By the lemma there exists a rational integer x such that $G_0(x, y)$ has a prime factor $q \equiv l \bmod m$ not dividing py. The contradiction obtained completes the proof.

Reference

[1] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berl. Math. Ges. 11, pp. 40-50.

Reçu par la Rédaction le 24. 8. 1965

ACTA ARITHMETICA
XI (1966)

Polynome, welche für gegebene Zahlen Permutationspolynome sind

von

W. Nöbauer (Wien)

Herrn Professor Hlawka zum 50. Geburtstag gewidmet

Man bezeichnet das ganzzahlige Polynom $g(x)$ als Permutationspolynom mod n (n natürliche Zahl), wenn die Abbildung $i \to g(i) \bmod n$, $i = 1, 2, \ldots, n$, eine Permutation der Restklassen mod n ist. Es sei $\mathfrak{M}(g(x))$ die Menge aller natürlichen Zahlen $n > 1$, für welche $g(x)$ Permutationspolynom ist. In dieser Note werden einige Aussagen hergeleitet, die sich auf $\mathfrak{M}(g(x))$ beziehen.

Es gilt, wie etwa in [5] gezeigt wurde: Ist $n = ab$ und $(a, b) = 1$, so ist $g(x)$ dann und nur dann Permutationspolynom mod n, wenn es Permutationspolynom mod a und Permutationspolynom mod b ist. Für die vollständige Kenntnis von $\mathfrak{M}(g(x))$ genügt daher die Kenntnis aller in $\mathfrak{M}(g(x))$ enthaltenen Primzahlpotenzen. Ebenfalls wurde etwa in [5] gezeigt: Ist $n = p^e$ eine Primzahlpotenz mit $e > 1$, so ist $g(x)$ dann und nur dann Permutationspolynom mod n, wenn es Permutationspolynom mod p ist und wenn $g'(\xi) \not\equiv 0 \bmod p$ für jedes ganze ξ. Daraus folgt sogleich: Die Menge der in $\mathfrak{M}(g(x))$ enthaltenen Potenzen einer Primzahl p ist entweder leer, oder sie besteht aus p allein, oder sie besteht aus allen Potenzen von p. Bezeichnen wir also mit $\mathfrak{P}(g(x))$ die Menge aller in $\mathfrak{M}(g(x))$ enthaltenen Primzahlen und mit $\mathfrak{G}(g(x))$ die Menge aller jener Primzahlen, deren sämtliche Potenzen in $\mathfrak{M}(g(x))$ enthalten sind, so ist durch Angabe von $\mathfrak{P}(g(x))$ und von $\mathfrak{G}(g(x))$ das $\mathfrak{M}(g(x))$ vollständig bestimmt.

Wie sofort zu sehen, ist $f(g(x))$ dann und nur dann ein Permutationspolynom mod n, wenn $f(x)$ und $g(x)$ Permutationspolynome mod n sind. Es gelten daher die Beziehungen

$$\mathfrak{A}\big(f(g(x))\big) = \mathfrak{A}\big(f(x)\big) \cap \mathfrak{A}\big(g(x)\big) \quad \text{für} \quad \mathfrak{A} = \mathfrak{M}, \mathfrak{P}, \mathfrak{G} \tag{1}$$

Selbstverständlich gilt $\mathfrak{G}(g(x)) \subseteq \mathfrak{P}(g(x))$.

Es ist bekannt, daß für ein Polynom $g(x)$ vom Grad $r>1$ stets gilt $p \notin \mathfrak{P}(g(x))$ für alle Primzahlen $p \equiv 1 \bmod r$ (vgl. etwa Carlitz [1]). Daraus folgt auf Grund des Satzes von Dirichlet sofort, daß $\mathfrak{P}(g(x))$ und damit auch $\mathfrak{G}(g(x))$ genau für die linearen Polynome $ax+b$ aus fast allen Primzahlen besteht, und daß $\mathfrak{N}(g(x))$ genau für die linearen Polynome der Gestalt $\pm x+b$ aus fast allen natürlichen Zahlen besteht.

In der Literatur wurde schon mehrfach die Frage untersucht, für welche $g(x)$ das $\mathfrak{P}(g(x))$ eine unendliche Menge ist (vgl. Dickson [3], Schur [7], Wegner [8], Kurbatov [4]). Die bisherigen Ergebnisse zu diesem Problem lassen sich folgendermaßen formulieren: Es sei $\mathfrak{R}$ die Halbgruppe der rationalzahligen Polynome mit der Polynomkomposition als Verknüpfung und $\mathfrak{T}$ die darin von den (nichtkonstanten) linearen Polynomen $ax+\beta$, den Potenzen x^k mit $(k, 2)=1$ und den Polynomen

$$d_k(x) = \sum_{\nu=0}^{\frac{k-1}{2}} \frac{k}{k-\nu}\binom{k-\nu}{\nu} a^\nu x^{k-2\nu}$$

mit ganzem $a \neq 0$ und $(k, 6)=1$ erzeugte Teilhalbgruppe, $\mathfrak{L}$ die Menge der ganzzahligen Polynome von $\mathfrak{T}$. Alle Polynome von $\mathfrak{L}$ haben unendliches $\mathfrak{P}(g(x))$, und für die Zahlen l der Gestalt $p_1^u, p_1^u p_2^v, p_1p_2p_3, p_1p_2p_3p_4$ (wobei p_1, p_2, p_3, p_4 voneinander verschiedene ungerade Primzahlen sind) weiß man, daß es außer den Polynomen von $\mathfrak{L}$ keine weiteren $g(x)$ vom Grad l mit unendlichem $\mathfrak{P}(g(x))$ gibt; auch für gerade Zahlen l trifft dies zu (es folgt nämlich aus den Ergebnissen von Davenport und Lewis [2], pp. 59-60 sofort(1), daß es keine $g(x)$ von geradem Grad mit unendlichem $\mathfrak{P}(g(x))$ geben kann). Es ist jedoch nicht bekannt, ob es auch bei anderen Graden l der Fall ist.

Die analoge Frage nach den $g(x)$ mit unendlichem $\mathfrak{G}(g(x))$ ist ebenfalls nicht gelöst (vgl. [5]). Ist $\mathfrak{T}_1$ die in $\mathfrak{R}$ von den $ax+\beta$ und den $d_k(x)$ von oben erzeugte Teilhalbgruppe und $\mathfrak{L}_1$ die Menge der ganzzahligen Polynome von $\mathfrak{T}_1$, so haben alle Polynome von $\mathfrak{L}_1$ unendliches $\mathfrak{G}(g(x))$, und für die oben angegebenen Grade l gibt es außer den Polynomen von $\mathfrak{L}_1$ keine weiteren $g(x)$ mit unendlichem $\mathfrak{G}(g(x))$.

Wir wollen nun zeigen, daß es stets ganzzahlige Polynome mit willkürlich vorgegebenem endlichen $\mathfrak{P}$ und $\mathfrak{G}$ gibt (wobei natürlich $\mathfrak{G} \subseteq \mathfrak{P}$ erfüllt sein muß), es gilt nämlich folgender

Satz 1. *Sind $\mathfrak{R}=\{p_1, p_2, \ldots, p_r\}$, $\mathfrak{G}=\{q_1, q_2, \ldots, q_s\}$ zwei zueinander fremde, endliche Mengen von Primzahlen (welche auch leer sein können), so gibt es stets ganzzahlige normierte Polynome $g(x)$ von unendlich vielen verschiedenen Graden, so daß*

$$\mathfrak{P}(g(x)) = \mathfrak{R} \cup \mathfrak{G} \quad \text{und} \quad \mathfrak{G}(g(x)) = \mathfrak{G}.$$

(1) Auf diese Tatsache hat mich der Referee hingewiesen.

Beweis. Ist $\mathfrak{R} \cup \mathfrak{G}$ leer, dann haben ersichtlich alle Polynome $g(x)=x^{2\nu}-x^{2\nu-2}$ $(\nu \geqslant 2)$ die gewünschten Eigenschaften. Ist aber $\mathfrak{R} \cup \mathfrak{G}$ nicht leer, dann setzen wir $P=\prod_{i=1}^{r} p_i$ wenn $\mathfrak{R}$ nicht leer, $P=1$ wenn $\mathfrak{R}$ leer, $Q=\prod_{i=1}^{s} q_i$ wenn $\mathfrak{G}$ nicht leer, $Q=1$ wenn $\mathfrak{G}$ leer (2). Nun wählen wir natürliche Zahlen u, v mit $u>v$ so, daß gilt $x^u \equiv x^v \bmod PQ$ für alle ganzen Zahlen x (daß dies möglich ist, ist leicht einzusehen, siehe etwa auch Sierpiński [6], S. 132). Sodann wähle man eine natürliche Zahl $k \geqslant 2$ so, daß $w=uPQk+1$ eine Primzahl ist (nach dem Satz von Dirichlet gibt es unendlich viele derartige k) und bilde das Polynom $a(x)=x^{uPQk+1}-x^{vPQk+1}$; dann gilt ersichtlich $a(x) \equiv 0 \bmod PQ$ und $a^l(x) \equiv 0 \bmod PQ$ für jedes ganze x. Weiter bilde man das Polynom

$$b(x) = a(x) + \sum_{\mu=1}^{r} \frac{PQ}{p_\mu} x^{p_\mu} + \sum_{\nu=1}^{s} \frac{PQ}{q_\nu} x$$

welches den Grad w hat und normiert ist. Dieses $b(x)$ erzeugt mod q_i dieselbe Abbildung wie $\frac{PQ}{q_i}x$, ist also Permutationspolynom mod q_i, weiter gilt $b^l(x) \equiv \frac{PQ}{q_i} \bmod q_i$ für jedes ganze x, also ist $b^l(x) \not\equiv 0 \bmod q_i$ für jedes ganze x; nach dem eingangs erwähnten Satz gilt also $q_i \in \mathfrak{G}(b(x))$. Das $b(x)$ erzeugt mod p_i die selbe Abbildung wie $\frac{PQ}{p_i}x^{p_i}$, da nun aber $x^{p_i} \equiv x \bmod p_i$ für jedes ganze x, ist $b(x)$ Permutationspolynom mod p_i; es gilt $b^l(x) \equiv 0 \bmod p_i$ für jedes ganze x, daher haben wir $p_i \in \mathfrak{P}(b(x))$, aber $p_i \notin \mathfrak{G}(b(x))$. Da w eine ungerade Primzahl ist, gehören nach einem früher erwähnten Satz alle Polynome $g(x)$ vom Grad w mit unendlichem $\mathfrak{P}(g(x))$ zu $\mathfrak{L}$, sind also entweder von der Gestalt $a(\alpha_1 x+\beta_1)^w+\beta$ oder von der Gestalt $ad_w(\alpha_1 x+\beta_1)+\beta$; von diesen Polynomen enthalten die mit $\beta_1 \neq 0$ ein nichtverschwindendes Glied mit x^{w-1}, die mit $\beta_1=0$ entweder außer dem Anfangsglied nur ein konstantes Glied oder ein nichtverschwindendes Glied mit x^{w-2}. Wegen

$$(uPQk+1)-(vPQk+1) = (u-v)PQk \geqslant 4$$

und

$$vPQk+1 > \max(p_1, p_2, \ldots, p_r, 1)$$

ist $b(x)$ nicht von einer dieser Gestalten, daher ist $\mathfrak{P}(b(x))$ endlich, somit

(2) Auch im folgenden soll ein leeres Produkt stets den Wert 1 haben.

haben wir $\mathfrak{P}(b(x)) = \mathfrak{R} \cup \mathfrak{G} \cup \mathfrak{T}$, wo $\mathfrak{T} = \{\pi_1, \pi_2, \ldots, \pi_t\}$ eine zu $\mathfrak{R} \cup \mathfrak{G}$ fremde, endliche Menge von Primzahlen ist. Wir setzen $T = \prod_{i=1}^{t} \pi_i$, wählen ein z, für welches $z \equiv 1 \bmod PQ$, $z \equiv 0 \bmod T$, und natürliche Zahlen l, m mit $l > m$ und $x^l \equiv x^m \bmod PQT$ für jedes ganze x. Nun bilden wir das normierte ganzzahlige Polynom $c(x) = x^{lPQ} - x^{mPQ} + zx$; für dieses gilt ersichtlich

$$\mathfrak{P}(c(x)) \supset \mathfrak{R} \cup \mathfrak{G}, \qquad \mathfrak{G}(c(x)) \supset \mathfrak{R} \cup \mathfrak{G} \qquad \text{sowie} \qquad \mathfrak{P}(c(x)) \cap \mathfrak{T} = \emptyset.$$

Wegen (1) haben wir daher für das normierte ganzzahlige Polynom $g(x) = b(c(x))$ die Beziehungen $\mathfrak{P}(g(x)) = \mathfrak{R} \cup \mathfrak{G}$, $\mathfrak{G}(g(x)) = \mathfrak{G}$, und da für die Wahl von k in $a(x)$ unendlich viele Möglichkeiten bestehen, gibt es auch für den Grad von $g(x)$ unendlich viele Möglichkeiten.

Sei π eine Permutation der Ziffern $1, 2, \ldots, n$. Wir sagen, π läßt sich polynomial darstellen, wenn es ein ganzzahliges Polynom $g(x)$ gibt, so daß gilt $\pi i \equiv g(i) \bmod n$ für $i = 1, 2, \ldots, n$. Wir wollen nun zeigen, daß sich jede überhaupt polynomial darstellbare Permutation auch darstellen läßt durch ein Polynom $g(x)$ mit kleinstmöglichem $\mathfrak{M}(g(x))$, und zwar beweisen wir folgenden

Satz 2. *Sei $n > 1$ und π eine Permutation der Ziffern $1, 2, \ldots, n$, welche sich polynomial darstellen läßt; es sei*

$$n = p_1 p_2 \ldots p_r q_1^{e_1} q_2^{e_2} \ldots q_s^{e_s} \qquad (\text{alle } e_i > 1)$$

die Primzahlzerlegung von n. Dann läßt sich π stets darstellen durch ein normiertes Polynom $g(x)$ mit

$$\mathfrak{P}(g(x)) = \{p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s\}$$

und

$$\mathfrak{G}(g(x)) = \{q_1, q_2, \ldots, q_s\}.$$

Beweis. Wir setzen $\{p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s\} = \mathfrak{P}$ und $\{q_1, q_2, \ldots, q_s\} = \mathfrak{G}$. Es sei $h(x)$ ein beliebiges ganzzahliges Polynom, welches π darstellt. Nun bestimmen wir für $\mu = 1, 2, \ldots, r$ Zahlen a_μ so, daß gilt (wenn $\delta_{\mu\nu}$ das Kroneckersymbol bedeutet)

$$a_\mu \equiv \delta_{\mu\nu} \bmod p_\nu \qquad \text{für} \qquad \nu = 1, 2, \ldots, r, \qquad a_\mu \equiv 0 \bmod \prod_{i=1}^{s} q_i^{e_i}$$

und bilden das Polynom

$$j(x) = h(x) + h'(0) \sum_{\mu=1}^{r} a_\mu (x^{p_\mu} - x). \tag{2}$$

Es gilt dann $j(x) \equiv h(x) \bmod n$ für jedes ganze x, also stellt auch $j(x)$ das π dar; weiter gilt $j'(x) \equiv h'(x) - h'(0) \bmod p_\nu$ für jedes ganze x,

und somit $j'(0) \equiv 0 \bmod p_\nu$, nach einem der eingangs erwähnten Sätze also $p_\nu \notin \mathfrak{G}(j(x))$. Ist b der Grad von $j(x)$, so wählen wir natürliche Zahlen u, v mit $u > v$ so, daß $x^u \equiv x^v \bmod n$ für alle ganzen x, und eine natürliche Zahl $k \geqslant 2$ so, daß $unk+1$ Primzahl und daß $vnk+1 > b$. Wir bilden $a(x) = x^{unk+1} - x^{vnk+1}$ und damit $f(x) = a(x) + j(x)$. Dieses $f(x)$ stellt ebenfalls das π dar und es gilt $f'(x) \equiv j'(x) \bmod n$ für jedes ganze x, also $p_\nu \notin \mathfrak{G}(f(x))$. Wie beim Beweis von Satz 1 sieht man, daß $\mathfrak{P}(f(x))$ endlich ist; sei $\mathfrak{T} = \mathfrak{P}(f(x)) - \mathfrak{P} = \{\pi_1, \pi_2, \ldots, \pi_t\}$. Wie im vorhergehenden Beweis setzen wir $T = \prod_i \pi_i$, wählen z mit $z \equiv 1 \bmod n$, $z \equiv 0 \bmod T$ und natürliche Zahlen l, m mit $l > m$ und $x^l \equiv x^m \bmod nT$ für jedes ganze x; hierauf setzen wir $c(x) = x^{ln} - x^{mn} + zx$ und bilden $f(c(x))$. Wegen $c(x) \equiv x \bmod n$ für jedes ganze x stellt das normierte Polynom $g(x) = f(c(x))$ das π dar; wegen (1) haben wir $\mathfrak{P}(g(x)) = \mathfrak{P}$ und $\mathfrak{G}(g(x)) = \mathfrak{G}$.

Durch Modifikation des beim Beweis von Satz 2 verwendeten Gedankenganges läßt sich zeigen der folgende

Satz 2a. *Unter den Voraussetzungen von Satz 2 läßt sich π stets darstellen durch ein Polynom $g(x)$ mit*

$$\mathfrak{P}(g(x)) = \{p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s\}$$

und

$$\mathfrak{G}(g(x)) = \{q_1, q_2, \ldots, q_s\},$$

dessen Grad gleich ist einer beliebigen Primzahl $w \geqslant n+3$.

Beweis. Auf Grund der für alle ganzen x bestehenden Beziehung $x^n \equiv x^{n-\varphi(n)} \bmod n$ (vgl. etwa [6], S. 132) können wir das im Beweis von Satz 2 als Ausgangspunkt verwendete $h(x)$ als Polynom vom Grad $\leqslant n-1$ annehmen, das nach (2) gebildete $j(x)$ hat dann jedenfalls einen Grad $\leqslant n$. Ist nun $w \geqslant n+3$ eine gegebene Primzahl, so ersetzen wir das $a(x)$ im vorhergehenden Beweis durch nx^w und bilden damit $f(x)$; auch jetzt ist $\mathfrak{P}(f(x))$ endlich. Mit dem so wie oben erklärten z bilden wir $g(x) = f(zx)$, dieses ist vom Grad w und erfüllt die Forderungen von Satz 2a.

Literaturverzeichnis

[1] L. Carlitz, *Permutations in finite fields*, Acta Sci. Math. Szeged 24 (1963), S. 196-203.

[2] H. Davenport and D. J. Lewis, *Notes on congruences I*, Quart. J. Math. Oxford, Ser. (2) 14 (1963), S. 51-60.

[3] L. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group I*, Ann. of Math. 11 (1896), S. 65-120.

[4] V. A. Kurbatov, *Über die Monodromiegruppe einer algebraischen Funktion*, Math. Sbornik, n. Ser. 25 (65) (1949), S. 51-94 (russisch).

[5] W. Nöbauer, *Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen*, Monatsh. Math. 69 (1965), S. 230-238.

[6] W. Sierpiński, *Arytmetyka teoretyczna*, Warszawa 1955.

[7] I. Schur, *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*, Berl. Ber., 1923, S. 123-134.

[8] U. Wegner, *Über die ganzzahligen Polynome, die für unendlich viele Primzahlmoduln Permutationen liefern*, Berlin, Philos. Diss., 1928.

Reçu par la Rédaction le 18. 10. 1965

ACTA ARITHMETICA
XI (1966)

A summation formula and an identity for a class of Dirichlet series

by

Marjorie Senechalle (Fortaleza, Ceará)

1. Introduction. The sum $\sum_{x<n\leqslant y} a(n)f(n)$, where $a(n)$ is a sequence of complex numbers and f is a complex-valued function defined on $(0, \infty)$, can sometimes be expressed by a formula involving the series $\sum_{n=1}^{\infty} a(n)f(n)$. The Poisson and Voronoï summation formulae are of this type, and many other such formulae have been obtained since Voronoï raised the problem in 1904 ([4]). In 1956 A. Sklar ([2]) derived a general formula from which many important examples can be obtained, including the two mentioned above, the Hardy-Landau formula for $\sum_{x<n\leqslant y} r_2(n)f(n)$, and the formula, due to Sklar, for $\sum_{x<n\leqslant y} \tau(n)f(n)$ (where $\tau(n)$ is Ramanujan's τ-function). In this paper we generalize the work of Sklar ([2], [3]) and present a simple and straightforward proof of a summation formula applicable to a large class of generalized Dirichlet series. We then show that this leads directly to an identity for the functions which are associated with the series.

2. Preliminaries. The letter s will denote a complex variable with real part σ and imaginary part t. A summation sign with the index of summation omitted will always precede an expression containing n. Accordingly, a bare summation sign will indicate summation over all positive integral values of n, while the symbol $\sum^{y}$, for $y>0$, will denote summation over all n such that $\lambda_n \in (0, y\rangle$, $\sum_{y}$ will denote summation over all n such that $\lambda_n \in (y, \infty)$, and $\sum_{x}^{y}$ will mean summation over all n for which $\lambda_n \in (x, y\rangle$. We will use $\int_{(a)}$, for real a, to denote the integral $\int_{a-i\infty}^{a+i\infty}$.

The series $\sum a(n)\lambda_n^{-s}$ which we will consider are those with the following properties:

(i) the coefficients $a(n)$ are complex numbers;

(ii) the sequence λ_n is positive, strictly increasing, and unbounded;