

## Werk

**Titel:** Vorlesungen über Zahlentheorie

**Autor:** Dirichlet, Peter

**Verlag:** Vieweg

**Ort:** Braunschweig

**Jahr:** 1871

**Kollektion:** Mathematica

**Digitalisiert:** Niedersächsische Staats- und Universitätsbibliothek Göttingen

**Werk Id:** PPN30976923X

**PURL:** <http://resolver.sub.uni-goettingen.de/purl?PPN30976923X>

**OPAC:** <http://opac.sub.uni-goettingen.de/DB=1/PPN?PPN=30976923X>

**LOG Id:** LOG\_0005

**LOG Titel:** Tabelle, Liste

**LOG Typ:** table\_list

## Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain these Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

## Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen  
Georg-August-Universität Göttingen  
Platz der Göttinger Sieben 1  
37073 Göttingen  
Germany  
Email: [gdz@sub.uni-goettingen.de](mailto:gdz@sub.uni-goettingen.de)

# I N H A L T.

---

## Erster Abschnitt: Von der Theilbarkeit der Zahlen.

	Seite
§. 1. Das Product aus zwei oder drei Factoren ist unabhängig von der Anordnung der Multiplication . . . . .	1
§. 2. Producte aus beliebig vielen Factoren . . . . .	3
§. 3. Erklärung der Theilbarkeit einer Zahl durch eine andere . . . . .	5
§. 4. Grösster gemeinschaftlicher Theiler zweier Zahlen . . . . .	6
§. 5. Relative Primzahlen . . . . .	8
§. 6. Grösster gemeinschaftlicher Theiler von beliebig vielen Zahlen	10
§. 7. Kleinstes gemeinschaftliches Vielfaches von beliebig vielen Zahlen . . . . .	11
§. 8. Primzahlen und zusammengesetzte Zahlen; Zerlegung der zusammengesetzten Zahlen in Primzahlen. Die Anzahl der Primzahlen ist unbegrenzt . . . . .	12
§. 9. Bildung aller Theiler einer Zahl aus den in ihr enthaltenen Primzahlen; Anzahl und Summe dieser Theiler . . . . .	16
§. 10. Bildung des grössten gemeinschaftlichen Theilers und des kleinsten gemeinschaftlichen Vielfachen von beliebig vielen Zahlen aus den in diesen enthaltenen Primzahlen . . . . .	18
§. 11. Bestimmung der Anzahl $\varphi(m)$ , welche angiebt, wie viele der ersten $m$ Zahlen 1, 2, 3 . . . $m$ relative Primzahlen zu der letzten $m$ sind . . . . .	19
§. 12. Beweis des Satzes, dass $\varphi(mm') = \varphi(m)\varphi(m')$ ist, wenn $m$ und $m'$ relative Primzahlen zu einander sind . . . . .	23
§. 13. Beweis des Satzes: $\sum \varphi(n) = m$ , wo sich das Summenzeichen auf alle Divisoren $n$ der Zahl $m$ bezieht . . . . .	24
§. 14. Anderer Beweis desselben Satzes . . . . .	26
§. 15. Bestimmung der höchsten Potenz einer Primzahl, welche in dem Producte 1.2.3 . . . $m$ der ersten $m$ ganzen Zahlen aufgeht. Folgerungen . . . . .	27
§. 16. Rückblick . . . . .	30

**Zweiter Abschnitt: Von der Congruenz der Zahlen.**

- §. 17. Erklärung der Congruenz zweier Zahlen in Bezug auf eine dritte. Einfachste Operationen mit Congruenzen . . . . . 32-
- §. 18. Vollständiges Restsystem in Bezug auf einen Modulus . . . . . 36
- §. 19. Beweis des verallgemeinerten Fermat'schen Satzes . . . . . 38
- §. 20. Anderer Beweis desselben Satzes . . . . . 40
- §. 21. Congruenzen mit unbekanntem Grössen; Grad derselben . . . . . 42
- §. 22. Congruenz ersten Grades mit einer Unbekannten; Kriterium ihrer Möglichkeit; erste Methode der Auflösung . . . . . 43
- §. 23. Digression über den Euler'schen Algorithmus . . . . . 46
- §. 24. Zweite Methode der Auflösung der Congruenzen ersten Grades mit einer Unbekannten . . . . . 51
- §. 25. Auflösung der Aufgabe, alle Zahlen zu finden, welche in Bezug auf gegebene Divisoren vorgeschriebene Reste lassen . . . . . 54
- §. 26. Eine Congruenz mit einer Unbekannten, deren Modulus eine Primzahl ist, kann nicht mehr incongruente Wurzeln haben, als ihr Grad Einheiten enthält . . . . . 57
- §. 27. Ableitung des Wilson'schen Satzes aus dem Fermat'schen . . . . . 61
- §. 28. Potenzreste; Exponent, zu welchem eine Zahl gehört . . . . . 62
- §. 29. Ist  $p$  eine Primzahl und  $d$  ein Divisor von  $p - 1$ , so gehören  $\varphi(d)$  nach  $p$  incongruente Zahlen zum Exponenten  $d$  . . . . . 64
- §. 30. Primitive Wurzeln einer Primzahl. Indices. Dritte Methode, Congruenzen ersten Grades aufzulösen . . . . . 66
- §. 31. Binomische Congruenzen, deren Modulus eine Primzahl ist. Kriterium ihrer Möglichkeit; Anzahl ihrer Wurzeln . . . . . 70

**Dritter Abschnitt: Von den quadratischen Resten.**

- §. 32. Quadratische Reste und Nichtreste . . . . . 74
- §. 33. Ist der Modulus eine ungerade Primzahl  $p$ , so zerfallen die durch  $p$  nicht theilbaren Zahlen in gleich viel Reste und Nichtreste. Charakter eines Productes aus mehreren Factoren. Symbol von Legendre . . . . . 75
- §. 34. Elementarer Beweis der vorhergehenden, so wie der Sätze von Fermat und Wilson . . . . . 78
- §. 35. Fall, in welchem der Modulus eine Potenz einer ungeraden Primzahl ist . . . . . 80
- §. 36. Fall, in welchem der Modulus eine Potenz der Zahl 2 ist . . . . . 82
- §. 37. Fall, in welchem der Modulus eine beliebige Zahl ist . . . . . 84
- §. 38. Der verallgemeinerte Wilson'sche Satz . . . . . 86
- §. 39. Reduction der Aufgabe, die Moduln zu finden, von denen eine gegebene Zahl quadratischer Rest ist . . . . . 87
- §. 40. Die Zahl  $-1$  ist quadratischer Rest aller Primzahlen von der Form  $4n + 1$ , und Nichtrest aller Primzahlen von der Form  $4n + 3$  . . . . . 89
- §. 41. Die Zahl 2 ist quadratischer Rest aller Primzahlen von der Form  $8n + 1$  und  $8n + 7$ , Nichtrest aller Primzahlen von der Form  $8n + 3$  und  $8n + 5$  . . . . . 90
- §. 42. Inhalt des Reciprocitätssatzes . . . . . 92

§. 43. Erster Theil des Beweises; Umformung des früheren Kriteriums für den Charakter einer Zahl. Neuer Beweis des Satzes über die Zahl 2 . . . . .	94
§. 44. Zweiter Theil des Beweises . . . . .	97
§. 45. Anwendung des Reciprocitätssatzes auf die Aufgabe, den Charakter einer gegebenen Zahl in Bezug auf eine gegebene Primzahl zu bestimmen . . . . .	101
§. 46. Jacobi's Verallgemeinerung des Symbols von Legendre. Verallgemeinerter Reciprocitätssatz . . . . .	102
§. 47. Anwendung dieser Verallgemeinerung auf die Werthbestimmung eines Symbols . . . . .	108
§. 48. Zweiter Beweis des Reciprocitätssatzes; Vorbereitungen . . . . .	110
§. 49. Erster Theil des Beweises . . . . .	111
§. 50. Lemma: ist $q$ eine Primzahl von der Form $8n + 1$ , so giebt es unterhalb $2\sqrt{q} + 1$ mindestens eine ungerade Primzahl, von welcher $q$ quadratischer Nichtrest ist . . . . .	114
§. 51. Zweiter Theil des Beweises für den Reciprocitätssatz . . . . .	115
§. 52. Aufstellung der Linearformen, in denen die Primzahlen enthalten sind, von welchen eine gegebene Zahl quadratischer Rest oder Nichtrest ist . . . . .	119

**Vierter Abschnitt: Von den quadratischen Formen.**

§. 53. Binäre quadratische Formen; Coefficienten und Variable derselben; ihre Determinante. Ausschluss der Formen, deren Determinante eine Quadratzahl ist . . . . .	126
§. 54. Transformation der Formen. Eigentliche und uneigentliche Substitutionen . . . . .	128
§. 55. Zusammengesetzte Substitutionen . . . . .	130
§. 56. Eigentliche und uneigentliche Aequivalenz der Formen . . . . .	132
§. 57. Formen, welche sich selbst uneigentlich äquivalent sind . . . . .	134
§. 58. Ambige Formen. Jede sich selbst uneigentlich äquivalente Form ist einer ambigen Form äquivalent . . . . .	136
§. 59. Eintheilung aller Formen von einer bestimmten Determinante in Classen; vollständiges System nicht äquivalenter Formen. Zwei Hauptprobleme der Lehre von der Aequivalenz . . . . .	138
§. 60. Eigentliche Darstellung der Zahlen durch quadratische Formen; Congruenzwurzeln, zu welchen die Darstellungen gehören. Zurückführung auf die beiden Hauptprobleme . . . . .	140
§. 61. Reduction des zweiten Problems, aus einer gegebenen Substitution, durch welche eine Form in eine ihr äquivalente Form übergeht, alle ähnlichen Substitutionen zu finden, auf den Fall, in welchem beide Formen identisch sind. Theiler der Formen und Classen . . . . .	143
§. 62. Reduction des Problems, alle Substitutionen zu finden, durch welche eine Form in sich selbst übergeht, auf die vollständige Auflösung der Pell'schen Gleichung. Lösung derselben für den Fall einer negativen Determinante . . . . .	146

- §. 63. Angriff des ersten Hauptproblems in der Lehre von der Aequivalenz: zu entscheiden, ob zwei Formen von gleicher Determinante äquivalent sind, oder nicht, und im erstern Falle eine Substitution zu finden, durch welche die eine der beiden Formen in die andere übergeht. Benachbarte Formen . . . . . 150
- §. 64. Negative Determinanten. Positive Formen; Reducirte Formen. Jede Form ist einer reducirten Form äquivalent . . . . . 151
- §. 65. Ausnahmefälle, in welchen zwei nicht identische reducirte Formen äquivalent sind . . . . . 154
- §. 66. Die Aequivalenz oder Nichtäquivalenz zweier Formen von gleicher negativer Determinante wird durch Vergleichung mit reducirten Formen erkannt . . . . . 156
- §. 67. Die Anzahl der Formenclassen für eine negative Determinante ist endlich . . . . . 158
- §. 68. Zerlegung der Zahlen in zwei Quadratzahlen . . . . . 161
- §. 69. Zerlegung der Zahlen in eine einfache und eine doppelte Quadratzahl . . . . . 163
- §. 70. Darstellung der Zahlen durch die Formen  $x^2 + 3y^2$  und  $2x^2 + 2xy + 2y^2$  . . . . . 165
- §. 71. Darstellung der Zahlen durch die Formen  $x^2 + 5y^2$  und  $2x^2 + 2xy + 3y^2$  . . . . . 168
- §. 72. Positive Determinanten. Erste und zweite Wurzel einer Form 170
- §. 73. Beziehungen zwischen den gleichnamigen oder ungleichnamigen Wurzeln zweier eigentlich oder uneigentlich äquivalenten Formen. Benachbarte Formen . . . . . 171
- §. 74. Reducirte Formen von positiver Determinante; Eigenschaften ihrer Wurzeln . . . . . 173
- §. 75. Es giebt nur eine endliche Anzahl reducirter Formen von einer gegebenen positiven Determinante . . . . . 176
- §. 76. Jede Form von positiver Determinante ist einer reducirten Form äquivalent . . . . . 177
- §. 77. Jede reducirte Form von positiver Determinante hat eine und nur eine nach rechts benachbarte reducirte Form, und ebenso eine und nur eine nach links benachbarte reducirte Form . . . . . 180
- §. 78. Eintheilung der reducirten Formen von positiver Determinante in Perioden von gerader Gliederanzahl . . . . . 182
- §. 79. Entwicklung der Wurzeln der reducirten Formen von positiver Determinante in periodische Kettenbrüche . . . . . 186
- §. 80. Digression über die Umformung unregelmässiger Kettenbrüche in regelmässige . . . . . 190
- §. 81. Lemma aus der Theorie der Kettenbrüche . . . . . 193
- §. 82. Je zwei äquivalente reducirte Formen von positiver Determinante gehören einer und derselben Periode an. Abschluss des Problems, zu entscheiden, ob zwei Formen von gleicher positiver Determinante äquivalent sind oder nicht . . . . . 195
- §. 83. Lösung der Pell'schen Gleichung für positive Determinanten in positiven Zahlen durch die Betrachtung der Perioden der reducirten Formen . . . . . 197

	Seite
§. 84. Kleinste positive Auflösung der Pell'schen Gleichung . . . . .	204
§. 85. Darstellung aller Auflösungen der Pell'schen Gleichung durch die kleinste positive Auflösung derselben . . . . .	206

**Fünfter Abschnitt: Bestimmung der Anzahl der Classen, in welche die binären quadratischen Formen von gegebener Determinante zerfallen.**

§. 86. Feststellung des Gebietes von Zahlen, welche durch das vollständige System ursprünglicher Formen der ersten oder zweiten Art eigentlich dargestellt werden . . . . .	210
§. 87. Anzahl dieser Darstellungen für den Fall einer negativen Determinante; für den Fall einer positiven Determinante wird die Anzahl der Darstellungen dadurch auf eine endliche reducirt, dass den darstellenden Zahlen neue Beschränkungen auferlegt werden . . . . .	212
§. 88. Recapitulation. Doppelte Erzeugungsart desselben Gebietes von Zahlen. Fundamentalgleichung . . . . .	216
§. 89. Umformung der rechten Seite . . . . .	218
§. 90. Die Fundamentalgleichung wird so umgeformt, dass auch uneigentliche Darstellungen zugelassen werden . . . . .	221
§. 91. Digression über die Anzahl aller Darstellungen einer Zahl durch das Formensystem. Anwendung auf die Zerlegung der Zahlen in zwei Quadratzahlen . . . . .	224
§. 92. Digression über einige in der Theorie der Elliptischen Functionen auftretende unendliche Reihen . . . . .	227
§. 93. Beschränkungen, welche den die Formenclassen repräsentirenden Formen auferlegt werden . . . . .	230
§. 94. Eintheilung der Werthenpaare der darstellenden Zahlen in eine bestimmte Anzahl von arithmetischen Doppelreihen . . . . .	232
§. 95. Grenzwert der linken Seite der Fundamentalgleichung für den Fall einer negativen Determinante . . . . .	236
§. 96. Ausdruck der Classenzahl für eine negative Determinante als Grenzwert einer unendlichen Reihe . . . . .	239
§. 97. Beziehung zwischen der Classenzahl der Formen der ersten Art und der Classenzahl der Formen der zweiten Art für eine negative Determinante . . . . .	240
§. 98. Grenzwert der linken Seite der Fundamentalgleichung für den Fall einer positiven Determinante; Ausdruck der Classenzahl als Grenzwert einer unendlichen Reihe . . . . .	241
§. 99. Beziehung zwischen der Classenzahl der Formen der ersten Art und der Classenzahl der Formen der zweiten Art für eine positive Determinante . . . . .	245
§. 100. Reduction der Bestimmung der Classenzahl auf den Fall, dass die Determinante durch keine Quadratzahl theilbar ist . . . . .	248
§. 101. Untersuchung über die Convergenz und über die Stetigkeit der zu betrachtenden unendlichen Reihen . . . . .	251
§. 102. Besondere Behandlung des ersten Hauptfalls, in welchem die Determinante die Form $4n + 1$ hat . . . . .	255

	Seite
§. 103. Summation der unendlichen Reihe für diesen Fall . . . . .	257
§. 104. Endresultat für diesen Fall . . . . .	261
§. 105. Summation der unendlichen Reihe in den übrigen Fällen . . . . .	264
§. 106. Zusammenstellung der Formeln, durch welche die Classenanzahl bestimmt wird . . . . .	272
§. 107. Betrachtung der den positiven Determinanten entsprechenden Formeln; Umformung des Endresultates für den Fall $D \equiv 1$ (mod. 4) . . . . .	274
§. 108. Umformung für den Fall $D \equiv 3$ (mod. 4) . . . . .	276
§. 109. Umformung für den Fall $D \equiv 2$ (mod. 8) . . . . .	278
§. 110. Umformung für den Fall $D \equiv 6$ (mod. 8) . . . . .	279

## S u p p l e m e n t e .

### I. Ueber einige Sätze aus der Theorie der Kreistheilung von Gauss.

§. 111. Lemma aus der Theorie der Fourier'schen Reihen . . . . .	283
§. 112. Bestimmung des Werthes der Summe $\varphi(h, n)$ für den Fall, in welchem $n \equiv 0$ (mod. 4) und $h = 1$ ist . . . . .	285
§. 113. Allgemeine Sätze über die Summen $\varphi(h, n)$ . . . . .	289
§. 114. Bestimmung von $\varphi(1, n)$ . . . . .	291
§. 115. Bestimmung von $\varphi(h, n)$ wenn $n$ eine ungerade Primzahl ist; dritter Beweis des Reciprocitätssatzes, und der Sätze über den Charakter der Zahlen $-1$ und $2$ . . . . .	293
§. 116. Beweis eines in den §§. 103, 105 benutzten Satzes . . . . .	296

### II. Ueber den Grenzwert einer unendlichen Reihe.

§. 117. Beweis eines Satzes aus der Theorie der harmonischen Reihen . . . . .	300
§. 118. Ausspruch und Erläuterung eines allgemeineren Satzes . . . . .	302
§. 119. Beweis desselben . . . . .	304

### III. Ueber einen geometrischen Satz.

§. 120. Zusammenhang zwischen dem Flächeninhalt einer ebenen Figur und der Anzahl der innerhalb dieser Figur liegenden Gitterpunkte . . . . .	307
---	-----

### IV. Ueber die Geschlechter, in welche die Classen der quadratischen Formen von bestimmter Determinante zerfallen.

§. 121. Sätze über den Charakter aller durch eine und dieselbe quadratische Form darstellbaren Zahlen . . . . .	309
§. 122. Eintheilung der quadratischen Formen in Geschlechter . . . . .	311
§. 123. Beweis, dass der einen Hälfte der angebbaren Totalcharaktere keine wirklich existirenden Formen entsprechen . . . . .	315

	Seite
§. 124. Beweis einer Gleichung zwischen zwei Producten aus je zwei unendlichen Reihen . . . . .	316
§. 125. Beweis, dass der einen Hälfte der angebbaren Totalcharaktere wirklich existirende Geschlechter entsprechen, und dass jedes dieser Geschlechter gleich viele Formenklassen enthält . . . . .	319
§. 126. Vervollständigung dieses Beweises . . . . .	324

**V. Theorie der Potenzreste für zusammengesetzte Moduli.**

§. 127. Dritter Beweis des verallgemeinerten Fermat'schen Satzes (§. 19) . . . . .	327
§. 128. Beweis der Existenz von primitiven Wurzeln für einen Modulus, der eine beliebige Potenz einer ungeraden Primzahl ist . . . . .	328
§. 129. Theorie der Indices für solche Moduli . . . . .	332
§. 130. Fall, wenn der Modulus eine Potenz der Zahl 2 ist; Indices . . . . .	333
§. 131. Fall, wenn der Modulus eine beliebig zusammengesetzte Zahl ist; Indices . . . . .	335

**VI. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält.**

§. 132. Beweis einer allgemeinen Gleichung zwischen einem unendlichen Product und einer unendlichen Reihe . . . . .	338
§. 133. Specialisirung dieses Satzes; Eintheilung der Reihen $L$ in drei Classen $L_1, L'_2, L_3$ . . . . .	341
§. 134. Grenzwerte dieser Reihen . . . . .	344
§. 135. Beweis, dass die Grenzwerte der Reihen $L_2$ von Null verschieden sind; Zusammenhang mit der Theorie der quadratischen Formen . . . . .	347
§. 136. Beweis, dass die Grenzwerte der Reihen $L_3$ von Null verschieden sind . . . . .	350
§. 137. Beweis des Satzes über die arithmetische Progression . . . . .	353

**VII. Ueber einige Sätze aus der Theorie der Kreistheilung.**

§. 138. Beweis einer Eigenschaft des Ausdrucks $\varphi(m)$ . . . . .	356
§. 139. Bildung der Gleichung, deren Wurzeln die primitiven $m$ ten Wurzeln der Einheit sind; Zerlegung der linken Seite derselben in zwei Factoren, für den Fall, dass $m$ eine ungerade durch kein Quadrat theilbare Zahl $P$ ist . . . . .	359
§. 140. Berechnung der Coefficienten dieser Factoren . . . . .	362

**VIII. Ueber die Pell'sche Gleichung.**

§. 141. Satz über die rationalen Näherungswerte für die Quadratwurzel aus einer positiven Zahl $D$ , welche keine vollständige Quadratzahl ist . . . . .	366
§. 142. Beweis des Satzes, dass der Gleichung $t^2 - Du^2 = 1$ immer durch ganze Zahlen $t, u$ Genüge geschehen kann, deren letztere $u$ von Null verschieden ist . . . . .	368

<b>IX. Ueber die Convergenz und Stetigkeit einiger unendlichen Reihen.</b>	
§. 143. Methode der theilweisen Summation . . . . .	371
§. 144. Eigenschaften der Dirichlet'schen Reihen . . . . .	375
<b>X. Ueber die Composition der binären quadratischen Formen.</b>	
§. 145. Lemma über die Congruenzen zweiten Grades . . . . .	380
§. 146. Composition zweier einigen Formen. Fundamentalsatz . . . . .	381
§. 147. Composition zweier oder mehrerer einigen Classen . . . . .	384
§. 148. Wichtigste specielle Fälle der Composition . . . . .	386
§. 149. Perioden und Gruppen von ursprünglichen Classen der ersten Art . . . . .	387
§. 150. Vergleichung der Anzahl der Classen von beliebigem-Theiler mit der Anzahl der ursprünglichen Classen der ersten Art . . . . .	389
§. 151. Resultat dieser Vergleichung . . . . .	392
§. 152. Composition der Geschlechter . . . . .	399
§. 153. Anzahl der ambigen ursprünglichen Classen erster Art . . . . .	401
§. 154. Vierter Beweis des Reciprocitätssatzes . . . . .	404
§. 155. Ueber die Anzahl der wirklich existirenden Geschlechter . . . . .	406
§. 156. Ableitung aller Lösungen der Gleichung $ax^2 + by^2 + cz^2 = 0$ aus einer gegebenen . . . . .	408
§. 157. Hauptsatz über die Lösbarkeit dieser Gleichung . . . . .	418
§. 158. Jede Classe des Hauptgeschlechtes entsteht durch Duplication . . . . .	422
§. 159. Endliche Körper . . . . .	423
§. 160. Ganze algebraische Zahlen . . . . .	436
§. 161. Theorie der Moduln . . . . .	442
§. 162. Ganze Zahlen eines endlichen Körpers . . . . .	445
§. 163. Theorie der Ideale eines endlichen Körpers . . . . .	452
§. 164. Idealclassen und Composition derselben . . . . .	462
§. 165. Zerlegbare Formen . . . . .	465
§. 166. Theorie der Einheiten . . . . .	471
§. 167. Methode zur Bestimmung der Anzahl der Idealclassen . . . . .	480
§. 168. Primideale in quadratischen Körpern . . . . .	485
§. 169. Moduln in quadratischen Körpern . . . . .	488
§. 170. Composition der quadratischen Formen . . . . .	490