ISSN 2220-5438

Moscow Journal of Combinatorics and Number Theory

URSS

Vol. 1 • Issue 1 2011

Moscow Journal of Combinatorics and Number Theory. 2011. Vol. 1. Iss. 1. 80 p.

The journal was founded in 2010

The aim of this journal is to publish original, high-quality research articles from a broad range of interests within combinatorics, number theory and allied areas. One volume of four issues is published annually.

Published by the Moscow Institute of Physics and Technology with the support of Yandex and Microsoft.

Website
http://mjcnt.phystech.edu

E-mail
mjcnt@phystech.edu

Address of the Editorial Board

Faculty of Innovations
and High Technology,
Laboratorny Korpus, k. 209,
9, Institutskii pereulok,
Dolgoprudny,
Moscow Region,
Russia,
141700

Адрес редакции

Факультет инноваций
и высоких технологий
Лабораторный корпус, к. 209,
Институтский переулок, д. 9,
г. Долгопрудный,
Московская область,
Российская Федерация,
141700

URSS Publishers

56, Nakhimovsky Prospekt,
Moscow,
Russia,
117335

Издательство «УРСС»

Нахимовский пр-т, 56
Москва,
Российская Федерация,
117335

Журнал зарегистрирован в Федеральной службе по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия 3 сентября 2010 г. Свидетельство ПИ № ФС77-41900.

Формат 70×100/16. Печ. л. 5. Зак. № 4714.
Отпечатано в ООО «ЛЕНАНД».
117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISSN 2220-5438

Moscow Journal of Combinatorics and Number Theory
2011. Vol. 1. Iss. 1.
PP. 11–16

Divisibility of the resultant of a polynomial and a cyclotomic polynomial

Artūras Dubickas (Vilnius)

Abstract: We investigate the divisibility of the resultant of a polynomial $f \in \mathbb{Z}[x]$ and a cyclotomic polynomial $x^\ell - 1$. We prove that for $\ell = s^k$ this resultant is divisible by s^{k+1} if $s | f(1)$. Some related results are also given. As a consequence, we obtain a result of Newman on the divisibility of $\det C_n$, where C_n is an integral circular $n \times n$ matrix.

Keywords: Cyclotomic polynomial, resultant, divisibility

AMS Subject classification: 11C08, 11B83, 11R04, 11R09

Received: 05.10.2010

1. Introduction

Let

$$f(x) := a \prod_{i=1}^{d} (x - \alpha_i)$$

be a polynomial in $\mathbb{Z}[x]$ with $a \in \mathbb{N}$. For each positive integer ℓ, we define

$$f_\ell(x) := a^\ell \prod_{i=1}^{d} (x - \alpha_i^\ell) \in \mathbb{Z}[x],$$

so that $f_1(x) = f(x)$. The sequence of values of such polynomials $f_\ell(x)$ at $x = 1$, $\ell = 1, 2, 3, \ldots$, for a monic polynomial f has been considered by Pierce [12] and Lehmer [9]. In particular, Lehmer used $f_\ell(1)$ for some special polynomials f and found some large (at that time!) prime numbers. For instance, he found the prime number 3233514251032733 as the value of $f_{127}(1)$ starting with $f(x) = x^3 - x - 1$. The values $f_\ell(1)$ also appear in knot theory; see, e.g., [13]. It is worth remarking that the integer sequence $f_1(1), f_2(1), f_3(1), \ldots$ is a *divisibility sequence*, i.e. $f_k(1) | f_m(1)$ whenever $k | m$. We shall often use this fact below without further notice.

In this note we prove the following divisibility result:

THEOREM 1. *Let $s, r, k \in \mathbb{N}$ and $f \in \mathbb{Z}[x]$. If $s^r | f(1)$ then $s^{k+r} | f_{s^k}(1)$.*

Theorem 1 can be easily verified for linear polynomials $f(x) = ax - b$. Then $f_{s^k}(x) = a^{s^k}x - b^{s^k}$, so that $f(1) = a - b$ and $f_{s^k}(1) = a^{s^k} - b^{s^k}$. Using binomial coefficients one can easily check that $s^r|(a-b)$ implies $s^{k+r}|(a^{s^k} - b^{s^k})$.

Note that $f_\ell(1)$ is $\pm$ the resultant of the polynomials $f(x)$ and $x^\ell - 1$:

$$|f_\ell(1)| = |a^\ell \prod_{i=1}^{d}(1-\alpha_i^\ell)| = \prod_{t=0}^{\ell-1}|f(e^{2\pi it/\ell})| = |\mathrm{Res}(f(x), x^\ell - 1)|. \tag{1}$$

In this context, Theorem 1 is comparable with the following divisibility result of Hare, McKinnon and Sinclair [6]. Let $f \in \mathbb{Z}[x]$ be a monic polynomial. Then, for any prime number p and any integers $m > k \geqslant 0$,

$$p^{(k+1)\deg f} | \mathrm{Res}(f_{p^m}(x), f_{p^k}(x)). \tag{2}$$

For the pair $(m, k) = (1, 0)$, this result was earlier proved by Dobrowolski [3]. A simple proof of (2) was recently given by the author in [4]. In fact, we will show that the same conclusion holds for every (not necessarily monic) $f \in \mathbb{Z}[x]$:

THEOREM 2. *Let p be a prime number, and let $m > k \geqslant 0$ be two integers. Then, for every $f \in \mathbb{Z}[x]$ of degree d, $p^{(k+1)d}$ divides the resultant of f_{p^m} and f_{p^k}.*

Our main tool in [4] was the following congruence. Suppose $\beta_1, \ldots, \beta_D$ are the roots of a monic polynomial with integer coefficients, and suppose p is a prime number. Then

$$\beta_1^{p^t} + \ldots + \beta_D^{p^t} \equiv \beta_1^{p^{t-1}} + \ldots + \beta_D^{p^{t-1}} \pmod{p^t} \tag{3}$$

for every $t \in \mathbb{N}$. See, for instance, the papers of Smyth [14], Vinberg [15], Zarelua [16] (the latter two motivated by Arnold's problems raised in [2]) for various proofs of the congruence (3) and [7] for a related result. Using (3) we shall also prove the following:

THEOREM 3. *Let p be a prime number, $k \in \mathbb{N}$ and $f \in \mathbb{Z}[x]$. If $p|f_n(1)$ and $p^k|n$ then $p|f_{n/p^k}(1)$.*

Theorems 1 and 3 yield the following corollary:

COROLLARY 1. *Let C_n be an $n \times n$ circulant matrix with integral entries, $m = \det C_n$. Suppose $\gcd(m, n) > 1$, and suppose p is a prime number dividing both m and n. If $p^k||n$ then $p^{k+1}|m$.*

Recall that the circulant matrix with the first row $(a_0, a_1, \ldots, a_{n-1})$ is defined by

$$C_n := \begin{pmatrix} a_0 & a_1 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \ldots & a_0 \end{pmatrix}. \tag{4}$$

A different proof of Corollary 1 was given by Newman [11] in connection with a question of Olga Taussky-Todd: *determine all possible values m of* $\det C_n$, *as C_n runs through all $n \times n$ circular integral matrices.* Newman's theorem proved to be an important tool in Kaiblinger's paper [8], where he disproved a conjecture of Lind [10] concerning some kind of Lehmer's problem for a cyclic group. More precisely, Lind asked for the smallest number $m > 1$ which can be attained as $|\det C_n|$ for some integer circular $n \times n$ matrix C_n. According to [8], this problem (which is only a subproblem to that of Olga Taussky-Todd) is still open for $n = 420$. It is known that for $n = 420$ this smallest m belongs to the set $\{8, 9, 11\}$.

2. Proof of Theorem 1

The statement of the theorem is trivial for $s = 1$ and for $f(1) = 0$, because then $f_\ell(1) = 0$ for each positive integer ℓ. Assume that $s \geqslant 2$ and $f(1) \neq 0$.

For each integer $s \geqslant 2$, set

$$u_s(x) := s - 1 + (s-2)x + \ldots + x^{s-2}.$$

Then

$$\frac{1-x^s}{1-x} = 1 + x + \ldots + x^{s-1} = s - (1-x)u_s(x)$$

for each complex number $x \neq 1$. It follows that

$$\frac{f_s(1)}{f(1)} = a^{s-1} \prod_{i=1}^{d} \frac{1-\alpha_i^s}{1-\alpha_i} = a^{s-1} \prod_{i=1}^{d} (s - (1-\alpha_i)u_s(\alpha_i)). \tag{5}$$

Putting

$$R_{s,0} := a^{s-2} \prod_{i=1}^{d} u_s(\alpha_i)$$

for the resultant of f and u_s and

$$g(x) := a^{s-1} \prod_{i=1}^{d} (x - (1-\alpha_i)u_s(\alpha_i)) \in \mathbb{Z}[x],$$

we obtain

$$(-1)^d f(1) R_{s,0} = a^{s-1}(-1)^d \prod_{i=1}^{d} (1-\alpha_i)u_s(\alpha_i) = g(0) \equiv g(s) \pmod{s}.$$

Note that $g(s)$ is the right hand side of (5), so

$$\frac{f_s(1)}{f(1)} \equiv (-1)^d f(1) R_{s,0} \pmod{s}. \tag{6}$$

By the same argument, for every $t \in \mathbb{N}$, replacing x by x^{s^t}, we obtain

$$\frac{f_{s^{t+1}}(1)}{f_{s^t}(1)} \equiv (-1)^d f_{s^t}(1) R_{s,t} \pmod{s} \tag{7}$$

with

$$R_{s,t} := a^{(s-2)s^t} \prod_{i=1}^{d} u_s(\alpha_i^{s^t}) \in \mathbb{Z}$$

provided that $f_{s^t}(1) \neq 0$.

Now, from $f(1) \neq 0$, $s^r | f(1)$ and (6) we deduce that the integer $f_s(1)/f(1)$ is divisible by s. Hence $s^{r+1} | f_s(1)$. Assume that $f_{s^l}(1) \neq 0$ for each $l \in \mathbb{N}$. Then, employing (7), by induction on $t = k-1$, we see that $s^{k-1+r} | f_{s^{k-1}}(1)$ and $s | f_{s^k}(1)/f_{s^{k-1}}(1)$. Thus $s^{k+r} | f_{s^k}(1)$ for every $k \in \mathbb{N}$, as claimed.

If $f_{s^l}(1) = 0$ for some $l \in \mathbb{N}$ and l is the smallest positive integer with this property then, by the above argument, $s^{k+r} | f_{s^k}(1)$ for $k < l$. Furthermore, $f_{s^k}(1) = 0$ for each $k \geqslant l$. Thus $s^{k+r} | f_{s^k}(1)$ for every $k \in \mathbb{N}$ in this case too.

3. Proofs of Theorems 2, 3 and Corollary 1

LEMMA 1. *Suppose that $f \in \mathbb{Z}[x]$, p is a prime number and $m > k \geqslant 0$ are integers. Then all the coefficients of the polynomial $f_{p^m}(x) - f_{p^k}(x)$ are divisible by p^{k+1}.*

PROOF. Write

$$f_{p^m}(x) - f_{p^k}(x) = a^{p^m} \prod_{i=1}^{d} (x - \alpha_i^{p^m}) - a^{p^k} \prod_{i=1}^{d} (x - \alpha_i^{p^k}).$$

Multiplying and collecting terms for x^{d-j}, $j = 0, 1, \ldots, d$, we deduce that

$$f_{p^m}(x) - f_{p^k}(x) = \sum_{j=0}^{d} (-1)^j x^{d-j} (a^{p^m} \sigma_j(\alpha^{p^m}) - a^{p^k} \sigma_j(\alpha^{p^k})), \tag{8}$$

where

$$\sigma_j(\alpha^v) := (\alpha_1 \ldots \alpha_j)^v + \ldots + (\alpha_{d-j+1} \ldots \alpha_d)^v$$

for $v \in \mathbb{N}$ is the jth elementary symmetric polynomial in $\alpha_1^v, \ldots, \alpha_d^v$ containing $\binom{d}{j}$ terms.

Fix an integer j satisfying $0 \leqslant j \leqslant d$. The numbers $\beta_1 = a\alpha_1 \ldots \alpha_j, \ldots, \beta_D = a\alpha_{d-j+1} \ldots \alpha_d$, where $D = \binom{d}{j}$, are the roots of a monic integer polynomial, since $a\alpha_{i_1} \ldots \alpha_{i_j}$ is an algebraic integer for every set of indices $i_1, \ldots, i_j$ satisfying $0 \leqslant i_1 < \ldots < i_j \leqslant d$ and every automorphism σ of the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha_1, \ldots, \alpha_d)/\mathbb{Q})$ maps the collection of $\binom{d}{j}$ (not necessarily distinct) numbers

$$\{a\alpha_{i_1} \ldots \alpha_{i_j} | 0 \leqslant i_1 < \ldots < i_j \leqslant d\}$$

into itself. Applying (3) to $t = k+1, \ldots, m$ and adding all such congruences we

derive that

$$\beta_1^{p^m} + \ldots + \beta_D^{p^m} \equiv \beta_1^{p^k} + \ldots + \beta_D^{p^k} \pmod{p^{k+1}}. \tag{9}$$

Here, the left hand side of (9) equals $a^{p^m}\sigma_j(\alpha^{p^m})$, whereas the right hand side of (9) equals $a^{p^k}\sigma_j(\alpha^{p^k})$. Thus the difference $a^{p^m}\sigma_j(\alpha^{p^m}) - a^{p^k}\sigma_j(\alpha^{p^k})$ is divisible by p^{k+1}. This proves the lemma, by (8). □

Proof of Theorem 2. Evidently, $\mathrm{Res}(g, h) = \mathrm{Res}(g, h - g)$ for any polynomials g and h satisfying either $\deg(h - g) = \deg h$ or g monic. Applying this formula to $g := f_{p^m}$ and $h := f_{p^n}$ (so that $\deg(h - g) = \deg h$ for $a > 1$ and g is monic for $a = 1$), we obtain $\mathrm{Res}(f_{p^m}, f_{p^k}) = \mathrm{Res}(f_{p^m}, f_{p^k} - f_{p^m})$. Expressing the latter resultant as the determinant of the Sylvester matrix (see, e.g., [1]), we see that, by Lemma 1, each entry of its last d rows is divisible by p^{k+1}. Hence this determinant (and so $\mathrm{Res}(f_{p^m}, f_{p^k})$) is divisible by $p^{(k+1)d}$, as claimed. □

Proof of Theorem 3. Fix two positive integers r, t. Now, we shall apply the lemma to f_r (instead of f), $m := t$ and $k := t - 1$. Then the coefficients of the polynomial $f_{p^t r}(x) - f_{p^{t-1} r}(x)$ are all divisible by p^t. In particular,

$$p^t \mid (f_{p^t r}(1) - f_{p^{t-1} r}(1)) \tag{10}$$

for all integers $t, r \geqslant 1$.

Selecting $r := n/p^k$ and applying (10) to $t = k, k - 1, \ldots, 1$, we find that

$$f_{n/p^u}(1) \equiv f_{n/p^{u+1}}(1) \pmod{p}$$

for $u = 0, 1, \ldots, k - 1$. Adding these k congruences, we derive that $f_n(1) \equiv f_{n/p^k}(1) \pmod{p}$. But $p \mid f_n(1)$, so $p \mid f_{n/p^k}(1)$, as claimed. □

Proof of Corollary 1. It is well known that the determinant of the matrix given in (4) can be written as

$$\det C_n = \prod_{t=0}^{n-1} f(e^{2\pi i t/n})$$

with the polynomial $f(x) = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$. (See, e.g., pp. 1111-1112 in [5].) Hence $|m| = |\det C_n| = |f_n(1)|$, by (1).

Suppose p is a prime number such that $p \mid m$ and $p^k \| n$. Since $p \mid f_n(1)$ and $p^k \mid n$, Theorem 3 implies $p \mid f_{n/p^k}(1)$. Now, applying Theorem 1 to the polynomial $f_{n/p^k}(x)$ (instead of $f(x)$), $s := p$ and $r := 1$, we deduce that p^{k+1} divides $f_{p^k(n/p^k)}(1) = f_n(1)$. This yields $p^{k+1} \mid m$, since $m = \pm f_n(1)$. □

Acknowledgements. I thank the referee for pointing out several inaccuracies in the first draft of the paper.

Bibliography

1. ***A.G. Akritas,*** *Sylvester's forgotten form of the resultant*, Fibonacci Quart. **31** (1993), 325–332.
2. ***V.I. Arnold,*** *On the matricial version of Fermat-Euler congruences*, Japanese J. Math. **1** (2006), 1–24.
3. ***E. Dobrowolski,*** *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
4. ***A. Dubickas,*** *An extended lemma of Dobrowolski and Smyth's congruence*, Acta Sci. Math. (Szeged), (to appear).
5. ***I.S. Gradshteyn, I.M. Ryzhik,*** *Table of integrals*, *series*, *and products*, 6th ed. San Diego, CA: Academic Press, 2000.
6. ***K.G. Hare, D. McKinnon, C.D. Sinclair,*** *Patterns and periodicity in a family of resultants*, J. Théor. des Nombres Bordeaux **21** (2009), 215–234.
7. ***I.M. Isaacs, M.R. Pournaki,*** *Generalizations of Fermat's little theorem via group theory*, Amer. Math. Monthly **112**(8) (2005), 734–740.
8. ***N. Kaiblinger,*** *On the Lehmer constant of finite cyclic groups*, Acta Arith. **142** (2010), 79–84.
9. ***D.H. Lehmer,*** *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.
10. ***D. Lind,*** *Lehmer's problem for compact abelian groups*, Proc. Amer. Math. Soc. **133** (2005), 1411–1416.
11. ***M. Newman,*** *On a problem suggested by Olga Taussky-Todd*, Illinois J. Math. **24** (1980), 156–158.
12. ***T.A. Pierce,*** *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, Ann. of Math. **18** (1916), 53–64.
13. ***R. Riley,*** *Growth of order of homology of cyclic branched covers of knots*, Bull. London Math. Soc. **22** (1990), 287–297.
14. ***C.J. Smyth,*** *A coloring proof of a generalization of Fermat's little theorem*, Amer. Math. Monthly **93**(6) (1986), 469–471.
15. ***E.B. Vinberg,*** *On some number-theoretic conjectures of V. Arnold*, Japanese J. Math. **2** (2007), 297–302.
16. ***A.V. Zarelua,*** *On matrix analogs of Fermat's little theorem*, Math. Notes **79**(6) (2006), 783–796.

Artūras Dubickas

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24, Vilnius LT-03225
and
Vilnius University Institute of Mathematics and Informatics
Akademijos 4, Vilnius LT-08663
Lithuania
arturas.dubickas@mif.vu.lt