Int. J. Open Problems Compt. Math., Vol. 13, No. 3, September 2020
ISSN 1998-6262; Copyright @ ICSRS Publication, 2020
www.i-csrs.org

Infinite classes of cyclotomic polynomials of order three and four

Seddik. ABDELALIM[1], MOSTAFA. EL GARN[1] and Jawad. SQUALLI[2]

[1]Department of Mathematics and Computer Science,
Faculty of Sciences Aïn Chock, University of Hassan II Casablanca, Morocco
Laboratory of Topology Algebra, Geometry and Discrete Mathematics
, B.P 5366 Maarif, Casablanca, 20100 Morocco
e-mail:seddikabd@hotmail.com
e-mail:elgarnmostafa@gmail.com

[2]Departemen of Mathematics and Computer Science. Ecole Normale Superieure of Casablanca
University of Hassan II Casablanca
e-mail:squjaw@gmail.com

Received 2 March; Accepted 12 July 2020

(Communicated by Tarek Sellami)

Abstract

The cyclotomic polynomials are used in many parts of mathematics. Several works have already treated them. Lenstra in [7]***, used the cyclotomic polynomials in discrete logarithm cryptosystems over Finite Fields. In*** 1883***, Migotti*** [8] ***showed that all coefficients in*** $\Phi_{p.q}$ ***the*** $p.q$***-cyclotomic polynomials are in*** $\{-1, 0, 1\}$ ***(where*** p ***and*** q ***are distincts primes numbers). Later, Lam*** [6]***, gave a quick and naturel construction of*** $\Phi_{p.q}$***. For*** $n > 2$ ***be an integer, let*** $A(n)$ ***denote the maximum of the absolute value of the coefficients of*** Φ_n***. Beiter*** [2]***, characterized the pairs*** p ***and*** q ***in*** $n = 3.p.q$ ***such that no coefficient of absolute value 2 can occur in*** Φ_n***. Beiter*** [3] ***conjectured that, for all*** $p < q < r$ ***primes numbers,*** $A(pqr) < (p + 1)/2$***. Kaplan*** [5]***, conjuctured that, if*** $A(n) > 1$ ***then for any prime*** p***,*** $A(p.n) > 1$ ***and gave an infinite family of cyclotomic polynomials of degre four.***

In this paper, we aim to characterize some infinite families of ternary cyclotomic polynomials, to characterized an infinite family of cyclotomic polynomials of degre four and using

some conjecture and theorems to give some others important results.

Keywords: cyclotomic polynomials, Euler's totient , degre, flat, Möbius.

1 Introduction

Using a theorem in [5], we can characterize any cyclotomic polynomials. This is acheived through a successful iterative process. Let $n > 2$ be a given integer, for which $A(n)$ is known. If we consider $m > n$ a prime number, such that $gcd(m, n) = 1$ then there exists n_m a unique positive integer number such that : $n_m < n$ and $n_m \equiv m\,(mod\, n)$. If we denote by $m_n > n$ the smallest prime number congruent to n_m then $A(m.n) = A(m_n.n)$. Nevertheless, this approach presents some technical difficulties, the congruence and the number m_n increases significatly. In the special case $n = p.q$, if we consider m a prime number, such that $p < q < m$ and $gcd(m, n) = 1$ then there exists a unique n_m positive integer number such that $n_m < \dfrac{n}{2}$ and $n_m \equiv \pm m\,(mod\, n)$. If we denote by m_n the smallest prime number congruent to n_m such that $m_n > q$ then $A(m.n) = A(m_n.n)$.
In the first part, we give some definitions and some importants results in the theory of cyclotomics polynomials. In the second part, we give characterization of somes infinite families of ternary cyclotomic polynomials. In the third part, we give a characterization of an infinite family of cyclotomic polynomials of degre four. And in the last part, using somes conjectures and theorems, we present some results for cyclotomic polynomials of higher degree.

2 Preliminary and notations

There are some many important results in this theory.

Definition 2.1. [1]
Let $n \in \mathbf{N}^*$. The nth cyclotomic polynomial is the monic polynomial whose roots are the primitive nth roots of unity and are all simple. It is defined by:

$$\Phi_n(x) = \prod_{k=1,(k,n)=1}^{k=n} (X - e^{2\pi i \frac{k}{n}}) = \sum_{k=0}^{k=\phi(n)} a_{n,i} x^k$$

- $(1)\,\Phi_n(x)$ *is a monic polynomial over integers.*
- $\Phi_n(x)$ *is an irreducible polynomial over* $\mathbf{Z}$.

- *where ϕ is the Euler totient function and $a_{n,\phi(n)} \neq 0$.*
- *(k, n) is the gcd of n and $k \in \{1, 2, ..., n\}$.*

We have the proof of (1), in the following proposition.

Proposition 2.2. [9]
The cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial over integers.

Definition 2.3. [5]
Let $n \in \mathbf{N}^*$. The largest absolute value of the coefficients of $\Phi_n(x)$ is denoted by $A(n) = max(\{|a_{n,k}| / 0 \leq k \leq \phi(n)\})$.
If $A(n) = 1$ we say that $\Phi_n(x)$ is flat.

Proposition 2.4. [2]
Let p and q be two distinct prime numbers. The nonzero coefficients of $\Phi_{pq}(x)$ alternate between 1 and -1.

Proposition 2.5. [9]
Let p and $p_1 < p_2 < ... < p_l$ is a sequence of prime numbers ($l \in \mathbf{N}^*$). Let $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_l^{\alpha_l}$, where α_1, α_2, ..., α_l and $N = p_1p_2...p_l$ are in $\mathbf{N}^*$. We have:

- *$x^{\phi(n)}\Phi_n(1/x) = \Phi_n(x)$ (That is, the coefficients of cyclotomic polynomials are symmetric).*
- *$2 \not| n \Longrightarrow \Phi_{2n}(x) = \Phi_n(-x)$.*
- *$p \not| n \Longrightarrow \Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.*
- *$p|n \Longrightarrow \Phi_{pn}(x) = \Phi_n(x^p)$, so $A(p.n) = A(n)$.*
- *$\Phi_n(x) = \Phi_N(x^{\frac{n}{N}})$*

Proposition 2.6. [9]*:*
Z *is the set of all coefficients of all cyclotomics polynomials.*

An important result is given by the following theorems :

Theorem 2.7. [2]*:*
If p and q are two distincts prime numbers, then Φ_{pq} flat.

Theorem 2.8. [5]*:*
Let p, q and r prime numbers such that $p < q < r$. If $r \equiv \pm 1 \mod pq$ then Φ_{pqr} is flat.

Remark 2.9. *:*
The condition $r \equiv \pm 1 \mod pq$ in the last theorem is not necessary. For examples:

- $23 \equiv 2 \mod 3.7$ *and* $\Phi_{3.7.23}$ *is flat.*
- $53 \equiv -2 \mod 5.11$ *and* $\Phi_{5.11.53}$ *is flat.*

Theorem 2.10. [5]*:*
Let p_1,p_2,...,p_r *be a prime numbers such that* $p_1 < p_2 < ... < p_r$ *and* $n = p_1.p_2...p_r$.
If s, t *are primes satisfying* $n < s < t$ *and* $s \equiv t \mod n$ *then* $A(ns) = A(nt)$.

Definition 2.11. [4]*:*
The Möbius function, μ*; is defined in* $\mathbf{N}^*$ *by :*

- $\mu(1) = 1$,
- $\mu(p_1.p_2...p_k) = (-1)^k$ *for distinct primes* p_1,p_2,...,p_k,
- $\mu(p_1^{r_1}.p_2^{r_2}..p_k^{r_k}) = 0$ *for distinct primes* p_1,p_2,...,p_k, *such that* $\max\{r_1, r_2, ..., r_k\} > 1$.

We have the following lemma :

Lemma 2.12. [9]*:*
let $n > 2$ *be an integer positif number. If* $\mu(n)$ *denotes the Möbius function, then* $\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$.

Lemma 2.13. [9]*:*
let $p > 2$ *be a prime number . We have* $\Phi_p = \sum_{i=0}^{i=p-1} X^i$.

Lemma 2.14. *:*
let $p > 2$ *be a prime number . We have :* $\Phi_p(1) = p$ *and* $\Phi_p(-1) = 1$

Proposition 2.15. *:*
Let $k > 1$ *be an integer and* $2 < p_1 < p_2 < ... < p_k$ *prime numbers. We have,* $\Phi_{p_1.p_2...p_k}(1) = \Phi_{p_1.p_2...p_k}(-1) = 1$.

Proof.
By recurrence on k.

- For $k = 2$, we know that $\Phi_{p_1.p_2}(X).\Phi_{p_1}(X) = \Phi_{p_1}(X^{p_2})$, then
  - $\Phi_{p_1.p_2}(1).\Phi_{p_1}(1) = \Phi_{p_1}(X^{p_2})(1)$. Then $\Phi_{p_1.p_2}(1).p_1 = p_1$ $\Longrightarrow \Phi_{p_1.p_2}(1) = 1$.
  - $\Phi_{p_1.p_2}(-1).\Phi_{p_1}(-1) = \Phi_{p_1}(X^{p_2})(-1)$. Then $\Phi_{p_1.p_2}(-1).1 = 1 \Longrightarrow \Phi_{p_1.p_2}(-1) = 1$.

- Let $k > 1$ be an integer and suppose that for all $2 < p_1 < p_2 < ... < p_k$ prime numbers, we have $\Phi_{p_1.p_2...p_k}(1) = \Phi_{p_1.p_2...p_k}(-1) = 1$.
  Let p_{k+1} be a prime number such that $\forall\, i \in \{1, 2, ..., k\} : p_{k+1} \neq p_i$. Without restriction, we can suppose that $2 < p_1 < p_2 < ... < p_k < p_{k+1}$.
  We know that $\Phi_{p_1.p_2...p_k.p_{k+1}}(X).\Phi_{p_1.p_2...p_k}(X) = \Phi_{p_1.p_2...p_k}(X^{p_{k+1}})$, then
  - $\Phi_{p_1.p_2...p_k.p_{k+1}}(1)\Phi_{p_1.p_2...p_k}(1) = \Phi_{p_1.p_2...p_k}(1) = 1$. Then, by recurrence hypothesis, $\Phi_{p_1.p_2...p_k.p_{k+1}}(1) = 1$.
  - $\Phi_{p_1.p_2...p_k.p_{k+1}}(-1)\Phi_{p_1.p_2...p_k}(-1) = \Phi_{p_1.p_2...p_k}(-1) = 1$. Then, by recurrence hypothesis, $\Phi_{p_1.p_2...p_k.p_{k+1}}(-1) = 1$.

□

Using this lemma, we can prove the following proposition :

Proposition 2.16. *:*
Let $k > 1$ be an integer number and $2 < p_1 < p_2 < ... < p_k$ be primes numbers. Set $m = p_1.p_2...p_k$ and $n = \phi(m)$.
If $\Phi_m = \sum_{i=1}^{i=n} a_i.X^i$, *then* $1 + a_{\frac{n}{2}} + 2(\sum_{i=1}^{i=\frac{n}{4}-1} a_{2i}) = 0$ *and* $\sum_{i=0}^{i=\frac{n}{4}-1} a_{2i+1} = 0$.

Proof.
According to the previous prop and the lemma, we have
$\Phi_m(1) = \sum_{i=0}^{i=n} a_i = 1$ and $\Phi_m(-1) = \sum_{i=0}^{i=n}(-1)^{-1}a_i = 1$, as desired. □

Remark 2.17. *:*

- *As a remark, we have $a_{\frac{n}{2}}$ is an odd number.*
- *If Φ_m flat then:*

$$a_{\frac{n}{2}} = -1 \ \ and \ \ \sum_{i=1}^{i=\frac{n}{4}-1} a_{2i} = 0$$

or

$$a_{\frac{n}{2}} = 1 \ and \ \sum_{i=1}^{i=\frac{n}{4}-1} a_{2i} = -1.$$

3 Characterization of infinite families of ternary cyclotomic polynomials

For ternary cyclotomic polynomials we have the following theorem :

Theorem 3.1. [5]*:*
Let p, q, r and s be prime numbers such that $p < q < r < s$.
If $s \equiv \pm r \mod pq$, then $A(p.q.s) = A(p.q.r)$.

As a consequence of this theorem, we have :

Corollary 3.2. *:*
Let p and q be prime numbers such that $p < q$.
For each prime r such that $r > q$ there exists a unique $i \in \{1, 2, ..., \frac{n-1}{2}\}$ such that $gcd(n, i) = 1$ and $i \equiv \pm r \mod n$, where $n = pq$.
If we denote by i_n the smallest prime number congruent to $\pm i$ modulo n such that $i_n > q$, then:

$$A(p.q.r) = A(p.q.i_n).$$

Proof.
We have $r \equiv \pm i \mod n$ and $i_n \equiv \pm i \mod n$ then $r \equiv \pm i_n \mod n$. Applying the previous theorem, we obtain $A(p.q.r) = A(pqi_n)$.
With this Corollary, we can caracterize any tennary cyclotomic polynomial. But the problem is to find the primes numbers i_n. We can do it with:
"$[\rangle$ for k from 1 to N do $i + kn$, type($i + kn$, prime) end do" and i_n is the first $i + kn$ for witch type($i + kn$, prime) is true. ($N = 1\, or\, 2\, or\, ...$) □

Let p, q and r be prime numbers such that $p < q < r$. As an applications, we have the following propositions:

Proposition 3.3. *:*
If r is a natural integer such that $r > 5$, then:

- $A(3.5.r) = 1$ *[i.e $\Phi_{3.5.r}$ flat] if and only if* $r \equiv \pm 1 \mod 15$.
- $A(3.5.r) = 2$ *if and only if* $r \equiv \pm 2\, or\, \pm 4\, or\, \pm 7 \mod 15$.

Proof.
It's easy to find that $1_{15} = 31$, $2_{15} = 17$, $4_{15} = 19$ and $7_{15} = 7$.
And by the previous lemma, we prove the proposition. □

Proposition 3.4. *:*
If r is a naturel integer such that $r > 7$, then:

- $A(3.7.r) = 1$ *[i.e $\Phi_{3.7.r}$ flat] if and only if* $r \equiv \pm 1\, or\, \pm 2\, or\, \pm 10 \mod 21$.
- $A(3.5.r) = 2$ *if and only if* $r \equiv \pm 4\, or\, \pm 5\, or\, \pm 8 \mod 21$.

Proof.
It's easy to find that $1_{21} = 43$, $2_{21} = 23$, $10_{21} = 11$, $4_{21} = 67$, $5_{21} = 47$ and $8_{21} = 29$.
And by the previous lemma, we prove the proposition. □

Remark 3.5. *:*
From the proposition, We can see that Φ_{pqr} flat without the condition $r \equiv \pm 1 \mod 21$. [$r \equiv \pm 2 \mod 21 \Longrightarrow \Phi_{pqr}$ flat].

Proposition 3.6. *:*
If r is a natural integer such that $r > 7$, then:

- $A(5.7.r) = 1$ *[i.e $\Phi_{5.7.r}$ flat] if and only if* $r \equiv \pm 1 \mod 35$.
- $A(5.7.r) = 2$ *if and only if* $r \equiv \pm 2$ *or* ± 3 *or* ± 4 *or* ± 6 *or* ± 8 *or* ± 9 *or* ± 12 *or* $\pm 13 \mod 35$.
- $A(5.7.r) = 3$ *if and only if* $r \equiv \pm 11$ *or* ± 16 *or* $\pm 17 \mod 35$.

Proof.
It's easy to find that $1_{35} = 71$, $2_{35} = 37$, $3_{35} = 73$, $4_{35} = 109$, $6_{35} = 41$, $8_{35} = 43$, $9_{35} = 79$, $11_{35} = 11$, $12_{35} = 47$, $13_{35} = 83$, $16_{35} = 191$ and $17_{35} = 17$.
And by the previous lemma, we prove the proposition. □

Proposition 3.7. *:*
If r is a natural integer such that $r > 11$, then:

- $A(5.11.r) = 1$ *[i.e $\Phi_{5.11.r}$ flat] if and only if* $r \equiv \pm 1$ *or* $\pm 2 \mod 55$.
- $A(5.11.r) = 2$ *if and only if r is others.*
- $A(5.11.r) = 3$ *if and only if* $r \equiv \pm 7$ *or* $\pm 17 \mod 55$.

Proof.
We have :
$1_{55} = 109$, $2_{55} = 53$, $3_{55} = 107$, $4_{55} = 59$, $6_{55} = 61$, $7_{55} = 103$, $8_{55} = 47$, $9_{55} = 101$, $12_{55} = 43$, $13_{55} = 13$, $14_{55} = 41$, $16_{55} = 71$, $17_{55} = 17$, $18_{55} = 37$, $19_{55} = 19$, $21_{55} = 89$, $23_{55} = 23$, $24_{55} = 31$, $26_{55} = 29$,$27_{55} = 83$.
And by the previous lemma, we prove the proposition. □

Proposition 3.8. *:*
If r is a natural integer such that $r > 13$, then:

- $A(5.13.r) = 1$ *[i.e $\Phi_{5.13.r}$ flat] if and only if* $r \equiv \pm 1 \mod 65$.

- $A(5.13.r) = 2$ *if and only if* r *is others.*

- $A(5.13.r) = 3$ *if and only if* $r \equiv \pm 7$ *or* ± 8 *or* ± 9 *or* ± 19 *or* ± 22 *or* ± 23 *or* $\pm 24 \mod 65$.

Proof.
We have :
$1_{65} = 131$, $2_{65} = 67$, $3_{65} = 127$, $4_{65} = 61$, $6_{65} = 59$, $7_{65} = 137$, $8_{65} = 73$, $9_{65} = 139$, $11_{65} = 271$, $12_{65} = 53$, $14_{65} = 79$, $16_{65} = 179$, $17_{65} = 17$, $18_{65} = 47$, $19_{65} = 19$, $21_{65} = 109$, $22_{65} = 43$, $23_{65} = 23$, $24_{65} = 41$, $27_{65} = 103$, $28_{65} = 37$, $29_{65} = 29$, $31_{65} = 31$, $32_{65} = 97$.
And by the previous lemma, we prove the proposition. □

Proposition 3.9. *:*
If r *is a natural integer such that* $r > 11$*, then:*

- $A(7.11.r) = 1$ *[i.e* $\Phi_{7.11.r}$ *flat] if and only if* $r \equiv \pm 1 \mod 77$.

- $A(7.11.r) = 2$ *if and only if* r *is others.*

- $A(7.11.r) = 3$ *if and only if* $r \equiv \pm 4$ *or* ± 5 *or* ± 9 *or* ± 16 *or* ± 17 *or* ± 19 *or* ± 25 *or* ± 27 *or* $\pm 30 \mod 77$.

- $A(7.11.r) = 4$ *if and only if* $r \equiv \pm 18$ *or* ± 20 *or* ± 24 *or* $\pm 37 \mod 77$.

Proof.
We have :
$1_{77} = 463$, $2_{77} = 79$, $3_{77} = 151$, $4_{77} = 73$, $5_{77} = 149$, $6_{77} = 71$, $8_{77} = 223$, $9_{77} = 163$, $10_{77} = 67$, $12_{77} = 89$, $13_{77} = 13$, $15_{77} = 139$, $16_{77} = 61$, $17_{77} = 17$, $18_{77} = 59$, $19_{77} = 19$, $20_{77} = 97$, $23_{77} = 23$, $24_{77} = 53$, $25_{77} = 179$, $26_{77} = 103$, $27_{77} = 127$, $29_{77} = 29$, $30_{77} = 47$, $31_{77} = 31$, $32_{77} = 109$, $34_{77} = 43$, $36_{77} = 41$, $37_{77} = 37$, $38_{77} = 193$.
And by the previous lemma, we prove the proposition. □

Proposition 3.10. *:*
If r *is a natural integer such that* $r > 13$*, then:*

- $A(7.13.r) = 1$ *[i.e* $\Phi_{7.13.r}$ *flat] if and only if* $r \equiv \pm 1 \mod 91$.

- $A(7.13.r) = 2$ *if and only if* r *is others.*

- $A(7.13.r) = 3$ *if and only if* $r \equiv \pm 9$ *or* ± 16 *or* ± 19 *or* ± 31 *or* ± 32 *or* $\pm 44 \mod 91$.

Proof.
We have :
$1_{91} = 181$, $2_{91} = 89$, $3_{91} = 179$, $4_{91} = 269$, $5_{91} = 359$, $6_{91} = 97$, $8_{91} = 83$, $9_{91} = 173$, $10_{91} = 101$, $11_{91} = 193$, $12_{91} = 103$, $15_{91} = 167$, $16_{91} = 107$, $17_{91} = 17$, $18_{91} = 73$, $19_{91} = 19$, $20_{91} = 71$, $22_{91} = 113$, $23_{91} = 23$, $24_{91} = 67$, $25_{91} = 157$, $27_{91} = 337$, $29_{91} = 29$, $30_{91} = 61$, $31_{91} = 31$, $32_{91} = 59$, $33_{91} = 149$, $34_{91} = 239$, $36_{91} = 127$, $37_{91} = 37$, $38_{91} = 53$, $40_{91} = 131$, $41_{91} = 41$, $43_{91} = 43$, $44_{91} = 47$, $45_{91} = 137$.
And by the previous lemma, we prove the proposition. □

4 Characterization of an infinite familie of cyclotomic polynomials of degree four

Lemma 4.1. *:*
Let p_1, p_2, ..., p_r and s be prime numbers such that $p_1 < p_2 < ... < p_r$, $n = p_1.p_2...p_r < s$.
There exists $i \in \{1, 2, ..., n-1\}$ such that $gcd(n, i) = 1$ and $s \equiv i \mod n$. If we denote by i_n the smallest prime number congruent to i modulo n and $i_n > n$, then:

$$A(n.r) = A(ni_n).$$

Proof.
We have $s \equiv i \mod n$ and $i_n \equiv i \mod n$ then $s \equiv i_n \mod n$. Applying the previous theorem (2.3), we obtain $A(n.r) = A(n.i_n)$.
With this lemma, we can characterize any cyclotomic polynomial. But the problem is to find the primes numbers i_n.We can do it with:
"⟩ for k from 1 to N do $i + kn$, type($i + kn$, prime) end do" and i_n is the first $i + kn$ for witch type($i + kn$, prime) is true. ($N = 1\, or\, 2\, or\, ...$) □

As an applications, we have the following proposition :

Proposition 4.2. *:*
If s is a natural integer such that $s > 105$ then

- $A(3.5.7.s) = 2$ *if and only if* $s \equiv \pm 1\, or\, \pm 4 \mod 105$.
- $A(3.5.7.s) = 3$ *if and only if* $s \equiv \pm 2\, or\, \pm 11\, or\, \pm 16\, or\, \pm 29\, or\, \pm 46\, or\, \pm 47\, or\, \pm 52 \mod 105$.
- $A(3.5.7.s) = 4$ *if and only if* $s \equiv \pm 8\, or\, \pm 13\, or\, \pm 19\, or\, \pm 22\, or\, \pm 23\, or\, \pm 31\, or\, \pm 32\, or\, \pm 41\, or\, \pm 43\, or\, \pm 44 \mod 105$.
- $A(3.5.7.s) = 5$ *if and only if* $s \equiv \pm 17\, or\, \pm 37\, or\, \pm 38 \mod 105$.

- $A(3.5.7.s) = 6$ *if and only if* $s \equiv \pm 26 \mod 105$.
- $A(3.5.7.s) = 7$ *if and only if* $s \equiv \pm 34 \mod 105$.

Proof.
For this theorem, we have the same result for $s \equiv i_n \mod n$ or $s \equiv -i_n \mod n$ It's easy to find that :
$1_{105} = 211$, $2_{105} = 107$, $4_{105} = 109$, $8_{105} = 113$, $11_{105} = 431$, $13_{105} = 223$, $16_{105} = 331$, $17_{105} = 227$, $19_{105} = 229$, $22_{105} = 127$, $23_{105} = 233$, $26_{105} = 131$, $29_{105} = 239$, $31_{105} = 241$, $32_{105} = 137$, $34_{105} = 139$, $37_{105} = 457$, $38_{105} = 353$, $41_{105} = 251$, $43_{105} = 463$, $44_{105} = 149$, $46_{105} = 151$, $47_{105} = 257$, $52_{105} = 157$. $53_{105} = 263$, $58_{105} = 163$, $59_{105} = 269$, $61_{105} = 271$, $62_{105} = 167$, $64_{105} = 379$, $67_{105} = 277$, $68_{105} = 173$, $71_{105} = 281$, $73_{105} = 283$, $74_{105} = 179$, $76_{105} = 181$, $79_{105} = 499$, $82_{105} = 397$, $83_{105} = 293$, $86_{105} = 191$, $88_{105} = 193$, $89_{105} = 509$, $92_{105} = 197$, $94_{105} = 199$, $97_{105} = 307$, $101_{105} = 311$, $103_{105} = 313$, $104_{105} = 419$.
And by the previous lemma, we prove the proposition. □

5 About some conjecture

Remark 5.1. *:*
In the paper [5]*, we have :*
Conjuncture:$[C_0]$
If $A(n) > 1$ *then for any prime* p, $A(pn) > 1$.

And a very important result is given in [1], by the following theorem.

Theorem 5.2. *:*
For any constant $c > 0$*, there exists* n *such that* $A(n) > n^c$.

If we use the conjecture $[C_0]$ and the last theorem, we have a new conjecture :

Conjuncture$[C_1]$:
There exists n_0 such that $A(n) > 1$ for each n a nonzero multiples of n_0.

Proof.
If we apply the theorem for $c = 1$ then there exists n_0 such that $A(n_0) > n_0 \Longrightarrow A(n_0) > 1$. And by the conjuncture $[C_0]$, $A(n_0) > 1 \Longrightarrow A(p.n_0) > 1$ for each p prime number. Then $A(n) > 1$ for each n a nonzero multiples of n_0. □

In [5], all flat cyclotomic polynomials Φ_n of order four with $n < 3.10^8$ are all of the form $n = p.q.r.s$ where $q \equiv -1 \mod p$, $r \equiv \pm 1 \mod p.q$ and $s \equiv \pm 1 \mod pqr$. This suspects that all flat cyclotomic polynomials of order four are of this form. If we conjecture this remark then:

Conjuncture:$[C_2]$
Let p, q, r and s be prime numbers such that $2 < p < q < r < s$.
If $\Phi_{p.q.r.s}$ is a flat cyclotomic polynomials then $q \equiv -1 \mod p$, $r \equiv \pm 1 \mod p.q$ and $s \equiv \pm 1 \mod pqr$.

As a direct consequence of this conjecture, and using the conjecture $[C_1]$, we have the following result :

Conjuncture: $[C_3]$
Let p, q, r, s and t be prime numbers such that $2 < p < q < r < s < t$.
If $\Phi_{p.q.r.s.t}$ is a flat cyclotomic polynomials then $q \equiv -1 \mod p$, $r \equiv -1 \mod p.q$, $s \equiv \pm 1 \mod pqr$ and $t \equiv \pm 1 \mod pqrs$.

Proof.
Let p, q, r, s and t be prime numbers such that $2 < p < q < r < s < t$.
By $[C_0]$ and $[C_2]$:

- $\Phi_{p.q.r.s}$ is a flat cyclotomic polynomials then $q \equiv -1 \mod p$, $r \equiv \pm 1 \mod p.q$ and $s \equiv \pm 1 \mod p.q.r$.
- $\Phi_{p.q.r.t}$ is a flat cyclotomic polynomials then $q \equiv -1 \mod p$, $r \equiv \pm 1 \mod p.q$ and $t \equiv \pm 1 \mod p.q.r$.
- $\Phi_{p.q.s.t}$ is a flat cyclotomic polynomials then $q \equiv -1 \mod p$, $s \equiv \pm 1 \mod p.q$ and $t \equiv \pm 1 \mod p.q.t$.
- $\Phi_{p.r.s.t}$ is a flat cyclotomic polynomials then $r \equiv -1 \mod p$, $s \equiv \pm 1 \mod p.r$ and $t \equiv \pm 1 \mod p.r.s$.
- $\Phi_{q.r.s.t}$ is a flat cyclotomic polynomials then $r \equiv -1 \mod q$, $s \equiv \pm 1 \mod q.r$ and $t \equiv \pm 1 \mod q.r.s$.

We have $r \equiv -1 \mod p$ then, $r \equiv 1 \mod p.q \Longrightarrow \exists (k, k') \in \mathbf{Z}$:
$r = -1 + kp = 1 + k'pq \Longrightarrow 2|p$, which it is false. So, $r \equiv -1 \mod p.q$.
We have $s \equiv \pm 1 \mod p.q.r$.
We have $t \equiv \pm 1 \mod p.q.r$ and $t \equiv \pm 1 \mod p.r.s$, then :

- if $t \equiv 1 \mod p.q.r \Longrightarrow t \equiv 1 \mod p.r.s \Longrightarrow t \equiv 1 \mod p.q.r.s$.
- if $t \equiv -1 \mod p.q.r \Longrightarrow t \equiv -1 \mod p.r.s \Longrightarrow t \equiv -1 \mod p.q.r.s$.

□

Remark 5.3. *:*
We can give a very important remark about flat cyclotomic polynomials $\Phi_{p_1.p_2...p_n}$ *of big order* $n \in \mathbf{N}$ *where* $2 < p_1 < p_2 < ... < p_n$ *are prime numbers. From the conjecture* $[C_1]$*, for all prime number* p*,* $A(p.m) > 1$ *once we have* $A(m) > 1$ *for an integer numbers.*
Suppose that $\Phi_{p_1.p_2...p_n}$ *flat, i.e* $A(p_1.p_2...p_n) = 1$*. Let* σ *be an increasing permutation over* $\{1, 2, ..., n\}$*. Applying the contraposition of the conjuncture* $[C1]$*, for every* $r \in \{1, 2, ..., n\}$ *such that* $r \geq 4$ $A(p_{\sigma(1)}.p_{\sigma(2)}...p_{\sigma(r)}) = 1$*.*
Therefore, we have a reason to believe the following result :

Conjuncture: $[C_4]$
If the cyclotomic polynomials $\Phi_{p_1.p_2...p_n}$ *is flat then :*

- $\forall i \in \{2, 3, ..., n-2\}$: $p_i \equiv -1 \mod \prod_{j=1}^{j=i-1} p_j$
- $p_{n-1} \equiv \pm 1 \mod \prod_{j=1}^{j=n-2} p_j$.
- $p_n \equiv \pm 1 \mod \prod_{j=1}^{j=n-1} p_j$.

Proof.
By recurrence on $n \geq 4$ and using the same idea in the proof of conjuncture $[C_3]$. □

6 Open Problem

Remark 6.1. *:*

- *Many other conditions are necessary to have* $\Phi_{p_1.p_2...p_n}$ *flat. This remark suggests that for a sufficiently large degree there will probably be no cyclotomic polynomial that are flat.*
- *If we suppose that the conjuncture* $[C_0]$ *is true and there are no cyclotomic polynomial of order five which are flat, then there are no flat cyclotomic polynomial of order bigger than five.*

ACKNOWLEDGEMENTS. In the end,we would to thank the referee for making time to analyse our paper and we will be at your disposition for any further information.

References

[1] Arnold, A., and Monagan, M., Calculating cyclotomic polynomials. Mathematics of Computation, 80(276), 2359-2379 (2011).

[2] Beiter, M., Magnitude of the coefficients of the cyclotomic polynomials $\Phi_{p.q.r}$, Amer. Math. Monthly, 75, 370-372 (1968).

[3] Beiter, M., Magnitude of the coefficients of the cyclotomic polynomials $\Phi_{p.q.r}$, II, Duke Math., J. 38 MR 43:6152, 591-594, (1971).

[4] Ge, Y., Elementary properties of cyclotomic polynomials. Mathematical Reflections, 2. (2008).

[5] Kaplan, N., Flat cyclotomic polynomials of order four and higher. Integers, 10(3), 357-363, (2010).

[6] Lam, T. Y., and Leung, K. H., On the cyclotomic polynomial $\Phi_{p.q}(X)$, The American Mathematical Monthly, 103(7), pp. 562-564. (1996).

[7] Lenstra, A. K., Cyclotomic polynomial construction of discrete logarithm cryptosystems over finite fields, (Vol. 59 Fasc. 3), U.S. Patent No. 6,665,405. Washington, DC: U.S. Patent and Trademark Office (2003).

[8] Migotti, A., Aur Theorie der Kreisteilungsgleichung, Z. B. der Math.-Naturwiss, Classe der Kaiserlichen Akademie der Wissenschaften, Wien, 87, 7-14, (1883).

[9] Thangadurai, R., On the coefficients of cyclotomic polynomials. Cyclotomic fields and related topics (Pune, 1999), 311-322, (2000).