Available online at http://scik.org
J. Math. Comput. Sci. 4 (2014), No. 1, 25-34
ISSN: 1927-5307

LEHMER'S EQUATIONS IN NEW DOMAINS

HAISSAM Y. CHEHADE

Department of Mathematics, Lebanese International University, Saida, Lebanon

Abstract. In this paper, we examine the equations $k\phi_G(\beta) = q(\beta) \pm 1$ and $k\phi_G(\beta) = q(\beta)$ in the domains of Gaussian integers $Z[i]$ and the polynomial rings over finite fields $Z_p[x]$, where p is prime in Z. Properties concerning the existence of solutions are studied. Complete characterization for the solutions of the above equations is given in the two domains.

Keywords: Lehmer's equations, generalized Euler's Phi function, unique factorization domains, rings of Gaussian integers and polynomial rings over finite fields.

2000 AMS Subject Classification: 11R04, 11R09, 11R27

1. Introduction

The Euler's totient function ϕ was generalized by El-Kassar [1] to any principle ideal domain(P.I.D) as follows: if G is a P.I.D and β is a non-zero element in G, then $\phi_G(\beta) = \prod_{j=1}^{r}\left[q(p_j)\right]^{\alpha_j - 1}\left[q(p_j) - 1\right]$, where $\prod_{j=1}^{r} {p_j}^{\alpha_j}$ is a factorization of β into distinct prime powers and $q(p_j)$ is the order of the factor ring $G/ < p_j >$. $\phi_G(\beta)$ is the order of the group of units of $G\,/ < \beta >$. If $\beta = a + ib$ is a non zero element in the domain of Gaussian integers $Z[i]$, then $q(\beta) = a^2 + b^2$ and $q(\beta\delta) = q(\beta)q(\delta)$ for any β and δ in $Z[i]$. An element β is a unit in $Z[i]$ if

Received October 7, 2013

and only if $q(\beta) = 1$ and an element $[\gamma] \in Z[i]/<\beta>$ is a unit if and only if $gcd(\gamma, \beta) \sim 1$, see [4]. Lehmer [2] introduced the equations $k\phi(n) = n \pm 1$, where k and n are positive integers.

The purpose of this paper is to study equations similar to that of Lehmer's and their generalization in unique factorization domain (U. F.Ds), in particular in the domain of Gaussian integers $Z[i]$ and the domain of polynomial rings over finite fields $Z_p[x]$. Throughout this paper, assume that p is a prime integer and k is a positive integer.

2. Equations in $Z[i]$

Consider the equations

$$k\phi_G(\beta) = q(\beta) + 1 \tag{2.1}$$

$$k\phi_G(\beta) = q(\beta) - 1 \tag{2.2}$$

$$k\phi_G(\beta) = q(\beta) \tag{2.3}$$

that are similar to that of Lehmer's but in the domain of Gaussian integers $Z[i]$.

Lemma 2.1 *Equation 2.3 is solvable if and only if $k = 2$, and the corresponding solution is of the form $(1+i)^{\alpha}$ where α is a positive integer.*

Proof. If $\beta = \prod_{j=1}^{r} {p_j}^{\alpha_j}$ is a solution to 2.3 with $r \geq 1$, then

$$k\prod_{j=1}^{r} \left[q(p_j)\right]^{\alpha_j - 1} \left[q(p_j) - 1\right] = \prod_{j=1}^{r} q(p_j)^{\alpha_j}. \tag{2.4}$$

Since the left hand side of 2.4 is even, then $p_j = 1+i$ for certain j with $1 \leq j \leq r$. Assume $p_1 = 1+i$, then $q(p_j)$ has the form $4k_j + 1$ for every $2 \leq j \leq r$ and

$$k\prod_{j=2}^{r} \left[q(p_j)\right]^{\alpha_j - 1} \left[q(p_j) - 1\right] = 2\prod_{j=2}^{r} q(p_j)^{\alpha_j}. \tag{2.5}$$

The right hand side of 2.5 is divisible by 2, while its left hand side is divisible by 2^{2r-2} with $r > 1$. Therefore $r = 1$, $\beta = (1+i)^{\alpha}$ with $\alpha \geq 1$ and the corresponding value of k is 2.

Lemma 2.2 *If $\beta = \prod_{j=1}^{r} {p_j}^{\alpha_j}$ is a solution to equations 2.1 or 2.2, then $\alpha_j = 1$ for every j.*

Proof. Equations 2.1 and 2.2 give

$$k\prod_{j=1}^{r} q(p_j)^{\alpha_j-1}(q(p_j)-1)=\prod_{j=1}^{r} q(p_j)^{\alpha_j}\pm 1$$

and $k\prod_{j=1}^{r} q(p_j)^{\alpha_j-1}(q(p_j)-1)-\prod_{j=1}^{r} q(p_j)^{\alpha_j}=\pm 1$. Since $\phi_G(\beta)$ and $q(\beta)$ are relatively prime, it follows that $q(p_j^{\alpha_j-1})=1$ for every $1\le j\le r$. Now, if $\alpha_j>1$, then p_j must be a unit in $G=Z[i]$, which contradicts that p_j is prime in G.

The above lemma states that any solution to equations 2.1 or 2.2 must be square free. In the next two lemmas, we will consider the case where β is a prime Gaussian integer.

Lemma 2.3 *$\beta=\gamma$ is a prime solution to 2.1 if and only if $\beta=1+i$ with $k=3$.*

Proof. Equation 2.1 gives

$$k=\frac{q(\beta)+1}{q(\beta)-1}=1+\frac{2}{q(\beta)-1}.$$

Then $q(\beta)-1=1$ or $q(\beta)-1=2$. The second case is dismissed since $q(\beta)=3$ has no solution in $Z[i]$. If $q(\beta)=2$, then $\beta=1+i$ with corresponding $k=3$. The converse is straight forward.

Lemma 2.4 *Equation 2.2 has prime solutions if and only if $k=1$.*

Proof. β is a prime solution to 2.2 implies that β has the form $1+i$, p or π where p is a prime integer of the form $4t+3$ and π is a Gaussian prime integer with $\pi\bar{\pi}$ is a prime integer of the form $4t'+1$. Each form of β results with $k=1$.

Lemma 2.5 *Any solution to equations 2.1 or 2.2 has the form $\prod_{j=1}^{r} p_j$, with $r>1$ and $p_j\neq 1+i$ for every $1\le j\le r$.*

Proof. By lemma 2.2, $\beta=\prod_{j=1}^{r} p_j$ and $k\prod_{j=1}^{r}\left[q(p_j)-1\right]=\prod_{j=1}^{r} q(p_j)\pm 1$. If $r>1$ and $p_j=1+i$ for certain $1\le j\le r$, then the left hand side of the last equation becomes even while its right hand side is odd.

Lemma 2.6 *Equation 2.1 has no solution of the form $\beta=\prod_{j=1}^{r} p_j$ with $r>1$.*

Proof. By lemma 2.5, $\beta=\prod_{j=1}^{r} p_j$ and $p_j\neq 1+i$ for every j. Hence,

$$k\prod_{j=1}^{r}\left[q(p_j)-1\right]=\prod_{j=1}^{r} q(p_j)+1.$$

Since $q(p_j)$ has the form $4k_j+1$ for every j, the last equation is reduced to the form $2^b k \prod_{j=1}^{r} k_j = T$ with $b \geq 3$ and T is a nonnegative odd integer.

Lemma 2.7 *Equation 2.2 has no solution of the form* $\beta = \prod_{j=1}^{r} p_j$ *with* $r > 1$.

Proof. If $p_j \neq 1+i$ for every j, then

$$k\prod_{j=1}^{r}\left[q(p_j)-1\right] = \prod_{j=1}^{r} q(p_j)-1.$$

Replacing $q(p_j)$ by $4k_j+1$, the preceding equation becomes

$$4^{r-1}k\prod_{j=1}^{r}k_j = \sum_{j=1}^{r}k_j + 4\sum_{\substack{j,l=1\\ j<l}}^{r} k_jk_l + 4^2\sum_{\substack{j,l,m=1\\ j<l<m}}^{r} k_jk_lk_m + \ldots + 4^{r-1}\prod_{j=1}^{r}k_j. \tag{2.6}$$

If k_j is an odd integer for some $1 \leq j \leq r$, then the left hand side of 2.6 is divisible by 4^{r-1} while its right hand side is not. If k_j is an even integer for every $1 \leq j \leq r$, that is $k_j = 2^{b_j}d_j$ where d_j is an odd integer, then equation 2.6 becomes

$$2^{e-s}k\prod_{j=1}^{r}k_j = T$$

where $e = 2r-2+\sum_{j=1}^{r} b_j$, $b_s = \min(b_1, b_2, \ldots, b_r)$ and T is an odd integer. Note that $e-s \geq r+1$.

3. Main Result

The following theorem summarizes the above section and characterizes completely the solutions to equations 2.1, 2.2 and 2.3 in the unique factorization domain $Z[i]$. It states that any solution to any equation must be a prime or a prime power.

Theorem 3.1 *Let* β *be a Gaussian integer of the form* $\beta = \prod_{j=1}^{r} {p_j}^{\alpha_j}$, *where* p_j *is prime in* $Z[i]$ *for every* $1 \leq j \leq r$. *Then*

(1) β *is a solution to equation 2.1 if and only if* $r = \alpha_1 = 1$, $p_1 = 1+i$ *and* $k = 3$.

(2) β *is a solution to equation 2.2 if and only if* $r = \alpha_1 = k = 1$.

(3) β *is a solution to equation 2.3 if and only if* $r = 1$, $p_1 = 1+i$, $\alpha \geq 1$ *and* $k = 2$.

4. Equations in $Z_p[x]$

In this section, the same previous equations are considered but in the domain of polynomial rings over finite fields $Z_p[x]$. Assume that $f(x)$ is a polynomial of degree n in $G = Z_p[x]$, and its factorization into distinct irreducible polynomials is $\prod_{j=1}^{r} h_j^{n_j}(x)$, where the degree of $h_j(x)$, $deg(h_j(x))$, is $m_j > 0$. The order of the group of units of the factor ring $G/ < f(x) >$ was given by El-Kassar [1] as follows:

$$\phi_G(f(x)) = \prod_{j=1}^{r} [q(h_j(x))]^{n_j-1} \left[q(h_j(x)) - 1\right]$$

with $q(h_j(x)) = p^{m_j}$. Hence,

$$\phi_G(f(x)) = p^s \prod_{j=1}^{r} (p^{m_j} - 1) \tag{4.1}$$

where $s = \sum_{j=1}^{r} m_j(n_j - 1)$.

Consider the equations

$$k\phi_G(f(x)) = q(f(x)) + 1 \tag{4.2}$$

$$k\phi_G(f(x)) = q(f(x)) - 1 \tag{4.3}$$

$$k\phi_G(f(x)) = q(f(x)) \tag{4.4}$$

Throughout this section, assume that $h_j(x)$ is an irreducible polynomial in $Z_p[x]$ of degree $m_j > 0$, $f(x) = \prod_{j=1}^{r} h_j^{n_j}(x)$ is a polynomial in $Z_p[x]$ of degree n and $t = \sum_{j=1}^{r} m_j n_j$.

Lemma 4.1 *$f(x)$ is a solution to 4.4 if and only if $f(x)$ is a product of powers of linear polynomials in $Z_2[x]$ with corresponding $k = 2^r$.*

Proof. Equation 4.4 gives

$$k \prod_{j=1}^{r} p^{m_j(n_j-1)}(p^{m_j} - 1) = p^t.$$

Hence,

$$k = \frac{p^{t'}}{\prod_{j=1}^{r} (p^{m_j} - 1)} \text{ with } t' = \sum_{j=1}^{r} m_j.$$

Note that p cannot be odd, so $p = 2$ and

$$k = \frac{2^{t'}}{\prod_{j=1}^{r} (2^{m_j} - 1)}.$$

It is seen easily that $m_j = 1$ for every j and $k = 2^r$. Since there are only two linear polynomials in $Z_2[x]$, then $r \leq 2$. The solutions are $\{x^{n_1}, (x+1)^{n_2}, x^{n_1}(x+1)^{n_2}\}$ with n_1 and n_2 are positive integers. The converse is straightforward.

Lemma 4.2 *If $f(x)$ is a solution to 4.2 or 4.3, then $f(x)$ is a square free polynomial in $Z_p[x]$.*

Proof. Using 4.2 and 4.3, we have

$$k\prod_{j=1}^{r} p^{m_j(n_j-1)}(p^{m_j}-1) - p^t = \pm 1.$$

This gives that

$$\gcd(p^t, \prod_{j=1}^{r} p^{m_j(n_j-1)}(p^{m_j}-1)) = 1.$$

Hence,

$$\prod_{j=1}^{r} p^{m_j(n_j-1)}(p^{m_j}-1) = 1$$

and $p^{m_j(n_j-1)} = 1$ for every j. Therefore $n_j = 1$ for every j.

Lemma 4.3 *$f(x)$ is a solution to $\phi_G(f(x)) = q(f(x)) - 1$ if and only if $f(x)$ is a power of an irreducible polynomial in $Z_p[x]$.*

Proof. If $k = 1$ in 4.3, then

$$1 = \prod_{j=1}^{r} p^{m_j n_j} - \prod_{j=1}^{r} p^{m_j(n_j-1)}(p^{m_j}-1). \tag{4.5}$$

It follows that

$$\gcd\left(p^s, p^{t'} \prod_{j=1}^{r}(p^{m_j}-1)\right) = 1,$$

where $t' = \sum_{j=1}^{r} m_j(n_j-1)$. Thus, $p^{t'} = 1$ and

$$p^{m_j(n_j-1)} = 1 \text{ for every } j.$$

Hence, $f(x)$ is a square free polynomial. Equation 4.5 gives

$$p^s - \prod_{j=1}^{r}(p^{m_j}-1) = 1,$$

where $s = \sum_{j=1}^{r} m_j$. Therefore $r = 1$ and p is any prime integer. The converse follows directly from the definition of $\phi_G(f(x))$ in $Z_p[x]$.

Lemma 4.4 *$f(x)=\prod_{j=1}^{r}h_j(x)$ is a solution to 4.2 if and only if $f(x)$ is a product of at most two irreducible polynomials in $Z_2[x]$ and $Z_3[x]$.*

Proof. If $r=1$, then

$$k=\frac{p^{m_1}+1}{p^{m_1}-1}=1+\frac{2}{p^{m_1}-1}.$$

Hence, $p^{m_1}-1$ must divide 2. So $m_1=1$ and $p=2$ or 3. If $r>1$, then

$$k=\frac{p^s+1}{\prod\limits_{j=1}^{r}(p^{m_j}-1)},$$

where $s=\sum_{j=1}^{r}m_j$. If p is odd prime integer, then $p\equiv 1\ (mod\ 4)$ or $p\equiv 3\ (mod\ 4)$. If $p\equiv 1\ (mod\ 4)$, then so is p^s for every integer s and p^s+1 has the form $4t+2$. Hence,

$$k=\frac{2T_1}{4^r\prod\limits_{j=1}^{r}t_j}=\frac{T_1}{2^{2r-1}T_2}, \tag{4.6}$$

with t_j, T_1 and T_2 are positive integers with T_1 is odd. For the case where $p\equiv 3\ (mod\ 4)$, we have

$$p^s\equiv\begin{cases}1\ (mod\ 4)\text{ if } s \text{ is even}\\ 3\ (mod\ 4)\text{ if } s \text{ is odd}\end{cases}.$$

For the case where s is even, consider the set $M=\{m_j|m_j\equiv 1\ (mod\ 2)\}$, then the order of M, $|M|$, is even and

$$k=\frac{4t'+2}{\prod\limits_{j=1}^{|M|}\left(4t_j+2\right)\prod\limits_{j=1}^{r-|M|}\left(4t'_j\right)}=\frac{2T_3}{2^{2r-|M|}\prod\limits_{j=1}^{|M|}\left(2t_j+1\right)\prod\limits_{j=1}^{r-|M|}t'_j}. \tag{4.7}$$

This contradicts that k is and integer since T_1 and T_3 are odd while the denominators of the expressions 4.6 and 4.7 are even. A similar procedure follows for the case where s is odd. Therefore, p must be an even prime. Now, if $r\geq 3$, then

$$k=\frac{2^s+1}{\prod\limits_{j=1}^{r}(2^{m_j}-1)}.$$

k is an integer if $m_j=1$ for at least 3 values of j and the only distinct linear irreducible polynomials in $Z_2[x]$ are x and $x+1$. Hence, $f(x)$ is divisible by x^2 or $(x+1)^2$ which contradicts lemma 4.2. For $r = 2$,

$$k = \frac{2^{m_1+m_2}+1}{(2^{m_1}-1)(2^{m_2}-1)} = 1 + \frac{2^{m_1}+2^{m_2}}{(2^{m_1}-1)(2^{m_2}-1)}.$$

This gives $m_1 = m_2 = 1$ or $m_1 = 1$ and $m_2 = 2$. Therefore, $f(x) \in \{x,\, x+1,\, x+2,\, 2x,\, 2x+1,\, 2x+2,\, x(x+1),\, x(x^2+x+1),\, (x+1)(x^2+x+1)\}$. The converse is immediate.

Note that the only quadratic irreducible polynomial in $Z_2[x]$ is x^2+x+1 and the only cubic irreducible polynomials in $Z_2[x]$ are x^3+x+1 and x^3+x^2+1.

Lemma 4.5 *Let $r > 1$, then $f(x)$ is a solution to 4.3 if and only if $f(x)$ is a product of at most three distinct irreducible polynomials in $Z_2[x]$.*

In the preceding lemma, $f(x) = x(x+1)$ when $r = 2$.

5. Characterizing the solutions

In this section, we consider the case where $f(x)$ is divisible by at most three distinct irreducible polynomials. The proof for the sufficient condition is straightforward and only the necessary condition is proved when necessary.

Lemma 5.1 *Let $f(x)$ be an irreducible polynomial. Then $f(x)$ is a solution to 4.2 if and only if it is a linear polynomial in $Z_2[x]$ or $Z_3[x]$.*

Proof. If $deg(f(x)) = n$, equation 4.2 becomes

$$k = 1 + \frac{2}{p^n - 1}.$$

Hence, $p^n = 2$ or 3. For $p^n = 2$, $f(x) = x$ or $x+1$ in $Z_2[x]$ with corresponding $k = 3$. For the second case, $f(x) \in \{x, x+1, x+2, 2x, 2x+1, 2x+2\}$ in $Z_3[x]$ with corresponding $k = 2$.

Lemma 5.2 *Equation 4.3 has an irreducible solution if and only if $k = 1$.*

In the following two lemmas, $f(x)$ is taken as a product of two irreducible polynomials.

Lemma 5.3 *$f(x) = h_1(x)h_2(x)$ is a solution to 4.2 if and only if $f(x) = x(x+1)$ in $Z_2[x]$ with $k = 5$.*

Lemma 5.4 *$f(x) = h_1(x)h_2(x)$ is solution to 4.3 if and only if $h_1(x)$ and $h_2(x)$ are linear polynomials in $Z_2[x]$ or $Z_3[x]$.*

Proof. Equation 4.3 results in

$$k(p^{m_1}-1)(p^{m_2}-1) = p^{m_1+m_2}-1.$$

Solving for k, we get

$$k = 1+\frac{1}{(p^{m_1}-1)}+\frac{1}{(p^{m_2}-1)}.$$

Hence, $p = 2$ and $m_1 = m_2 = 1$ with corresponding $k = 5$ or $p = 3$ and $m_1 = m_2 = 1$ with corresponding $k = 2$. The solutions are $x(x+1)$ in $Z_2[x]$, or $f(x) \in \{x(x+1), x(x+2), x(2x), x(2x+1), x(2x+2), 2x(x+1), 2x(x+2)\}$ in $Z_3[x]$.

Lemma 5.5 *$f(x) = h_1(x)h_2(x)h_3(x)$ is a solution to 4.3 if and only if $p = 2$ and*

a. $m_j = 2$ for exactly one j and $m_i = 1$ for $i \neq j$ with $k = 5$.

or

b. $m_i = i$ for $i = 1,2$ or 3 with $k = 3$.

6. Main Result

A complete characterization for the solutions to equations 4.2, 4.3 and 4.4 in $Z_p[x]$ is given in the next theorem.

Theorem 6.1 *Let $G = Z_p[x]$ and let $\prod_{j=1}^{r} h_j^{n_j}(x)$ be the factorization of $f(x)$ into distinct irreducible polynomials, where the deg $\big(h_j(x)\big) = m_j$. Then,*

(1) *$f(x)$ is a solution to equation 4.2 if and only if one of the following is true*

a. $p = 2, k = 3$ and $f(x) = x$ or $x+1$

b. $p = 3, k = 2$ and $f(x) \in \{x, x+1, x+2, 2x, 2x+1, 2x+2\}$.

c. $p = 2, k = 5$ and $f(x) = x(x+1)$.

d. $p = 2, k = 3$ and $f(x) =\in \{x(x^2+x+1), (x+1)(x^2+x+1)\}$.

2. *$f(x)$ is a solution to equation 4.3 if and only if one of the following is true*

a. p is any prime integer, $k = 1$ and $f(x) = h_1(x)$.

b. $p = 2$, $k = 5$ *and* $f(x) = x(x+1)$.

c. $p = 3$, $k = 2$ *and* $f(x) \in \{x(x+1), x(x+2), x(2x), x(2x+1),$
$x(2x+2)\}$.

d. $p = 2, m_j = 2$ *for exactly one* j *and* $m_i = 1$ *for* $i \neq j$ *with*
$k = 5$.

e. $p = 2, m_i = i$ *for* $i = 1,2,3$ *with* $k = 3$.

3. $f(x)$ *is a solution to equation 4.4 if and only if* $p = 2$ *and one of the following is true*

a. $k = 2$ *and* $f(x) = x^{n_1}$ *or* $(x+1)^{n_1}$.

b. $k = 4$ *and* $f(x) = x^{n_1}(x+1)^{n_2}$.

Conflict of Interests

The author declares that there is no conflict of interests.

References

[1] A.N. El-Kassar, Doctorate Dissertation, University of Southwestern Louisiana, 1991.

[2] D.H. Lehmer, On Euler's Totient Function, Bull. Amer. Math. Soc. 38 (1932), 745-751.

[3] I. Niven, H.S. Zuckerman, An Introduction to the theory of numbers, 5th edition John Wiley and Sons, New York, 1991.

[4] J.T. Cross, The Eulers ϕ-function in the Gaussian Integers, Amer. Math. Monthly 90 (1983), 518-528.