ist ihr kleinstes gemeinschaftliche Vielfache $m < abc \ldots l$; und dann gibt es nicht immer eine Zahl R, wie sie der Lehrsatz beschreibt. Denn weil R mit a den Rest α, mit b den Rest β geben soll, so muß R jederzeit sowohl unter der Form $pa + \alpha$ als auch unter der Form $qb + \beta$ enthalten seyn. Hieraus ergibt sich aber, wenn wir z. B. $\alpha > \beta$ annehmen, $\alpha - \beta = qb - pa$. Wenn nun die Zahlen a, b einen gemeinschaftlichen Theiler hätten; so müßte, weil $qb - pa$ theilbar durch diesen Theiler wäre, auch der Unterschied $\alpha - \beta$ theilbar durch ihn seyn. Und somit könnten die Zahlen $\alpha, \beta, \gamma, \ldots, \lambda$

jetzt nicht mehr ganz willkürlich angenommen werden. So gibt es z. B. keine Zahl, welche getheilt durch 4 und 6 beziehlich die Reste 3 und 4 gebe. Denn um bey der Division durch 4 den Rest 3 zu geben, müßte sie von der Form $4x+3$ also ungerade, und bey der Division durch 6 den Rest 4 zu geben. von der Form $6y+4$ also gerade seyn.

§. 95. Zusatz. Wenn von den Zahlen $a, b, c, \ldots, l$ je zwey und zwey relative Primzahlen sind; so gibt es nicht zwey Zahlen, die kleiner als das Product $a.b.c\ldots l$ sind und bey der Theilung mit $a, b, c, \ldots, l$ völlig dieselben Reste die eine wie die andere liefern. Denn eine Zahl, die $< abc\ldots l$ ist, ist kleiner als das kleinste gemeinschaftliche Vielfache der Zahlen $a. b. c, \ldots, l$ und somit gibt es nur eine einzige, welche bey jener Division dieselbe Reihe von Resten erzeugt (§. 92.). So überzeugt man sich z. B. bald, daß 23 die einzige Zahl sey, die $< 2.3.5 = 30$, durch Division mit 2, 3, 5 beziehlich die Reste 1, 2, 3; 29 die einzige, die beziehlich die Reste 1. 2, 4 liefert u. s. w.

§. 96. Zusatz. Da es also einerseits für jede beliebig angenommene Reihe von Resten $\alpha, \beta, \gamma, \ldots, \lambda$ (sind sie nur so gewählt, daß $\alpha < a$, $\beta < b$, $\gamma < c$, $\ldots$, $\lambda < l$ ist) eine Zahl gibt, die kleiner als das kleinste gemeinschaftliche Vielfache der Zahlen $a, b, c, \ldots, l$ ist und diese Reste liefert; und da es andererseits nur eine einzige dergleichen Zahl gibt: so muß die Menge aller Zahlen, die kleiner als das Product $abc\ldots l$, und doch durch keine dieser Zahlen theilbar sind, gerade so groß seyn, als die Menge der verschiedenen Reihen von Resten, die sich bey den mit $a, b, c, \ldots, l$ versuchten Divisionen gedenken lassen. Begreiflich aber ist die Menge der verschiedenen Reste, die bey der Division mit a Statt finden können, $= a-1$; weil die Anzahl aller wirklichen Zahlen, die $<$ als a sind, $= a-1$ ist. Ebenso ist die Menge der Reste, die der Divisor b lassen kann, $= b-1$ u. s. w. Also die Menge der verschiedenen Reste, die bey den Divisionen mit $a, b, c, \ldots, l$ Platz greifen können, offenbar gleich dem Producte $(a-1)(b-1)(c-1)\ldots(l-1)$. So groß ist demnach auch die Menge der Zahlen, die $< abc\ldots l$ und durch keine der Zahlen $a, b, c, \ldots, l$ theilbar sind. So sind z. B. die sämmtlichen Zahlen, die $< 2.3.5 = 30$ und sich durch keine der Zahlen 2, 3, 5 theilen lassen: 1, 7, 11, 13, 17, 19, 23, 29 und ihre Anzahl ist $= (2-1)(3-1)(5-1) = 8$.

§. 97. Zusatz. Unter diesen Zahlen befindet sich jederzeit auch die Einheit; weil auch 1 eine Zahl ist, welche durch keine

der gegebenen $a, b, c, \ldots$ (die alle größer als 1 sind) getheilt werden kann.

§. 98. Lehrsatz. Wenn die Zahlen $a, b, c \ldots, l$ absolute Primzahlen sind; so ist die Menge aller derjenigen Zahlen, die kleiner als das Product $abc \ldots l = m$, und zugleich auch relative Primzahlen zu denselben sind, immer gleich dem Producte $(a-1)(b-1)(c-1)\ldots(l-1)$.

Beweis. Zahlen, die absolute Primzahlen sind, sind auch relative Primzahlen unter einander. Also ist nach dem so eben Erwiesenen die Menge aller Zahlen, die $< a.b.c \ldots l$, und durch keine der Zahlen $a.b, c \ldots, l$ theilbar sind, $=(a-1)(b-1)(c-1)\ldots$ $\ldots(l-1)$. Jede dieser Zahlen muß mit der Zahl m in dem Verhältnisse einer relativen Primzahl stehen. Denn weil die Zahlen $a, b, c, \ldots, l$ absolute Primzahlen sind: so stehet jede Zahl, welche durch keine derselben theilbar ist, in dem Verhältnisse einer relativen Primzahl zu jeder einzelnen von ihnen und somit auch zu dem Producte aus allen oder zu m. Jede andere Zahl dagegen d. h. jede Zahl, welche durch eine oder die andere der Zahlen $a, b, c, \ldots, l$ theilbar ist, ist eben deshalb keine relative Primzahl zu dem Producte m. Also ist die Menge der sämmtlichen Zahlen, welche relative Primzahlen zu der Zahl m, und zugleich $< m$ sind, nicht größer und nicht kleiner als $(a-1)(b-1)(c-1)\ldots(l-1)$.

Beyspiel. So ist die Menge der sämmtlichen Zahlen, die < 30 und relative Primzahlen mit $30 = 2.3.5$ sind $= (2-1).(3-1)(5-1) = 8$. Diese Zahlen sind nähmlich 1. 7, 11, 13, 17, 19, 23, 29. Eben so ist die Menge der sämmtlichen relativen Primzahlen zu dem Producte $5.7 = 35$, die < 35 sind, nun $(5-1).(7-1) = 24$ nähmlich: 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34.

§. 99. Lehrsatz. Wenn die Zahlen $a, b, c, \ldots, l$ absolute Primzahlen sind; so ist die Menge aller derjenigen Zahlen, die kleiner sind als das Product $n.m = n.a.b.c \ldots l$, und zugleich auch relative Primzahlen gegen m sind, gleich dem Producte $n(a-1)(b-1)(c-1)\ldots(l-1)$: wobey n jede beliebige wirkliche Zahl vorstellen kann.

Beweis. Bezeichnet R eine Zahl, welche durch keine der Primzahlen $a, b, c, \ldots, l$ theilbar und zugleich $<$ als ihr Product $m = abc \ldots l$ ist: so bezeichnet auch $p.m + R$ eine Zahl, welche durch keine der Zahlen $a, b, c, \ldots, l$ theilbar ist, sondern bey der versuchten Division durch sie beziehlich dieselben Reste wie R läßt, wenn wir voraussetzen, daß p irgend eine Zahl

bedeute. Auch umgekehrt muß eine jede Zahl, welche durch $a, b, c, \ldots, l$ dividirt, beziehlich dieselben Reste wie R geben soll, unter der Form $p \cdot m + R$ enthalten seyn. Soll diese Zahl überdieß $< nm$ seyn, so darf p nicht $> n-1$ genommen werden. Jede dieser Zahlen erscheint somit in folgender Reihe: $R, m+R, 2m+R, 3m+R, \ldots, (n-1)m+R$. Nun ist die Anzahl der Glieder in dieser Reihe offenbar $= n$; und die Anzahl der Werthe, welche R annehmen kann, nach §. 98. $= (a-1)(b-1)(c-1)\ldots(l-1)$. Auch ist aus §. 98. offenbar, daß alle die Zahlen, die durch die Glieder dieser Reihe vorgestellt werden können, wenn man die eben erwähnten $(a-1)(b-1)(c-1)\ldots(l-1)$ Werthe für R setzt, von einander verschieden seyn müssen, weil $nm+R$ niemahls $n'm+R'$ seyn kann, weil n und n' und eben so R und R' zwey von einander verschiedene wirkliche Zahlen, die letztere überdieß $< m$ seyn sollen. Also ist die Menge aller Zahlen, welche durch keine der Primzahlen $a, b, c, \ldots, l$ theilbar, und dabey $<$ das Product $n \cdot a \cdot b \cdot c \ldots l$ sind, $= n(a-1)(b-1)(c-1)\ldots(l-1)$. Da nun alle diese Zahlen mit den Zahlen $a, b, c, \ldots, l$ zugleich in dem Verhältnisse von relativen Primzahlen stehen: so ist die Menge aller relativen Primzahlen zu $a, b, c, \ldots, l$, die zugleich $< n \cdot a \cdot b \cdot c \ldots l$ sind, immer $= n(a-1)(b-1)(c-1)\ldots(l-1)$.

Beyspiel. So ist die Menge der sämmtlichen Zahlen, die relative Primzahlen mit $3 \cdot 3$, und zugleich $< 4 \cdot 3 \cdot 3 = 60$ sind, $= 4(3-1)(3-1) = 32$. Diese Zahlen sind nähmlich 1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44, 46, 47, 49, 52, 53, 56, 58, 59.

§. 100. Lehrsatz. Wenn $a, b, c, \ldots, l$ absolute Primzahlen, $\alpha, \beta, \gamma, \ldots, \lambda$ aber beliebige Zahlen bedeuten: so ist die Menge der Zahlen, die gegen das Product $a^\alpha \cdot b^\beta \cdot c^\gamma \ldots l^\lambda$ relative Primzahlen und dabey kleiner sind als dasselbe

$$= \frac{a^\alpha \cdot b^\beta \cdot c^\gamma \ldots l^\lambda}{a \cdot b \cdot c \ldots l} (a-1)(b-1)(c-1)\ldots(l-1).$$

Beweis. Aus dem vorhergehenden Satze wissen wir, daß die Menge aller Zahlen, welche relative Primzahlen gegen das Product $abc \ldots l$ und dabey kleiner sind als das Product $n \cdot abc \ldots l$, immer $= n(a-1)(b-1)(c-1)\ldots(l-1)$ sey. Setzen wir nun die Zahl n, die hier ganz willkürlich ist $= \frac{a^\alpha b^\beta c^\gamma d^\delta \ldots l^\lambda}{abcd \ldots l}$, welches jederzeit, auch wenn einige der Zeichen $\alpha, \beta, \gamma, \delta, \ldots \lambda$ bloß Einheiten anzeigen, eine wirkliche Zahl ist, so kommt der obige Ausdruck

$\frac{a^\alpha b^\beta c^\gamma d^\delta \ldots l^\lambda}{abcd \ldots l}(a-1)(b-1)(c-1)\ldots(l-1)$ zum Vorschein. Da aber alle Zahlen, welche relative Primzahlen mit dem Producte $abcd\ldots l$ sind, auch relative Primzahlen mit dem Producte $a^\alpha b^\beta c^\gamma d^\delta \ldots l^\lambda$ sind: so erhellet die Wahrheit des Satzes.

§. 101. Zusatz. Da nun nach §. 43. jede beliebige wirkliche Zahl unter der Form $a^\alpha b^\beta c^\gamma d^\delta \ldots l^\lambda$ enthalten ist; so lehrt der obige Satz, wie viele Zahlen es gebe, die kleiner als eine gegebene Zahl und relative Primzahlen gegen sie sind. So ist z. B. die Zahl $100 = 2^2 . 5^2$, also ist die Menge der sämmtlichen Zahlen, die < 100 und relative Primzahlen zu 100 sind, $= 2 . 5 (2-1) . (5-1) = 40$. Und so ist es wirklich; denn diese Zahlen sind: 1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 91, 93, 97, 99.

§. 102. Zusatz. Bey einer absoluten Primzahl p beträgt die Anzahl der zu ihr relativen Primzahlen, die zugleich kleiner sind als sie, immer nur $p-1$. So gibt es nicht nur die obige Formel für diesen Fall; sondern so fließt es auch unmittelbar aus dem Begriffe einer solchen Zahl, vermöge dessen sie durch keine der Zahlen $2, 3, 4, \ldots, (p-1)$ theilbar seyn darf. Wird nun zu diesen Zahlen auch die Einheit, die eine relative Primzahl zu jeder Zahl ist (§. 33.), hinzugefügt: so ist die Menge der Zahlen $1, 2, 3, \ldots, (p-1)$ offenbar $= p-1$.

§. 103. Lehrsatz. Die Menge der sämmtlichen Theiler einer Zahl N, wenn wir die Einheit und die Zahl selbst mitrechnen, gleicht dem Ausdrucke $(1+\alpha)(1+\beta)(1+\gamma)\ldots(1+\lambda)$, in welchem die Anzahl der Glieder von der Form $(1+\alpha), (1+\beta), (1+\gamma)\ldots\ldots, (1+\lambda)$ so groß als die Anzahl der einfachen von Eins verschiedenen Factoren, in welche sich N zerschlagen läßt, und die Buchstaben $\alpha, \beta, \gamma \ldots, \lambda$ bezeichnen, wie oft ein jeder dieser Factoren in N vorkommt.

Beweis. Wenn die Zahl N eine Primzahl ist, so gibt es nur zwey einzige Theiler, die Einheit nähmlich und die Zahl N selbst. Für diesen Fall aber bekommt der Ausdruck $(1+\alpha)(1+\beta)\ldots\ldots(1+\lambda)$ die Gestalt $(1+1)=2$ d. h. er gibt die Zahl der Theiler richtig. Ebenso richtig gibt diese Formel die Zahl der Theiler, wenn N nur aus einem einzigen Factor a bestehet, der aber mehrmahls, nähmlich α mahl wiederholt ist. Offenbar ist dann N theilbar durch folgende Reihe von Zahlen $1, a, a^2, a^3, \ldots, a^\alpha$, die wir erhalten, wenn wir die Einheit zum ersten Gliede machen, dann aber das zweyte und jedes folgende bilden, indem wir das

nächstvorhergehende noch mit a multipliziren, und endlich abbrechen, bis wir zu einem Gliede kommen, daß dem Producte a^{α} gleicht, in welchem die Anzahl der Factoren $=\alpha$ ist. Die Menge der Glieder, aus welchen diese Reihe bestehet, ist aber sichtbar $=1+\alpha$. Also die Anzahl der Theiler $=(1+\alpha)$; und gerade so gibt auch die Formel für diesen Fall sie an. Die Formel ist also richtig, wenn sie aus einem einzigen Gliede bestehet. Ich werde nun darthun, daß, wenn diese Formel gilt, so fern sie aus einer gewissen Anzahl von Gliedern $=n$ bestehet, sie auch gelte, wenn sie aus $(n+1)$ Gliedern bestehet. Ist es nähmlich wahr, daß die Anzahl aller Theiler, die eine Zahl zuläßt, wenn in derselben n von einander verschiedene Factoren, der erste α mahl, der zweyte β mahl, ..., der n^{te} λ mahl erscheinen, $=(1+\alpha)(1+\beta)\ldots(1+\lambda)$ sey: so behaupte ich, die Anzahl aller Theiler, die eine Zahl zuläßt, welche nebst den vorigen noch einen neuen einfachen Factor m hat, der in derselben μ mahl erscheint, ist $=(1+\alpha)(1+\beta)\ldots(1+\lambda)(1+\mu)$. Wenn nähmlich der $(n+1)^{\text{te}}$ Factor nur ein einzigesmahl vorkommt; so ist offenbar, daß die Anzahl der Theiler, welche die ganze Zahl zuläßt, durch ihn verdoppelt werde. Denn zu den Theilern, die ohnehin Statt finden, kommen noch ebenso viele hinzu, die man erhält, wenn man jeden der vorigen noch mit m multiplizirt. Gerade so gibt es aber auch unsere Formel, indem für $\mu=1$ die Zahl $(1+\alpha)\,.\,(1+\beta)\ldots(1+\lambda)(1+\mu)$ das Doppelte wird von der Zahl $(1+\alpha)\,.\,(1+\beta)\ldots(1+\lambda)$. Erscheint der neue Factor m mehrmahl, wird er z. B. μ mahl wiederholt; so erhalten wir die sämmtlichen Theiler der neuen Zahl, wenn wir jeden Theiler der vorigen noch durch ein jedes Glied der folgenden Reihe multipliziren $1, m, m^2, m^3, m^4, \ldots, m^{\mu}$, deren Bildungsgesetz dasselbe wie das der früher betrachteten ist, so jedoch, daß ihr letztes Glied ein Product aus μ der Zahl m gleichen Factoren vorstellt. Die Anzahl der Glieder in dieser Reihe ist $1+\mu$. Und somit ist entschieden, daß die Menge der Theiler, welche die vorige Zahl durch den Zuwachs des neuen μ-fach vorkommenden Factors m erhält, $(1+\mu)$ fach so groß ist, als sie es vorhin war; sie ist sonach $=(1+\alpha)(1+\beta)\ldots(1+\lambda)(1+\mu)$. Also gilt die Formel, die unser Lehrsatz aufstellt, für 2, 3, ... und jede beliebige Anzahl von einander verschiedenen Factoren.

Beyspiel. Da die Zahl $60=2^2.3.5$, so ist die Anzahl ihrer sämmtlichen Theiler $=(1+2)(1+1)(1+1)=12$; diese Theiler sind nähmlich: 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

§. 104. Lehrsatz. Die Summe aller Theiler einer Zahl N, wenn wir die Einheit und sie selbst mitnehmen, ist immer gleich dem Ausdrucke $(1+a+a^2+\ldots+a^\alpha)(1+b+b^2+\ldots+b^\beta)(1+c+c^2+\ldots+c^\gamma)\ldots$ $\ldots(1+l+l^2+\ldots l^\lambda)$, wenn wir durch $a, b, c, \ldots, l$ die sämmtlichen einfachen Factoren dieser Zahl, und durch die Zeichen $\alpha, \beta, \gamma, \ldots \lambda$ andeuten, wie oft ein jeder dieser Factoren in ihr vorkommt.

Beweis. Bey der hier angenommenen Bezeichnung ist die Zahl N unter der Form $a^\alpha . b^\beta . c^\gamma \ldots l^\lambda$ enthalten: und für den Fall, daß sie selbst eine Primzahl ist, hat man bloß $N = a$. In diesem Falle aber hat sie nur zwey Theiler, 1 nähmlich und a, deren Summe sonach, gerade wie es die Formel des Lehrsatzes anzeigt, $= 1+a$ ist. Ist die Zahl N ein Product mehrerer einander gleichen Primfactoren $= a^\alpha$, so ist die Summe ihrer sämmtlichen Theiler offenbar $= 1+a+a^2+\ldots+a^\alpha$, abermahls, wie es die Formel des Lehrsatzes darstellt. Kommt zu dem Factor a^α noch ein zweyter b^β hinzu: so ist die Summe ihrer sämmtlichen Theiler $= (1+a+a^2+\ldots+a^\alpha)(1+b+b^2+\ldots+b^\beta)$. Denn zu den Theilern, die in der Summe $1+a+a^2+\ldots+a^\alpha$ stecken, kommen noch hinzu die Theiler, welche zum Vorschein kommen, wenn wir jeden der ersteren zuförderst mit b, dann mit b^2, dann mit b^3 und endlich mit b^β multipliziren. Allein das obige Product liefert bey seiner Entwicklung die Summe aller dieser Zahlen. Denn wenn wir den Factor $(1+a+a^2+\ldots+a^\alpha)$ mit dem Factor $(1+b+b^2+\ldots+b^\beta)$ multipliziren: so multipliziren wir ihn zuförderst mit 1, wobey er ungeändert bleibt; dann mit $b, b^2, \ldots b^\beta$ und addiren alle diese Producte; welches genau die vorhin beschriebene Summe darstellt. Also gilt unser Satz, wenn die Anzahl der von einander verschiedenen Factoren in $N = 2$ ist: und nun wird völlig auf ähnliche Art wie in dem vorigen §. erwiesen, daß der Satz allgemein gelte. Sonach ist z. B. die Summe aller Theiler von $100 = (1+2+2^2)(1+5+5^2) = 217$.

§. 105. Zusatz. Die Summe $1+a+a^2+\ldots+a^\alpha$ läßt sich (nach §.) weil $a > 1$ auch $= \frac{a^{\alpha+1}-1}{a-1}$, und ebenso $1+b+b^2+\ldots+b^\beta = \frac{b^{\beta+1}-1}{b-1}$ u. s. w. schreiben. Die Summe aller Theiler der Zahl $a^\alpha . b^\beta . c^\gamma \ldots l^\lambda$ kann also auch durch $\frac{a^{\alpha+1}-1}{a-1} \cdot \frac{b^{\beta+1}-1}{b-1} \cdot \frac{c^{\gamma+1}-1}{c-1} \cdots$ $\cdots \frac{l^{\lambda+1}-1}{l-1}$ ausgedrückt werden. Für die Zahl 100 gibt dieß $\frac{2^3-1}{2-1} \cdot \frac{5^3-1}{5-1} = 217$ wie vorhin.

§. 106. Lehrsatz. Wenn eine Zahl N einen Theiler p hat, der so beschaffen ist, daß das Quadrat $p^2 > N$; so hat sie auch einen von der Einheit verschiedenen Theiler q, der so beschaffen ist, daß $q^2 < N$.

Beweis. Ein solcher ist nähmlich gleich dem Quotienten, den N getheilt durch p gibt. Denn setzen wir $\frac{N}{p} = q$, oder $N = pq$; so ist auch $N^2 = p^2q^2$, und weil $p^2 > N$, durch Division (§.) $\frac{p^2q^2}{p^2} > N^2$ d. i. $q^2 < N$.

§. 107. Zusatz. Wenn also umgekehrt eine Zahl N keinen von der Einheit verschiedenen Theiler q hat, der so beschaffen wäre, daß $q^2 < N$; so hat sie auch keinen Theiler p, der so beschaffen wäre, daß $p^2 > N$ ist. Und wenn sie überdieß auch keinen Theiler q hat, der so beschaffen wäre, daß $q^2 = N$ ist, so hat sie überhaupt gar keinen Theiler, die Einheit und sich selbst abgerechnet; und ist somit eine Primzahl. Denn jeder Theiler, welchen sie hätte, müßte doch notwendig entweder so beschaffen seyn, daß sein Quadrat m^2 gleich oder kleiner oder größer als N ist.

§. 108. Aufgabe. Zu untersuchen, ob eine gegebene Zahl eine Primzahl sey, und wenn sie es nicht ist, die einfachen Factoren (Primzahlen), aus denen sie zusammengesetzt ist, anzugeben.

Auflösung. Man versuche die gegebene Zahl N der Ordnung nach zu dividiren mit den Zahlen der natürlichen Zahlenreihe 2, 3, 4, ... bis man zu einer Zahl p kommt, bey der die Division aufgeht. Findet sich eine solche, so ist diese einer von den verlangten einfachen Factoren der N. Denn sie ist ein Theiler der N, und selbst nicht theilbar, sondern eine Primzahl; weil im entgegengesetzten Falle, wenn p zusammengesetzt $= m \cdot n$ wäre; schon die beyden kleineren Zahlen m und n, mit denen man die Division früher als mit p versuchte, in N hätten aufgehen müssen. Mit diesem einen einfachen Factor der N dividire man N, und verfahre mit dem Quotienten N' ganz wie vorhin mit N; wobey es jedoch nicht nöthig ist, die Division mit Zahlen, die $< p$, wohl aber mit p selbst zu versuchen. Das Erste aus dem schon angezeigten Grunde; das Zweyte, weil N den Factor p mehrmahl enthalten kann. Offenbar wird man auf diese Weise allmählig alle einfachen Factoren der Zahl N', und wenn einer oder andere derselben mehrfach erscheint, diesen auch mehrfach

erhalten. Kommt man bey der versuchten Division der N oder einer aus ihr abgeleiteten Zahl N_n. mit der wie mit N selbst umzugehen ist, in der natürlichen Reihe der Zahlen $2, 3, 4 \ldots$ bis zu einem Divisor p, der so groß ist, daß $p^2 > N$ oder N_n, so braucht man nach §. 106. nicht ferner mehr zu untersuchen, ob sich nicht unter den größeren Zahlen ein Theiler finden werde; sondern es ist schon entschieden, daß diese Zahl eine Primzahl sey.

Beyspiel. Wenn wir nach dieser Art die einfachen Factoren der Zahl 46725 suchen; so zeigt sich zunächst ihre Theilbarkeit durch die Zahl 3; und es erscheint als Quotient 15575. Da nun diese Zahl nicht weiter theilbar ist durch 3, so versuchen wir die Division durch 4; dann, weil diese nicht aufgeht, durch 5; wobey wir den Quotienten 3115 erhalten. Indem wir bey diesem abermahls die Division mit 5 versuchen, erhalten wir zum Quotienten 623. Da diese Zahl nicht mehr theilbar durch 5 ist, so versuchen wir die Division durch 6, welche nicht aufgeht; dann die durch 7, die aufgeht, und den Quotienten 89 gibt. Bey diesem versuchen wir die Division mit 7, 8, 9 und 10 ohne Erfolg. Da nun die letztere Zahl 10 schon so groß ist, daß ihr Quadrat 100 bereits > 89 ist; so entnehmen wir hieraus, daß 89 eine Primzahl sey. Also ist 46725 aus den einfachen Factoren $3 . 5^2 . 7 . 89$ zusammengesetzt.

§. 109. Aufgabe. Die sämmtlichen Zahlen zu finden, deren kleinstes gemeinschaftliche Vielfache eine gegebene Zahl N ist.

Auflösung. Da vorausgesetzt wird, daß die gegebene Zahl keine Primzahl ist, so zerlege man sie in ihre sämmtlichen einfachen Factoren. Wenn nun der eine derselben a, α mahl, der andere b, β mahl vorkommt u. s. w. so weiß man bereits aus §. 103., daß die Menge der sämmtlichen Zahlen, deren kleinstes Vielfache die gegebene ist, (oder was eben soviel heißt, die Menge der sämmtlichen Theiler dieser Zahl), wenn wir die Einheit und sie selbst mit dazu rechnen, $= (1 + \alpha)(1 + \beta) \ldots (1 + \lambda)$ sey; und es wird ein Leichtes seyn, sie alle darzustellen, wenn man nach der Art, die im Beweise dieses Lehrsatzes angedeutet ist, verfährt.

Beyspiel. Wenn wir die sämmtlichen Zahlen, deren kleinstes gemeinschaftliche Vielfache die Zahl 100 ist, finden sollten; so zerlegen wir 100 erst in seine einfachen Factoren, welche $2^2 . 5^2$ sind. Dann zeigt sich, daß die verlangten Zahlen folgende seyn müssen:

$$\left.\begin{array}{llll} 1, & 2, & 2^2 \\ 3, & 2\,.\,3, & 2^2\,.\,3 \\ 3^2, & 2\,.\,3^2, & 2^2\,.\,3^2 \end{array}\right\} \text{ oder } \begin{array}{llll} 1, & 2, & 4 \\ 3, & 10, & 20 \\ 25, & 50, & 100 \end{array}$$

§. 110. Aufgabe. Den größten gemeinschaftlichen Theiler einer endlichen Menge gegebener Zahlen zu finden.

Auflösung. 1. Haben wir diese Zahlen alle zuerst in ihre einfachen Factoren zerlegt: so ist es ein Leichtes zu sehen, ob unter diesen Factoren einer oder einige allgemein sind. Dieser Eine, oder wenn ihrer mehrere sind, das Product aus ihnen allen wird den verlangten größten gemeinschaftlichen Theiler geben.

2. Aber auch ohne das zuweilen mühsame Geschäft der Zerlegung in ihre einfachen Factoren bey den gegebenen Zahlen verrichtet zu haben, können wir auf folgende Weise verfahren. Wir nehmen erst zwey dieser Zahlen, etwa die beyden kleinsten, und suchen den größten gemeinschaftlichen Theiler, den diese beyden haben, auf die Art, die im Beweise des Lehrsatzes §. 49. angedeutet ist. Wir versuchen nähmlich die größere von diesen beyden Zahlen durch die kleinere zu dividiren, und wenn die Division aufgeht: so ist diese kleinere Zahl selbst der größte gemeinschaftliche Theiler beyder Zahlen. Wenn sie aber nicht aufgeht, so dividiren wir mit dem gewonnenen Reste in den vorigen Divisor, und verfahren fortwährend so, bis wir zuletzt zu einer Division gelangen, die aufgeht. Bekanntlich ist dann der letztgebrauchte Divisor, wenn er nicht die Einheit selbst ist, der größte gemeinschaftliche Theiler beyder Zahlen. Geht die Division nicht eher als bis der Rest 1 ist, auf: so sind beyde Zahlen relative Primzahlen, und es gibt folglich für den ganzen gegebenen Inbegriff von Zahlen keinen größten gemeinschaftlichen Theiler. Haben aber die beyden zuerst betrachteten Zahlen a, b einen größten gemeinschaftlichen Theiler m: so suche man nur auf dieselbe Weise wieder den größten gemeinschaftlichen Theiler zwischen m und einer der übrigen Zahlen, z. B. c: finden wir einen, und ist dieser n: so ist er nach §. 85. zugleich auch der größte gemeinschaftliche Theiler zwischen den Zahlen a, b und c. Und so erhellet, daß wir auf diese Weise fortfahrend endlich die Zahl finden können, welche der größte gemeinschaftliche Theiler aller gegebenen Zahlen ist, wenn ihre Menge selbst nur eine endliche ist.

Beyspiel. Wenn die gegebenen Zahlen 36, 48, 102, 310, 627 wären: so gäbe die versuchte Division von 36 in 48 den Rest 12, der in dem vorigen Divisor 36 aufgeht, woraus erhellet, daß der größte

gemeinschaftliche Theiler der beyden ersten Zahlen 36 und 48, die Zahl 12 sey. Suchen wir nun auf eben die Art den größten gemeinschaftlichen Theiler zu den beyden Zahlen 12 und 102: so gibt die versuchte Division von 12 in 102 den Rest 6, der in 12 aufgeht. Mithin ist der größte gemeinschaftliche Theiler zwischen 12 und 102 die Zahl 6. Suchen wir nun den größten gemeinschaftlichen Theiler zwischen 6 und 510: so zeigt sich, daß dieser die Zahl 6 selbst sey, weil 6 in 510 aufgeht. Suchen wir endlich den größten gemeinschaftlichen Theiler zwischen 6 und 627: so gibt die Division von 6 in 627 den Rest 3, der in 6 aufgeht, und lehrt, daß die gegebenen Zahlen keinen größeren gemeinschaftlichen Theiler als die Zahl 3 haben.

§. 111. Aufgabe. Zu einer endlichen Menge gegebener Zahlen das kleinste gemeinschaftliche Vielfache zu finden.

Auflösung. 1. Wenn wir die einfachen Factoren, aus welchen jede dieser Zahlen zusammengesetzt ist, kennen; so ist nichts leichter, als eine Zahl zu bilden, welche die sämmtlichen in diesen Zahlen vorkommenden einfachen Factoren, diejenigen, die in der einen oder der anderen wiederholt vorkommen, so vielfach, als sie dort erscheinen, wo sie am Oeftesten erscheinen, zu ihren eigenen Factoren hat. Diese Zahl wird nach §. 80. das verlangte Vielfache seyn.

2. Ohne die einfachen Factoren der gegebenen Zahlen zu kennen, läßt sich dieß Vielfache auch finden, wenn wir den größten gemeinschaftlichen Theiler dieser Zahlen kennen. Ist nähmlich dieser m, so läßt sich jede der gegebenen Zahlen $a, b, c \ldots, l$ durch m theilen. Verrichten wir diese Divisionen und geben sie uns die Quotienten $\frac{a}{m} = \alpha$, $\frac{b}{m} = \beta$, $\frac{c}{m} = \gamma$, $\ldots$ $\frac{l}{m} = \lambda$, so wird das Product aus ihnen allen multiplizirt noch mit m, oder die Zahl $\alpha . \beta . \gamma \ldots \lambda . m$, das verlangte Vielfache seyn. Denn in dem Factor m stecken diejenigen Factoren der Zahlen $a, b, c \ldots . l$, welche sie alle gemeinschaftlich haben, in den Factoren $\alpha, \beta, \gamma, \ldots, \lambda$ aber diejenigen, die jede der Zahlen $a, b, c, \ldots, l$ noch eigenthümlich hat. Also ist kein Zweifel, daß das Product $\alpha . \beta . \gamma \ldots \lambda . m$ alle Factoren enthalte, die in den Zahlen $a, b, c \ldots . l$ vorkommen, und diejenigen, die darin mehrfach vorkommen, so oft als in derjenigen Zahl, die sie am Oeftesten enthält.

Beyspiel. Sind die gegebenen Zahlen 12, 24, 30, 42: so findet sich ihr größter gemeinschaftlicher Theiler $= 6$, und die versuchte Division durch diese gibt die Quotienten 2, 4, 5, 7. Also ist

$6 . 2 . 4 . 5 . 7 = 1680$ das kleinste gemeinschaftliche Vielfache jener Zahlen.

§. 112. Lehrsatz. Wenn ein Paar Zahlen M und N von einer solchen Beschaffenheit sind, daß man $M^m = N^n$ hat, wobey die Exponenten m und n ein Paar relative Primzahlen bezeichnen; so muß es irgendeine dritte Zahl C von der Art geben, daß $C^n = M$. und $C^m = N$ ist.

Beweis. Weil $M^m = N^n$ ist, so müssen beyde Zahlen M^m und N^n aus denselben einfachen Factoren in gleicher Anzahl zusammengesetzt seyn (§. 71.). Bezeichnen wir aber die einfachen Factoren der Zahl M durch $a. b. c. d, \ldots$ und die Anzahl, wie oft ein jeder dieser Factoren in M erscheint, beziehlich durch $\alpha, \beta, \gamma, \delta, \ldots$, so ist $M = a^\alpha b^\beta c^\gamma d^\delta \ldots$ und somit $M^m = a^{\alpha m} . b^{\beta m} . c^{\gamma m} . d^{\delta m} \ldots$, welches auch $= N^n$ seyn soll. Hiernächst muß einer der einfachen Factoren, aus welchen N^n zusammengesetzt ist, $= a$ seyn, und dieser Factor muß in N^n αm-mahl erscheinen. Kein Zweifel also, daß dieser Factor in N bloß $\frac{\alpha m}{n}$-mahl erscheint. Auf gleiche Weise erhellet, daß N auch den einfachen Factor b enthalten müsse und zwar diesen $\frac{\beta m}{n}$-mahl, sodann den einfachen Factor c, und zwar $\frac{\gamma m}{n}$-mahl u. s. w. Also ist $N = a^{\frac{\alpha m}{n}} . b^{\frac{\beta m}{n}} . c^{\frac{\gamma m}{n}} . d^{\frac{\delta m}{n}} \ldots$, wo $\frac{\alpha m}{n} . \frac{\beta m}{n} , \frac{\gamma m}{n} . \frac{\delta m}{n} \ldots$ wirkliche Zahlen seyn müssen. Da aber m und n keinen gemeinschaftlichen Theiler haben: so folgt aus §. 60., daß auch $\frac{\alpha}{n} . \frac{\beta}{n} , \frac{\gamma}{n} . \frac{\delta}{n} \ldots$ wirkliche Zahlen seyn müssen. Mithin wird auch $a^{\frac{\alpha}{n}} . b^{\frac{\beta}{n}} . c^{\frac{\gamma}{n}} . d^{\frac{\delta}{n}} \ldots$ eine wirkliche Zahl vorstellen. Bezeichnen wir diese durch C, so ist $C^n = a^\alpha . b^\beta . c^\gamma . d^\delta \ldots$, d. i. $= M$ und $C^m = a^{\frac{\alpha m}{n}} . b^{\frac{\beta m}{n}} . c^{\frac{\gamma m}{n}} . d^{\frac{\delta m}{n}} \ldots$. d. i. $= N$. So findet sich $36^3 = 216^2 = 46656$. Daher ist denn auch eine Zahl, nähmlich 6, angeblich von der Art, daß $6^2 = 36$ und $6^3 = 216$ ist.

§. 113. Lehrsatz. Wenn in dem Ausdrucke $x^2 - ay^2 - b$, die Zeichen a und b zwey beliebige positive oder negative, aber wirkliche Zahlen bezeichnen: so gibt es jederzeit gewisse an die Stelle von x und y zu setzende Werthe, welche entweder Null oder wirkliche, auf jeden Fall aber den Werth $\frac{c}{2}$ nicht übersteі-

gende Zahlen sind, die jenen Ausdruck theilbar durch die beliebige wirkliche Zahl c machen.

Beweis. Wenn b selbst theilbar durch c ist; so sind schon $x=0$ und $y=0$ ein Paar Werthe, wie sie der Lehrsatz verlangt. Allein ganz abgesehen von diesem besonderen Falle lasset uns unterscheiden, ob c gerade oder ungerade ist.

1. Wenn c gerade ist; so ist auch $\frac{c}{2}$ eine wirkliche Zahl; und es gibt der Werthe, welche die Zahl $\frac{c}{2}$ nicht übersteigen, wenn wir die Null mit dazu rechnen sollen, offenbar $\frac{c}{2}+1$. Werden nun alle diese Werthe in den Ausdruck $\frac{x^2}{c}$ sowohl als auch in den $\frac{ay^2+b}{c}$ nach und nach substituirt: so behaupte ich, es müsse unter den $\left(\frac{c}{2}+1\right)$ verschiedenen Werthen des Ausdrucks $\frac{x^2}{c}$ wenigstens Einen geben, bey welchem der durch die angezeigte Division mit c entstehende Rest derselbe ist, der auch bey einem der $\left(\frac{c}{2}+1\right)$ verschiedenen Werthe von $\frac{ay^2+b}{c}$ zum Vorschein kommt. Denn wären alle diese Reste von einander verschieden: so müßte es, weil ihre Anzahl $2\left(\frac{c}{2}+1\right)=c+2$ ist, $c+2$ verschiedene Reste geben, die durch die Division mit c entstehen können, welches doch ungereimt ist. Gibt es dagegen einen für x zu setzenden Werth z. B. ξ, der nicht $>\frac{c}{2}$ ist, und bey dem $\frac{x^2}{c}$ den Rest γ gibt, und eben so einen für y zu setzenden Werth, der abermahls nicht $>\frac{c}{2}$ und bey dem $\frac{ay^2+b}{c}$ denselben Rest γ gibt: so ist nach §. 10. der Unterschied ξ^2-ay^2-b theilbar durch c.

2. Wenn c ungerade ist; so gibt es der Werthe, welche nicht $>\frac{c}{2}$ sind, wenn wir die Null mit dazu nehmen, $=\frac{c+1}{2}$. Werden nun alle diese Werthe in $\frac{x^2}{c}$ sowohl als auch in $\frac{ay^2+b}{c}$ nach und nach substituirt: so leuchtet wie vorhin ein, daß es unter den $\frac{c+1}{2}$ verschiedenen Werthen von $\frac{x^2}{c}$ wenigstens Einen geben müsse, bey welchem eben derselbe Rest eintritt, der auch bey

einem der $\frac{c+1}{2}$ verschiedenen Werthen von $\frac{ay^2+b}{c}$ Statt findet; weil im widrigen Falle behauptet werden müßte, daß es $2\binom{c+1}{2}$ d. i. $c+1$ von einander verschiedene Reste gebe, die bey der Division durch c zum Vorschein kommen können. Ist aber ξ ein Werth nicht $>\frac{c}{2}$, bey welchem $\frac{x^2}{c}$ den Rest γ, und y ein Werth nicht $<\frac{c}{2}$, bey welchem $\frac{ay^2+b}{c}$ denselben Rest γ gibt: so ist ξ^2-ay^2-b offenbar theilbar durch c.

Beyspiel. Wenn x^2+y^2+1 theilbar durch 5 zu machen, und zwar durch Werthe von x und y, welche nicht $>\frac{5}{2}$ sind: erhalten wir $x=0$ und $y=2$ oder $x=2$ und $y=0$. Um x^2+7y^2-3 theilbar durch 6 zu machen vermittelst Werthen, welche nicht $>\frac{6}{2}$ sind, findet sich $x=2$, $y=1$: welches $\frac{4+7-3}{6}=1$ gibt. U. s. w.

§. 114. Lehrsatz. Jede Primzahl p läßt sich als eine Summe von höchstens vier Quadratzahlen betrachten.

Beweis. Nach dem vorigen Lehrsatze ist es immer möglich Werthe für x und y, welche entweder Null oder ganzzählig und dabey nicht größer als $\frac{p}{2}$ sind, zu wählen, mit dem Erfolge, daß der Ausdruck x^2+y^2+1 theilbar durch p werde. Folglich ist es auch möglich für die vier Zeichen x, y, w und z Werthe, welche entweder Null oder ganzzählig und dabey nicht $>\frac{p}{2}$ sind, mit dem Erfolge zu wählen, daß der Ausdruck $x^2+y^2+w^2+z^2$ theilbar durch die Zahl p werde. Denn dazu bedarf es nur x und y so zu bestimmen, daß x^2+y^2+1, und w und z so, daß w^2+z^2-1 theilbar durch p werde: oder, was noch kürzer ist, $w=1$ und $z=0$ zu setzen. Es seyen also x, y, w, z solche Werthe, dabey $x^2+y^2+w^2+z^2=p\,.\,p_1$ ist, wo p_1 eine beliebige wirkliche Zahl bezeichnet. Weil nun keine der vier Zahlen x, y, w und $z>\frac{p}{2}$ seyn soll: und $\frac{p}{2}$ ein wirklicher Bruch ist: so erhellet, daß jede der vier Zahlen $x, y, w, z<\frac{p}{2}$ seyn müsse. Daher muß denn (nach §.) auch $x^2+y^2+w^2+z^2<4\frac{p^2}{4}=p^2$ seyn: und somit ist $p\,.\,p_1<p^2$, also $p_1<p$. Wäre nun $p_1=1$: so hätte man $x^2+y^2+w^2+z^2=p$

und es wären die Quadratzahlen, deren Summe der Primzahl p gleich kommt, bereits gefunden. Ist aber p_1 noch >1; so setzen wir $x_1 = x - \alpha p_1$; $y_1 = y - \beta p_1$; $w_1 = w - \gamma p_1$; $z_1 = z - \delta p_1$, und nehmen $\alpha, \beta, \gamma, \delta$ so, daß x_1, y_1, w_1, z_1 sämmtlich nicht $> \frac{1}{2} p_1$ sind. Dieß ist (nach §. 12.) immer möglich, und bedarf für den Fall, daß etwa $z = 0$ ist, nur daß wir auch δ und $z_1 = 0$ nehmen.

Dann wird

$$x_1^2 + y_1^2 + w_1^2 + z_1^2 =$$
$$= x^2 + y^2 + w^2 + z^2 - 2(x\alpha + y\beta + w\gamma + z\delta)p_1 + \alpha^2 p_1^2 + \beta^2 p_1^2 + \gamma^2 p_1^2 + \delta^2 p_1^2.$$

Da nun $x^2 + y^2 + w^2 + z^2$ theilbar durch p_1; so ist das rechte Glied dieser Gleichung durchgängig theilbar durch p_1, mithin auch das linke, oder es muß $x_1^2 + y_1^2 + w_1^2 + z_1^2$ von der Form $p_1 . p_2$ seyn, wo sich, wie vorhin, darthun läßt, daß $p_2 < p_1$ sey. Wir wissen (aus §.), daß jedes Product aus zwey Factoren, deren jeder eine Summe von wenigstens vier Quadratzahlen ist, aufgelöst werden könne in eine Summe von höchstens vier Quadraten; so zwar, daß

$$(x^2 + y^2 + w^2 + z^2)(x_1^2 + y_1^2 + w_1^2 + z_1^2) =$$
$$(xx_1 + yy_1 + ww_1 + zz_1)^2 + (xy_1 - yx_1 + wz_1 - zw_1)^2 + (xw_1 - yz_1 - wx_1 + zy_1)^2 + (xz_1 + yw_1 - wy_1 - zx_1)^2.$$

Setzen wir in diese Formel für x_1, y_1, w_1, z_1 die Werthe $x - \alpha p_1$, $y - \beta p_1$, $w - \gamma p_1$, $z - \delta p_1$; so erhalten wir, wenn wir noch überdieß bemerken, daß $(x^2 + y^2 + w^2 + z^2) = pp_1$, $(x_1^2 + y_1^2 + w_1^2 + z_1^2)$ aber $= p_1 p_2$ sey,

$$pp_1^2 p_2 = [pp_1 - (\alpha x + \beta y + \gamma w + \delta z)p_1]^2 + [\alpha y - \beta x + \gamma z - \delta w]^2 p_1^2 + [\alpha w - \beta z - \gamma x + \delta y]^2 p_1^2 + [\alpha z + \beta w - \gamma y - \delta x]^2 p_1^2,$$

oder

$$pp_2 = [p - \alpha x - \beta y - \gamma w - \delta z]^2 + [\alpha y - \beta x + \gamma z - \delta w]^2 + [\alpha w - \beta z - \gamma x + \delta y]^2 + [\alpha z + \beta w - \gamma y - \delta x]^2.$$

Ist nun $p_2 = 1$; so ist die Primzahl p in eine Summe von vier oder weniger Quadratzahlen zerlegt. Ist aber $p_2 > 1$; so können wir durch Wiederholung desselben Verfahrens ein neues Vielfache von p, pp_3 finden, welches der Summe von vier oder weniger Quadratzahlen gleich kommen wird. In diesem Vielfachen wird p_3 abermahls $< p_2$ seyn. Da nun eine Reihe von wirklichen Zahlen, deren jede folgende kleiner als die vorhergehende ist, nie ins Unendliche fortschreiten kann; so leuchtet ein, daß wir nach einer gewissen Anzahl von Wiederholungen dieses Verfahrens auf eine Zahl p_n kommen müssen, welche $= 1$

ist. Somit ist dargethan, daß eine jede Primzahl in eine Summe von höchstens vier Quadratzahlen zerlegt werden könne.

§. 115. Zusatz. Also kann jede beliebige Zahl betrachtet werden als eine Summe von höchstens vier Quadratzahlen. Denn eine Zahl, die keine Primzahl ist, ist ein Product aus Primzahlen, und läßt sich also zerlegen in ein Product, dessen jeder einzelne Factor eine Summe von höchstens vier Quadratzahlen ist. Ein solches Product aber kann auf eine Summe von vier oder weniger Quadratzahlen zurückgeführt werden.

Beyspiel. So ist $2=1+1$; $3=1+1+1$; $4=2^2$; $5=2^2+1$; $6=2^2+1+1$; $7=2^2+1+1+1$; $8=2^2+2^2$; $9=3^2$; $10=3^2+1$; $11=3^2+1+1$; $12=3^2+1+1+1$; $13=3^2+2^2$; $14=3^2+2^2+1$; $15=3^2+2^2+1+1$; $16=4^2$ u. s. w.

§. 116. Lehrsatz. Wenn a und b ein Paar relative Primzahlen sind, und es bezeichnet β die Anzahl aller Zahlen, die $<b$ und mit b relative Primzahlen sind; so ist immer $a^\beta-1$ theilbar durch b.

Beweis. Wenn wir die sämmtlichen Zahlen, welche $<b$ und relative Primzahlen mit b sind, nach ihrer Größe geordnet durch die Zeichen (1), (2), (3),... vorstellig machen: so wird das erste dieser Zeichen (1) mit 1 selbst gleichgeltend seyn: das letzte aber wird, weil die Anzahl aller $=\beta$ ist, (β) seyn. Multipliziren wir nun eine jede dieser Zahlen durch a: so stellt

$$a(1),\ a(2),\ a(3),\ \ldots,\ a(\beta)$$

eine Reihe vor, darin kein Glied theilbar durch b ist; denn sowohl der Factor a als auch der andere von der Form (1),(2),... stehet zu b in dem Verhältnisse einer relativen Primzahl. Ferner behaupte ich, daß die versuchte Division mit b bey jedem dieser Glieder einen von dem der übrigen Glieder verschiedenen Rest hervorbringen werde. Denn sollten zwey dieser Glieder, ich will sie durch $a(\beta')$ und $a(\beta'')$ bezeichnen, einen gleichen Rest geben; so müßte die Differenz $a(\beta')-a(\beta'')=a[(\beta')-(\beta'')]$ nach §. 10. theilbar durch b seyn. Da aber b und a relative Primzahlen sind; so müßte es nur der Factor $(\beta')-(\beta'')$ seyn, der sich durch b theilen läßt. Dieß aber ist ungereimt, weil sowohl (β') als (β''), um so gewisser ihr Unterschied $(\beta')-(\beta'')$, $<b$ ist. Da also jedes Glied obiger Reihe durch die Division mit b einen Rest, und jedes einen einzigen gibt, die Anzahl aller aber $=\beta$ ist: so leuchtet ein, daß diese Reste, da sie insgesammt $<\beta$ seyn müssen, keine anderen seyn können, als die Zahlen

$$1), (2), (3), \ldots, (\beta),$$

was wir jedoch keineswegs so ausgelegt wissen wollen, als ob diese Reste in eben der Ordnung, in der sie hier stehen, zum Vorschein kämen, wenn man die Glieder der obigen Reihe in eben der Ordnung, in der sie oben vorkommen, durch die Zahl b dividirt. Hieraus ergibt sich (nach §.), daß es zu jedem Gliede der Reihe

$$a(1), a(2), a(3). \ldots, a(\beta)$$

eines, aber auch nur ein einziges der Reihe

$$(1), (2), (3), \ldots, (\beta)$$

gibt, deren Unterschied theilbar durch b ist. Nach §. 24. ist also auch der Unterschied zwischen den beyden Producten, welche zum Vorschein kommen, wenn wir in den vorhin erwähnten Unterschieden alle Minuenden und alle Subtrahenden untereinander multipliziren; d. i.

$$a(1) \,.\, a(2) \,.\, a(3) \ldots a(\beta) - (1)\,(2)\,(3) \ldots (\beta),$$

oder $[a^\beta - 1]\,(1)\,(2)\,(3) \ldots (\beta)$, theilbar durch b. Da aber jeder der Factoren $(1), (2), (3), \ldots, (\beta)$ eine relative Primzahl zu b ist; so ergibt sich nach §. 62., daß es der Factor $a^\beta - 1$ seyn müsse, in welchem b aufgehet.

Beyspiel. So sind 15 und 4 ein Paar relative Primzahlen, setzen wir also $15 = a$, und $4 = b$; so findet sich $\beta = 2$, und es muß $15^2 - 1$ theilbar durch 4 seyn: wie denn allerdings $\frac{15^2-1}{4} = \frac{224}{4} = 56$ ist. Setzen wir aber $4 = a$ und $15 = b$: so findet sich $\beta = 8$ und es soll $4^8 - 1$ theilbar durch 15 seyn. In der That ist $\frac{4^8-1}{15} = \frac{65535}{15} = 4369$.

§. 117. Zusatz. Ist die Zahl b eine absolute Primzahl $= p$; so ist $\beta = p - 1$ (§. 102.). Also ist, sofern a eine Zahl bedeutet, in welche die Primzahl p nicht aufgehet, jedesmahl $a^{p-1} - 1$ theilbar durch p. Ist z. B. $p = 5$ und $a = 11$; so ist $11^4 - 1 = 14640$ theilbar durch 5; weil $\frac{14640}{5} = 2928$.

§. 118. Anmerkung. Fermat ist der Erfinder dieses und des vorhergehenden Satzes; daher sie auch seinen Nahmen tragen.

§. 119. Lehrsatz. Wenn p eine Primzahl ist; so gibt es zu jedem Gliede der Reihe $2, 3, 4, \ldots, (p-2)$ ein, aber auch nur ein

einziges andere von der Beschaffenheit, daß das Product beyder, um Eins vermindert, theilbar durch p ist.

Beweis. 1. Wenn wir durch p' irgend eine Zahl $< p$ bezeichnen; so ist kein Glied der Reihe

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

theilbar durch p, weil jeder der beyden Factoren, aus welchen die Glieder dieser Reihe zusammengesetzet sind, $< p$ ist.

2. Jedes Glied aber gibt bey der versuchten Division durch p einen Rest, der von dem Reste, welchen ein anderes gibt, sich unterscheidet. Denn stellen wir durch $p''(p-p')$ und $p'''(p-p')$ zwey Glieder dieser Reihe vor (wo also auch p'' und p''' Zahlen, die $< p$ sind, bedeuten müssen): so müßte, wenn diese Glieder einerley Reste geben, der Unterschied

$$p''(p-p')-p'''(p-p')=(p''-p''')(p-p')$$

theilbar durch p seyn; welches doch ungereimt ist, weil sowohl $p''-p'''$ als auch $p-p'$ wirkliche Zahlen $< p$ bezeichnen.

3. Da also ein jedes Glied der obigen Reihe seinen eigenen Rest gibt, und diese Reste alle $< p$ seyn müssen, ihre Anzahl aber $= p-1$ ist: so erhellet, daß sie nur in den folgenden Zahlen $1, 2, 3, \ldots, (p-1)$ bestehen können.

4. Also muß es in unserer obigen Reihe für jeden Werth von p' immer ein, aber auch nur ein einziges Glied geben, das den Rest 1 läßt; und mithin so beschaffen ist, daß es, wenn wir erst 1 davon abziehen, theilbar durch p wird.

5. Dieß Glied ist, wenn wir $p' > 1$ und $< p-1$ annehmen, weder das erste noch letzte in jener obigen Reihe. Nicht das erste: denn $1(p-p')-1=p-p'-1$ ist sicher nicht theilbar durch p; weil es bey der angenommenen Beschaffenheit der Werthe von p stets eine wirkliche Zahl, aber $< p$ verbleibt. Auch nicht das letzte: denn

$$(p-1)(p-p')-1=p^2-p-pp'+p'-1=p(p-1-p')+p'-1$$

kann nur theilbar durch p werden, wenn $p'-1$ theilbar durch p oder 0 ist; und Beydes ist bey der angenommenen Beschaffenheit der Werthe von p' unmöglich.

6. Also muß, wenn wir das erste und letzte Glied aus unserer obigen Reihe weglassen, aber noch immer voraussetzen, daß p' nur immer > 1 und $< p-1$ genommen werde, auch die Reihe der noch übrigbleibenden Glieder

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

die Beschaffenheit haben, daß es für jeden Werth von p' Ein und nur Ein Glied in ihr gibt, welches um 1 vermindert theilbar durch p ist.

7. Bey der vorausgesetzten Beschaffenheit der Werthe von p' sind aber die sämmtlichen Werthe, die $p-p'$ annehmen kann, folgende

$$2, 3, 4, \ldots, (p-2).$$

Den ersten nähmlich erhält $p-p'$, wenn wir $p'=p-2$, den zweyten, wenn wir $p'=p-3$, den dritten, wenn wir $p'=p-4$, ... den letzten, wenn wir $p'=2$ nehmen. Diese Reihe ist völlig einerley mit der Reihe, welche die ersten Factoren der Glieder in der zuletzt betrachteten Reihe bilden: denn auch diese sind

$$2, 3, 4, \ldots, (p-2).$$

Indem wir also dem p' in der Reihe

$$2(p-p'), 3(p-p'), 4(p-p'), \ldots, (p-2)(p-p')$$

die verschiedenen zwischen 1 und $p-1$ liegenden Werthe ertheilen, bilden wir Producte, die alle auch zum Vorschein gebracht werden können, wenn wir ein jedes Glied der Reihe

$$2, 3, 4, \ldots, (p-2)$$

entweder mit sich selbst oder mit einem anderen derselben Reihe multipliziren.

8. Die Producte aber, welche entstehen, wenn wir ein Glied dieser letzten Reihe mit sich selbst multipliziren, können die in Rede stehenden Beschaffenheiten, nähmlich daß sie vermindert um 1 theilbar durch p werden, nicht haben. Denn sie sind von der Form $(p-p')^2-1=(p-p'+1)(p-p'-1)$ und keiner von diesen beyden Factoren ist, wenn $p'>1$ und $<p-1$ gewählt wird, theilbar durch p.

9. Also erhalten wir alle Producte von der erwähnten Beschaffenheit schon dann, wenn wir nur jedes Glied der Reihe

$$2, 3, 4, \ldots, (p-2)$$

mit einem anderen multipliziren.

10. Für jedes dieser Glieder aber gibt es gewiß ein zweytes, mit dem es ein Product von der besagten Beschaffenheit bildet. Denn gäbe es keines; so gäbe es auch in der Reihe

$$2(p-p'), 3(p-p'), 4(p-p'), \ldots, (p-2)(p-p')$$

ein Glied, welches für keinen der für p' möglichen Werthe die besagte Beschaffenheit, daß es nähmlich um 1 vermindert theil-

bar durch p wird, erhielte; dagegen dasjenige, was wir schon Nro 6. erwiesen.

11. Endlich erhellet auch noch, daß es für jedes Glied dieser Reihe $2, 3, 4, \ldots, (p-2)$ nur ein einziges anderes gebe, welches mit ihm ein Product von der besagten Beschaffenheit bildet. Denn gäbe es irgendein Glied dieser Reihe $p_{,}$, welches verbunden sowohl mit dem Gliede $p_{,,}$ als auch mit dem von $p_{,,}$ verschiedenem $p_{,,,}$ Producte von der besagten Beschaffenheit liefert; so müßte $p_{,}p_{,,}-1$, sowohl als auch $p_{,}p_{,,,}-1$ theilbar durch p seyn. Das hieße aber, daß auch $p_{,}p_{,,}-p_{,}p_{,,,}=p_{,}(p_{,,}-p_{,,,})$ theilbar durch p sey, welches doch ungereimt ist, weil sowohl p als auch $p_{,,}$ und $p_{,,,}$ und somit auch $p_{,,}-p_{,,,}<p$ und doch nicht Null seyn sollen.

Beyspiel. Für die Primzahl $p=11$ soll also die Reihe

$$2, 3, 4, 5, 6, 7, 8, 9$$

von einer solchen Beschaffenheit seyn, daß es zu jedem ihrer Glieder ein, aber auch nur ein einziges anderes gibt, das mit dem ersten ein Product bildet, welches vermindert um 1 theilbar durch 11 wird. Und so ist es wirklich; diese Producte sind nähmlich 2.6, 3.4, 5.9, 7.8, denn $\frac{2.6-1}{11}=1$, $\frac{3.4-1}{11}=1$, $\frac{5.9-1}{11}=4$, $\frac{7.8-1}{11}=5$.

§. 120. Erklärung. Solche je zwey und zwey zusammenhängende Zahlen der Reihe $2, 3, 4, \ldots, p-2$, deren Product, wenn es um Eins vermindert wird, theilbar durch die Primzahl p, nennt man (mit Euler und Gauß) Gefährten. So ist also z. B. für $p=11$ der Gefährte von 2 die Zahl 6, der Gefährte von 3 die Zahl 9 u. s. w.

§. 121. Lehrsatz. Wenn p eine Primzahl ist; so ist immer

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

theilbar durch p.

Beweis. Nach dem vorhergehenden Satze gibt es, wenn p eine Primzahl, für jedes Glied in der Reihe $2, 3, 4, \ldots, (p-2)$ ein, aber auch nur ein einziges andere, welches mit jenem ein Product liefert, das durch Verminderung um 1 theilbar durch die Zahl p wird. Wenn wir uns vorstellen, daß diese Producte alle gebildet wären, und daß bey einem jeden angemerkt wäre, daß man die Einheit noch von ihm abzuziehen habe: so hätten wir eine Anzahl von Differenzen vor uns, die alle theilbar durch p sind. Nach §. 24. wird denn also auch diejenige Differenz

theilbar durch p seyn, welche zum Vorschein kommt, wenn wir die sämmtlichen in diesen Differenzen vorkommenden Minuenden untereinander multiplizirt zum Minuendus, und die sämmtlichen in diesen Differenzen vorkommenden Subtrahenden abermahls untereinander multiplizirt zum Subtrahendus der neuen Differenz machen.

Das erste Product wird offenbar aus den sämmtlichen Zahlen

$$2, 3, 4, \ldots, (p-2)$$

bestehen, und somit $2.3.4\ldots(p-2)$ seyn; das zweyte aber wird als ein Product aus lauter Einern $=1$ seyn. Es erhellet also, daß auch die Differenz $2.3.4\ldots(p-2)-1$ theilbar durch p sey. Es ist aber offenbar auch die Differenz $(p-1)-(-1)$, weil sie $=(p-1)+1=p$ ist, theilbar durch p. Folglich nach §. 24. auch

$$2.3.4\ldots(p-2)(p-1)-1(-1)$$

theilbar durch p. Allein statt $2.3.4\ldots(p-2)(p-1)$ können wir auch schreiben $1.2.3.4\ldots(p-1)$ und statt $-(-1)$ auch $+1$; folglich ist $1.2.3.4\ldots(p-1)+1$ theilbar durch p.

Beyspiel. Für die Primzahl 11 findet sich $1.2.3.4\ldots$ $\ldots 10+1=3628801$, welches allerdings theilbar durch 11 ist, und den Quotienten 329891 gibt.

§. 122. Anmerkung. Der Erfinder dieses merkwürdigen Satzes soll John Wilson seyn.