C. R. Acad. Sci. Paris, Ser. I 355 (2017) 370–377

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory

Lehmer's totient problem over $\mathbb{F}_q[x]$ ☆

Le problème de Lehmer pour la fonction d'Euler sur $\mathbf{F}_q[x]$

Qingzhong Ji, Hourong Qin

Department of Mathematics, Nanjing University, Nanjing 210093, PR China

ARTICLE INFO

Article history:
Received 14 December 2016
Accepted 13 March 2017
Available online 21 March 2017

Presented by the Editorial Board

ABSTRACT

In this paper, we consider the function field analogue of the Lehmer's totient problem. Let $p(x) \in \mathbb{F}_q[x]$ and $\varphi(q, p(x))$ be the Euler's totient function of $p(x)$ over $\mathbb{F}_q[x]$, where $\mathbb{F}_q$ is a finite field with q elements. We prove that $\varphi(q, p(x)) | (q^{\deg(p(x))} - 1)$ if and only if (i) $p(x)$ is irreducible; or (ii) $q = 3$, $p(x)$ is the product of any 2 non-associate irreducibles of degree 1; or (iii) $q = 2$, $p(x)$ is the product of all irreducibles of degree 1, all irreducibles of degree 1 and 2, and the product of any 3 irreducibles one each of degree 1, 2 and 3.

RÉSUMÉ

Dans cette Note, nous considérons l'analogue dans les corps de fonctions du problème de Lehmer sur la fonction d'Euler. Soit $p(x) \in \mathbf{F}_q[x]$ et $\varphi(q, p(x))$ la fonction d'Euler de $p(x)$ sur $\mathbf{F}_q[x]$, où $\mathbf{F}_q$ désigne un corps fini à q éléments. Nous montrons que $\varphi(q, p(x)) \mid (q^{\deg(p(x))} - 1)$ si et seulement si (i) $p(x)$ est irréductible, ou (ii) $q = 3$ et $p(x)$ est le produit de deux polynômes irréductibles non associés de degré 1, ou (iii) $q = 2$ et $p(x)$ est le produit de tous les polynômes irréductibles de degré 1, ou le produit de tous les polynômes irréductibles de degrés 1 et 2, ou le produit de trois polynômes irréductibles de degrés 1, 2 et 3, respectivement.

1. Introduction

Throughout this paper, let $\mathbb{Q}$, $\mathbb{Z}$ and $\mathbb{N}$ denote the field of rational numbers, the ring of rational integers and the set of nonnegative integers, respectively. Let $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$. As usual, let ord_p denote the normalized p-adic valuation of $\mathbb{Q}_p$.

Lehmer's totient problem. Let φ be the Euler's totient function. In [6], Lehmer discussed the equation

$$k\varphi(n) = n - 1, \tag{1}$$

☆ Supported by NSFC (Nos. 11471154, 11271177, 11571163).
E-mail addresses: qingzhji@nju.edu.cn (Q. Ji), hrqin@nju.edu.cn (H. Qin).

http://dx.doi.org/10.1016/j.crma.2017.03.007
1631-073X/

where k is an integer. In his pioneering paper [6], Lehmer showed that if n is a solution to (1), then n is a prime or the product of seven or more distinct primes. One is tempted to believe that an integer n is a prime if and only if $\varphi(n)$ divides $n-1$. This problem has not been solved to this day. But some progress has been made in this direction. In the literature, some authors call these composite numbers n satisfying equation (1) the Lehmer numbers. Lehmer's totient problem is to determine the set of Lehmer numbers. To the best of our knowledge, the current best result is due to Richard G.E. Pinch (see [9]), which states that the number of prime factors of a Lehmer number n must be at least 15 and that there is no Lehmer number less than 10^{30}. For further results on this topic, we refer the reader to [1,2,4,5,7,10].

J. Schettler [11] generalizes the divisibility condition $\varphi(n)|(n-1)$, constructs a reasonable notion of Lehmer numbers and Carmichael numbers in a PID and gets some interesting results. Let R be a PID with the property: $R/(r)$ is finite whenever $0 \neq r \in R$. Denote the sets of units, primes and (non-zero) zero divisors, in R, by $U(R)$, $P(R)$ and $Z(R)$, respectively; additionally, define

$$L_R := \{r \in R \setminus (\{0\} \cup U(R) \cup P(R)) : \ |U(R/(r))| \,|\, |Z(R/(r))|\}. \tag{2}$$

Note that when $R = \mathbb{Z}$, $L_{\mathbb{Z}}$ is the set of Lehmer numbers. An element of L_R is also called a Lehmer number of R. Let $\mathbb{F}_q$ be a finite field with q elements. Then $\mathbb{F}_q[x]$ is a PID. Schettler obtains some properties of elements of $L_{\mathbb{F}_q[x]}$ as follows.

Proposition 1.1 *([11], Theorems 5.1, 5.2, 5.3).*

(1) *Suppose* $f(x) \in L_{\mathbb{F}_q[x]}$, $p(x) \in P(\mathbb{F}_q[x])$ *and* $p(x)|f(x)$. *Then* $\deg(p(x))|\deg(f(x))$.
(2) *Suppose* $f(x) \in L_{\mathbb{F}_q[x]}$. *Then* $f(x)$ *has at least* $[\log_2(q+1)]$ *distinct prime factors.*
(3) *There exists a PID* R *such that* $L_R \neq \emptyset$ (*e.g.,* $f(x) = x(x+1) \in L_{\mathbb{F}_2[x]}$).

Our work is inspired by the above proposition; in this paper, our goal is to determine the set $L_{\mathbb{F}_q[x]}$.

Euler's totient function over $\mathbb{F}_q[x]$. Let $f(x) \in \mathbb{F}_q[x]$ with $m = \deg(f(x)) \geq 1$. Put

$$\Phi(f(x)) = \{g(x) \in \mathbb{F}_q[x] \mid \deg(g(x)) \leq m-1, (f(x), g(x)) = 1\}.$$

The Euler's totient function $\varphi(q, f(x))$ of $f(x)$ is defined as follows:

$$\varphi(q, f(x)) = |\Phi(f(x))|.$$

If $f(x) \in \mathbb{F}_q[x]$ is irreducible, then $\varphi(q, f(x)) = q^{\deg(f(x))} - 1$. It is easy to see that the functions $\varphi(q, f(x))$ and $\varphi(n)$ have the following similar properties.

Proposition 1.2. *Let* $f(x) = p_1(x)^{r_1} \cdots p_k(x)^{r_k} \in \mathbb{F}_q[x]$ *of degree* $n \geq 1$, *where* $p_1(x), \ldots, p_k(x) \in P(\mathbb{F}_q[x])$ *are non-associate,* $\deg(p_i(x)) = n_i$ *and* $r_i \geq 1$, $1 \leq i \leq k$. *Then we have*

(1) $\varphi(q, f(x)) = q^n \prod_{i=1}^{k} (1 - \frac{1}{q^{n_i}})$;
(2) *If* $g(x) \in \mathbb{F}_q[x]$ *and* $(f(x), g(x)) = 1$, *then* $g(x)^{\varphi(q, f(x))} \equiv 1 \pmod{f(x)}$;
(3) *If* $\varphi(q, f(x))|(q^n - 1)$, *then* $r_i = 1$, *for all* $1 \leq i \leq k$.

Hence it is natural to consider the following Lehmer's totient problem over $\mathbb{F}_q[x]$.

Determine $f(x) \in \mathbb{F}_q[x]$ such that $\varphi(q, f(x))|(q^{\deg(f(x))} - 1)$.

Set

$$\mathcal{L}_{\mathbb{F}_q} = \{f(x) \in \mathbb{F}_q[x] \setminus \{0\} \mid \deg(f(x)) \geq 1, \ \varphi(q, f(x))|(q^{\deg(f(x))} - 1)\}.$$

By the definition (2), it is easy to see that

$$L_{\mathbb{F}_q[x]} = \{f(x) \in \mathbb{F}_q[x] \setminus \{0\} \mid f(x) \text{ is reducible}, \ \varphi(q, f(x))|(q^{\deg(f(x))} - 1)\}.$$

Hence $\mathcal{L}_{\mathbb{F}_q} = P(\mathbb{F}_q[x]) \cup L_{\mathbb{F}_q[x]}$.

For $q = 2, 3$, Lv Hengfei [8] gave some polynomials $f(x) \in L_{\mathbb{F}_q[x]}$ as follows:

(1) $q = 2$, $f(x) = x(x+1)(x^2+x+1)$, then $\varphi(2, f(x)) = 3$, hence $\varphi(2, f(x))|(2^4 - 1)$.
(2) $q = 3$, $f(x) = x(x+1)$, then $\varphi(3, f(x)) = 4$, hence $\varphi(3, f(x))|(3^2 - 1)$.

In this paper, we give the necessary and sufficient conditions for $f(x) \in L_{\mathbb{F}_q[x]}$ as follows.

Main theorem.

(1) *Assume* $q \geq 4$. *Then* $L_{\mathbb{F}_q[x]} = \emptyset$.
(2) *Assume* $q = 3$. *Then* $L_{\mathbb{F}_3[x]}$ *consists of the products of any* 2 *non-associate irreducibles of degree* 1, *i.e.*

$$L_{\mathbb{F}_3[x]} = \{ax(x+1), ax(x-1), a(x+1)(x-1) \in \mathbb{F}_3[x], a = 1, 2\}.$$

(3) *Assume* $q = 2$. *Then* $L_{\mathbb{F}_2[x]}$ *consists of the products of all irreducibles of degree 1, the products of all irreducibles of degree 1 and 2, and the products of any 3 irreducibles one each of degree 1, 2, and 3, i.e.*

$$\begin{aligned} L_{\mathbb{F}_2[x]} = \{&x(x+1), x(x+1)(x^2+x+1), x(x^2+x+1)(x^3+x+1),\\ &(x+1)(x^2+x+1)(x^3+x+1), x(x^2+x+1)(x^3+x^2+1),\\ &(x+1)(x^2+x+1)(x^3+x^2+1) \in \mathbb{F}_2[x]\}. \end{aligned}$$

The proof is essentially to give the necessary and sufficient conditions for $\varphi(q, f(x))|(q^{\deg(f(x))} - 1)$, which will be divided into two cases, $q \geq 3$ and $q = 2$.

2. Properties of cyclotomic polynomials

Let $n \in \mathbb{N}^*$ and ζ_n be a primitive n-th root of unity. The polynomial

$$\Phi_n(x) = \prod_{(j,n)=1} (x - \zeta_n^j)$$

is called the n-th cyclotomic polynomial. It is well known that $\Phi_n(x)$ is an irreducible polynomial of degree $\varphi(n)$ in $\mathbb{Z}[x]$ and

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{3}$$

Note that the polynomial factorization in (3) is complete. But it does not follow that the factorization

$$a^n - 1 = \prod_{d|n} \Phi_d(a), \quad a \in \mathbb{Z} \tag{4}$$

is complete, since the integer $\Phi_d(a)$ may not be prime.

Definition 2.1. Suppose $a > b > 0$ are coprime integers. A prime divisor p of $a^n - b^n$, $n \geq 2$, is called primitive if $p \nmid a^k - b^k$, for any $k < n$. Otherwise, it is called algebraic.

It is well known that the following Bang–Zsigmondy's Theorem provides the existence of a primitive prime factor.

Bang–Zsigmondy's Theorem *([14]). Suppose* $a > b > 0$ *are coprime integers. Then for any natural number* $n > 1$, *there is a primitive prime divisor* p *of* $a^n - b^n$ *with the following exceptions:*

$$a = 2,\ b = 1,\ \textit{and}\ n = 6;\ \textit{or}$$
$$a + b\ \textit{is a power of two, and}\ n = 2.$$

It is clear that for any n, and $d|n$, that any prime p dividing $\phi_d(a)$ will be an algebraic divisor of (4), since p must divide $a^d - 1$ as $\phi_d(a)$ does. On the other hand, any primitive factor of $a^n - 1$ will have to divide $\Phi_n(a)$. It is not true, however, that every prime factor of $\Phi_n(a)$ is primitive.

Lemma 2.2 *([3], III C1, p. lxviii). Let* p *be a prime and* $m \in \mathbb{N}^*$ *with* $(p, m) = 1$. *Suppose* $v \in \mathbb{N}^*$ *and* $a \in \mathbb{Z}$. *Then* $p|\Phi_{mp^v}(a)$ *if and only if* $p|\Phi_m(a)$. *Furthermore,*

(1) *if* $p|\Phi_m(a)$ *and* $mp^v > 2$, *then* $\operatorname{ord}_p(\Phi_{mp^v}(a)) = 1$;
(2) *if* $p|\Phi_m(a)$ *and* $mp^v = 2$, *i.e.,* $p = 2, m = v = 1$, *then*

$$\operatorname{ord}_2(\Phi_2(a)) = \operatorname{ord}_2(a+1) \geq 1.$$

Lemma 2.3. *Let p be a prime and $n \in \mathbb{N}^*$. Suppose $n = p^v m$ with $v = \mathrm{ord}_p(n)$. Then $p|\Phi_n(a)$ for some $a \in \mathbb{Z}$ if and only if $m|(p-1)$.*

Proof. It is obvious from Lemma 2.2 and ([13], Lemmas 2.9, 2.10). □

Corollary 2.4. *Let p be a prime and $a \in \mathbb{Z}$, $v \in \mathbb{N}$. Then $p|\Phi_{p^v}(a)$ if and only if $p|(a-1)$.*

Corollary 2.5. *Let $m > n$ be positive integers. For any $a \in \mathbb{Z}$, we obtain that $(\Phi_n(a), \Phi_m(a)) = 1$ or $(\Phi_n(a), \Phi_m(a))$ is a prime. Furthermore, if $(\Phi_n(a), \Phi_m(a)) = p$ is a prime, then $m = p^v n$ for some $v \geq 1$.*

Lemma 2.6. *Let $a, m \in \mathbb{N}^*$ and $a \geq 2$. Then $|\Phi_m(a)| = 1$ if and only if $m = 1, a = 2$.*

Proof. By the formula $\Phi_m(a) = \prod_{(j,m)=1} (a - \zeta_m^j)$, we know that $|a - \zeta_m^j| > 1$ for all $a \geq 2$ and $m \geq 2$, hence $|\Phi_m(a)| > 1$. On the other hand, $\Phi_1(x) = x - 1$. Therefore $\Phi_m(a) = 1$ if and only if $m = 1, a = 2$. □

To end this section, we recall an estimate for $\Phi_n(a)$.

Lemma 2.7 *([12], Theorem 5). For any integers $n \geq 2$ and $a \geq 2$, we have*

$$\frac{1}{2} a^{\varphi(n)} \leq \Phi_n(a) \leq 2 \cdot a^{\varphi(n)}.$$

3. Main results

Let the notation be the same as in §1 and §2.

Proposition 3.1. *Let $a, n \in \mathbb{N}^*$ and $a \geq 3$, $n \geq 2$. Assume $s \geq 2$ and $e_1, e_2, \ldots, e_s \in \mathbb{N}^*$ with $\sum_{i=1}^{s} e_i = n$. Then $\prod_{i=1}^{s} (a^{e_i} - 1) | (a^n - 1)$ if and only if*

(1) $a = 3, n = s = 2, e_1 = e_2 = 1$, *or*
(2) $a = 3, n = s = 4, e_1 = e_2 = e_3 = e_4 = 1$.

Proof. The sufficiency is trivial. It is sufficient to show the necessity. Suppose $\prod_{i=1}^{s} (a^{e_i} - 1) | (a^n - 1)$. First, we have

$$\frac{x^n - 1}{\prod_{i=1}^{s} (x^{e_i} - 1)} = \frac{\prod_{d \in T} \Phi_d(x)}{\prod_{d' \in T'} \Phi_{d'}(x)} = \frac{\prod_{d \in T} \Phi_d(x)}{(x-1)^{s-1} \cdot \prod_{d' \in T''} \Phi_{d'}(x)} = \frac{P(x)}{Q(x)}, \tag{5}$$

where $T = \{d > 1 \mid d | n,\ d \nmid e_i,\ 1 \leq i \leq s\}$, $P(x) = \prod_{d \in T} \Phi_d(x)$ and $Q(x) = \prod_{d' \in T'} \Phi_{d'}(x)$ for some index set T', and $T'' = \{d' \in T' \mid d' \geq 2\}$.

We have

(i) $(P(x), Q(x)) = 1$ and $\deg(P(x)) = \deg(Q(x))$;
(ii) for any $d' \in T'$, we have

$$d' | e_i \text{ for some } 1 \leq i \leq s, \text{ and } (\Phi_{d'}(x), \Phi_d(x)) = 1 \text{ for all } d \in T;$$

(iii) for any $d \in T$ and $d' \in T'$, we have $d \nmid d'$;
(iv) for any $d \in T$ and $d'_1, d'_2 \in T'$ such that

$$(\Phi_d(a), \Phi_{d'_1}(a)) \neq 1 \text{ and } (\Phi_d(a), \Phi_{d'_2}(a)) \neq 1.$$

Then $(\Phi_d(a), \Phi_{d'_1}(a)) = (\Phi_d(a), \Phi_{d'_2}(a)) = p$ for some prime p and $d = p^{v_1} d'_1 = p^{v_2} d'_2$ for some $v_1, v_2 \in \mathbb{N}^*$. Furthermore, $\mathrm{ord}_p(\Phi_d(a)) = 1$ except $d = 2, d'_1 = d'_2 = 1$.

The statements (i), (ii) and (iii) are obvious. We only prove (iv). In fact, by Corollary 2.5, there exist primes p_1 and p_2 such that $(\Phi_d(a), \Phi_{d'_1}(a)) = p_1$ and $(\Phi_d(a), \Phi_{d'_2}(a)) = p_2$. If $p_1 \neq p_2$, then by (iii) and Corollary 2.5, we have $d = p_1^{r_1} p_2^{r_2} d''$ for some $r_1, r_2, d'' \in \mathbb{N}^*$ with $(p_1, p_2 d'') = (p_2, p_1 d'') = 1$. By Lemma 2.3, we have $p_2^{r_2} d'' | (p_1 - 1)$ and $p_1^{r_1} d'' | (p_2 - 1)$. This is

a contradiction. Hence we obtain $(\Phi_d(a), \Phi_{d_1'}(a)) = (\Phi_d(a), \Phi_{d_2'}(a)) = p$ for some prime p. From (iii) and Corollary 2.5, we have $d = p^{v_1} d_1' = p^{v_2} d_2'$ for some $v_1, v_2 \in \mathbb{N}^*$. By Lemma 2.2, we have $\mathrm{ord}_p(\Phi_d(a)) = 1$ except $d = 2, d_1' = d_2' = 1$. Thus we complete the proof of (iv).

By assumption, we have

$$\frac{a^n - 1}{\prod_{i=1}^{s} (a^{e_i} - 1)} = \frac{\prod_{d \in T} \Phi_d(a)}{(a-1)^{s-1} \cdot \prod_{d' \in T''} \Phi_{d'}(a)} = \frac{P(a)}{Q(a)} \in \mathbb{N}^*.$$

By assumption $a \geq 3$, then either $a - 1 = 2^r$ or there exists an odd prime p such that $p^r \| (a-1)$ for some $r \in \mathbb{N}^*$. Then $2^{r(s-1)} | P(a)$ or $p^{r(s-1)} | P(a)$. If $a - 1 = 2^r$, then

$$\mathrm{ord}_2(\Phi_2(a)) = \mathrm{ord}_2(a+1) = \mathrm{ord}_2(2^r + 2) = \begin{cases} 1, & r \geq 2, \\ 2, & r = 1. \end{cases}$$

Case 1 Assume $p = 2$ and $r = 1$, *i.e.*, $a = 3$. Since $2 | T_d$ for some $d \in T$, d is even, so is n even.
(a) If $2 \notin T$, by Lemma 2.2 and Corollary 2.5, there exist positive integers $2 \leq j_1 < j_2 < \cdots < j_{s-1}$ such that

$$2^{j_1}, 2^{j_2}, \ldots, 2^{j_{s-1}} \in T, \text{ and } \mathrm{ord}_2(\Phi_{2^{j_k}}(3)) = 1, \ 1 \leq k \leq s-1.$$

(b) If $2 \in T$, then $e_1, \ldots, e_s$ are odd, hence s is even.
If $s \geq 4$, then $2, 2^2, \ldots, 2^{s-2} \in T$ and

$$\mathrm{ord}_2(\Phi_2(3)) = 2, \ \ \mathrm{ord}_2(\Phi_{2^k}(3)) = 1, \ \ 2 \leq k \leq s-2.$$

Case 2 Assume p is odd or $p = 2, a - 1 = 2^r, r \geq 2$. By Lemma 2.2 and Corollary 2.5, there exist positive integers $1 \leq i_1 < i_2 < \cdots < i_{r(s-1)}$ such that

$$p^{i_1}, p^{i_2}, \ldots, p^{i_{r(s-1)}} \in T, \text{ and } \mathrm{ord}_p(\Phi_{p^{i_k}}(a)) = 1, \ 1 \leq k \leq r(s-1).$$

We set

$$\Delta = \begin{cases} \{2\}, & \text{if } p = 2, a = 3, 2 \in T, s = 2, \\ \{2, 2^2, \ldots, 2^{s-2}\}, & \text{if } p = 2, a = 3, 2 \in T, s \geq 4, \\ \{2^{j_1}, 2^{j_2}, \ldots, 2^{j_{s-1}}\}, & \text{if } p = 2, a = 3, 2 \notin T, \\ \{p^{i_1}, p^{i_2}, \ldots, p^{i_{r(s-1)}}\}, & \text{if } p \text{ is odd or } p = 2, a - 1 = 2^r, r \geq 2. \end{cases}$$

If $T'' \neq \emptyset$, we define a map $f : T'' \longrightarrow T$ as follows. By Lemma 2.6, for any $d' \in T''$, we have $|\Phi_{d'}(a)| \neq 1$. Choose a prime factor of $\Phi_{d'}(a)$, say $p' | \Phi_{d'}(a)$, there exists $d = p'^{v} d' \in T$ for some $v \geq 1$. Define $f(d') = d$. By Lemma 2.2, we have $\mathrm{ord}_{p'}(\Phi_d(a)) = 1$. By (iv), the map f is injective and $f(d') \notin \Delta$. For any $d' \in T''$, we have $d' \geq 2$ and $p' | \Phi_{d'}(a)$, and if $p' = 2$, then $2 | d'$. Hence

$$\deg(\Phi_{f(d')}(x)) = \varphi(p'^{v} d') > \varphi(d') = \deg(\Phi_{d'}(x)), \ \ d' \in T''.$$

On the other hand, we always have

$$\sum_{m \in \Delta} \deg(\Phi_m(x)) \geq s - 1.$$

Hence the equality $\deg(P(x)) = \deg(Q(x))$ implies that $T'' = \emptyset$ and

$$\sum_{m \in \Delta} \deg(\Phi_m(x)) = s - 1 \text{ and } a - 1 = p^r.$$

Note that $T'' = \emptyset$ implies that

$$e_i | n \text{ and } (e_i, e_j) = 1, \ 1 \leq i \neq j \leq s.$$

It is easy to verify that $\sum_{m \in \Delta} \deg(\Phi_m(x)) = s - 1$ if and only if (i) $a = 3$, $p = 2$, $s = 2$, $e_1 = e_2 = 1$, or (ii) $a = 3$, $p = 2$, $s = 4$, $e_1 = e_2 = e_3 = e_4 = 1$. This completes the proof. □

Lemma 3.2. *Let $n \in \mathbb{N}^*$ and $n \geq 2$. Assume $s \geq 2$ and $e_1, e_2, \ldots, e_s \in \mathbb{N}^*$ with $\sum_{i=1}^{s} e_i = n$. If $\prod_{i=1}^{s} (2^{e_i} - 1) | (2^n - 1)$, then $e_i | n$ for all $1 \leq i \leq s$, and $(e_1, \ldots, e_s) = 1$.*

Proof. The assumption $\prod_{i=1}^{s}(2^{e_i}-1)|(2^n-1)$ implies that

$$\frac{2^n-1}{\prod_{i=1}^{s}(2^{e_i}-1)}=\frac{\prod_{d\in T}\Phi_d(2)}{\prod_{d'\in T''}\Phi_{d'}(2)}=\frac{P(2)}{Q(2)}\in\mathbb{N}^*,$$

where the sets T and T'' are defined by the formula (5). Suppose that there exists e_{i_0} for some $1\le i_0\le s$ such that $e_{i_0}\nmid n$. Hence there is a prime p and $r\in\mathbb{N}^*$ such that $p^r|e_{i_0}$ and $p^r\nmid n$. Thus $p^r\in T''$. By Lemma 2.6, we have $|\Phi_{p^r}(2)|\neq 1$. Let l be a prime such that $l|\Phi_{p^r}(2)$. Then there exists $d\in T$ such that $l|\Phi_d(2)$. From (iii) of the proof of Proposition 3.1 and Corollary 2.5, we have $d=l^v p^r$ for some $v\in\mathbb{N}^*$. Therefore $l^v p^r|n$. This contradicts the fact $p^r\nmid n$. Hence we have $e_i|n$ for all $1\le i\le s$.

Assume $(e_1,\dots,e_s)=d>1$. Put $a=2^d$, $e_i=e_i'd$, $1\le i\le s$, $n=n'd$. Then $a\ge 4$ and $n'=\sum_{i=1}^{s}e_i'$. By Proposition 3.1, we have $\prod_{i=1}^{s}(a^{e_i'}-1)\nmid(a^{n'}-1)$, hence $\prod_{i=1}^{s}(2^{e_i}-1)\nmid(2^n-1)$. This contradicts the assumption $\prod_{i=1}^{s}(2^{e_i}-1)|(2^n-1)$. Therefore we have $(e_1,\dots,e_s)=1$. □

Lemma 3.3. *Let $n\in\mathbb{N}^*$ and $h(n)=\frac{\sigma(n)}{n}$, where $\sigma(n)=\sum_{d|n}d$. Then we have $h(n)<1.28n^{\frac{1}{4}}$, for all $n\in\mathbb{N}^*$.*

Proof. Let $p\ge 5$ be a prime and $a\in\mathbb{N}^*$. It is easy to see that $\frac{h(p^a)}{p^{\frac{a}{4}}}<1$. For $p=2,\ 3$, we get

$$\frac{h(2^a)}{2^{\frac{a}{4}}}\begin{cases}<1.262, & \text{if } a=1,\\ <1.238, & \text{if } a=2,\\ <1.115, & \text{if } a=3,\\ <1, & \text{if } a\ge 4\end{cases}$$

and

$$\frac{h(3^a)}{3^{\frac{a}{4}}}\begin{cases}<1.014, & \text{if } a=1,\\ <1, & \text{if } a\ge 2.\end{cases}$$

Hence we have $h(n)<1.262\times 1.014n^{\frac{1}{4}}<1.28n^{\frac{1}{4}}$, for all $n\in\mathbb{N}^*$. □

Lemma 3.4. *Let $n\in\mathbb{N}^*$. Set*

$$c(n)=\begin{cases}0.59, & \text{if } \operatorname{ord}_2(n)=1,\\ 0.70, & \text{if } \operatorname{ord}_2(n)=2,\\ 0.84, & \text{if } \operatorname{ord}_2(n)=3,\\ 1, & \text{if } \operatorname{ord}_2(n)\ge 4, \text{ or } \operatorname{ord}_2(n)=0.\end{cases}$$

Then $\varphi(n)>c(n)n^{\frac{3}{4}}$, for any integer $n\ge 2$.

Proof. If p is an odd prime, then $\varphi(p^a)>p^{\frac{3a}{4}}$ for any $a\in\mathbb{N}^*$. On the other hand, we have

$$\frac{\varphi(2^a)}{2^{\frac{3a}{4}}}\begin{cases}>0.59, & \text{if } \operatorname{ord}_2(n)=1,\\ >0.70, & \text{if } \operatorname{ord}_2(n)=2,\\ >0.84, & \text{if } \operatorname{ord}_2(n)=3,\\ >1, & \text{if } \operatorname{ord}_2(n)\ge 4.\end{cases}$$

Hence $\varphi(n)>c(n)n^{\frac{3}{4}}$, for any integer $n\ge 2$. □

Proposition 3.5. *Let $n\ge s\ge 2$, $e_1\le e_2\le\cdots<e_s$ be positive integers such that $\sum_{i=1}^{s}e_i=n$. For each $d|n$, $d<n$, let $u_d=|\{e_i\mid e_i=d,\ 1\le i\le s\}|$. Assume that $u_1\le 2$ and $u_d\le\frac{2^d-1}{d}$ for any $d\ge 2$. Then $\prod_{i=1}^{s}(2^{e_i}-1)|(2^n-1)$ if and only if (1) $n=2, s=2, e_1=e_2=1$; or (2) $n=4, s=3, e_1=e_2=1, e_3=2$; or (3) $n=6, s=3, e_1=1, e_2=2, e_3=3$.*

Proof. The sufficiency is trivial. It is sufficient to show the necessity. Set

$$R = \frac{2^n - 1}{\prod_{i=1}^{s} (2^{e_i} - 1)} \in \mathbb{N}^*.$$

(1) Assume $2 \le n \le 6$. It is easy to show the necessity by Lemma 3.2.

(2) Assume $n \ge 7$. The primitive part M of $2^n - 1$ can not be reduced with the denominator, so $R \ge M$. By Lemma 2.7, we have

$$R \ge M \ge \frac{\Phi_n(2)}{n} \ge \frac{2^{\varphi(n)}}{2n}.$$

On the other hand, we have

$$R = \frac{2^n - 1}{2^n} \prod_{i=1}^{s} (1 - 2^{-e_i})^{-1} < \prod_{i=1}^{s} (1 - 2^{-e_i})^{-1}.$$

By assumption, $u_1 \le 2$, $u_2 \le 1$, hence

$$\begin{aligned}
\log R &< 2\log 2 + \delta(n)\log\tfrac{4}{3} - \textstyle\sum_{e_i \ge 3} \log(1 - 2^{-e_i}) \\
&< \log 4 + \delta(n)\log\tfrac{4}{3} + \textstyle\sum_{e_i \ge 3} \frac{1}{2^{e_i} - 1} \\
&< \log 4 + \delta(n)\log\tfrac{4}{3} + \textstyle\sum_{d \mid n,\ 3 \le d < n} \frac{u_d}{2^d - 1} \\
&\le \log 4 + \delta(n)\log\tfrac{4}{3} + \textstyle\sum_{d \mid n,\ 3 \le d < n} \frac{1}{d} \\
&= \log 4 + \delta(n)\log\tfrac{4}{3} - 1 - \tfrac{\delta(n)}{2} - \tfrac{1}{n} + h(n),
\end{aligned}$$

where $\delta(n) = \begin{cases} 1, & \text{if } n \equiv 0 \pmod 2, \\ 0, & \text{if } n \equiv 1 \pmod 2. \end{cases}$

By Lemmas 3.3, 3.4, we have

$$\log R > \varphi(n)\log 2 - \log 2n > c(n)\log 2 \cdot n^{\frac{3}{4}} - \log 2n,$$
$$\log R < \log 4 + \delta(n)\log\frac{4}{3} - 1 - \frac{\delta(n)}{2} - \frac{1}{n} + 1.28\, n^{\frac{1}{4}}.$$

It is easy to calculate that the inequality

$$\log 4 + \delta(n)\log\frac{4}{3} - 1 - \frac{\delta(n)}{2} - \frac{1}{n} + 1.28\, n^{\frac{1}{4}} > c(n)\log 2 \cdot n^{\frac{3}{4}} - \log 2n$$

holds for $n \ge 7$ if and only if

$$n \in \{7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 26, 30, 34, 38, 42, 46, 50, 54\}.$$

Hence the inequality

$$\log 4 + \delta(n)\log\frac{4}{3} - 1 - \frac{\delta(n)}{2} - \frac{1}{n} + h(n) > \varphi(n)\log 2 - \log 2n$$

holds for $n \ge 7$ if and only if $n \in D = \{8, 9, 10, 12, 14, 18, 20, 24, 30\}$. By Lemma 3.2, we can straightly calculate that there is no $n \in D$ meeting the assumptions. This completes the proof. □

We are now in the position to prove the main theorem.

Proof of the main theorem. The sufficiency is trivial. We need only to show the necessity. We may assume that $p(x) \in \mathbb{F}_q[x]$ is monic and reducible and of degree $n \ge 1$. Let

$$p(x) = p_1(x)^{r_1} \cdots p_k(x)^{r_k}$$

be the standard decomposition, where $p_i(x)$ is monic and irreducible and of degree $e_i \ge 1$, $r_i \ge 1$, $1 \le i \le k$. By (3) of Proposition 1.2, we have $r_1 = r_2 = \cdots = r_k = 1$. Hence

$$p(x) = p_1(x) \cdots p_k(x), \quad n = \sum_{i=1}^{k} e_i, \quad \text{and} \quad \prod_{i=1}^{k} (q^{e_i} - 1) \mid (q^n - 1).$$

If $q \geq 3$, then, by Proposition 3.1, we have $q = 3$, $k = 2$, $e_1 = e_2 = 1$, or $q = 3$, $k = 4$, $e_1 = e_2 = e_3 = e_4 = 1$. But there are only three distinct monic irreducible polynomials of degree one in $\mathbb{F}_3[x]$, hence $p(x)$ is the product of any 2 distinct monic irreducibles of degree 1. Hence

$$L_{\mathbb{F}_3[x]} = \{ax(x+1), ax(x-1), a(x+1)(x-1) \in \mathbb{F}_3[x], a = 1, 2\}.$$

If $q = 2$, then the $e_i's$ satisfy the assumptions of Proposition 3.5, hence we have (i) $n = 2, k = 2, e_1 = e_2 = 1$; or (ii) $n = 4$, $k = 3, e_1 = e_2 = 1, e_3 = 2$; or (iii) $n = 6, k = 3, e_1 = 1, e_2 = 2, e_3 = 3$. On the other hand, the irreducibles of degree 1 are x and $x+1$; x^2+x+1 is the unique irreducible of degree 2; the irreducibles of degree 3 are x^3+x+1 and x^3+x^2+1. Hence

$$\begin{aligned} L_{\mathbb{F}_2[x]} = \{&x(x+1), x(x+1)(x^2+x+1), x(x^2+x+1)(x^3+x+1), \\ &(x+1)(x^2+x+1)(x^3+x+1), x(x^2+x+1)(x^3+x^2+1), \\ &(x+1)(x^2+x+1)(x^3+x^2+1) \in \mathbb{F}_2[x]\}. \end{aligned}$$

This completes the proof. □

Acknowledgements

We would like to thank the referee, Prof. X. Guo and H. Lv for reading the manuscript carefully and for providing valuable comments and suggestions.

References

[1] W. Banks, A. Güloğlu, W. Nevans, On the congruence $N \equiv A \pmod{\varphi(n)}$, Integers 8 (2008), A59.
[2] W. Banks, F. Luca, Composite integers n for which $\varphi(n)|n-1$, Acta Math. Sin. Engl. Ser. 23 (10) (2007) 1915–1918.
[3] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, S.S. Wagstaff Jr., Factorizations of $b^n \pm 1$, $b = 2, 3, 6, 7, 10, 11, 12$ up to High Powers, third edition, Contemporary Mathematics, vol. 22, American Mathematical Society, Providence, RI, USA, 2002.
[4] G.L. Cohen, P. Hagis Jr., On the number of prime factors of n if $\varphi(n)|(n-1)$, Nieuw Arch. Wiskd. 28 (3) (1980) 177–185.
[5] J.M. Grau, A.M. Oller-Marcén, On k-Lehmer numbers, Integers 12 (5) (2012) 1081–1089.
[6] D.H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. 38 (10) (1932) 745–751.
[7] F. Luca, C. Pomerance, On composite integers n for which $\varphi(n)|n-1$, Bol. Soc. Mat. Mexicana 17 (2011) 13–21.
[8] H.F. Lv, Some series and congruences, master's thesis, Nanjing University, China, 2012.
[9] R.G.E. Pinch, A note on Lehmer's totient problem, Poster presented in ANTS VII, http://www.math.tu-berlin.de/~kant/ants/Poster/Pinch Poster3.pdf.
[10] C. Pomerance, On composite integers n for which $\varphi(n)|n-1$ (II), Pac. J. Math. 69 (1) (1977) 177–186.
[11] J. Schettler, Lehmer's totient problem and Carmichael numbers in a PID, http://math.arizona.edu/~jschettler/Schettler.pdf.
[12] R. Thangadurai, A. Vatwani, The least prime congruent to one modulo n, Amer. Math. Monthly 118 (8) (2011) 737–742.
[13] L. Washington, Introduction to Cyclotomic Fields, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, 1982.
[14] K. Zsigmondy, Zur Theorie der Potenzreste, Monatshefte Math. 3 (1) (1892) 265–284, http://dx.doi.org/10.1007/BF01692444.