R-Regular Integers Modulo n^r

M. GaneshwarRao[a]

[a]Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, Telangana

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Introducing the notion of ar-regular integer modulo n^r we obtain some basic properties of such integers and arithmetic properties of certain functions related to them.

Keywords: r-regular integer modulo n^r, unitary divisor, r-free integer, r-gcd of two integers

1. Introduction

Let r be a fixed positive integer. A positive integer a is said to be r-regular modulo n^r if there is an integer x such that $a^{r+1}x \equiv a^r \left(\bmod n^r\right).$ The case $r=1$ gives the notion of aregular integer moduleon, introduced by (Morgado, J, 1972; Morgado J , 1974) who made an investigation of their properties.

Clearly $a=0$ is r-regular modulo n^r for every $n \geq 1.$ Also if $a \equiv b\left(\bmod n^r\right)$ then a and b are r-regular modulo n^r simultaneously. Further, if a and b are r-regular modulo n^r then so is ab.

For positive integers a and b their greatest r$^{\text{th}}$ power common divisor is denoted by $(a,\ b)_r$ and is called the r-gcd of a and b. Note that $(a,\ b)_1 = (a,\ b),$ the gcd of a and b.

We recall the notions given in (McCarthy, 1985):

A complete set of residues modulo n^r is called a $(n,\ r)$-residue system. $C_{n,\ r} = \left\{a : 1 \leq a \leq n^r\right\}$ is the minimal $(n,\ r)$-residue system.The set of all a in an $(n,\ r)$-residue system such that $\left(a,\ n^r\right)_r = 1$ is called a reduced $(n,\ r)$-residue system. $R_{n,\ r} = \left\{a \in C_{n,\ r}\ :\ \left(a,\ n^r\right)_r = 1\right\}$ is the minimal reduced $(n,\ r)$-residue system.

(V.L.Klee, 1948) defined a generalization φ_r of the Euler's function by $\varphi_r(n) = \#\left\{a : 1 \leq a \leq n \text{ and } (a,\ n)_r = 1\right\}$ and proved that

$$\varphi_r(n) = \sum_{d|n} \mu_r(d).\frac{n}{d}, \qquad \text{------------------------- (1)}$$

Where μ_r is the r-analogue of the Mobius function μ given by

$$\mu_r(n) = \begin{cases} 1 & \text{if } n=1 \\ (-1)^t & \text{if } n = \left(p_1 p_2 ... p_t\right)^r \text{ where } p_1 < p_2 < ... < p_t \text{ are primes} \\ 0 & \text{otherwise} \end{cases} \qquad \text{------ (2)}$$

Note that $\mu_1 = \mu$ and that $\varphi_r(n^r) = \# R_{n,\, r}$.

Let $\mathrm{Reg}_r(n) = \{a \in C_{n,\, r} : a \text{ is r-regular modulo } n^r\}$ and $\rho_r(n^r) = \# \mathrm{Reg}_r(n)$.

Observe that any $a \in R_{n,\, r}$ is in $\mathrm{Reg}_r(n)$. In fact, if $a \in R_{n,\, r}$ then $(a,\, n^r)_r = 1$ so that $(a,\, n^r) = 1$ and therefore there is an integer x_0 such that $a\, x_0 \equiv 1 (\bmod\, n^r)$ which gives $a^{r+1} x_0 \equiv a^r (\bmod\, n^r)$ showing $a \in \mathrm{Reg}_r(n)$. Hence $\varphi_r(n^r) < \rho_r(n^r) \le n^r$ for every $n > 1$, with $\rho_r(n^r) = n^r$ if and only if n is squarefree.

Recently (Laszlo Toth, 2008; Yokesh, T.L., 2020) has studied several properties of the function $\rho(n) := \rho_1(n)$.

In this paper we prove some basic properties of the integers in the set $\mathrm{Reg}_r(n)$ and certain arithmetic properties of the function $\rho_r(n^r)$

2. Integers in Reg$_r$*(n)*

In all that follows $n > 1$ be of the canonical form:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t},$$

where $p_1 < p_2 < \ldots < p_t$ are primes and α_i are integers ≥ 1.

Theorem 1. For an integer $a \ge 1$ the following are equivalent:

1.1 $a \in \mathrm{Reg}_r(n)$

1.2 for every $i \in \{1,\ 2,\ \ldots,\ t\}$ we have either $p_i \nmid a$ or $p_i^{\alpha_i r} \mid a^r$

1.3 $(a,\, n^r)_r \| n^r$, ($d \| m$ means that $d \mid m$ and $\left(d,\, \frac{m}{d}\right) = 1$, in which case d is called a unitary divisor of m)

1.4 $a^{\varphi_r(n^r) + r} \equiv a^r (\bmod\, n^r)$

1.5 There is an integer $k \ge 1$ such that $a^{k+r} \equiv a^r (\bmod\, n^r)$.

Proof: Suppose $a \in \mathrm{Reg}_r(n)$ so that $a^{r+1} x_0 \equiv a^r (\bmod\, n^r)$ for some integer x_0. Therefore for each $i (1 \le i \le t),\ p_i^{\alpha_i r} \mid a^r (a x_0 - 1)$. Since $(a,\, a x_0 - 1) = 1$ we have $(a^r,\, a x_0 - 1) = 1$, we have either $p_i \nmid a$ or $p_i \mid a^r$ for each i, and in the latter case it follows $p_i^{\alpha_i r} \mid a^r$. Thus (i) $\Rightarrow$ (ii).

Assume (ii). That is, a is an integer ≥ 1 such that either $p_i \nmid a$ or $p_i^{\alpha_i r} \mid a^r$. We have to show $a \in \mathrm{Reg}_r(n)$.

In case $p_i \nmid a$ then $(a,\, p_i^{\alpha_i r}) = 1$ so that there is an integer x_i with $a\, x_i \equiv 1 (\bmod\, p_i^{\alpha_i r})$ and hence $a^{r+1} x_i \equiv a^r (\bmod\, p_i^{\alpha_i r})$.

In case $p_i^{\alpha_i r} \mid a^r$ then for any integer x, $a^{r+1}x \equiv a^r \left(\bmod p_i^{\alpha_i r}\right)$ holds. Thus $a^{r+1}x \equiv a^r \left(\bmod p_i^{\alpha_i r}\right)$ is solvable for $1 \le i \le t$ and hence $a^{r+1}x \equiv a^r \left(\bmod p_1^{\alpha_1 r}.p_2^{\alpha_2 r}....p_t^{\alpha_t r}\right)$ is solvable, showing $a \in \mathrm{Reg}_r(n)$. Thus (ii) $\Rightarrow$ (i).

Note that (ii) holds $\Leftrightarrow a^r = a_0.d^r$, where $d^r = \prod_{p_i \mid a} p_i^{\alpha_i r}$ and $(a_0, n) = 1$

$\Leftrightarrow \left(a^r, n^r\right) = d^r$, which is a unitary divisor of n^r

$\Leftrightarrow \left(a, n^r\right)_r = d^r \| n^r$, since $\left(a^r, n^r\right) = \left(a, n^r\right)_r$. Thus (ii) $\Leftrightarrow$ (iii).

(ii) $\Rightarrow$ (iv). If $p_i^{\alpha_i r} \mid a^r$ then $a^{\varphi_r\left(n^r\right)+r} \equiv a^r \left(\bmod n^r\right)$ is obvious. If $p_i \nmid a$, then by Euler-Fermat Theorem, $a^{\varphi\left(p_i^{\alpha_i r}\right)} \equiv 1 \left(\bmod p_i^{\alpha_i r}\right)$ so that

$$a^{\varphi_r\left(n^r\right)} = \left[a^{\varphi\left(p_i^{\alpha_i r}\right)}\right]^{\varphi_r\left(n^r\right)/\varphi\left(p_i^{\alpha_i r}\right)} \equiv 1 \left(\bmod p_i^{\alpha_i r}\right),$$

since

$$m := \frac{\varphi_r\left(n^r\right)}{\varphi\left(p_i^{\alpha_i r}\right)} = \frac{\varphi_r\left(p_1^{\alpha_1 r}\right)\varphi_r\left(p_2^{\alpha_2 r}\right)...\varphi_r\left(p_t^{\alpha_t r}\right)}{\varphi\left(p_i^{\alpha_i r}\right)} = \left(\prod_{j \ne i} \varphi_r\left(p_j^{\alpha_j r}\right)\right)\frac{\varphi_r\left(p_i^{\alpha_i r}\right)}{\varphi\left(p_i^{\alpha_i r}\right)}$$

$= \left(1 + p_i + ... + p_i^{r-1}\right)$. Mwhere $M = \prod_{j \ne i} \varphi_r\left(p_j^{\alpha_j r}\right)$ so that mis an integer.

Thus $a^{\varphi_r\left(n^r\right)+r} \equiv a^r \left(\bmod p_i^{\alpha_i r}\right)$ for $1 \le i \le t$, giving (iv)

(iv) $\Rightarrow$ (i). If $a^{\varphi_r\left(n^r\right)+r} \equiv a^r \left(\bmod n^r\right)$ then $a^{r+1}.x_0 \equiv a^r \left(\bmod n^r\right)$ where $x_0 = a^{\varphi_r\left(n^r\right)-1}$ showing $a \in \mathrm{Reg}_r(n)$.

(iv) $\Rightarrow$ (v) is immediate with $k = \varphi_r\left(n^r\right)$. Also if $a^{k+r} \equiv a^r \left(\bmod n^r\right)$ for some $k \ge 1$ implies $a^{r+1}.x_0 \equiv a^r \left(\bmod n^r\right)$, where $x_0 = a^{k-1}$, showing $a \in \mathrm{Reg}_r(n)$. Thus (v) $\Rightarrow$ (i).

3. The Function $\rho_r\left(n^r\right)$.

In this section we study the function $\rho_r\left(n^r\right)$ and its relation with $\varphi_r\left(n^r\right)$. Also we express the sum $S_r(n)$ of the r-regular integers modulo n^r in terms of $\rho_r\left(n^r\right)$

$$\rho_r\left(n^r\right)=\sum_{d^r\|n^r}\varphi_r\left(d^r\right).$$

Theorem 2: For every $n\geq 1,$

The function $\rho_r\left(n^r\right)$ is multiplicative and $\rho_r\left(p^{\alpha r}\right)=p^{\alpha r}-p^{(\alpha-1)r}+1,$ for any prime pand integer $\alpha\geq 1.$

Proof: We give two proofs for the first part.

First Proof: Let $a\in \mathrm{Reg}_r\left(n\right).$

If $p_i \nmid a$ for $1\leq i\leq t$ then $\left(a,\ n\right)=1$ so that $\left(a,\ n^r\right)_r=\left(a^r,\ n^r\right)=1$ and the number of such as $\varphi_r\left(n^r\right)$.

Suppose $p_i^{\alpha_i r}\left|a^r\right.$ for exactly one i so that $\left(a,\ p_j\right)=1$ for $j\neq i$ and $a=b.p_i^{\alpha_i r}$ where $1\leq b\leq \frac{n^r}{p_i^{\alpha_i r}}$ and $\left(b,\ \frac{n^r}{p_i^{\alpha_i r}}\right)=1;$ the number of such a's is $\varphi_r\left(\frac{n^r}{p_i^{\alpha_i r}}\right).$

Suppose $p_i^{\alpha_i r}\left|a^r\right.$ and $p_j^{\alpha_j r}\left|a^r\right.$ for $1\leq i<j\leq t;$ and for $k\notin\{i,\ j\}$ $\left(p_k,\ a\right)=1.$ Then $a=C.p_i^{\alpha_i r}.p_j^{\alpha_j r},$ where $1\leq C\leq \frac{n^r}{p_i^{\alpha_i r}p_j^{\alpha_j r}}$ and $\left(C,\ \frac{n^r}{p_i^{\alpha_i r}p_j^{\alpha_j r}}\right)=1;$ and the number of such integers is $\varphi_r\left(\frac{n^r}{p_i^{\alpha_i r}.p_j^{\alpha_j r}}\right);$ and so on. Thus

$$\rho_r\left(n^r\right)=\varphi_r\left(n^r\right)+\sum_{1\leq i\leq t}\varphi_r\left(\frac{n^r}{p_i^{\alpha_i r}}\right)+\sum_{1\leq i<j\leq t}\varphi_r\left(\frac{n^r}{p_i^{\alpha_i r}p_j^{\alpha_j r}}\right)+\ldots+\varphi_r\left(\frac{n^r}{p_i^{\alpha_i r}p_2^{\alpha_2 r}\ldots p_t^{\alpha_t r}}\right)$$

$$=y+\sum_{1\leq i\leq t}\frac{y}{y_i}+\sum_{1\leq i<j\leq t}\frac{y}{y_iy_j}+\ldots+\frac{y}{y_1y_2\ldots y_t}$$

Where $y_i=\varphi_r\left(p_i^{\alpha_i r}\right)$ and $y=y_1y_2\ldots y_t.$

Therefore

$$\rho_r\left(n^r\right)=\left(y_1+1\right)\left(y_2+1\right)\ldots\left(y_t+1\right)$$

$$=\left(\varphi_r\left(p_1^{\alpha_1 r}\right)+1\right)\left(\varphi_r\left(p_2^{\alpha_2 r}\right)+1\right)\ldots\left(\varphi_r\left(p_t^{\alpha_t r}\right)+1\right)$$

$$=\sum_{d^r\|n^r}\varphi_r\left(\frac{n^r}{d^r}\right)=\sum_{d^r\|n^r}\varphi_r\left(d^r\right).$$

Second Proof: Groupthe integers $a \in C_{n,\, r}$ according to the value $\left(a,\, n^r\right)_r = d^r$.

Note that $\left(a,\, n^r\right)_r = d^r \Leftrightarrow a = j.d^r$ where $1 \le j \le \dfrac{n^r}{d^r}$ and $\left(j,\, \dfrac{n^r}{d^r}\right)_r = 1.$ Hence the number of a's in $C_{n,\, r}$ with $\left(a,\, n^r\right)_r = d^r$ is $\varphi_r\left(\dfrac{n^r}{d^r}\right)$. Thus $\rho_r\left(n^r\right) = \sum_{d^r \| n^r} \varphi_r\left(\dfrac{n^r}{d^r}\right) = \sum_{d^r \| n^r} \varphi_r\left(d^r\right).$

Now
$$\rho_r\left(n^r\right) = \sum_{D \| n^r} \varphi_r\left(D\right).\chi_r\left(D\right), \qquad \text{--------------------------- (3)}$$

where $\chi_r\left(m\right) = 1$ or 0 according as m is therth power of an integer or not.

Therefore $\rho_r\left(n^r\right) = \left(\varphi_r \chi_r \circ I\right)\left(n^r\right),$ where $I\left(n\right) \equiv 1$ for all n and $\circ$ is the unitary convolution of arithmetic functions discussed by (Eckford Cohen, 1960). Since unitary convolution preserves multiplicativity, we get

$\rho_r\left(n^r\right)$ is multiplicative, because $\varphi_r,\, \chi_r$ and I are all multiplicative.

Also $\rho_r\left(p^{\alpha r}\right) = \varphi_r\left(p^{\alpha r}\right) + 1 = p^{\alpha r} - p^{(\alpha - 1)r} + 1,$ completing the proof of Theorem B.

Theorem 3. $\displaystyle\sum_{\substack{a \in C_{n,\, r} \\ \left(a,\, n^r\right)_r = 1}} a = \frac{1}{2} n^r.\varphi_r\left(n^r\right)$ for $n > 1.$

Proof: First observe that for positive integers a and b, $\left(a,\, b\right)_r = 1$ if and only if $\left(a,\, b\right)$ is r-free (Recall that an integer not divisible by the rth power of any prime is said to be r-free). Let $q_r\left(m\right) = 1$ or 0 according as m is r-free or not. Then it is well-known (Apostol, 1998, problem 6, p.47; Ranjeeth 2020) that

$$q_r\left(m\right) = \sum_{t^r | m} \mu\left(t\right), \qquad \text{----------------------(4)}$$

Where μ is the Mobius function

Now, by (4) and (1), we get

$$\sum_{\substack{a \in C_{n,\, r} \\ \left(a,\, n^r\right)_r = 1}} a = \sum_{1 \le a \le n^r} a.q_r\left(\left(a,\, n^r\right)\right)$$

$$= \sum_{1\le a\le n^r} a \left\{ \sum_{\substack{t^r s=a \\ t^r | n^r}} \mu(t) \right\}$$

$$= \sum_{\substack{t^r s\le n^r \\ t^r | n^r}} t^r s \mu(t)$$

$$= \sum_{t^r | n^r} \mu(t) t^r \left\{ \sum_{s\le \frac{n^r}{t^r}} s \right\}$$

$$= \sum_{t^r | n^r} \mu(t) t^r . \frac{1}{2} . \frac{n^r}{t^r} \left(\frac{n^r}{t^r} + 1 \right)$$

$$= \frac{n^r}{2} \sum_{t^r | n^r} \mu(t) \frac{n^r}{t^r} + \frac{n^r}{2} \sum_{t^r | n^r} \mu(t)$$

$$= \frac{n^r}{2} . \sum_{t_\circ | n^r} \mu(t_\circ) \frac{n^r}{t_\circ} + \frac{n^r}{2} \sum_{t^r | n^r} \mu(t)$$

$$= \frac{n^r}{2} . \varphi_r \left(n^r\right),$$

since $\sum_{t^r | n^r} \mu(t) = 0$ for $n > 1$.

Remark 1. The case $r = 1$ of Theorem C is the well-known formula:

$$\sum_{\substack{1\le a\le n \\ (a,\, n)=1}} a = \frac{n\varphi(n)}{2} \text{ for } n > 1.$$ (For example see (Apostol, 1998, Problem 16, *p*.48)

Theorem 4. If $S_r(n) := \sum_{a\in \mathrm{Reg}_{r(n)}} a$ then $S_r(n) = \frac{1}{2}\left[\rho_r\left(n^r\right)+1\right]$ for $n \ge 1$.

Proof: We have, by Theorem A, that $a \in \mathrm{Reg}_r(n) \Leftrightarrow \left(a,\ n^r\right)_r = d^r \| n^r$.

Therefore

$$S_r(n) = \sum_{\substack{a \in C_{r,n} \\ (a,\, n^r)_r \| n^r}} a = \sum_{d^r \| n^r} \sum_{\substack{(a,\, n^r)_r = d^r \\ a \in C_{r,n}}} a$$

$= \sum_{d^r \| n^r} d^r \sum_{\substack{j \in C_{\frac{n^r}{d^r}, r} \\ \left(j, \frac{n^r}{d^r}\right)_r = 1}} j$, Since $(a,\, n^r)_r = d^r \Leftrightarrow a = j.d^r$ where $1 \le j \le \dfrac{n^r}{d^r}$ and $\left(j,\, \dfrac{n^r}{d^r}\right)_r = 1.$

Now, in view of Theorem C and Theorem B, for $n \ge 1$ we have

$$S_r(n) = n^r + \sum_{\substack{d^r \| n^r \\ d^r < n^r}} d^r . \frac{1}{2} . \frac{n^r}{d^r} . \varphi^r\left(\frac{n^r}{d^r}\right)$$

$$= n^r + \frac{n^r}{2} \sum_{\substack{d^r \| n^r \\ d^r < n^r}} \varphi^r\left(\frac{n^r}{d^r}\right)$$

$$= n^r + \frac{n^r}{2} . \left[\rho_r\left(n^r\right) - 1\right]$$

$$= \frac{n^r}{2}\left[\rho_r\left(n^r\right) + 1\right],$$

proving the theorem.

References

1. Apostol, Tom M., (1998*) Introduction to Analytic Number Theory, Springer International Student Edition, Naroso Publishing House, New Delhi, 1998.*
2. Eckford Cohen, (1960)*Arithmetical Functions Associated with the Unitary Divisors of an Integer, Math. Zeitschr. 74, 66-80.*
3. Klee, V. L, (1948)*Generalization of Euler's Function, Amer. Math., Monthly, 55, 358-359.*
4. Laszlo Toth, Regular Integers Modulo n, (2008) *AnnalsUniv. Sci. Budapest., Sect. Comp. 29, 263-275.*
5. McCarthy, Paul J., (1985). *Introduction to Arithmetical Functions, Springer-Verlag, New York.*
6. Morgado, J, (1972). *InteiorsRegulares Modulo n, Gazeta de Mathematical (Lisboa), 33,.125-125, 1-5.*
7. Morgado, J. (1974)*A Property of the Euler φ-Function Concerning the Integers which are Regular Modulo n, Portugal. Math., 33, 185-191.*
8. Ranjeeth, S., Latchoumi, T. P., & Paul, P. V. (2020). *Role of gender on academic performance based on different parameters: Data from secondary school education. Data in brief, 29, 105257.*
9. Yookesh, T. L., Boobalan, E. D., & Latchoumi, T. P. (2020, March). *Variational Iteration Method to Deal with Time Delay Differential Equations under Uncertainty Conditions. In 2020 International Conference on Emerging Smart Computing and Informatics (ESCI) (pp. 252-256). IEEE.*