Zur Theorie der Kreisteilungsgleichung $K_m(x) = 0$.

von

O. Hölder in Leipzig.

§ 1. Die werte $K'_m(1)$.

Setzt man

$$K_m(x) = \prod_{(l,m)=1} \left(x - e^{\frac{2\pi i l}{m}}\right), \tag{1}$$

wo der Index l die zur festen Zahl m teilerfremden Zahlen $\leqq m$ durchläuft, so stellt

$$K_m(x) = 0 \tag{2}$$

die Gleichung $\varphi(m)$-ten Grades vor, der die primitiven m-ten Einheitswurzeln genügen. Falls $m > 2$ ist, zerfallen die Wurzeln der Gleichung in Paare von konjugiert komplexen, weshalb dann das Polynom $K_m(x)$ für reelle x stets positiv ist.

Bekanntlich ist nun

$$x^m - 1 = \prod_{d|m} K_m(x).$$

Logarithmiert gibt diese Gleichung

$$\log(x^m - 1) = \sum_{d|m} \log K_d(x), \tag{3}$$

woraus durch das Umkehrungsverfahren

$$\log K_m(x) = \sum_{d|m} \mu(d) \log \left(x^{\frac{m}{d}} - 1\right) \tag{4}$$

folgt. Hier bedeutet $\mu(n)$ die Moebiussche zahlentheoretische Funktion; es ist $\mu(n) = 0$, wenn n eine Primzahl doppelt enthält, und $\mu(n) = (-1)^r$ wenn n das Produkt von r verschiedenen Primzahlen ist. Damit hinsichtlich der Logarithmen keine Unklarheit entsteht, will ich annehmen, dass x reell > 1 und dass in den Gleichungen (3) und (4) die Logarithmen reell angenommen werden.

Es ist bereits von K r o n e c k e r *) gezeigt worden, dass für $m > 1$

$$K_m(1) = \begin{cases} 1 \\ p \end{cases}$$

ist, je nachdem m durch zwei verschiedene Primzahlen teilbar oder eine Potenz der Primzahl p ist.

Durch Differentiation der Gleichung (4) ergibt sich

$$\frac{K'_m(x)}{K_m(x)} = \sum_{d|m} \mu(d) \frac{\frac{m}{d} x^{\frac{m}{d}-1}}{x^{\frac{m}{d}} - 1}. \tag{5}$$

Da hier nur eine endliche Anzahl rationaler Ausdrücke vorkommt, erkennt man nachträglich, dass die neue Gleichung (5) für ganz beliebige Werte der Variablen x richtig sein muss. Ich setze

$$x = 1 + h$$

und entwickle für kleine h. Es ist dann

$$\mu(d) \frac{\frac{m}{d} x^{\frac{m}{d}-1}}{x^{\frac{m}{d}} - 1} = \mu(d) \frac{m}{d} \frac{1 + \left(\frac{m}{d} - 1\right) h + \ldots}{\frac{m}{d} h + \frac{1}{2} \frac{m}{d} \left(\frac{m}{d} - 1\right) h^2 + \ldots}$$

$$= \frac{\mu(d)}{h} \left(1 + \left(\frac{m}{d} - 1\right) h + \ldots\right) \left(1 + \frac{1}{2} \left(\frac{m}{d} - 1\right) h + \ldots\right)^{-1}$$

$$= \frac{\mu(d)}{h} + \frac{1}{2} \mu(d) \left(\frac{m}{d} - 1\right) + h \psi(h), \tag{6}$$

*) Vgl. Vorlesungen über Zahlentheorie, 1. Bd., 1901, S. 286. Der Satz selbst ist ohne Beweis von V. A. L e b e s g u e früher ausgesprochen worden (Liouvillesches Journ., 2. Ser., 4. Bd (1859), S. 106/07).

wo $\psi(h)$ eine „gewöhnliche" Potenzreihe von h bezeichnet. Summiert man nun über alle Teiler d von m, so gibt, falls $m > 1$ ist, das erste Glied rechts von (6) die Summe 0, und man erhält mit Rücksicht auf (5) beim Grenzübergang $x \to 1$ oder $h \to 0$, da ja $K_m(1) \neq 0$ ist,

$$\frac{K'_m(1)}{K_m(1)} = \frac{1}{2} \sum_{d|m} \mu(d) \left(\frac{m}{d} - 1\right) = \frac{1}{2} \sum_{d|m} \mu(d) \frac{m}{d}.$$

Die letzte Summe ist aber bekanntlich gleich der Eulerschen Funktion $\varphi(m)$, welche die Anzahl der zu m teilerfremden Zahlen $\leq m$ vorstellt.

Es ist also

$$K'_m(1) = \frac{1}{2} \varphi(m),$$

wenn m mehr als eine Primzahl enthält, und

$$K'_m(1) = \frac{1}{2} p^k (p - 1),$$

wenn $m = p^k$ und p eine Primzahl ist.

§ 2. Die Summe von Ramanujan.

Als „Summe von R a m a n u j a n" wird meist die Summe der n-ten Potenzen der primitiven m-ten Einheitswurzeln

$$c_m(n) = \sum_{(l,\, m) = 1} e^{\frac{2\pi i l}{m} n} \tag{7}$$

bezeichnet. *) R a m a n u j a n hat den Wert dieser Summe, der offenbar eine ganze Zahl ist, durch die Formel

$$c_m(n) = \sum_{d|(m,\, n)} \mu\left(\frac{m}{d}\right) d \tag{8}$$

bestimmt, **) in welcher der Summationsbuchstabe d alle gemeinsamen Teiler von m und n durchläuft.

*) E. P a s c a l, Repertorium der höheren Analysis, 2. Aufl. d. deutschen Ausgabe, hrsggb. v. E. S a l k o w s k i, 3. Teilband, 1929, S. 1529.

**) Transact. of the Cambridge Philos. Soc., vol. 22, p. 260, No. (2,7).

Dieser Wert kann in eine einfachere Form gesetzt werden. Ich will diese zunächst mit Hilfe des Ausdrucks ableiten, den (8) für $n=1$, d. h. für die Summe der primitiven m-ten Einheitswurzeln selbst liefert:

$$c_m(1) = \mu(m). \tag{9}$$

Hebt man in den Exponenten der Glieder von (7) den grössten gemeinsamen Teiler von m und n aus, so erhält man

$$c_m(n) = \sum_{(l,\, m)=1} e^{\frac{2\pi i l}{m'} n'}, \tag{10}$$

wo

$$\begin{aligned} m &= \tau m' \\ n &= \tau n' \end{aligned} \tag{11}$$

und n' und m' teilerfremd zu einander sind. Da l die zu m teilerfremden Zahlen $\leqslant m$ durchläuft und somit auch zu m' teilerfremd ist, so ist auch $l n'$ zu m' teilerfremd, und es besteht die Summe (10) aus $\varphi(m)$ Gliedern, die sämmtlich primitive m'-te Einheitswurzeln vorstellen, die aber nicht alle von einander verschieden sein werden. Man kann, wenn l' die zu m' teilerfremden Zahlen $\leqslant m'$ durchläuft.

$$c_m(n) = \sum_{(l',m')=1} a_{l'}\, e^{\frac{2\pi i l'}{m'}} = \sum_{(l',m')=1} a_{l'} \left(e^{\frac{2\pi i}{m'}}\right)^{l'} \tag{12}$$

setzen, wobei die $a_{l'}$ ganze Zahlen $\geqslant 0$ und ihre Summe gleich $\varphi(m)$ ist.

Das Polynom $K_m(x)$ ist ein irreduzibler Faktor *) von $x^m - 1$ mit ganzzahligen Koeffizienten und mit dem höchsten Koeffizienten 1. Die Summe $c_m(n)$ der n-ten Potenzen der Wurzeln der Gleichung (2) ist also eine ganze Zahl (positiv, negativ oder gleich Null). Wegen der Irreduzibilität von (2) kann man in (12) an Stelle von $e^{\frac{2\pi i}{m'}}$ irgend eine andere Wurzel $e^{\frac{2\pi i}{m'} h'}$ der Gleichung setzen, wo also h' zu m' teilerfremd ist. Es entsteht so die Relation

$$c_m(n) = \sum_{(l'\, m')=1} a_{l'}\, e^{\frac{2\pi i}{m'} l' h'}.$$

*) Die Irreduzibilität ist zuerst von Kronecker bewiesen worden (Liouvilles Journal., Bd. 19, S. 177); m. vrgl. auch Arndt, Journ. f. d. reine u. angewandte Math., Bd. 56, S. 178.

Hier lasse ich nun auch h' die sämmtlichen $\varphi(m')$ zu m' teilerfremden Zahlen $\leqslant m'$ durchlaufen und summiere noch einmal. Es erscheint dann rechts jedes $a_{l'}$ mit der Summe aller $\varphi(m')$ primitiven m'-ten Einheitswurzeln multipliziert, die nach (9) gleich $\mu(m')$ ist, und man erhält

$$\varphi(m') \cdot c_m(n) = \left(\sum_{(l',m')=1} a_{l'}\right) \mu(m').$$

Da aber die Summe der $a_{l'}$ gleich $\varphi(m)$ ist, erhält man

$$c_m(n) = \frac{\varphi(m)}{\varphi(m')}\, \mu(m'),$$

d. h. *es ist die Summe von Ramanujan,*

$$c_m(n) = \frac{\varphi(m)}{\varphi\left(\frac{m}{\tau}\right)}\, \mu\left(\frac{m}{\tau}\right), \tag{13}$$

falls (vgl. (11)) τ *den grössten gemeinsamen Teiler von m und n bedeutet.*

§ 3. **Neue Herleitung der Summe.**

Man kann die Formel (13) leicht unmittelbar, ohne Benutzung von (9), herleiten und ihre Uebereinstimmung mit der Formel (8) von Ramanujan zeigen. Es seien m_1 und m_2 zwei zu einander teilerfremde Zahlen. Wenn nun die Zahlen l_1 und l_2 unabhängig von einander die zu m_1 teilerfremden Zahlen $\leqslant m_1$ und die zu m_2 teilerfremden Zahlen $\leqslant m_2$ durchlaufen, so nimmt bekanntlich der Ausdruck

$$m_1 l_2 + m_2 l_1$$

jede Restklasse des Moduls $m_1 m_2$, die zu diesem teilerfremd ist, genau einmal an. Es ist deshalb

$$\begin{aligned} c_{m_1 m_2}(n) &= \sum_{l_1, l_2} e^{\frac{2\pi i (m_1 l_2 + m_2 l_1)}{m_1 m_2} n} \\ &= \left(\sum_{l_1} e^{\frac{2\pi i l_1}{m_1} n}\right) \left(\sum_{l_2} e^{\frac{2\pi i l_2}{m_2} n}\right) \\ &= c_{m_1}(n) \cdot c_{m_2}(n). \end{aligned} \tag{14}$$

Es handelt sich also nur darum, den Wert von $c_{p^\alpha}(n)$ zu bestimmen, wenn p eine Primzahl ist. Wenn l die nicht durch p teilbaren Zahlen $< p^\alpha$, aber ν innerhalb der jedesmal angegebenen Grenzen alle Zahlen durchläuft, so ist

$$c_{p^\alpha}(n) = \sum_{l} e^{\frac{2\pi i l}{p^\alpha} n} = \sum_{\nu=0}^{p^\alpha - 1} e^{\frac{2\pi i \nu}{p^\alpha} n} - \sum_{\nu=0}^{p^{\alpha-1}-1} e^{\frac{2\pi i p \nu}{p^\alpha} n}. \tag{15}$$

Falls n durch p^α teilbar, also p^α der grösste gemeinsame Teiler von p^α und n ist, sind alle Glieder der letzten beiden Summen gleich 1, und es wird somit

$$c_{p^\alpha}(n) = p^\alpha - p^{\alpha-1}. \tag{16}$$

Ist aber n durch $p^{\alpha-1}$ und nicht durch p^α teilbar, so ist von den beiden Summen die erste als Summe einer geometrischen Reihe gleich

$$\frac{1 - \left(e^{\frac{2\pi i n}{p^\alpha}}\right)^{p^\alpha}}{1 - e^{\frac{2\pi i n}{p^\alpha}}} = 0$$

und die andere besteht wieder aus lauter Gliedern 1 und ist deshalb gleich $p^{\alpha-1}$. Es ist also in diesem Fall

$$c_{p^\alpha}(n) = -p^{\alpha-1}. \tag{17}$$

Ist jedoch $\alpha \geqq 2$ und n nicht durch $p^{\alpha-1}$ teilbar, so sind in (15) die beiden Summen gleich Null, so dass also

$$c_{p^\alpha}(n) = 0 \tag{18}$$

ist.

Wird nun der grösste gemeinsame Teiler von p^α und n mit τ bezeichnet, so dass im ersten der drei genannten Fälle $\tau = p^\alpha$, im zweiten $\tau = p^{\alpha-1}$, im dritten τ gleich einer niedrigeren Potenz von p (bzw. gleich 1) ist, so stimmen die drei Ergebnisse (16), (17), (18) mit dem Ausdruck

$$\frac{\varphi(p^\alpha)}{\varphi\left(\frac{p^\alpha}{\tau}\right)} \mu\left(\frac{p^\alpha}{\tau}\right) \tag{19}$$

überein. *)

*) Für $\tau = p^\alpha$ kommt aus (19) augenscheinlich $\varphi(p^\alpha)$, für $\tau = p^{\alpha-1}$ kommt

$$\frac{\varphi(p^\alpha)}{\varphi(p)} \mu(p) = -p^{\alpha-1}$$

und für den Fall, dass p^α den Factor p mindestens zweimal häufiger enthält als n, kommt 0 heraus.

Hieraus ergibt sich nachher die allgemeine Formel (13) und die Uebereinstimmung mit dem von Ramanujan gefundenen Ausdruck (8) dadurch, dass die Funktionen $\varphi(n)$ und $\mu(n)$ „multiplikativ" sind, und auch die Begriffe gemeinsamer Teiler und „grösster gemeinsamer Teiler" sich in gewissem Sinne multiplikativ verhalten.

Ist nämlich die Zerlegung von m in Primzahlpotenzen

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

und bedeutet allgemein τ_i den grössten gemeinsamen Teiler von n mit $p_i^{\alpha_i}$, so ist der grösste gemeinsame Teiler von n und m

$$\tau = \tau_1 \tau_2 \ldots \tau_r \tag{20}$$

und es ist nach Gleichung (14)

$$c_m(n) = c_{p_1^{\alpha_1}}(n) c_{p_2^{\alpha_2}}(n) \ldots c_{p_r^{\alpha_r}}(n)$$

und somit nach (19)

$$c_m(n) = \frac{\varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \ldots \varphi(p_r^{\alpha_r})}{\varphi\left(\frac{p_1^{\alpha_1}}{\tau_1}\right) \varphi\left(\frac{p_2^{\alpha_2}}{\tau_2}\right) \ldots \varphi\left(\frac{p_r^{\alpha_r}}{\tau_r}\right)} \mu\left(\frac{p_1^{\alpha_1}}{\tau_1}\right) \mu\left(\frac{p_2^{\alpha_2}}{\tau_2}\right) \ldots \mu\left(\frac{p_r^{\alpha_r}}{\tau_r}\right). \tag{21}$$

Es ist also

$$c_m(n) = \frac{\varphi(m)}{\varphi\left(\frac{m}{\tau}\right)} \mu\left(\frac{m}{\tau}\right),$$

womit (13) unabhängig von dem früheren Ergebnis bewiesen ist.

Auf der anderen Seite verwandelt sich die Formel (8) von Ramanujan

$$\sum_{d|(m,n)} \mu\left(\frac{m}{d}\right) d$$

in das Summenprodukt

$$\left(\sum_{d_1|\tau_1} \mu\left(\frac{p_1^{\alpha_1}}{d_1}\right) d_1\right) \left(\sum_{d_2|\tau_2} \mu\left(\frac{p_2^{\alpha_2}}{d_2}\right) d_2\right) \ldots \left(\sum_{d_r|\tau_r} \mu\left(\frac{p_r^{\alpha_r}}{d_r}\right) d_r\right), \tag{22}$$

denn es durchläuft das Produkt

$$d = d_1 d_2 \ldots d_r$$

alle Teiler des Produkts (20) jeden einmal, wenn algemein d_i die Teiler von τ_i durchläuft und die Werte aller d_i beliebig kombiniert werden. Setzt man nun

$$\tau_i = p_i^{\beta_i} \qquad \beta_i \leqq \alpha_i\,,$$

so hat man bei der Erörterung der Summe

$$\sum_{d_i \mid \tau_i} \mu\left(\frac{p_i^{\alpha_i}}{d_i}\right) d_i \tag{23}$$

die drei Fälle zu bedenken: $\beta_i = \alpha_i$, $\beta_i = \alpha_i - 1$ und β_i um mehr als eine Einheit kleiner als α_i. Im ersten Fall sind nur zwei Glieder der Summe (23) von Null verschieden, für $d_i = p_i^{\alpha_i}$ und für $d_i = p_i^{\alpha_i - 1}$ und die Summe gibt

$$\mu\left(\frac{p_i^{\alpha_i}}{p_i^{\alpha_i}}\right) p_i^{\alpha_i} + \mu\left(\frac{p_i^{\alpha_i}}{p_i^{\alpha_i - 1}}\right) p_i^{\alpha_i - 1} = p_i^{\alpha_i} - p_i^{\alpha_i - 1}.$$

Im zweiten Fall liefert nur $d_i = p_i^{\alpha_i - 1}$ ein von Null verschiedenes Glied

$$\mu\left(\frac{p_i^{\alpha_i}}{p_i^{\alpha_i - 1}}\right) p_i^{\alpha_i - 1} = -p_i^{\alpha_i - 1}$$

und im dritten Fall verschwindet die Summe (23), da sie kein von Null verschiedenes Glied besitzt. Man kommt also auf die obigen drei Formeln (16), (17), (18) zurück, die in (19) zusammengefasst werden konnten.

Deshalb geht auch der Ausdruck (22) in (21) und somit auch in (13) über.

§ 4. Die Konvergenz einer Reihe.

Ramanujan hat für $m > 1$ die Formel

$$c_m(1) + \frac{1}{2} c_m(2) + \frac{1}{3} c_m(3) + \ldots = -\Lambda(m) \tag{24}$$

aufgestellt *), in der $c_m(n)$ die obige Bedeutung besitzt (Gleichung (7)), und $\Lambda(m)$ die zahlentheoretische Funktion ist, die den Wert 0 hat, falls m durch zwei verschiedene Primzahlen teilbar ist, und den Wert $\log p$ falls $m = p^k$. Diese Formel ist annähernd gleichbedeutend mit der Gleichung

$$\log K_m(1) = \Lambda(m), \tag{25}$$

*) a. a. O. p. 276 unten.

d. h. mit dem in § 1 angeführten Kroneckerschen Ergebnis, wonach

$$K_m(1) = \begin{cases} 1 \\ p \end{cases}$$

ist, je nachdem m keine Primzahlpotenz oder p^k ist.

Es ist nämlich für $|\rho| < 1$

$$\log\left(1 - \rho\, e^{\frac{2\pi i l}{m}}\right) = -\left(\rho\, e^{\frac{2\pi i l}{m}} + \frac{\rho^2}{2} e^{\frac{2\pi i l}{m}2} + \frac{\rho^2}{3} e^{\frac{2\pi i l}{m}3} + \ldots\right). \tag{26}$$

Summiert man hier über alle ganzen Zahlen l, die teilerfremd mit m und $\leqq m$ sind, so erhält man mit Rücksicht auf die Bedeutung von $c_m(n)$

$$\log \prod_{(l,m)=1}\left(1 - \rho\, e^{\frac{2\pi i l}{m}}\right) = -\left\{\rho\, c_m(1) + \frac{1}{2}\rho^2 c_m(2) + \frac{1}{3}\rho^3 c_m(3) + \ldots\right\}. \tag{27}$$

Da auf der linken Seite von (26) der Logarihtmus durch denjenigen Zweig der betreffenden Funktion des komplexen Arguments ρ zu deuten ist, der im Einheitskreis regulär ist und mit $\rho \to 0$ in Null übergeht, so ist auch in (27) für ein reelles ρ zwischen -1 und $+1$ der *reelle* Logarithmus des *positiven* Produkts

$$\prod_{(l,m)=1}\left(1 - \rho\, e^{\frac{2\pi i l}{m}}\right)$$

zu denken, der für $\rho \to 1$ in den reellen Logarithmus von $K_m(1)$ übergeht (Gleichung (1)). Der Abelsche Hilfssatz ergibt also die Gleichung

$$-\log K_m(1) = c_m(1) + \frac{1}{2} c_m(2) + \frac{1}{3} c_m(3) + \ldots,$$

vorausgesetzt, dass die letzte Reihe konvergiert.

Ramanujan hat die Gleichung (24) mit Hilfe der Zetafunktion bewiesen. Man erkennt aber jetzt, dass sie auch aus dem genannten Kroneckerschen Ergebnis, d. h. aus (25) gefolgert werden kann, falls man die Konvergenz der Reihe gesondert beweist. Dies geht aber leicht mit Hilfe der elementaren Analysis, nachdem man die vereinfachte Formel (13) für $c_m(n)$ hat.

Nimmt man nämlich die endliche Summe

$$\sum_{n \leqq x} \frac{1}{n} c_m(n)\,, \tag{28}$$

wo x eine positive Zahlgrösse bedeutet, so hat man nur immer die Glieder zusammenzufassen, deren Indizes n denselben grössten gemeinsamen Teiler τ mit m haben. Beim Addieren dieser Glieder erhält man mit Rücksicht auf (13)

$$\frac{\varphi(m)}{\varphi\left(\frac{m}{\tau}\right)}\,\mu\left(\frac{m}{\tau}\right)\frac{1}{\tau}\sum_{\tau n'\leq x}\frac{1}{n'}. \tag{29}$$

Man hat sich hier

$$m=\tau\,m'$$

$$n=\tau\,n'$$

und n' teilerfremd zu m' zu denken. Die letzte Summe aber, in der n' die zu $m'=\frac{m}{\tau}$ teilerfremden Zahlen $\leq\frac{x}{\tau}$ durchläuft, ist gleich *)

$$\sum_{d|\frac{m}{\tau}}\frac{\mu(d)}{d}\left(C+\log\frac{x}{\tau\,d}\right)+o(x), \tag{30}$$

wobei C die Eulersche Konstante bedeutet.

Jetzt hat man in (29) für τ alle Teiler von m zu setzen und zu summieren, um (28) zu erhalten. Man kann aber statt dessen auch

$$\frac{m}{\tau}=m',\qquad \tau=\frac{m}{m'}$$

setzen und über die Teiler m' von m summieren. Abgesehen von Gliedern, die einen bestimmt endlichen Wert haben, und von solchen, die mit unendlich werdendem x verschwinden, hat man dann nur noch einen mit $\log x$ multiplizierten Teil. Dieser wird mit Berücksichtigung von (30) gleich

$$\sum_{m'|m}\left\{\frac{\varphi(m)}{\varphi(m')}\,\mu(m')\,\frac{m'}{m}\sum_{d|m'}\frac{\mu(d)}{d}\right\}\log x\,.$$

Der Factor von $\log x$ kann aber auch in der Form

$$\frac{\varphi(m)}{m}\sum_{m'|m}\left\{\frac{\mu(m')}{\varphi(m')}\sum_{d|m'}\mu(d)\,\frac{m'}{d}\right\} \tag{31}$$

geschrieben werden. Die innere Summe ist hier $\varphi(m')$ und man erkennt, dass für $m>1$ der Ausdruck (31) gleich Null ist. Es strebt also in der Tat die Summe (28) bei unendlich wachsendem x einem endlichen und bestimmten Grenzwert zu.

*) Formel (30) wird am besten so bewiesen. Man betrachte die Summe

$$\sum_{d|m,\ d\nu\leq x}\frac{\mu(d)}{d\,\nu},$$

in der d die Teiler von m, und ν die ganzen Zahlen durchlaufen soll, die der Ungleichung $d\nu\leq x$ genügen. Nimmt man nun einmal die Glieder der Summe zusammen, in denen $d\nu=r$ denselben Zahlwert hat und ordnet ein anderes mal die Glieder zusammen, welche dasselbe d besitzen, so ergibt sich

$$\sum_{r'\leq x}\frac{1}{r'}=\sum_{d|m}\frac{\mu(d)}{d}\sum_{\nu=1}^{\frac{x}{d}}\frac{1}{\nu}=\sum_{d|m}\frac{\mu(d)}{d}\left(C+\log\frac{x}{d}\right)+o(x),$$

wobei in der linken Summe r' nur die zu m teilerfremden Zahlen durchläuft.