Eine alternative Produktdarstellung für die Kreisteilungspolynome

Autor(en): **Schramm, Wolfgang**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **70 (2015)**

Heft 4

PDF erstellt am: **10.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-630634

Elem. Math. 70 (2015) 137 – 143
0013-6018/15/040137-7
DOI 10.4171/EM/288

Elemente der Mathematik

Eine alternative Produktdarstellung für die Kreisteilungspolynome

Wolfgang Schramm

Der Verfasser ist Arzt und Universitätsdozent an der Medizinischen Universität Wien und beschäftigt sich in seiner Freizeit mit Freude mit Ideen und Problemen aus der elementaren Zahlentheorie.

1 Einleitung und Hauptergebnis

Das n-te Kreisteilungspolynom ist dasjenige ganzzahlige Polynom größten Grades mit Leitkoeffizient 1, das $x^n - 1$ teilt, jedoch zu allen $x^d - 1$ mit $d < n$ teilerfremd ist. Seine Nullstellen über $\mathbb{C}$ sind genau die primitiven n-ten Einheitswurzeln $e^{\frac{2\pi ik}{n}}$, wobei demnach k die zu n teilerfremden Zahlen zwischen 1 und n durchläuft. Die Zerlegung des n-ten Kreisteilungspolynoms in Linearfaktoren ist also das Produkt

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \mathrm{ggT}(k,n)=1}} (x - e^{\frac{2\pi ik}{n}}). \tag{1}$$

Da trivialerweise

$$\mathrm{ggT}(k, n) = \mathrm{ggT}(k \bmod n, n) \tag{2}$$

Für die Kreisteilungspolynome oder zyklotomischen Polynome Φ_n kennt man neben der Zerlegung in Linearfaktoren eine Reihe weiterer Darstellungen. Beispielsweise erhält man mit Hilfe der Möbius-Funktion die Formel $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(n/d)}$. Über die Koeffizienten der Φ_n ist einiges bekannt, so sind sie ganzzahlig und wenn n Produkt zweier Primzahlen ist, liegen die Koeffizienten in der Menge $\{-1, 0, 1\}$. Andererseits können sie beliebig gross werden, wie Schur bereits bemerkte. Eine besonders schöne Formel für Φ_n wird in der vorliegenden Arbeit präsentiert: Sie folgt aus der Betrachtung der diskreten Fourier-Transformation und zeigt auf einen Blick, dass die Koeffizienten reell sind. Als Nebenergebnis erscheint eine bekannte Summendarstellung der Eulerschen Phi-Funktion.

wie auch

$$e^{\frac{2\pi ik}{n}} = e^{\frac{2\pi i(k \bmod n)}{n}} \tag{3}$$

gilt, kann k auch ein beliebiges primes Restklassensystem durchlaufen. Es folgt daher aus (1) ebenso trivialerweise für den Grad des n-ten Kreisteilungspolynoms die Ordnung der primen Restgruppe, d. h.

$$\text{Grad } \Phi_n(x) = \sum_{\substack{1 \le k \le n \\ \text{ggT}(k,n)=1}} 1 = \varphi(n) \tag{4}$$

wobei $\varphi(n)$ die Eulersche Phi-Funktion ist. Ein Hauptresultat der vorliegenden Publikation ist das folgende

Theorem 1. $$\Phi_n(x) = \prod_{k=1}^{n} (x^{\text{ggT}(k,n)} - 1)^{\overline{e^{\frac{2\pi ik}{n}}}}.$$

Produktdarstellungen für Kreisteilungspolynome in dieser Form wurden (soweit jedenfalls dem Autor bekannt ist) bislang noch nicht publiziert. Das Produkt in Theorem 1 kann selbstverständlich aus demselben Grund wie zuvor auch über ein beliebiges, allerdings diesmal vollständiges Restsystem modulo n notiert werden.

Da für alle $x \in \mathbb{R}$ wegen $\text{ggT}(k, n) = \text{ggT}(-k, n) = \text{ggT}(n - k, n)$ in Gleichung (1) wie auch in Theorem 1 statt den n-ten Einheitswurzeln auch die dazu konjugiert komplexen $\overline{e^{\frac{2\pi ik}{n}}} = e^{\frac{2\pi i(-k)}{n}} = e^{\frac{2\pi i(n-k)}{n}}$ durchlaufen werden können und naturgemäß die Produktreihenfolge irrelevant ist, kann in Theorem 1 auf die komplexe Konjugation genauso gut verzichtet, bzw. Gleichung (1) auch komplex konjugiert werden, woraus folgt, dass alle $\Phi_n(x) \in \mathbb{R}[x]$ reelle Polynome sind. Die Koeffizienten von $\Phi_n(x)$ sind bekanntermaßen sogar ganzzahlig. Die Tatsache, dass die $\Phi_n(x)$ überdies irreduzibel über $\mathbb{Q}$ sind, ist nebenbei bemerkt ein Ergebnis, das für prime n auf C.F. Gauss [1] und allgemein auf Kronecker [2] zurückgeht.

Der Beweis von Theorem 1 ist mit einem Ergebnis aus [3], welches zuvor erläutert werden soll, erstaunlich einfach und kurz: Sei

$$c_n(m) := \sum_{\substack{k=1 \\ \text{ggT}(k,n)=1}}^{n} \overline{e^{\frac{2\pi imk}{n}}} = \sum_{k=1}^{n} \delta(\text{ggT}(k, n)) \cdot \overline{e^{\frac{2\pi imk}{n}}} \tag{5}$$

für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}$ die Ramanujan-Summe aus [4], wobei

$$\delta(n) := \begin{cases} 1 & \text{für } n = 1 \\ 0 & \text{sonst} \end{cases}$$

die Kronecker Deltafunktion ist. Mit nahezu analoger Argumentation wie zuvor folgt, dass

die $c_n(m)$ reell sein müssen:

$$\sum_{k=1}^{n} \delta(\mathrm{ggT}(k,n))\, \overline{e^{\frac{2\pi imk}{n}}} = \sum_{k=1}^{n} \delta(\mathrm{ggT}(k,n))\, e^{\frac{2\pi imn}{n}} e^{\frac{-2\pi imk}{n}}$$

$$= \sum_{k=1}^{n} \delta(\mathrm{ggT}(n-k,n)) e^{\frac{2\pi im(n-k)}{n}} = \sum_{k=1}^{n} \delta(\mathrm{ggT}(k,n)) e^{\frac{2\pi imk}{n}}$$

weshalb (5) auch komplex konjugiert werden durfte. Sei weiter mit $*$ die Dirichlet-Faltung

$$(h * g)(n) := \sum_{d|n} h(n/d) g(d) \tag{6}$$

zweier beliebiger zahlentheoretischer Funktionen $h, g : \mathbb{N} \to \mathbb{C}$ notiert. Für eine beliebige zahlentheoretische Funktion $f : \mathbb{N} \to \mathbb{C}$ wurde in [3] gezeigt, dass wiederum für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}$

$$\sum_{k=1}^{n} f(\mathrm{ggT}(k,n)) \cdot \overline{e^{\frac{2\pi imk}{n}}} = \sum_{d|n} f(n/d) c_d(m) = (f * c_\bullet(m))(n) \tag{7}$$

gilt. Mit $\bullet$ wurde die Faltungssummationsvariable, d.h. alle positiven (echten und unechten) Teiler d von n bzw. Koteiler n/d (was in der Summe letztlich auf dasselbe hinausläuft) angedeutet.

Bereits Ramanujan hat mit den nach ihm benannten Summen interessante Darstellungen für zahlentheoretische Funktionen gefunden und Nicol [5] hat sogar gezeigt, dass die Kreisteilungspolynome $\Phi_n(x)$ mittels der Ramanujan-Summen $c_n(m)$ darstellbar sind, eine sicherlich interessante Tatsache, die aber im Folgenden nicht benötigt wird.

Zunächst soll also Gleichung (7) erläutert und auch kurz motiviert werden. Die Ramanujan-Summe (5) erinnert zweifelsohne an die diskrete Fourier-Transformation (DFT) $\hat{a} = (\hat{a}_1, \ldots, \hat{a}_n) \in \mathbb{C}^n$ eines komplexen Vektors $a = (a_1, \ldots, a_n) \in \mathbb{C}^n$ mit den Fourierkoeffizienten $\hat{a}_m = \sum_{k=1}^{n} a_k \cdot \overline{e^{\frac{2\pi imk}{n}}}$ für $1 \le m \le n$. Die Koeffizienten der inversen DFT $a_k = \frac{1}{n} \sum_{m=1}^{n} \hat{a}_m \cdot e^{\frac{2\pi imk}{n}}$ von $\hat{a}$ sind bekanntlich genauso wie die Fourierkoeffizienten $\hat{a}_m$ selbst wegen (3) periodisch mit der Periode n. Auch die Koeffizienten $\delta(\mathrm{ggT}(k,n))$ in (5) haben wegen (2) dieselbe Perioden-Eigenschaft und selbstverständlich auch auf dem Wertebereich des $\mathrm{ggT}(k,n)$ definierte Funktionen des größten gemeinsamen Teilers wie etwa die Koeffizienten in (7). Es bieten sich dafür zahlentheoretische Funktionen $f : \mathbb{N} \to \mathbb{C}$ geradewegs an, wenn nicht gerade beide Argumente des ggT den Wert 0 annehmen, was aber in (7) ausgeschlossen werden kann, da n eine natürliche Zahl ist. Demnach kann (7) in gewissem Sinn als eine Verallgemeinerung der Ramanujan-Summen (5) betrachtet werden, indem in (5) die Kronecker Deltafunktion $\delta(n)$ durch eine beliebige zahlentheoretische Funktion $f(n)$ ersetzt wird. Der Beweis von (7) ist übrigens ebenso einfach und könnte sogar in drei Zeilen geführt werden [3, short proof], wenngleich der auch nur etwas mehr als eine halbe Seite umfassende "Standard"-Beweis in [3] vielleicht etwas einsichtiger ist.

Beweis von Theorem 1. Sei $\Phi_d(x)$ das d-te Kreisteilungspolynom (1), dann gilt bekanntlich

$$(x^n - 1) = \prod_{d|n} \Phi_d(x)$$

da $(x^n - 1) = \prod_{1\le k\le n} (x - e^{\frac{2\pi ik}{n}}) = \prod_{d|n} \prod_{\substack{1\le k\le n \\ \mathrm{ggT}(k,n)=d}} (x - e^{\frac{2\pi ik}{n}}) = \prod_{d|n} \Phi_{n/d}(x) = \prod_{d|n} \Phi_d(x)$

mit (1) ist.

Daraus folgt für ein beliebiges $1 \neq x \in \mathbb{C}$ durch Logarithmieren beider Seiten

$$\ln(x^n - 1) = \ln \prod_{d|n} \Phi_d(x)) = \sum_{d|n} \ln\Phi_d(x) = (I * \ln \Phi_\bullet(x))(n) \tag{8}$$

wobei auf der rechten Seite in der Dirichlet-Faltungsnotation (6) für $h(n)$ die für alle natürlichen Zahlen konstante zahlentheoretische Funktion $I(n) := 1$ und für $g(n) = \ln \Phi_n(x)$ gewählt wurde, sowie wiederum mit $\bullet$ die Summationsvariable angedeutet ist.

Für eine beliebige zahlentheoretische Funktion $g(n)$ gilt bekanntermaßen

$$f(n) = (I * g)(n) \Leftrightarrow g(n) = (\mu * f)(n) \tag{9}$$

worin $\mu(n)$ die Möbius-Funktion mit der Definitionsgleichung $(I * \mu)(n) = \delta(n)$ als Dirichlet-Inverser der Funktion $I(n)$ ist, womit letztlich (9) auch bewiesen wird. Die Richtung $\Rightarrow$ in (9) wird auch häufig als Möbius-Inversion bezeichnet.

Diese Möbius-Inversion auf (8), d. h. speziell für $g(n) = \ln \Phi_n(x)$ und $f(n) = \ln(x^n - 1)$ angewendet ergibt sodann:

$$\ln \Phi_n(x) = (\mu * \ln(x^\bullet - 1))(n) \tag{10}$$

wobei abermals mit $\bullet$ die Summationsvariable angedeutet wurde.

Wird nun in der eingangs angesprochenen Fourier-Transformationsidentität von Funktionen des größten gemeinsamen Teilers (7) speziell für $m = 1$ gewählt, dann folgt zunächst einmal aus (7) wegen der seit langem bekannten und bemerkenswerten Beziehung der Ramanujan-Summen zu der Möbius-Funktion $c_n(1) = \mu(n)$, welche überdies ebenso in wenigen Zeilen aus (7) [3; Eq. (5)] abgeleitet werden kann, die Gleichung

$$\sum_{k=1}^{n} f(\mathrm{ggT}(k, n)) \cdot \overline{e^{\frac{2\pi ik}{n}}} = \sum_{d|n} f(n/d)\mu(d) = (f * \mu)(n). \tag{11}$$

Sei nun darin speziell wieder $f(n) = \ln(x^n - 1)$ für ein beliebiges $x \in \mathbb{C}$ mit $x \neq 1$ gewählt, also

$$\sum_{k=1}^{n} \ln(x^{\mathrm{ggT}(k,n)} - 1) \cdot \overline{e^{\frac{2\pi ik}{n}}} = (\ln(x^\bullet - 1) * \mu)(n),$$

dann steht hier rechterhand (da die Dirichlet-Faltung kommutativ ist) die rechte Seite der Gleichung (10). Es folgt also

$$\sum_{k=1}^{n} \ln(x^{\mathrm{ggT}(k,n)} - 1) \cdot \overline{e^{\frac{2\pi ik}{n}}} = \ln \Phi_n(x).$$

Triviale Umformungen ergeben weiter:

$$\sum_{k=1}^{n} \ln(x^{\mathrm{ggT}(k,n)} - 1)^{\overline{e^{\frac{2\pi ik}{n}}}} = \ln \Phi_n(x)$$

$$\Leftrightarrow \ln \prod_{k=1}^{n} (x^{\mathrm{ggT}(k,n)} - 1)^{\overline{e^{\frac{2\pi ik}{n}}}} = \ln \Phi_n(x)$$

$$\Leftrightarrow \prod_{k=1}^{n} (x^{\mathrm{ggT}(k,n)} - 1)^{\overline{e^{\frac{2\pi ik}{n}}}} = \Phi_n(x). \tag{12}$$

Damit ist Theorem 1 bewiesen. □

Die Richtung $\Rightarrow$ im letzten Schritt (12) ist nebenbei bemerkt wegen der strengen Monotonie und damit Injektivität des Logarithmus im Reellen mit Sicherheit richtig und im komplexen (z. B. aus Stetigkeitsgründen) demnach auch. In der Einleitung wurde aber bereits gezeigt, daß das Argument des Logarithmus auf der linken Seite von (12) ein reelles Polynom ist, was auch unmittelbar zu sehen ist: Da zu jedem Faktor $(x^{\mathrm{ggT}(k,n)} - 1)^{e^{\frac{2\pi ik}{n}}}$ in Theorem 1 mit nicht verschwindendem Imaginärteil im Exponenten wegen $\mathrm{ggT}(k,n) = \mathrm{ggT}(-k,n) = \mathrm{ggT}(n-k,n)$ auch der dazu komplex konjugierte Faktor $(x^{\mathrm{ggT}(n-k,n)} - 1)^{e^{\frac{2\pi i\cdot(n-k)}{n}}} = (x^{\mathrm{ggT}(k,n)} - 1)^{\overline{e^{\frac{2\pi ik}{n}}}}$ vorkommt, folgt, dass sich in Theorem 1 die Imaginärteile $(x^{\mathrm{ggT}(k,n)} - 1)^{\cos(\frac{2\pi k}{n})+i\cdot\sin(\frac{2\pi k}{n})}(x^{\mathrm{ggT}(k,n)} - 1)^{\cos(\frac{2\pi k}{n})-i\cdot\sin(\frac{2\pi k}{n})} = (x^{\mathrm{ggT}(k,n)} - 1)^{2\cos(\frac{2\pi k}{n})}$ wechselseitig wegkürzen und demnach nur noch die Realteile übrig bleiben. Mit anderen Worten, nur der Realteil der Exponenten in Theorem 1 trägt zum Produkt bei. Daraus folgt das

Korollar 1.
$$\Phi_n(x) = \prod_{k=1}^{n} (x^{\mathrm{ggT}(k,n)} - 1)^{\cos(\frac{2\pi k}{n})}.$$

In dieser Darstellung ist schließlich auf den ersten Blick ersichtlich, dass die Kreisteilungspolynome reelle Koeffizienten haben müssen. Anzumerken ist aber auch, dass man in Korollar 1 unter Umständen (etwa für n prim) sehr viel mehr Faktoren zu betrachten hat, da über alle $1 \leq k \leq n$ das Produkt zu nehmen ist, in der Produktdarstellung (1) aber nur über jene k mit $\mathrm{ggT}(k,n) = 1$.

2 Beispiele

Die folgenden Beispiele sollen nun Theorem 1 bzw. Korollar 1 illustrieren:

$$\Phi_1(x) = \prod_{k=1}^{1} (x^{\mathrm{ggT}(k,1)} - 1)^{\overline{e^{\frac{2\pi ik}{1}}}} = x - 1$$

$$\Phi_2(x) = \prod_{k=1}^{2} (x^{\mathrm{ggT}(k,2)} - 1)^{\overline{e^{\frac{2\pi ik}{2}}}} = (x-1)^{-1}(x^2 - 1) = x + 1$$

$$\Phi_3(x) = \prod_{k=1}^{3} (x^{\mathrm{ggT}(k,3)} - 1)^{\overline{e^{\frac{2\pi ik}{3}}}} = (x-1)^{-\frac{1}{2}+i\frac{\sqrt{3}}{2}}(x-1)^{-\frac{1}{2}-i\frac{\sqrt{3}}{2}}(x^3-1)$$
$$= (x-1)^{-\frac{1}{2}}(x-1)^{-\frac{1}{2}}(x^3-1) = x^2+x+1$$
$$\Phi_4(x) = \prod_{k=1}^{4} (x^{\mathrm{ggT}(k,4)} - 1)^{\overline{e^{\frac{2\pi ik}{4}}}} = (x-1)^{i}(x^2-1)^{-1}(x-1)^{-i}(x^4-1)$$
$$= \frac{(x^4-1)}{(x^2-1)} = \frac{(x^2+1)(x^2-1)}{(x^2-1)} = x^2+1.$$

Die 5. Einheitswurzeln sind: $\frac{1}{4}\left(-1+\sqrt{5}+i\sqrt{2}\sqrt{5+\sqrt{5}}\right)$, $\frac{1}{4}\left(-1-\sqrt{5}+i\sqrt{2}\sqrt{5-\sqrt{5}}\right)$, $\frac{1}{4}\left(-1-\sqrt{5}-i\sqrt{2}\sqrt{5-\sqrt{5}}\right)$, $\frac{1}{4}\left(-1+\sqrt{5}-i\sqrt{2}\sqrt{5+\sqrt{5}}\right)$ und 1. Es gilt daher sogleich mit Korollar 1:

$$\Phi_5(x) = \prod_{k=1}^{5} (x^{\mathrm{ggT}(k,5)} - 1)^{\cos(\frac{2\pi k}{5})}$$
$$= (x-1)^{\frac{-1+\sqrt{5}}{4}}(x-1)^{\frac{-1-\sqrt{5}}{4}}(x-1)^{\frac{-1-\sqrt{5}}{4}}(x-1)^{\frac{-1+\sqrt{5}}{4}}(x^5-1)$$
$$= \frac{(x^5-1)}{(x-1)} = x^4+x^3+x^2+x^1+1.$$

3 Als Nebenergebnis, ein alternativer Beweis für eine bekannte Gleichung der Eulerschen Phi-Funktion

Der Grad der Kreisteilungspolynome in Korollar 1 muss natürlich wiederum die Eulersche Phi-Funktion (4) ergeben: Aus der binomischen Reihe $(x+y)^b = \sum_{k=0}^{\infty} \binom{b}{k} x^{b-k}y^k$ bzw. speziell aus $(x^a-1)^b = \sum_{k=0}^{\infty} \binom{b}{k} x^{a(b-k)}(-1)^k$ zusammen mit $\binom{b}{0} = 1$ folgt jedenfalls für alle reellen b, $x > 1$ und $a \geq 1$:

$$(x^a-1)^b = x^{ab} + O(x^{a(b-1)}), \tag{13}$$

worin $O(x^{a(b-1)})$ das Groß O Landau-Symbol für $x^{a(b-1)}$ bezeichnet. Wird nun für $a = \mathrm{ggT}(k,n)$ und $b = \cos(\frac{2\pi k}{n})$ gewählt und jeder Faktor in Korollar 1 durch die rechte Seite von (13) ersetzt, dann folgt mit der bekannten Identität [3; Beispiel 3] zur Eulerschen Phi-Funktion

$$\varphi(n) = \sum_{k=1}^{n} \mathrm{ggT}(k,n)\cos\left(\frac{2\pi k}{n}\right) \tag{14}$$

für den Grad des n-ten Kreisteilungspolynoms $\Phi_n(x)$ erwartungsgemäß wiederum (4) bzw. umgekehrt ein weiterer Beweis für (14).

Literatur

[1] Gauss Carl F.: Disquisitiones Arithmeticae, Leipzig 1801, in Untersuchungen über höhere Arithmetik (trans. H. Maser), American Mathematical Society/Chelsea, Providence 2006

[2] Kronecker Leopold: Mémoire sur les facteures irreductibles de l'expression $x^n - 1$, J. Math. Pures Appl. 19 (1854), 177–192.

[3] Schramm Wolfgang: The Fourier transform of functions of the greatest common divisor, Integers 8 (2008), #A50.

[4] Ramanujan Srinivasa: On Certain Arithmetical Functions. Transactions of the Cambridge Philosophical Society 22, Nr. 9 (1916) 159–184.

[5] Nicol Charles A.: Some formulas involving Ramanujan sums, Canad. J. Math. 14 (1962), 284–286.

Wolfgang Schramm
Schulgasse 62/11
A-1180 Wien Österreich
e-mail: wolfgang.schramm@meduniwien.ac.at