



The Midterm Coefficient of the Cyclotomic Polynomial $F_p(x)$

Author(s): Marion Beiter

Source: *The American Mathematical Monthly*, Vol. 71, No. 7 (Aug. - Sep., 1964), pp. 769-770

Published by: [Mathematical Association of America](#)

Stable URL: <http://www.jstor.org/stable/2310894>

Accessed: 20/01/2011 04:19

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions of Use, available at <http://www.jstor.org/page/info/about/policies/terms.jsp>. JSTOR's Terms and Conditions of Use provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

Please contact the publisher regarding any further use of this work. Publisher contact information may be obtained at <http://www.jstor.org/action/showPublisher?publisherCode=maa>.

Each copy of any part of a JSTOR transmission must contain the same copyright notice that appears on the screen or printed page of such transmission.

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.



Mathematical Association of America is collaborating with JSTOR to digitize, preserve and extend access to *The American Mathematical Monthly*.

<http://www.jstor.org>

THE MIDTERM COEFFICIENT OF THE CYCLOTOMIC POLYNOMIAL $F_{pq}(x)$

SISTER MARION BEITER, Rosary Hill College, Buffalo

Introduction. The interested reader will find the background in cyclotomy in [3] and [4] sufficient for the purpose of this note, although the investigation is based on results in [1] and [2].

The monic polynomial whose roots are the primitive m th roots of unity is defined to be the cyclotomic polynomial $F_m(x)$. By Dedekind's inversion formula ([4] p. 114),

$$(1) \quad F_m(x) = \prod_{d|m} (x^d - 1)^{\mu(m/d)}.$$

In [1] it is proved that if m is a product of two distinct odd primes, p and q , then the coefficients of $F_{pq}(x)$ can equal only ± 1 or 0.

General coefficient. Let $F_{pq}(x) = \sum_{n=0}^{\phi(pq)} c_n x^n$.

THEOREM I. In $F_{pq}(x)$

$$(2) \quad c_n = \begin{cases} (-1)^\delta & \text{if } n = \alpha q + \beta p + \delta \text{ in exactly one way,} \\ 0 & \text{otherwise,} \end{cases}$$

where α and β are nonnegative integers and $\delta = 0, 1$.

Proof. From (1) it follows that

$$\begin{aligned} F_{pq}(x) &= (x^{pq} - 1)(x - 1)/(x^p - 1)(x^q - 1) \\ &= (1 - x)(1 + x^q + \dots + x^{(p-1)q})(1 + x^p + x^{2p} + \dots) \\ &= \sum_{\alpha=0}^{p-1} x^{\alpha q} \sum_{\beta=0}^{\infty} x^{\beta p} - \sum_{\alpha=0}^{p-1} x^{\alpha q+1} \sum_{\beta=0}^{\infty} x^{\beta p} \\ &= \sum_{\alpha, \beta, \delta} (-1)^\delta x^{\alpha q + \beta p + \delta}, \end{aligned}$$

where α runs through the integers from zero to $p-1$, β is any nonnegative integer, and $\delta = 0, 1$. Then c_n in $F_{pq}(x)$ is the sum of the coefficients of all terms on the right with exponent $\alpha q + \beta p + \delta = n$. Where no such partition exists, c_n is zero. If there is exactly one partition, c_n equals $(-1)^\delta$.

Assume that n can be partitioned in two ways:

$$\begin{aligned} n &= \alpha_1 q + \beta_1 p + \delta_1 \\ &= \alpha_2 q + \beta_2 p + \delta_2, \end{aligned}$$

with $\delta_1 = \delta_2$. Then $q(\alpha_1 - \alpha_2) = p(\beta_2 - \beta_1)$. This implies that p divides $\alpha_1 - \alpha_2$. But since $\alpha < p$, $|\alpha_1 - \alpha_2| < p$. Therefore $\alpha_1 - \alpha_2 = \beta_2 - \beta_1 = 0$, and the two partitions are identical. Hence, when two distinct partitions of n in the form (2) exist, in one of them $\delta = 1$, in the other $\delta = 0$. In this case c_n is $(-1)^1 + (-1)^0 = 0$, and the theorem is proved.

A discussion similar to this occurs in [1]

Midterm coefficient. Set $n = \phi(pq)/2$ in (2). Then

$$\begin{aligned} (p - 1)(q - 1)/2 &= \alpha q + \beta p + \delta, \\ p(2\beta + 1) &\equiv 1 - 2\delta \pmod{q}, \\ px &\equiv \pm 1 \pmod{q}. \end{aligned}$$

Let k be the solution of $px \equiv 1 \pmod{q}$, $1 \leq k \leq q - 1$. Then $q - k$ is a solution of $px \equiv -1 \pmod{q}$.

Consider $pk \equiv 1 \pmod{q}$. Then

$$\begin{aligned} pk &= 1 + qh, & h &= (pk - 1)/q, \\ \beta &= (k - 1)/2 & \alpha &= (p - 1)/2 - h/2. \end{aligned}$$

In the case k is odd, these values of α and β are integral, $\delta = 0$, and the midterm coefficient is 1.

If k is even, $q - k$ is odd, $\delta = 1$, and the midterm coefficient is -1 . Thus we have

THEOREM II. In $F_{pq}(x)$, when $n = \phi(pq)/2$, $c_n = (-1)^{k-1}$, where k is the least positive solution of the congruence $px \equiv 1 \pmod{q}$.

Remarks. In the special case $q = sp + 1$, k is odd and the midterm coefficient is $+1$. Similarly, for $q = sp - 1$, k is even and the midterm coefficient is -1 .

In any case, the roles of p and q in the congruences may be reversed, without affecting the oddness or evenness of k .

The following table gives the value of the midterm coefficient c_n of $F_{pq}(x)$ when p is 3, 5, or 7. All values of $m = pq$ and less than 143 reduce to one of these special cases.

p	a	c_n
3	1	} ± 1 according as $q \equiv \pm a \pmod{p}$.
5	1, 2	
7	1, 3, 5	

The author thanks the referee for his suggestions.

Work done in part while a member of an NSF Postdoctoral Research Participation Program in Mathematics at the University of Oklahoma, Summer 1962.

References

1. A. S. Bang, Om Ligningen $\phi_n(x) = 0$, *Nyt Tidsskrift for Matematik*, 6 (1895) 6-12.
2. A. Migotti, Zur Theorie der Kreisteilungsgleichung, *S.-B. der Math.-Naturwiss. Classe der Kaiserlichen Akademie der Wissenschaften, Wien*, (2) 87 (1883) 7-14.
3. T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.
4. B. L. van der Waerden, *Modern Algebra*, transl. Fred Blum, Stechert-Hafner, New York, 1949.