Regular integers modulo n

László Tóth (Pécs, Hungary)

October 10, 2007

Abstract

Let $n = p_1^{\nu_1} \cdots p_r^{\nu_r} > 1$ be an integer. An integer a is called regular (mod n) if there is an integer x such that $a^2x \equiv a$ (mod n). Let $\varrho(n)$ denote the number of regular integers a (mod n) such that $1 \le a \le n$. Here $\varrho(n) = (\phi(p_1^{\nu_1}) + 1) \cdots (\phi(p_r^{\nu_r}) + 1)$, where $\phi(n)$ is the Euler function. In this paper we first summarize some basic properties of regular integers (mod n). Then in order to compare the rates of growth of the functions $\varrho(n)$ and $\phi(n)$ we investigate the average orders and the extremal orders of the functions $\varrho(n)/\phi(n)$, $\phi(n)/\varrho(n)$ and $1/\varrho(n)$.

Mathematics Subject Classification: 11A25, 11N37

Key Words and Phrases: regular integers (mod n), unitary divisor, Euler's function, average order, extremal order

1. Introduction

Let $n > 1$ be an integer. Consider the integers a for which there exists an integer x such that $a^2x \equiv a$ (mod n). In the background of this property is that an element a of a ring R is said to be regular (following J. von Neumann) if there is an $x \in R$ such that $a = axa$. In case of the ring $\mathbb{Z}_n$ this is exactly the condition of above.

Properties of these integers were investigated by J. Morgado [7], [8], who called them regular (mod n). In a recent paper O. Alkam and E. A. Osba [1] using ring theoretic considerations rediscovered some of the statements proved elementarly by J. Morgado. It was observed in [7], [8] that $a > 1$ is regular (mod n) if and only if the gcd (a, n) is a unitary divisor of n. We recall that d is said to be a unitary divisor of n if $d \mid n$ and gcd $(d, n/d) = 1$, notation $d \,||\, n$.

These integers occur in the literature also in an other context. It is said that an integer a possesses a weak order (mod n) if there exists an integer $k \ge 1$ such that $a^{k+1} \equiv a$ (mod n). Then the weak order of a is the smallest k with this property, see [4], [2]. It turns out that a is regular (mod n) if and only if a possesses a weak order (mod n).

Let $\text{Reg}_n = \{a : 1 \le a \le n,\ a \text{ is regular (mod } n)\}$ and let $\varrho(n) = \#\,\text{Reg}_n$ denote the number of regular integers a (mod n) such that $1 \le a \le n$. This function is multiplicative and $\varrho(p^\nu) = \phi(p^\nu) + 1 = p^\nu - p^{\nu-1} + 1$ for every prime power p^ν ($\nu \ge 1$), where ϕ is the Euler function. Consequently, $\varrho(n) = \sum_{d||n} \phi(d)$ for every $n \ge 1$, also $\phi(n) < \varrho(n) \le n$ for every $n > 1$, and $\varrho(n) = n$ if and only if n is squarefree, see [7], [4], [1].

Let us compare the functions $\varrho(n)$ and $\phi(n)$. The first few values of $\varrho(n)$ and $\phi(n)$ are given by the next tables ($\varrho(n)$ is sequence $A055653$ in Sloane's On-Line Encyclopedia of Integer Sequences [10]). Note that $\varrho(n)$ is even iff $n \equiv 2$ (mod 4), and $\sqrt{n} \le \rho(n) \le n$ for every $n \ge 1$, see [1].

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\varrho(n)$	1	2	3	3	5	6	7	5	7	10	11	9	13	14	15
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8

n	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\varrho(n)$	9	17	14	19	15	21	22	23	15	21	26	19	21	29	30
$\phi(n)$	8	16	6	18	8	12	10	22	8	20	12	18	12	28	8

For the Euler ϕ-function,

$$\lim_{x\to\infty} \frac{1}{x^2} \sum_{n\le x} \phi(n) = \frac{3}{\pi^2} \approx 0.3039.$$

The average order of the function $\varrho(n)$ was considered in [4], [2]. One has

$$\lim_{x\to\infty} \frac{1}{x^2} \sum_{n\le x} \varrho(n) = \frac{1}{2} A \approx 0.4407,$$

where

$$A = \prod_p \left(1 - \frac{1}{p^2(p+1)}\right) = \zeta(2) \prod_p \left(1 - \frac{1}{p^2} - \frac{1}{p^3} + \frac{1}{p^4}\right) \approx 0.8815$$

is the so called quadratic class-number constant. For its numerical evaluation see [9].

More exactly,

$$\sum_{n\le x} \varrho(n) = \frac{1}{2} A x^2 + R(x),$$

where $R(x) = O(x \log^3 x)$, given in [4] using elementary arguments. This was improved into $R(x) = O(x \log^2 x)$ in [12], and into $R(x) = O(x \log x)$ in [3], using analytic methods. Also, $R(x) = \Omega_{\pm}(x\sqrt{\log\log x})$, see [3].

In this paper we first summarize some basic properties of regular integers (mod n). We give also their direct proofs, because the proofs of [7], [8] are lengthy and those of [1] are ring theoretical.

Then in order to compare the rates of growth of the functions $\varrho(n)$ and $\phi(n)$ we investigate the average orders and the extremal orders of the functions $\varrho(n)/\phi(n)$, $\phi(n)/\varrho(n)$ and $1/\varrho(n)$. The study of the minimal order of $\varrho(n)$ was initiated in [1].

2. Characterization of regular integers (mod n)

The integer $a = 0$ and those coprime to n are regular (mod n) for each $n > 1$. If $a \equiv b$ (mod n), then a and b are regular (mod n) simultaneously. If a and b are regular (mod n), then ab is also regular (mod n).

In what follows let $n > 1$ be of canonical form $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$.

Theorem 1. *For an integer $a \ge 1$ the following assertions are equivalent:*
i) a is regular (mod n),
ii) for every $i \in \{1, ..., r\}$ either $p_i \nmid a$ or $p_i^{\nu_i} \mid a$,
iii) $(a, n) = (a^2, n)$,
iv) $(a, n) \,||\, n$,
v) $a^{\phi(n)+1} \equiv a$ (mod n),
vi) there exists an integer $k \ge 1$ such that $a^{k+1} \equiv a$ (mod n).

Proof. i) $\Rightarrow$ ii). If $a^2 x \equiv a$ (mod n) for an integer x, then $a(ax - 1) \equiv 0$ (mod $p_i^{\nu_i}$) for every i. We have two cases: $p_i \nmid a$ and $p_i \mid a$. In the second case, since $(a, ax - 1) = 1$, obtain that $a \equiv 0$ (mod $p_i^{\nu_i}$).

ii) $\Rightarrow$ i). If $p_i^{\nu_i} \mid a$, then $a^2 x \equiv a$ (mod $p_i^{\nu_i}$) for any x. If $p_i \nmid a$, then the linear congruence $ax \equiv 1$ (mod $p_i^{\nu_i}$) has solutions in x and obtain also $a^2 x \equiv a$ (mod $p_i^{\nu_i}$).

ii) $\Leftrightarrow$ iii). Follows at once by the property of the gcd.

ii) $\Leftrightarrow$ iv) Follows at once by the definition of the unitary divisors (the unitary divisors of a prime power p^ν are 1 and p^ν).

ii) $\Rightarrow$ v) ([1]) If $p_i^{\nu_i} \mid a$, then $a^{\phi(n)+1} \equiv a$ (mod $p_i^{\nu_i}$). If $p_i \nmid a$, then using Euler's theorem, $a^{\phi(n)+1} \equiv a(a^{\phi(p_i^{\nu_i})})^{\phi(n)/\phi(p_i^{\nu_i})} \equiv a$ (mod $p_i^{\nu_i}$). Therefore $a^{\phi(n)+1} \equiv a$ (mod $p_i^{\nu_i}$) for every i and $a^{\phi(n)+1} \equiv a$ (mod n).

v) $\Rightarrow$ i) ([1]) If $a^{\phi(n)+1} \equiv a$ (mod n), then $a^2 a^{\phi(n)-1} \equiv a$ (mod n), hence $a^2 x \equiv a$ (mod n) is verified for $x = a^{\phi(n)-1}$ (which is the von Neumann inverse of a in $\mathbb{Z}_n$).

v) $\Rightarrow$ vi) Immediate by taking $k = \phi(n)$.

vi) $\Rightarrow$ i) If $a^{k+1} \equiv a$ (mod n) for an integer $k \ge 1$, then $a^2 x \equiv a$ (mod n) holds for $x = a^{k-1}$, finishing the proof.

Note that the proof of i) $\Leftrightarrow$ v) given in [8] uses Dirichlet's theorem on arithmetic progressions, which is unnecessary.

Theorem 2. *The function $\varrho(n)$ is multiplicative and $\varrho(p^\nu) = p^\nu - p^{\nu-1} + 1$ for every prime power p^ν ($\nu \ge 1$). For every $n \ge 1$,*

$$\varrho(n) = \sum_{d||n} \phi(d).$$

Proof. By Theorem 1, a is regular (mod n) iff for every $i \in \{1, ..., r\}$ either $p_i \nmid a$ or $p_i^{\nu_i} \mid a$.

Let $a \in \text{Reg}_n$. If $p_i \nmid a$ for every i, then $(a, n) = 1$, the number of these integers a is $\phi(n)$. Suppose that $p_i^{\nu_i} \mid a$ for exactly one value i and that for all $j \ne i$, $(p_j, a) = 1$. Then $a = bp_i^{\nu_i}$, where $1 \le b \le n/p_i^{\nu_i}$ and $(b, n/p_i^{\nu_i}) = 1$. The number of such integers a is $\phi(n/p_i^{\nu_i})$. Now suppose that $p_i^{\nu_i} \mid a$, $p_j^{\nu_j} \mid a$, $i < j$, and for all $k \ne i, k \ne j$, $(p_i, a) = (p_j, a) = 1$. Then $a = cp_i^{\nu_i} p_j^{\nu_j}$, where $1 \le c \le n/(p_i^{\nu_i} p_j^{\nu_j})$ and $(c, n/(p_i^{\nu_i} p_j^{\nu_j})) = 1$. The number of such integers a is $\phi(n/(p_i^{\nu_i} p_j^{\nu_j}))$, etc. We obtain

$$\varrho(n) = \phi(n) + \sum_{1\le i\le r} \phi(n/p_i^{\nu_i}) + \sum_{1\le i<j\le r} \phi(n/p_i^{\nu_i} p_j^{\nu_j}) + ... + \phi(n/(p_1^{\nu_1} \cdots p_r^{\nu_r})).$$

Let $y_i = \phi(p_i^{\nu_i})$, $1 \le i \le r$, and $y = y_1 \cdots y_r$. Then $\phi(n) = y$ and

$$\varrho(n) = y + \sum_{1\le i\le r} \frac{y}{y_i} + \sum_{1\le i<j\le r} \frac{y}{y_i y_j} + ... + \frac{y}{y_1 \cdots y_r} =$$

$$= (y_1 + 1) \cdots (y_r + 1) = (\phi(p_1^{\nu_i}) + 1) \cdots (\phi(p_r^{\nu_r}) + 1).$$

The given representation of $\varrho(n)$ now follows at once taking into account that the unitary convolution preserves the multiplicativity of functions, see for example [5].

Another method, see [7]: Group the integers $a \in \{1, 2, ..., n\}$ according to the value (a, n). Here $(a, n) = d$ if and only if $(j, n/d) = 1$, where $a = jd$, $1 \le j \le n/d$, hence the number of integers a with $(a, n) = d$ is $\phi(n/d)$. According to Theorem 1, a is regular (mod n) if and only if $d = (a, n) \,||\, n$, and obtain that

$$\varrho(n) = \sum_{d||n} \phi(n/d) = \sum_{d||n} \phi(d).$$

Now the multiplicativity of $\varrho(n)$ is a direct consequence of this representation.

Let $S(n)$ denote the sum of regular integers $a \in \text{Reg}_n$. We give a simple formula for $S(n)$, not considered in the cited papers, which is analogous to $\sum_{1\le a\le n, (a,n)=1} a = n\phi(n)/2$ ($n > 1$).

Theorem 3. *For every $n \ge 1$,*

$$S(n) = \frac{n(\varrho(n) + 1)}{2}.$$

Proof. Similar to the counting procedure of above or by grouping the integers $a \in \{1, 2, ..., n\}$ according to the value (a, n):

$$S(n) = \sum_{a\in \text{Reg}_n} a = \sum_{d||n} \sum_{\substack{a\in \text{Reg}_n \\ (a,n)=d}} a = \sum_{d||n} d \sum_{\substack{j=1 \\ (j,n/d)=1}}^{n/d} j =$$

$$= n + \sum_{\substack{d||n \\ d<n}} d \frac{n\phi(n/d)}{2d} = n + \frac{n}{2} \sum_{\substack{d||n \\ d<n}} \phi(n/d) = \frac{n(\varrho(n) + 1)}{2}.$$

3. Average orders

Theorem 4. *For the quotient $\varrho(n)/\phi(n)$ we have*

$$\sum_{n\le x} \frac{\varrho(n)}{\phi(n)} = Bx + O(\log^2 x),$$

where $B = \pi^2/6 \approx 1.6449$.

Proof. By Theorem 2, $\varrho(p^\nu)/\phi(p^\nu) = 1 + 1/\phi(p^\nu)$ for every prime power p^ν ($\nu \geq 1$). Hence, taking into account the multiplicativity, for every $n \geq 1$,

$$\frac{\varrho(n)}{\phi(n)} = \sum_{d||n} \frac{1}{\phi(d)}.$$

Using this representation (given also in [1]) we obtain

$$\sum_{n\leq x} \frac{\varrho(n)}{\phi(n)} = \sum_{\substack{de\leq x\\(d,e)=1}} \frac{1}{\phi(d)} = \sum_{d\leq x} \frac{1}{\phi(d)} \sum_{\substack{e\leq x/d\\(e,d)=1}} 1 =$$

$$= \sum_{d\leq x} \frac{1}{\phi(d)} \left(\frac{\phi(d)x}{d^2} + O(2^{\omega(d)}) \right) = x \sum_{d\leq x} \frac{1}{d^2} + O\left(\sum_{d\leq x} \frac{2^{\omega(d)}}{\phi(d)} \right),$$

where $\omega(d)$ denotes, as usual, the number of distinct prime factors of d. Furthermore, let $\tau(n)$ and $\sigma(n)$ denote the number and the sum of divisors of n, respectively. Using that $\phi(n)\sigma(n) \gg n^2$, we have $2^{\omega(d)}/\phi(d) \ll \tau(d)\sigma(d)/d^2$. Here $\sum_{d\leq x} \tau(d)\sigma(d) \ll x^2 \log x$, according to a result of Ramanujan, and obtain by partial summation that the error term is $O(\log^2 x)$.

Consider now the quotient $f(n) = \phi(n)/\varrho(n)$, where $f(n) \leq 1$. According to a well-known result of H. Delange, $f(n)$ has a mean value given by

$$C = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \sum_{\nu=1}^\infty \frac{f(p^\nu)}{p^\nu}\right) = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + (1 - \frac{1}{p}) \sum_{\nu=1}^\infty \frac{1}{p^\nu - p^{\nu-1} + 1}\right).$$

Here $C \approx 0.6875$, which can be obtained using that for every $k \geq 1$,

$$C = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + (1 - \frac{1}{p}) \sum_{\nu=1}^k \frac{1}{p^\nu - p^{\nu-1} + 1} + \frac{1}{p^k r_p}\right),$$

where $p - 1 < r_p < p$ for each prime p.

An asymptotic formula can be given as follows.

Theorem 5. *For every* $\varepsilon > 0$,

$$\sum_{n\leq x} \frac{\phi(n)}{\varrho(n)} = Cx + O(x^\varepsilon).$$

Proof. Write $g = \mu * f$ in terms of the Dirichlet convolution, where μ is the Möbius function. Then for every prime p, $g(p) = -1/p$ and for every prime power p^ν, $\nu \geq 2$,

$$g(p^\nu) = \frac{p^{\nu-2}}{(p^{\nu-1} + (p-1)^{-1})(p^{\nu-2} + (p-1)^{-1})}.$$

Since $|g(p^\nu)| < 1/p^{\nu-1}$ for every $\nu \geq 2$, the Dirichlet series $G(s) = \sum_{n=1}^\infty g(n)/n^s$ is absolutely convergent for $\operatorname{Re} s > 0$, and we obtain by usual arguments,

$$\sum_{n\leq x} \frac{\phi(n)}{\varrho(n)} = \sum_{d\leq x} g(d) \left(\frac{x}{d} + O(1)\right) = x \sum_{d\leq x} \frac{g(d)}{d} + O\left(\sum_{d\leq x} |g(d)|\right) = G(1)x + O(x^\varepsilon),$$

where $G(1) = C$ of above.

Theorem 6.

$$\sum_{n\le x} \frac{1}{\varrho(n)} = D\log x + E + O\left(\frac{\log^9 x}{x}\right),$$

where D and E are constants,

$$D = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \prod_p \left(1 - \frac{p(p-1)}{p^2-p+1} \sum_{\nu=1}^{\infty} \frac{1}{p^\nu(p^\nu - p^{\nu-1}+1)}\right).$$

Proof. Write

$$\frac{1}{\varrho(n)} = \sum_{\substack{de=n\\(d,e)=1}} \frac{h(d)}{\phi(e)},$$

where h is multiplicative and for every prime power p^ν,

$$\frac{1}{\varrho(p^\nu)} = h(p^\nu) + \frac{1}{\phi(p^\nu)}, \quad h(p^\nu) = -\frac{1}{\phi(p^\nu)(\phi(p^\nu)+1)},$$

therefore $h(n) \ll 1/\phi^2(n)$. We need the following known result, cf. for example [6], p. 43,

$$\sum_{\substack{n\le x\\(n,k)=1}} \frac{1}{\phi(n)} = Ka(k)\left(\log x + \gamma + b(k)\right) + O\left(2^{\omega(k)}\frac{\log x}{x}\right),$$

where γ is Euler's constant,

$$K = \frac{\zeta(2)\zeta(3)}{\zeta(6)}, \; a(k) = \prod_{p|k}\left(1 - \frac{p}{p^2-p+1}\right) \le \frac{\phi(k)}{k},$$

$$b(k) = \sum_{p|k} \frac{\log p}{p-1} - \sum_{p\nmid k} \frac{\log p}{p^2-p+1} \ll \frac{\psi(k)\log k}{\phi(k)}, \quad \text{with} \quad \psi(k) = k\prod_{p|k}\left(1+\frac{1}{p}\right).$$

We have

$$\sum_{n\le x}\frac{1}{\varrho(n)} = \sum_{d\le x} h(d) \sum_{\substack{e\le x/d\\(e,d)=1}} \frac{1}{\phi(e)} =$$

$$= K\left((\log x + \gamma)\sum_{d\le x} h(d)a(d) + \sum_{d\le x} h(d)a(d)(b(d)-\log d)\right) + O\left(\frac{\log x}{x}\sum_{d\le x} d|h(d)|2^{\omega(d)}\right),$$

and we obtain the given result with the constants

$$D = K\sum_{n=1}^{\infty} h(n)a(n), \; E = K\gamma\sum_{n=1}^{\infty} h(n)a(n) + K\sum_{n=1}^{\infty} h(n)a(n)(b(n)-\log n),$$

these series being convergent taking into account the estimates of above. For the error terms,

$$\sum_{n>x} |h(n)|a(n) \ll \sum_{n>x}\frac{1}{n\phi(n)} \ll \sum_{n>x}\frac{\sigma(n)}{n^3} \ll \frac{1}{x}, \; \sum_{n>x} |h(n)|a(n)\log n \ll \frac{\log x}{x},$$

$$\sum_{n>x} |h(n)a(n)b(n)| \ll \sum_{n>x} \frac{\tau^3(n)\log n}{n^2} \ll \frac{\log^8 x}{x},$$

using that $\sum_{n\le x}\tau^3(n) \ll x\log^7 x$ (Ramanujan), and

$$\sum_{n\le x} n|h(n)|2^{\omega(n)} \ll \sum_{n\le x}\frac{\tau^3(n)}{n} \ll \log^8 x.$$

4. Extremal orders

Since $\varrho(n) \le n$ for every $n \ge 1$ and $\varrho(p) = p$ for every prime p, it is immediate that $\limsup_{n\to\infty} \varrho(n)/n = 1$. The minimal order of $\varrho(n)$ is also the same as that of $\phi(n)$, namely,

Theorem 7.

$$\liminf_{n\to\infty} \frac{\varrho(n)\log\log n}{n} = e^{-\gamma}.$$

Proof. We apply the following result ([11], Corollary 1): If f is a nonnegative real-valued multiplicative arithmetic function such that for each prime p,

i) $\rho(p) := \sup_{\nu\ge 0} f(p^\nu) \le (1-1/p)^{-1}$, and

ii) there is an exponent $e_p = p^{o(1)} \in \mathbb{N}$ satisfying $f(p^{e_p}) \ge 1 + 1/p$,

then

$$\limsup_{n\to\infty} \frac{f(n)}{\log\log n} = e^\gamma \prod_p \left(1 - \frac{1}{p}\right) \rho(p).$$

Take $f(n) = n/\varrho(n)$, where $f(p^\nu) = (1 - 1/p + 1/p^\nu)^{-1} < (1-1/p)^{-1} = \rho(p)$, and for $e_p = 3$,

$$f(p^3) > 1 + \frac{p^2-1}{p^3-p^2+1} > 1 + \frac{1}{p}$$

for every prime p.

It is immediate that $\liminf_{n\to\infty} \varrho(n)/\phi(n) = 1$. The maximal order of $\varrho(n)/\phi(n)$ is given by

Theorem 8.

$$\limsup_{n\to\infty} \frac{\varrho(n)}{\phi(n)\log\log n} = e^\gamma.$$

Proof. Now let $f(n) = \varrho(n)/\phi(n)$ in the result given above. Here

$$f(p^\nu) = 1 + \frac{1}{p^\nu - p^{\nu-1}} \le 1 + \frac{1}{p-1} = \left(1 - \frac{1}{p}\right)^{-1} = \rho(p),$$

and for $e_p = 1$, $f(p) > 1 + 1/(p-1) > 1 + 1/p$ for every prime p.

References

[1] **O. Alkam, E. A. Osba**, On the regular elements in $\mathbb{Z}_n$, *Turk. J. Math.*, **31** (2007), 1-9.

[2] **S. Finch**, Idempotents and nilpotents modulo n, 2006, Preprint available online at http://arxiv.org/abs/math.NT/0605019v1.

[3] **J. Herzog, P. R. Smith**, Lower bounds for a certain class of error functions, *Acta Arith.*, **60** (1992), 289-305.

[4] **V. S. Joshi**, Order-free integers (mod m), Number theory (Mysore, 1981), Lecture Notes in Math., 938, Springer, 1982. pp. 93-100.

[5] **P. J. McCarthy**, Introduction to Arithmetical Functions, Springer, 1986.

[6] **H. L. Montgomery, R. C. Vaughan**, Multiplicative Number Theory I. Classical Theory, Cambridge University Press, 2007.

[7] **J. Morgado**, Inteiros regulares módulo n, *Gazeta de Matematica (Lisboa)*, **33** (1972), no. 125-128, 1-5.

[8] **J. Morgado**, A property of the Euler φ-function concerning the integers which are regular modulo n, *Portugal. Math.*, **33** (1974), 185-191.

[9] **G. Niklasch, P. Moree**, Some number-theoretical constants, 2002, webpage, see
http://www.gn-50uma.de/alula/essays/Moree/Moree.en.shtml#r11-classno

[10] **N. J. A. Sloane**, The On-Line Encyclopedia of Integer Sequences, see
http://www.research.att.com/~njas/sequences

[11] **L. Tóth, E. Wirsing**, The maximal order of a class of multiplicative arithmetical functions, *Annales Univ. Sci. Budapest., Sect. Comp.*, **22** (2003), 353-364.

[12] **Zhao Hua Yang**, A note for order-free integers (mod m), J. China Univ. Sci. Tech. **16** (1986), no. 1, 116-118, MR855194 (88e:11006).

László Tóth
University of Pécs
Institute of Mathematics and Informatics
Ifjúság u. 6
7624 Pécs, Hungary
ltoth@ttk.pte.hu