ON THE MAGNITUDE OF THE COEFFICIENTS OF THE CYCLOTOMIC POLYNOMIAL

BY EMMA LEHMER

Until very recently all the results of the investigations into the magnitude of the coefficients of the cyclotomic polynomial

$$Q_n(x) = \prod_{\delta | n} (1 - x^{n/\delta})^{\mu(\delta)} \tag{1}$$

tended to show that these coefficients are very small indeed. In fact for $n<105$ all the coefficients are ± 1, and 0, and for $n<385$ they do not exceed 2 in absolute value.

In 1883 Migotti* showed that the coefficients of $Q_n(x)$ are all ± 1 or 0 for n a product of two primes, but noted that the coefficient of x^7 in $Q_{105}(x)$ is -2. In 1895 Bang† proved that no coefficient of $Q_n(x)$ for $n=pqr$, ($p<q<r$, odd primes), exceeds $p-1$.

Nothing further was done on the problem until 1931, when I. Schur gave a very ingenious proof of the following theorem.

SCHUR'S THEOREM. *There exist cyclotomic polynomials with coefficients arbitrarily large in absolute value.*

As this proof has not been published, it is given below.‡

PROOF. Let $n=p_1p_2 \cdots p_t$, where t is odd and $p_1<p_2< \cdots <p_t$ are odd primes such that§ $p_1+p_2>p_t$. To prove the theorem it is sufficient to show that the coefficient of x^{p_t} in $Q_n(x)$ is $1-t$. This can be done by taking $Q_n(x)$ modulo x^{p_t+1}. We then get

$$\begin{aligned} Q_n(x) &\equiv \prod_{i=1}^{t} (1 - x^{p_i})/(1 - x) \\ &\equiv (1 + x + \cdots + x^{p_t-1})(1 - x^{p_1})(1 - x^{p_2}) \cdots (1 - x^{p_{t-1}}) \\ &\equiv (1 + x + \cdots + x^{p_t-1})(1 - x^{p_1} - x^{p_2} - \cdots - x^{p_{t-1}}) \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\mathrm{mod}\ x^{p_t+1}). \end{aligned}$$

* Sitzungsberichte, Akademie der Wissenschaften, Wien. (math), (2), vol. 87 (1883), pp. 7–14.

† Nyt Tidsskrift for Mathematik, (B), vol. 6 (1895), pp. 6–12.

‡ This proof is essentially the one given by Schur in a letter to Landau.

§ Such a set of primes exists for every t.

Collecting the coefficient of x^{pt} in this last expression we see that it is precisely $-(t-1)$, so that as t increases we can exhibit arbitrarily large negative coefficients of the cyclotomic polynomials, which proves the theorem.

The question now remains as to the boundedness of the coefficients of $Q_n(x)$ for a fixed t. We have already seen that for $t=1$ and 2 these coefficients are actually bounded. The case $t=3$ was discussed by Bungers* who proved the following theorem.

BUNGERS' THEOREM. *As n runs over all products of three distinct primes, the cyclotomic polynomials $Q_n(x)$ contain arbitrarily large coefficients, provided there exist infinitely many prime pairs.*

His proof depends on choosing three primes, two of which differ by 2, and in exhibiting a coefficient of $Q_{pqr}(x)$ equal to $(p+1)/2$. It is the purpose of this note to modify Bungers' proof so as to eliminate the unproved assumption of the existence of infinitely many prime pairs.

Let $n=pqr$, where $q=kp+2$, and $r=(mpq-1)/2$. For a given p such primes q and r can always be found by Dirichlet's Theorem. We proceed to show that the coefficient of x^h, where $h=(p-3)(qr+1)/2$ is $(p-1)/2$ and hence can be made arbitrarily large with p. From (1) with $n=pqr$, we have

$$\begin{aligned} Q_{pqr}(x) &= \frac{(x^{pqr}-1)(x^p-1)(x^q-1)(x^r-1)}{(x-1)(x^{pq}-1)(x^{pr}-1)(x^{qr}-1)} \\ &\equiv (1+x+\cdots+x^{p-1})(1-x^q-x^r+x^{q+r}) \\ &\quad \cdot \sum x^{\nu qr+\lambda pr+\mu pq} \qquad (\text{mod } x^{pqr}). \end{aligned}$$

Since we are interested in the coefficient of x^h, the summation indices ν, λ, μ, satisfy the following inequalities:

$$(2) \qquad \nu qr \leqq h, \qquad \lambda pr \leqq h, \qquad \mu pq \leqq h.$$

We now consider the diophantine equation

$$(3) \quad \nu qr + \lambda pr + \mu pq + \omega + \epsilon q + \eta r = (p-3)(qr+1)/2 = h,$$

where $\omega < p$, and $\epsilon = 0$ or 1, $\eta = 0$ or 1.

The coefficient of x^h is now given by the number of solutions of (3) with $\epsilon=\eta$ minus the number of solutions of (3) with $\epsilon \neq \eta$.

---

* Göttingen Dissertation, 1934.

Taking (3) modulo p, q, and r we have, since $qr \equiv -1 \pmod{p}$,

$$\begin{aligned} \nu qr + \omega + \epsilon q + \eta r &\equiv 0 \pmod{p}, \\ \lambda pr + \omega + \qquad \eta r &\equiv (p-3)/2 \pmod{q}, \\ \mu pq + \omega + \epsilon q \qquad &\equiv (p-3)/2 \pmod{r}. \end{aligned}$$

Multiplying the last two congruences by k and m, respectively, and remembering that $kpr \equiv 1 \pmod{q}$, while $mpq \equiv 1 \pmod{r}$, also that $q \equiv 2 \pmod{p}$, and $r \equiv -1/2 \pmod{pq}$, we get

$$\omega \equiv \nu - 2\epsilon + \eta/2 \pmod{p}, \tag{4}$$

$$\lambda \equiv k((p-3)/2 - \omega + \eta/2) \pmod{q}, \tag{5}$$

$$\mu \equiv m((p-3)/2 - \omega - \epsilon q) \pmod{r}. \tag{6}$$

We shall now show that if $\epsilon = \eta = 0$, (3) has $(p-1)/2$ solutions, while in the other three cases (3) has no solutions.

If $\epsilon = \eta = 0$, (4) gives us $\omega \equiv \nu \pmod{p}$ and since both ω and ν are less than p, $\omega = \nu$. Equations (5) and (6) become in this case

$$\begin{aligned} \lambda &\equiv k((p-3)/2 - \nu) \pmod{q}, \\ \mu &\equiv m((p-3)/2 - \nu) \pmod{r}. \end{aligned}$$

Since $\nu \leqq (p-3)/2$, and $k(p-3)/2$ and λ are $< q$, while $m(p-3)/2$ and μ are $< r$, these congruences are actually equalities, and we have determined for each of the $(p-1)/2$ values of ν, corresponding values of λ and μ, which are such that $\lambda \leqq k(p-3)/2$, so that

$$\lambda pr \leqq kpr(p-3)/2 < qr(p-3)/2 < h,$$

and $\mu \leqq m(p-3)/2$, so that

$$\mu pq \leqq mpq(p-3)/2 \leqq (2r+1)(p-3)/2 < h,$$

so that all the variables are determined within the ranges (2), and hence in the case $\epsilon = \eta = 0$, (3) has $(p-1)/2$ solutions.

For $\epsilon = 1$, $\eta = 0$, (4) gives us $\omega \equiv \nu - 2 \pmod{p}$. Hence either $\omega = \nu - 2$, or $\omega = p - 1$, or $p - 2$. In the last two cases we can use (5) to get

$$\lambda \equiv k((p-3)/2 - \omega) \equiv -k(p \pm 1)/2 \pmod{q}.$$

That is,

$$\lambda = q - k(p \pm 1)/2 \geqq q - k(p-1)/2,$$

so that

$$\begin{aligned}\lambda pr &\geqq pqr - kpr(p-1)/2 > pqr - qr(p-1)/2\\ &= qr(p+1)/2 > h.\end{aligned}$$

Hence for $\omega = p-1$ or $p-2$, (2) is violated for λpr, and there are no solutions. If $\omega = \nu - 2 \leqq (p-7)/2$, we use (6) and obtain

$$\mu \equiv m((p-3)/2 - \omega - q) \pmod{r},$$

or

$$\mu = r + m((p-3)/2 - \omega - q) \geqq r + m(2-q).$$

Hence

$$\begin{aligned}\mu pq &\geqq pqr + (2r+1)(2-q)\\ &= (qr+1)(p-2) + (4r - p - q + 4)\\ &> (qr+1)(p-2) > h,\end{aligned}$$

so that (2) is again violated and there are no solutions of (3) for $\epsilon = 1$, $\eta = 0$.

In the next case $\epsilon = 0$, $\eta = 1$, we get from (4) $\omega = \nu + (p+1)/2$, and putting this value for ω in (6), we have

$$\mu \equiv m((p-3)/2 - \nu - (p+1)/2) \pmod{r}.$$

Hence $\mu = r - m(\nu+2) \geqq r - m(p+1)/2$, so that

$$\begin{aligned}\mu pq &\geqq pqr - (2r+1)(p+1)/2 > pqr - (2r+1)(q-1)/2\\ &= (qr+1)(p-1) + (2r - q - 2p + 3)/2\\ &> (qr+1)(p-1) > h.\end{aligned}$$

Thus this case does not yield any further solutions. We have now shown that (3) has at least $(p-1)/2$ solutions, since the remaining case $\epsilon = \eta = 1$ would contribute positively, if at all. In fact, it can be shown by a similar reasoning that this case does not contribute any solutions, so that the coefficient of x^h is precisely $(p-1)/2$. However, in any case, the coefficient of x^h increases with p, so that we have proved the following theorem.

THEOREM. *As n runs over all products of three distinct primes, the cyclotomic polynomials $Q_n(x)$ contain arbitrarily large coefficients.*

BETHLEHEM, PENNSYLVANIA