77. On Coefficients of Cyclotomic Polynomials

By Jiro SUZUKI
Department of Mathematics, Sophia University

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 14, 1987)

Let $c_i^{(n)}$ be the coefficient of X^i in the n-th cyclotomic polynomial; we put namely

$$\Phi_n(X)=\prod_{d|n}(1-X^d)^{\mu(n/d)}=\sum_{i=0}^{\varphi(n)} c_i^{(n)}X^i.$$

n being a positive integer and μ, φ denoting the Möbius and Euler functions, respectively. The purpose of this note is to prove the following.

Theorem. *For any integer $s\in \boldsymbol{Z}$, there exist n, i such that $c_i^{(n)}=s$.*

In other words, the range C of $c_i^{(n)}$ for $n=1, 2, 3, \cdots$ covers the whole set $\boldsymbol{Z}$ of integers. It is obvious that $C\supset\{-1, 0, 1\}$ as $c_1^{(1)}=-1$, $c_1^{(4)}=0$, $c_1^{(2)}=1$, for example. If $n=p^r$, p being a prime, we have $c_i^{(n)}=0$ or 1, and it is shown in [1] that $c_i^{(n)}\in\{-1, 0, 1\}$ if $n=pq$ for distinct primes p, q. [2] describes a proof given by I. Schur of the fact that the absolute value of $c_i^{(n)}$ can be arbitrarily large, based on the following proposition (*P*) on the distribution of primes:

(P) *Let t be any integer >2. Then there exist t distinct primes $p_1<p_2<\cdots<p_t$ such that $p_1+p_2>p_t$.*

The proof of (*P*) is not given in [2], but it is easy to supplement it as shown below, and complete the proof of the theorem by a simple observation.

Proof of (*P*). Fix an integer $t>2$ and suppose (*P*) to be false for t. Then for any t distinct primes $p_1<p_2<\cdots<p_t$, we should have $p_1+p_2\leq p_t$ so that $2p_1<p_t$ which would imply that the number of primes between 2^{k-1} and 2^k is always less than t. Then $\pi(2^k)<kt$ contrary to the prime number theorem.

Proof of Theorem. Let t be any odd integer >2 and $p_1<p_2<\cdots<p_t$ t primes satisfying $p_1+p_2>p_t$. Let $p=p_t$ and $n=p_1p_2\cdots p_t$, and consider $\Phi_n(X)$ mod. X^{p+1} after Shur. We have obviously

$$\Phi_n(X)\equiv\prod_{i=1}^{t}(1-X^{p_i})/(1-X) \qquad (\text{mod } X^{p+1}).$$
$$\equiv(1+X+\cdots+X^p)(1-X^{p_1}-\cdots-X^{p_t}) \qquad (\text{mod } X^{p+1}).$$

This yields $c_p^{(n)}=-t+1$, $c_{p-2}^{(n)}=-t+2$, which shows $C\supset\{s\in\boldsymbol{Z};\ s\leq -1\}$ as t takes any odd integral value ≥ 3.

For an odd positive integer m we have

$$\Phi_{2m}(X)=\Phi_m(-X).$$

As $n=p_1p_2\cdots p_t$ is odd for $p_1\geq 3$, this remark yields for the above n with $p_1\geq 3$ $c_p^{(2n)}=t-1$, $c_{p-2}^{(2n)}=t-2$ which implies $C\supset\{s\in\boldsymbol{Z};\ s\geq 1\}$. Since $C\ni 0$, we have $C=\boldsymbol{Z}$.