

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_0155

LOG Titel: S. 139. Bildung der Gleichung, deren Wurzeln die primitiven mten Wurzeln der Einheit sind; Zerlegung der linken Seite derselben in zwei Factoren, für den Fall, dass m eine ungerade durch kein Quadrat theilb

LOG Typ: chapter

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 there 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

§. 139.

Die sämtlichen Wurzeln ϱ der Gleichung

$$x^m = 1 \quad (1)$$

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

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

sämmtlich ungleich, und sie bilden die sämtlichen 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

$$x^\mu = 1, \quad (2)$$

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

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

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

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

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

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

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

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

$$\varphi(P) = (p-1)(p'-1)(p''-1)\dots = \sum \mu_1 - \sum \mu_2$$

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

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

so wird

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

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

$$w_1, w_2 \dots w_m$$

die Wurzeln einer Gleichung

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

und

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

so lauten diese Formeln folgendermaassen:

$$S_1 + c_1 = 0$$

$$S_2 + c_1 S_1 + 2 c_2 = 0$$

$$S_3 + c_1 S_2 + c_2 S_1 + 3 c_3 = 0$$

.....

$$S_m + c_1 S_{m-1} + c_2 S_{m-2} + \dots + c_{m-1} S_1 + m c_m = 0.$$

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

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

an, so ergibt sich, dass

$$S_k = \sum \theta^{ak} + \sum \theta^{bk}$$

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

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

und folglich

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

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

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

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

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 $\doteq 1$, 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