

1-1-2008

On the regular elements in Z_n

OSAMA ALKAM

EMAD ABU OSBA

Follow this and additional works at: <https://journals.tubitak.gov.tr/math>



Part of the [Mathematics Commons](#)

Recommended Citation

ALKAM, OSAMA and OSBA, EMAD ABU (2008) "On the regular elements in Z_n ," *Turkish Journal of Mathematics*: Vol. 32: No. 1, Article 4. Available at: <https://journals.tubitak.gov.tr/math/vol32/iss1/4>

This Article is brought to you for free and open access by TÜBİTAK Academic Journals. It has been accepted for inclusion in Turkish Journal of Mathematics by an authorized editor of TÜBİTAK Academic Journals. For more information, please contact academic.publications@tubitak.gov.tr.

On the regular elements in \mathbb{Z}_n

Osama Alkam and Emad Abu Osba

Abstract

All rings are assumed to be finite commutative with identity element. An element $a \in R$ is called a regular element if there exists $b \in R$ such that $a = a^2b$, the element b is called a von Neumann inverse for a . A characterization is given for regular elements and their inverses in \mathbb{Z}_n , the ring of integers modulo n . The arithmetic function $V(n)$, which counts the regular elements in \mathbb{Z}_n is studied. The relations between $V(n)$ and Euler's phi-function $\varphi(n)$ are explored.

Key Words: Regular elements, Euler's phi-function, von Neumann regular rings.

1. Introduction

All rings are assumed to be finite commutative with identity element 1. The numbers p and q are always assumed to be prime numbers.

Definition 1 *An element $a \in R$ is called a **regular element** if there exists $b \in R$ such that $a = a^2b$, the element b is called a **von Neumann inverse** for a . The ring R is called a **von Neumann regular ring (VNR)** if all elements of R are regular.*

The following proposition is well known; it shows some basic properties of the regular elements and their importance in ring theory, (see [3]).

Proposition 1 *If a is a regular element in R , then there exists a unique element $a^{(-1)} \in R$ such that:*

AMS Mathematics Subject Classification: Primary:11A25, Secondary:16E50.

- (1) $a = a^2 a^{(-1)}$ and $a^{(-1)} = (a^{(-1)})^2 a$.
- (2) $e = aa^{(-1)}$ is an idempotent.
- (3) $u = 1 - e + a$ is a unit.
- (4) $a = ue$.
- (5) $aR = eR$.

Recall that for each natural number n , the function $\varphi(n)$ is the number of integers t such that $1 \leq t \leq n$, and $\gcd(t, n) = 1$, $\varpi(n)$ is the number of distinct primes dividing n , $\tau(n)$ is the number of divisors of n and $\sigma(n)$ is the sum of the divisors of n ; see [5].

In section 2, we characterize regular elements in \mathbb{Z}_n , the ring of integers modulo n , and find their von Neumann inverses.

In section 3, a new arithmetic multiplicative function $V(n)$, which counts the regular elements in \mathbb{Z}_n , is introduced. This new function is related to the famous Euler's phi-function $\varphi(n)$. Different definitions of $V(n)$ are given and basic properties are studied. Many inequalities are proved relating V to some of the famous arithmetic functions. The asymptotic behavior of V is also studied.

In section 4, some open problems are posed for further research.

Studying and counting the regular elements in \mathbb{Z}_n is very interesting. The function V shares with the function φ many of its important properties, while it differs in some others. We think that the function V could be used in cryptography theory and would be a source for many research problems in ring and number theories.

2. Regular Elements in \mathbb{Z}_n

It is not always an easy task to determine if a particular element is a regular element and to find its von Neumann inverse. However if the ring R is a local ring, then computations are easier. In fact, in this case a regular element is either zero or a unit. In this section, we use this fact together with the decomposition theorem of finite commutative rings with identity to determine if a given element in \mathbb{Z}_n is regular or not and to find its von Neumann inverse. See also [1]. For each ring R , let $\text{Vr}(R)$ be the set of all regular elements in R .

Lemma 1 *Let R be a local ring with M its only maximal ideal. Then $\text{Vr}(R) = R \setminus (M \setminus \{0\})$.*

Proof. Let $a \in R \setminus (M \setminus \{0\})$. Then a is a unit or zero and so $a \in Vr(R)$. If $a \in Vr(R)$, then there exists $b \in R$ such that $a = a^2b$, which implies that $a(1 - ab) = 0$. If a is not a unit, then $(1 - ab)$ is a unit and so $a = 0$, therefore $a \in R \setminus (M \setminus \{0\})$. \square

Theorem 1 Let $R = \prod_{i \in I} R_i$ where R_i is a local ring for each $i \in I$. Then $(a_i)_{i \in I}$ is a regular element if and only if a_i is either zero or a unit in R_i for each $i \in I$.

Proof. $(a_i)_{i \in I}$ is regular

$$\begin{aligned} &\Leftrightarrow \text{there exists } (b_i)_{i \in I} \text{ such that } (a_i)_{i \in I} = ((a_i)_{i \in I})^2 (b_i)_{i \in I} = (a_i^2 b_i)_{i \in I} \\ &\Leftrightarrow a_i = a_i^2 b_i \text{ for all } i \in I \\ &\Leftrightarrow a_i = 0 \text{ or } a_i \text{ is a unit in } R_i \text{ for each } i \in I. \end{aligned} \quad \square$$

It follows immediately from this theorem that if $n = \prod_{i=1}^m p_i^{\alpha_i}$, then an element $m \in \mathbb{Z}_n$ is regular if and only if m is a unit (mod $p_i^{\alpha_i}$) or m is 0 (mod $p_i^{\alpha_i}$) for each i .

It is known (Euler's Theorem) that if a is a unit in \mathbb{Z}_n , then $a^{\varphi(n)} \equiv 1 \pmod{n}$ and so $a^{\varphi(n)-1} \pmod{n}$ is the multiplicative inverse of a in \mathbb{Z}_n . The following theorem generalizes Euler's Theorem.

Theorem 2 An element a is regular in \mathbb{Z}_n if and only if $a^{\varphi(n)+1} \equiv a \pmod{n}$.

Proof. Let $n = \prod_{i=1}^m p_i^{\alpha_i}$. Suppose that a is a regular element in \mathbb{Z}_n . If $a \equiv 0 \pmod{p_i^{\alpha_i}}$, then $a^{\varphi(n)+1} \equiv a \pmod{p_i^{\alpha_i}}$. So assume that a is a unit (mod $p_i^{\alpha_i}$), which implies, using Euler's theorem, that $a^{\varphi(n)} \equiv (a^{\varphi(p_i^{\alpha_i})})^{\frac{\varphi(n)}{\varphi(p_i^{\alpha_i})}} \equiv 1 \pmod{p_i^{\alpha_i}}$. Therefore, $a^{\varphi(n)+1} \equiv a \pmod{p_i^{\alpha_i}}$, hence $a^{\varphi(n)+1} \equiv a \pmod{n}$.

Conversely, $a \equiv a^{\varphi(n)+1} \equiv a^2 a^{\varphi(n)-1} \pmod{n}$, and so a is a regular element. \square

The following corollary determines the von Neumann inverse for a regular element in \mathbb{Z}_n .

Corollary 1 If a is a regular element in \mathbb{Z}_n , then $a^{\varphi(n)-1}$ is a von Neumann inverse for a in \mathbb{Z}_n . In fact, $a^{(-1)} \equiv a^{\varphi(n)-1} \pmod{n}$.

Remark 1 Let a be a regular element in \mathbb{Z}_n . As a consequence of Proposition 1, $(a^{(-1)})^{(-1)} = a$, therefore, by Corollary 1,

$$a \equiv (a^{(-1)})^{(-1)} \equiv (a^{(-1)})^{\varphi(n)-1} \equiv (a^{\varphi(n)-1})^{\varphi(n)-1} \pmod{n}.$$

Example 1 It is known that $\mathbb{Z}_{36} \simeq \mathbb{Z}_4 \times \mathbb{Z}_9$. $25 \equiv 1 \pmod{4}$ and $25 \equiv 7 \pmod{9}$, so 25 is a regular element in \mathbb{Z}_{36} . Moreover, $13 \equiv 25^{11} \equiv (25)^{\varphi(36)-1} \equiv (25)^{(-1)} \pmod{36}$ is a von Neumann inverse for 25 in \mathbb{Z}_{36} . On the other hand, $18 \equiv 2 \pmod{4}$ and $18 \equiv 0 \pmod{9}$, so 18 is not a regular element in \mathbb{Z}_{36} .

3. Number of Regular Elements in \mathbb{Z}_n

In this section, we study the function $V(n)$; it is the number of regular elements in the ring \mathbb{Z}_n . We also relate it to Euler's phi-function.

Using Lemma 1 and Theorem 1 in Section 2, one can deduce easily that if $R = \prod_{i=1}^m R_i$, where R_i is a local ring with M_i its unique maximal ideal for each i , then $|\text{Vr}(R)| = \prod_{i=1}^m (|R_i| - |M_i| + 1)$. Recall that if $n = \prod_{i=1}^m p_i^{\alpha_i}$, then $\mathbb{Z}_n \simeq \prod_{i=1}^m \mathbb{Z}_{p_i^{\alpha_i}}$ and $\varphi(n) = \prod_{i=1}^m (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n \prod_{p|n} (1 - \frac{1}{p})$. Hence the following theorem easily follows.

Theorem 3 (1) $V(p^\alpha) = p^\alpha - p^{\alpha-1} + 1 = \varphi(p^\alpha) + 1 = p^\alpha(1 - \frac{1}{p} + \frac{1}{p^\alpha})$.

(2) If $n = \prod_{i=1}^m p_i^{\alpha_i}$, then $V(n) = \prod_{i=1}^m V(p_i^{\alpha_i}) = \prod_{i=1}^m (p_i^{\alpha_i} - p_i^{\alpha_i-1} + 1) = \prod_{i=1}^m (\varphi(p_i^{\alpha_i}) + 1) = n \prod_{i=1}^m (1 - \frac{1}{p_i} + \frac{1}{p_i^{\alpha_i}})$.

(3) If $\text{gcd}(m, k) = 1$, then $V(mk) = V(m)V(k)$, i.e. the function V is a multiplicative function.

We now give another formula for finding $V(n)$. But first we give the following definition.

Definition 2 Let a and b be two positive integers. We say that a is a **unitary divisor** of b if $a \mid b$ and $\text{gcd}(a, \frac{b}{a}) = 1$. In this case, we write $a \parallel b$, see [7].

We now use the unitary divisors of an integer to calculate the number of regular elements.

Theorem 4 $V(n) = \sum_{d|n} \varphi(d)$. Moreover, $\frac{V(n)}{\varphi(n)} = \sum_{d|n} \frac{1}{\varphi(d)}$.

Proof. The proof follows immediately using the formula $V(n) = \prod_{p^\alpha || n} (\varphi(p^\alpha) + 1)$. \square

Example 2 $90 = 2^1 \times 3^2 \times 5^1$. The unitary divisors of 90 are: 1, 2, 5, 9, 10, 18, 45, 90. Hence $V(90) = 70 = \varphi(1) + \varphi(2) + \varphi(5) + \varphi(9) + \varphi(10) + \varphi(18) + \varphi(45) + \varphi(90)$.

3.1. Basic properties

It is well known that $\varphi(n)$ is even for all $n > 2$. But this is not true for $V(n)$ as it is shown below.

Theorem 5 $V(n)$ is even if and only if $2 \parallel n$, i.e. $n \equiv 2 \pmod{4}$.

Proof. $V(n) = \prod_{p^\alpha || n} (\varphi(p^\alpha) + 1)$. For $p \neq 2$, $\varphi(p^\alpha) + 1$ is an odd number. For $p = 2$ and $\alpha = 1$, $\varphi(2) + 1 = 2$ is even. For $p = 2$ and $\alpha > 1$, $\varphi(2^\alpha) + 1$ is odd. Hence the result. \square

Theorem 6 For each regular element $a \in \mathbb{Z}_n$, $a^{V(n)} \equiv a^{V(n)-\varphi(n)} \pmod{n}$.

Proof. Suppose that $n = \prod_{i=1}^m p_i^{\alpha_i}$. Let a be a regular element in \mathbb{Z}_n . If $a \equiv 0 \pmod{p_i^{\alpha_i}}$, then since $V(n) \geq \varphi(n)$, it follows that $a^{V(n)} \equiv a^{V(n)-\varphi(n)} \pmod{p_i^{\alpha_i}}$. So assume that a is a unit $\pmod{p_i^{\alpha_i}}$, hence $a^{V(n)} \equiv a^{V(n)-\varphi(n)} (a^{\varphi(p_i^{\alpha_i})})^{\frac{\varphi(n)}{\varphi(p_i^{\alpha_i})}} \equiv a^{V(n)-\varphi(n)} \pmod{p_i^{\alpha_i}}$.

Thus $a^{V(n)} \equiv a^{V(n)-\varphi(n)} \pmod{n}$. \square

We now calculate the summatory function of the arithmetic function V . Let $F(n) = \sum_{d|n} V(d)$.

Theorem 7 Let $n = \prod_{i=1}^m p_i^{\alpha_i}$. Then $F(n) = \prod_{i=1}^m F(p_i^{\alpha_i}) = \prod_{i=1}^m (p_i^{\alpha_i} + \alpha_i)$.

Proof. $F(p^\alpha) = \sum_{k=0}^{\alpha} V(p^k) = V(1) + \sum_{k=1}^{\alpha} V(p^k) = 1 + \sum_{k=1}^{\alpha} (\varphi(p^k) + 1) = \varphi(1) + \sum_{k=1}^{\alpha} \varphi(p^k) + \sum_{k=1}^{\alpha} 1 = \sum_{k=0}^{\alpha} \varphi(p^k) + \sum_{k=1}^{\alpha} 1 = p^\alpha + \alpha$.

Since the function V is multiplicative we can obtain the general case easily. \square

3.2. Inequalities

For each n , we have $\sqrt{n} \leq V(n) \leq n$, since $\sqrt{n} \leq \varphi(n)$ for all n not 2 or 6.

Since $p_i^{\alpha_i-1} \leq p_i^{\alpha_i-1} + 1 \leq p_i^{\alpha_i-1}(p_i - 1) + 1 \leq p_i^{\alpha_i}$, it follows that $\prod_{i=1}^m p_i^{\alpha_i-1} \leq \prod_{i=1}^m (p_i^{\alpha_i-1} + 1) \leq V(\prod_{i=1}^m p_i^{\alpha_i}) \leq \prod_{i=1}^m p_i^{\alpha_i}$.

It is known that $\frac{6}{\pi} < \frac{\varphi(n)\sigma(n)}{n^2} < 1$; see [6, 1.21]. It is clear that $\frac{V(4)\sigma(4)}{16} > 1$. In fact, if we choose the subsequence $\{n_k\}$ such that n_k is the product of the first k prime

numbers, then $V(n_k) = n_k$ and $\frac{V(n_k)\sigma(n_k)}{(n_k)^2} = \frac{\sigma(n_k)}{n_k} = \frac{\prod_{i=1}^k (p_i+1)}{\prod_{i=1}^k p_i} = \prod_{i=1}^k (1 + \frac{1}{p_i}) \rightarrow \infty$ as

$k \rightarrow \infty$. In fact, $V(p^\alpha)\sigma(p^\alpha) = (p^\alpha - p^{\alpha-1} + 1)(\sum_{k=0}^{\alpha} p^k) = p^\alpha(1 - p^{-1} + p^{-\alpha})(\sum_{k=0}^{\alpha} p^k) = p^\alpha(1 + p^\alpha + \sum_{k=2}^{\alpha} p^{-k}) = p^{2\alpha}(1 + p^{-\alpha} + \sum_{k=2}^{\alpha} p^{-(\alpha+k)})$.

Since both V and σ are multiplicative functions, if $n = \prod_{i=1}^m p_i^{\alpha_i}$, then $\frac{V(n)\sigma(n)}{n^2} = \prod_{i=1}^m (1 + p_i^{-\alpha_i} + \sum_{k=2}^{\alpha_i} p_i^{-(\alpha_i+k)})$.

It is known that $\sigma(n) + \varphi(n) \leq n \tau(n)$ with equality if and only if n is a prime; see [6]. For any prime number p , $\sigma(p) + V(p) = 2p + 1 > 2p = p\tau(p)$. We show now that if n is a composite number, then $\sigma(n) + V(n) \leq n \tau(n)$.

Theorem 8 If n is a composite number, then $\sigma(n) + V(n) \leq n \tau(n)$.

Proof. It is clear that $\sum_{d|n} \frac{1}{d} \leq \tau(n) - 1$, since there are at least 2 divisors d with $\frac{1}{d} \leq \frac{1}{2}$ (namely $d = n$ and any other divisor of n that is greater than 1). So $\frac{\sigma(n)}{n} = \sum_{d|n} \frac{1}{d} \leq \tau(n) - 1$. Thus $\sigma(n) + n \leq n\tau(n)$. Now the result follows, since $V(n) \leq n$. \square

3.3. Asymptotic Behaviour

The sequence $\{\frac{V(n)}{n}\}$ has no limit, since the subsequences $\{\frac{V(2^n)}{2^n}\}$ and $\{\frac{V(3^n)}{3^n}\}$ have different limits. However $\frac{V(p)}{p} = 1$ if p is a prime and since $V(n)$ is at most n for all n , one can conclude that $\limsup_{n \rightarrow \infty} \frac{V(n)}{n} = 1$.

Theorem 9 For any $\epsilon > 0$, $\lim_{n \rightarrow \infty} \frac{V(n)}{(n)^{1-\epsilon}} = \infty$.

Proof. It suffices to consider $n = p^m$.

$\frac{V(p^m)}{(p^m)^{1-\epsilon}} = \frac{p^m(1-p^{-1}+p^{-m})}{p^{m-m\epsilon}} = p^{m\epsilon}(1-p^{-1}+p^{-m}) \rightarrow \infty$ as $p^m \rightarrow \infty$. Now it is easy to deduce the general case. \square

The subsequence $\{\frac{V(p)}{\varphi(p)}\}_p$ is prime converges to 1, while the subsequence $\{\frac{V(n_k)}{\varphi(n_k)}\}$ where n_k is the product of the first k prime numbers, diverges since $\frac{V(n_k)}{\varphi(n_k)} = \prod_{i=1}^k (1 + \frac{1}{p_i-1})$, so one can conclude the following.

Theorem 10 (1) $\limsup_{n \rightarrow \infty} \frac{V(n)}{\varphi(n)} = \infty$. (2) $\liminf_{n \rightarrow \infty} \frac{V(n)}{\varphi(n)} = 1$.

3.4. Factorial Equations

It is known that for any prime number p ,

1. $\tau(p!) = 2\tau((p-1)!)$.
2. $\sigma(p!) = (p+1)\sigma((p-1)!)$.
3. $\varphi(p!) = (p-1)\varphi((p-1)!)$.

In the case of V , we have $V(p!) = V(p(p-1)!) = V(p)V((p-1)!) = pV((p-1)!)$.

Although $\lim_{n \rightarrow \infty} \frac{V(n)}{n}$ does not exist as shown above, the situation is different when dealing with factorials.

Theorem 11 $\lim_{n \rightarrow \infty} \frac{V(n!)}{n!} = 0$.

Proof. The result follows immediately since $\frac{V(n!)}{n!} = \prod_{p^\alpha \parallel n!} (1 - \frac{1}{p} + \frac{1}{p^\alpha}) = \prod_{p^\alpha \parallel n!} (1 - (\frac{1}{p} - \frac{1}{p^\alpha}))$. But $\sum (\frac{1}{p} - \frac{1}{p^\alpha})$ diverges, and $\text{Lim} (\frac{1}{p} - \frac{1}{p^\alpha}) = 0$, so $\frac{V(n!)}{n!} = \prod_{p^\alpha \parallel n!} (1 - \frac{1}{p} + \frac{1}{p^\alpha})$ diverges to zero, see [2, 12-55]. \square

We now extend the results of F. Luca in [4] to $V(n)$.

Theorem 12 *Let a be any positive rational number. Then the equation $\frac{V(n!)}{m!} = a$ has finitely many solutions (m, n) .*

Proof. Notice that $V(n!)$ is odd for all $n \geq 4$, (see Theorem 5). Let $a = \frac{c}{d}$ be a positive rational number. Consider the equation $V(n!) = \frac{c}{d}m!$. If there are infinitely many solutions (m, n) for the equation, then there is an $m_0 > d$ such that $\frac{c}{d}m!$ is even for all $m \geq m_0$, a contradiction. \square

We now use the above theorem to solve the equation $\frac{V(n!)}{m!} = a$, for $a = 1$.

Corollary 2 $\frac{V(n!)}{m!} = 1$, has a solution only for $n = 1, 2$, and 3 .

Proof. For $n, m \geq 4$, $V(n!)$ is odd while $m!$ is even. \square

4. Open Problems

1. If n is a product of distinct primes, then $V(n) = n$. It is clear that $\text{gcd}(p^\alpha, V(p^\alpha)) = 1$. So $V(qp^\alpha) \nmid qp^\alpha$. We use computer calculations to show that $V(n) \nmid n$ up to a large n such that n is not a product of distinct primes. Does $V(n) \nmid n$ for all n which is not a product of distinct primes?

2. Let $V_1(n) = V(n)$ and for all $j \geq 1$, $V_{j+1}(n) = V(V_j(n))$. Since n is a finite number and $V_{j+1}(n) \leq V_j(n)$, then for each n , there exist k and m such that $m = V_k(n) = V_j(n)$ for all $j \geq k$. Can one estimate k and m for each number n ?
3. For all $n \geq 2 \times 10^9$, $V(n) > \varphi(n) > \frac{n}{2 \ln(\ln n)}$, see [4]. Is it true that for all $n \geq 9$, $V(n) > \frac{n}{2 \ln(\ln n)}$? In fact we verified this using computer calculations for very large values of n .

References

- [1] Abu Osba, E., Henriksen, M., Alkam, O., Smith, F.: The maximal regular ideal of some commutative rings. *Comment. Math. Univ. Carolinae.* **47(1)**, 1-10 (2006).
- [2] Apostol, T.: *Mathematical analysis*, Addison -Wesley Publication Company, Inc, 1957.
- [3] Contessa, M.: On certain classes of PM-rings, *Communications in Algebra* **12**, 1447-1469 (1984).
- [4] Luca, F.: Equations involving arithmetic functions of factorials, *Divulgaciones Matemáticas* **8 (1)**, 15-23 (2000).
- [5] Niven, I., Zuckerman, H., Montgomery, H.: *An introduction to the theory of numbers*, John Wiley & Sons, Inc. 5th edition, 1991.
- [6] Sivaramakrishnan, R.: The many facets of Euler's Totient, I: A general perspective, *Nieuw Arch. Wisk.* **4**, 175-190 (1986).
- [7] Sivaramakrishnan, R.: *Classical Theory of arithmetic functions. Monographs and Textbooks in Pure and Applied Mathematics*, **126**. Marcel Dekker, Inc., New York, 1989.

Osama ALKAM
 Department of Mathematics,
 University of Jordan
 Amman 11942, JORDAN
 e-mail: oalkam@ju.edu.jo
 Emad Abu OSBA
 Department of Mathematics,
 University of Jordan
 Amman 11942, JORDAN
 e-mail: eabuosba@ju.edu.jo

Received 05.10.2006