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_0153
LOG Titel: VII. ueber einige Sätze aus der Theorie der Kreistheilung.
LOG Typ: chapter

Contact

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

VII. Ueber einige Sätze aus der Theorie der Kreistheilung.

§. 138.

Sind $p, p', p'' \ldots$ positive und von einander verschiedene Primzahlen, so stimmen (nach §. 9) die Glieder des entwickelten Productes

$$(p+1)\,(p'+1)\,(p''+1)\ldots$$

mit den sämmtlichen Divisoren des Productes

$$P = pp'p'' \ldots$$

überein; dieselben Divisoren entstehen offenbar auch durch die Entwicklung des Productes

$$(p-1)\,(p'-1)\,(p''-1)\ldots,$$

aber die eine Hälfte derselben wird mit positivem, die andere mit negativem Zeichen behaftet sein; wir wollen die erstern mit δ_1, die letztern mit δ_2 bezeichnen, so dass

$$(p-1)\,(p'-1)\,(p''-1)\ldots = \Sigma\,\delta_1 - \Sigma\,\delta_2$$

wird, und wir bemerken, dass die Zahl P selbst zu der Classe der erstern gehört. Ist nun δ irgend ein Divisor von P, aber $< P$, so lässt sich leicht zeigen, dass die Anzahl der durch δ theilbaren Zahlen δ_1 genau gleich der Anzahl der durch δ theilbaren Zahlen δ_2 ist. Denn wenn man mit $q, q', q'' \ldots$ alle diejenigen Primfactoren von P bezeichnet, welche nicht in δ aufgehen, so stimmen die durch δ theilbaren Zahlen δ_1 und $-\delta_2$ resp. mit den positiven und negativen Gliedern des entwickelten Productes

$$\delta(q-1)\,(q'-1)\,(q''-1)\ldots$$

überein, und da $\delta < P$ ist, also mindestens eine solche Primzahl q vorhanden ist, so ist die Anzahl der positiven Glieder dieses Productes genau gleich der Anzahl der negativen.

Dieser Satz lässt sich leicht verallgemeinern. Bedeutet m irgend eine positive ganze Zahl > 1, und sind $p, p', p'' \ldots$ die sämmtlichen von einander verschiedenen in m aufgehenden positiven Primzahlen, so kann man

$$m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\cdots = \Sigma\,\mu_1 - \Sigma\,\mu_2$$

setzen, wo mit μ_1 und $-\mu_2$ resp. alle positiven und negativen Glieder des entwickelten Productes linker Hand bezeichnet sind. Behält man die vorhergehenden Bezeichnungen bei, so stimmen offenbar die Zahlen μ_1 und μ_2 resp. mit den Zahlen $m'\delta_1$ und $m'\delta_2$ überein, wenn zur Abkürzung $m = m'P$ gesetzt wird. Bedeutet nun μ irgend einen Divisor von m, mit Ausnahme von m selbst, so folgt hieraus wieder, dass unter den Zahlen μ_1 ebenso viele durch μ theilbar sein werden, wie unter den Zahlen μ_2. Denn, wenn μ' der grösste gemeinschaftliche Divisor von μ und m' ist, so kann man $\mu = \mu'\delta$ setzen, wo δ nothwendig ein Divisor von P, und zwar $< P$ sein muss; und da eine Zahl $\mu_1 = m'\delta_1$ oder $\mu_2 = m'\delta_2$ stets und nur dann durch $\mu = \mu'\delta$ theilbar ist, sobald resp. δ_1 oder δ_2 durch δ theilbar ist, so ergiebt sich in der That, dass die Anzahl der durch μ theilbaren Zahlen μ_1 genau gleich der Anzahl der durch μ theilbaren Zahlen μ_2 ist.

Von dieser Eigenschaft der Zahlen μ_1 und μ_2 kann man vielfache Anwendungen machen. Hängen z. B. zwei Functionen $f(m)$ und $F(m)$ einer beliebigen ganzen Zahl m durch eine der beiden Relationen

$$\Sigma f(\mu) = F(m)$$

oder

$$\Pi f(\mu) = F(m)$$

zusammen, wo das Summen- oder Productzeichen sich jedesmal auf alle Divisoren μ (incl. m) der Zahl m bezieht, so folgt daraus resp. die Umkehrung

$$f(m) = \Sigma\,F(\mu_1) - \Sigma\,F(\mu_2)$$

oder

$$f(m) = \frac{\Pi\,F(\mu_1)}{\Pi\,F(\mu_2)},$$

wo die Summen- oder Productzeichen sich auf alle Werthe von μ_1 oder auf alle Werthe von μ_2 beziehen; denn ersetzt man rechts jeden Werth $F(\mu_1)$ und $F(\mu_2)$ durch die Summe oder das Product der Werthe $f(\mu)$, die den sämmtlichen Divisoren μ von μ_1 oder μ_2 entsprechen, so werden zufolge der obigen Eigenschaft der Zahlen μ_1, μ_2 alle Werthe $f(\mu)$ sich aufheben, in welchen $\mu < m$ ist, und es wird allein der Werth $f(m)$ zurückbleiben.

Als Beispiel wählen wir die Aufgabe, die Anzahl $\varphi(m)$ der ganzen Zahlen zu bestimmen, welche relative Primzahlen zu m und nicht grösser als m sind; aus dieser Definition der Function $\varphi(m)$ ist in §. 13 ohne alle Rechnung der Satz abgeleitet, dass

$$\Sigma\, \varphi(\mu) = m$$

ist, wo das Summenzeichen sich auf alle Divisoren μ von m bezieht; setzen wir daher $F(m) = m$, so ergiebt sich umgekehrt

$$\varphi(m) = \Sigma\, \mu_1 - \Sigma\, \mu_2,$$

also

$$\varphi(m) = m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{p''}\right)\cdots;$$

diese Function ist daher durch den Satz des §. 13 schon vollständig charakterisirt.

Ein anderes Beispiel ist folgendes. Ist der Werth der Function $f(m) = p$, sobald die Zahl m eine Potenz einer Primzahl p ist, dagegen $= 1$, so oft $m = 1$ oder durch mehrere verschiedene Primzahlen theilbar ist, so leuchtet ein, dass

$$\Pi\, f(\mu) = m$$

ist, wo das Productzeichen sich auf alle Divisoren μ von m bezieht; hieraus folgt nach dem obigen Satze, dass umgekehrt der Quotient

$$\frac{\Pi\, \mu_1}{\Pi\, \mu_2} = f(m),$$

also nur dann von 1 verschieden ist, wenn m eine Potenz einer Primzahl ist; und zwar ist dieser Quotient dann gleich dieser Primzahl.

Aus der Definition der Divisoren μ_1 und μ_2 folgt endlich auch, dass stets

$$\psi(m')\,(\psi(p)-1)\,(\psi(p')-1)\,(\psi(p'')-1)\ldots = \Sigma\,\psi(\mu_1) - \Sigma\,\psi(\mu_2)$$

ist, wenn die Function ψ die Eigenschaft $\psi(z)\,\psi(z') = \psi(zz')$ besitzt.

§. 139.

Die sämmtlichen Wurzeln ϱ der Gleichung

$$x^m = 1 \tag{1}$$

sind bekanntlich in der Form enthalten

$$\varrho = \cos\frac{2n\pi}{m} + i\sin\frac{2n\pi}{m},$$

wo n irgend ein vollständiges Restsystem (mod. m) durchlaufen muss.

Ist n relative Primzahl zu m, so sind die Potenzen

$$1, \varrho, \varrho^2, \ldots \varrho^{m-1}$$

sämmtlich ungleich, und sie bilden die sämmtlichen Wurzeln der obigen Gleichung (1); ϱ heisst in diesem Fall eine *primitive* Wurzel dieser Gleichung, und die Anzahl dieser primitiven Wurzeln ist offenbar $= \varphi(m)$. Ist allgemeiner ν der grösste gemeinschaftliche Divisor von n und $m = \mu\nu$, so ist ϱ eine primitive Wurzel der Gleichung

$$x^\mu = 1, \tag{2}$$

und da umgekehrt jede Wurzel der letztern Gleichung (2) auch eine Wurzel der Gleichung (1) ist, so leuchtet ein, dass die sämmtlichen Wurzeln der Gleichung (1) identisch sind mit allen primitiven Wurzeln aller der Gleichungen (2), die den sämmtlichen Divisoren μ der Zahl m entsprechen. Bezeichnet man daher mit ϱ' alle $\varphi(\mu)$ primitiven Wurzeln der Gleichung (2), und setzt

$$f(\mu) = \Pi(x - \varrho'),$$

wo das Productzeichen sich auf alle Wurzeln ϱ' bezieht, so ist

$$\Pi f(\mu) = x^m - 1,$$

wo das Productzeichen sich auf alle Divisoren μ der Zahl m bezieht; durch Umkehrung dieser für jede Zahl m geltenden Relation erhält man nach dem vorhergehenden Paragraphen

$$f(m) = \frac{\Pi(x^{\mu_1} - 1)}{\Pi(x^{\mu_2} - 1)},$$

woraus folgt, dass die Coefficienten der Function $f(m)$ sämmtlich ganze rationale Zahlen sind.

Von jetzt an betrachten wir nur noch den Fall, in welchem $m = P = pp'p'' \ldots$ eine ungerade und durch kein Quadrat theilbare ganze Zahl > 1 ist. Dann wird

$$\varphi(P) = (p-1)(p'-1)(p''-1)\ldots = \Sigma\mu_1 - \Sigma\mu_2$$

eine gerade Zahl, die wir mit 2τ bezeichnen wollen, und die sämmtlichen 2τ relativen Primzahlen zu P, welche $< P$ sind, zerfallen in τ Zahlen a und in τ Zahlen b von der Beschaffenheit, dass

$$\left(\frac{a}{P}\right) = +1, \quad \left(\frac{b}{P}\right) = -1$$

ist (§. 52. I. oder Supplemente §. 116). Setzen wir daher

$$\theta = \cos\frac{2\pi}{P} + i\sin\frac{2\pi}{P} = e^{\frac{2\pi i}{P}}$$

und

$$A(x) = \Pi(x-\theta^a), \quad B(x) = \Pi(x-\theta^b),$$

so wird

$$A(x)\,B(x) = \frac{\Pi(x^{\mu_1}-1)}{\Pi(x^{\mu_2}-1)},$$

und wir wollen im Folgenden die allgemeine Form der Coefficienten der Functionen $A(x)$, $B(x)$ bestimmen.

Zu diesem Zwecke erinnern wir zunächst an die Newton'schen Formeln, welche dazu dienen, aus den Coefficienten einer Gleichung die Summen gleich hoher Potenzen ihrer Wurzeln, und umgekehrt aus diesen jene abzuleiten. Es seien

$$w_1, \; w_2 \ldots w_m$$

die Wurzeln einer Gleichung

$$x^m + c_1 x^{m-1} + c_2 x^{m-2} + \cdots + c_m = 0,$$

und

$$S_k = w_1^k + w_2^k + \cdots + w_m^k,$$

so lauten diese Formeln folgendermaassen:

$$\begin{aligned}
&S_1 + c_1 = 0\\
&S_2 + c_1 S_1 + 2c_2 = 0\\
&S_3 + c_1 S_2 + c_2 S_1 + 3c_3 = 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&S_m + c_1 S_{m-1} + c_2 S_{m-2} + \cdots + c_{m-1} S_1 + m c_m = 0.
\end{aligned}$$

Aus der Form derselben geht hervor, dass S_1, S_2 ... S_m ganze rationale Zahlen sein werden, sobald die Coefficienten c_1, c_2 ... c_m sämmtlich ganze rationale Zahlen sind. Wenden wir dies auf die Gleichung

$$\frac{\Pi\,(x^{\mu_1}-1)}{\Pi\,(x^{\mu_2}-1)}=0$$

an, so ergiebt sich, dass

$$S_k=\Sigma\,\theta^{ak}+\Sigma\,\theta^{bk}$$

für jeden Werth $k=1, 2, 3\ldots$ eine ganze Zahl ist. Andererseits ist nun (Supplemente §. 116)

$$\Sigma\,\theta^{ak}-\Sigma\,\theta^{bk}=\left(\frac{k}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

und folglich

$$\Sigma\,\theta^{ak}=\tfrac{1}{2}\left(S_k+\left(\frac{k}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P}\right)$$

$$\Sigma\,\theta^{bk}=\tfrac{1}{2}\left(S_k-\left(\frac{k}{P}\right)i^{\frac{1}{4}(P-1)^2}\sqrt{P}\right);$$

hiermit sind die Summen der $k$ten Potenzen der Wurzeln von jeder der beiden Gleichungen

$$A(x)=0,\quad B(x)=0$$

gefunden, und da dieselben keine andere Irrationalität enthalten als die Quadratwurzel

$$i^{\frac{1}{4}(P-1)^2}\sqrt{P},$$

so gilt zufolge der Newton'schen Formeln dasselbe von sämmtlichen Coefficienten dieser beiden Gleichungen, und zwar werden zwei gleich hohe Coefficienten in beiden Gleichungen sich nur durch das Vorzeichen dieser Quadratwurzel von einander unterscheiden, d. h. zwei solche Coefficienten werden die Formen

$$y-zi^{\frac{1}{4}(P-1)^2}\sqrt{P}\quad\text{und}\quad y+zi^{\frac{1}{4}(P-1)^2}\sqrt{P}$$

haben, wo y und z rationale Zahlen bedeuten. Man kann ferner behaupten, dass y und z entweder ganze Zahlen oder Brüche mit dem Nenner 2 sind, obgleich dies aus den Newton'schen Formeln nicht unmittelbar hervorgeht; um den Beweis dieser Behauptung anzudeuten, wollen wir jede Gleichung, deren höchster Coefficient $=1$, und deren übrige Coefficienten ganze rationale Zahlen sind, eine primäre Gleichung nennen; dann überzeugt man sich leicht, dass die Summe und Differenz zweier Wurzeln von primären

Gleichungen (und ebenso ihr Product) wieder Wurzeln von primären Gleichungen sind; da nun θ die Wurzel einer primären Gleichung ist, so gilt dasselbe von jedem Coefficienten der Functionen $A(x)$ und $B(x)$ und folglich auch von

$$2y \quad \text{und} \quad 2z i^{\frac{1}{4}(P-1)^2} \sqrt{P},$$

und hieraus folgt sogleich, dass die rationalen Zahlen $2y$ und $2z$ *ganze* Zahlen sein müssen.

Fasst man dies zusammen, so ergiebt sich, dass man gleichzeitig

$$2A(x) = Y(x) - Z(x) i^{\frac{1}{4}(P-1)^2} \sqrt{P}$$
$$2B(x) = Y(x) + Z(x) i^{\frac{1}{4}(P-1)^2} \sqrt{P}$$

setzen kann, wo $Y(x)$ und $Z(x)$ ganze Functionen bedeuten, deren sämmtliche Coefficienten ganze rationale Zahlen sind*). Multiplicirt man die beiden Gleichungen mit einander, so erhält man

$$Y(x)^2 - \left(\frac{-1}{P}\right) P\, Z(x)^2 = 4 \frac{\prod (x^{\mu_1} - 1)}{\prod (x^{\mu_2} - 1)}.$$

§. 140.

Wir bemerken nun noch, dass man immer nur die Hälfte der Coefficienten von $Y(x)$ und $Z(x)$ zu berechnen braucht. Es ist nämlich

$$x^\tau A\left(\frac{1}{x}\right) = \prod (1 - \theta^a x) = (-1)^\tau \theta^{\Sigma a} \prod (x - \theta^{-a})$$

$$x^\tau B\left(\frac{1}{x}\right) = \prod (1 - \theta^b x) = (-1)^\tau \theta^{\Sigma b} \prod (x - \theta^{-b});$$

nun ist, je nachdem $P \equiv 1$, oder $P \equiv 3 \pmod 4$ ist,

$$\left(\frac{-1}{P}\right) = +1, \text{ oder } \left(\frac{-1}{P}\right) = -1,$$

und folglich

$$\prod (x - \theta^{-a}) = A(x), \quad \prod (x - \theta^{-b}) = B(x)$$

oder

$$\prod (x - \theta^{-a}) = B(x), \quad \prod (x - \theta^{-b}) = A(x);$$

*) Vergl. *Gauss: D. A.* art. 357.

ist ferner P nicht $= 3$, so existirt unter den Zahlen a eine Zahl a' von der Beschaffenheit, dass $(a'-1)$ relative Primzahl zu P ist, und da die Reste der Producte aa' mit den Zahlen a, und die Reste der Producte ba' mit den Zahlen b im Complex übereinstimmen, so ist

$$a' \Sigma a \equiv \Sigma a, \quad a' \Sigma b \equiv \Sigma b \pmod{P}$$

und folglich

$$\Sigma a \equiv 0, \quad \Sigma b \equiv 0 \pmod{P},$$

also

$$\theta^{\Sigma a} = 1, \quad \theta^{\Sigma b} = 1.$$

Mithin ergiebt sich (da τ gerade, sobald $P \equiv 1 \pmod 4$)

$$\left.\begin{aligned} A(x) &= x^\tau A\left(\frac{1}{x}\right) \\ B(x) &= x^\tau B\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod 4$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} A(x) &= (-x)^\tau B\left(\frac{1}{x}\right) \\ B(x) &= (-x)^\tau A\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod 4$$

und hieraus

$$\left.\begin{aligned} Y(x) &= x^\tau Y\left(\frac{1}{x}\right) \\ Z(x) &= x^\tau Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 1 \pmod 4$$

und, mit Ausnahme von $P = 3$,

$$\left.\begin{aligned} Y(x) &= (-x)^\tau Y\left(\frac{1}{x}\right) \\ -Z(x) &= (-x)^\tau Z\left(\frac{1}{x}\right) \end{aligned}\right\}, \text{ wenn } P \equiv 3 \pmod 4$$

Diese Gleichungen enthalten Relationen zwischen je zwei gleich weit vom Anfang und Ende abstehenden Coefficienten der Functionen $Y(x)$ und $Z(x)$.

Die wirkliche Berechnung der Coefficienten der beiden Functionen

$$Y(x) = y_0 x^\tau + y_1 x^{\tau-1} + \cdots + y_\tau$$
$$Z(x) = z_0 x^\tau + z_1 x^{\tau-1} + \cdots + z_\tau$$

geschieht nun auf folgende Art. Zuerst bildet man die Potenzsummen

$$S_k = \Sigma\, \theta^{ak} + \Sigma\, \theta^{bk}$$

für $k = 1, 2, 3 \ldots$ bis zu $\frac{1}{2}\tau$ oder $\frac{1}{2}(\tau - 1)$, je nachdem τ gerade oder ungerade ist; dies kann nach dem Obigen dadurch geschehen, dass man ebenso viele Coefficienten der ganzen Function

$$\frac{\Pi\,(x^{\mu_1} - 1)}{\Pi\,(x^{\mu_2} - 1)}$$

vom höchsten an gerechnet durch wirkliche Division bestimmt, und dann die Newton'schen Formeln anwendet; indessen hält es nicht schwer, durch Betrachtungen, welche ebenfalls auf der im §. 138 bewiesenen Haupteigenschaft der Zahlen μ_1 und μ_2 beruhen, folgende Regel abzuleiten: es sei Q der grösste gemeinschaftliche Divisor von k und $P = QR$, und r die Anzahl der in R aufgehenden Primzahlen, so ist*)

$$S_k = (-1)^r \varphi(Q).$$

Nachdem diese Werthe S_k gefunden sind, erhält man die Coefficienten der Functionen $Y(x)$ und $Z(x)$ durch die beiden aus den Newton'schen Formeln abgeleiteten Recursionsgleichungen

$$2k y_k = \left\{ \begin{array}{c} -\left[S_k y_0 + S_{k-1} y_1 + \cdots + S_1 y_{k-1}\right] \\ +\left(\frac{-1}{P}\right) P\left[\left(\frac{k}{P}\right) z_0 + \left(\frac{k-1}{P}\right) z_1 + \cdots + \left(\frac{1}{P}\right) z_{k-1}\right] \end{array} \right\}$$

$$2k z_k = \left\{ \begin{array}{c} +\left[\left(\frac{k}{P}\right) y_0 + \left(\frac{k-1}{P}\right) y_1 + \cdots + \left(\frac{1}{P}\right) y_{k-1}\right] \\ -\left[S_k z_0 + S_{k-1} z_1 + \cdots + S_1 z_{k-1}\right] \end{array} \right\}$$

wenn man noch berücksichtigt, dass

$$y_0 = 2, \quad z_0 = 0$$

ist.

---

*) Allgemeiner lautet diese Regel so: ist $m = m'P$ eine beliebige positive ganze Zahl, P das Product aus allen von einander verschiedenen in m aufgehenden Primzahlen, und S_k die Summe der $k$ten Potenzen aller primitiven Wurzeln der Gleichung $x^m = 1$, so ist $S_k = 0$, so oft k nicht durch m' theilbar ist; ist aber $k = m'K$, ferner Q der grösste gemeinschaftliche Divisor von K und $P = QR$, und r die Anzahl der in R aufgehenden Primzahlen, so ist

$$S_k = (-1)^r m' \varphi(Q).$$

Beispiel 1: $P = 3$; in diesem Falle müssen alle Coefficienten berechnet werden; da

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man

$$2y_1 = -S_1 y_0 = 2, \quad 2z_1 = \left(\frac{1}{P}\right) y_0 = 2,$$

und folglich

$$Y(x) = 2x + 1, \quad Z(x) = 1.$$

Beispiel 2: $P = 5$; $\tau = 2$; da wieder

$$S_1 = -1, \quad \left(\frac{1}{P}\right) = 1$$

ist, so erhält man auch wieder

$$y_1 = 1, \quad z_1 =$$

und folglich

$$Y(x) = 2x^2 + x + 2, \quad Z(x) = x.$$

Beispiel 3: $P = 15 = 3.5$; $\tau = 4$; hier ist

$$S_1 = S_2 = 1; \quad \left(\frac{1}{P}\right) = \left(\frac{2}{P}\right) = 1; \quad \left(\frac{-1}{P}\right) = -1;$$

und folglich erhält man successive

$$y_1 = -1, \quad z_1 = 1$$

und

$$y_2 = -4, \quad z_2 = 0;$$

also ist

$$Y(x) = 2x^4 - x^3 - 4x^2 - x + 2, \quad Z(x) = x^3 - x.$$