NNTDM 6 (2000) 4, 125-128

NOTE ON CYCLOTOMIC POLYNOMIALS AND LEGENDRE SYMBOL

Mladen V. Vassilev - Missana
5, V. Hugo Str., Sofia-1124, BULGARIA

In memory of my father

In the paper the following denotations are used: $\varphi(m)$ - for Euler's function; $(\frac{A}{p})$ - for Legendre symbol; (p,n) - for the greatest common divisor of p and n; $d|m$ - for the fact that d is a divisor of m; μ - for Möbius function; $\Phi_m(x)$ - for the $m-$th cyclotomic polynomial. Here we remind that

$$\Phi_m(x) = \prod_{d|m}(x^d - 1)^{\mu(\frac{m}{d})},$$

where d runs all divisors of m.

Let n and α be arbitrary positive integers and $k = n.p^\alpha$, where r is a fixed odd prime, such that $(p,n) = 1$.

Let

$$f(n;p) := \sum_{t=0}^{p-1}(\frac{\Phi_k(t)}{p}). \tag{1}$$

The following theorem is the mail result of the present paper.

THEOREM: The representation

$$f(n;p) = p - \varphi(n) \tag{2}$$

holds, when

$$p \equiv 1(\text{mod } n). \tag{3}$$

Otherwise

$$f(n;p) = p. \tag{4}$$

Let q be fixed prime number, which may satisfy everyone of the congruences:

$$q \equiv 3(\text{mod } 8); \tag{5}$$

$$q \equiv 7(\text{mod } 8); \tag{6}$$

and

$$g(n;q) := \sum_{t=0}^{q-1}(\frac{t^{2n}-1}{q}). \tag{7}$$

Then the second result in the paper is the following

Proposition: The identity

$$g(n;q) = -1 \tag{8}$$

is valid.

To prove the theorem we need three lemmas.

LEMMA 1: The congruences:

$$\Phi_n(t) \equiv 0(\text{mod } p); \tag{9}$$

$$\Phi_k(t) \equiv 0(\text{mod } p) \tag{10}$$

are fulfiled, or are not fulfiled simultaneously.

The proof of this lemma is a direct corollary from Theorem 94 and Theorem 95 [1] and we omit it.

LEMMA 2: The necessary and sufficient condition for every nonnegative integer t to have

$$\Phi_k(t) \equiv 1(\text{mod } p) \tag{11}$$

is (3) to be not fulfiled.

Proof: Fermat's Little Theorem immediatelly yields

$$\Phi_n(t^{p^\alpha}) \equiv \Phi_n(t^{p^{\alpha-1}})(\text{mod } p) \tag{12}$$

for every nonnegative integer t. Then (12) and the well known representation

$$\Phi_k(t) = \frac{\Phi_n(t^{p^\alpha})}{\Phi_n(t^{p^{\alpha-1}})} \tag{13}$$

yield

$$\Phi_k(t).\Phi_n(t) \equiv \Phi_n(t)(\text{mod } p). \tag{14}$$

First, let (3) be fulfiled. Then for every nonnegative integer t (9) is impossible, because of Theorem 94 [1]. Divide the both hand-sides of (14) by $\Phi_n(t)$ we obtain that (11) is fulfiled for every nonnegative integer t.

Second, let (11) be fulfiled for every nonnegative integer t. Then for every nonnegative integer t (10) is impossible and as a result of Lemma 1 (9) is impossible, too. Hence, (3) is impossible, because of Theorem 95 [1]. The lemma is proved.

LEMMA 3: If (3) holds, then the necessary and sufficient condition for some nonnegative integer t to have (11) is for the same t (9) to be not fulfilled.

Proof: Let (3) holds.

First, let us suppose that for some t (9) is impossible. Then (14) yields (11) immediatelly, because we may divide the both hand-sides of (14) by $\Phi_n(t) \neq 0$.

Second, let (11) be fulfiled for some t. Then, moreover we have that (10) is impossible, and as a result (9) is impossible, too, because of Lemma 1. The lemma is proved.

Proof of the Theorem: We consided the following two cases:

a_1) p satisfies (3);

a_2) p does not satisfy (3).

Let a_1 holds. In this case the both congruences (9) and (10) are solviable simultaneously, i.e., for one and the same values of t (because of Lemma 1).

If t runs the set $\{0,1,...,p-1\}$, then the number of these t, which satisfy (9) equals to $\varphi(n)$ (because of Theorem 94 [1]). The same number is for the solutions of (10) (because of Lemma 1). So, the number of these $t \in \{0,1,...,p-1\}$, which satisfy the condition

$$(\frac{\Phi_k(t)}{p}) \neq 0 \tag{15}$$

(i.e., for wnich (10) is impossible) is just equal to $p-\varphi(n)$. But (10) is impossible iff (11) holds (because of Lemma 1 and Lemma 3). Therefore, when $t \in \{0,1,...,p-1\}$ and (15) holds, we obtain

$$(\frac{\Phi_k(t)}{p}) = 1 \tag{16}$$

for $p-\varphi(n)$ values of t in the right hand-side of (1). This proves (2).

Let a_2 holds. In this case we have (11) for every $t \in \{0,1,...,p-1\}$ (because of Lemma 2) and as a result (16). Therefore,

$$f(n;p) = \sum_{t=0}^{p-1} 1 = p \tag{17}$$

(see (1)), which proves (4). The Theorem is proved.

Proof of the Proposition: Let q satisfying (5) or (6), be a fixed prime. Then we have

$$(\frac{-1}{q}) = -1. \tag{18}$$

If $t \in \{1,2,...,q-1\}$, then we denote by t^{-1} this number of the set $\{1,2,...,q-1\}$, which satisfies the congruence

$$t.t^{-1} \equiv (\text{mod } q).$$

Now, using (18) and some well known properties of Legendre symbol, we have:

$$g(n;q) = (\frac{-1}{q}) + \sum_{t=1}^{q-1}(\frac{t^{2n}-1}{q}) = -1 + \sum_{t=1}^{q-1}(\frac{(-1)(1-t^{2n})}{q})$$

$$= -1 + (\frac{-1}{q}) + \sum_{t=1}^{q-1}(\frac{1-t^{2n}}{q}) = -1 + \sum_{t=1}^{q-1}(\frac{t^{2n}}{q})(\frac{(t^{-1})^{2n}-1)}{q})$$

$$= -1 - \sum_{t=1}^{q-1}(\frac{(t^{-1})^{2n}-1)}{q}). \tag{19}$$

When t runs the set $\{1,2,...,q-1\}$, t^{-1} runs the same set. Therefore

$$\sum_{t=1}^{q-1}(\frac{t^{2n}-1}{q}) = \sum_{t=1}^{q-1}(\frac{(t^{-1})^{2n}-1)}{q}). \tag{20}$$

From (19) and (20) we obtain

$$g(n;q) = -1 - \sum_{t=1}^{q-1}(\frac{t^{2n}-1}{q}) = -1 + (\frac{-1}{q}) - \sum_{t=0}^{q-1}(\frac{t^{2n}-1}{q}) = -2 - g(n;q).$$

Hence

$$g(n;q) = -1$$

and the Proposition is proved.

APPENDIX:

Further $ord_p x$ denotes the maximal nonnegative integer γ with the property: p^γ divides x.

THEOREM 4 [1]: 1. The necessary and sufficient condition for the solviability of (9) is (3).

2. If (3) holds, then the solutions of (9) are the numbers, which belong to exponent n with respect to modulus p. The number of the nonnegative solutions of (9), which are $< p$, is just equal to $\varphi(n)$.

3. If x is a solution of (9), then

$$ord_p \Phi_n(x) = ord_p(x^n - 1).$$

THEOREM 5 [1]: 1. The necessary and sufficient condition for the solviability of (10) is (3).

2. If (3) holds, then the solutions of (10) are the numbers, which belong to exponent n with respect to modulus p. The number of the nonnegative solutions of (10), which are $< p$, is just equal to $\varphi(n)$.

3. If x is a solution of (10), then

$$ord_p \Phi_k(x) = 1,$$

if $k > 2$.

Reference:

[1] T. Nagell, Introduction to Number Theory. John Wiley & Sons, New York, 1950.

ERATA:

Formula (10) from M. Vassilev's paper "On a formula related to the $n-$th partial sum of the harmonic series" in NNTDM, Vol. 6 (2000), No. 2, 64-68:

$$\frac{1}{p}.(\ln(m+1+\frac{1}{p}).\ln(m+\frac{1}{p})) < \frac{1}{m.p+1}. \qquad (10)$$

must be read as:

$$\frac{1}{p}.(\ln(m+1+\frac{1}{p}) - \ln(m+\frac{1}{p})) < \frac{1}{m.p+1}. \qquad (10)$$