Journal of Integer Sequences, Vol. 29 (2026),
Article 26.2.4

On the Number of Regular Integers Modulo n and Its Significance for Cryptography

Klaus Dohmen and Mandy Lange-Geisler
Fachgruppe Mathematik
Hochschule Mittweida
Technikumplatz 17
09648 Mittweida
Germany
dohmen@hs-mittweida.de
mlange1@hs-mittweida.de

Abstract

We present four combinatorial proofs of Morgado's formula for the number $\varrho(n)$ of non-congruent regular integers modulo n, corresponding to sequence A055653 in the On-Line Encyclopedia of Integer Sequences (OEIS), where an integer m is said to be *regular modulo* n if the congruence $m^2x \equiv m \pmod{n}$ has a solution $x \in \mathbb{Z}$. To illustrate the significance of the sequence and Morgado's formula, we relate them to a recent multi-prime, multi-power generalization of the RSA cryptosystem.

1 Introduction

This work is motivated by a recent multi-prime, multi-power generalization of the RSA cryptosystem [3], where the modulus is an arbitrary integer $n > 1$ and the messages are regular integers modulo n. The number of regular integers m in $\mathbb{Z}_n = \{0, \ldots, n-1\}$ is crucial for estimating the probability of correct decryption in this generalized scheme for random messages m from the larger message space $\mathbb{Z}_n$.

Throughout this work, $\mathbb{N}$ denotes the set of positive integers. For $n \in \mathbb{N}$, the notion of a regular integer modulo n, introduced by Morgado [5], is closely related to the algebraic concept of a von Neumann regular element. Recall that, for a ring R, an element $m \in R$ is called *von Neumann regular* if there exists an element $x \in R$ such that $mxm = m$.

Definition 1 (Morgado [5]). For each $n \in \mathbb{N}$, an integer m is said to be *regular modulo* n if the congruence $m^2x \equiv m \pmod{n}$ has a solution $x \in \mathbb{Z}$.

For each $n \in \mathbb{N}$, we use $\mathbb{Z}_n^{\mathrm{reg}}$ to denote the set of all $m \in \mathbb{Z}_n$ that are regular modulo n, and $\varrho(n)$ to denote its cardinality. The sequence $(\varrho(n))_{n\geq 1}$ appears as sequence A055653 in the On-Line Encyclopedia of Integer Sequences (OEIS) [6]. It was first studied by Morgado [5] and has since been investigated by several authors [1, 2, 8].

Recall that $d \in \mathbb{N}$ is called a *unitary divisor* of n if d divides n and $\gcd(d, n/d) = 1$. Following Morgado [5], we write $d \,|^* n$, if d is a unitary divisor of n. Our focus is on the following formula, in which φ denotes Euler's totient function.

Theorem 2 (Morgado [5]). *For every* $n \in \mathbb{N}$,

$$\varrho(n) = \sum_{d \,|^* n} \varphi(d). \tag{1}$$

In this paper, we provide four proofs of (1). Unlike previously published proofs [1, 8], the proofs presented here are combinatorial in nature and do not rely on the multiplicativity of ϱ. Instead, we repeatedly use the bijection principle and, in our final proof, the inclusion-exclusion principle. Continuing along this line of reasoning, the multiplicativity of ϱ follows naturally from (1).

The paper is organized as follows. In Section 2 we provide a concise proof of Morgado's [5] characterization of regular integers modulo n, which we use in our proofs of Morgado's formula (1) in Sections 3–6. Each of our four combinatorial proofs is self-contained and sheds a different light on the formula. From the authors' perspective, the purely bijective proof in Section 4 is particularly noteworthy, as it yields an encoding of the regular integers modulo n and may provide further insight into the study of the sequence A055653.

In Section 7, we relate this sequence and Morgado's formula to the probability of correct decryption of a random message $m \in \mathbb{Z}_n$ in a multi-prime, multi-power generalization of the RSA cryptosystem, recently established by the present authors [3].

2 Preliminaries

The following proposition, which is due to Morgado [5], provides necessary and sufficient conditions for an integer m to be regular modulo n. To keep this paper self-contained, we provide our own concise proof.

Proposition 3 (Morgado [5]). *For all* $n \in \mathbb{N}$ *and* $m \in \mathbb{Z}$, *the following statements are equivalent:*

(a) m *is regular modulo* n,

(b) $\gcd(m^2, n) = \gcd(m, n)$,

(c) $\gcd(m,n) \,|^* n$.

Proof.

(a) $\Leftrightarrow$ (b): In general, for every $a, b \in \mathbb{Z}$, the congruence $ax \equiv b \pmod{n}$ has a solution $x \in \mathbb{Z}$ if and only if $\gcd(a,n) \mid b$. Hence, m is regular modulo n if and only if $\gcd(m^2,n) \mid m$, which in turn holds if and only if $\gcd(m^2,n) = \gcd(m,n)$.

(b) $\Rightarrow$ (c): Let $d = \gcd(m,n)$ and $g = \gcd(d, n/d)$. By induction on k we show that $g^k \mid d$ for all $k \geq 0$, which implies $g = 1$ and thus (c). The case $k = 0$ is trivial. For the induction step, assume that $k > 0$ and $g^{k-1} \mid d$. Then, $g^k \mid dg = \gcd(d^2, dn/d) \mid \gcd(m^2,n) = \gcd(m,n) = d$.

(c) $\Rightarrow$ (a): From the assumption we have $\gcd(\gcd(m,n), n/\gcd(m,n)) = 1$, that is, $\gcd(m, n/\gcd(m,n)) = 1$. By Bezout's lemma, there exist $x, y \in \mathbb{Z}$ such that $m^2x + \frac{nm}{\gcd(m,n)}y = m$, whence $m^2x \equiv m \pmod{n}$. $\square$

3 Proof by equivalence relation

Our first proof of (1) is inspired by Morgado's original proof [5], but is considerably more formal and combinatorial, as it makes explicit use of an equivalence relation and the bijection principle on the resulting equivalence classes. Recall that $\mathbb{Z}_n^* = \{m \in \mathbb{Z}_n \mid \gcd(m,n) = 1\}$.

Proof. For $m_1, m_2 \in \mathbb{Z}_n^{\text{reg}}$, let $m_1 \sim m_2$ if $\gcd(m_1,n) = \gcd(m_2,n)$; this defines an equivalence relation on $\mathbb{Z}_n^{\text{reg}}$. By Proposition 3, $m \in \mathbb{Z}_n^{\text{reg}}$ if and only if $\gcd(m,n) \,|^* n$, so the equivalence classes are of the form $C_{n,d}$ with $d \,|^* n$, where

$$C_{n,d} = \{m \in \mathbb{Z}_n^{\text{reg}} \mid \gcd(m,n) = d\}\,.$$

Using the bijection principle, we show that for every unitary divisor d of n,

$$|C_{n,d}| = |\mathbb{Z}_{n/d}^*|. \tag{2}$$

To this end, for $d \,|^* n$ define $h_{n,d} : C_{n,d} \to \mathbb{Z}_{n/d}^*$ by $h_{n,d}(m) = m \bmod (n/d)$. This map is well defined, since $\gcd(m \bmod (n/d), n/d) = \gcd(m, n/d) = \gcd(m, n, n/d) = \gcd(d, n/d) = 1$. It remains to show that $h_{n,d}$ is bijective.

Injectivity. Suppose that $h_{n,d}(m_1) = h_{n,d}(m_2)$. Then, $m_1 \equiv m_2 \pmod{n/d}$. Since $m_1, m_2 \in C_{n,d}$, we have $\gcd(m_1,n) = \gcd(m_2,n) = d$, which implies $m_1 \equiv m_2 \pmod{d}$. Because d and n/d are coprime, combining both congruences gives $m_1 \equiv m_2 \pmod{n}$, and hence $m_1 = m_2$.

Surjectivity. Let $d' \in \mathbb{Z}_{n/d}^*$, and define $m = d((d'i) \bmod (n/d))$, where i denotes an inverse of d modulo n/d. We claim the following:

(i) $m \in C_{n,d}$;

(ii) $h_{n,d}(m) = d'$.

For (i), it suffices to show that $\gcd(m,n) = d$. Indeed, since $d \mid m$ and $d \mid n$, and since $\gcd(d', n/d) = 1$ and $\gcd(i, n/d) = 1$, we have

$$\gcd(m,n) = d\gcd(d'i \bmod (n/d), n/d) = d\gcd(d'i, n/d) = d\gcd(i, n/d) = d.$$

Part (ii) follows immediately, since

$$h_{n,d}(m) = m \bmod (n/d) = (di \bmod (n/d))(d' \bmod (n/d)) = d'.$$

From (2) and the disjointness of the equivalence classes, we conclude that

$$\varrho(n) = \sum_{d\,|^*n} |C_{n,d}| = \sum_{d\,|^*n} |\mathbb{Z}^*_{n/d}| = \sum_{d\,|^*n} \varphi\left(\frac{n}{d}\right) = \sum_{d\,|^*n} \varphi(d),$$

which proves (1). $\square$

4 A purely bijective proof

Our next proof is purely bijective. The idea is to establish a bijection between $\mathbb{Z}_n^{\mathrm{reg}}$ and the set of pairs (d, d') with $d\,|^*n$ and $d' \in \mathbb{Z}_d^*$ that are counted by the right-hand side of (1). This bijection yields an encoding of $\mathbb{Z}_n^{\mathrm{reg}}$ that may prove useful beyond this proof.

Proof. Let U_n denote the set of unitary divisors of n. Consider the map

$$f_n : \mathbb{Z}_n^{\mathrm{reg}} \to \{(d, d') \mid d \in U_n, d' \in \mathbb{Z}_d^*\},$$

defined by

$$f_n(m) := \left(\frac{n}{\gcd(m,n)}, m \bmod \frac{n}{\gcd(m,n)}\right).$$

We first show that f_n is well defined. Let $d = n/\gcd(m,n)$. Then $d \in U_n$, and hence $\gcd(d, m \bmod d) = \gcd(d,m) = \gcd(d,m,n) = \gcd(d, \gcd(m,n)) = \gcd(d, n/d) = 1$, which implies $m \bmod d \in \mathbb{Z}_d^*$. To apply the bijection principle, we show that f_n is bijective.

Injectivity. Suppose that $f_n(m_1) = f_n(m_2)$. Then, $\gcd(m_1, n) = \gcd(m_2, n)$, which we denote by d. Evidently, $m_1 \bmod n/d = m_2 \bmod n/d$, which means that $m_1 \equiv m_2 \pmod{n/d}$. From $\gcd(m_1, n) = d$ we can write $m_1 = dm_1'$, $m_2 = dm_2'$, and $n = dn'$ with $\gcd(m_1', n') = \gcd(m_2', n') = 1$. Therefore, $m_1 - m_2 = d(m_1' - m_2')$, so $d \mid m_1 - m_2$, which gives $m_1 \equiv m_2 \pmod{d}$. Since d and n/d are coprime (because $d\,|^*n$), combining the congruences $m_1 \equiv m_2 \pmod{d}$ and $m_1 \equiv m_2 \pmod{n/d}$ gives $m_1 \equiv m_2 \pmod{n}$, and hence $m_1 = m_2$.

Surjectivity. Let $d \in U_n$ and $d' \in \mathbb{Z}_d^*$. We define m as

$$m = \frac{n}{d}\big((d'j) \bmod d\big), \tag{3}$$

where j is an inverse of n/d modulo d. We claim the following:

(i) $m \in \mathbb{Z}_n^{\text{reg}}$;

(ii) $f_n(m) = (d, d')$.

Since n/d divides both m and n, and since $\gcd(d', d) = 1$ and $\gcd(j, d) = 1$, we have

$$\gcd(m, n) = \frac{n}{d} \gcd\left((d'j) \bmod d, d\right) = \frac{n}{d} \gcd\left(d'j, d\right) = \frac{n}{d} \gcd\left(j, d\right) = \frac{n}{d}. \tag{4}$$

Hence $\gcd(m, n) \,|^* n$, and by Proposition 3, $m \in \mathbb{Z}_n^{\text{reg}}$, as claimed in (i). For part (ii), we note that $d = n/\gcd(m, n)$ follows from (4), and $d' = m \bmod d$ follows from (3), since j is an inverse of n/d modulo d. Thus, (i) and (ii) are shown, and the proof is complete. $\square$

To illustrate the proof, we list the assignments $m \mapsto f_{20}(m)$ for $m \in \mathbb{Z}_{20}^{\text{reg}}$:

$$\begin{array}{lllll} 0 \mapsto (1,0), & 4 \mapsto (5,4), & 8 \mapsto (5,3), & 12 \mapsto (5,2), & 16 \mapsto (5,1), \\ 1 \mapsto (20,1), & 5 \mapsto (4,1), & 9 \mapsto (20,9), & 13 \mapsto (20,13), & 17 \mapsto (20,17), \\ 3 \mapsto (20,3), & 7 \mapsto (20,7), & 11 \mapsto (20,11), & 15 \mapsto (4,3), & 19 \mapsto (20,19). \end{array}$$

Remark 4. In view of (3), the inverse of f_n takes the form $f_n^{-1}(d, d') = \frac{n}{d}(((n/d \bmod d)^{-1} d') \bmod d)$ for every $d \in U_n$ and $d' \in \mathbb{Z}_d^*$.

Remark 5. The proof can be restated by defining $f_n(m) := (\gcd(m, n), m \bmod n/\gcd(m, n))$, which maps from $\mathbb{Z}_n^{\text{reg}}$ to $\{(d, d') \mid d \in U_n, d' \in \mathbb{Z}_{n/d}^*\}$. In this setting, $f_n^{-1}(d, d') = d(((d \bmod (n/d))^{-1} d') \bmod (n/d))$.

5 Proof by reduced fractions

Our third proof is inspired Gauss's formula $n = \sum_{d|n} \varphi(d)$, as reproduced in the textbook by Graham, Knuth, and Patashnik [4, pp. 134–135]. The key idea is to establish a bijection between $\mathbb{Z}_n^{\text{reg}}$ and the set of reduced fractions of the form k/d, where $d \,|^* n$ and $k < d$.

Proof. Consider the fractions m/n with $m \in \mathbb{Z}_n^{\text{reg}}$. Reducing these fractions to lowest terms yields fractions of the form

$$k/d = (m/\gcd(m, n))/(n/\gcd(m, n)).$$

By Proposition 3, m is regular modulo n if and only if $\gcd(m, n) \,|^* n$, or equivalently, if and only if $n/\gcd(m, n) \,|^* n$. Hence, the denominators of these reduced fractions are precisely the unitary divisors d of n. Each reduced fraction k/d with $d \,|^* n$ and $k < d$ arises in this way by reducing $(kn/d)/n$ to lowest terms. To complete the argument, we show that $kn/d \in \mathbb{Z}_n^{\text{reg}}$. Because k and d, as well as d and n/d, are coprime,

$$\gcd(kn/d, n) = \gcd(k(n/d), d(n/d)) = n/d \,|^* n.$$

Hence, by Proposition 3, $kn/d \in \mathbb{Z}_n^{\text{reg}}$. Thus, the $\varrho(n)$ reduced fractions can be grouped according to their denominator $d \,|^* n$, with $\varphi(d)$ reduced fractions for each denominator d. $\square$

To illustrate the proof, consider the $\varrho(20)$ fractions $m/20$ for $m \in \mathbb{Z}_{20}^{\mathrm{reg}}$:

$$\frac{0}{20}, \quad \frac{1}{20}, \quad \frac{3}{20}, \quad \frac{4}{20}, \quad \frac{5}{20}, \quad \frac{7}{20}, \quad \frac{8}{20}, \quad \frac{9}{20}, \quad \frac{11}{20}, \quad \frac{12}{20}, \quad \frac{13}{20}, \quad \frac{15}{20}, \quad \frac{16}{20}, \quad \frac{17}{20}, \quad \frac{19}{20}.$$

Grouping the reduced fractions by their denominators yields

$$\frac{0}{1}, \quad \frac{1}{4}, \quad \frac{3}{4}, \quad \frac{1}{5}, \quad \frac{2}{5}, \quad \frac{3}{5}, \quad \frac{4}{5}, \quad \frac{1}{20}, \quad \frac{3}{20}, \quad \frac{7}{20}, \quad \frac{9}{20}, \quad \frac{11}{20}, \quad \frac{13}{20}, \quad \frac{17}{20}, \quad \frac{19}{20},$$

with $\varphi(1) = 1$ fraction having denominator 1, $\varphi(4) = 2$ fractions having denominator 4, $\varphi(5) = 4$ fractions having denominator 5, and $\varphi(20) = 8$ fractions having denominator 20. Hence $\varrho(20) = 1 + 2 + 4 + 8 = 15$.

Remark 6. There is an obvious connection with the proof in Section 4: a fraction a/b appears in the list of reduced fractions if and only if $f_n(m) = (b, a)$ for some $m \in \mathbb{Z}_n^{\mathrm{reg}}$.

6 Proof by inclusion-exclusion

Our final proof of (1) is based on a combined application of the inclusion-exclusion principle, the bijection principle, and the multiplicativity of Euler's totient function $\varphi(n)$.

Proof. For every integer $m \geq 0$ and every prime p, let $\nu_p(m)$ denote the multiplicity of p in the prime factorization of m. For every $m \in \mathbb{Z}_n$, we have $m \in \mathbb{Z}_n^{\mathrm{reg}}$ if and only if $\nu_p(m) = 0$ or $\nu_p(m) \geq \nu_p(n)$ for each prime divisor p of n, as follows from Proposition 3. Let $P(n)$ denote the set of prime divisors of n, and for each $p \in P(n)$, define

$$A_p = \{m \in \mathbb{Z}_n \mid 0 < \nu_p(m) < \nu_p(n)\}.$$

Then by the inclusion-exclusion principle,

$$\varrho(n) = \left| \bigcap_{p \in P(n)} \overline{A_p} \right| = \sum_{I \subseteq P(n)} (-1)^{|I|} \left| \bigcap_{i \in I} A_i \right|. \tag{5}$$

In this formula, $m \in \bigcap_{i \in I} A_i$ if and only if $m = k \prod_{i \in I} i$ for some $k \leq \frac{n}{\prod_{i \in I} i}$ such that $j^{\nu_j(n)-1} \nmid k$ for each $j \in I$; that is, if and only if $k \in \bigcap_{j \in I} \overline{B_j}$, where

$$B_j = \left\{ 1 \leq k \leq \frac{n}{\prod_{i \in I} i} \;\middle|\; j^{\nu_j(n)-1} \mid k \right\} \quad (j \in I).$$

Clearly, $m \mapsto \frac{m}{\prod_{i \in I} i}$ defines a bijection from $\bigcap_{i \in I} A_i$ to $\bigcap_{j \in I} \overline{B_j}$. Therefore, by the bijection principle and another application of the inclusion-exclusion principle, we have

$$\left| \bigcap_{i \in I} A_i \right| = \sum_{J \subseteq I} (-1)^{|J|} \left| \bigcap_{j \in J} B_j \right| = \sum_{J \subseteq I} (-1)^{|J|} \frac{n}{\prod_{i \in I} i \prod_{j \in J} j^{\nu_j(n)-1}}. \tag{6}$$

Combining (5) and (6) and then changing the order of summation, we obtain

$$\varrho(n) = \sum_{I\subseteq P(n)} \sum_{J\subseteq I} (-1)^{|I|+|J|} \frac{n}{\prod_{i\in I\setminus J} i \prod_{j\in J} j^{\nu_j(n)}} = \sum_{J\subseteq P(n)} \prod_{j\in J} \frac{n}{j^{\nu_j(n)}} \sum_{I\supseteq J} (-1)^{|I|+|J|} \prod_{i\in I\setminus J} \frac{1}{i}.$$

Replacing J by its complement in $P(n)$, and factoring the inner sum, it follows that

$$\varrho(n) = \sum_{J\subseteq P(n)} \prod_{j\in J} j^{\nu_j(n)} \sum_{I\subseteq J} (-1)^{|I|} \prod_{i\in I} \frac{1}{i} = \sum_{J\subseteq P(n)} \prod_{j\in J} j^{\nu_j(n)} \left(1 - \frac{1}{j}\right).$$

Using Euler's totient function and its multiplicativity, we obtain

$$\varrho(n) = \sum_{J\subseteq P(n)} \prod_{j\in J} \varphi(j^{\nu_j(n)}) = \sum_{J\subseteq P(n)} \varphi\left(\prod_{j\in J} j^{\nu_j(n)}\right).$$

We finally observe that the last sum ranges over all positive divisors $d = \prod_{j\in J} j^{\nu_j(n)}$ of n that are coprime to n/d, i.e., over all unitary divisors d of n, thus proving (1). □

7 Significance for cryptography

The authors [3] encountered regular integers modulo n while developing a generalization of the RSA scheme [7] to arbitrary multi-prime, multi-power moduli. For such a generalized modulus $n = p_1^{e_1} \cdots p_r^{e_r}$ with distinct primes $p_1, \ldots, p_r$ and exponents $e_1, \ldots, e_r \in \mathbb{N}$, the public key (n, e) and the private key (n, d) are established in the same way as in the classical RSA scheme: choose $1 < e < \varphi(n)$ such that $\gcd(e, \varphi(n)) = 1$, and compute $1 < d < \varphi(n)$ such that $ed \equiv 1 \pmod{\varphi(n)}$. As in classical RSA, a message $m \in \mathbb{Z}_n$ is encrypted by raising m to the e-th power modulo n and decrypted by raising m to the d-th power modulo n.

A key observation, proved by the present authors [3], is that decryption reverses encryption if and only if the message is regular modulo n. Consequently, by (1), the probability of correct decryption of a random message from $\mathbb{Z}_n$ is given by

$$\frac{\varrho(n)}{n} = \frac{1}{n} \sum_{d\,|^*n} \varphi(d),$$

which illustrates the significance of the sequence A055653 and Morgado's formula (1) in the context of cryptography. As further shown by the present authors [3],

$$\frac{\varrho(n)}{n} \geq 1 - \frac{r}{2^{k-1}},$$

where $n = p_1^{e_1} \cdots p_r^{e_r}$ with distinct k-bit primes $p_1, \ldots, p_r$. Therefore, even for today's standard choices of k, such as $k = 1024$, almost all messages in $\mathbb{Z}_n$ are decrypted correctly, and the restriction to regular messages is negligible. Although this conclusion is satisfactory from a practical point of view, there remains potential for sharper bounds on the correctness probability. Asymptotic results on $\varrho(n)$ and related quantities such as $\varrho(n)/\varphi(n)$, as obtained by Apostol and Petrescu [2] and by Tóth [8], may prove crucial in this regard.

References

[1] O. Alkam and E. A. Osba, On the regular elements in $\mathbb{Z}_n$, *Turkish J. Math.* **32** (2008), 31–39.

[2] B. Apostol and L. Petrescu, Extremal orders of certain functions associated with regular integers (mod n), *J. Integer Sequences* **16** (2013), Article 13.7.5.

[3] K. Dohmen and M. Lange-Geisler, General multi-prime multi-power RSA—a generalization of RSA and CRT-RSA to regular integers modulo n, preprint, Cryptology ePrint Archive 2025/1157, 2025. Available at https://eprint.iacr.org/2025/1157.

[4] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 2nd edition, 1994.

[5] J. Morgado, Inteiros regulares módulo n, *Gazeta de Matematica (Lisboa)* **33** (1972), 1–5.

[6] N. J. A. Sloane and The OEIS Foundation Inc., The On-Line Encyclopedia of Integer Sequences, 2026. Available at https://oeis.org.

[7] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **21** (1978), 120–126.

[8] L. Tóth, Regular integers modulo n, *Ann. Univ. Sci. Budapest. Sect. Comput.* **29** (2008), 263–275.

2020 *Mathematics Subject Classification*: Primary 11B83; Secondary 05A15, 11A25, 11T71.
Keywords: regular integer modulo n, unitary divisor, totient function, RSA cryptosystem.

(Concerned with sequence A055653.)

Received October 9 2025; revised versions received March 13 2026; March 18 2026. Published in *Journal of Integer Sequences*, April 21 2026.

Return to Journal of Integer Sequences home page.