LEHMERS TOTIENT PROBLEM OVER $\mathbb{Z}/p^n\mathbb{Z}[x]$

GONG LEIYU
GUANGDONG EXPERIMENTAL HIGH SCHOOL
ADVISOR: ZHANG JUNJIE

Abstract. In this paper, we consider an analogue of the Lehmer's totient problem. Let p be a prime, $n > 1$ an integer. Let $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1} + x^t \in \mathbb{Z}/p^n\mathbb{Z}[x]$ and $\varphi(p^n, f(x))$ be the Euler's totient function of $f(x)$ over $\mathbb{Z}/p^n\mathbb{Z}[x]$. We obtain some results on $\varphi(p^n, f(x))|p^{(n-1)t}(p^t - 1)$, which generalizes and solves the related Lehmer's totient problem in $\mathbb{Z}/p^n\mathbb{Z}[x]$.

1. Introduction

Throughout this paper, let $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{N}$ and P denote the field of rational numbers, the ring of rational integers, the set of positive integers and the set of primes in $\mathbb{N}$, respectively.

Eulers totient function φ is defined on $\mathbb{N}$ by taking $\varphi(n)$ to be the number of positive integers less than or equal to and relatively prime to n. Lehmers totient problem consists of determining the set of n such that

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

where k is an integer. In [6], Lehmer showed that if n is a solution of (1), then n is a prime or the product of seven or more distinct primes. The most interesting part of this problem is that we all 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.

In 1980 Cohen and Hagis [4] proved that, for any solution n to the problem, $n > 10^{20}$ and $\omega(n) \geq 14$. In 1988 Hagis [5] showed that if 3 divides any solution n then $n > 10^{1937042}$ and $\omega(n) \geq 298848$.

The best result is due to Richard G. E. Pinch(see [10]), that the number of prime factors of a Lehmer number n must be at least 15 and there is no Lehmer number less than 10^{30}. For other references on this subject, we refer to the references [1, 2, 3, 6, 8, 9, 11, 14].

J. Schettler [12] generalizes the divisibilty condition $\varphi(n)|(n-1)$, constructs 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

(2)

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

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 $\mathbb{F}_q$ is a finite field with q elements. Then $\mathbb{F}_q[x]$ is a PID. Schettler obtains some properties of elements of $L_{\mathbb{F}_q[x]}$.

Recently, Ji and Qin [13] determined the set $L_{\mathbb{F}_q[x]}$.

The main purpose of the present paper is to generalize the above problem to the ring $\mathbb{Z}/p^n\mathbb{Z}[x]$, where p is a prime and $n \in \mathbb{N}$.

2. Preliminaries

We first note that $R = \mathbb{Z}/p^n\mathbb{Z}[x]$ is not a PID, however R also have with the property: $R/(r)$ is finite whenever $0 \neq r \in R$. In this section, we prove some results on the units and zero divisors of $R = \mathbb{Z}/p^n\mathbb{Z}[x]$.

To begin with, we have

Lemma 1. *Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in \mathbb{Z}/p^n\mathbb{Z}[x]$. Then $f(x)$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[x]$ if and only if $a_0 \not\equiv 0 \pmod p$ and $a_i \equiv 0 \pmod p$, $1 \leq i \leq m$.*

Proof. We first prove the necessity. We have

$$f(x)^{p^n} \equiv a_0^{p^n} \pmod{p^n},$$

and $a_0 \not\equiv 0 \pmod p$, so $f(x)$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[x]$.

Next, if $f(x)$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[x]$, then there exists a polynomial

$$g(x) = b_0 + b_1x + \cdots + b_lx^l \in \mathbb{Z}/p^n\mathbb{Z}[x]$$

such that

$$(a_0 + a_1x + \cdots + a_mx^m)\left(b_0 + b_1x + \cdots + b_lx^l\right) = 1.$$

Hence $a_0b_0 = 1$ and $a_mb_l \equiv 0 \pmod{p^n}$, which implies that $a_0, b_0 \not\equiv 0 \pmod{p}$.

If $a_i \equiv 0 \pmod{p}$, $1 \le i \le m$, then we are done. If $a_j \equiv 0 \pmod{p}$, $1 \le j \le l$, then

$$f(x) = g(x)^{-1} = \frac{1}{b_0}g(x)^{p^n-1} = c_0 + c_1x + \cdots + c_kx^k \in \mathbb{Z}/p^n\mathbb{Z}[x].$$

It is easy to see that $c_0 \not\equiv 0 \pmod{p}$ and $c_i \equiv 0 \pmod{p}$, $1 \le i \le k$, and we are done.

Otherwise, we may assume that s is the maximal index such that $a_s \not\equiv 0 \pmod{p}$ and $a_i \equiv 0 \pmod{p}, s+1 \le i \le m$ and t is the maximal index such that $b_t \not\equiv 0 \pmod{p}$ and $b_j \equiv 0 \pmod{p}, t+1 \le j \le l$. Then

$$f(x)g(x) = 1 + \cdots + d_{s+t}x^{s+t} + \cdots + a_mb_lx^{m+l}.$$

Since $d_{s+t} \equiv a_sb_t \not\equiv 0 \pmod{p}$, which contradicts to $f(x)g(x) = 1$. Therefore we have proved the lemma. □

Lemma 2. *Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in \mathbb{Z}/p^n\mathbb{Z}[x]$. If $f(x)$ is an irreducible polynomial over $\mathbb{Z}/p\mathbb{Z}[x]$, then for any $g(x) \in Z(\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x)))$, we have $g(x) = ph(x)$ for some $h(x) \in \mathbb{Z}/p^n\mathbb{Z}[x]$.*

Proof. Obviously $(ph(x))^n = 0$, so $ph(x)$ is a zero divisor in $\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$. Now assume that $g(x) \in \mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$ is a zero divisor and $g(x) \ne ph(x)$, so $g(x) = b_0 + \cdots + b_tx^t \not\equiv 0 \pmod{p}$, $t < m$. Since $f(x) \pmod{p}$ is an irreducible polynomial, so $f(x)$ and $g(x)$ are coprime modulo p. It follows that there exist polynomials $u(x)$, $v(x)$, $w(x)$ such that

$$u(x)f(x) + v(x)g(x) = 1 + pw(x).$$

Note that $(1 + pw(x))^{p^n} \equiv 1 \pmod{p^n}$, we have

$$(1+pw(x))^{p^n-1}u(x)f(x)+(1+pw(x))^{p^n-1}v(x)g(x) \equiv 1 \pmod{p^n},$$

which implies that $g(x)$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$, a contradiction. This completes the proof. □

Lemma 3. *Let $f(x) = a_0 + a_1x + \cdots + a_mx^m \in \mathbb{Z}/p^n\mathbb{Z}[x]$ and $f(x)$ is not a constant and $f(x)$ is not an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$. Let*

$$f(x) = p_1^{e_1}(x) \cdot \cdots \cdot p_t^{e_t}(x),$$

where $p_i(x)$ are irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$, be the factorization of $f(x)$ over $\mathbb{Z}/p\mathbb{Z}[x]$. Then for any $g(x) \in Z(\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x)))$, *we have* $g(x) = d(x)g_1(x) + ph(x)$ *for some polynomials* $g_1(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ *and* $h(x) \in \mathbb{Z}/p^n\mathbb{Z}[x]$, *where* $d(x)|f(x)$ *in* $\mathbb{Z}/p\mathbb{Z}[x]$.

Proof. Obviously, $ph(x)$ is a non-zero zero-divisor in $\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$ when $ph(x) \neq 0$ in $\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$. Since $d(x)|f(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$, we have $f(x) = d(x)f_1(x) + pf_2(x), f_1(x), f_2(x) \in \mathbb{Z}[x]$. If $f_1(x) \equiv 0 \pmod p$, then we are done. If $f_1(x) \equiv 0 \pmod p$, we have

$$p^{n-1}f_1(x) \cdot (d(x)g_1(x) + ph(x)) = p^{n-1}f(x)g_1(x) + p^n h(x) = 0,$$

and $p^{n-1}f_1(x) \neq 0$, so $d(x)g_1(x)+ph(x)$ is a nonzero zero divisor in $\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$.

Now suppose that $g(x)$ and $f(x)$ are coprime modulo p, then as the same argument in the above lemma, we obtain that $g(x)$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$. Therefore, $g(x)$ and $f(x)$ are not coprime modulo p when $g(x)$ is a nonzero zero divisor in $\mathbb{Z}/p^n\mathbb{Z}[x]/(f(x))$. It follows that $g(x) = d(x)g_1(x) + ph(x)$ for some polynomials $g_1(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ and $h(x) \in \mathbb{Z}/p^n\mathbb{Z}[x]$, where $d(x)|f(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$. This completes the proof. □

Lemma 4. *Let* $\alpha \in \mathbb{N}$ *and* p *be a prime. Let*

$$f(X) = a_0 + a_1X + \cdots + a_sX^s + p^\alpha a_{s+1}X^{s+1} + \cdots + p^\alpha a_tX^t \in \mathbb{Z}[X],$$

where $s, t \in \mathbb{N}$, $s \leq t, a_i \in \mathbb{Z}$ *for* $0 \leq i \leq t$ *and* $p \nmid a_s$. *Then there is a polynomial*

$$U(X) = 1 + p^\alpha b_1X + \cdots + p^\alpha a_mX^m \in \mathbb{Z}[X],$$

where $m \in \mathbb{N}$ *and* $b_i \in \mathbb{Z}$ *for* $1 \leq i \leq m$, *such that*

$$f(X)U(X) = c_0 + c_1X + \cdots + c_sX^s + p^{\alpha+1}c_{s+1}X^{s+1} + \cdots + p^{\alpha+1}c_{m+t}X^{m+t} \in \mathbb{Z}[X],$$

where $c_i \in \mathbb{Z}$ *for* $0 \leq i \leq m+t$ *and* $p \nmid c_s$.

Proof. If $t = s$, then we can take $U(X) = 1$ and we are done. Assume from now on that $t > s$.

Now we take $m = t - s$. For a polynomial

$$U(X) = 1 + p^\alpha b_1X + \cdots + p^\alpha a_mX^m \in \mathbb{Z}[X],$$

we have

$$\begin{aligned} f(X)U(X) &= a_0 + a_1X + \cdots + a_sX^s \\ &\quad + p^\alpha(a_0 + a_1X + \cdots + a_sX^s)(b_1X + \cdots + b_mX^m) \\ &\quad + p^\alpha(a_{s+1}X^{s+1} + \cdots + a_tX^t) \\ &\quad + p^{2\alpha}(a_{s+1}X^{s+1} + \cdots + a_tX^t)(b_1X + \cdots + b_mX^m). \end{aligned}$$

We consider the coefficients of

$p^\alpha(a_0+a_1X+\cdots+a_sX^s)(b_1X+\cdots+b_mX^m)+p^\alpha(a_{s+1}X^{s+1}+\cdots+a_tX^t)$.

Let $d_0, d_1, \ldots, d_t \in \mathbb{Z}$ such that

$$(a_0+a_1X+\cdots+a_sX^s)(b_1X+\cdots+b_mX^m)+(a_{s+1}X^{s+1}+\cdots+a_tX^t) = d_0 + d_1X + \cdots + d_tX^t.$$

Then we have

$$\begin{aligned}
&d_t = d_{s+m} = a_sb_m + a_t,\\
&d_{t-1} = d_{s+m-1} = a_sb_{m-1} + a_{s-1}b_m,\\
&\cdots\cdots\cdots,\\
&d_{s+k} = a_sb_k + \cdots + a_{s+k-m}b_m,\\
&\cdots\cdots\cdots,\\
&d_{s+1} = a_sb_1 + a_{s-1}b_2 + \cdots + a_{s+1-m}b_m,
\end{aligned}$$

where we let $a_i = 0$ if $i < 0$ for convenience. Since $p \not| a_s$, we choose $b_m \in \mathbb{Z}$ such that $a_sb_m + a_t \equiv 0 \pmod p$, that is $p|d_{s+m}$. Suppose we have chosen b_j for $k+1 \le j \le m$. Since $p \not| a_s$ again, we choose $b_k \in \mathbb{Z}$ such that $a_sb_k + \cdots + a_{s+k-m}b_m \equiv 0 \pmod p$, that is $p|d_{s+k}$. Therefore we have $p|d_i$ for $s+1 \le i \le t$. Hence

$$\begin{aligned}
f(X)U(X) &= (a_0 + p^\alpha d_0) + (a_1 + p^\alpha d_1)X + \cdots + (a_s + p^\alpha d_s)X^s\\
&\quad +p^{\alpha+1}(d_{s+1}/pX^{s+1} + \cdots + d_t/pX^t)\\
&\quad p^{2\alpha}(a_{s+1}X^{s+1} + \cdots + a_tX^t)(b_1X + \cdots + b_mX^m)\\
&= c_0 + c_1X + \cdots + c_sX^s + p^{\alpha+1}c_{s+1}X^{s+1} + \cdots + p^{\alpha+1}c_{m+t}X^{m+t}.
\end{aligned}$$

Since $p \not| a_s$ and $c_s = a_s + p^\alpha d_s$, we have $p \not| c_s$. This completes the proof.

$\square$

Applying the above lemma repeatedly, we obtain

Proposition 1. *Let p be a prime and $q = p^n$ with $n \ge 2$. Let $f(x) = a_0+a_1X+\cdots+a_sX^s+pa_{s+1}X^{s+1}+\cdots+pa_tX^t \in \mathbb{Z}/p^n\mathbb{Z}[X]$, where $s, t \in \mathbb{N}$, $s \le t$ and $a_i \in \mathbb{Z}/p^n\mathbb{Z}$ for $0 \le i \le t$ and $p \not| a_s$. Then there is a unit*

$$U(X) = b_0 + pb_1X + \cdots + pb_mX^m \in \mathbb{Z}/p^n\mathbb{Z}[X]$$

where $m \in \mathbb{N}$, $b_i \in \mathbb{Z}/p^n\mathbb{Z}$ for $0 \le i \le m$ and $p \not| b_0$, such that

$$f(X)U(X) = c_0 + c_1X + c_{s-1}X^{s-1} + X^s \in \mathbb{Z}/p^n\mathbb{Z}[X],$$

where $c_i \in \mathbb{Z}/p^n\mathbb{Z}$ *for* $0 \leq i \leq s-1$.

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

$$\varphi(f(x)) = \{g(x) \in \mathbb{Z}/p\mathbb{Z}[x] | deg(g(x)) \leq m-1,\ \gcd(f(x), g(x)) = 1\}.$$

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

$$\varphi(p, f(x)) = \sharp\Phi(f(x)).$$

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

Proposition 2. [13] Proposition 1.2 *Let* $f(x) = p_1^{e_1}(x) \cdot \cdots \cdot p_t^{e_t}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ *of degree* $n \geq 1$, *where* $p_1(x), \ldots, p_t(x) \in P(\mathbb{Z}/p\mathbb{Z}[x])$ *are non-associate,* $deg(p_i(x)) = n_i$ *and* $e_i \geq 1$, $1 \leq i \leq t$. *Then we have*

(1) $\varphi(p, f(x)) = p^n \prod_{i=1}^{t}(1 - \frac{1}{p^{n_i}})$;

(2) If $g(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ *and* $\gcd(f(x),\ g(x)) = 1$, *then* $g(x)^{\varphi(p,f(x))} \equiv 1 \pmod{f(x)}$;

(3) If $\varphi(p, f(x)) | (p^n - 1)$, *then* $r_i = 1$ *for all* $1 \leq i \leq t$.

First we have the following theorem.

Theorem 1. *Let* p *be a prime and* $t, n \in \mathbb{N}$, $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1} + x^t \in \mathbb{Z}/p^n\mathbb{Z}[x]$, $a_i \in \mathbb{Z}/p^n\mathbb{Z}$. *Let*

$$f(x) = p_1(x)^{e_1} \cdot \cdots \cdot p_s(x)^{e_s} \pmod{p}$$

be the standard decomposition of $f(x)$ *over* $\mathbb{Z}/p\mathbb{Z}[x]$ *with* $deg(p_i(x)) = n_i$. *Let* $\varphi(f(x), p^n)$ *denote the number of polynomials* $g(x) = b_0 + b_1x + \cdots + b_{t-1}x^{t-1} \in \mathbb{Z}/p^n\mathbb{Z}[x], 0 \leq b_i < p^n$ *with* $\gcd(g(x), f(x)) = 1$. *Then*

$$\varphi(f(x), p^n) = p^{nt} \prod_{i=1}^{s} \left(1 - \frac{1}{p^{n_i}}\right).$$

Proof. By the assumptions and Lemma 3, if $\gcd(g(x), f(x)) = 1$, then $g(x)$ is of the form $g(x) = g_1(x) + ph(x)$, $\gcd(g_1(x), f(x)) = 1 \pmod{p}$, $g_1(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ and $h(x) \in \mathbb{Z}/p^n\mathbb{Z}[x]$. By proposition 2, the number of $g_1(x)$ is

$$p^t \prod_{i=1}^{s} \left(1 - \frac{1}{p^{n_i}}\right)$$

and the number of $h(x)$ is $p^{(n-1)t}$. Hence

$$\varphi(f(x), p^n) = p^{nt}\prod_{i=1}^{s}\left(1-\frac{1}{p^{n_i}}\right).$$

□

3. A Generalization and Some Results

To simplify the notation, denote $\mathbb{Z}/p^n\mathbb{Z}[x]$ by R in this section.

Let $f(x) = a_0 + a_1x + \cdots + a_tx^t + ph(x)x^{t+1} \in R$ with $p \not| a_t$. By proposition 1, there exists a unit $U(x) \in R$ such that

$$f(x)U(x) = c_0 + c_1x + \cdots + x^t.$$

Since $R/(f(x)) = R/(f(x)U(x))$, so without loss of generality, when we discuss the quotient ring $R/(f(x))$, we may assume that

$$f(x) = c_0 + c_1x + \cdots + x^t$$

and we denote $deg_u(f(x)) = t$, i.e., $deg_u(f(x))$ denote the usual degree of $f(x)$ in $\mathbb{Z}/p\mathbb{Z}[x]$.

Since $R/(r)$ is finite commutative ring, so we have the following obvious fact

$$R/(r) = \{0\} \cup U(R/(r)) \cup Z(R/(r)).$$

Moreover, $U(R/(r))$ is a finite multiplicative abelian group.

Note that $|R/(f(x))| = p^{nt}$, we know that $\mathbb{Z}/p^n\mathbb{Z}[x], n \geq 2$ has no prime elements since

$$\varphi(f(x), p^n) = p^{nt}\prod_{i=1}^{s}\left(1-\frac{1}{p^{n_i}}\right) < p^{nt}-1$$

by Theorem 1. Another observation is that

$$\varphi(f(x), p^n) \not| p^{nt}-1$$

for any $f(x)$ with $deg_u(f(x)) = t \geq 1$.

Denote the sets of units, irreducibles and (non-zero) zero divisors, in R, by $U(R)$, $I(R)$ and $Z(R)$, respectively. Define

(3)

$$L_R := \{r \in R\backslash(\{0\} \cup U(R) \cup I(R)) : |U(R/(r))|||U(R/(p))|\},$$

where $p \in R$ is a polynomial such that $deg_u(p) = deg_u(r)$ and that $|U(R/(p)|$ is maximal.

Note that the above definition coincides with $L_{R[x]}$ defined by J. Schettler [12] when $R = \mathbb{F}_q$.

We also need the following results.

Main Theorem [13] (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.,

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

(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.,

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

Proposition 3. ([13] 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) $a = 3, p = 2, s = 2, e_1 = e_2 = 1$ or

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

Proposition 4. ([13] Proposition 3.5) *Let $n \geq s \geq 2$, $e_1 \leq e_2 \leq \cdots \leq e_s$ be positive integers such that $\sum_{i=1}^{s} e_i = n$. For each $d|n, d < n$. Let $u_d = \sharp\{e_i | e_i = d, 1 \leq i \leq s\}$. Assume that $u_1 \leq 2$ and $u_d \leq \frac{2^d - 1}{d}$ for any $d \geq 2$. Then $\prod_{i=1}^{s}(2^{e_i} - 1)|(a^n - 1)$ 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) $n = 6, s = 3, e_1 = 1, e_2 = 2, e_3 = 3$.

Now we consider the analogous Lehmer's totient problem over $\mathbb{Z}/p^n\mathbb{Z}[x]$. By Proposition 1, we may assume $f(x) = a_0 + a_1 x + \cdots + a_{t-1}x^{t-1} + x^t \in \mathbb{Z}/p^n\mathbb{Z}[x]$. If $f(x) \pmod p$ is irreducible, then by Theorem 1,

$$\varphi(f(x), p^n) = p^{(n-1)t}(p^t - 1).$$

It is well-known that for any $t \geq 1$, there exists an irreducible polynomial $p(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ with $deg(p(x)) = t$, by Theorem 1, for the above $p(x)$, $|U(R/(p(x))| = p^{(n-1)t}(p^t - 1)$, $p(x)$ is irreducible in R and $|U(R/(p(x))|$ it is maximal for any $p(x)$ with $deg_u(p(x)) = t$. Hence the analogous Lehmer's totient

<<S17>>

problem over $\mathbb{Z}/p^n\mathbb{Z}[x]$ is to determine $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1} + x^t \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that $f(x)$ is not irreducible in $\mathbb{Z}/p^n\mathbb{Z}[x]$ and

$$\varphi(f(x), p^n)|p^{(n-1)t}(p^t - 1).$$

Denote $\mathfrak{L}(p^n, 1)$ be the set of $f(x) = a_0+a_1x+\cdots+a_{t-1}x^{t-1}+x^t \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that $f(x)$ is not irreducible in $\mathbb{Z}/p^n\mathbb{Z}[x]$ and $\varphi(f(x), p^n)|p^{(n-1)t}(p^t - 1)$. We have the following theorem as the main theorem of the paper.

Theorem 2. *(1) Assume $p > 4$. Then $\mathfrak{L}(p^n, 1) = \emptyset$.*

(2) Assume $p = 3$. Then

$$\mathfrak{L}(3^n, 1) \subseteq \{ax(x + 1) + 3h(x),\ ax(x - 1) + 3h(x),$$

$$a(x + 1)(x - 1) + 3h(x) \in \mathbb{Z}/3^n\mathbb{Z}[x],\ a = 1,\ 2\},$$

where $h(x) = b_0 + b_1x + b_2x^2 \in \mathbb{Z}/3^n\mathbb{Z}[x]$.

(3) Assume $p = 2$. Then

$$\mathfrak{L}(2^n, 1) \subseteq$$

$$\{x(x+1)+2h_1(x),\ x(x+1)(x^2+x+1)+2h_2(x),\ x(x^2+x+1)(x^3+x+1)+2h_3(x),$$
$$(x+1)(x^2+x+1)(x^3+x+1)+2h_4(x),\ x(x^2+x+1)(x^3+x^2+1)+2h_5(x),$$
$$(x + 1)(x^2 + x + 1)(x^3 + x^2 + 1) + 2h_6(x) \in \mathbb{Z}/2^n\mathbb{Z}\},$$

where $h_i(x) \in \mathbb{Z}/2^n\mathbb{Z}[x]$ are polynomials with $deg(h_1(x)) \leq 2$, $deg(h_2(x)) \leq 4$, $deg(h_i(x)) \leq 6, i = 3, 4, 5, 6$.

Proof. The proof is similar to the proof of the Main Theorem in [13]. For completeness, we present the proof here. The sufficiency is trivial. We need only prove the necessity. Assume that $f(x) = a_0 + a_1x + \cdots + a_{t-1}x^{t-1} + x^t \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that $f(x) \pmod p$ is reducible. Let

$$f(x) = p_1(x)^{e_1} \cdot \cdots \cdot p_s(x)^{e_s} \pmod p$$

be the standard decomposition of $f(x)$ over $\mathbb{Z}/p\mathbb{Z}[x]$, where $p_i(x)$ is irreducible over $\mathbb{Z}/p\mathbb{Z}[x]$ with $deg(p_i(x)) = n_i$. By Proposition 2, we have $e_1 = e_2 = \cdots = e_s = 1$. Hence

$$f(x) \pmod p = p_1(x) \cdots p_s(x) \text{ and } t = \sum_{i=1}^{s} n_i.$$

If $p \geq 3$, then, by Proposition 3, we have $p = 3, s = 2, n_1 = n_2 = 1$ or $p = 3, s = 4, n_1 = n_2 = n_3 = n_4 = 1$. But there are only three distinct irreducible polynomials of degree one in

$\mathbb{Z}/3\mathbb{Z}[x]$, hence $f(x) \pmod p$ is a product of two non-associate irreducible of degree 1, i.e.,

$$\mathfrak{L}(3^n,1) \subseteq \{ax(x+1)+3h(x),\ ax(x-1)+3h(x),$$
$$a(x+1)(x-1)+3h(x) \in \mathbb{Z}/3^n\mathbb{Z}[x],\ a=1,\ 2\},$$

where $h(x) = b_0 + b_1x + b_2x^2 \in \mathbb{Z}/3^n\mathbb{Z}[x]$.

If $p = 2$, then the n_i's satisfy the assumptions of Proposition 4, hence we have

(i) $t = 2, s = 2, n_1 = n_2 = 1$; or (ii) $t = 4, k = 3, n_1 = n_2 = 1, n_3 = 3$ or (iii) $t = 6, s = 3, n_1 = 1, n_2 = 2, n_3 = 3$.

On the other hand, the irreducibles of degree one are x and $x + 1$; $x^2 + x + 1$ is the unique irreducible of degree 2; the irreducible of degree 3 are $x^3 + x + 1$ and $x^3 + x^2 + 1$. Hence

$$\mathfrak{L}(2^n,1) \subseteq$$
$$\{x(x+1)+2h_1(x),\ x(x+1)(x^2+x+1)+2h_2(x),\ x(x^2+x+1)(x^3+x+1)+2h_3(x),$$
$$(x+1)(x^2+x+1)(x^3+x+1)+2h_4(x),\ x(x^2+x+1)(x^3+x^2+1)+2h_5(x),$$
$$(x+1)(x^2+x+1)(x^3+x^2+1)+2h_6(x) \in \mathbb{Z}/2^n\mathbb{Z}\},$$

where $h_i(x) \in \mathbb{Z}/2^n\mathbb{Z}[x]$ are polynomials with $deg(h_1(x)) \leq 2$, $deg(h_2(x)) \leq 4$, $deg(h_i(x)) \leq 6, i = 3,4,5,6$. This completes the proof. $\square$

References

[1] W. Banks, A. G*ddotu*loğlu and W. Nevans, On the congruence $N \equiv A \pmod n$. Integers: Electronic Journal of combinatorial number theory 8 (2008), A59.

[2] W. Banks and F. Luca, Composite integers n for which $\varphi(n)|n-1$. Acta Math. Sin. (Engl.Ser.) 23(10) (2007), 1915-1918.

[3] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman and S. S. Wagstaff, Jr., Factorizations of $b^n - 1, b = 2,3,6,7,10,11,12$ up to high powers, Third Edition, Contemporary Mathematics 22, Amer. Math, Soc., Providence, Rhode Island, 2002.

[4] G. L. Cohen and P. Hagis, On the number of prime factors of n if $\varphi(n)|(n-1)$, Nieuw Archief Wiskunde 28(3) (1980), 177-185.

[5] P. Hagis, On the equation $M\varphi(n) = n - 1$. Nieuw Arch. Wisk. 6(1988), no. 3, 255-261

[6] J. M. Grau and A. M. Oller-Marcén, On k-Lehmer numbers, Integers 12 (2012), 1-8, http://www.emis.de/journals/INTEGERS/papers/m37/m37.pdf

[7] D. H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc., 38(10) (1932), 745-751.

[8] F. Luca and C. Pomerance, On composite integers n for which $\varphi(n)|n-1$, Bol. Soc. Mat. Mexicana, 17 (2011), 13-21.

[9] H. F. Lv, Some series and congruences, master's thesis, Nanjing university, 2012.

[10] 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.

[11] C. Pomerance, On composite integers n for which $\varphi(n)|n-1$(II), Pacific J. Math., 69(1)(1977), 177-186.

[12] J. Schettler, Lehmer's totient problem and Carmichael numbers in a PID, http://math.arizona.edu/.jschettler/Schettler.pdf.

[13] Qingzhong Ji and Hourong Qin, Lehmer's toitient problem over $\mathbb{F}_q[x]$, arXiv: 1312.3107v2.

[14] R. Thangadurai, A. Vatwani, The least prime congruent to one modulo n, American Math. Monthly, 118(8) (2011) , 737-742.

Guangdong Experimental High School