

Inhaltsverzeichnis.

| | Seite |
|--|-------|
| Einleitung: Überblick über die Geschichte der Zahlentheorie. | 1—15 |
| Pythagoras. Euclid. Diophantus. Die Inder. Die Araber. Leonardo von Pisa. Fermat. Leonhard Euler, Lagrange, Legendre. Gauß's Disquisitiones arithmeticae. Die Zahlentheorie seit Gauß. | 1—15 |
| Erstes Kapitel: Die ganze Zahl und die einfachsten Rechnungsoperationen | 16—29 |
| Nr. 1. Mehrheit, Gesamtheit, Vielheit | 16—18 |
| Nr. 2. Die Ordinalzahlen | 18 |
| Nr. 3. Ähnliche Mehrheiten | 18—19 |
| Nr. 4. Endliche und unendliche Mehrheiten | 19—20 |
| Nr. 5. Abschnitte der Zahlenreihe; sie sind endliche Mehrheiten. | 20—21 |
| Nr. 6. Die Kardinalzahlen. Die Anzahl | 21—22 |
| Nr. 7. Addition und Subtraktion. Kleinste und größte Zahlen einer endlichen Mehrheit | 23—25 |
| Nr. 8. Multiplikation | 25—26 |
| Nr. 9. Negative Zahlen. Die Null | 26—29 |
| Zweites Kapitel: Von der Teilbarkeit der Zahlen. | 30—67 |
| Nr. 1. Grundformel der Zahlentheorie. Brüche, Quotienten. Das größte Ganze $[x]$ | 30—33 |
| Nr. 2. Gemeinsame und der größte gemeinsame Teiler zweier Zahlen; relativ prime (teilerfremde) Zahlen. Modulus ganzer Zahlen. Die Euclidischen Fundamentalsätze von der Teilbarkeit | 33—36 |
| Nr. 3. Die gemeinsamen und der größte gemeinsame Teiler mehrerer Zahlen. Zerlegung dreier Zahlen in ihre Kerne | 36—37 |
| Nr. 4. Die gemeinsamen und das kleinste gemeinsame Vielfache mehrerer Zahlen. Besonderer Fall von Zahlen, die zu je zweien teilerfremd sind. Satz von Lucas | 38—40 |
| Nr. 5. Zusammengesetzte und unzerlegbare Zahlen (Primzahlen). Hauptsatz: Zerlegung einer Zahl in Primzahlfaktoren | 40—42 |
| Nr. 6. Legendre's Satz zur Entscheidung, ob eine Zahl Primzahl sei. Das Sieb des Eratosthenes | 42—43 |
| Nr. 7. Es giebt unendlich viel Primzahlen (Euclid, Kummer). Dirichlet's Satz von der arithmetischen Progression; die Progression $6x - 1$ (Lucas). Unmöglichkeit der Gleichung $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p = a^m \pm b^m$ für $m > 1$ | 43—46 |
| Nr. 8. Alle Teiler einer Zahl, deren Anzahl, Summe, Summe ihrer h^{ten} Potenzen. Die Anzahl der Zerlegungen einer Zahl in zwei (insbesondere teilerfremde) Faktoren | 46—49 |
| Nr. 9. Bestimmung des größten gemeinsamen Teilers sowie des kleinsten gemeinsamen Vielfachen mehrerer Zahlen | 49—50 |
| Nr. 10. Die Faktoriellen. Bestimmung der höchsten darin aufgehenden Potenz p^ν einer Primzahl p | 50—52 |
| Nr. 11. Darstellung einer Zahl im Ziffernsysteme einer gegebenen Grundzahl. Beispiele: das dekadische System, die Grundzahlen 2 und 3. Legendre's Formel für ν | 52—55 |

| | Seite |
|---|---------|
| Nr. 12. Der Polynomial- insbesondere der Binomialkoeffizient . . . | 55—57 |
| Nr. 13. Der Bruch $\frac{(nq)!}{(q!)^n}$; Untersuchungen von Weill, André und de Polignac | 57—62 |
| Nr. 14. Sätze von Catalan und Bourguet | 62—64 |
| Nr. 15. Ihre Verallgemeinerung durch Landau | 64—66 |
| Nr. 16. Ein Satz von Liouville über das Produkt $m(m+1)\cdots(m+n-1)$ | 66—67 |
| Drittes Kapitel: Reste und Kongruenzen | 67—99 |
| Nr. 1. Kongruente Zahlen (Gauß); Restklassen, Restsysteme (mod. n). Reduzierte Restsysteme. Die (Eulersche) Funktion $\varphi(n)$. . | 67—69 |
| Nr. 2. Einfachste Kongruenzsätze | 69—71 |
| Nr. 3. Regeln für die Teilbarkeit einer (dekadischen) Zahl durch eine gegebene Zahl | 71—73 |
| Nr. 4. Lösungen und Wurzeln einer Kongruenz $f(x) \equiv 0$; ihr Grad; Anzahl ihrer Wurzeln für einen Primzahlmodulus | 73—75 |
| Nr. 5. Auflösung der Kongruenz ersten Grades, Möglichkeitsbedingung, Anzahl der Wurzeln. Die Gleichung $ax + by = c$ | 75—78 |
| Nr. 6. Zerlegung eines Bruchs $\frac{m}{n}$ in Partialbrüche und in einfache Brüche | 78—80 |
| Nr. 7. Gleichzeitige Wurzeln mehrerer Kongruenzen $x \equiv \alpha \pmod{a}$, $x \equiv \beta \pmod{b}$, | 80—83 |
| Nr. 8. Zweite Methode der Auflösung für den Fall teilerfremder Mo- dulen. Jede Kongruenz ersten Grades kommt auf solche zurück, deren Moduln Primzahlen sind | 83—86 |
| Nr. 9. Herleitung der Formel $\varphi(mn) = \varphi(m)\varphi(n)$, falls m, n teiler- fremd sind. Ausdruck von $\varphi(n)$ mittels der Primfaktoren von n . Veränderung der fundamentalen Formel, falls m, n nicht teilerfremd sind. | 86—89 |
| Nr. 10. Der Satz $\sum_d \varphi\left(\frac{n}{d}\right) = n$. Formel von Pepin und Moret-Blanc | 89—91 |
| Nr. 11. Verallgemeinerung von $\varphi(n)$ durch Schemmel und Lucas; die dann geltenden analogen Sätze. | 91—94 |
| Nr. 12. Allgemeiner Satz über die Verteilung der Teiler einer Zahl in zwei bestimmte Gruppen. Umkehrung der Beziehung $f(n) = \sum_d \psi(d)$ | 94—97 |
| Nr. 13. Determinante von St. Smith | 97—99 |
| Viertes Kapitel: Der Euclidische Algorithmus | 99—153 |
| Nr. 1. Der Euclidische Algorithmus als Quelle für die Fundamentals- sätze von der Teilbarkeit | 99—101 |
| Nr. 2. Daraus ihm entspringende Kettenbruch, seine Näherungsbrüche, Bildungsgesetz ihrer Zähler und Nenner | 101—104 |
| Nr. 3. Die Gaußsischen Klammern | 104—105 |
| Nr. 4. Grund der Bezeichnung „Näherungsbrüche“ | 105—107 |
| Nr. 5. Weitere bezügliche Sätze. Die Gleichung $mx + ny = 1$. . | 107—109 |
| Nr. 6. Symmetrische Kettenbrüche. Satz über Quadratsummen . . | 109—112 |
| Nr. 7. Modifizierte Euclidische Algorithmen und die ihnen entsprechen- den Kettenbrüche. Für jeden irreduzibeln echten Bruch $\frac{m}{n}$ gibt es n Kettenbruchentwicklungen | 112—114 |
| Nr. 8 und 9. Ausdehnung der verschiedenen Algorithmen; Unter- suchungen von Lamé, Binet, Dupré | 114—118 |
| Nr. 10. Binet's Algorithmus. Satz von Lambert über Zerlegung eines Bruchs in Stammbrüche | 118—121 |
| Nr. 11. Die Fareyschen Reihen verschiedener Ordnung. Sätze von Cauchy und Farey | 121—125 |

| | Seite |
|--|----------------|
| Nr. 12. Die Näherungswerte einer GröÙe w ; die, falls w irrational ist, unendliche Reihe der aufeinanderfolgenden; die Charakteristik (Christoffel, Hurwitz) und Grund dieser Bezeichnung | 125—128 |
| Nr. 13. Zusammenhang zwischen der Charakteristik und dem gewöhnlichen Kettenbruche für w | 128—130 |
| Nr. 14. Die Charakteristiken äquivalenter GröÙen. | 130—133 |
| Nr. 15. Zusammenhang zwischen den Näherungswerten von w und den übrigen Kettenbruchentwicklungen | 133—138 |
| Nr. 16. Längste und kürzeste Kettenbruchentwicklungen. | 138—142 |
| Nr. 17. Die Sternsche Entwicklung (r, s) ; Mittelglied, Stamm- und Summenglieder | 142—143 |
| Nr. 18. Die einfachste Entwicklung $(1, 1)$ und ihre Eigenschaften. | 144—146 |
| Nr. 19—21. Die daraus folgenden Eigenschaften von (r, s) | 146—151 |
| Nr. 22. Eine Eisensteinsche Funktion | 151—153 |
| Fünftes Kapitel: Die Sätze von Fermat und von Wilson | 153—179 |
| Nr. 1. Der allgemeine Fermatsche Satz: $a^{p(n)} \equiv 1 \pmod{n}$. Euler's Beweis des einfachen Satzes $a^{p-1} \equiv 1 \pmod{p}$ | 153—154 |
| Nr. 2. Lagrange's Beweis des letztern; Wilson's Satz | 155—156 |
| Nr. 3. Übergang vom einfachen zum allgemeinen Fermatschen Satze | 156—158 |
| Nr. 4. Wie der (einfache) Fermatsche Satz umzukehren ist (Lucas); 65537 ist Primzahl | 158—159 |
| Nr. 5. Untersuchung der durch die Kongruenz $a^{p-1} \equiv 1 + p \cdot q(a) \pmod{p^2}$ definierten Zahl $q(a)$ durch Stern. | 159—162 |
| Nr. 6. Spezialfall: der Rest von $\frac{2^{p-1} - 1}{p} \pmod{p}$ | 162—165 |
| Nr. 7. Bestimmung von $q(a)$ nach Mirimanoff | 165—169 |
| Nr. 8. Der verallgemeinerte Wilsonsche Satz (Gauß). Hilfsbetrachtung: Anzahl der Wurzeln von $x^2 \equiv 1 \pmod{n}$ | 170—172 |
| Nr. 9. Beweis des allgemeinen Wilsonschen Satzes | 172—174 |
| Nr. 10. Er ist enthalten in einem Satze von Schemmel; Beweis eines Spezialfalls des letztern | 174—175 |
| Nr. 11. Ein bezüglicher Satz von Steiner | 176—177 |
| Nr. 12. Unmöglichkeit der Gleichung $1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) + 1 = p^k$, falls $p > 5$ (Liouville). Für $p = 4z + 3$ ist $1 \cdot 2 \cdot 3 \cdot \dots \cdot \frac{p-1}{2} \equiv \pm 1 \pmod{p};$ Entscheidung über das Vorzeichen (Dirichlet). Ergänzung zu Kap. 2, Nr. 10: Rest von $\frac{n!}{p^v} \pmod{p}$, (Stickelberger). | 177—179 |
| Sechstes Kapitel: Die Theorie der quadratischen Reste | 180—318 |
| Nr. 1. Die Kongruenz $ax^2 + bx + c \equiv 0 \pmod{n}$ kommt zurück auf $x^2 \equiv m \pmod{n}$. Bedingungen der Möglichkeit für die letztere, Anzahl ihrer Wurzeln | 180—184 |
| Nr. 2. Quadratische Reste und Nichtreste, die Anzahl derselben je $\frac{p-1}{2}$; die Symbole von Legendre und von Jacobi, ihre Eigenschaften. | 184—187 |
| Nr. 3. Eulersches Kriterium von Schering verallgemeinert; neuer Beweis des Fermatschen Satzes | 187—190 |
| Nr. 4. Das Gaußsche Lemma und seine Verallgemeinerung durch Schering: $\left(\frac{Q}{P}\right) = (-1)^{\mu(Q,P)}$ | 190—194 |
| Nr. 5. Das Reziprozitätsgesetz und seine beiden Ergänzungssätze. Beweise des ersten Ergänzungssatzes | 194—196 |
| Nr. 6. Beweis des zweiten Ergänzungssatzes | 196—197 |

| | Seite |
|---|---------|
| Nr. 7. Ausdehnung der Ergänzungssätze auf das Jacobische Symbol; allgemeinsten Ausdruck des Reziprozitätsgesetzes | 197—200 |
| Nr. 8. Geschichtliches über Entdeckung und Beweis des Reziprozitätsgesetzes; chronologische Tabelle all' seiner bisherigen Beweise; ihre verschiedenen Kategorien; die hier behandelten | 200—206 |
| Nr. 9. Der erste Gaußsche Beweis in Dirichlet's Darstellung; der Gaußsche Hilfssatz | 206—212 |
| Nr. 10. Hilfsbegriffe und Bezeichnungen (Kronecker): der Unterschied $R(x) = x - \left[x + \frac{1}{2} \right]$; $\text{sgn. } x = \frac{x}{ x }$; die neue Form des verallgemeinerten Gaußschen Lemma; die verschiedenen Ausdrücke des Reziprozitätsgesetzes | 212—216 |
| Nr. 11. Die fundamentalen Beziehungen $R(x+1) = R(x), \quad R(x) + R(-x) = 0.$ Der fünfte Gaußsche Beweis | 216—220 |
| Nr. 12. Weitere Eigenschaft von $R(x)$: $\text{sgn. } R(x) = (-1)^{[2x]}$; die Kongruenz $\mu(Q, P) \equiv \sum_{h=1}^{\frac{P-1}{2}} \left[\frac{hQ}{P} \right] \pmod{2}$. Der dritte Gaußsche Beweis, seine geometrische Darstellung nach Eisenstein, seine Modifikation durch Voigt und Fields | 220—227 |
| Nr. 13. Genocchi's Beweis, seine ursprüngliche Quelle, seine arithmetische Grundlage; zwei interessante Summenformeln; wesentlich damit identisch ist Schering's Beweis. | 228—233 |
| Nr. 14. Kronecker's andere Formulierung der letzten zwei Beweise. Modifikation des Scheringschen auf Grund der Formel $\text{sgn. } R(x) = \text{sgn. } \prod_k (x-k) \left(x + \frac{1}{2} - k \right);$ Herleitung der Formeln $\left(\frac{Q}{P} \right) = \text{sgn. } \prod_{h,k} \left(\frac{h}{P} - \frac{k}{Q} \right) \cdot \left(\frac{h}{P} + \frac{k}{Q} - \frac{1}{2} \right) = \text{sgn. } \prod_{h,k} \left(\frac{k}{Q} - \frac{h}{P} \right).$ Diese folgen auch unmittelbar aus Gauß's Bestimmung für $\text{sgn. } R(x)$ mittels der Formel $(-1)^{[2x]} = \text{sgn. } \prod_i (i-2x)$ | 233—237 |
| Nr. 15. Auf der gleichen Formel beruht schon Schaar's Beweis, dem sich die Beweise Gegenbauer's wie der von Lucas anreihen | 237—242 |
| Nr. 16. Einfachste Gestalt des dritten Gaußschen Beweises (Kronecker). Bemerkungen von Schering. Verhältnis jenes Beweises zu denjenigen von Genocchi und Schering (logarithmische Umgestaltung) | 242—245 |
| Nr. 17. Kronecker's Beweis (auch Hermes') „durch Umkehrung“ | 245—249 |
| Nr. 18. Busche's erster Beweis auf Grund eines allgemeinen arithmetischen Satzes | 249—254 |
| Nr. 19. Busche's zweiter Beweis auf Grund des modifizierten Gaußschen Lemma. | 254—256 |
| Nr. 20. Lange's Beweise, denen wieder eine neue Modifikation desselben zu Grunde liegt | 256—261 |
| Nr. 21. Zwei weitere Eigenschaften der Funktion $R(x)$, deren die Beweise von Zeller und von Petersen bedürfen; Darstellung des ersteren | 261—265 |
| Nr. 22. Der Beweis von Petersen, auf einer anderen Form des Gaußschen Lemma begründet. Modifizierter Kroneckerscher Beweis. Neue Ableitung des zweiten Ergänzungssatzes | 266—269 |

| | Seite |
|---|----------------|
| Nr. 23. Beweis von Bouniakowsky; erster Beweis von Schmidt . . . | 270—274 |
| Nr. 24. Zweiter Beweis von Schmidt eine Modifikation des fünften Gaußsichen | 274—277 |
| Nr. 25. Dritter Beweis von Schmidt | 277—280 |
| Nr. 26. Hilfssatz von Zolotareff, seine Verallgemeinerung durch Lerch. Beweis von Zolotareff | 280—286 |
| Nr. 27. Arithmetische Reihen, welche die Zahlen m liefern, für welche $\left(\frac{m}{n}\right)$ einen bestimmten Wert hat. Primteiler der Form $x^2 - my^2$ | 286—290 |
| Nr. 28 und 29. Direkte Wertbestimmung von $\left(\frac{m}{n}\right)$: 1) nach Gauß auf Grund des gewöhnlichen Euclidischen Algorithmus, Unter- suchungen von Zeller und Schering; 2) nach den Regeln von Eisenstein, Lebesgue, Kronecker, Sylvester, Gegenbauer . . . | 290—300 |
| Nr. 30. Verteilung der quadratischen Reste und Nichtreste im Inter- valle $0, p$ | 300—306 |
| Nr. 31. Die trigonalen und bitrigonalen Reste | 306—311 |
| Nr. 32 und 33. Beziehungen zwischen Summen quadratischer, trigo- naler und bitrigonaler Reste oder Nichtreste | 311—318 |
| Siebentes Kapitel: Die höheren Kongruenzen | 318—399 |
| Nr. 1. Die binomische Kongruenz $x^m \equiv a \pmod{n}$ zurückgeführt auf $z^m \equiv 1 \pmod{n}$. Exponent, zu welchem eine Zahl $(\text{mod. } n)$ gehört. Neuer Beweis des Fermatschen Satzes | 318—322 |
| Nr. 2. Primitive Wurzeln. Existenz primitiver Wurzeln $(\text{mod. } p)$; ihre Anzahl | 322—324 |
| Nr. 3. Andere Herleitung derselben Resultate | 324—327 |
| Nr. 4. Existenz primitiver Wurzeln $(\text{mod. } p^\alpha)$; ihre Anzahl | 327—330 |
| Nr. 5. Die Moduln $n = 2, n = 4$. Für den Modulus $n = 2^l$ ($l > 2$) gibt es keine primitive Wurzeln $(\text{mod. } n)$, aber primitive Lösungen von $z^{2^l - 2} \equiv 1 \pmod{2^l}$, z. B. $z = 5$ | 331—333 |
| Nr. 6. Sätze über Produkt und Summe aller $(\text{mod. } p^\alpha, 2p^\alpha)$ zu gleichem Exponenten gehörigen Zahlen | 333—336 |
| Nr. 7. Neuer Beweis des allgemeinen Wilsonschen Satzes. | 336—338 |
| Nr. 8. Theorie der Indices $(\text{mod. } n)$ | 338—341 |
| Nr. 9. Methoden zur Ermittlung einer primitiven Wurzel $(\text{mod. } p)$ | 341—343 |
| Nr. 10. Potenzreste m^{ten} Grades $(\text{mod. } p^\alpha)$, charakteristische Bedingung für dieselben. Sätze über Summe und Produkt aller m^{ten} Po- tenzreste. Auflösung der Kongruenz $x^m \equiv a \pmod{p^\alpha}$ | 343—348 |
| Nr. 11. Die m^{ten} Potenzreste $(\text{mod. } 2^l)$ | 348—351 |
| Nr. 12. Entwicklung irreduktibler echter Brüche $\frac{r}{n}$ nach den nega- tiven Potenzen einer Grundzahl g ; insbesondere in Dezimal- brüche | 351—354 |
| Nr. 13. Ihre Periodizität; Länge der Periode | 355—357 |
| Nr. 14. Anwendung auf Dezimalbrüche. | 357—359 |
| Nr. 15. Satz über die Ziffern der Zahl $\frac{g^{\varphi(n)} - 1}{n}$ | 359—361 |
| Nr. 16. Beziehung zwischen den Entwicklungen von $\frac{r}{n}$, welche zwei $(\text{mod. } n)$ kongruenten oder associierten Grundzahlen ent- sprechen | 361—363 |
| Nr. 17. Die allgemeine Kongruenz $f(x) \equiv 0 \pmod{n}$; n wird als Prim- zahl p vorausgesetzt. Grad von $f(x)$, Grad eines Produktes. Satz über Teilbarkeit eines Produktes durch p . Zerlegbarkeit von $f(x) \pmod{p}$ in Faktoren, und Wurzeln von $f(x)$ | 363—366 |

| | Seite |
|--|---------|
| Nr. 18. Kongruenz von Funktionen (mod. p); inkongruente Klassen primärer Funktionen m^{ten} Grades und deren Anzahl. Teiler von $f(x)$ (mod. p), irreduktible oder Primfunktionen | 366—368 |
| Nr. 19. Größter gemeinsamer Teiler zweier Funktionen (mod. p); relativ prime Funktionen. Fundamentalsätze von der Teilbarkeit der Funktionen (mod. p). | 368—370 |
| Nr. 20. Möglichkeit der Zerlegung einer Funktion in Primfunktionen (mod. p). Über gemeinsame Teiler einer Funktion und ihrer Ableitung | 370—372 |
| Nr. 21. Ermittlung der Anzahl (m) inkongruenter primärer Primfunktionen m^{ten} Grades nach Gaußs | 372—375 |
| Nr. 22. Kongruenz von Funktionen nach dem Doppelmodulus $p, P(x)$; Anzahl der inkongruenten Funktionen. Reduziertes Restsystem. Analogon des Fermatschen Satzes; die Kongruenz $X^{p^m} \equiv X \pmod{p, P(x)}$ hat p^m Wurzeln. Allgemeiner Satz über die Anzahl Wurzeln einer Kongruenz. Analogon des Wilsonschen Satzes; | 375—378 |
| Nr. 23. Zerlegung der Funktion $x^{p^m} - x$ in Primfunktionen (mod. p). Neue Herleitung der Anzahl (m). Ausdruck für das Produkt aller Primfunktionen m^{ten} Grades | 378—382 |
| Nr. 24. Ermittlung der Primteiler einer gegebenen Funktion | 382—383 |
| Nr. 25. Exponent, zu welchem eine Funktion (mod. $p, P(x)$) gehört; Anzahl derjenigen Funktionen, die zu einem bestimmten Exponenten gehören | 384—385 |
| Nr. 26. Zerlegung von $x^d - 1$ in Primfaktoren (mod. p). Sätze über die Zerlegung von $\frac{x^q - 1}{x - 1}$, wenn q eine von p verschiedene Primzahl ist | 385—388 |
| Nr. 27. Exponent μ , zu welchem eine Funktion (mod. $p, P(x)$) paßt. Die zu μ passenden sind die Wurzeln der irreduktibeln Kongruenzen $P_\mu(x) \equiv 0 \pmod{p, P(x)}$ vom Grade μ . Ihre Anzahl ist $\mu \cdot (\mu)$. Es giebt stets Primfunktionen $P(x)$ so beschaffen, daß eine Kongruenz n^{ten} Grades $F(X) \equiv 0 \pmod{p, P(x)}$ genau n Wurzeln hat | 388—394 |
| Nr. 28. Die Galoisschen Imaginären | 394—396 |
| Nr. 29. Gaußs' siebenter Beweis des Reziprozitätsgesetzes | 396—399 |
| Zusätze | 400—402 |