LEHMER'S TOTIENT PROBLEM AND CARMICHAEL NUMBERS IN A PID

JORDAN SCHETTLER

Abstract. Lehmer's totient problem consists of determining the set of positive integers n such that $\varphi(n)|n-1$ where φ is Euler's totient function. It is not obvious whether there are any composite n satisfying this divisibility condition; in fact, any such composite n is a Carmichael number (although every *known* Carmichael number doesn't actually have this property). We will generalize the above divisibility condition (with the cardinality [when finite] of the group of units in a quotient ring playing the role of $\varphi(n)$), construct a reasonable notion of Carmichael numbers in a PID and use a pair of handy short exact sequences to show how similar statements to those above follow in more generality. Also, we'll pick up a couple of generalizations for classical identities involving φ along the way. Included will be a generalization of the work of Korselt and an extension of the work of Alford, Granville and Pomerance.

1. Introduction

Euler's totient function φ is defined on $\mathbb{Z}^+$ by taking $\varphi(n)$ to be the number of positive integers less than or equal to and relatively prime to n. Lehmer's totient problem consists of determining the set of n such that $\varphi(n)|n-1$. Let P denote the set of primes in $\mathbb{Z}^+$. It is clear that $\varphi(p) = p-1|p-1$ for all $p \in P$ and that $\varphi(1) = 1|0 = 1-1$; however, it is not obvious whether there are any composite n satisfying this divisibility condition. It can be shown that

$$\varphi(n) = n \prod_{\substack{p|n \\ p\in P}} (1 - p^{-1})$$

for all $n \in \mathbb{Z}^+$. Define $K := \mathbb{Z}^+ \backslash (\{1\} \cup P)$ and $L := \{n \in K : \varphi(n)|n-1\}$. Using the product formula, one may easily deduce the following facts.

Fact 1.1. *If $n \in L$, then*

(1) *$n \in K$ is squarefree, and*
(2) *$p|n \Rightarrow p-1|n-1$ for all $p \in P$.*

Having these necessary conditions, one is lead to ask if there are any squarefree, composite $n \in \mathbb{Z}^+$ with $p-1|n-1$ for all primes p dividing n. Indeed, there are n having these properties, such integers being Carmichael numbers. More formally, a Fermat pseudoprime to base $a \in \mathbb{Z}$ is an integer $n \in K$ such that $a^n \equiv a (\text{mod } n)$; we then define a Carmichael number as a positive integer which is a Fermat pseudoprime to every integer base. Let C denote the set of Carmichael numbers. In 1899, Korselt established the following characterization of C.

Fact 1.2. *$n \in C \Leftrightarrow n \in K$ is squarefree, and $p|n \Rightarrow p-1|n-1$ for all $p \in P$.*

The inclusion $L \subseteq C$ follows immediately from 1.1 and 1.2, so that if C were finite, then L would be finite; however, it has been shown (in [1]) by Alford, Granville, and Pomerance, that there are, in fact, infinitely many Carmichael numbers. On the other hand, there are Carmichael numbers n such that $n \notin L$ (actually, this is true of every *known* Carmichael number), so the above containment is proper. For example, $1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number by the Korselt criterion since it is clearly squarefree, composite, and $6, 12, 18|1728$, but $\varphi(1729) = 6 \cdot 12 \cdot 18 = 2^4 \cdot 3^4$ does not divide $2^6 \cdot 3^3 = 1728$, so $1729 \notin L$.

Next we seek a generalization of Lehmer's totient problem and the notion of Carmichael numbers in a PID. We denote the sets of units, primes and (non-zero) zero divisors, in a ring Q (with identity) by $U(Q)$, $P(Q)$ and $Z(Q)$, respectively; additionally, we define $K_Q := Q \backslash (\{0\} \cup U(Q) \cup P(Q))$. Throughout, we let R be a PID.

2. A Few Preliminaries and Observations

Fact 2.1. *If $r \in R$, then*

(1) *$R/\langle r\rangle$ is the disjoint union $\{\langle r\rangle\} \cup U(R/\langle r\rangle) \cup Z(R/\langle r\rangle)$,*
(2) *$r \notin U(R) \Rightarrow U(R/\langle r\rangle) = \{s + \langle r\rangle \in R/\langle r\rangle : \gcd\{s, r\} = 1\}$, and*
(3) *$r \neq 0 \Rightarrow Z(R/\langle r\rangle) = \{z + \langle r\rangle \in R/\langle r\rangle : \langle r\rangle \subset \langle \gcd\{z, r\}\rangle \subset R\}$.*

Theorem 2.2. *Let $0 \neq r \in R$ and choose a set D of proper divisors of r (i.e., divisors of r which are neither units nor associates of r) such that every proper divisor of r is the associate of some unique element in D. Then the mapping*

$$\Phi : \bigcup_{d \in D} U(R/\langle d\rangle) \to Z(R/\langle r\rangle) : e + \langle d\rangle \mapsto e\frac{r}{d} + \langle r\rangle$$

is a bijection.

Proof. First, if $e_1 + \langle d_1\rangle = e_2 + \langle d_2\rangle \in \mathrm{Dom}(\Phi)$, then wlog $d_1 = d_2 \in D$ since the union is disjoint and associates in D are equal, so that $e_1 - e_2 = qd_1$ for some $q \in R$, and hence $e_1 r/d_1 - e_2 r/d_2 = qr$, giving $\Phi(e_1 + \langle d_1\rangle) = \Phi(e_2 + \langle d_2\rangle)$; thus Φ is well-defined. Secondly, if $e + \langle d\rangle \in \mathrm{Dom}(\Phi)$ with $d \in D$, then r/d is a gcd of $\{er/d, r\}$ since $\gcd\{e, d\} = 1$ by 2 in 2.1, but $\langle r\rangle \subset \langle d\rangle \subset R$, so that $\langle r\rangle \subset \langle r/d\rangle = \langle \gcd\{er/d, r\}\rangle \subset R$, and hence $\Phi(e + \langle d\rangle) \in Z(R/\langle r\rangle)$ by 3 in 2.1; thus Φ is into. Next, if $z + \langle r\rangle \in Z(R/\langle r\rangle)$, then we may choose a gcd g of $\{z, r\}$ with $r/d \in D$, so that by writing $z = eg$ for some $e \in R$, we get $1 = \gcd\{z/g, r/g\} = \gcd\{e, r/g\}$ while $\langle r\rangle \subset \langle \gcd\{z, r\}\rangle = \langle g\rangle \subset R$ by 3 in 2.1, and hence $\langle r\rangle \subset \langle r/g\rangle \subset R$, giving $e + \langle r/g\rangle \in \mathrm{Dom}(\Phi)$ with $\Phi(e + \langle r/g\rangle) = er/(r/g) + \langle r\rangle = z + \langle r\rangle$; thus Φ is surjective. Finally, if $\Phi(e_1 + \langle d_1\rangle) = \Phi(e_2 + \langle d_2\rangle)$ with $d_1, d_2 \in D$, then $e_1 r/d_1 - e_2 r/d_2 = qr$ for some $q \in R$, so that $e_1 d_2 - e_2 d_1 = qd_1 d_2$, and hence $d_1|d_2$ and $d_2|d_1$ since $\gcd\{e_1, d_1\} = 1 = \gcd\{e_2, d_2\}$ by 2 in 2.1, giving $d_1 = d_2$, which shows $e_1 - e_2 = qd_1$, so $e_1 + \langle d_1\rangle = e_2 + \langle d_2\rangle$; thus Φ is injective. Therefore Φ is a bijection. □

Note that if $r \in R$ and $R/\langle r\rangle$ is finite (as we shall later assume for $r \neq 0$), then $\langle r\rangle \subset \langle d\rangle \subset R \Rightarrow |R/\langle r\rangle| \geq |R/\langle d\rangle| \geq |U(R/\langle d\rangle)|$, so that

$$\sum_{\langle r\rangle \subset \langle d\rangle \subset R} |U(R/\langle d\rangle)| = |Z(R/\langle r\rangle)| = |R/\langle r\rangle \backslash (\{\langle r\rangle\} \cup U(R/\langle r\rangle))| = |R/\langle r\rangle| - |U(R/\langle r\rangle)| - 1$$

by 2.2 and 1 in 2.1. In this way, 2.2 generalizes the identity

$$\sum_{d|n} \varphi(d) = n$$

for each $n \in \mathbb{Z}^+$ since the above comments show that

$$\sum_{\substack{d|n \\ 1\neq d\neq n}} \varphi(d) = \sum_{n\mathbb{Z}\subset d\mathbb{Z}\subset\mathbb{Z}} |U(\mathbb{Z}/d\mathbb{Z})| = |\mathbb{Z}/n\mathbb{Z}| - |U(\mathbb{Z}/n\mathbb{Z})| - 1 = n - \varphi(n) - \varphi(1).$$

In 1932, Lehmer showed that any $n \in L$ must have at least 7 distinct prime factors, but this bound has since been improved to 14 (see [3]); we will use 2.2 to prove a similar statement in $F[x]$ where F is a finite field.

3. Useful Homomorphisms

Next, we review a series of mappings and decomposition properties (proofs some of these can found, for example, in [4]) which will be used to prove 1.1, 1.2, and the product formula for φ, in a more general setting.

Fact 3.1. *If $n, \alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{Z}^+$, and $p_1, p_2, \dots, p_n \in P(R)$ are pairwise non-associate, then*

(1) $R/\langle p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}\rangle \cong R/\langle p_1^{\alpha_1}\rangle \oplus R/\langle p_2^{\alpha_2}\rangle \oplus \cdots \oplus R/\langle p_n^{\alpha_n}\rangle$, *and*
(2) $U(R/\langle p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}\rangle) \cong U(R/\langle p_1^{\alpha_1}\rangle) \oplus U(R/\langle p_2^{\alpha_2}\rangle) \oplus \cdots \oplus U(R/\langle p_n^{\alpha_n}\rangle)$.

Fact 3.2. *If $r \in R$ and $\alpha \in \mathbb{Z}^+$, then*

$$\beta_1 : R/\langle r\rangle \to R/\langle r^\alpha\rangle : e + \langle r\rangle \mapsto er^{\alpha-1} + \langle r^\alpha\rangle$$

is a group monomorphism, and if, in addition, $r \notin U(R)$ and $\alpha > 1$, then

$$\beta_2 : R/\langle r\rangle \to U(R/\langle r^\alpha\rangle) : e + \langle r\rangle \mapsto 1 + er^{\alpha-1} + \langle r^\alpha\rangle$$

is a group monomorphism.

Fact 3.3. *If $d, r \in R$ and $d|r$, then*

$$\gamma_1 : R/\langle r\rangle \to R/\langle d\rangle : e + \langle r\rangle \mapsto e + \langle d\rangle$$

is a group epimorphism, and if, in addition, $d \notin U(R)$, then

$$\gamma_2 : U(R/\langle r\rangle) \to U(R/\langle d\rangle) : e + \langle r\rangle \mapsto e + \langle d\rangle$$

is a group epimorphism.

Fact 3.4. *If $r \in R$ and $\alpha \in \mathbb{Z}^+$, then*

$$0 \longrightarrow R/\langle r\rangle \xrightarrow{\beta_1} R/\langle r^\alpha\rangle \xrightarrow{\gamma_1} R/\langle r^{\alpha-1}\rangle \longrightarrow 0$$

is a short exact sequence, and if, in addition, $r \notin U(R)$ and $\alpha > 1$, then

$$0 \longrightarrow R/\langle r\rangle \xrightarrow{\beta_2} U(R/\langle r^\alpha\rangle) \xrightarrow{\gamma_2} U(R/\langle r^{\alpha-1}\rangle) \longrightarrow 0$$

is a short exact sequence.

4. Generalizations of L and C

Now we are ready to restate Lehmers totient problem in R. We know that $\mathbb{Z}/a\mathbb{Z}$ is finite for each $a \in \mathbb{Z}\backslash\{0\}$, and we analogously suppose that $R/\langle r\rangle$ is finite whenever $0 \neq r \in R$. If $n \in K$, then taking $R = \mathbb{Z}$ and $r = n$ in 2.1, we get $n \in L \Leftrightarrow |U(\mathbb{Z}/n\mathbb{Z})| = \varphi(n)|n-1 = |\mathbb{Z}/n\mathbb{Z}| - 1 = |U(\mathbb{Z}/n\mathbb{Z})| + |Z(\mathbb{Z}/n\mathbb{Z})| \Leftrightarrow |U(\mathbb{Z}/n\mathbb{Z})| \mid |Z(\mathbb{Z}/n\mathbb{Z})|$. In this way, we are motivated to make the definition $L_R := \{r \in K_R : |U(R/\langle r\rangle)| \mid |Z(R/\langle r\rangle)|\}$; we remove the primes in R from consideration since (as in $\mathbb{Z}$) such elements provide trivial satisfaction of the divisibility condition. We being by generalizing the product formula for φ stated in the introduction.

Theorem 4.1. *Let $0 \neq r \in R\backslash U(R)$. Then*

$$|U(R/\langle r\rangle)| = |R/\langle r\rangle| \prod_{\substack{\langle r\rangle\subseteq\langle p\rangle \\ p\in P(R)}} \left(1 - |R/\langle p\rangle|^{-1}\right).$$

Proof. Let $p \in P(R)$. We claim that $|U(R/\langle p^\alpha\rangle)| = |R/\langle p^\alpha\rangle|(1-|R/\langle p\rangle|^{-1})$ for all $\alpha \in \mathbb{Z}^+$, which we prove by induction. If $\alpha = 1$, then $|U(R/\langle p^\alpha\rangle)| = |U(R/\langle p\rangle)| = |R/\langle p\rangle| - 1 = |R/\langle p^\alpha\rangle|(1-|R/\langle p\rangle|^{-1})$ since $R/\langle p\rangle$ is a field. Now suppose $\alpha > 1$ and $|U(R/\langle p^{\alpha-1}\rangle)| = |R/\langle p^{\alpha-1}\rangle|(1-|R/\langle p\rangle|^{-1})$. Then setting $r = p$ in 3.4, we get

$$\begin{aligned}
|U(R/\langle p^\alpha\rangle)| &= |\mathrm{Ker}(\gamma_2)||U(R/\langle p^{\alpha-1}\rangle)| = |\mathrm{Im}(\beta_2)||U(R/\langle p^{\alpha-1}\rangle)| \\
&= |R/\langle p\rangle||U(R/\langle p^{\alpha-1}\rangle)| = |R/\langle p\rangle||R/\langle p^{\alpha-1}\rangle|(1-|R/\langle p\rangle|^{-1}) \\
&= |R/\langle p\rangle|(|R/\langle p^\alpha\rangle|/|\mathrm{Ker}(\gamma_1)|)(1-|R/\langle p\rangle|^{-1}) = |R/\langle p\rangle|(|R/\langle p^\alpha\rangle|/|\mathrm{Im}(\beta_1)|)(1-|R/\langle p\rangle|^{-1}) \\
&= |R/\langle p\rangle|(|R/\langle p^\alpha\rangle|/|R/\langle p\rangle|)(1-|R/\langle p\rangle|^{-1}) = |R/\langle p^\alpha\rangle|(1-|R/\langle p\rangle|^{-1}).
\end{aligned}$$

Now write $r = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$ where $u \in U(R)$, $n, \alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}^+$, and $p_1, p_2, \ldots, p_n \in P(R)$ are pairwise non-associate. Then using 3.1, we have

$$\begin{aligned}
|U(R/\langle r\rangle)| &= |U(R/\langle p_1^{\alpha_1}\rangle)|\cdots|U(R/\langle p_n^{\alpha_n}\rangle)| \\
&= |R/\langle p_1^{\alpha_1}\rangle|(1-|R/\langle p_1\rangle|^{-1})\cdots|R/\langle p_n^{\alpha_n}\rangle|(1-|R/\langle p_n\rangle|^{-1}) \\
&= |R/\langle r\rangle| \prod_{\substack{\langle r\rangle\subseteq\langle p\rangle \\ p\in P(R)}} \left(1 - |R/\langle p\rangle|^{-1}\right).
\end{aligned}$$

□

We now attempt to justify our definition of L_R with the following theorem, which is a generalization of 1.1.

Theorem 4.2. *If $r \in L_R$, then*

1. *$r \in K_R$ is squarefree, and*
2. *$p|r \Rightarrow |R/\langle p\rangle| - 1 \mid |R/\langle r\rangle| - 1$ for all $p \in P(R)$.*

Proof. Let $r \in L_R$, so that, by definition, $r \in K_r$. Suppose r is not squarefree. Then there is a $p \in P(R)$ such that $p^\alpha|r$ with $\alpha > 1$. Hence $|R/\langle p\rangle| \mid |U(R/\langle p^\alpha\rangle)|$ by 3.2, but $|U(R/\langle p^\alpha\rangle)| \mid |U(R/\langle r\rangle)|$ by 3.1 and also $|U(R/\langle r\rangle)| \mid |Z(R/\langle r\rangle)| = |R/\langle r\rangle| - 1 - |U(R\langle r\rangle)|$ by assumption and 1 in 2.1, so $|R/\langle p\rangle| \mid |R/\langle r\rangle| - 1$. On the other hand, $|R/\langle p\rangle| \mid |R/\langle p^\alpha\rangle| \mid |R/\langle r\rangle|$ by 3.2 and 3.1, which is a contradiction since $|R/\langle p\rangle| > 1$ because $p \in P(R)$. Next, if $p \in P(R)$ and $p|r$, then $|R/\langle p\rangle| - 1 = |U(R/\langle p\rangle)| \mid |U(R/\langle r\rangle)| \mid |R/\langle r\rangle| - 1$ by 3.1 and assumption since r is squarefree.
□

Next we prove a statement similar to the Korselt criterion in 1.2. First, for each $a \in R$ we define ${}_aF_R := \{r \in K_R : r | a^{|R/\langle r\rangle|} - a\}$, so that for $a \in \mathbb{Z}$, ${}_aF_{\mathbb{Z}}$ is the set of Fermat pseudoprimes to base a along with their negatives. Also, we once again exclude units and primes from consideration. It is then fitting to define $C_R := \{r \in R : r \in {}_aF_R \ \ \forall a \in R\}$ as an analog of C.

Theorem 4.3. *$r \in C_R \Leftrightarrow r \in K_R$ is squarefree, and $p|r \Rightarrow |R/\langle p\rangle| - 1 \ \mid \ |R/\langle r\rangle| - 1$ for all $p \in P(R)$.*

Proof. ($\Rightarrow$) First, suppose $r \in C_R$, so that $r \in K_R$ since $C_R \subseteq {}_1F_R \subseteq K_R$. If $p \in P(R)$ and $p|r$, then $r|p^{|R/\langle r\rangle|} - p$ while $|R/\langle r\rangle| > 1$ since $r \notin U(R)$, so p^2 does not divide r, giving that r is squarefree; also, $U(R/\langle p\rangle)$ is cyclic since $p \in P(R)$, so $|a + \langle p\rangle| = |U(R/\langle p\rangle)| = |R/\langle p\rangle| - 1$ for some $a + \langle p\rangle \in U(R/\langle p\rangle)$, but $p|r$ and $r|a^{|R/\langle r\rangle|} - a$ with $\gcd\{a, p\} = 1$, giving $p|a^{|R/\langle r\rangle|-1} - 1$, giving $a^{|R/\langle r\rangle|-1} + \langle p\rangle = 1 + \langle p\rangle$, so $|R/\langle p\rangle| - 1 = |a + \langle p\rangle| \ \mid \ |R/\langle r\rangle| - 1$. ($\Leftarrow$) Conversely, suppose $r \in K_R$ is squarefree, and $p|r \Rightarrow |R/\langle p\rangle| - 1 \ \mid \ |R/\langle r\rangle| - 1$ for all $p \in P(R)$. Let $a \in R$ and $p \in P(R)$ with $p|r$. Then $|R/\langle r\rangle| - 1 = q(|R/\langle p\rangle| - 1)$ for some $q \in R$. If p does not divide a, then $a + \langle p\rangle \in U(R/\langle p\rangle)$, so $a^{|R/\langle r\rangle|-1} + \langle p\rangle = a^{q(|R/\langle p\rangle|-1)} + \langle p\rangle = 1 + \langle p\rangle$, giving $p|a^{|R/\langle r\rangle|-1} - 1$ and $p|a^{|R/\langle r\rangle|} - a$; also, if $p|a$, then clearly $p|a^{|R/\langle r\rangle|} - a$. In either case, each prime divisor of r divides $a^{|R/\langle r\rangle|} - a$, so $r|a^{|R/\langle r\rangle|} - a$ since r is squarefree. Thus $r \in {}_aF_R$ for all $a \in R$, so $r \in C_R$. ☐

Corollary 4.4. *$L_R \subseteq C_R$.*

Proof. If $r \in L_R$, then $r \in K_R$, but r is squarefree and $|R/\langle p\rangle| - 1 \ \mid \ |R/\langle r\rangle| - 1$ for all primes p dividing r by 4.2, so $r \in C_R$ by 4.3. ☐

5. A Couple of Examples

Using the above results, we now examine L_R and C_R for some specific cases. First, let F be a field, so that $F[x]$ is a PID. Now let $f(x) \in F[x]$ with $n = \deg(f(x)) > 0$. Then the set $\{1 + \langle f(x)\rangle, x + \langle f(x)\rangle, \ldots, x^{n-1} + \langle f(x)\rangle\}$ forms a basis of $F[x]/\langle f(x)\rangle$ as an F-vector space. Hence $F[x]/\langle f(x)\rangle$ is finite for all nonzero $f(x) \Leftrightarrow F$ is finite. Accordingly, we now assume that F is finite.

Theorem 5.1. *Suppose $f(x) \in L_{F[x]}$ and $p(x) \in P(F[x])$. Then $p(x)|f(x) \Rightarrow \deg(p(x))|\deg(f(x))$.*

Proof. Suppose $p(x)|f(x)$, and let $m = \deg(p(x)), n = \deg(f(x))$ and $q = |F|$. Then $q^m - 1 = |F[x]/\langle p(x)\rangle| - 1 \ \mid \ |F[x]/\langle f(x)\rangle| - 1 = q^n - 1$, so $q^m - 1 = (q^m - 1, q^n - 1) = q^{(m,n)} - 1$, giving $m = (m, n)$, and hence $\deg(p(x)) = m|n = \deg(f(x))$. ☐

Now we use 2.2 to obtain a lower bound for the number of distinct prime factors of elements of $L_{F[x]}$.

Theorem 5.2. *Suppose $f(x) \in L_{F[x]}$. Then $f(x)$ has at least $\lceil \log_2(|F| + 1)\rceil$ distinct prime factors.*

Proof. First, $f(x) \notin U(F[x])$ and $f(x) \notin P(F[x])$, so using 2.2 gives

$$1 \le \frac{|Z(F[x]/\langle f(x)\rangle)|}{|U(F[x]/\langle f(x)\rangle)|} = \sum_{\langle f(x)\rangle \subset \langle d(x)\rangle \subset F[x]} \frac{|U(F[x]/\langle d(x)\rangle)|}{|U(F[x]/\langle f(x)\rangle)|}.$$

Now let $d(x)$ be a proper divisor of $f(x)$. Then $f(x)/d(x) \notin U(F[x])$, so $p(x)|f(x)/d(x)$ for some $p(x) \in P(F[x])$. Hence

$$|F|^{\deg(p(x))} - 1 = |U(F[x]/\langle p(x)\rangle)| \;\Big|\; |U(F[x]/\langle f(x)/d(x)\rangle)| = \frac{|U(F[x]/\langle f(x)\rangle)|}{|U(F[x]/\langle d(x)\rangle)|}$$

since $f(x)$ is squarefree by 4.3. Now $\deg(p(x)) > 0$ since $p(x)$ is prime, so

$$\frac{|U(F[x]/\langle d(x)\rangle)|}{|U(F[x]/\langle f(x)\rangle)|} \leq \frac{1}{|F|^{\deg(p(x))} - 1} \leq \frac{1}{|F| - 1},$$

but the number of proper divisors (up to associate) of $f(x)$ is $2^k - 2$ where k is the number of distinct prime factors of $f(x)$ again since $f(x)$ is squarefree, so summing over the last inequality gives

$$1 \leq \sum_{\langle f(x)\rangle \subset \langle d(x)\rangle \subset F[x]} \frac{1}{|F| - 1} = \frac{2^k - 2}{|F| - 1},$$

and hence $\log_2(|F| + 1) = \log_2(|F| - 1 + 2) \leq \log_2(2^k - 2 + 2) = k$. □

As mentioned above, it is unknown whether or not $L = \emptyset$; however, the following simple, yet important, example demonstrates that L_R isn't always empty.

Theorem 5.3. *There exists a PID R such that $L_R \neq \emptyset$.*

Proof. Consider $f(x) = x(x + 1) \in \mathbb{Z}/2\mathbb{Z}[x]$. Now $f(x)$ is clearly nonzero, nonunit, nonprime and of degree 2, while $x, x + 1 \in P(\mathbb{Z}/2\mathbb{Z}[x])$ are nonassociate and of degree 1. Hence, using 4.1, $|U(\mathbb{Z}/2\mathbb{Z}[x]/\langle f(x)\rangle)| = 2^2(1 - 1/2)(1 - 1/2) = 1$ divides every positive integer, so $f(x) \in L_{\mathbb{Z}/2\mathbb{Z}[x]}$. □

We now turn our attention to $C_{F[x]}$ and immediately obtain the following corollary of 4.3, which shows, in particular, that $C_{F[x]}$ is always nonempty.

Corollary 5.4. *Let $f(x) \in F[x]$ be a product of two or more pairwise nonassociate linear factors. Then $f(x) \in C_{F[x]}$.*

Proof. Write $f(x) = u(x - a_1) \cdots (x - a_k)$ for some $u, a_1, \ldots, a_k \in F$ where the a_is are distinct and $k > 1$. For each $i \in \{1, \ldots, k\}$, $x - a_i \in P(F[x])$ with $\deg(x - a_i) = 1$, so $|F[x]/\langle x - a_i\rangle| - 1 = |F| - 1 \mid |F|^k - 1 = |F[x]/\langle f(x)\rangle| - 1$. Therefore $f(x) \in C_{F[x]}$ by 4.3 since $f(x) \in K_{F[x]}$ is squarefree by construction. □

Next, we consider the Gaussian integers $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$. First, $\mathbb{Z}[i]$ is clearly a subring (with 1) of the field $\mathbb{C}$ of complex numbers, so that $\mathbb{Z}[i]$ is an integral domain. Also, the square modulus is a Euclidean norm on $\mathbb{Z}[i]$, so $\mathbb{Z}[i]$ is a Euclidean domain, and hence a PID. Also, if $0 \neq w \in \mathbb{Z}[i]$, then there are finitely many lattice points in the open disk centered at the origin with radius $|w|$ in the complex plane, so $\mathbb{Z}[i]/\langle w\rangle$ is finite. Next, we recall a few statements about $\mathbb{Z}[i]$.

Fact 5.5. $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Fact 5.6. *$P(\mathbb{Z}[i])$ is the disjoint union of the sets $\{a : |a| \in P \wedge a \equiv 3 \pmod 4\}$, $\{bi : |b| \in P \wedge b \equiv 3 \pmod 4\}$ and $\{a + ib \in \mathbb{Z}[i] \backslash (\mathbb{Z} \cup \mathbb{Z}i) : a^2 + b^2 \in P\}$.*

Fact 5.7. $|\mathbb{Z}[i]/\langle n\rangle| = n^2 \;\; \forall n \in \mathbb{Z}^+$.

It was commented above that C is infinite (see [1]). We now show that the corresponding statement holds in $\mathbb{Z}[i]$. We make use of some elementary number theory.

Theorem 5.8. *$C_{\mathbb{Z}[i]}$ is infinite.*

Proof. By Dirichlet's theorem on primes in arithmetic progression (or by a simpler argument with a weaker statement), we know that there are infinitely many primes in $\mathbb{Z}^+$ of the form $4n+1$. We claim that each such prime is in $C_{\mathbb{Z}[i]}$. Let $p = 4n+1 \in P \subseteq \mathbb{Z}[i]$, so that p is nonzero, nonunit by 5.5 and nonprime by 5.6 since $|p| = 4n+1 \equiv 1 \pmod 4$. Also, by Fermat's theorem, we know that $p = a^2+b^2 = (a+bi)(a-bi)$ for some $a, b \in \mathbb{Z}^+$, but then $a+bi, a-bi \in P(\mathbb{Z}[i])$ again by 5.6. It cannot be the case that $a = b$ since otherwise $a|p$ and $a = 1$ because $a < p$ with $p = 1+1 = 2$ not of the required form. On the other hand, the set of associates of $a+bi$ is, by 5.5, exactly $\{a+bi, -a-bi, -b+ai, b-ai\}$, so if $a-bi$ were an associate of $a+bi$, then $a-bi = b-ai$ since $b-ai$ is the only associate of $a+bi$ with a positive real part and a negative imaginary part because $a, b > 0$, but this is a contradiction since $a \neq b$. Thus, p is squarefree in $\mathbb{Z}[i]$, so $p^2 = |\mathbb{Z}[i]/\langle p\rangle| = |\mathbb{Z}[i]/\langle a+bi\rangle||\mathbb{Z}[i]/\langle a-bi\rangle|$ by 5.7 and 3.1, which gives $|\mathbb{Z}[i]/\langle a+bi\rangle| = p = |\mathbb{Z}[i]/\langle a-bi\rangle|$ since $\mathbb{Z}[i]/\langle a+bi\rangle$ and $\mathbb{Z}[i]/\langle a-bi\rangle$ are nontrivial and p is prime. Therefore $p \in C_{\mathbb{Z}[i]}$ by 4.3 since $|\mathbb{Z}[i]/\langle a \pm bi\rangle| - 1 = p-1|(p+1)(p-1) = p^2-1 = |\mathbb{Z}[i]/\langle p\rangle| - 1$. □

References

[1] W.R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, Ann. of Math., **140** (1994), 703-722.

[2] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Springer-Verlag, New York, 2001.

[3] A. Grytczuk and M. Wójtowicz, On a Lehmer problem concerning Euler's totient function, Proc. Japan Acad., Ser. A, **79** (2003), 136-138.

[4] T.W. Hungerford, *Algebra*, Springer, New York, 1974.

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