On Generalization Of The Carmichael Numbers

Abstract

In this paper we venture beyond the classical understanding of Carmichael numbers, a distinct category of composite numbers within number theory. The study first introduces a construction for the proposed generalization, aiming to provide a comprehensive extension of their traditional concept. Subsequently, we delve into a series of carefully curated examples that effectively demonstrate the proposed generalization's applicability and potential.

1 Introduction

In the field of elementary number theory, Fermat's Little Theorem is recognized as a pivotal result. It stipulates that for every prime number p, the equality

$$a^p \equiv a \pmod{p}$$

holds true for all integers a.

This theorem forms the basis of the rudimentary Fermat Compositeness Test, which postulates that if $a^n \not\equiv a \mod n$ for some integer a, then n is confirmed as composite. Despite the advantage of this test being computationally straightforward, a notable limitation arises when it fails to correctly determine the nature of some composite numbers n

For instance, if $n = 5731$ and $a = 5$, a calculation reveals that $5^{5731} \equiv 5 \pmod{5731}$. However, this inconclusive outcome is remedied by choosing a different integer, such as $a = 6$, which gives $6^{5731} \equiv 1832 \pmod{5731}$, thus proving that 5731 is composite $5731 = 11 \cdot 521$.

However, the occurrence of such fortuity is not universal. Certain composite numbers n exist that evade the Fermat Compositeness Test regardless of the chosen integer a. This leads us to the introduction of Carmichael numbers, a distinctive subset of composite numbers in number theory, which defy common composite number properties.

In its simplest form, a Carmichael number n, is a positive composite integer that satisfies the condition $a^{n-1} = 1 \pmod{n}$ for all integers a relatively prime to n. This property echoes Fermat's Little Theorem, which is typically associated with prime numbers, thereby underscoring the intriguing nature of Carmichael numbers in the landscape of pseudoprimes.

Additionally, in this work, the so-called Korselt's criterion plays a very crucial role. This criterion specifies the conditions under which a given integer is a Carmichael number. A positive composite integer n is a Carmichael number if and only if n is square-free, and for every prime divisor p of n, the condition $p - 1 \mid n - 1$ holds true. This criterion is important to us because in many generalizations of Carmichael numbers, a similar assertion is encountered in one way or another, as we will soon ascertain.

In the present study, we aim to extend the boundaries of the classical definition of Carmichael numbers, introducing a generalized version that pushes the confines of our current understanding. Throughout the process of defining the main constructions of the article, we will rely on the existing examples of various generalizations of Carmichael numbers. Our goal will be to create a language in which each of the considered examples can be described uniformly.

2 Main Idea

In this section, we present the main construction of the paper, based on a continuation of the ideas taken from the classical definition of Carmichael numbers.

Following the construction behind the Carmichael numbers, we might see that each natural number n is associated with a certain group, namely $(\mathbb{Z}/n\mathbb{Z})^\times$, and some integer $f(n) = n - 1$, in such a way that the whole construction satisfies important property:

For any prime number p and every choice of element $g \in (\mathbb{Z}/n\mathbb{Z})^\times$ the equality $g^{f(p)} = 1$ holds.

Subsequently, Carmichael numbers are defined as those which comply with the same condition, yet retain their composite nature.

The pathway towards generalization should be relatively apparent at this point. Specifically, alterations may be made to the corresponding groups and the function f. However, certain factors warrant careful consideration in the process. Primarily, the correspondence of groups must be done in a manner that transfers the properties of numbers and their relations, to a significant extent, onto the properties of corresponding groups and their respective relations. Secondly, the function f should not be irregular, it must be logically defined for primes and then naturally extended to composite numbers.

We will start with the choice of the groups. As we mentioned above, the choice must at some extent preserve relations within integers, so the most consistent way to accomplish that is choosing the right type of a functor. The most straightforward one is a functor from posetal category of $\mathbb{Z}$[1] to **Grp**, but as we will see in the examples, the better option of domain category is actually **CRing**, since the constructions from the examples we have considered are naturally defined not only on objects from posetal category of $\mathbb{Z}$, but rather on commutative rings. The category of commutative rings contains, in particular, the family $\mathbb{Z}/n\mathbb{Z}$, thus it encodes some relations of integers. Furthermore, it is initially tempting to postulate that the functor preserves limits. However, we aim to impose more rigorous constraints on the functor, namely we will assume that underlying **CRing** $\to$ **Set** functor of $\mathfrak{G}$ is representable. Despite the stringency, these restriction are consistent and validated by the examples.

The next step is defining the function f in a consistent manner for the selected functor $\mathfrak{G}$ in such a way, that it will provide the analogue of Fermat primality test. After that we should naturally define f over all integers.

3 Formal definitions

Definition 1. Let $\mathbf{C}$ be a locally small category. A functor $\mathfrak{F} : \mathbf{C} \to \mathbf{Set}$ is said to be representable if there is some object A of $\mathbf{C}$ such that the functor $\mathfrak{F}$ is naturally isomorphic to the hom-functor $\mathbf{h}^A = \mathbf{Hom}(A, -)$.

In particular, the functor $\mathbf{G}(R) = R^\times$ which participates in the definition of the classical Carmichael numbers is representable. The ring of Laurent polynomials $\mathbb{Z}[T, T^{-1}]$ together with natural isomorphism $\xi : \mathbf{h}^{\mathbf{A}} \to \mathfrak{G},\ \xi_R(f) = f(T)$ is a representation of $\mathfrak{G}$.

Theorem 1. The functor $\mathfrak{F} : \mathbf{CRing} \to \mathbf{Set}$ is representable iff there exists a system X of polynomial equations over $\mathbb{Z}$ with a variables $\{T_i\}_{i\in I}$ such that the functor $\mathfrak{V}_X : \mathbf{CRing} \to \mathbf{Set}$ defined by $\mathfrak{V}_X(R) = \{(r_i)_{i\in I} \mid r_i \in R,\ (r_i)_{i\in I} \in \mathbf{Sol}_R(X)\}$ is naturally isomorphic to $\mathfrak{F}$.

Proof. Consider the ideal $\mathfrak{a}$ in $\mathbb{Z}[T_i]_{i\in I}$, generated by all the equations from the system X. We are going to show, that there exists a natural isomorphism μ from $\mathfrak{V}_X$ to $\mathbf{Hom}(\mathbb{Z}[T_i]_{i\in I}/\mathfrak{a}, -)$.
Indeed, let R be a commutative ring and $(r_i)_{i\in I} \in \mathbf{Sol}_R(X)$, then there exists a homeomorphism $\mathbb{Z}[T_i]_{i\in I} \xrightarrow{\varphi} R$, which maps T_i to r_i for all $i \in I$. At this point it is clear to see, that $\ker\varphi \supset \mathbf{Sol}_R(X)$, this allows φ to be factored throught $\mathbb{Z}[T_i]_{i\in I}/\mathfrak{a} \to R$ and gives us homomorphism $\varphi' \in \mathbf{Hom}(\mathbb{Z}[T_i]_{i\in I}/\mathfrak{a}, R)$. So function μ_R maps $(r_i)_{i\in I}$ to φ'.
Conversely, suppose there is given a homomorphism $\varphi' : \mathbb{Z}[T_i]_{i\in I}/\mathfrak{a} \to R$. It uniquely determines a composite homomorphism $\varphi : \mathbb{Z}[T_i]_{i\in I} \to \mathbb{Z}[T_i]_{i\in I}/\mathfrak{a} \to R$ which sends T_i to r_i and $(r_i)_{i\in I} \in \mathbf{Sol}_R(X)$,

[1] Objects are elements of $\mathbb{Z}$ and arrows are divisibility relations.

because it filtrates through the φ' and $\mathbf{Sol}_R(X) \subset \ker \varphi'$.
It is easy to verify that the constructed mappings are mutually inverse, which proves that $\mathfrak{V}_X$ and $\mathbf{Hom}(\mathbb{Z}[T_i]_{i\in I}/\mathfrak{a}, -)$ are naturally isomorphic and thus $\mathfrak{V}_X$ is representable.
From the other side, let $\mathbf{A}$ be the commutative ring, that represents $\mathfrak{F}$. Then, there exists free ring $\mathbb{Z}[T_i]_{i\in I}$ and surjective homomorphism $\phi : \mathbb{Z}[T_i]_{i\in I} \twoheadrightarrow \mathbf{A}$. So we may conclude, that $\mathbf{A}$ is isomorphic to $\mathbb{Z}[T_i]_{i\in I}/\mathfrak{a}$, where $\mathfrak{a} = \ker \phi$. Clearly, from the ring $\mathbb{Z}[T_i]_{i\in I}$ and the ideal $\mathfrak{a}$ it is easy to reconstruct the system of equations X, and consequently, the functor $\mathfrak{V}_X$. □

Definition 2. A functor $\mathfrak{G} : \mathbf{CRing} \to \mathbf{Grp}$ such that the underlying set-valued functor is presentable is called *affine group over* $\mathbb{Z}$. Let $\mathfrak{G}_n$ denote $\mathfrak{G}(\mathbb{Z}/n\mathbb{Z})$.

We can also consider affine groups as group objects in the category of representable functors $\mathbf{CRing} \to \mathbf{Set}$.

Definition 3. We call a function $f : \mathbb{Z} \to \mathbb{N}$ *Fermat-suitable* if for each prime number p, the condition

$$\forall a \in \mathfrak{G}_p : a^{f(p)} = 1.$$

is satisfied.

One approach to constructing the function f is as follows: for each group $\mathfrak{G}_p$, we find its exponent, and thereafter, it usually becomes clear how exactly the function f should be defined for all positive integers.

Now we may advance to the definition of the Carmichael numbers of this particular construction.

Definition 4. Let $\mathfrak{G}$ be an affine group over $\mathbb{Z}$ and let f be a Fermat-suitable function. Then, ($\mathfrak{G}$,f)-*Carmichael number* is a positive composite integer n that satisfies the condition:

$$\forall a \in \mathfrak{G}_n : a^{f(n)} = 1.$$

Upon establishing the construction, it becomes compelling to investigate the inherent properties of the $(\mathfrak{G}, f)$-Carmichael numbers.

4 Examples

In this section we will look at some examples of affine groups.

Example 1. $\mathfrak{G}(R) = \left(R[x]\Big/(x^2+1)\right)^\times = R[i]^\times$ and $i^2 = -1$.

Now we will describe the invertible elements in $R[i]$.

Let $x \in R[i]$ then $x = a + bi$ and $a, b \in R$.
Consider the monoid homomorphism $R[i]^* \xrightarrow{N} R^*$, that is given by the formula $N(a+bi) = a^2 + b^2$. Let's check that N is homomorphism. By definition, put $\overline{x} = a - bi$. It is easy to check that $N(x) = x\overline{x}$ hence, $N(xy) = xy\overline{xy}$. We get that N is a homomorphism iff $\overline{xy} = \overline{x} \cdot \overline{y}$. Last equality can be proved trivially.

Lemma 1. $x \in R[i]$ invertible if and only if $N(x)$ is invertible in R.

Proof.

1. $\Longrightarrow : x \in R[i]^\times,\ N - homomorphism \implies N(x^{-1}) = N(x)^{-1} \implies N(x) \in R^\times$.
2. $\Longleftarrow : N(x) \in R^\times \iff x\overline{x} \in R^\times \implies N(x)^{-1}x\overline{x} = 1 \iff (N(x)^{-1}\overline{x})x = 1 \implies x \in R[i]^\times$.

□

Now we can easily see that the pair (A, ξ) such that $A = \dfrac{\mathbb{Z}[T_1, T_2, T_3]}{\langle T_1^2 T_3 + T_2^2 T_3 - 1\rangle}$ and $\xi_R(f) = f(T_1) + f(T_2)i$ is a representation of the functor.

In this case $\exp(\mathfrak{G}_p) = \begin{cases} 2 & \text{if } p = 2 \\ p-1 & \text{if } p \equiv 1 \pmod 4 \\ p^2-1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$

Then f can be naturally extended to positive integers as follows: $f(n) = 2(n^2 - 1)$.

Using brute force algorithm we found the first 10 ($\mathfrak{G}$,f)-*Carmichael numbers*:

$$\begin{aligned} 15 &= 3 \cdot 5 & 35 &= 5 \cdot 7 \\ 51 &= 3 \cdot 17 & 65 &= 5 \cdot 13 \\ 85 &= 5 \cdot 17 & 91 &= 7 \cdot 13 \\ 119 &= 7 \cdot 17 & 221 &= 13 \cdot 17 \\ 255 &= 3 \cdot 5 \cdot 17 & 377 &= 13 \cdot 29 \end{aligned}$$

Example 2. $\mathfrak{G}(R) = \left(R[x]\Big/(x^2+x+1)\right)^\times = R[\omega]^\times$ and $\omega^2 = -1 - \omega$.

Now we will describe the invertible elements in $R[\omega]$.

Let $x \in R[\omega]$ then $x = a + b\omega$ and $a, b \in R$.
Consider the monoid homomorphism $R[\omega]^* \xrightarrow{N} R^*$, that is given by the formula $N(a+b\omega) =$
$= a^2 + b^2 - ab$. Let's check that N is homomorphism. By definition, put $\overline{x} = a + b(-1-\omega) = a + b\omega^2$. It is easy to check that $N(x) = x\overline{x}$ hence, $N(xy) = xy\overline{xy}$. We get that N is a homomorphism iff $\overline{xy} = \overline{x} \cdot \overline{y}$. Last equality can be proved trivially.

Lemma 2. $x \in R[\omega]$ invertible if and only if $N(x)$ is invertible in R.

Proof.

1. $\Longrightarrow : x \in R[\omega]^\times,\ N - homomorphism \implies N(x^{-1}) = N(x)^{-1} \implies N(x) \in R^\times$.
2. $\Longleftarrow : N(x) \in R^\times \iff x\overline{x} \in R^\times \implies N(x)^{-1}x\overline{x} = 1 \iff (N(x)^{-1}\overline{x})x = 1 \implies x \in R[\omega]^\times$.

□

In this example the representation of the functor is $A = \dfrac{\mathbb{Z}[T_1, T_2, T_3]}{\langle T_1^2 T_3 + T_2^2 T_3 - T_1 T_2 T_3 - 1\rangle}$ and $\xi_R(f) = f(T_1) + f(T_2)\omega$.

In this case $\exp(\mathfrak{G}_p) = \begin{cases} 6 & \text{if } p = 3 \\ p-1 & \text{if } p \equiv 1 \pmod 3 \\ p^2-1 & \text{if } p \equiv 2 \pmod 3 \end{cases}$.

Then f can be naturally extended to positive integers as follows: $f(n) = 3(n^2-1)(n-1)$.

Example 3. $\mathfrak{G}(R) = \left(R[x]/(x^2)\right)^\times = R[\epsilon]^\times$ and $\epsilon^2 = 0$.

Now we will describe the invertible elements in $R[\epsilon]$.
Let $x \in R[\epsilon]$ then $x = a + b\epsilon$ and $a, b \in R$.

Lemma 3. $x \in R[\epsilon]$ invertible if and only if a is invertible in R.

Proof.

1. $\Longrightarrow : x = a + b\epsilon \in R[\epsilon]^\times \implies \exists x^{-1} = c + d\epsilon \implies (a + b\epsilon)(c + d\epsilon) = ac + (dc + ad)\epsilon = 1 \implies ac = 1 \implies a \in R^\times$.
2. $\Longleftarrow : a \in R^\times, b \in R, x = a + b\epsilon \implies x^{-1} = a^{-1}(1 + a^{-1}b\epsilon) \implies x \in R[\epsilon]^\times$.

□

The representation of the functor is $A = \dfrac{\mathbb{Z}[T_1, T_2, T_3]}{\langle T_1 T_3 - 1\rangle}$ and $\xi_R(f) = f(T_1) + f(T_2)\epsilon$.

In this case $\exp(\mathfrak{G}_p) = p(p-1)$.

Then f can be naturally extended to positive integers as follows: $f(n) = n(n-1)$.

In the most comprehensive generality, examples employing polynomials can be articulated as follows.

Example 4. For any monic polynomial $f \in \mathbb{Z}[x]$ we define $\mathfrak{G}(R) = \left(R[x]/(f)\right)^\times$.

Now we shall proceed to the subsequent series of examples related to rings of polynomials.

Example 5. The functor $\mathfrak{G} = \mathbb{GL}_k$ is representable for every natural k. We can check that the representation is $A = \dfrac{\mathbb{Z}[T_1, ..., T_{k^2+1}]}{\langle Det(T_1, ...T_{k^2})T_{k^2+1} - 1\rangle}$[2] and $\xi_R(f) = \begin{pmatrix} f(T_1) & \cdots & f(T_k) \\ \vdots & \ddots & \vdots \\ f(T_{k^2-k+1}) & \cdots & f(T_{k^2}) \end{pmatrix}$.

This affine group, along with the corresponding series of Carmichael numbers, was examined in [1].

In this case $\exp(\mathfrak{G}_\mathfrak{p}) = p^{\lceil \log_p k \rceil} \prod_{m=1}^{k} \Phi_m(p)$, where $\Phi_m(p)$ is a mth cyclotomic polynomial.

Then f can be naturally extended to positive integers as follows: $f(n) = n^{\lceil \log_n k \rceil} \prod_{m=1}^{k} \Phi_m(n)$.

Now, let us consider a more particular example.

Example 6. $\mathfrak{H}(R) = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \middle| \, a \in R^\times, b \in R \right\}$.

In this example $A = \mathbb{Z}[T_1, T_1^{-1}T_2]$, $\xi_R(f) = \begin{pmatrix} f(T_1) & f(T_2) \\ 0 & 1 \end{pmatrix}$ and thus (A, ξ) is a representation of $\mathfrak{H}$.

[2] $Det(T_1, ..., T_{k^2})$ denotes $Det \begin{pmatrix} T_1 & \cdots & T_k \\ \vdots & \ddots & \vdots \\ T_{k^2-k+1} & \cdots & T_{k^2} \end{pmatrix}$

Now will show, that in this case $\exp(\mathfrak{H}_\mathfrak{p}) = p(p-1)$.

Consider the element $h_1^n = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} a^n & 0 \\ 0 & 1 \end{pmatrix}$, where $\mathrm{ord}(a) = p-1$. It shows, that $h_1^n = 1$ only if $p-1 \mid \exp(\mathfrak{H}_\mathfrak{p})$. The next element $h_2^n = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $h_2^n = 1$ only if $p \mid \exp(\mathfrak{H}_p)$. In respect that $\gcd(p, p-1) = 1$ and $|\mathfrak{H}_p| = p(p-1)$ we get $\exp(\mathfrak{H}_p) = p(p-1)$.

So the function f can be naturally extended to positive integers as follows: $f(n) = n(n-1)$.

Remark 4.1. Note also that for any ring R the group $\mathfrak{H}(R)$ is a subgroup of $\mathfrak{G}(R)$ (for $k = 2$) in a natural way. It means that there exists a morphism of affine groups $i : \mathfrak{H} \to \mathfrak{G}$. Evidently, the diagram below is commutative for any $R, N \in \mathbf{CRing}$ and any homomorphism $f : R \to N$.

$$\begin{array}{ccc} \mathfrak{H}(R) & \xrightarrow{\mathfrak{H}[f]} & \mathfrak{H}(N) \\ \downarrow{\scriptstyle i_R} & & \downarrow{\scriptstyle i_N} \\ \mathfrak{G}(R) & \xrightarrow{\mathfrak{G}[f]} & \mathfrak{G}(N) \end{array}$$

Since all i_R are injective, we should conclude, that for all primes $p \exp(\mathfrak{H}_p) \mid \exp(\mathfrak{G}_p)$ and a quick calculation confirms that: $p(p-1) \mid p(p^2-1)$.

5 Conclusion

In conclusion, we would like to note that at this stage, the construction we propose is overly flexible and requires much more work than we initially anticipated. Some aspects of it also need to be reconsidered. For example, we could shift from considering positive integers to the consideration of ideals, which may pave the way for studying so-called Carmichael ideals in an arbitrary commutative ring. With such a transition, the category **CRing** (of commutative $\mathbb{Z}$-algebras / commutative rings) is replaced by the category R-**CAlg** (of commutative R-algebras), thus considering affine groups over R. The greatest difficulties, however, will arise in the attempt to find an analogue of the object for the Fermat-suitable function f. Most likely, such a transition will require a complete revision of the constructions associated with the function f.
Additionally, it should be noted that affine groups are closely related to affine schemes. This, hypothetically, could introduce geometric imagery and tools into the problem being considered, and may also suggest new possibilities for defining a construction to replace the one with f.

In closing, this work has laid a foundation for the advanced understanding of Carmichael numbers. Through an generalization approach and analysis of examples, we have sought to broaden the conceptual framework around these intriguing mathematical entities. While the study of Carmichael numbers themselves is an endeavor for future research, the groundwork established in this paper serves as a significant stepping stone towards that goal. We trust that this foundational work will inspire further studies and lively discussions within the mathematical community, advancing our collective comprehension of these fascinating constructs.

References

[1] Eugene Karolinsky and Dmytro Seliutin (2020) *Carmichael numbers for GL(m).*

[2] J.S. Milne (2012) *Basic Theory of Affine Group Schemes.*