

Inhaltsverzeichnis.

Einleitung.

	Seite
Nr. 1 u. 2. Der Begriff der ganzen Zahl	1--4
Nr. 3. Die einfachsten Rechnungsoperationen; die Addition .	4--6
Nr. 4 u. 5. Die Subtraktion; negative Zahlen; die Null; Grössenordnung der negativen Zahlen	6--11
Nr. 6. Die Multiplikation; sie ist commutativ, associativ, distributiv. Multiplikation negativer Zahlen mit posi- tiven und unter einander.	11--15

Erster Abschnitt.

Von der Theilbarkeit der Zahlen.

Nr. 1. Vielfache, Theiler, Reste, grösste Ganzen. Gemein- samer und grösster gemeinsamer Theiler zweier Zahlen; relative Primzahlen	16--18
Nr. 2. Ableitung des Euclidischen Fundamentalsatzes nach Poincot	18--21
Nr. 3. Einfachste Folgesätze	21--23
Nr. 4. Primzahlen und zusammengesetzte Zahlen; Zerlegung der letztern in Primfaktoren. Legendre's Hilfsmittel zur Erkenntniss von Primzahlen; ihre Anzahl ist un- endlich gross	23--26
Nr. 5. Aufsuchung aller Theiler einer Zahl, ihre Anzahl, ihre Summe	26--28
Nr. 6. Gemeinsame Theiler gegebener Zahlen, grösster gemeinsamer Theiler. Gemeinsame Vielfache und kleinstes gemeinsames Vielfaches. Der Fall relativ primer Zahlen.	28--30
Nr. 7. Höchste Potenz einer Primzahl p , welche im Produkte $1 \cdot 2 \cdot 3 \dots n$ aufgeht. Besondere Fälle $p = 2$, $p = 3$	30--35
Nr. 8. Der Polynomialcoefficient und der Binomialcoefficient sind ganze Zahlen.	35--36
Nr. 9. Satz von Catalan	37--39
Nr. 10. Ein allgemeiner Satz über die Theiler einer Zahl . .	40--41
Nr. 11. Anwendung zur Bestimmung der zahlentheoretischen Funktion $\varphi(n)$	41--44

Zweiter Abschnitt.

Von den Congruenzen.

	Seite
Nr. 1. Definition congruenter Zahlen (mod. n). Vollständige Restsysteme, insbesondere das der kleinsten positiven und das der absolut kleinsten Reste . . .	45—47
Nr. 2. Reducirtes Restsystem (mod. n). Einfachste Sätze über Congruenzen	47—49
Nr. 3. Die Rechnung mit Restclassen.	49—51
Nr. 4. Dedekind's Definition eines Modulus von Zahlen. Die Congruenz in Bezug auf einen solchen. Die Anzahl incongruenter ganzer Funktionen m^{ten} Grades (mod. n)	51—54
Nr. 5. Bedeutung einer Congruenz $f(x) \equiv 0 \pmod{n}$; Wurzeln einer solchen. Ist n Primzahl, so hat die Congruenz höchstens soviel Wurzeln, als ihr Grad beträgt	54—57
Nr. 6. Begriff einer (endlichen) Gruppe von Zahlen oder Elementen. Einfachste Sätze über Gruppen	57—61
Nr. 7 u. 8. Die Anwendung auf die Gruppe der Restclassen (mod. n) ergibt die Auflösung der Congruenzen und unbestimmten Gleichungen ersten Grades.	61—66
Nr. 9. Lösungen der Aufgabe: eine Zahl zu finden, welche nach gegebenen Moduln gegebene Reste lässt. Beispiel	66—69
Nr. 10. Folgerungen. Die Formel $\varphi(abc\dots) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c) \dots$	69—70
Nr. 11. Herleitung des allgemeinen Fermat'schen Satzes aus Nr. 6	71—73
Nr. 12. Euler's Herleitung desselben	73—75
Nr. 13. Lagrange's Herleitung des einfachen Fermat'schen Satzes und Wilson'scher Satz	75—78
Nr. 14—16. Der allgemeine Kronecker'sche Satz über Zusammensetzung aller Elemente einer commutativen Gruppe aus Fundamentelementen.	79—88
Nr. 17. Anwendung zum Nachweis von der Existenz primitiver Wurzeln (mod. p); Anzahl der incongruenten primitiven Wurzeln.	88—91
Nr. 18. Der einer primitiven Wurzel (mod. p) entsprechende Index einer Zahl. Einfache Sätze über die Rechnung mit Indices	91—94
Nr. 19. Anwendung zur Herleitung eines Satzes	94—97
Nr. 20. Primitive Wurzeln für zusammengesetzte Moduln. Der Fall (mod. p^a) sowie (mod. 2^k)	97—102
Nr. 21. Der Fall eines beliebigen Modulus.	102—104

Dritter Abschnitt.

Von den quadratischen Resten.

	Seite
Nr. 1. Congruenzen zweiten Grades. Quadratische Reste und Nichtreste eines Modulus; quadratischer Charakter einer Zahl	105—106
Nr. 2. Die Congruenz $x^2 \equiv n \pmod{p}$. Euler'sches Criterium zur Entscheidung ihrer Möglichkeit. Legendre'sches Symbol $\left(\frac{n}{p}\right)$; einfachste Sätze	106—109
Nr. 3. Die Congruenz $x^2 \equiv n \pmod{p^\mu}$, desgleichen $\pmod{2^\nu}$	109—113
Nr. 4. Die Congruenz $x^2 \equiv n \pmod{m}$, Anzahl ihrer Wurzeln im Falle ihrer Auflösbarkeit.	113—114
Nr. 5. Beispiele	114—117
Nr. 6. Die Frage, in Bezug auf welche Moduln eine gegebene Zahl quadratischer Rest oder Nichtrest ist, wird vereinfacht. Satz betr. die Zahl -1 :	
	$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad$
Nr. 7. Das Gaussische Lemma; die Gaussische Charakteristik. Satz über die Zahl 2:	
	$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad$
Nr. 8. Das Legendre'sche Reciprocitätsgesetz:	
	$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$
	Geschichtliches über seine Erfindung und Begründung 122—125
Nr. 9. Die Gaussischen Beweise; vier Kategorien, in welche alle bekannten Beweise des Gesetzes sich vertheilen lassen	125—127
Nr. 10. Der Beweis des Pfarrers Zeller	128—131
Nr. 11. Verallgemeinerung des Legendre'schen Symbols durch Jacobi. Verallgemeinerung der Sätze in Nr. 6, 7, 8 vermittelt des allgemeineren Symbols	131—137
Nr. 12. Eisenstein's Regel zur Entscheidung, ob eine Primzahl p von einer anderen Primzahl q quadratischer Rest ist oder nicht	137—141
Nr. 13. Verallgemeinerung des Gaussischen Lemma; Vorbemerkungen	141—144
Nr. 14. Das verallgemeinerte Lemma selbst	144—148
Nr. 15. Schering's Beweis des verallgemeinerten Reciprocitätsgesetzes vermittelt desselben	148—151
Nr. 16. Darstellung dieses Beweises für das einfache Gesetz in der Auffassung von Kronecker	151—152

	Seite
Nr. 17. Kronecker's Darstellung des Symbols $\left(\frac{Q}{P}\right)$ durch den Vorzeichenwerth gewisser Produkte. Einfachste Form des dritten Gaussischen Beweises	153—157
Nr. 18. Direkter Nachweis der Identität zwischen dem Symbol $\left(\frac{Q}{P}\right)$ und jenem Vorzeichenwerth	157—160
Nr. 19. Man bedarf dazu des Hilfssatzes aus Gauss' erstem Beweise	160—162
Nr. 20. Man gewinnt dann aber auch einen neuen Beweis des verallgemeinerten Reciprocitätsgesetzes	162—164

Vierter Abschnitt.

Die quadratischen Formen.

Nr. 1. Die Theorie der quadratischen Reste kann aufgefasst werden als Frage nach den Theilern gewisser quadratischer Formen. Allgemeiner Ausdruck solcher Formen; abgeleitete, primitive; eigentlich und uneigentlich primitive; man beschränkt die Betrachtung auf die ersteren	165—167
Nr. 2. Aufgabe: Die Darstellung einer Zahl durch eine gegebene quadratische Form. Geschichtliches. Es werden nur eigentliche Darstellungen betrachtet	168—170
Nr. 3. Determinante einer Form (a, b, c) : $D = b^2 - 4ac$. 1) Der Fall $D = 0$; 2) der Fall $D < 0$; positive und negative Formen, nur die positiven brauchen betrachtet zu werden; 3) der Fall $D < 0$; Formen einer solchen Determinante heissen unbestimmte Formen	170—173
Nr. 4. Durch eine gegebene eigentlich primitive Form (a, b, c) sind stets Zahlen eigentlich darstellbar, welche dasselbe Vorzeichen haben wie a und zu einer gegebenen Zahl n prim sind	173—174
Nr. 5. Nothwendige Bedingung der Darstellbarkeit einer Zahl m durch (a, b, c) : D muss quadratischer Rest von m sein. Jede Darstellung gehört dann zu einer Wurzel der Congruenz $x^2 \equiv D \pmod{m}$	174—177
Nr. 6. Darstellungsgruppen. Wichtige Eigenschaft der Form $x^2 - Dy^2$. Zusammenhang aller Darstellungen einer Gruppe mit den ganzzahligen Auflösungen der Pell'schen Gleichung $t^2 - Du^2 = 1$	177—180
Nr. 7. Auflösung der letztern und der Aufgabe Nr. 2 im Falle $D < 0$. Beispiel	180—182
Nr. 8 u. 9. Auflösung der Pell'schen Gleichung im Falle $D > 0$ und Zurückführung aller Lösungen auf die Fundamentalauflösung, nach Dirichlet	182—189

	Seite
Nr. 10. Geschichtliches	189—192
Nr. 11. Anwendung auf die Pythagoräischen Zahlen	192—196
Nr. 12. Alle Darstellungen einer Zahl m durch eine Form (a, b, c) von positiver Determinante; man setzt zu- nächst a, m von gleichem Vorzeichen voraus	196—201
Nr. 13. Aequivalenz von Formen; (a, b, c) und (m, n, m_1) sind äquivalent, wenn m durch jene Form zur Wurzel n gehörig dargestellt werden kann	201—205
Nr. 14. Ergänzung von Nr. 12 für den Fall, dass a, m un- gleiches Vorzeichen haben. Beispiel	205—208
Nr. 15. Weitere Aequivalenzsätze. Der arithmetischen De- finition der Aequivalenz entspricht eine algebraische. Transformationen einer Form in sich selbst	209—213
Nr. 16. Classen äquivalenter Formen einer gegebenen Deter- minante. Reducirte Formen. Die Anzahl der Classen ist eine endliche	213—217
Nr. 17. Formensystem einer gegebenen Determinante. Bei- spiel $D = +5$	217—219
Nr. 18. Darstellungen einer gegebenen Zahl durch das Formensystem.	220—222
Nr. 19. Beispiel: $D = -1$ d. i. Darstellungen durch die Form $x^2 + y^2$	222—226
Nr. 20. Uneigentliche Darstellungen für diesen Fall; Zer- legungen in die Summe zweier Quadratzahlen; die Anzahl derselben	226—230
Nr. 21. Satz über Primzahlen von der Form $4n + 1$	230—232
Nr. 22. Entgegengesetzte Formen und Classen; ambige Classen; in jeder ambigen Classe befindet sich auch eine ambige Form.	232—237
Nr. 23. Die Hauptform und Hauptklasse. Ueber Darstel- lungen durch dieselbe. Vereinbare Wurzeln der Congruenz $x^2 \equiv D$ nach verschiedenen Modulu	237—240
Nr. 24. Zusammensetzbare Formen und die aus ihnen zu- sammengesetzte Form	240—242
Nr. 25. Arithmetische Bedeutung dieser Zusammensetzung	242—245
Nr. 26. Zusammensetzung oder Multiplikation von Classen; dieselbe ist commutativ, associativ und einpaarig	245—249
Nr. 27. Zusammensetzung aller Classen aus gewissen Funda- mentalclassen. Anzahl der ambigen Classen	249—252
Nr. 28. Ueber den zweiten Gaussischen und die analogen Beweise des Reciprocitätsgesetzes	252—254
Nr. 29. Der zweite Kummer'sche Beweis; Vorbemerkungen	254—259
Nr. 30. Der Beweis selbst	259—262
Erläuternde Zusätze	263—264