THE SET OF $k$-UNITS MODULO $n$

JOHN H. CASTILLO AND JHONY FERNANDO CARANGUAY MAINGUEZ

Abstract. Let $R$ be a ring with identity, $\mathcal{U}(R)$ the group of units of $R$ and $k$ a positive integer. We say that $a \in \mathcal{U}(R)$ is a $k$-unit if $a^k = 1$. Particularly, if the ring $R$ is $\mathbb{Z}_n$, for a positive integer $n$, we will say that $a$ is a $k$-unit modulo $n$. We denote with $\mathcal{U}_k(n)$ the set of $k$-units modulo $n$. By $du_k(n)$ we represent the number of $k$-units modulo $n$ and with $rdu_k(n) = \frac{\phi(n)}{du_k(n)}$, the ratio of $k$-units modulo $n$, where $\phi$ is the Euler phi function. Recently, S. K. Chebolu proved that the solutions of the equation $rdu_k(n) = 1$ are the divisors of 24. The main result of this work, is that for a given $k$, we find the positive integers $n$ such that $rdu_k(n) = 1$. Finally, we give some connections of this equation with Carmichael’s numbers and two of its generalizations: Knödel numbers and generalized Carmichael numbers.

S. K. Chebolu [2] proved that in the ring $\mathbb{Z}_n$ the square of any unit is 1 if and only if $n$ is a divisor of 24. This property is known as the diagonal property for the ring $\mathbb{Z}_n$. Later, K. Genzlinger and K. Lockridge [7] introduced the function $du(R)$, which is the number of involutions in $R$ (that is the elements in $R$ such that $a^2 = 1$), and provided another proof to Chebolu’s result about the diagonal property. The diagonal property also has been studied in other rings. For instance, S. K. Chebolu [4] found that the polynomial ring $\mathbb{Z}_n[x_1, x_2, \ldots, x_m]$ satisfies the diagonal property if and only if $n$ is a divisor of 12 and S. K. Chebolu et al. [3] also characterized the group algebras that verify this property.

Let $R$ be a ring with identity and $\mathcal{U}(R)$ the group of units of $R$. The aim of this paper is to study the elements of a ring with the following property: for a given $k \in \mathbb{Z}^+$, we say that an element $a$ in $\mathcal{U}(R)$ is a $k$-unit if $a^k = 1$. So, we ask for the number of this elements, and for that we extend the definitions of the functions given by K. Genzlinger and K. Lockridge [7], particularly $du_k(R)$ will represent the number of $k$-units of $R$. Here we present a formula for this function when $\mathcal{U}(R)$ can be expressed as a finite direct product of finite cyclic groups and when $R = \mathbb{Z}_n$. Furthermore, we study the case when $R = \mathbb{Z}_n$ and each unit is a $k$-unit. Previously, as mentioned before, this problem has been considered when $k = 2$ and more generally for fields and group algebras when $k$ is a prime number, see [3].

In the other hand, a well studied topic in number theory are the Carmichael’s numbers, which in terms of the $k$-unit concept, are composite positive integers such that any unit is an $(n - 1)$-unit. Here, we find some connections between the equation $rdu_k(n)$ and the concepts of Knödel and generalized Carmichael numbers.

In the sequel, for $x$ an element of a group $G$, by $|x|$ we denote the order of $x$. Besides, for a prime number $p$ and a positive integer $n$, the symbol $\nu_p(n)$ means the exponent of the greatest power of $p$ that divides $n$, $\gcd(a, b)$ denotes the greatest common divisor of $a$ and $b$, and $\phi$ is the Euler’s totient function. If $A = \{a_1, a_2, \ldots, a_n\}$ and $f$ is a defined function on $A$, we write

$$\prod_{a \in A} f(a) = f(a_1) \cdot f(a_2) \cdots f(a_n),$$

and when $A = \emptyset$, we assume that $\prod_{a \in A} f(a) = 1$.

1. SET OF $k$-UNITS OF A RING

In this section we give some definitions and get some preliminary results.
Definition 1. Let $R$ be a ring with identity, $a \in R$ and $k \in \mathbb{Z}^+$. We say that $a$ is a $k$-unit of $R$ if $a^k = 1$. We will denote with $\mathcal{U}_k(R)$ the set of $k$-units of $R$.

When $R = \mathbb{Z}_n$, for a given $n \in \mathbb{Z}^+$, we will use the symbol $\mathcal{U}_k(n)$ to denote the set of $k$-units of $\mathbb{Z}_n$, and we will call it the set of $k$-units modulo $n$.

Example 2. In $\mathbb{Z}_5$, when we square the elements of $\mathcal{U}(\mathbb{Z}_5)$ we have that
\[
1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 4, \quad 4^2 = 1.
\]

Then, the 2-units modulo 5 are 1 and 4, that is, $\mathcal{U}_2(5) = \{1, 4\}$.

We can verify that $\mathcal{U}_2(5)$ is a subgroup of $\mathcal{U}(\mathbb{Z}_5)$. Actually, this is a property for rings with an abelian unit group.

Theorem 3. Let $R$ be a ring with identity such that $\mathcal{U}(R)$ is an abelian group. Then $\mathcal{U}_k(R)$ is a subgroup of $\mathcal{U}(R)$.

Proof. It is sufficient to prove that if $a, b \in \mathcal{U}_k(R)$, then $ab^{-1} \in \mathcal{U}_k(R)$. Indeed, if $a^k = 1$ and $b^k = 1$, then $(ab^{-1})^k = a^k(b^k)^{-1} = 1$. \hfill \Box

When $\mathcal{U}_k(R)$ is a finite set, we will denote with $du_k(R)$ the number of $k$-units of $R$; that is,
\[
(1) \quad du_k(R) = |\mathcal{U}_k(R)|.
\]

Specially, if $R = \mathbb{Z}_n$, $du_k(n)$ will represents the number of $k$-units modulo $n$.

Although, in our definitions $k$ can be any positive integer, actually we could restrict it to the set of divisors of $|\mathcal{U}(R)|$, of course when the latter is finite. In fact, take $d = \gcd(k, |\mathcal{U}(R)|)$. If $x \in \mathcal{U}_k(R)$, then $x^k = 1$, and therefore the order of $x$ divides $k$. Moreover, as $|x|$ is a divisor of $|\mathcal{U}(R)|$, also divides $d$. Thus, $x^d = 1$, and then $x \in \mathcal{U}_d(R)$, which implies that $\mathcal{U}_k(R) \subseteq \mathcal{U}_d(R)$. Similarly, we can prove that if $x \in \mathcal{U}_d(R)$, then $x \in \mathcal{U}_k(R)$. So, we have proved that $\mathcal{U}_k(R) = \mathcal{U}_d(R)$, result that we summarize in the next proposition.

Proposition 4. Let $k$ be a positive integer and assume that $\mathcal{U}(R)$ is finite. Then
\[
\mathcal{U}_k(R) = \mathcal{U}_d(R),
\]
where $d = \gcd(k, |\mathcal{U}(R)|)$.

The following result is an special case of the previous one.

Theorem 5. If $\mathcal{U}(R)$ is a finite cyclic group, then $du_k(R) = \gcd(k, |\mathcal{U}(R)|)$.

Proof. Let $x \in \mathcal{U}_k(R)$ and $g$ a generator of $\mathcal{U}(R)$. So, there exists an integer $0 \leq l < |\mathcal{U}(R)|$ such that $x = g^l$.

Then, $x^k = g^{kl} = 1$ if and only if $kl \equiv 0 \pmod{|\mathcal{U}(R)|}$. The last congruence has $\gcd(k, |\mathcal{U}(R)|)$ solutions modulo $|\mathcal{U}(R)|$, see [9, Prop. 3.3.1]. Thus, $x$ takes $\gcd(k, |\mathcal{U}(R)|)$ values and, therefore, $du_k(R) = \gcd(k, |\mathcal{U}(R)|)$. \hfill \Box

We can give another proof to the Theorem 5 using the following property of the Euler’s $\phi$ function, $\sum_{e \mid d} \phi(e) = d$, see [9, Prop. 2.2.4].

Proof. Take $d = \gcd(k, |\mathcal{U}(R)|)$. Then $x \in \mathcal{U}_k(R) = \mathcal{U}_d(R)$ if and only if the order of $x$ divides $d$. Thus, the number of $k$-units in $R$ is equal to the number of elements of $\mathcal{U}(R)$ such that its order is a divisor of $d$. So,
\[
\begin{align*}
\text{du}_k(R) &= \text{du}_d(R) = |\{x \in \mathcal{U}(R) : |x| \text{ divides } d\}| \\
&= \sum_{e \mid d} |\{x \in \mathcal{U}(R) : |x| = e\}|.
\end{align*}
\]
As $e$ is a divisor of $d$, then it is also a divisor of $|\mathcal{U}(R)|$. Therefore, the number of elements of order $e$ in $\mathcal{U}(R)$ is $\phi(e)$, see [6, Thm. 4.4] and thus

$$d_{uk}(R) = \sum_{e|d} \phi(e) = d.$$  

Now we are interested in finding an expression to this function when the group $\mathcal{U}(R)$ is isomorphic to the direct product of finite cyclic groups. Here and subsequently $C_r$ denotes the cyclic group of order $r$.

In some occasions we will apply our definition of $k$-unit and the function $d_{uk}$, $p_{duk}$ and $r_{duk}$ for groups. Previously, it was unnecessary, because it might be ambiguous, for instance, $d_{uk}(\mathbb{Z}_n)$ could be understand as the quantity of $k$-units of a ring or a group.

**Theorem 6.** Let $R$ be a commutative ring with identity. If $\mathcal{U}(R) \cong C_{r_1} \times \cdots \times C_{r_s}$ for some positive integers $r_1, \ldots, r_s$, then

$$d_{uk}(R) = \prod_{i=1}^{s} \gcd(k, r_i).$$  

**Proof.** By the given isomorphism we get that $d_{uk}(R) = d_{uk}(C_{r_1} \times \cdots \times C_{r_s})$. Let $a$ be a $k$-unit of $R$ and $b$ its image under the isomorphism. Then $b$ is a $k$-unit of $C_{r_1} \times \cdots \times C_{r_s}$ if and only if each $i$-th component of $b$ is a $k$-unit in $C_{r_i}$. So, $d_{uk}(R) = d_{uk}(C_{r_1}) \cdots d_{uk}(C_{r_s})$. In this way, from Theorem 5, we obtain that $d_{uk}(R) = \gcd(k, |C_{r_1}|) \cdots \gcd(k, |C_{r_s}|)$, and the result follows. \qed

If $\mathcal{U}(R)$ is finite, we define the proportion and ratio functions of $k$-units of $R$, $p_{duk}(R)$ and $r_{duk}(R)$, respectively as follows

$$p_{duk}(R) = \frac{d_{uk}(R)}{|\mathcal{U}(R)|},$$  

$$r_{duk}(R) = \frac{|\mathcal{U}(R)|}{d_{uk}(R)} = \frac{1}{p_{duk}(R)}.$$  

When $\mathcal{U}(R)$ is an abelian group, Theorem 3 and Lagrange’s Theorem, see [6, Thm. 7.1], guarantee that $d_{uk}(R)$ divides $|\mathcal{U}(R)|$, and therefore $r_{duk}(R) \in \mathbb{Z}^+$. For the ring $\mathbb{Z}_n$, we will use $p_{duk}(n)$ and $r_{duk}(n)$ to denote the proportion and ratio functions of the $k$-units modulo $n$, respectively. Since $|\mathcal{U}(\mathbb{Z}_n)| = \phi(n)$, we have that

$$p_{duk}(n) = \frac{d_{uk}(n)}{\phi(n)}$$  

and

$$r_{duk}(n) = \frac{\phi(n)}{d_{uk}(n)}.$$  

**Example 7.** Previously, we got that $\mathcal{U}_2(5) = \{1, 4\}$. Thus,

$$d_{u2}(5) = |\mathcal{U}_2(5)| = 2, \quad p_{du2}(5) = \frac{d_{u2}(5)}{|\mathcal{U}(\mathbb{Z}_5)|} = \frac{1}{2}, \quad \text{and} \quad r_{du2}(5) = \frac{1}{p_{du2}(5)} = 2.$$

**2. The group of $k$-units modulo $n$**

In this section we find an expression for $d_{uk}(n)$ from the prime factorization of $n$.

The following theorem shows that the functions given by (1) and (2) are multiplicatives when $R = \mathbb{Z}_n$, which implies that the task is reduced to calculate $d_{uk}$ for powers of primes.

**Theorem 8.** The functions $d_{uk}$, $p_{duk}$ and $r_{duk}$ defined on $\mathbb{Z}_n$ are multiplicatives.
Proof. We will demonstrate that if $s$ and $t$ are relatively primes positives integers, then $\text{d}_k(st) = \text{d}_k(s) \text{d}_k(t)$.

By the Chinese Remainder Theorem, see [9, Thm. 1’, p. 35], we have that $\mathbb{Z}_{st} \cong \mathbb{Z}_s \times \mathbb{Z}_t$, so the number of $k$-units modulo $n$ is equal to the number of $k$-units in $\mathbb{Z}_s \times \mathbb{Z}_t$.

Let $(x, y) \in \mathbb{Z}_s \times \mathbb{Z}_t$ be a $k$-unit. Then $(x, y)^k = (x^k, y^k) = (1, 1)$ if and only if $x^k = 1$ in $\mathbb{Z}_s$ and $y^k = 1$ in $\mathbb{Z}_t$. Thus, $(x, y)$ is a $k$-unit of $\mathbb{Z}_s \times \mathbb{Z}_t$ if and only if $x$ is a $k$-unit modulo $s$ and $y$ is a $k$-unit modulo $t$. Therefore, $\text{d}_k(st) = \text{d}_k(Z_s \times Z_t) = \text{d}_k(s) \text{d}_k(t)$.

Since $\text{d}_k$ and $\phi$ are multiplicatives, we have that

\[
\text{p}_d u_k(st) = \frac{\text{d}_k(st)}{\phi(st)} = \left( \frac{\text{d}_k(s)}{\phi(s)} \right) \left( \frac{\text{d}_k(t)}{\phi(t)} \right) = \text{p}_d u_k(s) \text{p}_d u_k(t), \text{ and } \\
\text{r}_d u_k(st) = \frac{1}{\text{p}_d u_k(st)} = \left( \frac{1}{\text{p}_d u_k(s)} \right) \left( \frac{1}{\text{p}_d u_k(t)} \right) = \text{r}_d u_k(s) \text{r}_d u_k(t).
\]

\[\square\]

By the last theorem and with the aim of finding an expression to $\text{d}_k(n)$ using the prime factorization of $n$, we will consider when $n$ is a prime power. In order to apply the Theorem 6, we recall the following result, see [6, p. 160], which expresses $U(\mathbb{Z}_{p^\alpha})$ as an external direct product of cyclic subgroups, where $p$ is a prime number and $\alpha$ is a positive integer.

**Proposition 9.** Let $p$ be a prime number and $\alpha$ a positive integer. Then

\[
U(\mathbb{Z}_{p^\alpha}) \cong \begin{cases} 
C_1, & \text{if } p^\alpha = 2^1; \\
C_2, & \text{if } p^\alpha = 2^2; \\
C_2 \times C_{2^{\alpha-2}}, & \text{if } p = 2 \text{ and } \alpha \geq 3; \\
C_{\phi(p^\alpha)}, & \text{if } p \text{ is odd.}
\end{cases}
\]

**Theorem 10.** If $\alpha$ is a positive integer greater than or equal to 3, then

\[
\text{d}_k(2^\alpha) = \begin{cases} 
1, & \text{if } k \text{ is odd;} \\
2 \gcd(k, 2^{\alpha-2}), & \text{if } k \text{ is even.}
\end{cases}
\]

**Proof.** By Proposition 9, we have that $U(\mathbb{Z}_{2^\alpha}) \cong C_2 \times C_{2^{\alpha-2}}$. Applying Theorem 6, we get that $\text{d}_k(2^\alpha) = \gcd(k, 2) \gcd(k, 2^{\alpha-2})$.

\[\square\]

From theorems 5, 8 and 10 we obtain the following result.

**Theorem 11.** Assume that $n = 2^\alpha m$, where $\alpha$ is a non-negative integer and $m$ is an odd positive integer. If $m = \prod_{i=1}^r p_i^{r_i}$ is the prime factorization of $m$, then

\[
\text{d}_k(n) = \begin{cases} 
\prod_{i=1}^{r_i} \gcd(k, \phi(p_i^{r_i})) & \text{if } k \text{ is odd or } \alpha = 1; \\
2 \prod_{i=1}^{r_i} \gcd(k, \phi(p_i^{r_i})) & \text{if } k \text{ is even and } \alpha = 2; \\
2 \gcd(k, 2^{\alpha-2}) \prod_{i=1}^{r_i} \gcd(k, \phi(p_i^{r_i})) & \text{if } k \text{ is even and } \alpha \geq 3.
\end{cases}
\]

3. ON THE EQUATION $\text{r}_d u_k(n) = 1$

Recently, S. K. Chebolu [2] studied the positive integers $n$ such that each $u \in U(\mathbb{Z}_n)$ satisfies that $u^2 = 1$, which is equivalent to study the $n$’s that verify the equation $\text{r}_d u_2(n) = 1$. In this section, for a given positive integer $k$ we characterize the solutions of the equation $\text{r}_d u_k(n) = 1$, which clearly is an extension of the work made by S. K. Chebolu. As a consequence, at the end of the section we obtained a new proof of the principal result of S. K. Chebolu [2].

In general, we say that a ring satisfies the equation $\text{r}_d u_k(R) = 1$, if its unit group is equal to its $k$-units set; it means that, $a^k = 1$ for each $a \in U(R)$.

From Theorem 5, we get the result below.
Theorem 12. Let \( R \) be a ring such that \( \mathcal{U}(R) \) is a cyclic finite group. Then \( \text{rd}_k(R) = 1 \) if and only if \( |\mathcal{U}(R)| \) divides \( k \).

The following theorem gives a condition to a ring \( R \) to satisfy the equation \( \text{rd}_k(R) = 1 \) when \( \mathcal{U}(R) \) is isomorphic to a finite external direct product of finite cyclic groups.

Theorem 13. Let \( R \) be a commutative ring with identity such that \( \mathcal{U}(R) \cong C_{r_1} \times \cdots \times C_{r_s} \) for some positive integers \( r_1, \ldots, r_s \). Then, \( \text{rd}_k(R) = 1 \) if and only if \( r_i \) divides \( k \).

Proof. By the hypothesis \( |\mathcal{U}(R)| = \prod_{i=1}^{s} r_i \) and, from Theorem 6, we have that \( \text{du}_k(R) = \prod_{i=1}^{s} \gcd(k, r_i) \). Thus, \( \text{rd}_k(R) = 1 \) if and only if \( \prod_{i=1}^{s} \gcd(k, r_i) = \prod_{i=1}^{s} r_i \).

Since that \( \gcd(k, r_i) \leq r_i \), then \( \gcd(k, r_i) = r_i \), which happens only when each \( r_i \) divides \( k \). \( \square \)

In the following theorem, for a given positive integer \( n \), we give necessary and sufficient conditions on \( k \) such that \( \text{rd}_k(n) = 1 \).

Theorem 14. Assume that \( n = 2^\alpha m \), where \( \alpha \) is a non-negative integer and \( m \) is an odd positive integer. Then, \( \text{rd}_k(n) = 1 \) if and only if for each prime divisor \( p \) of \( m \) we have that \( \phi(p^{\nu_p(m)}) \) divides \( k \) and one of the following conditions is satisfied

(1) \( \alpha \in \{0, 1\} \),

(2) \( \alpha = 2 \) and \( k \) is even,

(3) \( 3 \leq \alpha \leq \nu_2(k) + 2 \).

Particularly, if \( k \) is odd then either \( n = 1 \) or \( n = 2 \).

Proof. The proof is straightforward from the fact that \( \text{rd}_k \) is multiplicative. Indeed, if the prime factorization of \( m \) is

\[ m = \prod_{p|m} p^{\nu_p(m)}, \]

we have that \( \text{rd}_k(n) = 1 \) if and only if \( \text{rd}_k(2^\alpha) = 1 \) and \( \text{rd}_k(p^{\nu_p(m)}) = 1 \) for each prime divisor \( p \) of \( m \).

Therefore, from Theorem 12, we obtain that \( \phi(p^{\nu_p(m)}) \) is a divisor of \( k \). Besides, \( \phi(2^\alpha) \) divides \( k \), when \( \alpha \leq 2 \), which demonstrates 1 and 2. On the other hand, if \( \alpha \geq 3 \), as \( \text{du}_k(2^\alpha) = 2^{\alpha-1} \), Theorem 10 implies that \( \alpha - 2 \leq \nu_2(k) \).

Conversely, we can prove that if \( \alpha \) satisfies the given conditions, then \( \text{rd}_k(2^\alpha) = 1 \).

Since \( \phi \) takes even values (except in 1 or 2), from the facts we have proved previously, then when \( k \) is odd, we get that either \( n = 1 \) or \( n = 2 \). \( \square \)

The above result allow us to conclude that the study of the equation \( \text{rd}_k(n) = 1 \), is relevant when \( k \) is even. We can now formulate our main result.

Theorem 15. Assume that \( k = 2^\beta M \), with \( \beta > 0 \) and \( M \) is an odd positive integer. Then \( \text{rd}_k(n) = 1 \) if and only if \( n \) is a divisor of

\[ 2^{\beta+2} \prod_{p \in \mathcal{A}} p \prod_{q \in \mathcal{B}} q^{\nu_q(M)+1}, \]

where

\[ \mathcal{A} := \left\{ p : p \text{ is prime, } p \nmid M \text{ and } p = 2^{l}d + 1, \text{ with } 0 < l \leq \beta \text{ and } d|M \right\}, \]

and

\[ \mathcal{B} := \left\{ q : q \text{ is prime, } q|M \text{ and } q = 2^{l}d + 1, \text{ with } 0 < l \leq \beta \text{ and } d|M \right\}. \]
Proof. Suppose that \( n = 2^\alpha m \), with \( m \) an odd integer and \( \alpha \) a non-negative integer. First of all, since \( k \) is even Theorem 14 guarantees the inequality \( 0 \leq \alpha \leq \beta + 2 \).

Additionally, Theorem 14 implies that \( \phi(t^{e(t)})|k \) for each prime divisor \( t \) of \( m \); that is

\[
\nu_t(m) - 1 | (t - 1)k. \tag{3}
\]

We will study the expression \( (3) \) in two cases, depending on whether or not \( t \) divides \( M \).

**Case 1.** Assume that \( t \) does not divide \( M \). Then, \( (3) \) implies that \( \nu_t(m) = 1 \) and \( t - 1 | k \). Thus,

\[
t - 1 = 2^l d,
\]

with \( 0 < l \leq \beta \) and \( d \) is a divisor of \( M \). The primes \( t \) that verify the last conditions are joined in the set \( A \) defined at the statement of the theorem.

**Case 2.** Suppose that \( t \) divides \( M \). Again, from \( (3) \) we obtain that \( \nu_t(m) - 1 \leq \nu_t(M) \) and \( t - 1 \) is a divisor of \( k \).

This means

\[
t - 1 = 2^l d,
\]

where \( 0 < l \leq \beta \) and \( d \) is a divisor of \( M \). These primes are the elements of the set \( B \) of the theorem.

Therefore, \( n \) is a solution of the equation \( rdu_k(n) = 1 \), if it has the form

\[
n = 2^\alpha \prod_{p \in A} p^{r(p)} \prod_{q \in B} q^{s(q)},
\]

with \( 0 \leq \alpha \leq \beta + 2 \), \( r(p) \in \{0, 1\} \) for each \( p \in A \) and \( 0 \leq s(q) \leq \nu_q(M) + 1 \) for each \( q \in B \). \qed

An immediate consequence of the above theorem is the following result.

**Corollary 16.** Assume that \( k = 2^\beta M \), with \( \beta > 0 \) and \( M \) an odd positive integer. Then, the number of solutions of \( rdu_k(n) = 1 \) is given by

\[
(\beta + 3)2^{\lvert A \rvert} \prod_{q \in B} (\nu_q(M) + 2),
\]

where \( A \) and \( B \) are as in the previous theorem.

**Theorem 15** allow us to obtain some well known results as we will see in the next section; specially here we give another proof of the principal result of S. K. Chebolu about the divisors of 24, see [2, Thm. 1.1].

**Corollary 17.** Let \( n \) be a positive integer. Then, \( n \) has the diagonal property if and only if \( n \) is a divisor of 24.

**Proof.** Suppose that \( n \) has the diagonal property, that is \( rdu_2(n) = 1 \). It is sufficient to find the sets \( A \) and \( B \) of the statement of Theorem 15. In fact, it is easy to check that \( A = \{3 = 2^1 \times 1 + 1\} \) and \( B = \emptyset \). Therefore, the solutions of the given equation are the divisors of \( 2^{1+2} \times 3 = 24 \).

For the reciprocal, it is enough to verify that \( rdu_2(n) = 1 \) when \( n \) is a divisor of 24. \qed

In the sequel, we give some examples.

**Example 18.** Take \( k = 10 = 2 \times 5 \). Then
\[
A = \{3 = 2^1 \times 1 + 1, 11 = 2^1 \times 5 + 1\} \text{ and } B = \emptyset.
\]

Thus, the roots of \( rdu_{10}(n) = 1 \) are the divisors of \( 2^{1+2} \times 3 \times 11 = 264 \).

In the proof of the Corollary 17 and in the above example \( B \) is empty; however, this not happen always as we can see in the next example.
Example 19. Consider \( k = 252 = 2^2 \times 3^2 \times 7 \). Then,
\[
\mathcal{A} = \{5, 13, 19, 29, 37, 43, 127\} \text{ and } \mathcal{B} = \{3, 7\},
\]
where, for instance, \( 3 = 2^1 \times 1 + 1 \) and \( 7 = 2^1 \times 3 + 1 \). Therefore, the solutions of \( \text{rdu}_{252}(n) = 1 \) are the divisors of
\[
2^4 \times 5 \times 13 \times 19 \times 29 \times 37 \times 43 \times 127 \times 3^3 \times 7^2 = 153185861359440,
\]
and there are \( 5 \times 2^7 \times (3 + 1) \times (2 + 1) = 7680 \) solutions.

4. Consequences and further work

Finally, in this section, we present how the results demonstrated previously serve to obtain some well-known results about Carmichael numbers \( A002997 \), and to establish some connections with two of its generalizations: Knödel numbers \( A033553, A050990, A050993 \) and generalized Carmichael numbers \( A014117 \), see [5, 8, 10, 12].

4.1. Carmichael numbers. Let \( a \) be a positive integer. We say that a composite number \( n \) is a pseudoprime base \( a \) if
\[
(4) \quad a^{n-1} \equiv 1 \pmod{n}.
\]
When we do not know whether \( n \) is composite or prime, but satisfies the congruence (4), we say that \( n \) is a probable prime base \( a \).

The next theorem gives the number of bases \( a \) in \( U(\mathbb{Z}_n) \) such that \( n \) is a probable prime base \( a \), see [5, p. 165]

**Theorem 20.** Let \( n \) be an odd positive integer. Then the number of bases \( a \) such that \( n \) is a probable prime base \( a \) is
\[
B_{pp}(n) = \prod_{p|n} \gcd(n - 1, p - 1).
\]

**Proof.** Let \( n = \prod_{p|n} p^{\nu_p(n)} \) be the prime factorization of \( n \). First, we observe that \( B_{pp}(n) = \text{du}_{n-1}(n) \). Then, from Theorem 11, we have that
\[
B_{pp}(n) = \text{du}_{n-1}(n) = \prod_{p|n} \gcd(n - 1, \phi(p^{\nu_p(n)})) = \prod_{p|n} \gcd(n - 1, p^{\nu_p(n)-1}(p - 1)).
\]
Since \( \gcd(n - 1, p) = 1 \), we obtain that
\[
B_{pp}(n) = \prod_{p|n} \gcd(n - 1, p - 1).
\]

\( \square \)

**Definition 21.** Let \( n \) be an odd composite integer. We say that \( n \) is a Carmichael number if \( a^{n-1} \equiv 1 \pmod{n} \) for each positive integer \( a \) relatively prime to \( n \).

Actually, \( n \) is a Carmichael number if it is composite and \( \text{rdu}_{n-1}(n) = 1 \). This allow us, to use the previous theorems to prove some known results about Carmichael numbers.

**Theorem 22.** Let \( n \) be an odd and composite integer and \( k \) relatively prime to \( n \). Then, \( \text{rdu}_{k}(n) = 1 \) if and only if \( n \) is squarefree and \( p - 1 \) divides \( k \) for each prime divisor \( p \) of \( n \).

**Proof.** Assume that \( n = \prod_{p|n} p^{\nu_p(n)} \) is the prime factorization of \( n \). By Theorem 15, we have that \( \text{rdu}_{k}(n) = 1 \) if and only if \( \phi(p^{\nu_p(n)}) = p^{\nu_p(n)-1}(p - 1) \) divides \( k \), which only happens when \( \nu_p(n) = 1 \) and \( p - 1 \) divides \( k \). \( \square \)
Corollary 23 (Korselt criterion). Suppose that $n$ is an odd and composite integer. Then, $n$ is a Carmichael number if and only if $n$ is squarefree and for each prime $p$ dividing $n$ we have $p - 1$ divides $n - 1$.

Proposition 24. Any Carmichael number has at least three prime factors.

Proof. Suppose that $n = pq$, with $p$ and $q$ different primes. As $\text{rdu}_{pq-1}(n) = 1$, then $\text{rdu}_{pq-1}(pq) = \text{rdu}_{pq-1}(p) \cdot \text{rdu}_{pq-1}(q) = 1$.

This implies $\text{rdu}_{pq-1}(p) = 1$ and $\text{rdu}_{pq-1}(q) = 1$. Now, since

$$\text{rdu}_{pq-1}(p) = \frac{\phi(p)}{\gcd(pq - 1, \phi(p))} = \frac{p - 1}{\gcd(pq - 1, p - 1)},$$

then $\gcd(pq - 1, p - 1) = p - 1$. Similarly, we can prove that $\gcd(pq - 1, q - 1) = q - 1$. Furthermore, we have that $\gcd(pq - 1, p - 1) = \gcd(pq - 1, q - 1)$ because $pq - 1 = (p - 1)(q - 1) + (p - 1) + (q - 1)$; that is $p - 1 = q - 1$, which is a contradiction. □

A. Makowski [10] gave an extension to the concept of Carmichael number, named Knödel numbers, in honour of the Austrian mathematician W. Knödel [11, p. 125].

Definition 25. For $i \geq 1$, let $K_i$ be the set of all the composite integers $n > i$ such that $a^{n-i} \equiv 1 \pmod{n}$ for any positive integer $a$ relatively prime to $n$. We call $K_i$ the $i$-Knödel set and its elements the $i$-Knödel numbers.

It is clear that, $K_1$ is the set Carmichael numbers. Similarly, as we did with the Carmichael numbers, we can give an interpretation of the Knödel sets from the concepts studied in this article; in fact, it is easy to stabilsh that $n \in K_i$ if and only if $n$ is composite and $\text{rdu}_{n-i}(n) = 1$.

For a fixed $k \in \mathbb{Z}^+$, using Theorem 15, we demonstrated that the set of solutions of the equation $\text{rdu}_k(n) = 1$ is finite. Although, this is not necessarily always true when $k$ depends on $n$; for instance $K_i$ is infinite, see [1, 10].

L. Halbeisen and N. Hungerbühler [8] proposed another generalization of the Carmichael number concept.

Definition 26. Fix an integer $k$, and let be

$$C_k = \{n \in \mathbb{N} : \min\{n, n + k\} > 1 \text{ and } a^{n+k} \equiv a \pmod{n} \text{ for all } a \in \mathbb{N}\}. $$

L. Halbeisen and N. Hungerbühler proved that $C_1 = \{2, 6, 42, 1806\}$ and $C_k$ is infinite if $1 - k > 1$ is squarefree. We can establish that for $k \in \mathbb{Z}$

$$C_k \subset \{n \in \mathbb{Z}^+ : \text{rdu}_{n+k-1}(n) = 1\}. $$

Therefore, the set $C_1$ joint with 1 are the solutions of $\text{rdu}_n(n) = 1$. Furthermore, expression (5) shows that when $1 - k > 1$ is squarefree, there are infinitely many solutions to the equation $\text{rdu}_{n+k-1}(n) = 1$.

In the sequel, we pose certain questions regarding the number of solutions of the equation $\text{rdu}_k(n) = 1$, when $k$ depends on $n$.

- Are there infinitely many $n \in \mathbb{Z}^+$ such that $\text{rdu}_{n+1}(n) = 1$?
  From Theorem 22, this question is equivalent to ask for the infinitude of positive square-free integers $n$ such that $p - 1$ divides $n + 1$ for each prime divisor $p$ of $n$.

  Let $i \in \mathbb{N}$ and $a, b \in \mathbb{Z}$

- Are there infinitely many $n \in \mathbb{Z}^+$ such that $\text{rdu}_{n+i}(n) = 1$?
• Are there infinite \( n \in \mathbb{Z}^+ \) such that \( rdu_{an+b}(n) = 1? \)

When \( b = 0 \), from Theorem 14, it is enough to take \( n \) as a power of 2.

• In general, are there infinitely many \( n \in \mathbb{Z}^+ \) such that \( rdu_{f(n)}(n) = 1 \), for a polynomial \( f(x) \) with integer coefficients? If the answer is negative, for which polynomials \( f(x) \) the equation \( rdu_{f(n)}(n) = 1 \) has infinite many solutions and for which has finite many solutions?

5. Acknowledgements

The authors are members of the research group: “Algebra, Teoría de Números y Aplicaciones, ERM”. J. H. Castillo was partially supported by the Vicerrectoría de Investigaciones Postgrados y Relaciones Internacionales at Universidad de Nariño. The authors also were partially supported by COLCIENCIAS under the research project “Aplicaciones a la teoría de la información y comunicación de los conjuntos de Sidon y sus generalizaciones (110371250560)”.

We are grateful to Professor Gilberto García-Pulgarín for his suggestions that help to improve this article.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, Ann. of Math. (2) 139(3) (1994), 703–722.
[2] S. K. Chebolu, What is special about the divisors of 24?, Math. Mag. 85(5) (2012), 366–372.
[3] S. K. Chebolu, K. Lockridge, and G. Yamskulna, Characterizations of Mersenne and 2-rooted primes, Finite Fields Appl. 35 (2015), 330–351.
[4] S. K. Chebolu and M. Mayers, What is special about the divisors of 127, Mathematics Magazine 86(2) (2013), 143–146.
[5] R. Crandall and C. Pomerance, Prime numbers. A computational perspective, Springer, New York, second edition, 2005.
[6] J. Gallian, Contemporary Abstract Algebra, Cengage Learning, Belmont, 7th edition.
[7] K. Genzlinger and K. Lockridge, Sophie Germain primes and involutions of \( \mathbb{Z}_n^* \), Involve 8(4) (2015), 653–663.
[8] L. Halbeisen and N. Hungerbühler, On generalized Carmichael numbers, Hardy-Ramanujan J. 22 (1999), 8–22.
[9] K. Ireland and M. Rosen, A classical introduction to modern number theory, Vol. 84 of Graduate Texts in Mathematics, Springer-Verlag, New York, second edition, 1990.
[10] A. Makowski, Generalization of Morrow’s \( D \) numbers, Simon Stevin 36 (1962/1963), 71.
[11] P. Ribenboim, The new book of prime number records, Springer-Verlag, New York, 1996.
[12] N. J. A. Sloane, The on-line encyclopedia of integer sequences, June published electronically at http://oeis.org.

2010 Mathematics Subject Classification: Primary 11A05, 11A07, 11A15, 16U60.

Keywords: Diagonal property, diagonal unit, unit set of a ring, \( k \)-unit, Carmichael number, Knödel number and Carmichael generalized number.

(Concerned with sequences A033553, A050990, A050993 and A014117.)

John H. Castillo, Departamento de Matemáticas y Estadística, Universidad de Nariño
E-mail address: jhcascillo@udenar.edu.co

Jhony Fernando Caranguay Mainguez, Departamento de Matemáticas y Estadística, Universidad de Nariño
E-mail address: jfernandomainguez@gmail.com