# Die schwierigeren Probleme der Zahlentheorie in systematischem Zusammenhange bearbeitet zur beabsichtigten Einreihung dieses Stoffes in den Unterricht der Prima höherer Lehranstalten.

Von

ROBERT JAENSCH,
Oberlehrer am Königl. Gymnasium zu Rastenburg.

---

Wissenschaftliche Beilage zum Programm des Königl. Gymnasiums zu Rastenburg. Michaelis 1876.

1876. Progr. Nr. 22.

# Die schwierigeren Probleme der Zahlentheorie in systematischem Zusammenhange, bearbeitet zur beabsichtigten Einreihung dieses Stoffes in den Unterricht der Prima höherer Lehranstalten.

## § 1.

**Geschichtliches.** In neuerer Zeit beschäftigte sich die Arithmetik mit der Qualität der Zahlen, nicht mit der Quantität, daher trifft die von Plato gegebene Erklärung, sie sei die Wissenschaft des Geraden und Ungeraden jedenfalls ihr Wesen, wenn auch die heutige Wissenschaft sich in Betrachtung und Auffassung der Eigenschaften der Zahlen andere und weitere Grenzen stellte und stellen musste. Auch ihr Namen deutet schon dieses Ziel an, denn Arithmos heisst die ganze Zahl; das Verhältniss der Grösse jedoch zur Einheit wurde durch Logos bezeichnet. Die neuere Geschichte der Mathematik knüpft sich überhaupt in allen ihren Punkten an die Trümmer des Alterthums an, indem man die Alten theils restituirte, theils commentirte. So schloss sich die Zahlenlehre an Diophant an, namentlich durch eine von einem Franzosen besorgte griechische Auflage. Während nun diese Wissenschaft als solche von den Alten erfunden ist und ihnen eine Menge Sätze bekannt waren, so scheinen ihnen doch meistens die Beweise für die Sätze gefehlt zu haben und wir finden nur wenige, z. B. den Beweis des Satzes: die Anzahl der Primzahlen ist unendlich gross. Der Jurist und berühmte Mathematiker Fermat unternahm es die Beweise herzuleiten. Leider ist von seinen Arbeiten nichts übrig geblieben, als eine Ausgabe des Diophant, in deren Noten er die Sätze angiebt; hier sind jedoch die Sätze, deren Beweis er zu haben behauptet, wohl zu trennen von denen, für welche er diese Behauptung nicht aufstellt; die ersteren sind alle richtig, während unter den anderen sich eine Anzahl falscher gefunden hat.

Die Auffindung der Beweise dieser von ihm angegebenen Sätze haben den späteren Mathematikern: Legendre, Lagrange, Euler, Gauss, Cauchy, Jacoby, Dirichlet viel Mühe und Aufwand von Scharfsinn gekostet, und zu einzelnen Beweisen gehören Disciplinen, welche den Alten wie Fermat durchaus unbekannt waren. Nachdem für einen der aufgestellten Sätze nur erst ein Beweis gefunden, gelang es später auch bald den Beweis vieler Sätze auf Sätze zurück zu führen, welche auch den minder Eingeweihten zugänglich und handlich waren, und es ist der Zweck der vorliegenden Arbeit, aus dem ganzen Gebiet dieser Wissenschaft einen systematisch geordneten Theil, der als Lehrstoff für die Prima einer höheren Lehranstalt fassbar ist, als abgerundetes Ganze hinzustellen und selbstverständlich bei der Beweisführung nur Mittel zu gebrauchen, welche diesem Kreise zu Gebote stehen.

§ 2.

**Erklärung:** Die Zahlen werden eingetheilt in Primzahlen und abgeleitete Zahlen. Primzahlen sind diejenigen, welche nur 1 und sich selbst als Factor haben; die abgeleiteten Zahlen sind Producte aus Potenzen von Primzahlen. Relative Primzahlen zu einander sind zwei Zahlen, welche keinen gemeinschaftlichen Factor haben.

§ 3.

**Die Anzahl der Primzahlen ist unendlich gross.**

Beweis 1. Es ist $\frac{1}{1-1/a} = 1 + \frac{1}{a} + \frac{1}{a^2} + \frac{1}{a^3} + \frac{1}{a^4} + \cdot\ \cdot\ \cdot\ \cdot$

$$\frac{1}{1-1/b} = 1 + \frac{1}{b} + \frac{1}{b^2} + \frac{1}{b^3} + \frac{1}{b^4} + \cdot\ \cdot\ \cdot\ \cdot$$

Entwickelt man mehrere dieser Gleichungen und multiplicirt sie alsdann mit einander, so erhält man auf der rechten Seite ein Aggregat von Gliedern, in denen sämmtliche Potenzen von $1/a$, $1/b$ etc. und die Combinationen der verschiedenen Potenzen von $1/a$, $1/b$ etc. und deren Potenzen enthalten sind. Setzt man nun für a, b etc. der Reihe nach die Primzahlen, so befinden sich auf der rechten Seite die reciproken Werthe sämmtlicher natürlicher Zahlen und nur diese, während die linke Seite in ein Product übergeht von Brüchen, deren Zähler die Primzahlen, deren Nenner die um 1 verkleinerten Primzahlen sind; man erhält also die Gleichung

$$\frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1} \cdot \cdot \cdot \cdot = 1 + 1/2 + 1/3 + 1/4 + 1/5 + \cdot\ \cdot\ \cdot\ \cdot$$

Der Logarithmus von $\frac{1}{1-x}$ ist gleich $x + \frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} \cdot \cdot \cdot$,

in welchen Ausdruck für x jeder ächte Bruch bis 1 gesetzt werden kann; die Substitution von 1 für x giebt links den Logarithmus von Unendlich, der unendlich gross ist, und rechts die Summe der reciproken Werthe der natürlichen Zahlen, welche mithin auch unendlich gross ist. Hierdurch ist bewiesen, dass das Product $\frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1} \cdot \cdot \cdot$ unendlich gross ist. Ein Product von mehreren Brüchen kann nur in zwei Fällen unendlich gross sein; entweder ist einer der Nenner gleich 0, oder einer der Zähler ist unendlich gross, von den Nennern ist aber keiner gleich 0, folglich muss

einer der Zähler unendlich gross sein; die Zähler sind die Primzahlen, folglich giebt es eine unendlich grosse Primzahl, d. h. die Anzahl der Primzahlen ist unendlich gross.

Beweis 2. Sei a die letzte angegebene Primzahl; multipliciren wir alsdann alle Primzahlen von 1 bis a mit einander und addiren wir 1 hinzu, so erhalten wir eine Zahl, welche keine der vorhergehenden Primzahlen als Factor hat, sondern durch eine der Primzahlen dividirt den Rest 1 giebt, folglich eine Primzahl ist.

§ 4.

Das Product a b ist gleich b a; ferner a mal b c ist $=$ a b mal c $=$ ac . b.

§ 5.

Wenn ein Product durch eine Zahl theilbar ist und es ist diese Zahl nicht in dem einen Factor enthalten, so steckt sie in dem andern oder die Factoren der Zahl sind einzeln in den Factoren des Products enthalten.

§ 6.

Wenn eine Primzahl ein Product theilt, so muss sie wenigstens in einem der Factoren enthalten sein, weil sie eben als Primzahl nicht in Factoren zerlegt werden kann. Es ist also auch keine Potenz einer Zahl durch eine Primzahl theilbar, wenn die Zahl nicht selbst theilbar ist durch die Primzahl.

§ 7.

Jede Zahl kann nur auf eine Art als Product von Primzahlen dargestellt werden.

§ 8.

Lassen zwei Zahlen durch m dividirt die Reste a und b, so lässt ihre Summe den Rest a + b, die Differenz den Rest a—b, das Product den Rest a b.

Beweis. Ist $x = m\,p + a$, $y = m\,q + b$, so ist

$$x + y = m\,(p + q) + a + b,$$

$$x - y = m\,(p - q) + a - b,$$

$$xy = m^2\,pg + m\,(pb + aq) + ab.$$

Es lauten also in den Ausdrücken rechts die Terme, welche den Factor m nicht enthalten der Reihe nach a + b, a − b, ab; d. h. bei der Division durch m bleiben die Reste a + b, a—b, ab. Hieraus folgt, dass die Differenz zweier Zahlen, welche durch p dividirt denselben Rest lassen, den Factor p enthält, d. h. den Rest 0 lässt.

§ 9.

Das Quadrat einer ungeraden Zahl lässt durch 8 dividirt den Rest 1; das Quadrat einer geraden hat den Factor 4.

Beweis. Die Form für eine ungerade Zahl ist 2a + 1, für eine gerade Zahl 2a. Ist nun $x = 2a + 1$, so ist $x^2 = 4a^2 + 4a + 1 = 4a\,(a + 1) + 1$, folglich hat, weil entweder a oder a + 1 den Factor 2 enthält, 4a (a + 1) den Factor 8; das Quadrat lässt also durch 8 dividirt den Rest 1.

Ist $x = 2a$, so ist $x^2 = 4a^2$, hat also mindetens den Factor 4.

Hieraus folgt, dass die Summa zweier Quadrate, wenn sie ungerade ist, durch 4 dividirt

den Rest 1 giebt, denn diese ungerade Summe ist nur zu erhalten durch die Addition eines geraden und eines ungeraden Quadrats. Wir erhalten also $4b^2 + 4a^2 + 4a + 1$, d. h. ein Aggregat, in dem jeder Term den Factor 4 hat mit Ausschluss des letzten, der gleich 1 ist.

§ 10.

Eine Zahl, welche durch 8 dividirt den Rest 7 lässt, kann nie die Summe dreier Quadrate sein.

Beweis: Das Quadrat der geraden Zahl lässt entweder den Rest 4 oder 0, das Quadrat der ungeraden Zahl den Rest 1. Sind alle drei Quadrate gerade, so erhalte ich als Rest

entweder $4 + 4 + 4$, d. h. 4,
oder $4 + 4 + 0$, d. h. 0,
oder $4 + 0 + 0$, d. h. 4,
oder $0 + 0 + 0$, d. h. 0.

Sind zwei gerade und eins ungerade, so erhalte ich

entweder $4 + 4 + 1$, d. h. 1,
oder $4 + 0 + 1$, d. h. 5,
oder $0 + 0 + 1$, d. h. 0.

Sind zwei ungerade und eins gerade, so erhalte ich

entweder $4 + 1 + 1$, d. h. 6,
oder $0 + 1 + 1$, d. h. 2.

Sind endlich alle drei ungerade, so erhalte ich als Rest $1 + 1 + 1$, d. h. 3; mithin in keinem Falle den Rest 7.

§ 11.

Dividirt man alle Zahlen durch die Primzahl p, so erhält man als Rest die Zahlen von 1 bis $p - 1$; rücksichtigt man nur auf das Zeichen des Restes und nicht auf seine Grösse, so erhält man die absolut kleinsten Reste und deren Zahl ist $\frac{p-1}{2}$, weil eben statt der Reste $p - 2$, $p - 3$, die Reste $-2$, $-3$, gesetzt werden können.

§ 12.

Multiplicirt man jeden der Reste in Bezug auf p, d. h. die Zahlen von 1 bis $p - 1$ mit einer zu p relativen Primzahl, mit a, so erhält man die Grössen a, 2a, 3a . . . $(p - 1)$ a; dividirt man nun jedes dieser Producte durch p, so erhält man wieder die Reste von 1 bis $p - 1$.

Beweis: Wären unter den Grössen a, 2a etc. zwei, welche durch p gleiche Reste lassen, so müsste nach § 8 deren Differenz durch p aufgehen; hiessen diese Grössen ka und la, so müsste $\frac{ka - la}{p}$ eine ganze Zahl sein; $\frac{ka - la}{p}$ ist $= a\left(\frac{k-l}{p}\right)$, a ist relative Primzahl zu p, also geht p nicht in a auf; k und l sind Reste von p, also $k - l$ kleiner als p, also ist p nicht in $k - l$ enthalten, folglich ist $a\left(\frac{k-l}{p}\right)$ keine ganze Zahl, mithin lassen ka und la nicht gleiche Reste.

Da endlich $p - 1$ Grössen sind, jede Grösse einen anderen Rest lässt, so erhalte ich $p - 1$ verschiedene Reste, d. h. die Reste von 1 bis $p - 1$; nur nicht in natürlicher Reihenfolge.

§ 13.

Ist a relative Primzahl zu p, so lässt $a^{p-1}$ durch p dividirt den Rest 1.

Beweis: Multiplicirt man jeden der Reste der Zahl p, d. h. 1, 2, 3 bis bis p — 1, mit a, so erhält man die Grössen a, 2a, 3a, bis (p — 1) a; diese lassen durch p dividirt nach § 13 die Reste 1 bis p — 1, oder das Product a. 2a. 3a. . (p — 1) a lässt denselben Rest wie 1. 2. 3. . . . (p—1); oder $a^{p-1}$ 1. 2. 3 (p — 1) — 1. 2. 3 — (p — 1) lässt den Rest 0.

$a^{p-1}$ . 1. 2. . . (p — 1) — 1. 2. 3. . . (p — 1) = 1. 2. 3. . . (p — 1) $(a^{p-1} - 1)$. Da nun 1. 2. 3. . . (p—1) nicht durch p aufgeht, weil p Primzahl ist, so muss $a^{p-1} - 1$ aufgehen, d. h. $a^{p-1}$ lässt durch p den Rest 1.

Beweis 2. Nach dem binomischen Lehrsatz ist $(1 + b)^p = 1 + p\,b + \frac{p \cdot (p-1)}{1 \cdot 2} b^2 + . . bp$; da die Binomial-Coefficienten ganze Zahlen sind, jeder derselben aber als Factor die Primzahl p enthält, so gehen alle Terme durch p auf mit Ausnahme des ersten und des letzten, es lässt also $(1 + b)^p$ denselben Rest wie $1 + b^p$; zieht man nun von $(1 + b)^p$ und $1 + b^p$ 1 + b ab, so müssen diese Differenzen wieder gleiche Reste lassen, also $(1 + b)^p - (1 + b)$ denselben Rest wie $1 + b^p - 1 - b$ oder $b^p - b$, d. h., die Differenzen der pten Potenz einer Zahl und die Zahl selbst lässt durch p denselben Rest wie die Differenz der pten Potenz der nächst kleineren Zahl und dieser Zahl; schliesst man so fort, so ergiebt sich, dass die pte Potenz einer Zahl weniger der Zahl selbst, durch p dividirt, denselben Rest giebt für alle Zahlen, also auch für 1. Nun giebt $1^p - 1$ den Rest o, folglich muss auch $a^p - a$, oder $a\,(a^{p-1} - 1)$ den Rest 0 geben, d. h., weil a durch p nicht theilbar ist, lässt der andere Factor $a^{p-1}$ durch p den Rest 1. Dieser wichtige Satz ist bekannt unter dem Namen des Fermat'schen Satzes.

§ 14.

Erhebt man alle Zahlen ins Quadrat und dividirt diese durch p, so erhält man $\frac{p-1}{2}$ verschiedene Reste.

Beweis. Da $a^2$ denselben Rest lässt wie $(p + a)^2 + (2p + a)^2, (3p + a)^2$ etc., so braucht man nur die Zahlen von 1 bis p — 1, d. h., die Reste von p zu untersuchen. Unter diesen lassen aber die Quadrate von 1 und p — 1, 2 und p — 2, 3 und p — 3 etc. durch p denselben Rest, es bleiben also die Grössen von 1 bis $\frac{p-1}{2}$ übrig. Wären unter diesen zwei, z. B. m und q, deren Quadrate gleiche Reste lassen, so müsste die Differenz $m^2 - q^2$ durch p aufgehen, $\frac{m^2 - q^2}{p}$ eine ganze Zahl sein; $m^2 - q^2$ ist $= (m + q)(m - q)$. m — q ist jedenfalls kleiner

als p, weil m und q kleiner als p, ja kleiner als $\frac{p-1}{2}$ sind, also steckt p nicht in m — q; ebenso ist m + q, weil m und q kleiner als $\frac{p-1}{2}$ sind, kleiner als p, also p nicht in m + q; da nun p weder in m — q noch in m + q enthalten ist, so ist $\frac{(m+q)(m-q)}{p}$ keine ganze Zahl, d. h., $m^2 - q^2$ ist nicht durch p theilbar, oder $m^2$ und $q^2$ lassen verschiedene Reste. Endlich weil nur $\frac{p-1}{2}$ Grössen sind, so sind auch nur $\frac{p-1}{2}$ solcher Reste; d. h., die Quadrate der Zahlen von 1 bis p — 1 lassen auch nur $\frac{p-1}{2}$ verschiedene Reste, also auch die Quadrate sämmtlicher Zahlen.

§ 15.

Lässt unter den Resten von 1 bis p — 1 das Quadrat eines Restes x durch p den Rest i, so giebt es noch einen zweiten, aber auch nur einen, nämlich p — x, dessen Quadrat denselben Rest i lässt.

Beweis. Lässt $x^2$ den Rest i und liesse auch $q^2$ den Rest i, so müsste $x^2 - q^2$ den Rest 0 lassen, also (x + q) (x — q) durch p aufgehen; x — q ist kleiner als p, kann also durch nicht aufgehen; x + q kann höchstens = 2p — 3 sein, unter den Zahlen von 1 bis 2p — 3 giebt es aber, weil p Primzahl ist, nur eine, nämlich p, welche durch x theilbar ist, also musste x + q = p sein, oder q = p — x.

§ 16.

Multiplicirt man 2 Zahlen x und y aus der Reihe der Reste von 1 bis p — 1 mit einander und dividirt das Product durch p, so erhält man einen Rest z; es giebt nun zu jeder Zahl x eine Zahl y und nur diese, mit welcher multiplicirt sie durch p den Rest z lässt.

Beweis. Gäbe es ausser der Zahl y noch eine Zahl t, mit welcher x multiplicirt den Rest z durch p liesse, so erhielten wir für xy und xt denselben Rest z, d. h. x y — x t oder x (y—t) gäbe den Rest 0; das ist aber nicht möglich, denn x geht durch p nicht auf, weil es Rest von p ist und y — t ebenfalls nicht, denn y — t ist kleiner als p, also auch Rest von p.

§ 17.

Unter den Zahlen grösser als p giebt es noch unendlich viele, welche mit x multiplicirt, durch p dividirt den Rest z lassen; sie haben aber alle die Form mp + y und es giebt zwischen je zwei Vielfachen von p, also zwischen 2p und 3p, oder 3p und 4p . . . rp und (r + 1) p immer nur eine solche.

Beweis. Giebt xy den Rest z, so giebt x (mp + y) = xmp + xy ebenfalls den Rest z; denn xmp geht durch p auf und es bleibt nur xy übrig; da ferner zwischen 1 und p — 1 nur die Zahl y dieser Bedingung Genüge leistete, so giebt es unter den Zahlen zwischen p und 2p welche p + 1, p + 2, p + 3 . . . 2p — 1, lauten, nur die Zahl p + y, welche dieser Bedingung Genüge leistet, denn nur diese giebt das Product xp + xy, während die anderen Producte

lauten $xp + x$, $xp + 2x$ u. s. w. und unter x, 2x, 3x bis $(p - 1)$, wie vorhin bewiesen, ist kein Product, welches durch p den Rest z lässt.

§ 18.

Multiplicire ich alle Reste der Primzahl p der Reihe nach mit einem derselben, so erhalte ich Producte, welche durch p die Reste 1 bis $p - 1$ lassen, wenn auch in veränderter Reihenfolge.

Beweis: Nach dem vorigen Satze giebt nur das Product der Reste x und y den Rest z und nie das Product der Reste x und s oder x und t; wenn man nun jede Zusammenstellung einen andern Rest giebt, so müssen wir, da $p - 1$ Reste vorhanden sind, wenn wir noch x mit x zusammenstellen, auch wieder $p - 1$ verschiedene Reste erhalten, d. h. die Reste von 1 bis $p - 1$.

§ 19.

Sämmtliche Reste der Zahl p lassen sich zu je zwei d. h. in $\frac{p-1}{2}$ Paare zusammenstellen, deren jedes Paar denselben Rest i giebt.

Beweis: Nach dem vorigen Satz erhalte ich sämmtliche Reste von 1 bis $p - 1$, wenn ich den beliebigen Rest x der Reihe nach mit allen Resten von 1 bis $p - 1$ multiplicire und durch p dividire. Es giebt also 1x, 2x, 3x . . . $p - 1$x, die Reste 1 bis $p - 1$, ebenso 1y. 2y. 3y . . . $(p - 1)$ y etc. . . . . 1z. 2z. 3z. . . . $(p - 1)$ z u. s. w.

Hebe ich den Rest i heraus, so ist in jeder Reihe von Producten eins, z. B. dx, fy, hz, welches den Rest i lässt. Jedes dieser Producte kommt zweimal vor, nämlich das Product dx in der Reihe x und xd in der Reihe d, oder fy in der Reihe y und yf in der Reihe f, alle übrigen sind verschieden, mithin erhalte ich, da $p - 1$ Reste sind, $\frac{p-1}{2}$ Producte verschiedener Factoren, welche alle den Rest i lassen. Die beiden Factoren eines solchen Products nennt man zugehörige Zahlen.

§ 20.

Das Product der Zahlen von 1 bis $p - 1$ giebt durch p dividirt den Rest $-m^{\frac{p-1}{2}}$ oder $m^{\frac{p-1}{2}}$ je nachdem unter den Resten von 1 bis $p - 1$ sich eine Zahl befindet, deren Quadrat den Rest m giebt oder nicht; für m kann jede der Zahlen 1 bis $p - 1$ gesetzt werden.

Beweis: Da nach dem vorhergehenden Satze der Rest x stets mit einem solchen Rest y aus der Reihe 1 bis $p - 1$ multiplicirt werden kann, dass das Product den Rest m giebt und wir das Gleiche mit den Resten y, z u. s. w. machen können, d. h. da wir $\frac{p-1}{2}$ Paare haben, deren jedes den Rest m lässt, so wird das Product aller dieser Paare als Rest ein Product aus lauter Factoren m lassen, wenn $x^2$ nicht den Rest m lässt. Die Anzahl dieser Factoren m ist gleich der Anzahl der Paare; die Anzahl dieser ist $= \frac{p-1}{2}$, also hat das Product den Rest $m^{\frac{p-1}{2}}$

Die Factoren in den einzelnen Paaren waren aber alle von einander verschieden und zwar die Reste von 1 bis p — 1, also giebt das Product der Paare auch das Product 1. 2. 3. . . . p — 1.

Mithin giebt das Product 1. 2. 3. . . . p — 1 durch p den Rest $m^{\frac{p \cdot 1}{2}}$. Was von dem Reste m gilt, gilt von jedem Reste nach dem vorhergehenden Satze, also giebt das Product 1 bis p — 1 den Rest $m^{\frac{p-1}{2}}$, wo für m jede Zahl von 1 bis p — 1 gesetzt werden kann, wenn $x^2$ nicht den Rest m lässt. Lässt aber $x^2$ den Rest m, so lässt auch $(p - x)^2$ den Rest m und das Product x (p — x) den Rest — m. Da nach dem Vorstehenden jedes der anderen Producte, deren Zahl $\frac{p-3}{2}$ ist, den Rest m lässt, so lässt das Product aller Producte incl. x (p — x) den Rest $(m^{\frac{p-3}{2}})$ (— m) oder den Rest $-m^{\frac{p-1}{2}}$. Dieser Satz ist das erweiterte Wilson'sche Theorem.

## § 21.

Das Product der Zahlen 1 bis p — 1 giebt durch p dividirt den Rest — 1. Wilson'sches Theorem.

Beweis: Das Product der Zahlen von 1 bis p — 1 giebt nach dem Vorigen den Rest $m^{\frac{p-1}{2}}$, wenn das Quadrat keiner Zahl den Rest m giebt und den Rest $-m^{\frac{p-1}{2}}$, wenn ein solcher vorhanden ist. Nun giebt das Quadrat des Restes 1, also $1^2$ den Rest 1 für jedes p, also giebt 1. 2. 3 . . . (p — 1) für jedes p den Rest $-1^{\frac{p-1}{2}}$, d. h. — 1.

## § 22.

Eine andere Form des Wilson'schen Theorems: Theile ich die Zahlen von 1 bis p — 1 in 2 Abtheilungen 1 . . . $\frac{p-1}{2}$ und $\frac{p+1}{2}$ . . . p — 1 und setze ich sie folgendermassen unter einander:

1. 2. 3. . . . $\frac{p-3}{2}$ $\frac{p-1}{2}$

(p — 1), (p — 2) $\frac{p+3}{2}$ $\frac{p+1}{2}$

und multiplicire ich je zwei unter einander stehende, so erhalte ich das Product:

1. (p — 1). 2. (p — 2). 3. (p — 3) . . . $\frac{p-3}{2}$ $\frac{p+3}{2}$ $\frac{p-1}{2}$ $\frac{p+1}{2}$. Da 1 (p — 1) den Rest — $1^2$, 2. (p — 2) den Rest — $2^2$ etc., ferner $(\frac{p-1}{2})$ $(\frac{p+1}{2})$ den Rest $\frac{p^2-1^2}{4}$ oder — $\frac{p^2+1}{4}$ oder den Rest — $\frac{p^2-2p+1}{4}$, d. h. den Rest — $(\frac{p-1}{2})^2$, und $\frac{p-3}{2}$

$\frac{p+3}{2}$ den Rest $\frac{p^2-3^2}{4}$ oder $-\frac{p^2+3^2}{4}$ oder $-\frac{p^2-6p+3^2}{4}$ d. h. den Rest $-\left(\frac{p-3}{2}\right)^2$.

giebt, so lässt das obige Product den Rest $-1^2 . -2^2 . -3^2 . -4^2$ bis $-\left(\frac{p-3}{2}\right)^2 . -\left(\frac{p-1}{2}\right)^2$

Aus jedem dieser $\frac{p-1}{2}$ Factoren kann ich den Factor $-1$ herausheben, also aus dem ganzen Product den Factor $(-1)^{\frac{p-1}{2}}$ und wir haben dann: das Product $1^2, 2^2, 3^2 \ldots \left(\frac{p-1}{2}\right)^2$ $(-1)^{\frac{p-1}{2}}$ lässt denselben Rest als das Product $1.2.3 \ldots p-1$. Das Product $1.2.3 \ldots p-1$ lässt aber den Rest $-1$, also lässt $(-1)^{\frac{p-1}{2}}$ $1^2, 2^2, 3^2 \ldots \left(\frac{p-3}{2}\right)^2 \left(\frac{p-1}{2}\right)^2$ den Rest $-1$. Hieraus folgt, dass $1^2, 2^2, 3^2 \left(\frac{p-1}{2}\right)^2$ den Rest $-1$ lässt, wenn $(-1)^{\frac{p-1}{2}} = +1$, und den Rest $+1$, wenn $(-1)^{\frac{p-1}{2}} = -1$ ist; d. h. wenn $\frac{p-1}{2}$ gerade oder wenn $\frac{p-1}{2}$ ungerade ist. $\frac{p-1}{2}$ ist gerade, wenn $p = 4n+1$ oder $4n-3$ und ungerade, wenn $p = 4n-1$ oder $4n+3$ ist. Oder das Product $1^2, 2^2, 3^2 \ldots \left(\frac{p-1}{2}\right)^2$ lässt den Rest $-1$, wenn p von der Form $4n+1$ oder $4n-3$, den Rest $+1$, wenn p von der Form $4n-1$ oder $4n+3$ ist.

1. Beispiel: 17 hat die Form $4n+1$, also muss $1^2, 2^2 \ldots 8^2$ den Rest $-1$ lassen; es lässt

| | | | | | |
|---|---|---|---|---|---|
| $1^2$ | den Rest | 1 | $5^2$ | den Rest | 8 |
| $2^2$ | „ „ | 4 | $6^2$ | „ „ | 2 |
| $3^2$ | „ „ | 9 | $7^2$ | „ „ | 15 |
| $4^2$ | „ „ | 16 | $8^2$ | „ „ | 13 |

ferner lässt $1 \times 8$ den Rest 8 $\quad 9 \times 15$ den Rest 16

$4 \times 2$ „ „ 8 $\quad 16 \times 13$ „ „ 4

dann lässt $8 \times 16$ „ „ 9

$8 \times 4$ „ „ 15

und endlich $9 \times 15$ „ „ 16 oder $-1$.

2. Beispiel. 19 hat die Form $4n+3$, es lässt

| | | | | | |
|---|---|---|---|---|---|
| $1^2$ | den Rest | 1 | $6^2$ | den Rest | 17 |
| $2^2$ | „ „ | 4 | $7^2$ | „ „ | 11 |
| $3^2$ | „ „ | 9 | $8^2$ | „ „ | 7 |
| $4^2$ | „ „ | 16 | $9^2$ | „ „ | 5 |
| $5^2$ | „ „ | 6 | | | |

ferner $1 \times 17$ den Rest 17 $\quad 9 \times 7$ den Rest 6

$4 \times 11$ „ „ 6 $\quad 16 \times 5$ „ „ 4

und 6 „ „ 6

ferner $17 \times 6$ den Rest 7
$6 \times 4$ „ „ 5
$6 \times 6$ „ „ 6
und endlich $7 \times 5$ „ „ 16 und $16 + 6$ den Rest $+ 1$.

Zusatz. Da nach dem eben Gesagten $1^2, 2^2 \ldots \left(\frac{p-1}{2}\right)^2$ den Rest $-1$ giebt, wenn p die Form $4n + 1$ hat, so können wir, wenn wir für $1^2, 2^2 \left(\frac{p-1}{2}\right)^2$ $a^2$ setzen, sagen, es giebt, wenn p die Form $4n + 1$ hat, stets eine Zahl, deren Quadrat den Rest 1 lässt, oder es giebt eine Zahl a die so beschaffen ist, dass $\frac{a^2 + 1}{p}$ eine ganze Zahl ist.

Da ferner $1^2, 2^2 \ldots \left(\frac{p-1}{2}\right)^2$ den Rest $+ 1$ giebt, wenn p von der Form $4n - 1$ ist, so wird, wenn wir wieder für $1^2, 2^2 \ldots \left(\frac{p-1}{2}\right)^2$ $a^2$ setzen, $a^2$ durch p den Rest $+ 1$ lassen, wenn p die Form $4n - 1$ hat; d. h. es wird eine Zahl geben, die so beschaffen ist, dass $\frac{a^2 - 1}{p}$ eine ganze Zahl ist, d. h. $\frac{a - 1 \,.\, a + 1}{p}$ ist durch p theilbar; d. h. wenn p eine Primzahl von der Form $4n - 1$ ist, und $a^2$ den Rest $+ 1$ durch p lässst, so lässt $\frac{a}{p}$ entweder den Rest $+ 1$ oder $- 1$.

§ 23.

Befindet sich unter den Zahlen von 1 bis $p - 1$ eine Zahl deren Quadrat durch p den Rest i giebt, so nennt man i einen quadratischen Rest von p, residuum quadraticum.

§ 24.

Die Frage, ob i quadratischer Rest oder Nichtrest von p ist, lässt sich immer auf die Frage zurückführen, ob $i^{\frac{p-1}{2}}$ den Rest $+ 1$ oder $- 1$ giebt.

Beweis. Nach § 22 giebt das Product aller Zahlen von 1 bis $p - 1$ durch p den Rest $i^{\frac{p-1}{2}}$, wenn das Quadrat keiner der Zahlen von 1 bis $p - 1$ den Rest i lässt und den Rest $- i^{\frac{p-1}{2}}$, wenn das Quadrat einer der Zahlen den Rest i lässt. Da aber nach dem Wilson'schen Theorem das Product aller Zahlen von 1 bis $p - 1$ unter allen Bedingungen den Rest $- 1$ lässt, so wird $i^{\frac{p-1}{2}}$ den Rest $- 1$ lassen, wenn i quadratischer Nichtrest, und $- i^{\frac{p-1}{2}}$ den Rest $- 1$, wenn i quadratischer Rest ist. Wenn aber $- i^{\frac{p-1}{2}}$ den Rest $- 1$ lässt, so lässt $i^{\frac{p-1}{2}}$ den Rest $+ 1$, also lässt $i^{\frac{p-1}{2}}$ den Rest $- 1$, wenn i quadratischer Nichtrest und den Rest $+ 1$, wenn i quadratischer Rest ist.

Es soll nun die Form derjenigen Zahlen untersucht werden, von denen eine bestimmte Zahl quadratischer Rest ist von p.

+ 1 ist quadratischer Rest von jeder Zahl.

§ 25.

— 1 ist quadratischer Rest der Zahlen von der Form 4n + 1, aber niemals der Zahlen von der Form 4n + 3 oder was dasselbe ist von der Form 4n — 1.

Beweis. Nach § 24 ist i quadratischer Rest von p, wenn $i^{\frac{p-1}{2}}$ durch p den Rest + 1 giebt; demnach ist — 1 quadratischer Rest von p, wenn $(-1)^{\frac{p-1}{2}}$ den Rest + 1 lässt, oder was dasselbe ist, wenn $(-1)^{\frac{p-1}{2}}$ gleich + 1 ist, d. h. wenn $\frac{p-1}{2} = 2n$ ist. Ist $\frac{p-1}{2} = 2n$, so ist $p - 1 = 4n$, $p = 4n + 1$, aber niemals $= 4n + 3$ oder $4n - 1$.

Nach § 25 soll — 1 quadratischer Rest sein der Zahlen von der Form 4n + 1, nicht aber der Zahlen von der Form 4n — 1. 13 hat die Form 4n + 1, also muss — 1 quadratischer Rest sein von 13 und dies ist der Fall, denn $5^2$ und $8^2$ geben beide den Rest — 1. 19 hat die Form 4n — 1 oder 4n — 3 und keines der Quadrate der Zahlen von 1 bis 18 giebt den Rest — 1.

§ 26.

2 ist quadratischer Rest der Zahlen von der Form 8n + 1, aber niemals von der Form 8n + 3.

Die Frage, ob 2 quadratischer Rest ist oder nicht, ist beantwortet durch die Frage, ob $2^{\frac{p-1}{2}}$ den Rest + 1 oder — 1 lässt. Bezeichnen wir zuerst den Rest des Products von $1 \ldots \frac{p-1}{2}$ mit r; denselben Rest r erhalte ich auf anderem Wege. Multiplicire ich alle Zahlen von 1 bis $p/_4$ mit 2, so erhalte ich die geraden Zahlen zwischen o bis $p/_2$; multiplicire ich die Zahlen zwischen $p/_4$ und $p/_2$ mit 2, so erhalte ich die geraden Zahlen zwischen $p/_2$ und p; ziehe ich diese von p ab, suche die absolut kleinsten Reste von p und multiplicire jeden derselben mit — 1, so erhalte ich die ungeraden Zahlen zwischen 0 und $p/_2$. Im Ganzen erhalte ich also die Reste von $1 - \frac{p-1}{2}$, wenn ich jede der Zahlen von $1 - \frac{p-1}{2}$ mit 2 und ausserdem noch alle Zahlen zwischen $p/_4 - p/_2$ mit — 1 multiplicire. Ist nun die Anzahl der Zahlen zwischen $p/_4$ und $p/_2 = q$, so habe ich im Ganzen multiplicirt mit $(-1)^q$. Wir sind also zu dem Resultat gekommen, dass das Product $\left(1 \ldots \frac{p-1}{2}\right)$ denselben Rest giebt wie $\left(1 \ldots \frac{p-1}{2}\right) 2^{\frac{p-1}{2}} (-1)^q$; ihre Differenz muss also den Rest o geben. Statt dieser Differenz kann ich schreiben $\left\{2^{\frac{p-1}{2}} (-1)^q - 1\right\} \left(1.2.3 \ldots \frac{p-1}{2}\right)$ und wenn dieses Product den Rest o geben soll, so muss $2^{\frac{p-1}{2}} (-1)^q$ den Rest 1 geben. $(-1)^q$ giebt den Rest + 1 oder den Rest — 1, je nachdem

q gerade oder ungerade ist; da $2^{\frac{p-1}{2}} (-1)^q$ den Rest 1 geben soll, so muss also $2^{\frac{p-1}{2}}$ den Rest + 1 geben, wenn q gerade ist, und den Rest — 1, wenn q ungerade ist. Demnach ist die Frage, ob 2 quadratischer Rest ist, zurückgeführt auf die Frage, ob q eine gerade oder ungerade Zahl ist, d. h., ob die Anzahl der Zahlen zwischen $p/_4$ und $p/_2$ eine gerade oder ungerade ist. Ist nun p von der Form 8n + 1, so haben wir nach dem eben Gesagten nur zu berücksichtigen die Zahlen zwischen o und $p/_2$, d. h. die Zahlen von 1, 2, 3 . . . 4n, und von diesen wurden nur die Zahlen von 2n + 1 bis 4n gezählt, diese Anzahl ist aber gerade, folglich ist q gerade, folglich giebt $2^{\frac{p-1}{2}}$ den Rest + 1, folglich ist 2 quadratischer Rest der Zahlen von der Form 8n + 1. Ist p von der Form 8n + 3, so haben wir die Anzahl der Zahlen zu bestimmen zunächst von o bis $p/_2$ d. h. von 1 bis 4n + 1 und dann die Anzahl der Zahlen von $p/_4$ bis $p/_2$, d. h. von 2n + 1 bis 4u + 1, diese Anzahl ist stets ungerade, also q ungerade, also giebt $2^{\frac{p-1}{2}}$ den Rest — 1, also ist 2 quadratischer Nichtrest dieser Zahlen.

Ist p von der Form 8n + 5 oder, was dasselbe ist, 8n — 3, so haben wir bis $p/_2$ 4n + 2 Zahlen und von $p/_4$ — $p/_2$, d. h. von 2n + 1 bis 4n + 2 eine ungerade Anzahl Zahlen; d. h. q ist ungerade, $2^{\frac{p-1}{2}}$ giebt den Rest — 1, also ist 2 quadratischer Nichtrest dieser Zahlen.

Ist p endlich von der Form 8n + 7 oder, was dasselbe ist von der Form 8n — 1, so haben wir bis $p/_2$ 4n + 3 Zahlen und von $p/_4$ bis $p/_2$, d. h. von 2n + 2 bis 4n + 3 eine gerade Anzahl Zahlen; d. h. q ist gerade, $2^{\frac{p-1}{2}}$ lässt den Rest + 1, oder 2 ist quadratischer Rest.

Es ist also 2 quadratischer Rest der Zahlen an der Form 8n + 1 und 8n + 7, oder von der Form 8n + 1, und quadratischer Nichtrest von den Zahlen von der Form 8n + 3 und 8n + 5 oder $8n \pm 3$.

## § 27.

— 2 ist quadratischer Rest der Primzahlen von der Form 8n + 1 und 8n + 3, quadratischer Nichtrest der Primzahlen von der 8n + 5 und 8n — 7 oder 8n — 3 und 8n — 1.

Beweis. Wir wollen den Rest, welchen das Product $-1.-2.-3. . .-\left(\frac{p-1}{2}\right)$ lässt, mit r bezeichnen; denselben Rest erhalte ich auf folgende Weise: Multiplicire ich jede der Zahlen von o bis $p/_4$ mit — 2, so erhalte ich die negativen geraden Zahlen von o bis $p/_2$, multiplicire ich die Zahlen von $p/_4$ — $p/_2$ mit — 2, so erhalte ich die negative geraden Zahlen zwischen $p/_2$ und p, suche ich zu diesem die absolut kleinsten Reste, so erhalte ich als solche die positiven ungeraden Zahlen zwischen o und $p/_2$, will ich diese negativ haben, so muss ich jede derselben noch mit (— 1) d. h. im Ganzen mit $(-1)^q$ multipliciren, wo q gleich der Anzahl dieser Reste

d. h. gleich der Anzahl der Zahlen zwischen $p/_4$ und $p/_2$ ist. Es lassen also die beiden Producte $(-1)(-2)(-3)\ldots-\binom{(p-1)}{2}$ und $(1)(2)\ldots\binom{(p-1)}{2}(-2)^{\frac{p-1}{2}}(-1)^q$ oder die Producte $(1.2.3.\ldots^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}$ und $\left(1.2.3-\frac{p-1}{2}\right)(-2)^{\frac{p-1}{2}}(-1)^q$ denselben Rest r, folglich lässt die Differenz $\left(1.2.3.\ldots\frac{p-1}{2}\right)\left\{(-1)^{\frac{p-1}{2}}-(-2)^{\frac{p-1}{2}}(-1)^q\right\}$ den Rest o. Diese Differenz lässt aber nur den Rest o, wenn $(-1)^{\frac{p-1}{2}}-(-2)^{\frac{p-1}{2}}(-1)^q$ oder $(-1)^q\left\{(-1)^{\frac{p-1}{2}-q}-(-2)^{\frac{p-1}{2}}\right\}$ den Rest o lässt, und dieses Product wieder nur den Rest o, wenn $(-1)^{\frac{p-1}{2}-q}$ denselben Rest lässt wie $(-2)^{\frac{p-1}{2}}\cdot(-1)^{\frac{p-1}{2}-q}$ lässt aber nur den Rest + 1 oder — 1, je nachdem $\frac{p-1}{2}-q$ eine gerade oder ungerade Zahl ist, also wird auch $(-2)^{\frac{p-1}{2}}$ den Rest + 1 oder — 1 lassen, d. h. — 2 wird quadratischer Rest oder Nichtrest sein, je nachdem $\frac{p-1}{2}-q$ gerade oder ungerade ist.

Geben wir der Zahl p die Form 8n + 1, so ist die Anzahl der Zahlen von 1 bis $p/_2$ . . 4n und die Anzahl der Zahlen von $p/_4$ bis $p/_2$, d. h. von 2n + 1 bis 4n = 2n, also heisst der Exponent $\frac{8n+1-1}{2}-2n=2n$, d. h. er ist gerade; $(-1)^{\frac{p-1}{2}-q}$ ist also = + 1, d. h. $(-2)^{\frac{p-1}{2}}$ lässt den Rest + 1, also ist — 2 quadratischer Rest der Zahlen von der Form 8n + 1. Hat p die Form 8n + 3, so sind von o bis $p/_2$ 4n + 1 Zahlen und von $p/_4$ bis $p/_2$ oder von 2n + 1 bis 4n + 1 2n + 1 Zahlen, d. h. q ist = 2n + 1 und $\frac{p-1}{2}-q=\frac{8n+3-1}{2}-(2n+1)=4n+1-2n-1=2n$ d. h. gerade, folglich ist $(-1)^{\frac{p-1}{2}-q}=+1$, also lässt $(-2)^{\frac{p-1}{2}}$ den Rest + 1, und — 2 ist quadratischer Rest der Zahlen von der Form 8n + 3. Ist p = 8n + 5 oder = 8n — 3, so sind von o bis $p/_2$ 4n + 2, und von $p/_4$ — $p/_2$ oder von 2n + 2 bis 4n + 2 2n + 1 Zahlen, d. h. q ist = 2n + 1, folglich ist $\frac{p-1}{2}-q=\frac{8n+5-1}{2}-(2n+1)=4n+2-2n-1=4n+1$ d. h. ungerade, dann ist $(-1)^{\frac{p-1}{2}+q}=-1$, also lässt $(-2)^{\frac{p-1}{2}}$ den Rest — 1, also ist — 2 quadratischer Nichtrest der Zahlen von der Form 8n + 5 oder 8n — 3. Setzen wir für p die Form 8n + 7 oder 8n — 1, so sind von o bis $p/_2$ 4n + 3 und von $p/_4$ bis $p/_2$ oder

von $2n + 2$ bis $4n + 3$ $2n + 2$ Zahlen, d. h. q ist $= 2n + 2$, oder $\frac{p-1}{2} - q$ ist $= \frac{8n + 7 - 1}{2} - (2n + 2) = 4n + 3 - 2n - 2 = 2n + 1$ d. h. ungerade, also $(-1)^{\frac{p-1}{2} - q} = -1$ d. h. $(-2)^{\frac{p-1}{2}}$ lässt den Rest $-1$, oder $-2$ ist quadratischer Nichtrest der Zahlen von der Form $8n + 7$ oder $8n - 1$. Es ist also $-2$ quadratischer Rest der Zahlen von der Form $8n + 1$ und $8n + 3$ und quadratischer Nichtrest der Zahlen von der Form $8n + 5$ und $8n + 7$ oder $8n - 3$ und $8n - 1$.

Zusatz: $\pm 2$ ist quadratischer Rest der Zahlen von der Form $8n + 1$,

$+ 2$ ist quadratischer Nichtrest der Zahlen von der Form $8n + 5$ oder $8n - 3$,

$+ 2$ ist quadratischer Nichtrest, $- 2$ quadratischer Rest der Zahl von der Form $8n + 3$,

$+ 2$ ist quadratischer Rest, $- 2$ quadratischer Nichtrest der Zahlen von der Form $8n + 7$ oder $8n - 1$.

## § 28.

3 ist quadratischer Rest der Zahlen von der Form $12n + 1$ und $12n + 11$ oder $12n \pm 1$ und quadratischer Nichtrest der Zahlen von der Form $12n + 5$ und $12n + 7$ oder $12n \pm 5$.

Beweis: Wir bezeichnen wieder den Rest des Products $1. 2. - \frac{p-1}{2}$ in Bezug auf p durch r. Denselben Rest erhalten wir auf folgende Weise: theilen wir die Zahlen von o bis $p/_2$ in 3 Abtheilungen von o bis $p/_6$ in $p/_6$ bis $p/_3$ und von $p/_3$ bis $p/_2$ und multipliciren wir dann jede dieser Zahlen mit 3, d. h. das ganze Product mit $3^{\frac{p-1}{2}}$, so erhalten wir Zahlen zwischen o und $p/_2$, $p/_2$ und p, p und $3/_2$ p. Ziehen wir die Zahlen zwischen $p/_2$ und p von p ab und multipliciren jede derselben mit $(-1)$, im Ganzen also mit $(-1)^q$, wo q die Anzahl der Zahlen zwischen $p/_6$ und $p/_3$ ist, so erhalten wir ein zweites Drittel der Zahlen zwischen o und $p/_2$ und an Stelle des dritten Drittels dieser Zahlen treten die Reste der erhaltenen Zahlen zwischen p und $3/_2$ p.

Auf diese Weise haben wir ein Product mit demselben Rest und dieses Product lautet:

$$1. 2. 3. \frac{p-1}{2} \; 3^{\frac{p-1}{2}} \; (-1)^q$$

Die Differenz

$$1. 2. 3. . . \frac{p-1}{2} \; 3^{\frac{p-1}{2}} \; (-1)^q - 1. 2. 3. \frac{p-1}{2}$$

$$\text{oder } 1. 2. 3. \frac{p-1}{2} \left\{ 3^{\frac{p-1}{2}} \cdot (-1)^q - 1 \right\}$$

muss also den Rest o geben, d. h. $3^{\frac{p-1}{2}}(-1)^{q}$ muss den Rest 1 geben.

$(-1)^{q}$ ist $= +1$, wenn q gerade und $= -1$, wenn q ungerade; folglich wird $3^{\frac{p-1}{2}}$ den Rest $+1$ lassen, wenn q gerade, und $-1$ wenn q ungerade, oder 3 ist quadratischer Rest, wenn q gerade und quadratischer Nichtrest, wenn q ungerade.

Geben wir p die Form $12n + 1$, so haben wir zwischen o und $p/_2$ $6n$ Zahlen, also in jeder der 3 Abtheilungen $2n$ Zahlen, d. h. q ist gerade und 3 ist quadratischer Rest der Zahlen von der Form $12n + 1$.

Ist $p = 12n + 5$, so haben wir von o bis $p/_2$ $6n + 2$ Zahlen und diese vertheilen sich auf die 3 Abtheilungen zu $2n$, $2n + 1$ und $2n + 1$; folglich ist q ungerade und 3 quadratischer Nichtrest.

Ist $p = 12n + 7$ oder $12n - 5$, so ist die Anzahl der Zahlen zwischen o und $p/_2$ $6n + 3$, und es befinden sich in jeder der 3 Abtheilungen $2n + 1$ Zahlen, also ist q wieder ungerade und 3 quadratischer Nichtrest.

Hat endlich p die Form $12n + 11$ oder $12n - 1$, so ist die Anzahl der Zahlen zwischen o und $p/_2$ $6n + 5$ und wir haben in den 3 Abtheilungen resp. $2n + 1$, $2n + 2$ und $2n + 2$ Zahlen, folglich ist q gerade also 3 quadratischer Rest.

Mithin ist 3 quadratischer Rest der Zahlen von der Form $12n + 1$ und $12n + 11$ oder $12n \pm 1$ und quadratischer Nichtrest der Zahlen von der Form $12n + 5$ und $12 + 7$ oder $12n \pm 5$.

## § 29.

$-3$ ist quadratischer Rest der Zahlen von der Form $12n + 1$ und $12n + 7$ oder $12n + 1$ und $12n - 5$ und quadratischer Nichtrest der Zahlen von der Form $12n + 5$ und $12n + 11$ oder $12n + 5$ und $12n - 1$.

Beweis: Um wieder 2 Producte zu erhalten, welche denselben Rest o lassen, multiplicire ich jede der Zahlen von 1 bis $\frac{p-1}{2}$ mit $(-1)$, d. h. das ganze Product mit $(-1)^{\frac{p-1}{2}}$. Dann multiplicire ich jede der Zahlen von o bis $\frac{p-1}{2}$ mit $(-3)$ also im Ganzen mit $(-3)^{\frac{p-1}{2}}$ theile die Zahlen wieder in 3 Abtheilungen, deren erste Zahlen zwischen o und $p/_2$ enthält, deren zweite Zahlen zwischen $p/_2$ und p, welche ich, um Zahlen zwischen o und $p/_2$ zu erhalten, von p abziehen oder mit $(-1)$ multipliciren muss, also mit $(-1)^{q}$, wo q die Anzahl der Zahlen zwischen $p/_0$ und $p/_3$ ist, und deren dritte endlich Zahlen zwischen p und $^3/_2$ p enthält, welche Reste lassen zwischen o und $p/_2$. Es lassen also folgende 2 Producte gleiche Reste

$(-1)^{\frac{p-1}{2}}$ 1. 2. 3 $\frac{p-1}{2}$ und $(-1)^{q}(-3)^{\frac{p-1}{2}}$ 1. 2. 3 $\frac{p-1}{2}$ oder die Differenz

$(-1)^{\frac{p-1}{2}} 1.2.3\ldots\frac{p-1}{2} - (-1)^q (-3)^{\frac{p-1}{2}} 1.2\ldots\frac{p-1}{2}$ oder

$\left(1.2.3\ldots\frac{p-1}{2}\right)\left\{(-1)^{\frac{p-1}{2}} - (-1)^q (-3)^{\frac{p-1}{2}}\right\}$ lässt den Rest o, oder

$(-1)^{\frac{p-1}{2}}$ und $(-1)^q (-3)^{\frac{p-1}{2}}$ lassen denselben Rest oder

$(-1)^{\frac{p-1}{2}} - (-1)^q (-3)^{\frac{p-1}{2}}$ d. h. $(-1)^q \left\{(-1)^{\frac{p-1}{2}-q} - (-3)^{\frac{p-1}{2}}\right\}$ den Rest o,

d. h. $(-1)^{\frac{p-1}{2}-q}$ und $(-3)^{\frac{p-1}{2}}$ denselben Rest.

$(-1)^{\frac{p-1}{2}-q}$ lässt den Rest + 1 oder — 1, je nachdem $\frac{p-1}{2} - q$ gerade oder ungerade ist, folglich lässt auch $(-3)^{\frac{p-1}{2}}$ den Rest + 1 oder — 1, je nachdem $\frac{p-1}{2} - q$ gerade oder ungerade ist, folglich lässt auch $(-3)^{\frac{p-1}{2}}$ den Rest + 1 oder — 1, je nachdem $\frac{p-1}{2} - q$ gerade oder ungerade ist, d. h. — 3 ist quadratischer Rest oder Nichtrest, je nachdem $\frac{p-1}{2} - q$ gerade oder ungerade ist.

Ist nun $p = 12n + 1$, so ist $\frac{p-1}{2}$ gleich 6n und in jeder der 3 Abtheilungen sind 2n Zahlen, also ist q gerade $\frac{p-1}{2} - q = \frac{12n+1-1}{2} - 2n = 4n$ und mithin 3 quadratischer Rest der Zahlen von der Form $12n + 1$.

Ist $p = 12n + 5$, so ist $\frac{p-1}{2} = 6n + 2$ und die Zahlen vertheilen sich auf die 3 Abtheilungen zu 2n, 2n + 1, 2n + 1, folglich ist $\frac{p-1}{2} - q = \frac{12n+5-1}{2} - (2n+1)$ $= 6n + 2 - 2n - 1 = 4n + 1$, d. h. ungerade und (— 3) quadratischer Nichtrest.

Ist $p = 12n + 7$, so ist die Anzahl der Zahlen zwischen o und $p/_2$ $6n + 3$; es sind also in jeder Abtheilung $2n + 1$ Zahlen, mithin $q = 2n + 1$ und $\frac{p-1}{2} - q = \frac{12n+7-1}{2} - 2n - 1 = 6n + 3 - 2n - 1 = 4n + 2$, d. h. gerade, folglich (— 3) quadratischer Rest.

Ist p endlich $12n + 11$, so haben wir zwischen o und $p/_2$ $6n + 5$ Zahlen, also in den 3 Abtheilungen resp. $2n + 1$, $2n + 2$, $2n + 2$ Zahlen und es ist $\frac{p-1}{2} - q = \frac{12n+11-1}{2} - 2n - 2 = 6n + 5 - 2n - 2 = 4n + 3$, d. h. ungerade und (— 3) ist quadratischer Nichtrest.

— 3 ist demnach quadratischer Rest der Zahlen von der Form $12n + 1$ und $12n + 7$ und quadratischer Nichtrest der Zahlen von der Form $12n + 5$ und $12n + 11$, oder resp. der Zahlen von der Form $12n + 1$ und $12n - 5$, und $12n + 5$ und $12n - 1$.

Zusatz. $\pm 3$ sind quadratische Reste der Zahlen von der Form . . . . . $12n + 1$,

$\pm 3$ sind quadratische Nichtreste der Zahlen von der Form . . . . $12n + 5$,

$+ 3$ ist quadr. Rest und $(-3)$ quadr. Nichtrest der Zahlen von der Form $12n + 11$,

$+ 3$ ist quadr. Nichtrest und $(- 3)$ quadr. Rest der Zahlen von der Form $12n + 7$.

## § 30.

Um die Form der Zahlen zu bestimmen, zu denen 5 quadratischer Rest ist, müsste man die Zahlen von 0 bis $p/_2$ in fünf Abtheilungen theilen; alsdann sämmtliche Zahlen aller Abtheilungen mit 5 multipliciren und ausserdem noch die Zahlen der zweiten und vierten Abtheilung mit — 1, d. h. wenn wir die Anzahl der Zahlen dieser beiden Abtheilungen resp. mit q und s bezeichnen, mit $(- 1)^q$ und $(- 1)^s$; auf diese Weise wäre festgestellt, dass denselben Rest lassen

$$1.\ 2.\ \ldots\ \frac{p-1}{2} \text{ und } 1.\ \ldots\ \frac{p-1}{2} \cdot 5^{\frac{p-1}{2}} \cdot (-1)^q\ (-1)^s.$$

Es müsste demnach $1.\ 2.\ \ldots\ \frac{p-1}{2}\left\{1 - 5^{\frac{p-1}{2}} \cdot (-1)^q\ (-1)^s\right\}$ den Rest 0, oder

$5^{\frac{p-1}{2}} \cdot (-1)^q \cdot (-1)^s$ den Rest + 1 lassen, d. h. wenn $(-1)^{q+s} = +1$ ist, so lässt auch $5^{\frac{p-1}{2}}$ den Rest + 1, also ist 5 in diesem Falle quadratischer Rest, und ist $(-1)^{q+s} = -1$, so lässt auch $5^{\frac{p-1}{2}}$ den Rest — 1, und 5 ist quadratischer Nichtrest.

Wir hätten alsdann zu untersuchen die Zahlen von der Form

$20n + 1$, $20n + 3$, $20n + 7$, $20n + 9$, $20n + 11$, $20n + 13$, $20n + 17$ und $20n + 19$.

Im ersten Falle befänden sich in jeder Abtheilung $2n$ Zahlen, also sind q und s gerade.

Im zweiten Falle sind $10n + 1$ Zahlen, und zwar befinden sich in der ersten, zweiten, dritten und fünften Abtheilung je $2n$, in der vierten $2n + 1$ Zahlen, mithin ist $p + q$ ungerade.

Im dritten Falle sind $10n + 3$ Zahlen; es befinden sich in der ersten und vierten Abtheilung je $2n$, in der zweiten, dritten und fünften Abtheilung je $2n + 1$, mithin ist $q + s$ ungerade.

Im vierten Falle sind $10n + 4$ Zahlen, und es befinden sich in der ersten Abtheilung $2n$, in jeder der vier übrigen Abtheilungen $2n + 1$ Zahlen; mithin ist $q + s$ gerade.

Im fünften Falle sind $10n + 5$ Zahlen; in jeder Klasse befinden sich $2n + 1$ Zahlen, also ist $q + s$ gerade.

Im sechsten Falle sind $10n + 6$ Zahlen; es befinden sich in der vierten Abtheilung $2n + 2$, in den übrigen Abtheilungen je $2n + 1$ Zahlen, mithin ist $q + s$ ungerade.

Im siebenten Falle sind $10n + 8$ Zahlen; es befinden sich in der ersten und vierten Abtheilung je $2n + 1$, in der zweiten, dritten und fünften Abtheilung je $2n + 2$ Zahlen; mithin ist $q + s$ ungerade.

Im achten Falle sind $2n + 9$ Zahlen; in der ersten Abtheilung befinden sich $2n + 1$, in jeder der übrigen Abtheilungen $2n + 2$ Zahlen; mithin ist $q + s$ gerade.

Es ist also $q + s$ gerade für den Fall, dass die Zahl die Form hat: $20n + 1$, $20n + 9$, $20n + 11$, $20n + 19$, und ungerade bei den Zahlen von der Form $20n + 3$, $20n + 7$, $20n + 13$ und $20n + 17$.

Folglich ist in den Fällen 1, 4, 5 und 8, $(-1)^{q+s} = +1$, mithin muss $5^{\frac{p-1}{2}}$ in diesen Fällen den Rest $+1$ lassen, also 5 quadratischer Rest sein; in den Fällen 2, 3, 6, 7 ist $(-1)^{q+s} = -1$, also lässt auch $5^{\frac{p-1}{2}}$ den Rest $-1$, d. h. 5 ist quadratischer Nichtrest.

Also 5 ist quadratischer Rest der Zahlen von der Form

$$20n + 1.\quad 20n + 9.\quad 20n + 11.\quad 20n + 19, \text{ oder } 20n \pm 1.\quad 20n \pm 9,$$

und 5 ist quadratischer Nichtrest der Zahlen von der Form

$$20n + 3.\quad 20n + 7.\quad 20n - 13.\quad 20n + 17, \text{ oder } 20n \pm 3.\quad 20n \pm 7.$$

Auf diesem Wege ist leicht eine Verallgemeinerung des Vorgehens zu erzielen.

## § 31.

Die Anzahl der Factoren einer Zahl

$m = a^{\alpha} \cdot b^{\beta} \cdot c^{\gamma} \cdot d^{\delta} \cdot \ldots$ ist gleich $(\alpha + 1)\ (\beta + 1)\ (\gamma + 1)\ (\delta + 1)\ (\ldots)$

oder gleich dem Product der um 1 vergrösserten Exponenten der Primfactoren der Zahl.

Beweis: Entwickeln wir das Product

$$(1 + a + a^2 + \ldots a^{\alpha})\ (1 + b + b^2 + \ldots b^{\beta})\ (1 + c + c^2 + \ldots c^{\gamma})\ (1 + d + d^2 + \ldots d^{\delta}),$$

so erhalten wir in den einzelnen Termen die Combinationen von a, b, c, d zu je 1, je 2 . . bis zu je $\alpha + \beta + \gamma + \delta$, in denen a, b, c, d resp. mit $\alpha$, $\beta$, $\gamma$, $\delta$ maliger Wiederholung vorkommen. Jeder dieser Termen ist ein Factor der Zahl m, und das Aggregat dieser Terme enthält andererseits wieder sämmtliche mögliche Combinationen, also sämmtliche Factoren und nur Factoren der Zahl m. Die Anzahl dieser wird also gleich sein der Anzahl der Terme. Das Product $(1 + a + \ldots a^{\alpha})\ (1 + b + \ldots b^{\beta})$ hat aber $(1 + \alpha)\ (1 + \beta)$ Terme; multipliciren wir dieses mit $(1 + c + c^2 + \ldots c^{\gamma})$, so erhalten wir $(1 + \alpha)\ (1 + \beta)\ (1 + \gamma)$ Terme, und endlich durch Multiplication dieses Products mit $1 + \delta$ erhalten wir $(1 + \alpha)\ (1 + \beta)\ (1 + \gamma)\ (1 + \delta)$ Terme. Die Anzahl der Factoren ist mithin $= (\alpha + 1)\ (\beta + 1)\ (\gamma + 1)\ (\delta + 1)$ u. s. w.

Da jede Zahl ein Product von Potenzen der Primzahlen ist, so braucht man zur Beschaffung einer Tabelle der Factoren-Anzahl in diese nur aufzunehmen die Potenzen der Prim-

zahlen nebst ihrer Factoren-Anzahl; um nun die Factoren-Anzahl einer beliebigen Zahl zu erhalten, multiplicirt man mit einander die aus jenen Tabelle entnommenen Factoren-Anzahlen der zu der Zahl gehörigen Potenzen von Primzahlen.

## Tabelle.

Z. bedeutet Zahl, F.-A. Factoren-Anzahl.

| Z. | F.-A. | Z. | F.-A. |
|---|---|---|---|
| 1 | 1 | 25 | 3 |
| 2 | 2 | 27 | 4 |
| 3 | 2 | 29 | 2 |
| 4 | 3 | 31 | 2 |
| 5 | 2 | 32 | 6 |
| 7 | 2 | 37 | 2 |
| 8 | 4 | 41 | 2 |
| 9 | 3 | 43 | 2 |
| 11 | 2 | 47 | 2 |
| 13 | 2 | 49 | 3 |
| 16 | 5 | 53 | 2 |
| 17 | 2 | 59 | 2 |
| 19 | 2 | 61 | 2 |
| 23 | 2 | 64 | 7 |

Demnach wäre die Factoren-Anzahl von 34400, da diese Zahl gleich $2^5 . 5^2 . 43$ ist, $= 2 . 3 . 6$, welche Zahlen neben 32, 25 und 43 stehen.

§ 32.

Die Summe der Factoren einer Zahl

$$m = a^{\alpha}\, b^{\beta}\, c^{\gamma} \text{ ist } = \frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1} \cdot \frac{c^{\gamma+1} - 1}{c - 1} \cdot \ldots$$

Beweis. Da das Product $(1 + a + a^2 + \ldots . a^{\alpha})\,(1 + b + b^2 + \ldots . b^{\beta})\,(1 + c + c^2 + \ldots . c^{\gamma})\,(\ldots .)$ in seinen Termen sämmtliche Factoren und nur Factoren der Zahl m giebt, so wird die Summe aller dieser Terme gleich der Summe sämmtlicher Factoren sein. Die Summe dieser erhalte ich aber, wenn ich vor der Multiplication erst die Glieder jedes Factors $(1 + a + a^2 \ldots a^{\alpha})$ und $(1 + b + b^2 + \ldots b^{\beta}) \ldots .$ summire; jeder dieser Factoren ist aber eine geometrische Reihe mit resp. $\alpha + 1$, $\beta + 1 \ldots .$ Gliedern und den Quotienten a, b .... Das Summenglied s einer solchen Reihe ist $= a \frac{e^n - 1}{e - 1}$, wo a erstes Glied, n die Anzahl der Glieder und e der Quotient der Reihe ist. Also erhalte ich

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

Ist die Zahl eine Primzahl, so ist ihre Factoren-Summe = der Primzahl + 1; hat man die Zahl dargestellt als ein Product von Primzahl-Potenzen, so wird die Factoren-Summe gleich sein dem Product der Factoren-Summe dieser Primzahlpotenzen. Man hat also bei Aufstellung einer Tabelle in diese nur hineinzunehmen die Potenzen der Primzahlen.

## Tabelle.

Z. bedeutet Zahl, F.-S. Factoren-Summe.

| Z. | F.-S. | Z. | F.-S. |
|---|---|---|---|
| 1 | 1 | 25 | 31 |
| 2 | 3 | 27 | 40 |
| 3 | 4 | 29 | 30 |
| 4 | 7 | 31 | 32 |
| 5 | 6 | 32 | 63 |
| 7 | 8 | 37 | 38 |
| 8 | 15 | 41 | 42 |
| 9 | 13 | 43 | 44 |
| 11 | 12 | 47 | 48 |
| 13 | 14 | 49 | 57 |
| 16 | 31 | 53 | 54 |
| 17 | 18 | 59 | 60 |
| 19 | 20 | 61 | 62 |
| 23 | 24 | 64 | 127 |

Hiernach wäre die Factoren-Summe von 34400, welche Zahl $= 2^5 . 5^2 . 43$ ist, gleich dem Product der bei 32, 25 und 43 stehenden Zahlen, d. h. $= 63 . 31 . 44 . = 85932$.

Die Factoren-Anzahl sowohl als auch die Factoren-Summe befolgt ein höchst unregelmässiges Gesetz; es ist daher merkwürdig, dass diese Zahlen in der Analysis als Coefficienten vorkommen. Beide waren den Alten nicht fremd.

### § 33.

Eine vollkommene Zahl oder numerus perfectus ist eine solche, deren Factoren-Summe gleich dem Zweifachen der Zahl selbst ist. Die Formel für eine solche Zahl m würde lauten:

$$2\,(a\ b\ c)^{(\alpha\ \beta\ \gamma)} = \frac{a^{\alpha+1}-1}{a-1}\cdot\frac{b^{\beta+1}-1}{b-1}\cdot\frac{c^{\gamma+1}-1}{c-1}\cdot\cdot\cdot$$

Es wäre nun zu untersuchen, welche Werthe a, b, c, $\alpha$, $\beta$, $\gamma$ . . . annehmen müssen, um dieser Gleichung zu genügen. Nehmen wir den einfachsten Fall, und setzen b, c . . . = 1, so

würden wir den numerus perfectus $2a^{\alpha} = \frac{a^{\alpha+1} - 1}{a - 1}$ haben, und es fragt sich, für welche Werthe von a und $\alpha$ diese Gleichung gilt. Untersuchen wir zuerst die Gleichung für a = 2 d. h. die Gleichung $2.\ 2^{\alpha} = 2^{\alpha+1} - 1$, so finden wir, dass 2 nicht für a gelten kann, denn wir haben $2^{\alpha+1} = 2^{\alpha+1} - 1$ oder $0 = -1$. Setzen wir für a. 3 ein, so heisst die Gleichung $2.\ 3^{\alpha} = \frac{3^{\alpha+1} - 1}{2}$ oder $4.\ 3^{\alpha} = 3.\ 3^{\alpha} - 1$ oder $3^{\alpha} = -1$, welche Gleichung auch unmöglich ist, denn die Potenz einer positiven Grösse kann nie negativ werden. Und allgemein

es soll sein . . . . . $2a^{\alpha} = \frac{a^{\alpha+1} - 1}{a - 1}$

$$\text{oder } 2(a-1)\,a^{\alpha} = a^{\alpha+1} - 1$$

$$a^{\alpha}(2a - a - 2) = -1$$

$$a^{\alpha}(a - 2) = -1;$$

eine Gleichung, welche für positive Werthe von a unmöglich ist. Hieraus folgt, dass keine Potenz einer Primzahl ein numerus perfectus sein kann.

Betrachten wir den Fall $2a^{\alpha} b^{\beta} = \frac{a^{\alpha+1} - 1}{a - 1} \cdot \frac{b^{\beta+1} - 1}{b - 1}$ und setzen wir, um den einfachsten Fall zu erhalten, für $\alpha$ und $\beta$ . . . 1 ein, so heisst die Gleichung

$$2ab = \frac{a^2 - 1}{a - 1} \cdot \frac{b^2 - 1}{b - 1} = (a + 1)(b + 1)$$

$$\text{oder } 2ab = ab + a + b + 1$$

$$\text{oder } ab = a + b + 1$$

$$\text{oder } b(a - 1) = a + 1, \text{ d. h.}$$

$$b = \frac{a + 1}{a - 1}.$$

Der Bruch $\frac{a + 1}{a - 1}$ ist nur gleich einer ganzen Zahl, wenn a = 2 ist, und dann erhalten wir b = 3. Es ist also 2. 3 oder 6 eine vollkommene Zahl, und in der That ist auch 1 + 2 + 3 + 6 = 2. 6 = 12. Setzen wir $\alpha = 2$ und $\beta = 1$, so heisst die Gleichung

$$2a^2\,b = \frac{a^3-1}{a-1}\cdot\frac{b^2-1}{b-1} = (a^2+a+1)(b+1)$$

$$2a^2\,b = a^2\,b + a^2 + ab + a + b + 1$$

$$a^2\,b - ab - b = a^2 + a + 1$$

$$b = \frac{a^2+a+1}{a^2-a-1}.$$

$\frac{a^2+(a+1)}{a^2-(a+1)}$ kann nur für $a = 2$ eine ganze Zahl sein, weil dieselbe Zahl $a + 1$ im Zähler zu $a^2$ addirt und im Nenner abgezogen ist, und dann ist $b = 7$ und der numerus perfectus heisst $2^2 . 7$ oder 28. Es ist auch $1 + 2 + 4 + 7 + 14 + 28 = 2 . 28$.

Euclid stellt für vollkommene Zahlen eine Regel auf, deren Richtigkeit schon in der Mitte des vorigen Jahrhunderts von Tobias Meier in Göttingen bewiesen und von dessen Schüler Kraft in den Petersburger Commentarien niedergelegt wurde. Sie lautet folgendermassen: Ist a eine Potenz von 2 und ist $2a - 1$ eine Primzahl, so ist $a\,(2a - 1)$ eine vollkommene Zahl. Dies lässt sich leicht nachweisen, denn wenn $2a - 1$ eine Primzahl ist, so ist deren Factoren-Summe $2a$, und ist a eine Potenz von 2, so ist die Factoren-Summe von $a \ldots (2^{\alpha+1} - 1)$. Die Gleichung für die Zahl würde also lauten:

$$2 . 2^{\alpha}(2 . 2^{\alpha} - 1) = (2^{\alpha+1} - 1)\,2 . 2^{\alpha}$$

oder $2 . 2^{\alpha} - 1 = 2^{\alpha+1} - 1$

d. h. $0 = 0$.

Um eine Reihe von vollkommenen Zahlen zu erhalten, darf man also nur die Potenzen von 2 hinschreiben und unter jeder derselben diese Potenzen — 1; ist diese eine Primzahl, so ist das Product der beiden über einanderstehenden Zahlen ein numerus perfectus

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1. | 2. | 4. | 8. | 16. | 32. | 64. | 128. | 256. |
| 3. | 7. | 15. | 31. | 63. | 127. | 255. | 511. | |

Es sind also 6. 28. 496. 8128.

vollkommene Zahlen.

## § 34.

Es soll die Gleichung gelöst werden $ax - by = c$ unter der Bedingung, dass x und y ganze Zahlen und a und b relative Primzahlen zu einander sind. Setze ich für x . . . cx, und für y . . . cy, ein, so erhalte ich die Gleichung $acx - bcy = c$ oder $ax - by = 1$, und es wird die Aufgabe gelöst sein, wenn die Werthe für x, und y, bestimmt sind.

Dividire ich die Gleichung $ax - by = 1$ durch bx, so erhalte ich $\frac{a}{b} - \frac{y}{x} = \frac{1}{bx}$ d. h. die Differenz zweier Brüche, die gleich ist einem Bruche, dessen Zähler = 1 und dessen Nenner = dem Product der Nenner der beiden Brüche ist. Diese Gleichung findet aber statt

zwischen zwei auf einander folgenden Näherungswerthen eines und desselben Kettenbruchs. Die Differenz zweier solcher Näherungswerthe ist gleich + oder — 1, dividirt durch das Product der Nenner der beiden Näherungswerthe. Ich habe also einen Kettenbruch zu suchen, in welchem der Näherungswerth $\frac{a}{b}$ vorkommt, oder überhaupt $\frac{a}{b}$ in einen Kettenbruch zu verwandeln, dann wird der vor $\frac{a}{b}$ liegende Näherungswerth der Werth von $\frac{x}{y}$ sein. Sollte das Zeichen nicht stimmen, so gebe ich durch Zerlegung des letzten Nenners n in $n - 1 + \frac{1}{1}$ dem Kettenbruch einen Näherungswerth mehr.

Beispiel 1. $17x - 23y = -1$

durch 23x dividirt $\frac{17}{23} - \frac{y}{x} = -\frac{1}{23x}$.

Nun ist $\frac{17}{23}$ gleich dem Kettenbruch $\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{5}}}}$

und die Näherungswerthe heissen $\frac{1}{1}$, $\frac{2}{3}$, $\frac{3}{4}$, $\frac{17}{23}$; mithin ist $\frac{y}{x} = \frac{3}{4}$ oder $y = 3$ und $x = 4$.

Beispiel 2. $99x - 301y = 3$.

Für x und y gesetzt 3x, und 3y, giebt die Gleichung

$99x, - 301y, = 1$ oder

$99x - 301y = 1$

Dividire ich durch 301x, so erhalte ich $\frac{99}{301} - \frac{y}{x} = \frac{1}{301x}$.

Der Kettenbruch für $\frac{99}{301}$ heisst $\cfrac{1}{3+\cfrac{1}{24+\cfrac{1}{1+\cfrac{1}{3}}}}$

und dessen Näherungswerthe sind: $\frac{1}{3}$, $\frac{24}{73}$, $\frac{25}{76}$ und $\frac{99}{301}$; es wäre also der Werth für $\frac{y}{x}$, $\frac{25}{76}$. Nun giebt aber 76. 99 — 25. 301 nicht + 1, sondern — 1, und ich muss dadurch, dass ich statt des letzteren Nenners 3 setze $2 + \frac{1}{1}$ dem Kettenbruch einen Näherungswerth

mehr geben, dann heisst der Kettenbruch $\cfrac{1}{3+\cfrac{1}{24+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1}}}}}$

Seine Näherungswerthe sind $\frac{1}{3}$, $\frac{24}{73}$, $\frac{25}{76}$, $\frac{74}{225}$, $\frac{99}{301}$ und der Werth für $\frac{y}{x}$, $\frac{74}{225}$. Und in der That ist 225. 99 — 74. 301 = 1. Die der ursprünglichen Gleichung genügenden Werthe werden sein 3. 225 und 3. 74 oder 675 und 222.

§ 35.

Hat man aus der Gleichung ax — by = 1 erst einen Werth für x und y bestimmt z. B. x = z und y = v, so erhält man für sie eine ganze Reihe von Werthen, wenn man für x setzt u + bm und für y: v + am, wo wieder für m jede ganze Zahl gilt, denn wenn au — bo = 1 ist, so ist auch a (u + bm) — b (v + am) = 1. Die so erhaltenen Werthe für x und y sind die Glieder von arithmetischen Reihen, deren erste Glieder u und z, deren Differenz b und a sind.

§ 36.

Wir gehen jetzt zur sogenannten Pell'schen Aufgabe, von welcher sich schon Spuren im Diophant und bei den indischen Mathematikern finden und mit welcher die Mathematiker neuerer Zeit sich viel beschäftigt haben. Den indischen Mathematikern war die Theorie der unendlichen Reihen schon bekannt und sie haben sich überhaupt mit Aufgaben beschäftigt, welche in die Zahlentheorie fallen; z. B. Dreiecke zu construiren, deren Höhen und Seiten rational sind, oder ein Viereck in einen Kreis zu zeichnen, dessen Seiten ganze Zahlen sind. Unter den englischen Mathematikern muss hier zuerst Pell genannt werden, dann Ougthread und Harriot, nach dem der Satz von den Gleichungen genannt ist. Sie lebten zur Zeit der Elisabeth. Von späteren Engländern, namentlich von Wallis, die sich mit dieser Aufgabe beschäftigt haben, befindet sich vieles in Euler's Algebra; es sind dies jedoch alles nur Vorarbeiten, welche durch Lagrange ihren Abschluss gefunden haben. Der zur Lösung einzuschlagende Weg stützt sich auf die Periodicität der Kettenbrüche bei Benutzung derselben zum Ausziehen von Quadratwurzeln. Der Beweis der Periodicität dieser Kettenbrüche gehört zu den glorreichsten Arbeiten Lagrange's, Stifters der Turiner Akademie, später in Berlin, zuletzt in Paris. Ihm und Euler verdanken wir, dass die Zahlentheorie eine Wissenschaft geworden.

§ 37.

Aufgabe: Zu einer gegebenen Zahl a, welche kein Quadrat ist, sollen zwei Quadrate $x^2$ und $y^2$ gesucht werden, welche der Gleichung genügen $x^2 - ay^2 = 1$. x und y sind ganze Zahlen.

Wenn $x^2$ und $y^2$ mässig gross sind, so wird man ohne Fehler sagen können: $x^2 - ay^2 = o$, oder $x^2 = ay^2$, oder $\frac{x}{y} = \sqrt{a}$; und es käme dann darauf an, $\sqrt{a}$ in Form eines gemeinen Bruchs zu geben. Wir wollen hier erst einzelne Fälle untersuchen, in denen die Gleichung möglich oder unmöglich ist.

Ist $a = 4n + 1$ und sind x und y ungerade, so liesse $x^2$ sowohl wie $y^2$ durch 4 den Rest 1, und dann auch $x^2$ und $ay^2$ den Rest 1, oder deren Differenz den Rest 0, oder ein Vielfaches von 4; aber niemals 1.

Sind x und y gerade, so haben $x^2$ und $ay^2$ den Factor 4, ihre Differenz kann also nie den Rest 1 lassen, sondern lässt stets den Rest 0 oder das Vielfache von 4.

Ist x gerade und y ungerade, so lässt $x^2$ durch 4 den Rest 0, $y^2$ den Rest 1, $ay^2$ den Rest 1, und die Gleichung würde dann lauten $4q - 4z - 1 = 1$; eine Gleichung, welche für ganze Zahlen von q und z unmöglich ist.

Ist x ungerade und y gerade, so lässt $x^2$ durch 4 dividirt den Rest 1, $y^2$ den Rest 0, also $ay^2$ den Rest 0, und die Gleichung lautet $4q + 1 - 4z = 1$, welche Gleichung unter der gestellten Bedingung möglich ist.

Demnach ist also die Gleichung $x^2 - ay^2 = 1$, wenn x ungerade und y gerade ist, für ein a von der Form $4n + 1$ möglich.

Wir wollen dieses noch in einem Beispiel nachweisen; es sei $a = 13$ d. h. $x^2 - 13y^2 = 1$. Die $\sqrt{13}$ soll auf folgende Weise in Form eines gemeinen Bruchs bestimmt werden: $\sqrt{13} = 3 + \sqrt{13} - 3$. Der reciproke Werth von $\sqrt{13} - 3$ ist $\frac{1}{\sqrt{13} - 3}$ und aus ihm erhalten wir durch Multiplication des Zählers und Nenners mit $\sqrt{13} + 3$, um den letzteren rational zu machen, $\frac{\sqrt{13} + 3}{4}$; ziehen wir aus diesem Bruch die grösstmöglichste Anzahl von Ganzen, so wird er gleich $1 + \frac{\sqrt{13} - 1}{4}$. Nun nehmen wir wieder von $\frac{\sqrt{13} - 1}{4}$ den reciproken Werth, machen wieder den Nenner rational und ziehen wieder die grösstmöglichste Zahl von Ganzen heraus, so erhalten wir folgende Rechnung:

$$\sqrt{13} = 3 + \sqrt{13} - 3$$

$$\frac{1}{\sqrt{13} - 3} = \frac{\sqrt{13} + 3}{4} = 1 + \frac{\sqrt{13} - 1}{4}$$

$$\frac{4}{\sqrt{13} - 1} = \frac{\sqrt{13} + 1}{3} = 1 + \frac{\sqrt{13} - 2}{3}$$

$$\frac{3}{\sqrt{13} - 2} = \frac{\sqrt{13} + 2}{3} = 1 + \frac{\sqrt{13} - 1}{3}$$

$$\frac{3}{\sqrt{13}-1} = \frac{\sqrt{13}+1}{4} = 1 + \frac{\sqrt{13}-3}{4}$$

$$\frac{4}{\sqrt{13}-3} = \frac{\sqrt{13}+3}{1} = 6 + \frac{\sqrt{13}-3}{1}$$

$\frac{1}{\sqrt{13}-3}$. Hier beginnt, da dieser Bruch gleich dem ersten ist, die oben erwähnte Periodicität. Es ist demnach:

$$\sqrt{13} = 3 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6}}}}}}}}}$$

Die Näherungswerthe dieses Kettenbruchs sind der Reihe nach:

$$\frac{4}{1}, \frac{7}{2}, \frac{11}{3}, \frac{18}{5}, \frac{119}{33}, \frac{137}{38}, \frac{256}{71}, \frac{393}{109}, \frac{649}{180}.$$

Der Werth $\frac{649}{180}$ genügt, denn $649^2 - 13 \cdot 180^2$, oder $421201 - 421200$ ist $= 1$ und in der That ist hier x ungerade, y gerade.

2. Beispiel: $x^2 - 57y^2 = 1$.

$$\sqrt{57} = 7 + \sqrt{57} - 7$$

$$\frac{1}{\sqrt{57}-7} = \frac{\sqrt{57}+7}{8} = 1 + \frac{\sqrt{57}-1}{8}$$

$$\frac{8}{\sqrt{57}-1} = \frac{\sqrt{57}+1}{7} = 1 + \frac{\sqrt{57}-6}{7}$$

$$\frac{7}{\sqrt{57}-6} = \frac{\sqrt{57}+6}{3} = 4 + \frac{\sqrt{57}-6}{3}$$

$$\frac{3}{\sqrt{57}-6} = \frac{\sqrt{57}+6}{7} = 1 + \frac{\sqrt{57}-1}{7}$$

$$\frac{7}{\sqrt{57}-1} = \frac{\sqrt{57}+1}{8} = 1 + \frac{\sqrt{57}-7}{8}$$

$$\frac{8}{\sqrt{57}-7} = \frac{\sqrt{57}+7}{1} = 14 + \ldots$$

Es ist demnach:

$$\sqrt{57} = 7 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{14}}}}}}$$

und die Näherungswerthe des Kettenbruchs heissen:

$$\frac{1}{1}, \frac{1}{2}, \frac{5}{9}, \frac{6}{11}, \frac{11}{20}, \frac{160}{291} \text{ oder}$$

$$\frac{8}{1}, \frac{15}{2}, \frac{68}{9}, \frac{83}{11}, \frac{151}{20}, \frac{2197}{291}.$$

Im Näherungswerthe $\frac{151}{20}$ ist x ungerade und y gerade, und in der That ist:

$$151^2 - 57.\ 20^2 \text{ oder}$$
$$22801 - 22800 = 1.$$

3. Beispiel: $x^2 - 17y^2 = 1.$

$$\sqrt{17} = 4 + \sqrt{17} - 4$$

$$\frac{1}{\sqrt{17} - 4} = \frac{\sqrt{17} + 4}{1} = 8 + \frac{\sqrt{17} - 4}{1}.$$

Die Näherungswerthe sind 4 und $4 + \frac{1}{8}$ oder 4 und $\frac{33}{8}$. Auch hier ist x ungerade und y gerade, und wieder ist:

$$33^2 - 17.\ 8^2 \text{ oder}$$
$$1089 - 1088 = 1.$$

Hat a die Form $4n + 3$ und sind x und y ungerade, so lassen $x^2$ und $y^2$ den Rest 1, also $ay^2$ den Rest + 3, und die Gleichung hiesse: $4q + 1 - 4z - 3 = 1$; sie ist für ganze Zahlenwerthe von q und z, also auch von x und y, unmöglich.

Sind x und y gerade, so lassen $x^2$ und $y^2$ den Rest 0, also $ay^2$ auch den Rest 0, und unsere Gleichung hiesse $4q - 4z = 1$, welche Gleichung wiederum unmöglich.

Ist x gerade und y ungerade, so lässt $x^2$ durch 4 den Rest 0, $y^2$ den Rest 1, also $ay^2$ den Rest 3. Die alsdann erhaltene Gleichung $4q - 4z - 3 = 1$ ist möglich, denn $4q - 4z$ ist ein Vielfaches von 4, kann also überhaupt auch einmal $= 4$ sein.

Ist x ungerade, y gerade, so lässt $x^2$ den Rest 1, $y^2$ den Rest 0, also $ay^2$ ebenfalls den Rest 0, die nun erhaltene Gleichung $4q + 1 - 4z = 1$ ist ebenfalls möglich.

Die Gleichung $x^2 - ay^2 = 1$ ist also zwiefach möglich für $a = 4n + 3$, nämlich wenn x ungerade und y gerade, und wenn x gerade und y ungerade, aber nie, wenn beide gerade oder ungerade sind.

1. Beispiel: $x^2 - 19y = 1.$

$$\sqrt{19} = 4 + \sqrt{19} - 4$$

$$\frac{1}{\sqrt{19} - 4} = \frac{\sqrt{19} + 4}{3} = 2 + \frac{\sqrt{19} - 2}{3}$$

$$\frac{3}{\sqrt{19} - 2} = \frac{\sqrt{19} + 2}{5} = 1 + \frac{\sqrt{19} - 3}{5}$$

$$\frac{5}{\sqrt{19} - 3} = \frac{\sqrt{19} + 3}{2} = 3 + \frac{\sqrt{19} - 3}{2}$$

$$\frac{2}{\sqrt{19} - 3} = \frac{\sqrt{19} + 3}{5} = 1 + \frac{\sqrt{19} - 2}{5}$$

$$\frac{5}{\sqrt{19} - 2} = \frac{\sqrt{19} + 2}{3} = 2 + \frac{\sqrt{19} - 4}{3}$$

$$\frac{3}{\sqrt{19} - 4} = \frac{\sqrt{19} + 4}{1} = 8 + \ldots.$$

Die Näherungswerthe sind:

$$\frac{1}{2}, \frac{1}{3}, \frac{4}{11}, \frac{5}{14}, \frac{14}{39}, \frac{117}{326} \text{ oder:}$$

$$\frac{9}{2}, \frac{13}{3}, \frac{48}{11}, \frac{61}{14}, \frac{170}{39}, \frac{1421}{326}.$$

Für x gilt hier der Werth 170, für y 39, denn es ist in der That $28900 - 19 \cdot 1521$ oder $28900 - 28899 = 1$ und x ist gerade, y ungerade.

2. Beispiel: $x^2 - 23y^2 = 1.$

$$\sqrt{23} = 4 + \sqrt{23} - 4$$

$$\frac{1}{\sqrt{23} - 4} = \frac{\sqrt{23} + 4}{7} = 1 + \frac{\sqrt{23} - 3}{7}$$

$$\frac{7}{\sqrt{23} - 3} = \frac{\sqrt{23} + 3}{2} = 3 + \frac{\sqrt{23} - 3}{2}$$

$$\frac{2}{\sqrt{23} - 3} = \frac{\sqrt{23} + 3}{7} = 1 + \frac{\sqrt{23} - 4}{7}$$

$$\frac{7}{\sqrt{23} - 4} = \frac{\sqrt{23} + 4}{1} = 8 + \ldots.$$

Die Näherungswerthe dieses Kettenbruchs $4 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{8}}}}$

sind: $\frac{5}{1}, \frac{19}{4}, \frac{24}{5}, \frac{355}{74}$ und von diesen genügt $\frac{24}{5}$ unserer Gleichung, denn $24^2 - 23 \cdot 5^2$ oder: $576 - 575$ ist wirklich $= 1$ und x ist hier gerade, y ungerade.

3. Beispiel: $x^2 - 95y^2 = 1.$

$$\sqrt{95} = 9 + \sqrt{95} - 9$$

$$\frac{1}{\sqrt{95} - 9} = \frac{\sqrt{95} + 9}{14} = 1 + \frac{\sqrt{95} - 5}{14}$$

$$\frac{14}{\sqrt{95} - 5} = \frac{\sqrt{95} + 5}{5} = 2 + \frac{\sqrt{95} - 5}{5}$$

$$\frac{5}{\sqrt{95} - 5} = \frac{\sqrt{95} + 5}{14} = 1 + \frac{\sqrt{95} - 9}{14}$$

$$\frac{14}{\sqrt{95} - 9} = \frac{\sqrt{95} + 9}{1} = 18 + \ldots.$$

Der Kettenbruch heisst $9 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{18}}}}$

und seine Näherungswerthe sind: $\frac{10}{1}, \frac{29}{3}, \frac{39}{4} \ldots.$

Aus dem Näherungswerth $\frac{39}{4}$ ergiebt sich $x = 39$ d. h. ungerade und $y = 4$ d. h. gerade, und diese Werthe von x und y genügen auch, denn $39^2 - 95.\ 4^2$ oder $1521 - 1520$ ist $= 1$.

4. Beispiel: $57^2 - 203.\ 4^2 = 1.$

$$\sqrt{203} = 14 + \sqrt{303} - 14$$

$$\frac{1}{\sqrt{203} - 14} = \frac{\sqrt{203} + 14}{7} = 4 + \frac{\sqrt{203} - 14}{7}$$

$$\frac{7}{\sqrt{203} - 14} = \frac{\sqrt{203} + 14}{1} = 28 + \ldots.$$

Der Kettenbruch lautet: $14 + \cfrac{1}{4 + \cfrac{1}{28}}$

und seine Näherungswerthe sind: $\frac{57}{4} \ldots.$

Der Näherungswerth $\frac{57}{4}$ giebt für x einen ungeraden Werth $= 57$, für y einen geraden $= 4$ und es ist wieder: $57^2 - 203.\ 4^2$ oder $3249 - 3248 = 1$.

Die Lösung der Pell'schen Aufgabe besteht also in der Bestimmung der $\sqrt{a}$ auf dem vorhin mehrfach beschrittenen Wege durch einen Kettenbruch. Dann bestimmt man die Näherungswerthe dieses Kettenbruchs und sucht aus diesen unter Zugrundelegung der Regeln für die beiden nur möglichen Formen für a, nämlich $4n + 1$ und $4n + 3$ den passenden Näherungswerth.

Beispiel: $x^2 - 391y^2 = 1.$

$$\sqrt{391} = 19 + \sqrt{391} - 19$$

$$\frac{1}{\sqrt{391} - 19} = \frac{\sqrt{391} + 19}{30} = 1 + \frac{\sqrt{391} - 11}{30}$$

$$\frac{30}{\sqrt{391} - 11} = \frac{\sqrt{391} + 11}{9} = 3 + \frac{\sqrt{391} - 16}{9}$$

$$\frac{9}{\sqrt{391} - 16} = \frac{\sqrt{391} + 16}{15} = 2 + \frac{\sqrt{391} - 14}{15}$$

$$\frac{15}{\sqrt{391} - 14} = \frac{\sqrt{391} + 14}{13} = 2 + \frac{\sqrt{391} - 12}{13}$$

$$\frac{13}{\sqrt{391} - 12} = \frac{\sqrt{391} + 12}{19} = 1 + \frac{\sqrt{391} - 7}{19}$$

$$\frac{19}{\sqrt{391} - 7} = \frac{\sqrt{391} + 7}{18} = 1 + \frac{\sqrt{391} - 11}{18}$$

$$\frac{18}{\sqrt{391} - 11} = \frac{\sqrt{391} + 11}{15} = 2 + \frac{\sqrt{391} - 19}{15}$$

$$\frac{15}{\sqrt{391} - 19} = \frac{\sqrt{391} + 19}{2} = 19 + \frac{\sqrt{391} - 19}{2}$$

$$\frac{2}{\sqrt{391} - 19} = \frac{\sqrt{391} + 19}{15} = 2 + \frac{\sqrt{391} - 11}{15}$$

$$\frac{15}{\sqrt{391} - 11} = \frac{\sqrt{391} + 11}{18} = 1 + \frac{\sqrt{391} - 7}{18}$$

$$\frac{18}{\sqrt{391} - 7} = \frac{\sqrt{391} + 7}{19} = 1 + \frac{\sqrt{391} - 12}{19}$$

$$\frac{19}{\sqrt{391} - 12} = \frac{\sqrt{391} + 12}{13} = 2 + \frac{\sqrt{391} - 14}{13}$$

$$\frac{13}{\sqrt{391} - 14} = \frac{\sqrt{391} + 14}{15} = 2 + \frac{\sqrt{391} - 16}{15}$$

$$\frac{15}{\sqrt{391} - 16} = \frac{\sqrt{391} + 16}{9} = 3 + \frac{\sqrt{391} - 11}{9}$$

$$\frac{9}{\sqrt{391} - 11} = \frac{\sqrt{391} + 11}{30} = 1 + \frac{\sqrt{391} - 19}{30}$$

$$\frac{30}{\sqrt{391} - 19} = \frac{\sqrt{391} + 19}{1} = 38 + \ldots.$$

Der Kettenbruch lautet also:

$$19 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{19 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{38}}}}}}}}}}}}}}}}$$

und seine Näherungswerthe sind:

$$\frac{1}{1}, \frac{3}{4}, \frac{7}{9}, \frac{17}{22}, \frac{24}{31}, \frac{41}{53}, \frac{106}{137}, \frac{2055}{2656}, \frac{4216}{5449}, \frac{6271}{8105}, \frac{10487}{13554}, \frac{27245}{35213}, \frac{64977}{83980}, \frac{222176}{287153},$$

$$\frac{287153}{371133} \ldots \text{ oder:}$$

$$\frac{20}{1}, \frac{79}{4}, \frac{178}{9}, \frac{435}{22}, \frac{613}{31}, \frac{1048}{53}, \frac{2709}{137}, \frac{52519}{2656}, \frac{107747}{5449}, \frac{160266}{8105}, \frac{268013}{13554}, \frac{696292}{35213}, \frac{1660597}{83980},$$

$$\frac{5678083}{287153}, \frac{7338680}{371133}.$$

Der Näherungswerth $\frac{7338680}{371133}$ giebt die erfüllenden Werthe von x und y, denn

$7338680^2 - 391 \cdot 371133^2$ oder: $53856224142400 - 53856224142399$ ist wirklich $= 1$.

a hat die Form $4n + 3$ und nach der früheren Aufstellung ist auch x gerade und y ungerade.

# Berichtigungen:

Seite 3 Zeile 14 von unten lies: $m^2pq$ statt $m^2pg$

„ 3 „ 1 von unten lies: Summe statt Summa

„ 4 „ 15 von oben lies: d. h. 1. statt d. h. 0.

„ 5 „ 4 von oben lies: § 12 statt § 13

„ 5 „ 9 von oben lies: $+ \ldots b^{p}$; statt $+ \ldots bp$;

„ 9 „ 5 von oben lies beide Male: 1. 2. 3. . . (p — 1) statt 1. 2. 3 — p — 1

„ 9 „ 6 von oben und im Folgg. lies stets: $1^2. 2^2. 3^2. \ldots$ statt $1^2, 2^2, 3^2 \ldots$

„ 10 „ 12 von oben lies: $\frac{(a-1)(a+1)}{p}$ statt $\frac{a-1 \,.\, a+1}{p}$

„ 11 „ 7 von unten lies beide Male: 1 bis $\frac{p-1}{2}$ statt $1 - \frac{p-1}{2}$

„ 11 „ 8 von unten
„ 12 „ 14 von oben und 4 von unten } lies: $p/_4$ bis $p/_2$ statt $p/_4 - p/_2$

„ 12 „ 8 von unten lies: von der Form $8n + 5$ statt von der $8n + 5$

„ 13 „ 2 von oben und im Folgg. lies stets: $1. 2. 3 \ldots . \frac{p-1}{2}$ statt der fehlerhaften Schreibweisen dieses Productes.

„ 21 „ 4 von oben lies: 3 für a statt für a. 3