ON THE PRIME FACTORS OF $\Phi_P(M)$

Luis H. Gallardo
Univ. Brest, Laboratoire de Mathématiques de Bretagne Atlantique, Brest, France
Luis.Gallardo@univ-brest.fr

Received: 8/14/20, Revised: 2/16/21, Accepted: 6/15/21, Published: 7/9/21

Abstract

We prove the non-existence of Mersenne primes M on $\mathbb{F}_2[x]$ such that all prime divisors of the cyclotomic polynomial $\Phi_p(M)$ are also Mersenne in a few new cases.

1. Introduction

The following problem has attracted some interest (see [1, 2, 3, 5, 6, 9, 10, 17, 18, 19, 21, 22, 23]). Let $f(x)$ be an irreducible polynomial over a finite field $\mathbb{F}_q$, let $g(x)$ be a polynomial over the same field. What can be said about the composite polynomial $F(x) = f(g(x))$? The second polynomial $g(x)$ has been chosen as a power of x, as a *linearized* polynomial, e.g., $g(x) = x^{p^r} - x$ with p the characteristic of $\mathbb{F}_q$, or as a quotient A/B of two other polynomials. In particular, recently Panario et al. [21] worked on the case $g(x) = 1/(cx+1)$, with nonzero $c \in \mathbb{F}_q$, in order to obtain conditions such that $f(x)$ irreducible implies $F(x)$ irreducible. More generally, Lidl and Niederreiter [20], and Swan [25], give the most classic results about polynomials over finite fields.

However, to our knowledge, one has not yet considered the case in which $g(x) \neq f(x)$ is itself an irreducible polynomial of some specific type. Our choice in the present paper is to take for $g(x)$ a binary polynomial (reason: we might think of the ring $\mathbb{F}_2[x]$ as the *closest* analogue of the integers $\mathbb{Z}$), and for $f(x)$ the cyclotomic polynomial $\Phi_p(x) = (x^p+1)/(x+1) \in \mathbb{F}_2[x]$, with p a prime number.

A few words on the notation used throughout the paper. If $A \in \mathbb{F}_2[x]$ is irreducible then we say that A is *prime*, and a *Mersenne* polynomial $M \in \mathbb{F}_2[x]$ (an analogue of a Mersenne number) is a polynomial such that $M+1$ is a product of powers of x and powers of $x+1$. We say that $M+1$ *splits*. When a Mersenne polynomial M is irreducible, we say that M is a *Mersenne prime*. A binary polynomial A is *complete* [7] if all coefficients of A are equal to 1. A binary polynomial B is *odd* if $B(0) = B(1) = 1$, otherwise B is *even*. More standard notations are the following: $\omega(P)$ is the number of pairwise distinct prime factors of $P \in \mathbb{F}_q[x]$, q

even, $o_p(b)$ is the multiplicative order of a nonzero element b of the finite field $\mathbb{F}_p$, $o(\alpha)$ is the multiplicative order of an element α in some appropriate extension of $\mathbb{F}_2$, $ord(H)$ is the minimal positive integer m such that the binary polynomial H divides the binomial $x^m - 1$. Finally, $\overline{\mathbb{F}_2}$ is a fixed algebraic closure of $\mathbb{F}_2$.

It is easy to check that $\Phi_p(x)$ is square-free, but very little is known about its *prime* (i.e., irreducible) factors [20, Theorem 2.47]. The special equation that we consider, in which we take $f(x) = \Phi_p(x)$ and $g(x) = M$, with M a Mersenne prime, is the following:

$$\Phi_p(M) = M_1 \cdots M_s. \tag{1}$$

Equation (1) is related to the search of perfect polynomials over $\mathbb{F}_2[x]$ (*binary perfect* polynomials); see [7, 8, 11, 12, 13, 14, 15, 16]. We recall that a binary perfect polynomial A is defined by the equality $\sigma(A) = A$, where $\sigma(A) = \sum_{D|A} D \in \mathbb{F}_2[x]$ is the sum of all divisors of A, including 1 and A. For coprime binary polynomials X, Y one has, as over the integers $\mathbb{Z}$, $\sigma(XY) = \sigma(X)\sigma(Y)$. The σ function is more natural, but also more complex, than the usual sum of divisor function $\sigma_1(A) = \sum_{D|A} 2^{\deg(A)}$. For instance, some divisors D of A can sum up to 0, while a sum over D of $2^{\deg D}$ is always positive. It is easy to check that for any non-negative integer n, the polynomial $T(n) = (x(x+1))^{2^n-1}$ is (*trivial*) perfect. There are only 11 non-trivial (known) binary perfect polynomials. We call them *sporadic perfect*. The exact link with our Equation (1) is that if Equation (1) holds then we are able to characterize 9 of these 11 sporadic perfect, as the only even binary perfect polynomials, all of whose odd prime divisors (i.e., prime divisors coprime with $x(x+1)$) are Mersenne primes [14, 15, 16].

The binary perfect polynomials are a polynomial analogue of the multiperfect numbers over $\mathbb{Z}$ since for $A \in \mathbb{F}_2[x]$, $\sigma(A)/A \in \mathbb{F}_2[x]$ is equivalent to $A = \sigma(A)$. Canaday [7], the first Ph. D. student of Leonard Carlitz, started the work on binary perfect polynomials in 1941.

Equation (1) seems very difficult to resolve. The contribution of the present paper consists in giving a simple generalization of some properties of the only known example, Equation (2), as well as describing a simple necessary condition.

The following theorem is our main result.

Theorem 1. *Let p be an odd prime number and let s be a positive integer. Let $M := x^a(x+1)^b+1 \in \mathbb{F}_2[x]$ be a Mersenne prime, and $T := M+1$. For $j = 1, \ldots, s$, let $M_j := x^{a_j}(x+1)^{b_j} + 1$ be a Mersenne prime. Let $k_j := \deg(M_j)/o_p(2)$, let K_0 be the number of k's such that $a_k = 1$, and let K_1 be the number of ℓ's such that $b_\ell = 1$. Consider Equation (1), i.e.,*

$$1 + M + \cdots + M^{p-1} = M_1 \cdots M_s.$$

Consider also the statements:

(a) *K_0 is even when (without loss of generality) a is even and b is odd; K_1 is even when $b > 1$, and $K_1 \equiv (p-1)/2 \pmod 2$ when $b = 1$. If both a and b are odd, then $K_0 \equiv 0 \pmod 2$ when $a > 1$, while $K_0 \equiv (p-1)/2 \pmod 2$ when $a = 1$. Moreover, $a = 1$ implies that $K_1 \equiv 0 \pmod 2$ when $b > 1$, and implies that $K_1 \equiv (p-1)/2 \pmod 2$ when $b = 1$.*

(b) *For some j the Euclidean (Long Division) division of M by M_j gives a remainder equal to x, and 4 does not divide the degrees of all M_j.*

(c) *The degree of M is a prime number q, and, for some positive integers c, s, $k_1, \ldots, k_s$ are in an arithmetic progression $k_1 := c, k_2 := c+1, \ldots, k_s := c+s-1$.*

(d) *One has $k_1 \leq k_2$ and $k_2 = \cdots = k_s = d$, where d is bounded from above by a constant d_0, (in particular this holds in Equation (2)), and $\deg(M)$ is big enough relative to p.*

(e) *One has $p \neq 7$, and $\Phi_p(x) \mid \Phi_p(M)$ (say, $M_1 = \Phi_p(x)$), all the other M_js have the same degree $d > p-1$. Moreover, $\deg(M) - 1$ is a prime number, and $\deg(M)$ is big enough relative to p.*

We assume in each of the statements (b), (c), (d), *and* (e), *that* 2 *is a primitive root of unity modulo p.*

We have that Equation (1) *implies* (a). *Moreover, Equation* (1) *is impossible when any of the statements* (b), (c), (d), *or* (e), *hold; besides in the only two known cases in which Equation* (1) *holds (switch x and $x+1$ to obtain the other case):* $p = 3$, $s = 2$, $M = x(x+1)^2+1 = x^3+x+1$, $M_1 = x^2+x+1$, *and* $M_2 = x^4+x^3+1$; *namely,*

$$1 + M + M^2 = (x(x+1)+1)(x^3(x+1)+1). \tag{2}$$

Remark 1. The statements (b), (c), (d), and (e) in Theorem 1 hold in the known case of Equation (2). Thus, we may think that if there exist some exception to the Conjecture (i.e., if Equation (1) holds, besides the known case), then these (possible) exceptions must be of another (unknown) nature.

We have a new result for a special case, in which p is an arbitrary odd prime, but the Mersenne prime M is also a trinomial. We consider the case in which $p = 7$. The case $p = 7$ is exceptional. In fact, for $p = 3$, and for any Mersenne prime $p > 7$, Equation (1) is impossible [16]. However, for $p = 7$ (and for any Mersenne prime M) we do not know if Equation (1) holds.

The following theorem is our second result.

Theorem 2. *Let $M := x^{c+1} + x^c + 1 \in \mathbb{F}_2[x]$ be prime. Let p be an odd prime, and $r = \omega(\Phi_p(M))$. Then:*

(a) *If $c > 2$ is even, then r is odd.*

(b) *If $c > 1$ is odd, then r is even.*

(c) *Assume that $p = 7$. For c from 1 to 12540, Equation (1) has no solutions.*

(d) *If Equation (1) holds with $p = 7$, and $c > 1$ is odd, then $r \geq 6$.*

2. Tools

Although well known, the following lemma is very useful, since we do not know the exact form of the prime factors of $\Phi_p(x)$ in $\mathbb{F}_2[x]$ (we know, however, how many they are, and which degrees they have [20, Theorem 2.47]).

Lemma 1. *Let p be an odd prime number. The cyclotomic polynomial $\Phi_p(x) \in \mathbb{F}_2[x]$ is irreducible if and only if 2 is a primitive element of the finite field $\mathbb{F}_p$.*

It is not yet proved, that there exist an infinity of such prime numbers.

Lemma 2. (Satz 5 in [22]). *Let $f(x) \in \mathbb{F}_2[x]$ be a prime polynomial of degree k, and let $g(x) \in \mathbb{F}_2[x]$. Let $F(x) = f(g(x))$. Then the degree of every prime divisor of $F(x)$ is divisible by k.*

The following lemma follows from Lemma 2.

Lemma 3. *Let p be a prime number such that $o_p(2) = p - 1$. Let $g(x) \in \mathbb{F}_2[x]$ be such that*

$$\Phi_p(g(x)) = m_1(x) \cdots m_s(x) \tag{3}$$

for s pairwise distinct prime polynomials in $\mathbb{F}_2[x]$. Then for $j = 1, \ldots, s$, we have that $p - 1$ divides $\deg(m_j(x))$, and

$$\deg(g(x)) = k_1 + \cdots + k_s, \tag{4}$$

where $k_j := \deg(m_j(x))/(p - 1)$.

Lemma 4. (Theorem 1.4 in [15] and Theorem 1.4 in [16]). *With the notations of Theorem 1, assume that (1) holds. Then:*

(a) *One has $s > 2$.*

(b) *One has $\deg(M) > 4$.*

It is also useful to know necessary conditions on $c \geq 1$, provided that $x^{c+1}+x^c+1$ is prime.

Lemma 5. *Let c be a positive integer, and $M(x,c) := x^{c+1} + x^c + 1 \in \mathbb{F}_2[x]$. Assume that $M(x,c)$ is prime. Then:*

(a) *If c is odd, then $c \in \{3,5\} \pmod 8$.*

(b) *If c is even, then: either $c = 2$ or $c \in \{0,6\} \pmod 8$.*

(c) *If for some non-negative integer m, $c = 2^m - 1$ (respectively, $c = 2^m + 1$) then $c \in \{1,3\}$ (respectively, $c \in \{2,3,5\}$).*

Proof. Part (a) follows from [15, Corollary 3.3 (i)] with $a = c$ and $b = 1$. Part (b) follows from [15, Corollary 3.3 (ii)] with $a = 1$ and $b = c$. Part (c) follows from [15, Lemma 4.2] by switching x and $x + 1$. □

Lemma 6. (Theorems 3.3 and 3.4 in [26]). *Let c be a positive integer, $M(x,c) := x^{c+1} + x^c + 1 \in \mathbb{F}_2[x]$, and let $D(x) := x^{d_1}(x+1)^{d_2} + 1$ be a Mersenne prime. Let $\alpha \in \overline{\mathbb{F}_2}$ be a zero of $D(x)$, $L(c,\alpha) := x^{c+1} + x^c + \alpha^c(\alpha+1) \in K = \mathbb{F}_2[\alpha]$, and $r = \omega(L(c,\alpha))$.*

(1) *Assume that $c > 2$. Then $r \equiv c+1 \pmod 2$ if and only if one of the following assertions holds.*

  (a) *We have that $[K\colon \mathbb{F}_2]$ is even.*

  (b) *We have $c \in \{0,6,7\} \pmod 8$.*

  (c) *We have $c \equiv 1 \pmod 8$.*

(2) *Assume that $c > 2$. Then r is even if and only if one of the following assertions holds.*

  (a) *We have $c \equiv 7 \pmod 8$.*

  (b) *We have $c \in \{1,3,5\} \pmod 8$ and $[K\colon \mathbb{F}_2]$ is even.*

  (c) *We have $c \in \{2,4\} \pmod 8$ and $[K\colon \mathbb{F}_2]$ is odd.*

  (d) *We have $c \equiv 1 \pmod 8$.*

The following lemma generalizes a theorem of Capelli.

Lemma 7. (Lemma 2.1 in [4] and Lemma 3.6 in [24]). *Let $f(x), g(x) \in \mathbb{F}_2[x]$ with $f(x)$ prime. Let $\beta \in \overline{\mathbb{F}_2}$ be a zero of $f(x)$. Put $K = \mathbb{F}_2[\beta]$. Assume that $g(x) - \beta$ is square-free in $K[x]$ and that*

$$g(x) - \beta = F_1 \cdots F_r, \tag{5}$$

with $F_1, \ldots, F_r$ irreducible in $K[x]$. Then

$$f(g(x)) = N(F_1) \cdots N(F_r), \tag{6}$$

with $N(F_1), \ldots, N(F_r)$ irreducible in $\mathbb{F}_2[x]$, where N is the norm from K to $\mathbb{F}_2$.

3. Proof of Theorem 1

In order to prove (a) we consider first the case in which ab is even, so that we can assume that, say, a is even and b is odd. Put $M_k := x^{a_k}(x+1)^{b_k}+1$. Observe that the derivative of a Mersenne polynomial $P := x^c(x+1)^d+1$ is equal to

$$P' = x^{c-1}(x+1)^{d-1}((c+d)x+c). \tag{7}$$

Write Equation (1) as

$$M^p + 1 = (M+1)M_1 \cdots M_s. \tag{8}$$

By differentiation of Equation (8) relative to x, we got

$$pM^{p-1}M' = M'M_1 \cdots M_s + (M+1)(\sum_k M_1 \cdots M_k' \cdots M_s). \tag{9}$$

Since a is even and b is odd we obtain

$$(M+1)/M' = x(x+1)/((a+b)x+a) = x(x+1)/x = x+1. \tag{10}$$

Divide both sides of Equation (9) by M' to get

$$pM^{p-1} = M_1 \cdots M_s + (x+1)(\sum_k M_1 \cdots M_k' \cdots M_s). \tag{11}$$

Replace $x = 0$ in both sides of Equation (11) to get

$$1 = 1 + K_0 \in \mathbb{F}_2.$$

Thus, K_0 is even in this case. Consider now Equation (8) written as Equation (1). By differentiation of Equation (1) relative to x, we obtain

$$(1 + M + \cdots + M^{(p-3)/2})^2 M' = \sum_k M_1 \cdots M_k' \cdots M_s. \tag{12}$$

But Equation (7) implies that, independently of the value of a, one has $M'(1) = 0$ if $b > 1$, and $M'(1) = 1$ if $b = 1$. Putting $x = 1$ into both sides of Equation (12) we get $0 = K_1 \in \mathbb{F}_2$, when $b > 1$, and $(p-1)/2 = K_1 \in \mathbb{F}_2$, when $b = 1$. Take now, both a and b odd. Observe that Equation (7) implies that, independently of the value of b, $M'(0) = 0$ if $a > 1$, and $M'(0) = 1$ if $a = 1$. Putting $x = 0$ into both sides of Equation (12) we get $0 = K_0 \in \mathbb{F}_2$, when $a > 1$, and $(p-1)/2 = K_0 \in \mathbb{F}_2$, when $a = 1$. This proves (a).

We prove (b): Assume that for some $Q \in \mathbb{F}_2[x]$ one has, say,

$$M = QM_1 + x. \tag{13}$$

Let $\gamma \in \overline{\mathbb{F}_2}$ be a zero of M_1. It follows from Equation (1) that $M(\gamma)^p = 1$. Thus, Equation (13) implies that

$$\gamma^p = 1. \tag{14}$$

In other words

$$o(\gamma) = p. \tag{15}$$

Put $r := ord(M_1)$. Since M_1 is prime, r is equal to the multiplicative order of γ, i.e., $r = p$. By definition of r, one has for a certain $K \in \mathbb{F}_2[x]$

$$x^p - 1 = M_1 K. \tag{16}$$

But 2 is a primitive root modulo p, thus Lemma 1 implies that the cyclotomic polynomial $\Phi_p(x) \in \mathbb{F}_2[x]$ is prime. Since the odd polynomial M_1 is also prime, Equation (16) implies that

$$M_1 = \Phi_p(x). \tag{17}$$

But, $\Phi_p(x)$ is also complete. Therefore, it follows from Equation (17), and from [7, Theorem 8], that we have $M_1 \in \{\Phi_3(x), \Phi_5(x), \Phi_7(x)\}$. In other words

$$M_1 \in \{x^2 + x + 1, x^4 + x^3 + x^2 + x + 1, (x^3 + x + 1)(x^3 + x^2 + 1)\}. \tag{18}$$

Thus, either $p = 3$ and $M_1 = x^2 + x + 1$, or $p = 5$ and $M_1 = x^4 + x^3 + x^2 + x + 1$. The case $p = 3$ is impossible by [16]. The case $p = 5$ is also impossible, since in this case Lemma 3 implies that 4 divides $\deg(M_j)$ for all $j = 1, \ldots, 4$. This proves (b).

We prove (c): By taking degrees in both sides of Equation (1) one has

$$(p-1)q = \sum_{j=1}^{s} \deg(M_j). \tag{19}$$

By Lemma 3, there exist some integers $k_j \geq 1$ with $j = 1, \ldots, s$, such that $\deg(M_j) = (p-1)k_j$. So, Equation (19) reads

$$q = \sum_{j=1}^{s} k_j. \tag{20}$$

Using now our hypothesis, one has for each such j, $k_j = c + j - 1$, and we can write Equation (20) as

$$q = \frac{s}{2} \cdot (2c + s - 1), \tag{21}$$

when s is even, and as

$$q = s \cdot \left(c + \frac{s-1}{2} \right), \tag{22}$$

otherwise. Assume that s is even. Since q is prime, it follows from Equation (21) that one of the following cases (u),(v) is true:

(u) We have $q = s/2$; so that $2 = 2c + s$. But both c and s are ≥ 1, thus $2 \geq 3$. This contradiction proves the result in this case.

(v) We have $s/2 = 1$, so that $s = 2$. This is impossible, since we know (by Lemma 4) that $s \geq 3$.

Assume now that s is odd. As before, using Equation (22), we have two cases to consider.

(w) We have $q = s$; so that $3 = 2c + s$. But both c and s are ≥ 1, thus $s = c = 1$. This contradicts again the fact that $s \geq 3$.

(z) We have $q = c + (s-1)/2$ so that $s = 1$. This is impossible. Thus, (c) is proved.

We prove (d): Observe that the total number of Mersenne polynomials of given degree n equals $n - 1$. Thus, crudely, the number $N(n)$ of prime Mersenne polynomials of degree n is bounded above by $n - 1$. Let N_p be the number of distinct Mersenne prime divisors of $\Phi_p(M)$. From our hypothesis, it follows that $N_p = N(k_1(p-1)) + N(d(p-1))$. Hence,

$$N_p \leq (d + k_1)(p - 1). \tag{23}$$

We claim that the following lower bound $\ell(M)$ for $\deg(M)$:

$$\ell(M) := 2d_0^2(p-1) + d_0, \tag{24}$$

implies a contradiction, so that the result follows from Equation (24).

Proof of the claim: assume that

$$\deg(M) \geq \ell(M). \tag{25}$$

Remember, that by Lemma 3 we have $\deg(M) = k_1 + (s-1)d$. Thus, using that $d_0 \geq d \geq k_1$, Equation (25) implies

$$k_1 + (s-1)d \geq k_1 + d^2(p-1) + dk_1(p-1) > k_1 + d^2(p-1) + dk_1(p-1) - d. \tag{26}$$

But Equation (26) says that

$$s > (d + k_1)(p - 1). \tag{27}$$

Therefore, Equation (27) together with Equation (23), imply that

$$\omega(\Phi_p(M)) = s > N_p. \tag{28}$$

Clearly, Equation (28) is impossible, thereby proving the claim and the result.

We prove (e): Besides Equation (1), one has $\Phi_p(M) = \Phi_p(x)A(x)$ for some $A(x) \in \mathbb{F}_2[x]$. Thus, $\Phi_p(x)$ is a complete polynomial that is a product of Mersenne prime polynomials. Thus, [7, Theorem 8] implies that

$$\Phi_p(x) \in \{x^2 + x + 1, x^4 + x^3 + x^2 + x + 1, x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\}. \quad (29)$$

In other words, we have $\Phi_p(x) \in \{\Phi_3(x), \Phi_5(x), \Phi_7(x)\}$ so that

$$p \in \{3, 5, 7\}. \quad (30)$$

But, by Lemma 1, $\Phi_p(x)$ is prime since $o_p(2) = p - 1$. Therefore, $p \in \{3, 5\}$ since

$$\Phi_7(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$$

is not prime. The case $p = 3$ does not happen by [16] (non-trivial proof). Thus, we are left with the (open, and possibly non-trivial) case in which $p = 5$. We can take, say, $M_1 := \Phi_5(x)$. From Equation (1) and our conditions we get

$$4 \deg(M) = 4 + (s - 1)d. \quad (31)$$

Put $\ell := \deg(M) - 1$. By Lemma 3 one has $d = 4k_j$ for all $j = 2, \ldots, s$. Thus, Equation (31) implies that

$$\ell = (s - 1)k_j \quad (32)$$

for all $j = 2, \ldots, s$. The case $s = 2$ was done in [15, Theorem 1.4], and ℓ is a prime number. Therefore, Equation (32) implies that

$$k_1 = 1, k_2 = 1, \ldots, k_s = 1. \quad (33)$$

The result follows then by part (d). This finishes the proof of the theorem.

4. Proof of Theorem 2

We prove part (a). Put $M_j = x^{d_1}(x + 1)^{d_2} + 1$, and let $\alpha \in \overline{\mathbb{F}_2}$ be a zero of M_j. Consider $D = M_j$ and $M(x, c) = M$ in Lemma 6. Observe that $L(c, \alpha) = M - M(\alpha)$. By Lemma 7 one has $r = s$ (this also follows from [21, Corollary 2.12]). More precisely, since $L(c, \alpha)$ is square-free, one has

$$L(c, \alpha) = \prod_{i=1}^{r} \psi_i(x)$$

for some prime polynomials $\psi(x) \in \mathbb{F}_2(\alpha)[x]$, while

$$\Phi_p(M) = \prod_{i=1}^{r} N(\psi_i(x)) = M_1 \cdots M_s,$$

where N is the norm from $\mathbb{F}_2(\alpha)$ to $\mathbb{F}_2$. Thus, Lemma 6 implies that r is odd, since by Lemma 5 (b) we have $c \in \{0, 6\} \pmod 8$. This proves part (a).

In order to prove part (b), observe that Lemma 5 implies that $c \in \{3, 5\} \pmod 8$, since c is odd. Proceeding as before, we have now by Lemma 6 (2)(b) that r is even.

Part (c) follows from a straightforward computation in gp-PARI, that took about ten days for $c = 1, \ldots 10000$, and fifteen days, 4 hours, for $c = 10001, \ldots, 12540$.

In order to prove part (d), observe that by part (b), $s = r = \omega(\Phi_7(M))$ is even. Thus Lemma 4 implies that $s \geq 4$. Assume that $s = 4$. By [16, Corollary 3.15] one has that $\Phi_7(x)$ divides $\Phi_7(M)$. Thus, we can take, say, $M_1 := x^3 + x + 1$, and $M_2 := x^3 + x^2 + 1$. Put $M_3 := x^{a_3}(x+1)^{b_3} + 1$, and $M_4 := x^{a_4}(x+1)^{b_4} + 1$. Put also $R := M^3 + M + 1$ and $S := M^3 + M^2 + 1$. One has $\Phi_7(M) = RS$. Hence, R cannot be prime, since R prime implies, by Equation (1), that R is a Mersenne prime. Thus, $R + 1 = M(M+1)^2$ splits. This is impossible, since M is odd. The same argument proves that S is not prime. Therefore, both $\omega(R)$ and $\omega(S)$ are equal to 2. We now discuss the possible cases.

(i) Both M_1 and M_2 divides R. This implies that $R = M_1 M_2$, thus $\deg(M) = 2$. This contradicts the fact (see Lemma 4) that $\deg(M) > 4$ when Equation (1) holds.

(ii) Both M_1 and M_2 divide S. Same proof as that in case (a).

(iii) One has that M_1 divides R, and M_2 divides S. We can assume that $R = M_1 M_3$, so that $S = M_2 M_4$. Put $d_1 := R - M_1 M_3$ and $d_2 := S - M_2 M_4$. One has

$$d_1 = x^{a_3+3}(x+1)^{b_3} + x^{a_3+1}(x+1)^{b_3} + x^{a_3}(x+1)^{b_3} + P_1, \tag{34}$$

where

$$P_1 := x^{3a}(x+1)^{3b} + x^3 + x, \tag{35}$$

and

$$d_2 = x^{a_4+3}(x+1)^{b_4} + x^{a_4+2}(x+1)^{b_4} + x^{a_4}(x+1)^{b_4} + P_2, \tag{36}$$

where

$$P_2 := x^{3a}(x+1)^{3b} + x^a(x+1)^b + x^3 + x^2. \tag{37}$$

Comparing coefficients in x, it follows from Equations (34), (35), (36), and Equation (37), that $a_3 = 1$ and $a_4 = 1$. By substituting these values into the four equations, we get also that $b_3 = 1$ and $b_4 = 1$. Thus, we obtain that $M_3 = M_4 = x^2 + x + 1$. This is impossible, since $\gcd(R, S) = 1$. This proves the result.

(iv) One has that M_1 divides S, and M_2 divides R. The proof is analogue to the proof of part (c), just a little more involved, since we must now compare the coefficients in x, x^2 and x^3, in order to obtain a contradiction. We find in one

of the two possible cases, that in d_1 the coefficient of x^4 is equal to 1, while in the other case, the coefficient of x^2 in d_1 is equal to 1.

Acknowledgement. We thank the referee and the editor for detailed comments and suggestions. We thank also Reinhardt Euler for help with the English.

References

[1] S. Agou, Irréducibilité des polynômes $f(x^{p^r} - ax)$ sur un corps fini $\mathbb{F}_{p^s}$, *J. Reine Angew. Math.* **292** (1977), 191-195.

[2] S. Agou, Irréducibilité des polynômes $f(x^{p^{2r}} - ax^{p^r} - bx)$ sur un corps fini $\mathbb{F}_{p^s}$, *J. Number Theory* **10** (1978), 64-69, **11** (1979), 20.

[3] O. Ahmadi and M.-S. Khosro, A note on the stability of trinomials over finite fields, *Finite Fields Appl.* **63** (2020), 101649, 13 pp.

[4] I. Anca, N. Bonciocat and M. Cipu, Irreducibility criteria for compositions and multiplicative convolutions of polynomials with integer coefficients, *An. Ştiinţ. Univ. "Ovidius" Constanţa, Ser. Mat.* **22(1)** (2014), 73-84.

[5] F.-E. Brochero-Martínez and L. Reis, Factoring polynomials of the form $f(x^n) \in \mathbb{F}_q[x]$, *Finite Fields Appl.* **49** (2018), 166-179.

[6] M. C. R. Butler, The irreducible factors of $f(x^m)$ over a finite field, *J. London Math. Soc.* **30** (1955), 480-482.

[7] E. F. Canaday, The sum of the divisors of a polynomial, *Duke Math. J.* **8** (1941), 721-737.

[8] U. C. Cengiz, P. Pollack and E. Treviño, Counting perfect polynomials, *Finite Fields Appl.* **47** (2017), 242-255.

[9] S. D. Cohen, On irreducible polynomials of certain types in finite fields, *Proc. Camb. Philos. Soc.* **66** (1969), 335-344.

[10] S. D. Cohen, The irreducibility of compositions of linear polynomials over a finite field, *Compositio Math.* **47** (1982), 149-152.

[11] L. H. Gallardo and O. Rahavandrainy, Odd perfect polynomials over $\mathbb{F}_2$, *J. Théor. Nombres Bordx.* **19(1)** (2007), 165-174.

[12] L. H. Gallardo and O. Rahavandrainy, There is no odd perfect polynomial over $\mathbb{F}_2$ with four prime factors, *Port. Math.* **66(2)** (2009), 131-145.

[13] L. H. Gallardo and O. Rahavandrainy, On even (unitary) perfect polynomials over $\mathbb{F}_2$, *Finite Fields Appl.* **18(5)** (2012), 920-932.

[14] L. H. Gallardo and O. Rahavandrainy, Characterization of sporadic perfect polynomials over $\mathbb{F}_2$, *Funct. Approx. Comment. Math.* **55(1)** (2016), 7-21.

[15] L. H. Gallardo and O. Rahavandrainy, On Mersenne polynomials over $\mathbb{F}_2$, *Finite Fields Appl.* **59** (2019), 284-296.

[16] L. H. Gallardo and O. Rahavandrainy, On (unitary) perfect polynomials over $\mathbb{F}_2$ with only Mersenne primes as odd divisors, arXiv:1908.00106 [math.NT].

[17] M. K. Kyuregyan, Recurrent methods for constructing irreducible polynomials over $GF(2)$, *Finite Fields Appl.* **8(1)** (2002), 52-68.

[18] M. K. Kyuregyan and G. H. Kyuregyan, Irreducible compositions of polynomials over finite fields, *Des. Codes Cryptogr.* **61(3)** (2011), 301-314.

[19] A. F. Long, Factorization of irreducible polynomials over a finite field with the substitution $x^{q^r} - x$ for x, *Acta Arith.* **25** (1973), 65-80.

[20] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications,* 20, Cambridge: Cambridge University Press, 1996.

[21] D. Panario, L. Reis and Q. Wang, Construction of irreducible polynomials through rational transformations, *J. Pure Appl. Algebra* **224(5)** (2020), 106241, 17 pp.

[22] E. L. Petterson, Über die Irreduzibilität ganzzahliger Polynome nach einem Primzahlmodul, *J. Reine Angew. Math.* **175** (1936), 209-220.

[23] L. Reis, Factorization of a class of composed polynomials, *Des. Codes Cryptogr.* **87(7)** (2019), 1657-1671.

[24] L. Reis, On the factorization of iterated polynomials, arXiv:1810.07715 [math.NT].

[25] R. G. Swan, Factorization of polynomials over finite fields, *Pacific J. Math.* **12** (1962), 1099-1106.

[26] U. Vishne, Factorization of trinomials over Galois fields of characteristic 2, *Finite Fields Appl.* **3(4)** (1997), 370-377.