BÉZOUT'S IDENTITY FOR CYCLOTOMIC POLYNOMIALS OVER THE INTEGERS

ANDREA PREVITALI

Abstract. We determine the smallest positive integer lying in the ideal generated by cyclotomic polynomials over the integers and deduce that their evaluations at a given integer are almost always coprime.

1. Introduction

Let $\Phi_n(x)$ be the minimal polynomial over $\mathbb{Q}$ of a primitive n-th root of unity. Then Φ_n, the n-th cyclotomic polynomial, is monic and, as proved by Gauss, irreducible. In particular

$$\Phi_n(x)A + \Phi_m(x)A = A,$$

where $A = \mathbb{Q}[x]$, $n \neq m$. Set $B = \mathbb{Z}[x]$. Then

$$(\Phi_n(x)B + \Phi_m(x)B) \cap \mathbb{Z}$$

is an ideal in $\mathbb{Z}$, thus has shape $t\mathbb{Z}$, for some positive integer $t = t(n,m)$ depending on n, m. In this short note we prove that $t(n,m)$ equals 1 unless $n = r^i m$, r prime, in which case $t(n,m) = r$. We deduce information on $\gcd(\Phi_n(a), \Phi_m(a))$, for $a \in \mathbb{Z}$, showing that this value is almost always 1. This question was motivated by the analysis of cryptographical protocols involving finite fields lite XTR or LUC (see [FMP^2]).

2. Proof

By symmetry, we may assume that $n > m \geq 1$. We first reduce to the case where m divides n

Lemma 1. *$t(n,m) = 1$ except when $m|n$.*

Proof. Let $d = \gcd(n,m)$. Then $x^{n-m} - 1 = x^n - 1 - x^{n-m}(x^m - 1)$ proves that $x^{n-m} - 1 \in (x^n - 1)B + (x^m - 1)B$. Inducing on $n + m$ we obtain that

$$x^d - 1 \in (x^n - 1)B + (x^m - 1)B.$$

In particular $x^d - 1 = (x^n - 1)u(x) + (x^m - 1)v(x)$, $u, v \in \mathbb{Z}[x]$. If $d < m$, then $x^\ell - 1 \in (x^d - 1)\Phi_\ell(x)B$, $\ell = n, m$. So

$$1 \in \Phi_n(x)B + \Phi_m(x)B.$$

□

We now show that $t(nd, md) | t(n,m)$.

Date: June 8, 2011.

2000 *Mathematics Subject Classification.* 12A35, 12E10, 94A60.

Key words and phrases. Cyclotomic Polynomials, Gcd, Bézout's identity.

Lemma 2. *$t(nr, mr)|t(n, m)$ for any prime r.*

Proof. For $s, r \in \mathbb{N}$, r prime, let $\varepsilon(s, r)$ equal 1 if $s \not\equiv_r 0$, 0 otherwise. Then $\Phi_s(x^r) = \Phi_{sr}(x)\Phi_s(x)^{\varepsilon(s,r)}$ (see [LN, Exercise 2.57 (a),(b)]). Let $\Phi_n(x)u(x) + \Phi_m(x)v(x) = t(n, m)$, for $u, v \in \mathbb{Z}[x]$. Then substituting x with x^r, we obtain

$$\Phi_{nr}(x)\Phi_n(x)^{\varepsilon(s,r)}u(x^r) + \Phi_{mr}(x)\Phi_m(x)^{\varepsilon(m,r)}v(x^r) = t(n, m),$$

forcing $t(nr, mr)$ to divide $t(n, m)$. □

We deduce our claim $t(nd, md)|t(n, m)$ by induction on the number of prime divisors of d counting multiplicities. We are now ready to state the main result of this note.

Theorem 3. *$t(n, m) = 1$ except when $n = r^i m$, r prime, in which case $t(n, m) = r$.*

Proof. By Lemma 1, we may assume $n = md$. If d is not a prime power, we prove $t(n, m) = 1$ by induction on m. If $m = 1$, then $n = d$. Now $\Phi_d(x) = \Phi_1(x)u(x) + \Phi_d(1)$. The assumption on d forces $\Phi_d(1) = 1$, so $t(d, 1) = 1$. By Lemma 2 $t(n, m) = t(md, m)|t(d, 1) = 1$. We are left with the case $d = r^i$, r prime. Now $r = \Phi_d(1)$ and $= \Phi_1(1) = 0$. Let $\Phi_d(x)u(x) + \Phi_1(x)v(x) = t(d, 1)$, $u, v \in \mathbb{Z}[x]$. Then $ru(1) = t(d, 1)$, so $r|t(d, 1)$. On the other hand, $r = \Phi_d(x) - \Phi_1(x)q(x) \in \Phi_d(x)B + \Phi_1(x)B$. So $t(r^i, 1) = r$. Again Lemma 2 forces $t(mr^i, m) \in \{1, r\}$.

By Proposition 1 in [KO], $\Phi_n(\mu) \in r\mathbb{Z}[\mu]$, where μ is a primitive m-th root of unity. If $t(n, m) = 1$, then evaluating $\Phi_n(x)u(x) + \Phi_m(x)v(x) = 1$ at μ would yield $ra = 1$ for some $a \in \mathbb{Z}[\mu]$. Thus $\frac{1}{r}$ would be an algebraic integer, a contradiction. Therefore $t(r^i m, m) = r$. □

Corollary 4. *Let $d = \gcd(\Phi_n(a), \Phi_m(a))$, where $n, m \in \mathbb{N}$, $a \in \mathbb{Z}$. Then $d = 1$ or $n = r^i m$, r prime and $d = 1$ or $d = r$.*

Proof. Clearly d must divide $t(n, m)$, so the result is an immediate consequence of Theorem 3. □

With a more subtle analysis one can prove that $d = r$ if $n = r^i f$, $m = r^j f$, $i \geq j \geq 0$, a is coprime to r and f is the multiplicative order of a modulo r (see [FMP^2, Theorem 5]).

References

[FMP^2] P. Fragneto, A. Montanari, G. Pelosi and A. Previtali, "Ring Generators of Prime Order for Finite Fields", submitted to Journal of Cryptology.

[KO] R. P. Kurshan, A. M. Odlyzko, "Values of cyclotomic polynomials at roots of unity", *Math. Scand.* Vol. 49 (1981), no. 1, pp. 15–35

[LN] R. Lidl, H. Niederreiter, Finite Fields, Reading, MA: Addison-Wesley, 1983.

E-mail address: andrea.previtali@uninsubria.it

Webpage address: http://scienze-como.uninsubria.it/previtali/Research.html

Dipartimento di Fisica e Matematica, Università dell'Insubria, Via Valleggio, 11 Como–22100, Italy