4. The table on the preceding page lists the value of $s(n)$ for all $n \leq 113$. All entries for $s(n)$ were computed individually and checked by means of Theorem 2.

References


University of New Mexico

ON THE CONTENT OF POLYNOMIALS

FRED KRAKOWSKI

1. Introduction. The content $C(f)$ of a polynomial $f$ with coefficients in the ring $R$ of integers of some algebraic number field $K$ is the ideal in $R$ generated by the set of coefficients of $f$. This notion plays an important part in the classical theory of algebraic numbers. Answering a question posed to the author by S. K. Stein, we show in the present note that content, as a function on $R[x]$ with values in the set $J$ of ideals of $R$, is characterized by the following three conditions:

(1) $C(f)$ depends only on the set of coefficients of $f$;
(2) if $f$ is a constant polynomial, say $f(x) = a$, $a \in R$, then $C(f) = (a)$, where $(a)$ denotes the principal ideal generated by $a$;
(3) $C(f \cdot g) = C(f) \cdot C(g)$ (Theorem of Gauss-Kronecker, see [1, p. 105]).

2. Characterization of content. Denote by $[f]$ the set of nonzero coefficients of $f \in R[x]$ and call $f$, $g$ equivalent, of $f \sim g$, if $[f] = [g]$. A polynomial is said to be primitive if its coefficients are rational integers and if the g.c.d. of its coefficients is 1.

Lemma. Let $S$ be a set of polynomials with coefficients in $R$ and suppose it satisfies:

(1) $1 \in S$;
(2) if $f \in S$ and $f \sim g$, then $g \in S$;
(3) if $f \cdot g \in S$, then $f \in S$ and $g \in S$.

Then $S$ contains all primitive polynomials.

Received by the editors April 27, 1964.
Proof. We will call a polynomial \( f \) with rational integer coefficients special, if \( 1 \in [f] \) and \( a \in f \) implies \(-a \in f \). If \( \rho(x) = \sum_{k=0}^{n} c_k x^k \) is primitive, let \( g(x) = \sum_{k=0}^{n} d_k x^k \), where \( d_0, d_1, \ldots, d_n \) are rational integers such that \( \sum_{k=0}^{n} c_k d_{n-k} = 1 \). Then \( [pg] \) contains 1 and \( pg(x^{2n+1} - 1) \) is special. By virtue of condition (3) it suffices to show that every special polynomial is in \( S \).

Let therefore \( f \) be special and let \( m_f \) be the maximum of the absolute values of the coefficients of \( f \). We now proceed by induction on \( m_f \).

If \( m_f = 1 \), then \( f \sim x^2 - x + 1 \) and since \( (x+1)(x^2-x+1) = x^3 + 1 \sim 1 \) and \( 1 \in S \), it follows that \( f \in S \).

Let now \( m_f > 1 \) and \([f] = \{1, -1, m, -m, a_1, -a_1, \ldots, a_n, -a_n\}, \)
\( |a_k| < m, \ k = 1, \ldots, n \). Consider the polynomial \( f_1(x) = -1 + mx - mx^2 + x^4 + a_1 x^6 + a_1 x^7 + \ldots + a_n x^{4n+1} - a_n x^{4n+3}. \) Clearly \( f_1 \sim f \). Multiplying \( f_1 \) by \( x + 1 \) we obtain
\[
g(x) = f_1(x)(x + 1)
\]
\[
= -1 + (m - 1)x - (m - 1)x^3 + x^4 + a_1 x^6 + a_1 x^7 - a_1 x^8 + \ldots + a_n x^{4n+1} + a_n x^{4n+2} - a_n x^{4n+3} - a_n x^{4n+4}.
\]
g is special and \( m_g = m - 1 \). Applying the induction hypothesis, we get \( g \in S \). Hence \( f_1 \in S \) by (3) and \( f \in S \) by (2), which proves the lemma.

Theorem. Let \( J \) be the set of ideals in \( R \) and \( h \) a function on \( R[x] \) with values in \( J \) satisfying the conditions:

1. If \( f, g \in R[x] \) and \( f \sim g \), then \( h(f) = h(g) \);
2. If \( f \) is constant, say \( f(x) = a, a \in R \), then \( h(f) = (a) \);
3. \( h(fg) = h(f) \cdot h(g) \).

Then \( h(f) = C(f) \) for all \( f \in R[x] \).

Proof. Consider first the case, where \( 1 \in [f] \). We may assume \( f \) is of the form \( x^n + a_1 x^{n-1} + \ldots + a_n, a_i \in R, i = 1, \ldots, n \). Let \( \theta_i \) be a primitive element of the field \( K \) and \( \theta_2, \ldots, \theta_r \) its conjugates. Each \( a_i \) is then a polynomial \( p_i(\theta_j) \) with rational coefficients. Let \( a_{ij} = p_i(\theta_j), \ i = 1, \ldots, n, \ j = 1, \ldots, r \), and consider \( f_j(x) = x^n + a_1 x^{n-1} + \ldots + a_{nj}. \) Since the coefficients of \( f \) are integers of \( K \), the product \( F(x) = f_1 f_2 \ldots f_r \) has rational integer coefficients and those of \( f_2 \ldots f_r \) are also in \( R \). Now \( F \) is primitive as \( 1 \in [F] \). Since the set of all polynomials on which \( h \) assumes the value (1) satisfies the conditions of the lemma, we have \( h(F) = (1) \) and therefore \( h(f) = (1) \).

Next let \( C(f) \) be a principal ideal with generating element \( a \neq 0 \).

1 For this proof, I am indebted to E. P. Specker.
Then \( f(x) = af'(x) \), where \( C(f') = (1) \). We can find a polynomial 
\( g'(x) \in \mathbb{R}[x] \) such that \( 1 \in [f' \cdot g'] \). Then 
\( h(f'g') = h(f')h(g') = (1) \) and thus also \( h(f') = (1) \). Hence 
\( h(f) = h(a)h(f') = (a)(1) = (a) = C(f) \).

If, finally, \( C(f) \) is arbitrary, there is a positive integer \( k \) such that 
\( (C(f))^k \) is principal (see \([1, \text{p. 121}]\)). Now \( (C(f))^k = C(f^k) = h(f^k) = (h(f))^k \) and hence \( h(f) = C(f) \), because factorization into prime ideals is unique in \( \mathbb{R} \). This proves the theorem.

3. **An example.** The Gauss-Kronecker theorem applies to more general rings than just to the rings of integers in a number field. Our theorem however does not remain true if the elements of \( \mathbb{R} \) are no longer algebraic over the rationals, as will now be shown by an example.

Take for \( \mathbb{R} \) the ring of polynomials in one indeterminate \( y \) and with rational coefficients. \( \mathbb{R} \) is a principal ideal ring and clearly the Gauss-Kronecker theorem holds for the polynomials of \( \mathbb{R}[x] \). However, if \( f \in \mathbb{R}[x] \), say 
\[ f(x) = \sum_{i=0}^{n} a_i(y)x^i, \quad a_i(y) \in \mathbb{R}, \] 
let \( m(y) = \text{g.c.d.} (a_0(y), \ldots, a_n(y)) \) and let \( d \) be the degree of \( f/m \) with respect to \( y \). Take a fixed but arbitrary nonzero element \( r \in \mathbb{R} \) and define:

\[
\begin{align*}
    h(f) &= (m \cdot r^d), & \text{if } f \neq 0, \\
    h(0) &= 0.
\end{align*}
\]

The function \( h \) thus defined satisfies the assumptions of the theorem, but clearly \( h(f) \neq C(f) \), if \( f \) is not a constant polynomial.

**Reference**


**University of California at Davis**