Sechster Abschnitt.

Verschiedene Anwendungen der vorhergehenden Untersuchungen.

308.

Wie fruchtbar die höhere Arithmetik an Wahrheiten ist, welche auch in andern Teilen der Mathematik Nutzen gewähren, haben wir bereits an mehreren Stellen vorübergehend berührt; wir haben es aber für nicht unnützlich gehalten, gewisse Anwendungen, welche eine ausführlichere Auseinandersetzung verdienen, für sich zu behandeln, nicht sowohl um diesen Gegenstand, mit dem man leicht mehrere Bände füllen könnte, zu erschöpfen, als vielmehr ihn durch einige Proben in ein helleres Licht zu setzen. Im gegenwärtigen Abschnitte werden wir zuerst von der Zerlegung der Brüche in einfachere, sodann von der Verwandlung der gemeinen Brüche in Decimalbrüche handeln; darauf werden wir eine neue Ausschliessungsmethode, welche zur Auflösung der unbestimmten Gleichungen zweiten Grades dient, auseinandersetzen; endlich werden wir neue einfache Methoden angeben, um die Primzahlen von den zusammengesetzten zu unterscheiden und die Factoren der letzteren zu ermitteln. Im folgenden Abschnitte aber werden wir die allgemeine Theorie einer besonderen in der gesamten Analysis sehr häufig angewandten Art von Functionen, soweit sie mit der höheren Arithmetik in innigstem Zusammenhange steht, begründen und insbesondere die Theorie der Kreisteilung, von der bisher nur die ersten Elemente bekannt waren, durch neue Zuthaten zu erweitern suchen.

Zerlegung der Brüche in einfachere.

309.

Aufgabe. Den Bruch $\frac{m}{n}$, dessen Nenner das Product aus zwei zu einander primen Zahlen a, b ist, in zwei andere zu zerlegen, deren Nenner a und b sind.

Auflösung. Sind die gesuchten Brüche $\frac{x}{a}$, $\frac{y}{b}$, so muss $bx + ay = m$ werden; demnach ist x die Wurzel der Congruenz $bx \equiv m \pmod{a}$, die man nach Abschnitt II finden kann; y aber wird gleich $\frac{m - bx}{a}$.

Übrigens ist bekannt, dass die Congruenz $bx \equiv m$ unendlich viele, aber nach dem Modul a congruente Wurzeln besitzt, dass es aber nur eine einzige positive Wurzel, welche kleiner als a ist, giebt; ferner kann es aber auch geschehen, dass y negativ wird. Es wird kaum nötig sein, darauf hinzuweisen, dass y auch durch die Congruenz $ay \equiv m \pmod{b}$ und x durch die Gleichung $x = \frac{m - ay}{b}$ gefunden werden kann. — Ist z. B. der Bruch $\frac{58}{77}$ gegeben, so ist 4 der Wert des Ausdrucks $\frac{58}{11} \pmod{7}$, und somit zerfällt $\frac{58}{77}$ in $\frac{4}{7} + \frac{2}{11}$.

310.

Ist ein Bruch $\frac{m}{n}$ gegeben, dessen Nenner n das Product aus beliebig vielen zu einander primen Zahlen $a, b, c, d, \ldots$ ist, so kann derselbe nach dem vorigen Artikel zunächst in zwei zerlegt werden, deren Nenner a und $bcd\ldots$ sind; der zweite wiederum in zwei mit den Nennern b und $cd\ldots$; der letztere wiederum in zwei u. s. f., bis endlich der gegebene Bruch auf die Form gebracht ist:

$$\frac{m}{n} = \frac{\alpha}{a} + \frac{\beta}{b} + \frac{\gamma}{c} + \frac{\delta}{d} + \cdots$$

Die Zähler $\alpha, \beta, \gamma, \delta\ldots$ kann man offenbar positiv und kleiner als ihre Nenner annehmen, mit Ausnahme des letzten, welcher, nachdem die übrigen bestimmt sind, nicht weiter willkürlich ist und auch negativ und grösser als der Nenner werden kann (wofern wir nicht $m < n$ voraussetzen). Dann wird es meistens zweckmässig sein, ihn auf die Form $\frac{\varepsilon}{e} \mp k$ zu bringen, so dass ε eine positive Zahl und kleiner als e, k aber eine ganze Zahl ist. Endlich ist klar, dass $a, b, c, \ldots$ so angenommen werden können, dass sie entweder Primzahlen oder Potenzen von Primzahlen sind.

Beispiel. Der Bruch $\frac{391}{924}$, dessen Nenner gleich $4 \cdot 3 \cdot 7 \cdot 11$ ist, wird auf diese Weise zerlegt in $\frac{1}{4} + \frac{40}{231}$; $\frac{40}{231}$ in $\frac{2}{3} - \frac{38}{77}$; $-\frac{38}{77}$ in $\frac{1}{7} - \frac{7}{11}$, so dass, wenn man $\frac{4}{11} - 1$ für $-\frac{7}{11}$ schreibt, $\frac{391}{924} = \frac{1}{4} + \frac{2}{3} + \frac{1}{7} + \frac{4}{11} - 1$ wird.

311.

Der Bruch $\frac{m}{n}$ lässt sich nur auf eine einzige Weise auf die Form $\frac{\alpha}{a}+\frac{\beta}{b}+\cdots\mp k$ derart bringen, dass α, β, ... positiv und kleiner als a, b, ... respective sind; denn nimmt man an, dass

$$\frac{m}{n}=\frac{\alpha}{a}+\frac{\beta}{b}+\frac{\gamma}{c}+\cdots\mp k=\frac{\alpha'}{a}+\frac{\beta'}{b}+\frac{\gamma'}{c}+\cdots\mp k'$$

sei, und dass auch α', β', ... positive Zahlen und bezüglich kleiner als a, b, ... seien, so muss notwendig $\alpha=\alpha'$, $\beta=\beta'$, $\gamma=\gamma'$, ..., $k=k'$ sein. Multipliciert man nämlich mit $n=abc\ldots$, so wird offenbar $m\equiv abcd\ldots\equiv\alpha'bcd\ldots \pmod a$ und daher, weil $bcd\ldots$ zu a prim ist, notwendig $\alpha\equiv\alpha'$ und somit $\alpha=\alpha'$, und ebenso $\beta=\beta'$, u. s. w., woraus von selbst $k=k'$ folgt. Da es nun vollständig willkürlich ist, für welchen Nenner der Zähler zuerst berechnet wird, so ist ersichtlich, dass alle Zähler so wie α im vorigen Artikel gefunden werden können, nämlich β durch die Congruenz $\beta acd\ldots\equiv m \pmod b$, γ durch $\gamma abd\ldots\equiv m \pmod c$, u. s. w. Die Summe aller so gefundenen Brüche ist entweder gleich dem gegebenen Bruche $\frac{m}{n}$ oder der Unterschied ist eine ganze Zahl k, so dass wir auf diese Weise zugleich eine Bestätigung der Rechnung erhalten. So ergeben z. B. im Beispiel des vorigen Artikels die Werte der Ausdrücke $\frac{391}{231} \pmod 4$, $\frac{391}{308} \pmod 3$, $\frac{391}{132} \pmod 7$, $\frac{391}{84} \pmod{11}$ sogleich die den Nennern 4, 3, 7, 11 entsprechenden Zähler 1, 2, 1, 4, und man findet, dass die Summe dieser Brüche den gegebenen Bruch um eine Einheit übersteigt.

Verwandlung der gemeinen Brüche in Decimalbrüche.

312.

Erklärung. Wenn ein gemeiner Bruch in einen Decimalbruch verwandelt wird, so nennen wir die Reihe der Decimalzahlen*) (mit Ausschluss der ganzen Zahl, wenn eine vorhanden ist), mag dieselbe endlich sein oder ins Unendliche gehen, die **Mantisse** des Bruches, indem wir den Ausdruck, der sonst nur bei den Logarithmen gebräuchlich ist, in einer weiteren Bedeutung nehmen. So ist z. B. die Mantisse des Bruches $\frac{1}{8}$ gleich 125, die Mantisse des Bruches $\frac{35}{16}$ gleich 1875, die Mantisse des Bruches $\frac{2}{37}$ gleich 054054 .... *in inf.*

*) Der Kürze halber beschränken wir die folgende Untersuchung auf das gemeine decadische System, da sie sich leicht auf jedes beliebige System ausdehnen lässt.

Aus dieser Erklärung geht sogleich hervor, dass Brüche mit demselben Nenner $\frac{l}{n}$, $\frac{m}{n}$ dieselben oder verschiedene Mantissen haben, je nachdem die Zähler l, m nach n congruent oder incongruent sind. Eine endliche Mantisse wird nicht geändert, wenn man rechts beliebig viele Nullen ansetzt. Die Mantisse des Bruches $\frac{10m}{n}$ erhält man, wenn man von der Mantisse des Bruches $\frac{m}{n}$ die erste Ziffer abschneidet, und allgemein, die Mantisse des Bruches $\frac{10^\nu m}{n}$ findet man, wenn man von der Mantisse des Bruches $\frac{m}{n}$ die ν ersten Ziffern abschneidet. Die Mantisse des Bruches $\frac{1}{n}$ beginnt sogleich mit einer geltenden (d. h. von Null verschiedenen) Ziffer, wenn n nicht grösser als 10 ist; ist aber $n > 10$ und keiner Potenz von 10 gleich, und die Anzahl der Ziffern, aus denen sie besteht, gleich k, so sind die $k-1$ ersten Ziffern der Mantisse Nullen und erst die folgende k^{te} ist eine geltende Ziffer. Hieraus folgt leicht, dass, wenn $\frac{l}{n}$, $\frac{m}{n}$ verschiedene Mantissen haben (d. h. wenn l, m nach n incongruent sind), diese sicher nicht in den ersten k Ziffern übereinstimmen können, sondern wenigstens in der k^{ten} von einander abweichen müssen.

313.

Aufgabe. Wenn der Nenner des Bruches $\frac{m}{n}$ und die ersten k Ziffern seiner Mantisse gegeben sind, so soll man den Zähler m finden, den wir kleiner als n voraussetzen.

Auflösung. Man betrachte jene k Ziffern als eine ganze Zahl, multipliciere dieselbe mit n und dividiere das Product durch 10^k (oder schneide die k letzten Ziffern ab). Ist der Quotient eine ganze Zahl (oder sind die abgeschnittenen Ziffern Nullen), so ist derselbe selbst der gesuchte Zähler und die gegebene Mantisse vollständig; wenn nicht, so ist der gesuchte Zähler die nächsthöhere ganze Zahl oder jener um eine Einheit vermehrte Quotient, nachdem die folgenden Decimalstellen abgeschnitten worden sind. Der Grund dieser Regel ist aus unsern Bemerkungen am Schlusse des vorigen Artikels so leicht ersichtlich, dass es einer weiteren Auseinandersetzung nicht bedarf.

Beispiel. Wenn man weiss, dass die beiden ersten Ziffern der Mantisse eines Bruches, dessen Nenner 23 ist, 69 seien, so hat man das Product $23 \cdot 69 = 1587$; wirft man hiervon die beiden letzten Ziffern weg und addiert 1, so ergiebt sich der gesuchte Zähler gleich 16.

314.

Wir beginnen mit der Betrachtung solcher Brüche, deren Nenner Primzahlen oder Potenzen von Primzahlen sind, und werden nachher zeigen, wie man die übrigen auf diese zurückführen kann. Zunächst bemerken wir sogleich, dass die Mantisse des Bruches $\frac{a}{p^\mu}$ (von dessen Zähler a wir stets voraussetzen, dass er durch die Primzahl p nicht teilbar sei) endlich ist und aus μ Ziffern besteht, wenn $p = 2$ oder $p = 5$ ist; im ersteren Falle ist diese Mantisse, als ganze Zahl betrachtet, gleich $5^\mu a$, im letzteren gleich $2^\mu a$. Dies ist so klar, dass es einer Auseinandersetzung nicht bedarf.

Ist aber p eine andere Primzahl, so wird $10^r a$ durch p^μ niemals teilbar sein, wie gross man auch r annehmen möge, woraus unmittelbar folgt, dass die Mantisse des Bruches $F = \frac{a}{p^\mu}$ notwendig ins Unendliche fortgeht. Nehmen wir an, 10^e sei die niedrigste Potenz von 10, welche der Einheit nach dem Modul p^μ congruent ist (vgl. Abschnitt III, wo wir gezeigt haben, dass e entweder gleich der Zahl $(p-1)\,p^{\mu-1}$ oder ein aliquoter Teil derselben ist), so erkennt man leicht, dass auch $10^e a$ in der Reihe $10a$, $100a$, $1000a$, ... die erste Zahl ist, welche a nach demselben Modul congruent ist. Da nun nach Artikel 312 die Mantissen der Brüche $\frac{10a}{p^\mu}$, $\frac{100a}{p^\mu}$, ..., $\frac{10^e a}{p^\mu}$ entstehen, indem man von der Mantisse des Bruches F die erste Ziffer oder die beiden, u. s. w., e ersten Ziffern respective fortlässt, so ist klar, dass in dieser Mantisse nach den e ersten Ziffern und nicht eher dieselben Ziffern sich nochmals wiederholen. Diese ersten e Ziffern, aus deren unendlich oftmaliger Wiederholung die Mantisse gebildet ist, können wir die **Periode** dieser Mantisse oder des Bruches F nennen, und es ist ersichtlich, dass die Grösse der Periode oder die Anzahl der Ziffern, aus denen sie besteht, und welche gleich e ist, vom Zähler a vollständig unabhängig ist und nur allein durch den Nenner bestimmt wird. So ist z. B. die Periode des Bruches $\frac{1}{11}$ gleich 09, die Periode des Bruches $\frac{3}{7}$ gleich 428571.*)

315.

Sobald man daher die Periode irgend eines Bruches hat, kann die Mantisse auf beliebig viele Stellen fortgesetzt werden. Ferner ergiebt sich, dass, wenn $b \equiv 10^\lambda a \pmod{p^\mu}$ ist, die Periode des Bruches $\frac{b}{p^\mu}$ entsteht,

*) Robertson deutet den Anfang und das Ende der Periode durch zwei über die erste und letzte Ziffer derselben gesetzte Punkte an *(Theory of circulating fractions, Phil. Trans., 1769, p. 207)*, was wir hier nicht für nötig halten.

wenn man die ersten λ Ziffern des Bruches F (wenn wir, was erlaubt ist, $\lambda < e$ annehmen) hinter die übrigen $e - \lambda$ schreibt, und dass man somit zugleich mit der Periode des Bruches F die Perioden sämtlicher Brüche hat, deren Zähler den Zahlen $10a$, $100a$, $1000a$, ... nach dem Nenner p^μ congruent sind. So wird z. B., da $6 \equiv 3 \cdot 10^2 \pmod 7$ ist, die Periode des Bruches $\frac{6}{7}$ sofort aus der Periode des Bruches $\frac{3}{7}$ gleich 857142 gefunden.

So oft daher für den Modul p^μ die Zahl 10 primitive Wurzel ist (Artikel 57, 89), lässt sich aus der Periode des Bruches $\frac{1}{p^\mu}$ sofort die Periode jedes andern Bruches $\frac{m}{p^\mu}$ (dessen Zähler m durch p nicht teilbar ist) ableiten, indem man soviel Stellen von jener links abschneidet und rechts wieder ansetzt, als der Index von m Einheiten besitzt, wenn 10 als Basis genommen wird. Hieraus ist ersichtlich, warum in diesem Falle die Zahl 10 in der Tafel I stets als Basis genommen ist (Artikel 72).

Wenn dagegen 10 keine primitive Wurzel ist, so können aus der Periode des Bruches $\frac{1}{p^\mu}$ die Perioden nur von denjenigen Brüchen abgeleitet werden, deren Zähler irgend einer Potenz von 10 nach dem Modul p^μ congruent sind. Es sei 10^e die niedrigste Potenz von 10, welche der Einheit nach dem Modul p^μ congruent ist, ferner $(p-1)p^{\mu-1} = ef$ und eine solche primitive Wurzel r zur Basis genommen, dass der Index der Zahl 10 gleich f wird (Artikel 71). In diesem System haben somit die Zähler der Brüche, deren Perioden aus der Periode des Bruches $\frac{1}{p^\mu}$ abgeleitet werden können, die Indices $f, 2f, 3f, \ldots, ef-f$; analog können aus der Periode des Bruches $\frac{r}{p^\mu}$ die Perioden der Brüche, deren Zähler $10r$, $100r$, $1000r$, ... den Indices $f+1$, $2f+1$, $3f+1$, ... entsprechen, gefunden werden; aus der Periode des Bruches mit dem Zähler r^2 (dessen Index 2 ist) ergeben sich die Perioden der Brüche mit Zählern, deren Indices $f+2$, $2f+2$, $3f+2$, ... sind, und allgemein lassen sich aus der Periode des Bruches mit dem Zähler r^i die Perioden der Brüche mit Zählern, deren Indices $f+i$, $2f+i$, $3f+i$, ... sind, herleiten. Hieraus schliesst man leicht, dass, wenn man nur die Perioden der Brüche mit den Zählern $1, r, r^2, r^3, \ldots, r^{f-1}$ hat, alle übrigen daraus durch blosse Transposition nach folgender **Regel** abgeleitet werden können:

Es sei der Index des Zählers m eines gegebenen Bruches $\frac{m}{p^\mu}$ in dem System, in welchem r als Basis genommen ist, gleich i (welche Zahl wir kleiner als $(p-1)p^{\mu-1}$ annehmen); es werde (durch Division mit f) $i = \alpha f + \beta$ gesetzt, so dass α, β ganze positive Zahlen (oder auch 0) sind

und $\beta < f$ ist. Ist dies geschehen, so ergiebt sich die Periode des Bruches $\frac{m}{p^\mu}$ aus der Periode des Bruches, dessen Zähler r^β (und daher 1, wenn $\beta = 0$) ist, wenn man die α ersten Ziffern hinter die übrigen setzt (und somit diese Periode selbst beibehält, wenn $\alpha = 0$ ist). Dies wird hinreichend erklären, warum wir bei der Aufstellung der Tafel I die im Artikel 72 entwickelte Regel befolgt haben.

316.

Nach diesen Prinzipien haben wir für alle Nenner von der Form p^μ unterhalb 1000 eine Tafel der notwendigen Perioden aufgestellt, die wir ganz oder auch in noch weiterer Fortsetzung bei gegebener Gelegenheit veröffentlichen werden. Hier möge die bis zu 100 nur fortgeführte Tafel III als Probe genügen, und wird eine Erklärung derselben kaum nötig sein. Für diejenigen Nenner, für welche 10 primitive Wurzel ist, stellt sie die Perioden der Brüche mit dem Zähler 1 dar (nämlich für 7, 17, 19, 23, 29, 47, 59, 61, 97), für die übrigen die f den Zählern 1, r, r^2, ..., r^{f-1} entsprechenden Perioden, welche durch die beigeschriebenen Zahlen (0), (1), (2), ... unterschieden sind; für die Basis r ist immer dieselbe primitive Wurzel genommen wie in Tafel I. Hiernach kann also die Periode eines jeden Bruches, dessen Nenner in dieser Tafel enthalten ist, mittelst der Vorschriften des vorigen Artikels abgeleitet werden, nachdem der Index des Zählers nach der Tafel I berechnet ist. Übrigens lässt sich für so kleine Nenner die Aufgabe ebenso leicht ohne die Tafel I erledigen, wenn man durch gewöhnliche Division soviel Anfangsziffern der gesuchten Mantisse berechnet, als nach Artikel 313 erforderlich sind, um sie von allen andern desselben Nenners unterscheiden zu können (für die Tafel III nicht mehr als 2), und sämtliche demselben Nenner entsprechende Perioden durchmustert, bis man zu jenen Anfangsziffern gelangt, welche den Anfang der Periode unzweifelhaft anzeigen; es muss jedoch darauf hingewiesen werden, dass jene Ziffern auch getrennt sein können, so dass die erste (oder mehrere) das Ende irgend einer Periode, die andere (oder die anderen) den Anfang derselben Periode bilden.

Beispiel. Man sucht die Periode des Bruches $\frac{12}{19}$. Hier hat man für den Modul 19 nach Tafel I $\text{ind. } 12 = 2 \text{ ind. } 2 + \text{ind. } 3 = 39 \equiv 3 \pmod{18}$ (Artikel 57). Somit muss man, da man für diesen Fall nur eine dem Zähler 1 entsprechende Periode hat, die drei ersten Ziffern derselben an das Ende setzen, woraus man die gesuchte Periode 631578947368421052 erhält. — Ebenso leicht hätte man den Anfang der Periode aus den beiden ersten Ziffern 63 gefunden.

Wenn man die Periode des Bruches $\frac{45}{53}$ haben will, so ist, für den Modul 53, $\text{ind. } 45 = 2 \text{ ind. } 3 + \text{ind. } 5 = 49$; die Anzahl der Perioden ist hier

$4 = f$ und $49 = 12f + 1$; daher sind in der mit (1) bezeichneten Periode die 12 ersten Ziffern hinter die übrigen zu setzen, und die gesuchte Periode ist 8490566037735. Die Anfangsziffern 84 sind in diesem Falle in der Tafel von einander getrennt.

Wir bemerken noch, dass man mit Hülfe der Tafel III auch eine Zahl finden kann, welche für einen gegebenen Modul (der in ihr unter dem Namen Nenner enthalten ist) einem gegebenen Index entspricht, was zu zeigen wir schon im Artikel 59 versprochen haben. Denn offenbar kann man nach dem Vorhergehenden die Periode eines Bruches finden, dessen Zähler (auch wenn er unbekannt ist) der gegebene Index entspricht; es reicht jedoch hin, soviel Anfangsziffern dieser Periode aus der Tafel zu entnehmen, als der Nenner Ziffern hat; aus jenen leitet man dann nach Artikel 313 den Zähler oder die gesuchte dem gegebenen Index entsprechende Zahl her.

317.

Nach dem Vorhergehenden kann die Mantisse eines jeden Bruches, dessen Nenner eine Primzahl oder eine Potenz einer Primzahl innerhalb der Grenzen der Tafel ist, auf beliebig viele Ziffern ohne Rechnung abgeleitet werden; aber vermöge der Untersuchungen im Anfange dieses Abschnittes erstreckt sich die Anwendung der Tafel noch viel weiter und umfasst sämtliche Brüche, deren Nenner Producte aus Primzahlen oder Potenzen von Primzahlen innerhalb ihrer Grenzen sind. Denn da ein solcher Bruch in solche zerlegt werden kann, deren Nenner diese Factoren sind, und man diese in Decimalbrüche bis auf beliebig viele Stellen verwandeln kann, so bleibt nur übrig, die letzteren zu einer Summe zu vereinigen. Übrigens wird es kaum nötig sein, darauf hinzuweisen, dass die letzte Ziffer dieser Summe kleiner als die richtige werden kann; offenbar kann aber der Unterschied nicht auf soviele Einheiten ansteigen, als Teilbrüche addiert werden, so dass es also gut sein wird, diese auf einige Stellen weiter zu berechnen, als der gegebene Bruch richtig werden soll. Beispielshalber betrachten wir den Bruch $\frac{6099380351}{1271808720} = F$*), dessen Nenner das Product aus den Zahlen 16, 9, 5, 49, 13, 47, 59 ist. Nach den oben angegebenen Principien findet man $F = 1 + \frac{11}{16} + \frac{4}{9} + \frac{4}{5} + \frac{22}{49} + \frac{5}{13} + \frac{7}{47} + \frac{52}{59}$, und diese Teilbrüche werden in folgender Weise in Decimalbrüche verwandelt:

*) Dieser Bruch ist einer von denen, welche der Quadratwurzel aus 23 möglichst nahe kommen, und zwar ist der Unterschied kleiner als 7 Einheiten in der zwanzigsten Decimalstelle.

$$
\begin{array}{lll}
1 = 1 & & \\
\frac{11}{16} = 0{,}6875 & & \\
\frac{4}{5} = 0{,}8 & & \\
\frac{4}{9} = 0{,}4444444444 & 4444444444 & 44 \\
\frac{22}{49} = 0{,}4489795918 & 3673469387 & 75 \\
\frac{5}{13} = 0{,}3846153846 & 1538461538 & 46 \\
\frac{7}{47} = 0{,}1489361702 & 1276595744 & 68 \\
\frac{52}{59} = 0{,}8813559322 & 0338983050 & 84 \\
\hline
F = 4{,}7958315233 & 1271954166 & 17
\end{array}
$$

Der Unterschied dieser Summe von dem richtigen Werte ist sicher kleiner als fünf Einheiten in der letzten zweiundzwanzigsten Decimalstelle, so dass dadurch die zwanzig ersten nicht geändert werden können. Führt man die Rechnung auf noch mehr Decimalstellen weiter, so ergeben sich für die beiden letzten Ziffern 17 die folgenden 1893936...

Übrigens wird jeder, auch ohne dass wir besonders darauf hinweisen, einsehen, dass diese Methode, gemeine Brüche in Decimalbrüche zu verwandeln, besonders für denjenigen Fall berechnet ist, wo man viele Decimalstellen haben will; denn wenn wenige genügen, kann die gewöhnliche Division oder die Rechnung mit Logarithmen meistens ebenso bequem angewendet werden.

318.

Da somit die Verwandlung solcher Brüche, deren Nenner aus mehreren verschiedenen Primzahlen zusammengesetzt sind, bereits auf denjenigen Fall zurückgeführt ist, wo der Nenner eine Primzahl oder eine Potenz einer Primzahl ist, so wollen wir nur noch Einiges über die Mantissen jener hinzufügen. Wenn der Nenner den Factor 2 oder 5 nicht enthält, so wird die Mantisse auch hier aus Perioden bestehen, da man auch für diesen Fall in der Reihe 10, 100, 1000,... schliesslich zu einem Gliede gelangt, welches der Einheit nach diesem Nenner congruent ist, und zugleich wird der Exponent dieses Gliedes, welcher nach Artikel 92 leicht bestimmt werden kann, die von dem Zähler nicht abhängende Grösse der Periode anzeigen, wofern der Zähler prim zum Nenner ist. — Ist aber der Nenner von der Form $2^\alpha 5^\beta N$, wo N eine zu 10 prime Zahl ist und α, β Zahlen bezeichnen, von denen wenigstens eine nicht gleich 0 ist, so wird die Mantisse des Bruches

erst nach den ersten α oder β Ziffern (je nachdem α oder β grösser ist) nur noch aus lauter Perioden bestehen, welche mit den Perioden der Brüche, deren Nenner N ist, hinsichtlich ihrer Länge übereinstimmen. Dies leitet man leicht daraus her, dass jener Bruch in zwei andere mit den Nennern $2^\alpha 5^\beta$ und N zerlegbar ist, von denen der erstere nach den ersten α oder β Ziffern abbricht. — Übrigens könnten wir über diesen Gegenstand noch viele andere Bemerkungen hinzufügen, besonders in Bezug auf die Kunstgriffe, welche man anwenden kann, um eine solche Tafel wie III möglichst schnell zu construieren; doch unterdrücken wir dies an dieser Stelle der Kürze wegen um so lieber, da mehreres hierher gehörige sowohl von Robertson a. a. O., als auch von Bernoulli (*Nouv. Mém. de l'Ac. de Berlin 1771, p. 273*) bereits angegeben worden ist.

Auflösung der Congruenz $x^2 \equiv A$ durch die Methode der Ausschliessung.

319.

Die Möglichkeit der Congruenz $x^2 \equiv A$ (mod. m), welche mit der unbestimmten Gleichung $x^2 = A + my$ übereinstimmt, haben wir im Abschnitt IV (Artikel 146) in einer Weise behandelt, dass nichts mehr zu wünschen übrig bleiben dürfte; hinsichtlich der Ermittlung der Unbekannten selbst aber haben wir schon oben (Artikel 152) bemerkt, dass indirecte Methoden den directen bei Weitem vorzuziehen seien. Ist m eine Primzahl (auf welchen Fall die übrigen leicht zurückgeführt werden können), so könnten wir zu diesem Zwecke die Tafel I der Indices (nach der Bemerkung im Artikel 316 in Verbindung mit Tafel III) benutzen, wie wir im Artikel 60 allgemeiner gezeigt haben; doch würde dieses Verfahren auf die Grenzen der Tafel beschränkt sein. Aus diesen Gründen wird hoffentlich die folgende allgemeine und bequeme Methode den Liebhabern der Arithmetik nicht unerwünscht sein.

Vor Allem bemerken wir, dass es genügt, wenn man nur diejenigen Werte von x hat, welche positiv und nicht grösser als $\frac{1}{2}m$ sind, da jeder andere irgend einem von diesen Werten selbst oder einem mit negativen Vorzeichen genommenen nach dem Modul m congruent ist; für einen solchen Wert von x aber wird der Wert von y notwendig zwischen den Grenzen $-\frac{A}{m}$ und $\frac{1}{4}m - \frac{A}{m}$ enthalten sein. Die Methode, welche sich unmittelbar darbietet, würde also darin bestehen, dass man für die einzelnen innerhalb dieser Grenzen liegenden Werte von y, deren Gesamtheit wir mit Ω bezeichnen, den Wert von $A + my$, den wir mit V bezeichnen, berechnet und nur diejenigen beibehält, für welche V ein Quadrat wird. Ist m eine kleine Zahl (z. B. unterhalb 40 gelegen), so ist dieser Versuch so kurz, dass er

einer Zusammenziehung kaum bedarf; wenn aber m gross ist, so kann die Arbeit durch die folgende Methode der Ausschliessung, soweit man will, abgekürzt werden.

320.

Es sei E eine beliebige ganze Zahl, welche prim zu m und grösser als 2 ist; ferner seien alle ihre verschiedenen (d. h. nach E incongruenten) quadratischen Reste: $a, b, c, \ldots$; endlich die Wurzeln der Congruenzen

$$A + my \equiv a, \quad A + my \equiv b, \quad A + my \equiv c, \ldots \pmod{E}$$

gleich $\alpha, \beta, \gamma, \ldots$ respective, die wir sämtlich positiv und kleiner als E annehmen dürfen. Wenn man nun y einen Wert beilegt, der irgend einer von den Zahlen $\alpha, \beta, \gamma, \ldots$ nach dem Modul E congruent ist, so wird der daraus entstehende Wert von $V = A + my$ irgend einer der Zahlen $a, b, c, \ldots$ congruent und somit Nichtrest von E sein; mithin kann er kein Quadrat sein. Hieraus geht hervor, dass aus Ω sogleich alle Zahlen als untauglich ausgeschlossen werden können, welche unter den Formen $Et + \alpha$, $Et + \beta$, $Et + \gamma, \ldots$ enthalten sind, und es wird genügen, den Versuch mit den übrigen, deren Complex Ω' sei, anzustellen. Bei jener Operation kann man der Zahl E den Namen **Exkludent** geben.

Nimmt man aber als Exkludenten eine andere passende Zahl E', so findet man auf ganz dieselbe Weise soviel Zahlen $\alpha', \beta', \gamma', \ldots$, als man verschiedene quadratische Nichtreste hat, denen y nach dem Modul E' nicht congruent sein kann. Daher kann man wiederum aus Ω' alle unter den Formen $E't + \alpha'$, $E't + \beta'$, $E't + \gamma', \ldots$ enthaltenen Zahlen weglassen. Auf diese Weise kann man fortfahren, indem man immer andere und andere Exkludenten anwendet, bis die Anzahl der Zahlen in Ω soweit verringert ist, dass es nicht schwieriger erscheint, mit allen übrigbleibenden den Versuch wirklich anzustellen, als neue Ausschliessungen vorzunehmen.

Beispiel. Ist die Gleichung $x^2 = 22 + 97y$ gegeben, so sind die Grenzen der Werte von y gleich $-\frac{22}{97}$ und $24\frac{1}{4} - \frac{22}{97}$, so dass (da die Untauglichkeit von 0 unmittelbar klar ist) Ω die Zahlen 1, 2, 3, ..., 24 umfasst. Für $E = 3$ erhält man den einzigen Nichtrest $a = 2$; hieraus wird $\alpha = 1$; daher sind aus Ω alle Zahlen von der Form $3t + 1$ auszuschliessen; die Anzahl der übrigbleibenden Ω' ist 16. Ebenso erhält man für $E = 4$: $a = 2$, $b = 3$, woraus $\alpha = 0$, $\beta = 1$ wird; demnach sind alle Zahlen von der Form $4t$ und $4t + 1$ wegzulassen, und es bleiben die folgenden acht: 2, 3, 6, 11, 14, 15, 18, 23. Ebenso findet man für $E = 5$, dass die Zahlen von den Formen $5t$ und $5t + 3$ auszuschliessen sind; es bleiben also die folgenden: 2, 6, 11, 14. Der Exkludent 6 würde die Zahlen von den Formen $6t + 1$ und $6t + 4$ beseitigen; diese aber (welche mit den Zahlen von der Form $3t + 1$ übereinstimmen) sind schon weggelassen. Der Exkludent 7 beseitigt die Zahlen

von den Formen $7t+2, 7t+3, 7t+5$ und lässt die folgenden übrig: 6, 11, 14. Substituiert man diese für y, so ergiebt sich $V = 604, 1089, 1380$, von denen nnr der zweite Wert ein Quadrat ist. Aus diesem wird $x = \pm 33$.

321.

Da die mit dem Exkludenten E angestellte Operation von den Werten von V, welche den Werten von y in Ω entsprechen, alle diejenigen ausschliesst, welche quadratische Nichtreste von E sind, die Reste derselben Zahl aber unberührt lässt, so sieht man leicht, dass sich die Anwendung von E und $2E$ in nichts unterscheidet, wenn E ungerade ist, da in diesem Falle E und $2E$ dieselben Reste und Nichtreste haben. Hieraus geht hervor, dass, wenn man der Reihe nach die Zahlen 3, 5, 7, ... als Exkludenten anwendet, die ungerademal geraden Zahlen 6, 10, 14, ... als unnütz übergangen werden müssen. Ferner ist ersichtlich, dass die doppelte mit den Exkludenten E, E' angestellte Operation alle diejenigen Werte von V beseitigt, welche Nichtreste entweder jeder der beiden Zahlen E, E' oder nur einer von ihnen sind, während diejenigen, welche Reste von beiden sind, zurückbleiben. Da nun in dem Falle, wo E und E' keinen gemeinschaftlichen Teiler haben, jene weggeworfenen Zahlen sämtlich Nichtreste und diese übrig bleibenden Reste des Products EE' sind, so ist klar, dass die Anwendung des Exkludenten EE' in diesem Falle ganz dasselbe bewirkt, wie die Anwendung von E und E', und dass somit jene nach dieser überflüssig wird. Daher kann man auch alle diejenigen Exkludenten übergehen, welche in zwei zu einander prime Factoren zerlegt werden können, und es reicht aus, diejenigen zu benützen, welche entweder (in m nicht aufgehende) Primzahlen oder Potenzen von Primzahlen sind. Endlich ist klar, dass nach der Anwendung des Exkludenten p^μ, welcher eine Potenz einer Primzahl p ist, der Exkludent p oder p^ν, falls $\nu < \mu$ ist, überflüssig wird; denn da p^μ unter den Werten von V nur Reste von sich übrig lässt, so werden um so weniger Nichtreste von p oder irgend einer niedrigeren Potenz p^ν noch vorhanden sein. Ist aber p oder p^ν schon vor p^μ angewendet worden, so kann dieses offenbar nur solche Werte von V beseitigen, welche gleichzeitig Reste von p (oder p^ν) und Nichtreste von p^μ sind; daher wird es ausreichen, nur solche Nichtreste von p^μ für $a, b, c, \ldots$ zu nehmen.

322.

Die Berechnung der Zahlen $\alpha, \beta, \gamma, \ldots$, welche irgend einem gegebenen Exkludenten E entsprechen, wird durch die folgenden Bemerkungen erheblich zusammengezogen. Es seien $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ die Wurzeln der Congruenzen $my \equiv a$, $my \equiv b$, $my \equiv c, \ldots$ (mod. E) und k die Wurzel der Congruenz $my \equiv -A$, so wird offenbar $\alpha \equiv \mathfrak{A} + k$, $\beta \equiv \mathfrak{B} + k$, $\gamma \equiv \mathfrak{C} + k, \ldots$. Wenn wir nun $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ wirklich durch Auflösung jener Congruenzen ermitteln müssten, so würde dieser Weg, die Zahlen $\alpha, \beta, \gamma, \ldots$ zu finden,

jedenfalls um nichts kürzer sein, als der, welchen wir oben gezeigt haben; doch ist jenes keineswegs notwendig. Wenn nämlich zunächst E eine Primzahl und m quadratischer Rest von E ist, so geht aus Artikel 98 hervor, dass $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ..., welches die Werte der Ausdrücke $\frac{a}{m}$, $\frac{b}{m}$, $\frac{c}{m}$, ... (mod. E) sind, verschiedene Nichtreste von E werden und daher mit α, β, γ, ... vollständig übereinstimmen, abgesehen von ihrer Reihenfolge, auf die hier nichts ankommt; wenn dagegen unter derselben Voraussetzung m Nichtrest von E ist, so werden die Zahlen $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... mit sämtlichen quadratischen Resten nach Weglassung der 0 übereinstimmen. — Ist E das Quadrat einer (ungeraden) Primzahl, etwa gleich p^2, und ist schon p als Exkludent benutzt, so reicht es nach dem vorigen Artikel aus, für a, b, c, ... diejenigen Nichtreste von p^2 zu nehmen, welche Reste von p sind, d. h. die Zahlen p, $2p$, $3p$, ..., p^2-p (nämlich alle Zahlen unterhalb p^2, ausser 0, welche durch p teilbar sind); hieraus aber ist leicht ersichtlich, dass für $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... ganz dieselben Zahlen, nur in anderer Reihenfolge, hervorgehen müssen. Analog wird es, wenn nach der Anwendung der Exkludenten p und p^2 $E=p^3$ gesetzt wird, ausreichen, für a, b, c, ... die Producte der einzelnen Nichtreste von p mit p^2 zu nehmen, wodurch für $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... entweder dieselben Zahlen, oder die Producte von p^2 in die einzelnen Reste von p ausser 0 hervorgehen werden, je nachdem m Rest oder Nichtrest von p ist. Allgemein nimmt man für E eine beliebige Potenz einer Primzahl, etwa p^μ, nachdem alle niedrigeren Potenzen bereits angewendet worden sind, so wird man für $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... die Producte von $p^{\mu-1}$ entweder in sämtliche Zahlen, die kleiner als p sind, (0 immer ausgeschlossen), falls μ gerade ist, oder in alle unterhalb p liegende Nichtreste von p, falls μ ungerade und mRp ist, oder in alle Reste, falls mNp ist, erhalten. — Ist $E=4$ und daher $a=2$, $b=3$, so erhalten wir für $\mathfrak{A}$, $\mathfrak{B}$ entweder 2 und 3 oder 2 und 1, je nachdem $m\equiv 1$ oder $\equiv 3$ (mod. 4) ist. Wenn nach Anwendung des Exkludenten 4 $E=8$ gesetzt wird, so haben wir $\alpha=5$, woraus $\mathfrak{A}$ gleich 5, 7, 1, 3 wird, je nachdem $m\equiv 1$, 3, 5, 7 (mod. 8) ist. Allgemein aber, wenn E eine beliebig höhere Potenz von 2 etwa 2^μ ist, so muss man, nachdem die niedrigeren Potenzen von 2 bereits angewendet sind, $a=2^{\mu-1}$, $b=3\cdot 2^{\mu-2}$ setzen, wenn μ gerade ist, woraus $\mathfrak{A}=2^{\mu-1}$, $\mathfrak{B}=3\cdot 2^{\mu-2}$ oder $=2^{\mu-2}$ wird, je nachdem $m\equiv 1$ oder $\equiv 3$ ist; ist aber μ ungerade, so muss man $a=5\cdot 2^{\mu-3}$ setzen, wonach $\mathfrak{A}$ gleich dem Producte der Zahl $2^{\mu-3}$ in eine der Zahlen 5, 7, 1 oder 3 wird, je nachdem $m\equiv 1$, 3, 5, oder 7 (mod. 8) ist.

Übrigens werden Kundige sich leicht einen Apparat ersinnen, durch welchen die untauglichen Werte von y aus Ω mechanisch entfernt werden können, nachdem für so viele Exkludenten, als nötig erscheinen, die Zahlen α, β, γ, ... berechnet sind; doch können wir hierüber wie über andere Kunstgriffe, um die Arbeit abzukürzen, an dieser Stelle nicht handeln.

Lösung der unbestimmten Gleichung $mx^2 + ny^2 = A$ nach der Ausschliessungsmethode.

323.

Wir haben im Abschnitt V gezeigt, wie man sämtliche Darstellungen einer gegebenen Zahl A durch die binäre Form $mx^2 + ny^2$ oder die Lösungen der unbestimmten Gleichung $mx^2 + ny^2 = A$ nach einer allgemeinen Methode findet, die an Kürze nichts zu wünschen übrig lassen dürfte, wenn man bereits sämtliche Werte des Ausdrucks $\sqrt{-mn}$ nach dem Modul A selbst und nach dem durch seine quadratischen Factoren geteilten Modul hat; hier werden wir aber für denjenigen Fall, wo mn positiv ist, eine Auflösung darlegen, die viel bequemer ist als die directe, wenn man für diese jene Werte erst vorher berechnen muss. Wir werden aber annehmen, dass die Zahlen m, n und A positiv und prim zu einander sind, da die übrigen Fälle auf diesen leicht zurückgeführt werden können. Offenbar genügt es auch, nur positive Werte von x, y zu suchen, da die übrigen aus diesen durch blosse Aenderung der Vorzeichen erhalten werden.

Es ist klar, dass x so beschaffen sein muss, dass $\frac{A - mx^2}{n}$, für welchen Bruch wir kurz V schreiben werden, positiv, ganz und eine Quadratzahl werde. Die erste Bedingung erfordert, dass x nicht grösser sei als $\sqrt{\frac{A}{m}}$; die zweite findet bereits von selbst statt, wenn $n = 1$, sonst erfordert sie, dass der Wert des Ausdrucks $\frac{A}{m}$ (mod. n) quadratischer Rest von n sei; und bezeichnet man sämtliche verschiedene Werte des Ausdrucks $\sqrt{\frac{A}{m}}$ (mod. n) mit $\pm r$, $\pm r'$, ..., so müssen die Werte von x unter einer der Formen $nt + r$, $nt - r$, $nt + r'$, ... enthalten sein. Es würde daher das einfachste sein, alle unterhalb der Grenze $\sqrt{\frac{A}{m}}$ liegenden Zahlen dieser Formen, deren Complex wir mit Ω bezeichnen, für x zu substituieren und nur diejenigen beizubehalten, für welche V ein Quadrat wird. Wir werden im folgenden Artikel zeigen, wie man dieses heuristische Verfahren, soweit man will, zusammenziehen kann.

324.

Die Methode der Ausschliessungen, nach welchen wir dies bewirken werden, besteht ebenso wie in der vorigen Untersuchung darin, dass man mehrere Zahlen, die wir auch hier Exkludenten nennen, nach Belieben annimmt, sodann untersucht, für welche Werte von x der Wert von V quadratischer Nichtrest von diesen Exkludenten wird, und derartige x aus Ω wegwirft. Durch eine Schlussreihe, die derjenigen, welche wir im Art. 321

auseinandergesetzt haben, vollkommen analog ist, geht hervor, dass nur solche Exkludenten anzuwenden sind, welche Primzahlen oder Potenzen von Primzahlen sind, und für einen Exkludenten der letzteren Art nur diejenigen Nichtreste desselben aus den Werten von V wegzulassen sind, welche Reste sämtlicher niederen Potenzen derselben Primzahl sind, wofern die Ausschliessung mit diesen bereits durchgeführt ist.

Es sei daher der Exkludent $E = p^\mu$ (einschliesslich desjenigen Falles, wo $\mu = 1$ ist), wo p eine in m nicht aufgehende Primzahl ist, und es werde angenommen*), dass p^ν die höchste Potenz derselben Primzahl sei, durch welche n teilbar ist. Es seien ferner $a, b, c, \ldots$ quadratische Nichtreste von E (und zwar sämtliche, wenn $\mu = 1$, die notwendigen oder diejenigen, welche Reste der niedrigeren Potenzen sind, wenn $\mu > 1$ ist). Berechnet man die Wurzeln der Congruenzen $mz \equiv A - na$, $mz \equiv A - nb$, $mz \equiv A - nc$, $\ldots$ (mod. $Ep^\nu = p^{\mu+\nu}$), welche $\alpha, \beta, \gamma, \ldots$ sein mögen, so ergiebt sich leicht, dass, wenn für irgend einen Wert von x $x^2 \equiv \alpha$ (mod. Ep^ν) wird, der entsprechende Wert von $V \equiv a$ (mod. E) oder Nichtrest von E wird, und ebenso in Bezug auf die übrigen Zahlen $\beta, \gamma, \ldots$ Ebenso leicht ist umgekehrt ersichtlich, dass, wenn irgend ein Wert von x die Congruenz $V \equiv a$ (mod. E) zu Stande bringt, für ebendenselben $x^2 \equiv \alpha$ (mod. Ep^ν) ist, und dass somit sämtliche Werte von x, für welche x^2 keiner der Zahlen $\alpha, \beta, \gamma, \ldots$ nach dem Modul Ep^ν congruent ist, solche Werte von V hervorbringen, welche keiner der Zahlen, $a, b, c, \ldots$ nach dem Modul E congruent sind. Man wähle nun aus den Zahlen $\alpha, \beta, \gamma, \ldots$ sämtliche quadratischen Reste von Ep^ν, welche $g, g', g'', \ldots$ sein mögen, aus, berechne die Werte der Ausdrücke $\sqrt{g}$, $\sqrt{g'}$, $\sqrt{g''}$, $\ldots$ (mod. Ep^ν) und nehme an, dass sich hieraus die Werte $\pm h$, $\pm h'$, $\pm h''$, $\ldots$ ergeben. Wenn dies in dieser Weise geschehen, so ist klar, dass sämtliche Zahlen von den Formen $Ep^\nu t \pm h$, $Ep^\nu t \pm h'$, $Ep^\nu t \pm h''$, $\ldots$ sicher aus Ω weggelassen werden können, und dass keinem nach dieser Ausschliessung in Ω noch verbleibenden Werte von x ein Wert von V entsprechen kann, der unter den Formen $Eu + a$, $Eu + b$, $Eu + c$, $\ldots$ enthalten ist. Übrigens werden offenbar solche Werte von V schon an und für sich aus keinem Werte von x hervorgehen können, wenn sich unter den Zahlen $\alpha, \beta, \gamma, \ldots$ keine quadratischen Reste von Ep^ν vorfinden, und daher kann in diesem Falle die Zahl E als Exkludent nicht angewendet werden. — Derartige Exkludenten kann man so viele, als man will, anwenden, und daher können auf diese Weise die Zahlen in Ω nach Belieben verringert werden.

Wir wollen nun zusehen, ob man nicht auch Primzahlen, welche in m aufgehen; oder Potenzen solcher Primzahlen als Exkludenten benutzen kann. Ist B der Wert des Ausdrucks $\frac{A}{n}$ (mod. m), so ergiebt sich, dass

*) Der Kürze wegen fassen wir die beiden Fälle, in denen n durch p teilbar und nicht teilbar ist, zusammen; im letzteren muss man $\nu = 0$ setzen.

V stets B nach dem Modul m congruent wird, welcher Wert auch für x genommen werden möge, und dass somit zur Möglichkeit der gegebenen Gleichung notwendig erforderlich ist, dass B quadratischer Rest von m ist. Bezeichnet daher p irgend einen ungeraden Primteiler von m, welcher nach Voraussetzung in n und A und somit auch in B nicht aufgeht, so ist V für jeden beliebigen Wert von x Rest von p und daher auch von jeder beliebigen Potenz von p; mithin können p und seine Potenzen nicht als Exkludenten genommen werden. — Aus ganz analogem Grunde ist, wenn m durch 8 teilbar ist, zur Möglichkeit der gegebenen Gleichung notwendig erforderlich, dass $B \equiv 1 \pmod 8$ sei, weshalb auch für jeden beliebigen Wert von x: $V \equiv 1 \pmod 8$ wird und somit die Potenzen von 2 als Exkludenten nicht geeignet sind. — Wenn aber m durch 4 jedoch nicht durch 8 teilbar ist, so muss aus ähnlichem Grunde $B \equiv 1 \pmod 4$ und der Wert des Ausdrucks $\frac{A}{n} \pmod 8$ entweder 1 oder 5 sein; derselbe möge mit C bezeichnet werden. Man sieht ohne Schwierigkeit, dass für einen geraden Wert von x hier $V \equiv C$, für einen ungeraden $V \equiv C + 4 \pmod 8$ wird, woraus hervorgeht, dass die geraden Werte zu verwerfen sind, wenn $C = 5$, die ungeraden, wenn $C = 1$ ist. — Ist endlich m durch 2 aber nicht durch 4 teilbar, so sei wie vorher C der Wert des Ausdrucks $\frac{A}{n} \pmod 8$, welcher gleich 1, 3, 5 oder 7 ist, und D der Wert von $\frac{\frac{1}{2}m}{n} \pmod 4$, welcher gleich 1 oder 3 ist. Da nun der Wert von V offenbar immer $\equiv C - 2Dx^2 \pmod 8$ und daher für ein gerades $x: \equiv C$, für ein ungerades $\equiv C - 2D$ ist, so folgert man hieraus leicht, dass alle ungeraden Werte von x zu verwerfen sind, wenn $C = 1$, alle geraden, wenn $C = 3$ und $D = 1$ oder $C = 7$ und $D = 3$ ist, und dass für alle übrigbleibenden Werte $V \equiv 1 \pmod 8$ oder also Rest einer jeden Potenz von 2 ist; in den übrigen Fällen aber, nämlich wenn $C = 5$ oder $C = 3$ und $D = 3$ oder $C = 7$ und $D = 1$ ist, wird $V \equiv 3$, 5 oder 7 (mod. 8), mag x gerade oder ungerade genommen werden, woraus erhellt, dass in diesen Fällen die gegebene Gleichung überhaupt keine Lösung besitzt.

Da wir übrigens auf ganz ähnliche Weise, wie wir hier den Wert von x durch Ausschliessungen finden lehrten, auch, mit den notwendigen Änderungen, den Wert von y hätten ableiten können, so kann man die Methode der Ausschliessung auf die Lösung des vorgelegten Problems stets auf zweierlei Art anwenden (falls nicht $m = n = 1$ ist, wo beide Arten zusammenfallen), von denen in den meisten Fällen diejenige vorzuziehen ist, für welche Ω eine kleinere Anzahl von Gliedern enthält, was sich leicht von vornherein abschätzen lässt. — Schliesslich wird es kaum nötig sein zu bemerken, dass, wenn nach einigen Ausschliessungen sämtliche Zahlen aus Ω herausgefallen sind, dies als ein sicheres Zeichen für die Unmöglichkeit der gegebenen Gleichung zu betrachten ist.

325.

Beispiel. Es sei gegeben die Gleichung $3x^2 + 455y^2 = 10857362$, die wir auf doppelte Weise lösen wollen, zuerst dadurch, dass wir die Werte von x, sodann dadurch, dass wir die Werte von y suchen. — Die Grenze jener ist in diesem Falle $\sqrt{3619120\frac{2}{3}}$, welche zwischen 1902 und 1903 fällt; der Wert des Ausdrucks $\frac{A}{3}$ (mod. 455) ist 354, und die Werte des Ausdrucks $\sqrt{354}$ (mod. 455) sind ± 82, ± 152, ± 173, ± 212. Hiernach besteht Ω aus den folgenden 33 Zahlen: 82, 152, 173, 212, 243, 282, 303, 373, 537, 607, 628, 667, 698, 737, 758, 828, 992, 1062, 1083, 1122, 1153, 1192, 1213, 1283, 1447, 1517, 1538, 1577, 1608, 1647, 1668, 1738, 1902. Die Zahl 3 kann in diesem Falle nicht als Exkludent genommen werden, da sie in m aufgeht. Für den Exkludenten 4 hat man $a = 2$, $b = 3$, woraus $\alpha = 0$, $\beta = 3$; $g = 0$ und als Werte des Ausdrucks $\sqrt{g}$ (mod. 4) die folgenden: 0 und 2; hieraus folgt, dass alle Zahlen von den Formen $4t$ und $4t + 2$, d. h. alle geraden Zahlen aus Ω wegzulassen sind; die (sechzehn) übrigen mögen mit Ω' bezeichnet werden. Für $E = 5$, welche Zahl auch in n aufgeht, erhalten wir als Wurzeln der Congruenzen $mz \equiv A - 2n$ und $mz \equiv A - 3n$ (mod. 25) die Werte 9 und 24, welche beide Reste von 25 sind, und die Werte der Ausdrücke $\sqrt{9}$ und $\sqrt{24}$ (mod. 25) werden ± 3, ± 7; lässt man aus Ω' sämtliche Zahlen von den Formen $25t \pm 3$, $25t \pm 7$ weg, so bleiben die folgenden zehn (Ω''): 173, 373, 537, 667, 737, 1083, 1213, 1283, 1517, 1577. Für $E = 7$ hat man als Wurzeln der Congruenzen $mz \equiv A - 3n$, $mz \equiv A - 5n$, $mz \equiv A - 6n$ (mod. 49) die Werte 32, 39, 18, welche sämtlich Reste von 49 sind, und als Werte der Ausdrücke $\sqrt{32}$, $\sqrt{39}$, $\sqrt{18}$ (mod. 49) die folgenden: ± 9, ± 23, ± 19; lässt man aus Ω'' die Zahlen von den Formen $49t \pm 9$, $49t \pm 23$, $49t \pm 19$ weg, so bleiben die folgenden fünf (Ω'''): 537, 737, 1083, 1213, 1517. Für $E = 8$ erhält man $a = 5$, somit $\alpha = 5$, welches Nichtrest von 8 ist; daher lässt sich der Exkludent 8 nicht anwenden. Die Zahl 9 ist aus demselben Grunde zu übergehen wie 3. Für $E = 11$ werden die Zahlen a, b, ... respective 2, 6, 7, 8, 10, ferner $\nu = 0$, somit die Zahlen α, β, ... $= 8$, 10, 5, 0, 1, von denen nur drei Reste von 11 sind, nämlich 0, 1, 5; hieraus ergiebt sich, dass aus Ω''' die Zahlen von den Formen $11t$, $11t \pm 1$, $11t \pm 5$ wegzulassen sind, so dass nur noch 537, 1083, 1213 übrig bleiben. Stellt man mit diesen die Probe an, so ergeben sich für V die Werte 21961, 16129, 14161 respective, von denen nur der zweite und dritte Quadrate sind. Daher besitzt die gegebene Gleichung zwei Lösungen durch positive Werte von x, y, nämlich $x = 1083$, $y = 127$ und $x = 1213$, $y = 119$.

Zweitens. Wenn man die andere der beiden Unbekannten derselben Gleichung durch Ausschliessungen ermitteln will, so setze man diese Gleichung unter die Form $455x^2 + 3y^2 = 10857362$, indem man x mit y

vertauscht, um sämtliche Bezeichnungen der Artikel 323, 324 beibehalten zu können. Die Grenze der Werte von x fällt hier zwischen 154 und 155; der Wert von $\frac{A}{m} \pmod{n}$ ist 1, die Werte von $\sqrt{1} \pmod{3}$ sind $+1$ und -1. Daher enthält Ω alle Zahlen von den Formen $3t+1$ und $3t-1$, d. h. alle durch 3 nicht teilbaren Zahlen bis zu 154 einschliesslich, deren Anzahl gleich 103 ist; wendet man aber die oben gegebenen Prinzipien an, so findet man, dass für die Exkludenten 3; 4; 9; 11; 17; 19; 23 auszuschliessen sind die Zahlen von den Formen: $9t \pm 4$; $4t$, $4t \pm 2$ oder alle geraden Zahlen; $27t \pm 1$, $27t \pm 10$; $11t$, $11t \pm 1$, $11t \pm 3$; $17t \pm 3$, $17t \pm 4$, $17t \pm 5$, $17t \pm 7$; $19t \pm 2$, $19t \pm 3$, $19t \pm 8$, $19t \pm 9$; $23t$, $23t \pm 1$, $23t \pm 5$, $23t \pm 7$, $23t \pm 9$, $23t \pm 10$. Werden diese weggelassen, so bleiben übrig: 119, 227, welche beide für V ein Quadrat und dieselben Lösungen ergeben, zu denen wir oben gelangt waren.

326.

Die vorstehend angegebene Methode ist schon an und für sich so bequem. dass sie kaum etwas zu wünschen übrig lässt; trotzdem kann sie noch durch mannigfache Kunstgriffe, von denen wir hier nur einige kurz berühren können, erheblich zusammengezogen werden. Wir beschränken unsere Untersuchung auf denjenigen Fall, wo der Exkludent eine ungerade in A nicht aufgehende Primzahl oder eine Potenz einer solchen Primzahl ist, zumal da die übrigen Fälle entweder auf diesen zurückgeführt oder nach einer analogen Methode behandelt werden können. Nimmt man zunächst an, dass der Exkludent $E = p$ eine in m, n nicht aufgehende Primzahl sei, und dass die Werte der Ausdrücke $\frac{A}{m}, -\frac{na}{m}, -\frac{nb}{m}, -\frac{nc}{m}, \ldots$ $(\mathrm{mod.}\, p)$ respective $k, \mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ seien, so findet man die Zahlen $\alpha, \beta, \gamma, \ldots$ mit Hülfe der Congruenzen: $\alpha \equiv k + \mathfrak{A}$, $\beta \equiv k + \mathfrak{B}$, $\gamma \equiv k + \mathfrak{C}, \ldots \pmod{p}$. Die Zahlen $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$ können aber durch einen Kunstgriff, der dem im Artikel 322 benutzten ganz ähnlich ist, ohne Auflösung der Congruenzen ermittelt werden, und werden entweder mit sämtlichen Nichtresten oder mit sämtlichen Resten von p (ausser 0) übereinstimmen, je nachdem der Wert des Ausdrucks $-\frac{m}{n} \pmod{p}$ oder (was hier auf dasselbe hinauskommt) die Zahl $-mn$ Rest oder Nichtrest von p ist.. So wird in dem Beispiel II des vorigen Artikels für $E = 17$: $k = 7$; $-mn = -1365 \equiv 12$ ist Nichtrest von 17; daher sind die Zahlen $\mathfrak{A}, \mathfrak{B}, \ldots$ respective 1, 2, 4, 8, 9, 13, 15, 16 und daher die Zahlen $\alpha, \beta, \ldots$ respective 8, 9, 11, 15, 16, 3, 5, 6; von diesen sind 8, 9, 11, 15, 16 Reste; somit werden $\pm h, h', \ldots$ hier: $\pm 5, 3, 7, 4$. — Diejenigen, welche öfters Gelegenheit haben, derartige Probleme zu lösen, werden sich die Sache erheblich erleichtern, wenn sie für mehrere Primzahlen p die Werte von $h, h', \ldots$, welche den einzelnen Werten von $k (1, 2, 3, \ldots, p-1)$ entsprechen, unter jeder der beiden Annahmen (nämlich dass $-mn$ Rest

oder Nichtrest von p sei) berechnen. Übrigens bemerken wir noch, dass die Anzahl der Zahlen $h, -h, h', \ldots$ stets gleich $\frac{1}{2}(p-1)$, wenn jede der beiden Zahlen k und $-mn$ Rest oder jede Nichtrest von p ist; ferner gleich $\frac{1}{2}(p-3)$, wenn die erste Rest, die zweite Nichtrest, und gleich $\frac{1}{2}(p+1)$ ist, wenn die erste Nichtrest, die zweite Rest ist; doch müssen wir den Beweis dieses Satzes, um nicht zu weitläufig zu werden, unterdrücken.

Was aber zweitens diejenigen Fälle betrifft, wo E eine in n aufgehende Primzahl oder die Potenz einer (ungeraden) Primzahl ist, mag dieselbe in n aufgehen oder nicht, so können dieselben noch einfacher behandelt werden. Alle diese Fälle behandeln wir gleichzeitig und setzen, unter Beibehaltung sämtlicher Bezeichnungen des Artikels 324, $n = n'p^\nu$, so dass n' durch p nicht teilbar ist. Die Zahlen $a, b, c, \ldots$ sind Producte der Zahl $p^{\mu-1}$ entweder in alle unterhalb p gelegene Zahlen (ausser 0) oder in alle Nichtreste von p unterhalb p, je nachdem μ gerade oder ungerade ist; dieselben mögen unbestimmt durch $up^{\mu-1}$ dargestellt werden. Ist k der Wert des Ausdrucks $\frac{A}{m} \pmod{p^{\mu+\nu}}$, so ist derselbe durch p nicht teilbar, weil dieselbe Eigenschaft bei A vorausgesetzt wird; ferner ist klar, dass alle Zahlen $\alpha, \beta, \gamma, \ldots$ der Zahl k nach dem Modul p congruent werden und daher p^μ in Ω keine Ausschliessung bewirkt, wenn kNp ist; ist aber kRp und daher auch $kRp^{\mu+\nu}$, so sei r der Wert des Ausdrucks $\sqrt{k} \pmod{p^{\mu+\nu}}$, welcher durch p nicht teilbar ist, und e der Wert von $-\frac{n'}{2mr} \pmod{p}$; dann ist $\alpha \equiv r^2 + 2erap^\nu \pmod{p^{\mu+\nu}}$, woraus leicht folgt, dass α Rest von $p^{\mu+\nu}$ ist und die Werte von $\sqrt{\alpha} \pmod{p^{\mu+\nu}}$ werden: $\pm(r + eap^\nu)$. Demnach werden sämtliche Werte $h, h'\ h'', \ldots$ dargestellt durch $r + uep^{\mu+\nu-1}$. Endlich schliesst man hieraus leicht, dass die Zahlen $h, h', h'', \ldots$ entstehen durch Addition der Zahl r und der Producte der Zahl $p^{\mu+\nu-1}$ entweder in alle Zahlen unterhalb p (ausser 0), falls μ gerade ist, oder in alle Nichtreste von p unterhalb dieser Grenze, falls μ ungerade und eRp oder, was hier auf dasselbe hinauskommt, falls $-2mrn'Rp$ ist, oder in alle Reste (ausser 0), falls μ ungerade und $-2mrn'Np$ ist.

Übrigens wird man auch, sobald für die einzelnen Exkludenten, welche man anwenden will, die Zahlen $h, h', \ldots$ ermittelt sind, die Ausschliessung selbst auch durch mechanische Operationen bewirken können, wie sie sich jeder in diesen Dingen Erfahrene leicht selbst wird ersinnen können, wenn es sich der Mühe lohnen sollte.

Endlich müssen wir bemerken, dass jede Gleichung $ax^2 + 2bxy + cy^2 = M$, in welcher $b^2 - ac$ eine negative Zahl $= -D$ ist, leicht auf die im Vorstehenden betrachtete Form zurückgeführt werden kann. Bezeichnet man nämlich den grössten gemeinschaftlichen Teiler der Zahlen a, b mit m und setzt man:

$$a = ma',\ b = mb',\ \frac{D}{m} = a'c - mb'^2 = n,\ a'x + b'y = x',$$

so ist jene Gleichung offenbar der folgenden Gleichung $mx'^2 + ny^2 = a'M$, welche nach den oben angegebenen Regeln gelöst werden kann, äquivalent. Von den Lösungen dieser sind aber nur die beizubehalten, in denen $x' - b'y$ durch a' teilbar ist, oder aus denen sich ganze Werte für x ergeben.

Andere Methode, die Congruenz $x^2 \equiv A$ zu lösen für den Fall, in welchem A negativ ist.

327.

Während die im Abschnitt V enthaltene directe Lösung der Gleichung $ax^2 + 2bxy + cy^2 = M$ die Werte des Ausdrucks $\sqrt{b^2 - ac}$ (mod. M) als bekannt voraussetzt, liefert umgekehrt in dem Falle, wo $b^2 - ac$ negativ ist, die im Vorhergehenden auseinandergesetze indirecte Auflösung eine sehr einfache Methode, jene Werte zu ermitteln, welche besonders für einen sehr grossen Wert von M der Methode des Artikels 322 u. ff. bei weitem vorzuziehen ist. Wir nehmen aber an, dass M eine Primzahl sei, oder dass wenigstens, wenn sie eine zusammengesetzte Zahl ist, ihre Factoren noch unbekannt seien; denn wenn man wüsste, dass die Primzahl p in M aufgeht, und $M = p^\mu M'$ ist, so dass M' den Factor p nicht mehr enthält, so würde es weit bequemer sein, die Werte des Ausdrucks $\sqrt{b^2 - ac}$ für die Moduln p^μ und M' einzeln (die ersteren aus den Werten für den Modul p, Artikel 101) zu ermitteln und aus der Combination dieser die Werte nach dem Modul M abzuleiten (Artikel 105).

Es sind daher sämtliche Werte des Ausdrucks $\sqrt{-D}$ (mod. M) zu suchen, wo D und M als positiv und M unter der Form der Teiler von $x^2 + D$ enthalten vorausgesetzt werden (Artikel 147 u. ff.), letzteres deshalb, weil sonst von vornherein feststände, dass keine Zahlen dem gegebenen Ausdruck genügen können. Es seien die gesuchten Werte, von denen stets je zwei einander entgegengesetzt sind, $\pm r, \pm r', \pm r'', \ldots$ und $D + r^2 = Mh$ $D + r'^2 = Mh'$, $D + r''^2 = Mh'', \ldots$; ferner mögen die Klassen, zu denen die Formen (M, r, h), $(M, -r, h)$, (M, r', h'), $(M, -r', h')$, (M, r'', h''), $(M, -r'', h''), \ldots$ gehören, respective mit $\mathfrak{C}, -\mathfrak{C}, \mathfrak{C}', -\mathfrak{C}', \mathfrak{C}'', -\mathfrak{C}'', \ldots$ und ihr Complex mit $\mathfrak{G}$ bezeichnet werden. Diese Klassen sind zwar, allgemein zu reden, als unbekannt zu betrachten; trotzdem ist ersichtlich, erstens dass sie sämtlich positiv und eigentlich primitiv sind, zweitens, dass sie sämtlich zu demselben Geschlechte gehören, dessen Character aus der Beschaffenheit der Zahl M, d. h. aus ihren Beziehungen zu den einzelnen Primteilern von D (und überdies zu 4 und 8, wenn diese nötig sind) leicht erkannt werden kann (Artikel 230). Da vorausgesetzt ist, dass M unter der Form der Teiler von $x^2 + D$ enthalten sei, so können wir von vornherein sicher sein, dass diesem Character notwendig ein positives, eigentlich primitives Geschlecht von Formen mit der Determinante $-D$ entspricht, ob-

gleich man vielleicht dem Ausdruck $\sqrt{-D}$ (mod. M) nicht genügen kann; da nun also dieses Geschlecht bekannt ist, kann man alle in ihm enthaltenen Klassen ermitteln; dieselben seien $C, C', C'', \ldots$ und ihr Complex G. Nun ist klar, dass jede einzelne Klasse $\mathfrak{C}, -\mathfrak{C}, \ldots$ mit irgend einer Klasse in G identisch sein muss; es kann auch geschehen, dass mehrere Klassen in $\mathfrak{G}$ unter sich und daher mit derselben Klasse in G identisch sind, und wenn G nur eine einzige Klasse enthält, so werden alle Klassen in $\mathfrak{G}$ mit dieser übereinstimmen. Wenn daher aus den Klassen $C, C', C'', \ldots$ die (einfachsten) Formen $f, f', f'', \ldots$ ausgewählt werden (je eine aus jeder), so wird sich von den einzelnen Klassen in $\mathfrak{G}$ je eine unter diesen vorfinden. Wenn nun $ax^2 + 2bxy + cy^2$ die in der Klasse $\mathfrak{C}$ enthaltene Form ist, so giebt es zwei zum Werte r gehörige Darstellungen der Zahl M durch sie, und zwar ist, wenn die eine $x = m$, $y = n$ ist, die andere $x = -m$, $y = -n$, nur der eine Fall, wo $D = 1$ ist, muss ausgenommen werden, da es in diesem vier Darstellungen giebt (Vgl. Artikel 180).

Hieraus schliesst man, dass, wenn man alle Darstellungen der Zahl M durch die einzelnen Formen $f, f', f'', \ldots$ (nach der im Vorstehenden angegebenen indirecten Methode) ermittelt und daraus die Werte des Ausdrucks $\sqrt{-D}$ (mod. M), zu welchen die einzelnen gehören, ableitet (Artikel 154), sämtliche Werte dieses Ausdrucks daraus erhalten werden und zwar jeder einzelne zweimal oder, falls $D = 1$ ist, viermal, womit die Aufgabe gelöst ist. Finden sich unter $f, f', f'', \ldots$ irgend welche Formen, durch welche M nicht dargestellt werden kann, so ist dies ein Zeichen, dass sie zu keiner Klasse in $\mathfrak{G}$ gehören und somit weggelassen werden müssen; wenn aber M durch keine von jenen Formen dargestellt werden kann, so muss notwendig $-D$ quadratischer Nichtrest von M sein.

Hinsichtlich dieser Operationen beachte man noch folgende Bemerkungen.

I. Es werden unter den Darstellungen der Zahl M durch die Formen $f, f', \ldots$, die wir hier anwenden, solche verstanden, in denen die Werte der Unbestimmten prim zu einander sind; erhält man irgend welche andern, in denen diese Werte einen gemeinschaftlichen Teiler haben (was nur dann der Fall sein kann, wenn μ^2 in M aufgeht, und sicher eintritt, wenn $-DR\frac{M}{\mu^2}$ ist), so müssen dieselben für den vorliegenden Zweck ganz weggelassen werden, obwohl sie in anderer Hinsicht nützlich sein können.

II. Unter sonst gleichen Umständen ist offenbar die Arbeit um so leichter, je kleiner die Anzahl der Klassen $f, f', f'', \ldots$ ist, und somit am kürzesten, wenn D eine von den 65 im Artikel 303 angegebenen Zahlen ist, für die es in den einzelnen Geschlechtern nur eine einzige Klasse giebt.

III. Da je zwei solche Darstellungen wie $x = m, y = n; x = -m, y = -n$ stets zu demselben Werte gehören, so reicht es offenbar aus, nur diejenigen Darstellungen zu betrachten, in denen y positiv ist. Derartige verschiedene

Darstellungen entsprechen daher immer verschiedenen Werten des Ausdruckes $\sqrt{-D} \pmod{M}$, sodass die Anzahl aller verschiedenen Werte der Anzahl aller sich ergebenden Darstellungen dieser Art gleich ist (immer den Fall $D = 1$ ausgenommen, in welchem jene die Hälfte dieser ist).

IV. Da man, sobald der eine der beiden entgegengesetzten Werte $+r$, $-r$ bekannt ist, auch sofort den andern kennt, so lassen sich die Operationen noch etwas abkürzen. Wird der Wert r aus der Darstellung der Zahl M durch eine in der Klasse C enthaltene Form gefunden, d. h. ist $\mathfrak{C} = C$, so wird sich offenbar der entgegengesetzte Wert $-r$ aus der Darstellung durch eine Form ergeben, welche in der zu C entgegengesetzten Klasse enthalten ist, die von der Klasse C verschieden ist, falls nicht etwa letztere ambig ist. Hieraus folgt, dass man, wenn nicht alle Klassen in G ambig sind, von den übrigen nur die Hälfte zu betrachten braucht, nämlich von je zwei entgegengesetzten nur die eine, während die andere wegzulassen ist, da aus ihr, wie man auch ohne Rechnung voraussetzen kann, sich Werte ergeben, welche denen, die die erstere liefert, entgegengesetzt sind. Ist aber C ambig, so werden sich aus ihr die beiden Werte r und $-r$ gleichzeitig ergeben; es wird nämlich, wenn aus C die ambige Form $ax^2 + 2bxy + cy^2$ ausgewählt wurde und der Wert r aus der Darstellung $x = m$, $y = n$ sich ergeben hat, der Wert $-r$ sich aus der folgenden $x = -m - \frac{2bn}{a}$, $y = n$ ergeben.

V. Für denjenigen Fall, in welchem $D = 1$ ist, giebt es überhaupt nur eine Klasse, aus der, wie wir annehmen dürfen, die Form $x^2 + y^2$ ausgewählt worden sei. Wenn nun der Wert r aus der Darstellung $x = m$, $y = n$ entsteht, so wird derselbe auch aus den Darstellungen $x = -m$, $y = -n$; $x = -m$, $y = n$; $x = m$, $y = -n$ und der entgegengesetzte $-r$ aus den Darstellungen $x = m$, $y = -n$; $x = -m$, $y = n$; $x = n$, $y = m$; $x = -n$, $y = -m$ sich ergeben. Daher genügt von diesen acht Darstellungen, welche nur eine Zerlegung geben, eine, wenn man nur dem daraus entstehenden Werte den entgegengesetzten associiert.

VI. Der Wert des Ausdrucks $\sqrt{-D} \pmod{M}$, zu welchem die Darstellung $M = am^2 + 2bmn + cn^2$ gehört, ist nach Artikel 155: $\mu(mb + nc) - \nu(ma + nb)$ oder irgend eine diesem Werte nach dem Modul M congruente Zahl, wenn μ, ν so angenommen sind, dass $\mu m + \nu n = 1$ ist. Bezeichnet man daher einen solchen Wert mit v, so ist:

$$mv \equiv \mu m(mb + nc) - \nu(M - mnb - n^2c) \equiv (\mu m + \nu n)(mb + nc)$$
$$\equiv mb + nc \pmod{M}.$$

Hieraus geht hervor, dass v der Wert des Ausdrucks $\frac{mb + nc}{m} \pmod{M}$ ist, und auf ähnliche Weise findet man, dass v der Wert des Ausdrucks

$-\frac{ma+nb}{n}$ (mod. M) ist. Diese Formeln sind sehr häufig derjenigen, aus welcher sie abgeleitet sind, vorzuziehen.

328.

Beispiele. I. Man sucht sämtliche Werte des Ausdrucks $\sqrt{-1365}$ (mod. $5428681 = M$). Die Zahl M ist hier $\equiv 1, 1, 1, 6, 11$ (mod. 4, 3, 5, 7, 13) und daher unter der Form der Teiler von x^2+1, x^2+3, x^2-5 und unter der Form der Nichtteiler von x^2+7, x^2-13, also unter der Form der Teiler von x^2+1365 enthalten; der Character des Geschlechts, in welchem sich die Klassen $\mathfrak{G}$ vorfinden, ist 1, 4; $R3$; $R5$; $N7$; $N13$. In diesem Geschlecht ist nur eine einzige Klasse enthalten, aus welcher wir die Form $6x^2+6xy+229y^2$ auswählen. Um alle Darstellungen der Zahl M durch diese zu erhalten, setzen wir $2x+y=x'$, wodurch sie übergehen muss in $3x'^2+455y^2=2M$. Diese Gleichung besitzt vier Lösungen, in denen y positiv ist, nämlich $y=127$, $x'=\pm 1083$; $y=119$, $x'=\pm 1213$. Hieraus ergeben sich vier Lösungen der Gleichung $6x^2+6xy+229y^2=M$, in denen y positiv ist, nämlich:

x	478	-605	547	-666
y	127	127	119	119.

Die erste Lösung giebt für v den Wert des Ausdrucks $\frac{30517}{478}$ oder $-\frac{3249}{127}$ (mod. M), woraus man 2350978 findet; die zweite bringt den entgegengesetzten Wert -2350978, die dritte den Wert 2600262, die vierte den entgegengesetzten Wert -2600262 hervor.

II. Wenn die Werte des Ausdrucks $\sqrt{-286}$ (mod. $4272943 = M$) gesucht werden sollen, so findet man als Character des Geschlechts, in welchem die Klassen $\mathfrak{G}$ enthalten sind: 1 u. 7, 8; $R11$; $R13$; daher ist es das Hauptgeschlecht, in welchem drei Klassen enthalten sind, die durch die Formen $(1, 0, 286)$, $(14, 6, 23)$, $(14, -6, 23)$ dargestellt werden; von diesen kann man die dritte, da sie der zweiten entgegengesetzt ist, weglassen. Durch die Form x^2+286y^2 findet man zwei Darstellungen der Zahl M, in denen y positiv ist, nämlich $y=103$, $x=\pm 1113$, aus denen sich die folgenden Werte des gegebenen Ausdrucks ergeben: 1493445, -1493445. Durch die Form $(14, 6, 23)$ aber ist die Zahl M nicht darstellbar, woraus folgt, dass es ausser den beiden gefundenen Werten keine andern weiter giebt.

III. Ist der Ausdruck $\sqrt{-70}$ (mod. 997331) gegeben, so müssen die Klassen $\mathfrak{G}$ in einem Geschlechte enthalten sein, dessen Character 3 u. 5, 8; $R5$; $N7$ ist; in diesem findet sich nur eine einzige Klasse, deren repräsentierende Form $(5, 0, 14)$ ist. Stellt man aber die Rechnung an, so findet man, dass die Zahl 997331 durch die Form $(5, 0, 14)$ nicht darstellbar ist, weshalb -70 notwendig quadratischer Nichtrest jener Zahl ist.

Zwei Methoden, zusammengesetzte Zahlen von primen zu unterscheiden und ihre Factoren zu ermitteln.

329.

Dass die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfactoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten wie auch der neueren Geometer in Anspruch genommen hat, ist so bekannt, dass es überflüssig wäre, hierüber viele Worte zu verlieren. Trotzdem muss man gestehen, dass alle bisher angegebenen Methoden entweder auf sehr specielle Fälle beschränkt oder so mühsam und weitläufig sind, dass sie schon für solche Zahlen, welche die Grenzen der von verdienstvollen Männern aufgestellten Tafeln nicht überschreiten, d. h. für welche künstliche Methoden überflüssig sind, die Geduld sogar eines geübten Rechners ermüden, auf grössere Zahlen aber meistenteils kaum angewendet werden können. Obwohl aber jene Tafeln, die sich in aller Händen befinden, und die, wie wir hoffen dürfen, bald eine weitere Fortsetzung erfahren werden, in den meisten gewöhnlich vorkommenden Fällen jedenfalls ausreichen, so bietet sich doch dem erfahrenen Rechner nicht selten die Gelegenheit dar, aus der Zerlegung grosser Zahlen in Factoren grosse Vorteile zu ziehen, welche den mässigen Aufwand an Zeit reichlich wieder ausgleichen; ausserdem aber dürfte es die Würde der Wissenschaft erheischen, alle Hülfsmittel zur Lösung jenes so eleganten und berühmten Problems fleissig zu vervollkommnen. Aus diesen Gründen zweifeln wir nicht, dass die beiden folgenden Methoden, deren Wirksamkeit und Kürze wir durch eine lange Erfahrung bestätigen können, den Liebhabern der Arithmetik nicht unerwünscht sein werden. Übrigens ist es in der Natur der Aufgabe begründet, dass jede beliebige Methode fortwährend um so weitläufiger wird, je grösser die Zahlen sind, auf die sie angewandt wird; für die folgenden Methoden aber wachsen die Schwierigkeiten sehr langsam, und die aus sieben, acht, ja noch mehr Ziffern bestehenden Zahlen sind besonders nach der zweiten Methode stets mit glücklichem Erfolge und mit aller Schnelligkeit, die man billiger Weise für so grosse Zahlen erwarten kann, welche nach allen bisher bekannten Methoden eine auch dem unermüdlichen Rechner unerträgliche Arbeit erforderten, behandelt worden.

Bevor man die folgenden Methoden anwendet, ist es immer vorteilhaft, die Division irgend einer gegebenen Zahl durch einige der kleinsten Primzahlen, z. B. durch 2, 3, 5, 7, ... bis zu 19 oder noch weiter hinaus, zu versuchen, nicht nur, damit es nicht reut, eine solche Zahl, falls sie Divisor ist, durch subtile und künstliche Methoden erhalten zu haben, die man viel leichter durch blosse Division hätte finden können*), sondern auch deshalb,

*) Um so mehr, weil sich, allgemein zu reden, unter sechs Zahlen kaum eine findet, die nicht durch eine der Zahlen 2, 3, 5, ..., 19 teilbar wäre.

weil dann, wenn keine Division Erfolg hatte, die Anwendung der zweiten Methode sich der aus jenen Divisionen entstandenen Reste mit grossem Nutzen bedient. Soll z. B. die Zahl 314159265 in ihre Factoren zerlegt werden, so gelingt die Division durch 3 zweimal und sodann auch die Division durch 5 und 7, so dass man erhält: $314159265 = 9 \cdot 5 \cdot 7 \cdot 997331$ und es genügt, die Zahl 997331, die durch 11, 13, 17, 19 nicht teilbar befunden wird, einer eingehenderen Untersuchung zu unterwerfen. Analog werden wir von der gegebenen Zahl 43439448 den Factor 8 absondern und die künstlicheren Methoden auf den Quotienten 5428681 anwenden.

330.

Die Grundlage der **ersten Methode** bildet der Satz, dass jede positive oder negative Zahl, welche von einer andern Zahl M quadratischer Rest ist, auch quadratischer Rest jedes Teilers von M ist. Es ist allgemein bekannt, dass, wenn M durch keine Primzahl unterhalb $\sqrt{M}$ teilbar ist, M sicher eine Primzahl ist; dass aber, wenn alle Primzahlen unterhalb dieser Grenze, welche in M aufgehen, $p, q, \ldots$ sind, die Zahl M entweder aus diesen allein (und deren Potenzen) zusammengesetzt ist, oder nur einen einzigen andern Primfactor, der grösser als $\sqrt{M}$ ist, enthalten kann, welchen man findet, indem man M durch $p, q, \ldots$ so oft es geht dividiert. Bezeichnet man daher durch Ω den Complex aller Primzahlen unterhalb $\sqrt{M}$ (mit Ausschluss derjenigen, mit denen die Division bereits vergeblich versucht worden ist), so genügt es offenbar, wenn man alle in Ω enthaltenen Primteiler von M hat. Wenn man man nun irgend woher weiss, dass irgend eine (nichtquadratische) Zahl r quadratischer Rest von M ist, so kann sicher keine Primzahl, von welcher r Nichtrest ist, ein Teiler von M sein; daher wird man aus Ω sämtliche derartige Primzahlen (welche meistenteils ungefähr die Hälfte aller ausmachen) weglassen dürfen. Wenn überdies von einer andern nichtquadratischen Zahl r' bekannt ist, dass sie Rest von M ist, so wird man von den nach der ersten Ausschliessung in Ω übrig gebliebenen Primzahlen wiederum diejenigen ausschliessen können, von denen r' Nichtrest ist, und die wiederum ungefähr die Hälfte jener ausmachen, wofern die Reste r und r' unabhängig von einander sind (d. h., wenn nicht der eine notwendig an und für sich Rest aller Zahlen ist, von denen der andere Rest ist, was der Fall sein würde, wenn rr' ein Quadrat wäre). Sind noch andere Reste von M bekannt, $r'', r''', \ldots$, welche alle von den übrigen unabhängig sind*), so können mit den einzelnen analoge Ausschliessungen

*) Wenn das Product aus beliebig vielen Zahlen $r, r', r'', \ldots$ ein Quadrat ist, so ist jede von ihnen, z. B. r, Rest jeder (in keiner von ihnen aufgehenden) Primzahl, welche Rest der übrigen $r', r'', \ldots$ ist. Um also beliebig viele Reste als unabhängig betrachten zu können, darf kein Quadrat aus je zweien oder je dreien u. s. w. ein Quadrat sein.

vorgenommen werden, wodurch die Anzahl der Zahlen in Ω sehr rasch abnimmt, so dass bald entweder alle gestrichen sind, in welchem Falle M sicher eine Primzahl ist, oder nur so wenige übrigbleiben (unter denen sich offenbar alle Primteiler von M, wenn M solche hat, vorfinden), dass die Division durch sie ohne Mühe versucht werden kann. Bei einer Zahl, die eine Million nicht übersteigt, werden meistens sechs oder sieben, bei einer aus acht oder neun Ziffern bestehenden Zahl neun oder zehn Ausschliessungen vollauf genug sein. Nur über zwei Punkte müssen wir noch handeln, erstens, wie man passende und genügend viele Reste von M finden, zweitens, wie man die Ausschliessung selbst am bequemsten vornehmen kann. Jedoch wollen wir die Reihenfolge dieser Fragen umkehren, zumal da die zweite zeigen wird, was für Reste vornehmlich für diesen Zweck bequem sind.

331.

Wir haben im vierten Abschnitt ausführlich gezeigt, wie man die Primzahlen, von denen eine gegebene Zahl r (die wir durch kein Quadrat teilbar annehmen können) Rest ist, von denjenigen, von welchen sie Nichtrest ist, oder also wie man die Teiler des Ausdrucks $x^2 - r$ von den Nichtteilern unterscheiden kann, dass nämlich alle ersteren unter gewissen Formeln wie $rz + a$, $rz + b$, ... oder wie $4rz + a$, $4rz + b$, ... und die letzteren unter andern analogen Formeln enthalten seien. Ist r eine ziemlich kleine Zahl, so können die Ausschliessungen mit Hülfe dieser Formeln sehr bequem ausgeführt werden; z. B. sind alle Zahlen von der Form $4z + 3$, wenn $r = -1$, alle Zahlen von den Formen $8z + 3$, $8z + 5$, falls $r = 2$ ist, u. s. w. auszuschliessen. Da es aber nicht immer in unserer Macht steht, derartige Reste einer gegebenen Zahl zu finden, noch auch die Anwendung der Formeln für einen grossen Wert von r bequem genug ist, so ist es ein ungeheurer Vorteil und erleichtert die Mühe der Ausschliessung in erstaunlicher Weise, wenn man für eine hinreichend grosse Anzahl von positiven und negativen durch ein Quadrat nicht teilbaren Zahlen (r) bereits eine Tafel construiert hat, in welcher die Primzahlen, deren Reste jene einzelnen r sind, von denjenigen, deren Nichtreste sie sind, unterschieden sind. Eine solche Tafel kann in derselben Weise eingerichtet werden, wie die am Schlusse dieses Werkes angefügte und schon oben beschriebene Probe; damit dieselbe aber für den gegenwärtigen Zweck hinreichend grossen Nutzen gewähre, müssen die am Rande stehenden Primzahlen (Moduln) viel weiter, nämlich mindestens bis zu 1000 oder 10000 fortgesetzt werden; überdies wird die Bequemlichkeit noch bedeutend vermehrt werden, wenn man am Kopfe der Tafel auch die zusammengesetzten und negativen Zahlen aufnimmt, obwohl dies, wie aus dem vierten Abschnitt hervorgeht, nicht absolut notwendig ist. Am bequemsten aber wird der Gebrauch einer solchen Tafel, wenn die einzelnen Vertikalkolonnen, aus denen sie besteht, ausgeschnitten und auf Streifen von Blech oder auf (den Neper'schen ähnliche) Holz-

stäbchen aufgeklebt werden, so dass diejenigen, welche in jedem Falle erforderlich sind, d. h. welche den Zahlen $r, r', r'', \ldots$, den Resten der gegebenen in Factoren zu zerlegenden Zahl, entsprechen, für sich untersucht werden können. Werden diese in der richtigen Weise neben die erste Kolonne der Tafel (welche die Moduln darstellt) gelegt, d. h. so, dass die Plätze der einzelnen derselben Primzahl der ersten Kolonne entsprechenden Stäbchen mit dieser Primzahl in gerader Richtung liegen oder in dieselbe Horizontallinie fallen, so werden offenbar diejenigen Primzahlen, welche nach den Ausschliessungen vermittelst der Reste $r, r', r'', \ldots$ in Ω noch übrig bleiben, durch den blossen Anblick unmittelbar erkannt werden können; es werden nämlich diese übereinstimmen mit denjenigen in der ersten Kolonne, welchen in allen anliegenden Stäbchen Striche entsprechen, und es sind alle, bei welchen in irgend einem Stäbchen ein leerer Raum sich befindet, wegzulassen. Durch ein Beispiel wird dies hinreichend deutlich werden. Wenn man irgend woher weiss, dass die Zahlen $-6, +13, -14, +17, +37, -53$ Reste von 997331 sind, so muss man die erste Kolonne (welche in diesem Falle bis zu 997 fortgesetzt werden muss, d. h. bis zu der grössten Primzahl unterhalb $\sqrt{997331}$) und die Streifen, an deren Kopfe die Zahlen $-6, +13, \ldots$ stehen, nebeneinander legen. Wir geben hier einen Teil des auf diese Weise hervorgehenden Schemas:

	-6	$+13$	-14	$+17$	$+37$	-53
3	—	—	—		—	—
5	—		—			
7	—		—		—	
11	—				—	
13		—	—	—		—
17		—		—		—
19			—	—		—
23		—	—			—
			u. s. w.			
113		—	—			—
127	—	—	—	—	—	—
131	—	—	—			
			u. s. w.			

Wie man nun hier aus dem blossen Anblick erkennt, dass von denjenigen Primzahlen, welche in diesem Teil des Schemas enthalten sind, nur die Zahl 127 nach den Ausschliessungen vermittelst der Reste -6, $+13, \ldots$ in Ω übrig bleibt, so zeigt das ganze bis zur Zahl 997 erstreckte Schema, dass durchaus keine andere Zahl weiter in Ω übrig bleibt; versucht man aber die Division, so findet man, dass 997331 in der That durch 127 teilbar ist. Auf diese Weise ist daher jene Zahl in die Primfactoren $127 \cdot 7853$ zerlegt.

Übrigens geht aus dieser Auseinandersetzung zur Genüge hervor, dass nicht allzugrosse oder wenigstens in nicht allzugrosse Primzahlen zerlegbare Reste besonders vorteilhaft sind, da die unmittelbare Anwendung der Hülfstafel sich nicht über die am Kopfe befindlichen Zahlen hinaus erstreckt und die mittelbare Anwendung nur solche umfasst, welche in Factoren zerlegt werden können, die in der Tafel enthalten sind.

332.

Um die Reste der gegebenen Zahl M zu finden, werden wir drei verschiedene Methoden angeben, deren Auseinandersetzung wir zwei Bemerkungen vorausschicken, vermittelst deren man aus weniger geeigneten Resten einfachere ableiten kann. Erstens, wenn die Zahl ak^2, welche durch das Quadrat k^2 (das wir prim zu M voraussetzen) teilbar ist, Rest von M ist, so wird auch a Rest sein; daher sind die durch grosse Quadrate teilbaren Reste ebenso vorteilhaft, wie kleine, und wir werden somit voraussetzen, dass alle durch die nachstehenden Methoden gelieferten Reste sogleich von ihren quadratischen Factoren befreit seien. Zweitens, wenn zwei oder mehrere Zahlen Reste sind, so wird auch das Product aus ihnen ein Rest sein. Verbindet man diese Bemerkung mit der vorigen, so kann man sehr häufig aus mehreren Resten, welche nicht alle einfach genug sind, einen andern sehr einfachen ableiten, wofern nur jene viele gemeinsame Factoren haben. Aus diesem Grunde leisten auch solche Reste sehr gute Dienste, welche aus vielen nicht allzugrossen Factoren zusammengesetzt sind, und man wird gut thun, sogleich alle in ihre Factoren zu zerlegen. Die Bedeutung dieser Bemerkungen wird man besser durch Beispiele und häufigen Gebrauch als durch theoretische Vorschriften erkennen.

I. Die einfachste und für diejenigen, welche sich durch häufige Übung bereits einige Gewandtheit erworben haben, bequemste Methode besteht darin, dass man M oder allgemeiner irgend ein Vielfaches von M in zwei Teile zerlegt $km = a + b$ (mögen beide positiv oder der eine positiv, der andere negativ sein), deren Product mit verändertem Vorzeichen Rest von M sein wird; denn es ist $-ab \equiv a^2 \equiv b^2 \pmod{M}$ und daher $-abRM$. Die Zahlen a, b sind so anzunehmen, dass ihr Product durch ein grosses Quadrat teilbar und der Quotient entweder klein oder wenigstens in nicht zu grosse Factoren zerlegbar wird, was immer ohne Schwierigkeit ausgeführt werden kann. Besonders zu empfehlen ist es, für a entweder ein Quadrat oder ein doppeltes oder dreifaches u. s. w. Quadrat zu nehmen, welches von der Zahl M um eine entweder kleine oder in bequeme Factoren zerlegbare Zahl abweicht. So findet man z. B. $997331 = 999^2 - 2 \cdot 5 \cdot 67 = 994^2 + 5 \cdot 11 \cdot 13^2 = 2 \cdot 706^2 + 3 \cdot 17 \cdot 3^2 = 3 \cdot 575^2 + 11 \cdot 31 \cdot 4^2 = 3 \cdot 577^2 - 7 \cdot 13 \cdot 4^2 = 3 \cdot 578^2 - 7 \cdot 19 \cdot 37 = 11 \cdot 299^2 + 2 \cdot 3 \cdot 5 \cdot 29 \cdot 4^2 = 11 \cdot 301^2 + 5 \cdot 12^2$, u. s. w. Hieraus erhält man die folgenden Reste: $2 \cdot 5 \cdot 67$, $-5 \cdot 11$, $-2 \cdot 3 \cdot 17$, $-3 \cdot 11 \cdot 31$, $3 \cdot 7 \cdot 13$, $3 \cdot 7 \cdot 19 \cdot 37$, $-2 \cdot 3 \cdot 5 \cdot 11 \cdot 29$; die letzte Zerlegung liefert den Rest $-5 \cdot 11$, den wir schon haben. An Stelle der

Reste $-3\cdot11\cdot31$, $-2\cdot3\cdot5\cdot11\cdot29$ kann man die folgenden nehmen: $3\cdot5\cdot31$, $2\cdot3\cdot29$, welche aus ihrer Combination mit $-5\cdot11$ entstehen.

II. Die zweite und dritte Methode gründet sich darauf, dass, wenn zwei binäre Formen (A, B, C), (A', B', C') mit derselben Determinante M oder $-M$ oder allgemeiner $\pm kM$ zu demselben Geschlechte gehören, die Zahlen AA', AC', $A'C$ Reste von kM sind; dies erkennt man ohne Schwierigkeit daraus, dass jede characteristische Zahl der einen Form, etwa m, auch eine characteristische Zahl der andern ist und somit mA, mC, mA', mC' sämtlich Reste von kM sind. Ist daher (a, b, a') eine reducierte Form mit der positiven Determinante M oder allgemeiner kM und sind (a', b', a''), (a'', b'', a'''),... Formen aus ihrer Periode und somit ihr äquivalent und um so mehr unter demselben Geschlecht mit ihr enthalten, so sind die Zahlen aa', aa'', aa''', ... sämtlich Reste von M. Die Berechnung einer grossen Anzahl von Formen einer solchen Periode kann man mit Hülfe des Algorithmus im Artikel 187 sehr leicht durchführen; die einfachsten Reste ergeben sich meistens, wenn man $a = 1$ setzt; diejenigen, welche zu grosse Factoren enthalten, sind zu verwerfen. Nachstehend sieht man die Anfänge der Perioden der Formen $(1, 998, -1327)$ und $(1, 1412, -918)$, deren Determinanten 997331 und 1994662 sind:

(1, 998, −1327)	(1, 1412, − 918)
(−1327, 329, 670)	(− 918, 1342, 211)
(670, 341, −1315)	(211, 1401, − 151)
(−1315, 974, 37)	(− 151, 1317, 1723)
(37, 987, − 626)	(1723, 406, −1062)
(− 626, 891, 325)	(−1062, 656, 1473)
(325, 734, −1411)	(1473, 817, − 901)
(−1411, 677, 382)	(− 901, 985, 1137)
(382, 851, − 715)	u. s. w.
u. s. w.	

Es sind daher Reste der Zahl 997331 sämtliche Zahlen -1327, 670, ... Lässt man aber diejenigen fort, welche zu grosse Factoren enthalten, so hat man die folgenden: $2\cdot5\cdot67$, 37, 13, $-17\cdot83$, $-5\cdot11\cdot13$, $-2\cdot3\cdot17$, $-2\cdot59$, $-17\cdot53$. Den Rest $2\cdot5\cdot67$, sowie den Rest $-5\cdot11$, welcher aus der Combination des dritten mit dem fünften entsteht, hatten wir schon oben gefunden.

III. Ist C irgend eine von der Hauptklasse verschiedene Klasse der Formen mit der negativen Determinante $-M$ oder allgemeiner $-kM$, und ist $2C$, $3C$, ... ihre Periode (Artikel 307), so gehören die Klassen $2C$, $4C$, ... zum Hauptgeschlecht, die Klassen $3C$, $5C$, ... aber zu demselben Geschlecht wie C. Wenn daher (a, b, c) die (einfachste) Form aus C und (a', b', c') eine Form aus irgend einer Klasse jener Periode, etwa aus nC, ist, so wird entweder a' oder aa' Rest von M sein, je nachdem n gerade oder ungerade ist (im ersteren Falle offenbar auch c', im letzteren ac', ca'

und cc'). Die Entwicklung der Periode, d. h. der einfachsten Formen in ihrer Klasse, lässt sich mit erstaunlicher Leichtigkeit ausführen, wenn a sehr klein ist, zumal im Fall $a = 3$, den man immer herbeiführen kann, wenn man $kM \equiv 2 \pmod 3$ macht. Nachstehend sieht man den Anfang der Periode der Klasse, in welcher die Form (3, 1, 332444) enthalten ist.

$C = (\ 3,\ \ 1, 332444)$	$6C = (\ 729, -209, 1428)$
$2C = (\ 9, -2, 110815)$	$7C = (\ 476,\ \ 209, 2187)$
$3C = (\ 27,\ \ 7,\ \ 36940)$	$8C = (1027,\ \ 342, 1085)$
$4C = (\ 81,\ \ 34,\ \ 12327)$	$9C = (\ 932, -437, 1275)$
$5C = (243,\ \ 34,\ \ 4109)$	$10C = (\ 425,\ \ 12, 2347).$

Hieraus ergeben sich die Reste (mit Beiseitelassung der untauglichen): $3 \cdot 476$, 1027, 1085, 425 oder (wenn man die quadratischen Factoren weglässt): $3 \cdot 7 \cdot 17$, $13 \cdot 79$, $5 \cdot 7 \cdot 31$, 17, und verbindet man diese in angemessener Weise mit den acht in II gefundenen, so findet man leicht die folgenden zwölf: $-2 \cdot 3$, 13, $-2 \cdot 7$, 17, 37, -53, $-5 \cdot 11$, 79, -83, $-2 \cdot 59$, $-2 \cdot 5 \cdot 31$, $2 \cdot 5 \cdot 67$. Die sechs ersten sind dieselben, deren wir uns im Artikel 331 bedient haben. Es hätten noch die Reste 19 und -29 hinzugefügt werden können, wenn wir auch diejenigen hätten anwenden wollen, die in I gefunden sind; die übrigen dort erhaltenen Reste sind von den hier abgeleiteten bereits abhängig.

333.

Die **zweite Methode**, eine gegebene Zahl M in Factoren zu zerlegen, geht aus von der Betrachtung der Werte eines Ausdrucks wie $\sqrt{-D} \pmod M$ und stützt sich auf folgende Bemerkungen:

I. Ist M eine Primzahl oder eine Potenz einer (ungeraden in D nicht aufgehenden) Primzahl, so ist $-D$ Rest oder Nichtrest von M, je nachdem M in der Form der Teiler oder in der Form der Nichtteiler von $x^2 + D$ enthalten ist, und im ersteren Falle besitzt der Ausdruck $\sqrt{-D} \pmod M$ nur zwei verschiedene Werte, welche entgegengesetzt sind.

II. Ist aber M eine zusammengesetzte Zahl, etwa $= pp'p'' \ldots$, wo p, $p', p'', \ldots$ (ungerade in D nicht aufgehende verschiedene) Primzahlen oder Potenzen solcher Primzahlen bezeichnen, so ist $-D$ nur dann Rest von M, wenn es Rest der einzelnen $p, p', p'', \ldots$ ist, d. h. wenn diese Zahlen sämtlich in den Formen der Teiler von $x^2 + D$ enthalten sind. Bezeichnet man aber die Werte des Ausdrucks $\sqrt{-D}$ nach den Moduln $p, p', p'', \ldots$ bezüglich mit $\pm r, \pm r' \pm r'', \ldots$, so entstehen sämtliche Werte desselben Ausdrucks nach dem Modul M, wenn man die Zahlen sucht, welche nach p entweder $\equiv r$ oder $\equiv -r$, nach p' entweder $\equiv r'$ oder $\equiv -r'$, u. s. w. sind, so dass also ihre Anzahl gleich 2^μ wird, wenn μ die Anzahl der Zahlen $p, p', p'', \ldots$ bezeichnet. Wenn nun diese Werte $R, -R, R', -R', R'', \ldots$ sind, so ist von selbst $R \equiv R$ nach allen Zahlen $p, p', p'', \ldots$; aber nach keiner $R \equiv -R$,

so dass der grösste gemeinschaftliche Teiler der Zahlen M und $R - R$ gleich M und der grösste gemeinschaftliche Teiler von M und $R + R$ gleich 1 ist; zwei Werte aber, die weder identisch noch entgegengesetzt sind, wie z. B. R und R' werden notwendig nach einer oder mehreren von den Zahlen $p, p', p'', \ldots$ aber nicht nach allen congruent sein und nach den übrigen ist $R \equiv -R'$; daher ist das Product jener der grösste gemeinschaftliche Teiler der Zahlen M und $R - R'$, und das Product dieser der grösste gemeinschaftliche Teiler der Zahlen M und $R + R'$. Hieraus folgt leicht, dass, wenn alle grössten gemeinschaftlichen Teiler von M und der Differenzen zwischen den einzelnen Werten des Ausdrucks $\sqrt{-D}$ (mod. M) und irgend eines gegebenen Wertes berechnet werden, der Complex derselben die Zahlen $1, p, p', p'', \ldots$ sowie die Producte von je zweien, je dreien u. s. w. dieser Zahlen enthält. Auf diese Weise ist man daher im Stande, aus den Werten jenes Ausdrucks die Zahlen $p, p', p'', \ldots$ abzuleiten.

Da übrigens die Methode des Artikels 327 diese einzelnen Werte auf die Werte von Ausdrücken von der Form $\frac{m}{n}$ (mod. M) reduciert, so dass der Nenner n zu M prim ist, so ist es für den gegenwärtigen Zweck nicht einmal notwendig, diese selbst zu berechnen. Denn der grösste gemeinschaftliche Divisor der Zahl M und der Differenz zwischen R und R', welche mit $\frac{m}{n}, \frac{m'}{n'}$ übereinstimmen, ist offenbar auch grösster gemeinschaftlicher Teiler von M und $nn'(R - R')$ oder von M und $mn' - m'n$, da dieser Zahl die Zahl $nn'(R - R')$ nach dem Modul M congruent ist.

334.

Die vorstehenden Bemerkungen lassen sich auf das vorliegende Problem in doppelter Weise anwenden; die erstere entscheidet nicht nur, ob eine gegebene Zahl M eine Primzahl oder eine zusammengesetzte Zahl ist, sondern sie liefert auch in diesem Falle die Factoren selbst; die letztere aber verdient insofern den Vorzug, als sie meistens eine einfachere Rechnung gestattet, indessen giebt sie nicht immer, wofern sie nicht mehrmals wiederholt wird, die Factoren der zusammengesetzten Zahlen selbst, jedoch unterscheidet auch sie die zusammengesetzten Zahlen von den Primzahlen.

I. Man suche eine negative Zahl $-D$, welche quadratischer Rest von M ist, zu welchem Zwecke man die im Artikel 332 unter I und II angegebenen Methoden benutzen kann. An sich zwar ist es willkürlich, welchen Rest man wählt, auch ist es hier nicht wie in der vorigen Methode erforderlich, dass D eine kleine Zahl sei; indessen wird die Rechnung um so kürzer sein, je kleiner die Anzahl der in den einzelnen eigentlich primitiven Geschlechtern mit der Determinante $-D$ enthaltenen Klassen binärer Formen ist, so dass besonders solche Reste, welche unter den 65 Zahlen des Artikels 303 enthalten sind, wenn sich solche darbieten, günstig sind. So würde für $M = 997331$ von allen oben ermittelten negativen Resten

der Rest — 102 am geeignetsten sein. Man entwickle sodann alle von einander verschiedenen Werte des Ausdrucks $\sqrt{-D}$ (mod. M); wenn sich nur zwei (entgegengesetzte) ergeben, so ist M sicher eine Primzahl oder eine Potenz einer Primzahl; wenn dagegen mehrere, etwa 2^μ, hervorgehen, so ist M zusammengesetzt aus μ verschiedenen Primzahlen oder Potenzen von Primzahlen, und diese Factoren können nach der Methode des vorigen Artikels gefunden werden. Ob aber diese Factoren Primzahlen oder Potenzen von Primzahlen sind, lässt sich nicht nur an sich sehr leicht entscheiden, es giebt auch das Verfahren selbst, nach welchem die Werte des Ausdrucks $\sqrt{-D}$ gefunden werden, sämtliche Primzahlen, von denen irgend eine Potenz in M aufgeht, unmittelbar an. Ist nämlich M durch das Quadrat einer Primzahl π teilbar, so wird jene Rechnung sicher auch eine oder mehrere Darstellungen der Zahl M, $M = am^2 + 2bmn + cn^2$, von der Art zum Vorschein bringen, dass in ihnen der grösste gemeinschaftliche Teiler der Zahlen m, n gleich π ist (und zwar deshalb, weil in diesem Falle $-D$ auch Rest von $\frac{M}{\pi^2}$ ist). Wenn sich aber keine Darstellung ergiebt, in welcher m und n einen gemeinschaftlichen Teiler haben, so ist dies ein sicheres Zeichen, dass M durch kein Quadrat teilbar ist und somit alle Zahlen p, p', p'', ... Primzahlen sind.

Beispiel. Nach der oben angegebenen Methode findet man vier Werte des Ausdrucks $\sqrt{-408}$ (mod. 997331), welche mit den Werten $\pm \frac{1664}{113}$, $\pm \frac{2824}{3}$ übereinstimmen; als grösste gemeinschaftliche Factoren der Zahl 997331 und der Zahlen $3 \cdot 1664 - 113 \cdot 2824$ und $3 \cdot 1664 + 113 \cdot 2824$ oder der Zahlen 314120 und 324104 findet man 7853 und 127, daher $997331 = 127 \cdot 7853$, wie oben.

II. Man nehme irgend eine negative Zahl $-D$ von der Art an, dass M in der Form der Teiler von $x^2 + D$ enthalten ist. An sich ist es willkürlich, was für eine Zahl dieser Art man nimmt; der Bequemlichkeit halber aber muss man besonders darauf sehen, dass die Anzahl der Klassen in den Geschlechtern mit der Determinante $-D$ möglichst klein ist. Übrigens ist die Ermittlung einer solchen Zahl keinen Schwierigkeiten unterworfen, wenn man sie durch Probieren versucht; denn meistenteils ist M unter einer beträchtlichen Anzahl probierter Zahlen ungefähr für ebenso viele in der Form der Teiler, wie in der Form der Nichtteiler enthalten. Daher ist es am zweckmässigsten, den Versuch mit den 65 Zahlen des Artikels 303 (und zwar mit den grössten) zu beginnen und erst, wenn es sich träfe, dass keine derselben geeignet ist (was jedoch allgemein zu reden unter 16384 Fällen nur einmal eintritt), zu andern fortzuschreiten, bei denen je zwei Klassen in den einzelnen Geschlechtern enthalten sind. — Sodann ermittle man die Werte des Ausdrucks $\sqrt{-D}$ (mod. M) und leite, wenn man solche

Werte findet, die Factoren von M in ganz derselben Weise daraus her wie oben. Wenn aber keine solchen Werte hervorgehen und daher $-D$ Nichtrest von M ist, so wird sicher M weder eine Primzahl noch eine Potenz einer Primzahl sein können. Will man nun in diesem Falle die Factoren selbst haben, so muss man entweder dieselbe Operation wiederholen, indem man andere Werte für D nimmt, oder zu einer andern Methode seine Zuflucht nehmen.

Stellt man z. B. den Versuch mit der Zahl 997331 an, so findet man, dass dieselbe in der Form der Nichtteiler von $x^2 + 1848$, $x^2 + 1365$, $x^2 + 1320$, dagegen in der Form der Teiler von $x^2 + 840$ enthalten ist; als Werte des Ausdruckes $\sqrt{-840}$ (mod. 997331) erhält man die Ausdrücke $\pm \frac{1272}{163}$, $\pm \frac{3288}{125}$, woraus man dieselben Factoren ableitet wie oben. — Wer mehr Beispiele wünscht, möge Artikel 328 zu Rate ziehen, wo das erste Beispiel zeigt, dass $5428681 = 307 \cdot 17683$, das zweite, dass 4272943 eine Primzahl, das dritte, dass 997331 sicher aus mehreren Primzahlen zusammengesetzt ist.

Übrigens gestatteten es die Grenzen dieses Werkes nur, die Hauptmomente beider Methoden, die Factoren zu ermitteln, darzulegen; eine ausführlichere Untersuchung nebst mehreren Hülfstafeln und andern Hülfsmitteln behalten wir uns für eine andere Gelegenheit vor.