Journal of Integer Sequences, Vol. 13 (2010),
Article 10.2.1

On the Multiplicative Order of a^n Modulo n

Jonathan Chappelon[1]
Université Lille Nord de France
F-59000 Lille
France
jonathan.chappelon@lmpa.univ-littoral.fr

Abstract

Let n be a positive integer and α_n be the arithmetic function which assigns the multiplicative order of a^n modulo n to every integer a coprime to n and vanishes elsewhere. Similarly, let β_n assign the projective multiplicative order of a^n modulo n to every integer a coprime to n and vanishes elsewhere. In this paper, we present a study of these two arithmetic functions. In particular, we prove that for positive integers n_1 and n_2 with the same square-free part, there exists a relationship between the functions α_{n_1} and α_{n_2} and between the functions β_{n_1} and β_{n_2}. This allows us to reduce the determination of α_n and β_n to the case where n is square-free. These arithmetic functions recently appeared in the context of an old problem of Molluzzo, and more precisely in the study of which arithmetic progressions yield a balanced Steinhaus triangle in $\mathbb{Z}/n\mathbb{Z}$ for n odd.

1 Introduction

We start by introducing some notation relating to the order of certain elements modulo n. For every positive integer n and every prime number p, we denote by $v_p(n)$ the *p-adic valuation* of n, i.e., the greatest exponent $e \geqslant 0$ for which p^e divides n. The prime factorization of n may then be written as

$$n = \prod_{p\in\mathbb{P}} p^{v_p(n)},$$

where $\mathbb{P}$ denotes the set of all prime numbers. We denote by $\mathrm{rad}(n)$ *the radical of* n, i.e., the largest square-free divisor of n, namely

$$\mathrm{rad}(n) = \prod_{\substack{p\in\mathbb{P}\\ p|n}} p.$$

[1]ULCO, LMPA J. Liouville, B.P. 699, F-62228 Calais, France and CNRS, FR 2956, France.

For every positive integer n and every integer a coprime to n, we denote by $\mathcal{O}_n(a)$ *the multiplicative order of a modulo n*, i.e., the smallest positive integer e such that $a^e \equiv 1 \pmod{n}$, namely

$$\mathcal{O}_n(a) = \min \left\{ e \in \mathbb{N}^* \mid a^e \equiv 1 \pmod{n} \right\}$$

and we denote by $\mathcal{R}_n(a)$ the *multiplicative remainder* of a modulo n, i.e., the multiple of n defined by

$$\mathcal{R}_n(a) = a^{\mathcal{O}_n(a)} - 1.$$

The multiplicative order of a modulo n also corresponds with the order of the element $\pi_n(a)$, where $\pi_n : \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ is the canonical surjective morphism, in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$, the group of units of $\mathbb{Z}/n\mathbb{Z}$. Note that $\mathcal{O}_n(a)$ divides $\varphi(n)$, φ being the Euler's totient function.

For every positive integer n, we define and denote by α_n the arithmetic function

$$\begin{array}{rccl} \alpha_n : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & \left\{ \begin{array}{cl} \mathcal{O}_n\left(a^n\right), & \text{for all } \gcd(a,n) = 1; \\ 0, & \text{otherwise,} \end{array} \right. \end{array}$$

where $\gcd(a,n)$ denotes the greatest common divisor of a and n, with the convention that $\gcd(0,n) = n$. Observe that, for every a coprime to n, the integer $\alpha_n(a)$ divides $\varphi(n)/\gcd(\varphi(n),n)$. This follows from the previous remark on $\mathcal{O}_n(a)$ and the equality $\alpha_n(a) = \mathcal{O}_n(a^n) = \mathcal{O}_n(a)/\gcd(\mathcal{O}_n(a),n)$.

For every positive integer n and every integer a coprime to n, we denote by $\mathcal{PO}_n(a)$ *the projective multiplicative order of a modulo n*, i.e., the smallest positive integer e such that $a^e \equiv \pm 1 \pmod{n}$, namely

$$\mathcal{PO}_n(a) = \min \left\{ e \in \mathbb{N}^* \mid a^e \equiv \pm 1 \pmod{n} \right\}.$$

The projective multiplicative order of a modulo n also corresponds with the order of the element $\overline{\pi_n(a)}$ in the multiplicative quotient group $(\mathbb{Z}/n\mathbb{Z})^*/\{-1,1\}$.

For every positive integer n, we define and denote by β_n the arithmetic function

$$\begin{array}{rccl} \beta_n : & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & a & \longmapsto & \left\{ \begin{array}{cl} \mathcal{PO}_n\left(a^n\right), & \text{for all } \gcd(a,n) = 1; \\ 0, & \text{otherwise.} \end{array} \right. \end{array}$$

Observe that we have the alternative $\alpha_n = \beta_n$ or $\alpha_n = 2\beta_n$.

In this paper, we study in detail these two arithmetic functions. In particular, we prove that, for every positive integers n_1 and n_2 such that

$$\left\{ \begin{array}{ll} \operatorname{rad}(n_1) | n_2 \text{ and } n_2 | n_1, & \text{if } v_2(n_1) \leqslant 1; \\ 2\operatorname{rad}(n_1) | n_2 \text{ and } n_2 | n_1, & \text{if } v_2(n_1) \geqslant 2, \end{array} \right.$$

the integer $\alpha_{n_1}(a)$ (respectively $\beta_{n_1}(a)$) divides $\alpha_{n_2}(a)$ (resp. $\beta_{n_2}(a)$), for every integer a. More precisely, we determine the exact relationship between the functions α_{n_1} and α_{n_2} and between β_{n_1} and β_{n_2}. We prove that we have

$$\alpha_{n_1}(a) = \frac{\alpha_{n_2}(a)}{\gcd\left(\alpha_{n_2}(a), \frac{\gcd(n_1,\mathcal{R}_{n_2}(a))}{n_2}\right)} \text{ for all } \gcd(a,n_1) = 1$$

in Theorem 6 of Section 2 and that we have

$$\beta_{n_1}(a) = \frac{\beta_{n_2}(a)}{\gcd\left(\beta_{n_2}(a), \frac{\gcd(n_1,\mathcal{R}_{n_2}(a))}{n_2}\right)} \text{ for all } \gcd(a,n_1)=1$$

in Theorem 13 of Section 3. Thus, for every integer a coprime to n, the determination of $\alpha_n(a)$ is reduced to the computation of $\alpha_{\mathrm{rad}(n)}(a)$ and $\mathcal{R}_{\mathrm{rad}(n)}(a)$ if $v_2(n) \leqslant 1$ and of $\alpha_{2\,\mathrm{rad}(n)}(a)$ and $\mathcal{R}_{2\,\mathrm{rad}(n)}(a)$ if $v_2(n) \geqslant 2$. These theorems on the functions α_n and β_n are derived from Theorem 7 of Section 2, which states that

$$\mathcal{O}_{n_1}(a) = \mathcal{O}_{n_2}(a) \cdot \frac{n_1}{\gcd(n_1, \mathcal{R}_{n_2}(a))},$$

for all integers a coprime to n_1 and n_2. This result generalizes the following theorem of Nathanson which, in the above notation, states that for every odd prime number p and for every positive integer k, we have the equality

$$\mathcal{O}_{p^k}(a) = \mathcal{O}_p(a) \cdot \frac{p^k}{\gcd(p^k, \mathcal{R}_p(a))}$$

for all integers a not divisible by p.

Theorem 3.6 of [3]. *Let p be an odd prime, and let $a \neq \pm 1$ be an integer not divisible by p. Let d be the order of a modulo p. Let k_0 be the largest integer such that $a^d \equiv 1 \pmod{p^{k_0}}$. Then the order of a modulo p^k is d for $k = 1, \ldots, k_0$ and dp^{k-k_0} for $k \geqslant k_0$.*

For every finite sequence $S = (a_1, \ldots, a_m)$ of length $m \geqslant 1$ in $\mathbb{Z}/n\mathbb{Z}$, we denote by ΔS the *Steinhaus triangle* of S, that is the finite multiset of cardinality $\binom{m+1}{2}$ in $\mathbb{Z}/n\mathbb{Z}$ defined by

$$\Delta S = \left\{ \sum_{k=0}^{i} \binom{i}{k} a_{j+k} \;\middle|\; 0 \leqslant i \leqslant m-1\ ,\ 1 \leqslant j \leqslant m-i \right\}.$$

A finite sequence S in $\mathbb{Z}/n\mathbb{Z}$ is said to be *balanced* if each element of $\mathbb{Z}/n\mathbb{Z}$ occurs in its Steinhaus triangle ΔS with the same multiplicity. For instance, the sequence $(2, 2, 3, 3)$ of length 4 is balanced in $\mathbb{Z}/5\mathbb{Z}$. Indeed, as depicted in Figure 1, its Steinhaus triangle is composed by each element of $\mathbb{Z}/5\mathbb{Z}$ occuring twice.

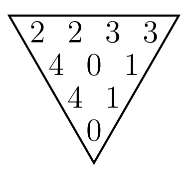

Figure 1: The Steinhaus triangle of a balanced sequence in $\mathbb{Z}/5\mathbb{Z}$

Note that, for a sequence S of length $m \geqslant 1$ in $\mathbb{Z}/n\mathbb{Z}$, a necessary condition on m for S to be balanced is that the integer n divides the binomial coefficient $\binom{m+1}{2}$. In 1976, John C. Molluzzo [2] posed the problem to determine whether this necessary condition on m is also sufficient to guarantee the existence of a balanced sequence. In [1], it was proved that, for each odd number n, *there exists a balanced sequence of length* m *for every* $m \equiv 0$ *or* $-1 \pmod{\alpha_n(2) \cdot n}$ *and for every* $m \equiv 0$ *or* $-1 \pmod{\beta_n(2) \cdot n}$. This was achieved by analyzing the Steinhaus triangles generated by arithmetic progressions. In particular, since $\beta_{3^k}(2) = 1$ for all $k \geqslant 1$, the above result implies a complete and positive solution of Molluzzo's problem in $\mathbb{Z}/n\mathbb{Z}$ for all $n = 3^k$.

2 The arithmetic function α_n

The table depicted in Figure 2 gives us the first values of $\alpha_n(a)$ for every positive integer n, $1 \leqslant n \leqslant 20$, and for every integer a, $-20 \leqslant a \leqslant 20$.

$n \backslash a$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
3	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
4	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
5	1	4	4	2	0	1	4	4	2	0	1	4	4	2	0	1	4	4	2	0
6	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
7	1	3	6	3	6	2	0	1	3	6	3	6	2	0	1	3	6	3	6	2
8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
9	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2
10	1	0	2	0	0	0	2	0	1	0	1	0	2	0	0	0	2	0	1	0
11	1	10	5	5	5	10	10	10	5	2	0	1	10	5	5	5	10	10	10	5
12	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
13	1	12	3	6	4	12	12	4	3	6	12	2	0	1	12	3	6	4	12	12
14	1	0	3	0	3	0	0	0	3	0	3	0	1	0	1	0	3	0	3	0
15	1	4	0	2	0	0	4	4	0	0	2	0	4	2	0	1	4	0	2	0
16	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
17	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2	0	1	8	16
18	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
19	1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2	0	1
20	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0

Figure 2: The first values of $\alpha_n(a)$

The positive integer $\alpha_n(a)$ seems to be difficult to determine. Indeed, there is no general formula known to compute the multiplicative order of an integer modulo n but, however, we get the following helpful propositions.

Lemma 1. *Let* n_1 *and* n_2 *be two positive integers such that* $\operatorname{rad}(n_1) = \operatorname{rad}(n_2)$. *Then, an integer* a *is coprime to* n_1 *if, and only if, it is also coprime to* n_2.

Proof. This follows from the definition of the greatest common divisor of two integers and from the definition of the radical of an integer. □

Proposition 2. *Let n_1 and n_2 be two positive integers such that $\operatorname{rad}(n_1)|n_2$ and $n_2|n_1$. Then, for every integer a, the integer $\alpha_{n_1}(a)$ divides $\alpha_{n_2}(a)$.*

Proof. If a is not coprime to n_1 and n_2, then, by definition of the functions α_{n_1} and α_{n_2} and by Lemma 1, we have

$$\alpha_{n_1}(a) = \alpha_{n_2}(a) = 0.$$

Suppose that a is coprime to n_1 and n_2. If $v_p(n_1) = 1$ for all prime factors p of n_1, then $n_2 = n_1$. Otherwise, let p be a prime factor of n_1 such that $v_p(n_1) \geqslant 2$. We shall show that $\alpha_{n_1}(a)$ divides $\alpha_{n_1/p}(a)$. By definition of $\alpha_{n_1/p}(a)$, there exists an integer u such that

$$a^{\alpha_{n_1/p}(a)\cdot \frac{n_1}{p}} = 1 + u \cdot \frac{n_1}{p}.$$

Therefore, by the binomial theorem, we have

$$a^{\alpha_{n_1/p}(a)\cdot n_1} = \left(a^{\alpha_{n_1/p}(a)\cdot \frac{n_1}{p}}\right)^p = \left(1 + u\cdot\frac{n_1}{p}\right)^p = 1 + u\cdot n_1 + \sum_{k=2}^{p}\binom{p}{k}\cdot u^k\cdot\left(\frac{n_1}{p}\right)^k.$$

Since $v_p(n_1) \geqslant 2$, it follows that $(n_1/p)^k$ is divisible by n_1 for every integer $k \geqslant 2$ and so

$$a^{\alpha_{n_1/p}(a)\cdot n_1} \equiv 1 \pmod{n_1}.$$

Hence $\alpha_{n_1}(a)$ divides $\alpha_{n_1/p}(a)$. This completes the proof. □

An exact relationship between $\alpha_{n_1}(a)$ and $\alpha_{n_2}(a)$, for every integer a coprime to n_1 and n_2, is determined at the end of this section. We first settle the easy prime power case.

Proposition 3. *Let p be a prime number and let a be an integer. Then we have*

$$\alpha_{p^k}(a) = \mathcal{O}_p(a)$$

for every positive integer k.

Proof. Let k be a positive integer. If a is not coprime to p, then we have $\alpha_{p^k}(a) = \alpha_p(a) = 0$. Suppose now that a is coprime to p. By Proposition 2, the integer $\alpha_{p^k}(a)$ divides $\alpha_p(a)$. It remains to prove that $\alpha_p(a)$ divides $\alpha_{p^k}(a)$. The congruence

$$a^{\alpha_{p^k}(a)\cdot p^k} \equiv 1 \pmod{p^k}$$

implies that

$$a^{\alpha_{p^k}(a)\cdot p^k} \equiv 1 \pmod{p},$$

and hence, by Fermat's Little Theorem, it follows that

$$a^{\alpha_{p^k}(a)\cdot p} \equiv a^{\alpha_{p^k}(a)\cdot p^k} \equiv 1 \pmod{p}.$$

Therefore $\alpha_p(a)$ divides $\alpha_{p^k}(a)$. Finally, we have

$$\alpha_{p^k}(a) = \alpha_p(a) = \mathcal{O}_p(a^p) = \mathcal{O}_p(a).$$

This completes the proof. □

Remark 4. If $p = 2$, then, for every positive integer k, we obtain

$$\alpha_{2^k}(a) = \mathcal{O}_2(a) = \begin{cases} 0, & \text{for } a \text{ even;} \\ 1, & \text{for } a \text{ odd.} \end{cases}$$

Proposition 5. *Let n_1 and n_2 be two coprime numbers and let a be an integer. Then $\alpha_{n_1 n_2}(a)$ divides $\operatorname{lcm}(\alpha_{n_1}(a), \alpha_{n_2}(a))$, the least common multiple of $\alpha_{n_1}(a)$ and $\alpha_{n_2}(a)$.*

Proof. If $\gcd(a, n_1 n_2) \neq 1$, then $\gcd(a, n_1) \neq 1$ or $\gcd(a, n_2) \neq 1$ and so

$$\alpha_{n_1 n_2}(a) = \operatorname{lcm}(\alpha_{n_1}(a), \alpha_{n_2}(a)) = 0.$$

Suppose now that $\gcd(a, n_1 n_2) = 1$ and hence that the integers a, n_1 and n_2 are coprime pairwise. Let $i \in \{1, 2\}$. The congruences

$$a^{\alpha_{n_i}(a) \cdot n_i} \equiv 1 \pmod{n_i}$$

imply that

$$a^{n_1 n_2 \operatorname{lcm}(\alpha_{n_1}(a), \alpha_{n_2}(a))} \equiv 1 \pmod{n_i}.$$

Therefore $\alpha_{n_1 n_2}(a)$ divides $\operatorname{lcm}(\alpha_{n_1}(a), \alpha_{n_2}(a))$ by the Chinese remainder theorem. □

Let n_1 and n_2 be two positive integers such that

$$\begin{cases} \operatorname{rad}(n_1) | n_2 \text{ and } n_2 | n_1, & \text{if } v_2(n_1) \leqslant 1; \\ 2 \operatorname{rad}(n_1) | n_2 \text{ and } n_2 | n_1, & \text{if } v_2(n_1) \geqslant 2. \end{cases}$$

By definition, we know that $\alpha_{n_1}(a) = \alpha_{n_2}(a) = 0$ for every integer a not coprime to n_1 and n_2. We end this section by determining the exact relationship between $\alpha_{n_1}(a)$ and $\alpha_{n_2}(a)$ for every integer a coprime to n_1 and n_2.

Theorem 6. *Let n_1 and n_2 be two positive integers such that*

$$\begin{cases} \operatorname{rad}(n_1) | n_2 \textit{ and } n_2 | n_1, & \textit{if } v_2(n_1) \leqslant 1; \\ 2 \operatorname{rad}(n_1) | n_2 \textit{ and } n_2 | n_1, & \textit{if } v_2(n_1) \geqslant 2. \end{cases}$$

Then, for every integer a coprime to n_1 and n_2, we have

$$\alpha_{n_1}(a) = \frac{\alpha_{n_2}(a)}{\gcd\left(\alpha_{n_2}(a), \frac{\gcd(n_1, \mathcal{R}_{n_2}(a))}{n_2}\right)}$$

This result is a corollary of the following theorem.

Theorem 7. *Let n_1 and n_2 be two positive integers such that*

$$\begin{cases} \operatorname{rad}(n_1) | n_2 \textit{ and } n_2 | n_1, & \textit{if } v_2(n_1) \leqslant 1; \\ 2 \operatorname{rad}(n_1) | n_2 \textit{ and } n_2 | n_1, & \textit{if } v_2(n_1) \geqslant 2. \end{cases}$$

Then, for every integer a coprime to n_1 and n_2, we have

$$\mathcal{O}_{n_1}(a) = \mathcal{O}_{n_2}(a) \cdot \frac{n_1}{\gcd(n_1, \mathcal{R}_{n_2}(a))}.$$

The proof of this theorem is based on the following lemma.

Lemma 8. *Let n be a positive integer and let a be an integer coprime to n. Let m be an integer such that* $\operatorname{rad}(m) | \operatorname{rad} n$*. Then, there exists an integer u_m, coprime to n if m is odd, or coprime to $n/2$ if m is even, such that*

$$a^{\mathcal{O}_n(a)\cdot m} = 1 + u_m \cdot \mathcal{R}_n(a) \cdot m.$$

Proof. We distinguish different cases based upon the parity of m. First, we prove the odd case by induction on m. If $m = 1$, then, by definition of the integer $\mathcal{R}_n(a)$, we have

$$a^{\mathcal{O}_n(a)} = 1 + \mathcal{R}_n(a).$$

Therefore the assertion is true for $m = 1$.

Now, let p be a prime factor of m and suppose that the assertion is true for the odd number m/p, i.e., there exists an integer $u_{m/p}$, coprime to n, such that

$$a^{\mathcal{O}_n(a)\cdot \frac{m}{p}} = 1 + u_{m/p} \cdot \mathcal{R}_n(a) \cdot \frac{m}{p}.$$

Then, we obtain

$$\begin{aligned}
a^{\mathcal{O}_n(a)\cdot m} &= \left(a^{\mathcal{O}_n(a)\cdot \frac{m}{p}}\right)^p = \left(1 + u_{m/p} \cdot \mathcal{R}_n(a) \cdot \frac{m}{p}\right)^p \\
&= 1 + u_{m/p} \cdot \mathcal{R}_n(a) \cdot m + \sum_{k=2}^{p-1} \binom{p}{k} \left(u_{m/p} \cdot \mathcal{R}_n(a) \cdot \frac{m}{p}\right)^k + \left(u_{m/p} \cdot \mathcal{R}_n(a) \cdot \frac{m}{p}\right)^p \\
&= \ 1 + \left(u_{m/p} + \sum_{k=2}^{p-1} \frac{\binom{p}{k}}{p} \cdot (u_{m/p})^k \cdot \mathcal{R}_n(a)^{k-1} \cdot \left(\frac{m}{p}\right)^{k-1} + \right. \\
&\qquad \left. + (u_{m/p})^p \cdot \frac{\mathcal{R}_n(a)^{p-1}}{p} \cdot \left(\frac{m}{p}\right)^{p-1}\right) \cdot \mathcal{R}_n(a) \cdot m \\
&= 1 + u_m \cdot \mathcal{R}_n(a) \cdot m.
\end{aligned}$$

Since n divides $\mathcal{R}_n(a)$ which divides

$$u_m - u_{m/p} = \sum_{k=2}^{p-1} \frac{\binom{p}{k}}{p} \cdot (u_{m/p})^k \cdot \mathcal{R}_n(a)^{k-1} \cdot \left(\frac{m}{p}\right)^{k-1} + (u_{m/p})^p \cdot \frac{\mathcal{R}_n(a)^{p-1}}{p} \cdot \left(\frac{m}{p}\right)^{p-1},$$

it follows that $\gcd(u_m, n) = \gcd(u_{m/p}, n) = 1$. This completes the proof for the odd case.

Suppose now that n and m are even. We proceed by induction on $v_2(m)$. If $v_2(m) = 1$, then $m/2$ is odd and by the first part of this proof,

$$a^{\frac{m}{2}\cdot \mathcal{O}_n(a)} = 1 + u_{m/2} \cdot \frac{m}{2} \cdot \mathcal{R}_n(a)$$

where $u_{m/2}$ is coprime to n and hence to $n/2$. Now assume that $v_2(m) > 1$ and that

$$a^{\frac{m}{2}\cdot \mathcal{O}_n(a)} = 1 + u_{m/2} \cdot \frac{m}{2} \cdot \mathcal{R}_n(a)$$

with $u_{m/2}$ coprime to $n/2$. Then, we obtain

$$\begin{aligned} a^{\mathcal{O}_n(a)\cdot m} &= \left(a^{\mathcal{O}_n(a)\cdot\frac{m}{2}}\right)^2 = \left(1 + u_{m/2}\cdot\mathcal{R}_n(a)\cdot\frac{m}{2}\right)^2 \\ &= 1 + u_{m/2}\cdot\mathcal{R}_n(a)\cdot m + \left(u_{m/2}\cdot\mathcal{R}_n(a)\cdot\frac{m}{2}\right)^2 \\ &= 1 + \left(u_{m/2} + (u_{m/2})^2\cdot\frac{\mathcal{R}_n(a)}{2}\cdot\frac{m}{2}\right)\cdot\mathcal{R}_n(a)m \\ &= 1 + u_m\cdot\mathcal{R}_n(a)\cdot m. \end{aligned}$$

Since $n/2$ divides $\mathcal{R}_n(a)/2$ which divides $u_m - u_{m/2}$, it follows that $\gcd(u_m, n/2) = \gcd(u_{m/2}, n/2) = 1$. This completes the proof. □

We are now ready to prove Theorem 7.

Proof of Theorem 7. The proof is by induction on the integer n_1/n_2. If $n_1 = n_2$, then we have

$$\frac{n_1}{\gcd(n_1, \mathcal{R}_{n_2}(a))} = \frac{n_1}{\gcd(n_1, \mathcal{R}_{n_1}(a))} = \frac{n_1}{n_1} = 1,$$

since $\mathcal{R}_{n_1}(a)$ is divisible by n_1, and thus the statement is true. Let p be a prime factor of n_1 and n_2 such that n_2 divides n_1/p and suppose that

$$\mathcal{O}_{n_1/p}(a) = \mathcal{O}_{n_2}(a)\cdot\frac{n_1/p}{\gcd(n_1/p, \mathcal{R}_{n_2}(a))}.$$

First, the congruence

$$a^{\mathcal{O}_{n_1}(a)} \equiv 1 \pmod{n_1}$$

implies that

$$a^{\mathcal{O}_{n_1}(a)} \equiv 1 \pmod{\frac{n_1}{p}}$$

and so $\mathcal{O}_{n_1/p}(a)$ divides $\mathcal{O}_{n_1}(a)$. We consider two cases.

First Case: $v_p(n_1) \leqslant v_p\left(\mathcal{R}_{n_2}(a)\right)$.
Since n_2 divides n_1/p, it follows that $\mathcal{O}_{n_2}(a)$ divides $\mathcal{O}_{n_1/p}(a)$. Let $r = \frac{\mathcal{O}_{n_1/p}(a)}{\mathcal{O}_{n_2}(a)}$. Hence

$$\begin{aligned} \mathcal{R}_{n_1/p}(a) &= a^{\mathcal{O}_{n_1/p}(a)} - 1 = a^{\mathcal{O}_{n_2}(a)\cdot r} - 1 = \left(a^{\mathcal{O}_{n_2}(a)} - 1\right)\left(\sum_{k=0}^{r-1} a^{k\mathcal{O}_{n_2}(a)}\right) \\ &= \mathcal{R}_{n_2}(a)\left(\sum_{k=0}^{r-1} a^{k\mathcal{O}_{n_2}(a)}\right) \end{aligned}$$

and so $\mathcal{R}_{n_1/p}(a)$ is divisible by $\mathcal{R}_{n_2}(a)$. This leads to

$$v_p(n_1) \leqslant v_p\left(\mathcal{R}_{n_2}(a)\right) \leqslant v_p\left(\mathcal{R}_{n_1/p}(a)\right).$$

Therefore $\mathcal{R}_{n_1/p}(a)$ is divisible by n_1 and hence we have

$$a^{\mathcal{O}_{n_1/p}(a)} = 1 + \mathcal{R}_{n_1/p}(a) \equiv 1 \pmod{n_1}.$$

This implies that $\mathcal{O}_{n_1}(a) = \mathcal{O}_{n_1/p}(a)$. Moreover, the hypothesis $v_p(n_1) \leqslant v_p(\mathcal{R}_{n_2}(a))$ implies that $\gcd(n_1/p, \mathcal{R}_{n_2}(a)) = \gcd(n_1, \mathcal{R}_{n_2}(a))/p$. Finally, we obtain

$$\mathcal{O}_{n_1}(a) = \mathcal{O}_{n_1/p}(a) = \mathcal{O}_{n_2}(a) \cdot \frac{n_1/p}{\gcd(n_1/p, \mathcal{R}_{n_2}(a))} = \mathcal{O}_{n_2}(a) \cdot \frac{n_1}{\gcd(n_1, \mathcal{R}_{n_2}(a))}.$$

Second Case: $v_p(n_1) > v_p(\mathcal{R}_{n_2}(a))$.
If $v_2(n_1) \leqslant 1$, then $(n_1/p)/\gcd(n_1/p, \mathcal{R}_{n_2}(a))$ is odd. Otherwise, if $v_2(n_1) \geqslant 2$, then $v_2(n_2) \geqslant 2$ and every integer coprime to $n_2/2$ is also coprime to n_2. In both cases, $v_2(n_1) \leqslant 1$ or $v_2(n_1) \geqslant 2$, we know, by Lemma 8, that there exists an integer u, coprime to n_2, such that

$$\begin{aligned} a^{\mathcal{O}_{n_1/p}(a)} &= a^{\mathcal{O}_{n_2}(a) \cdot \frac{n_1/p}{\gcd(n_1/p, \mathcal{R}_{n_2}(a))}} = 1 + u \cdot \mathcal{R}_{n_2}(a) \cdot \frac{n_1/p}{\gcd(n_1/p, \mathcal{R}_{n_2}(a))} \\ &= 1 + u \cdot \frac{\mathcal{R}_{n_2}(a)}{\gcd(n_1/p, \mathcal{R}_{n_2}(a))} \cdot \frac{n_1}{p}. \end{aligned}$$

As $v_p(\mathcal{R}_{n_2}(a)) \leqslant v_p(n_1/p)$, it follows that $\mathcal{R}_{n_2}(a)/\gcd(n_1/p, \mathcal{R}_{n_2}(a))$ is coprime to p, and hence $\mathcal{O}_{n_1/p}(a)$ is a proper divisor of $\mathcal{O}_{n_1}(a)$ since

$$a^{\mathcal{O}_{n_1/p}(a)} \not\equiv 1 \pmod{n_1}.$$

Moreover, by Lemma 8 again, there exists an integer u_p such that

$$a^{\mathcal{O}_{n_1/p}(a) \cdot p} = 1 + u_p \cdot \mathcal{R}_{n_1/p}(a) \cdot p \equiv 1 \pmod{n_1}.$$

This leads to

$$\mathcal{O}_{n_1}(a) = \mathcal{O}_{n_1/p}(a) \cdot p = \mathcal{O}_{n_2}(a) \cdot \frac{n_1}{\gcd(n_1/p, \mathcal{R}_{n_2}(a))} = \mathcal{O}_{n_2}(a) \cdot \frac{n_1}{\gcd(n_1, \mathcal{R}_{n_2}(a))}.$$

This completes the proof of Theorem 7. □

We may view Theorem 7 as a generalization of Theorem 3.6 of [3], where $n_2 = p$ is an odd prime number and $n_1 = p^k$ for some positive integer k. Note that the conclusion of Theorem 7 fails in general in the case where $v_2(n_1) \geqslant 2$ and $n_2 = \mathrm{rad}(n_1)$. For instance, for $n_1 = 24 = 3 \cdot 2^3$, $n_2 = 6 = 3 \cdot 2$ and $a = 7$, we obtain that $\mathcal{O}_{n_1}(a) = 2$ while $\mathcal{O}_{n_2}(a) n_1/\gcd(n_1, \mathcal{R}_{n_2}(a)) = 24/\gcd(24, 6) = 4$.

We now turn to the proof of the main result of this paper.

Proof of Theorem 6. From Theorem 7, we obtain

$$\begin{aligned} \alpha_{n_1}(a) &= \mathcal{O}_{n_1}(a^{n_1}) = \frac{\mathcal{O}_{n_1}(a)}{\gcd(\mathcal{O}_{n_1}(a), n_1)} = \frac{\mathcal{O}_{n_2}(a) \cdot \frac{n_1}{\gcd(n_1, \mathcal{R}_{n_2}(a))}}{\gcd\left(\mathcal{O}_{n_2}(a) \cdot \frac{n_1}{\gcd(n_1, \mathcal{R}_{n_2}(a))}, n_1\right)} \\ &= \frac{\mathcal{O}_{n_2}(a)}{\gcd(\mathcal{O}_{n_2}(a), n_1, \mathcal{R}_{n_2}(a))}. \end{aligned}$$

Thus,

$$\frac{\alpha_{n_2}(a)}{\alpha_{n_1}(a)} = \frac{\frac{\mathcal{O}_{n_2}(a)}{\gcd(\mathcal{O}_{n_2}(a),n_2)}}{\frac{\mathcal{O}_{n_2}(a)}{\gcd(\mathcal{O}_{n_2}(a),n_1,\mathcal{R}_{n_2}(a))}} = \frac{\gcd(\mathcal{O}_{n_2}(a),n_1,\mathcal{R}_{n_2}(a))}{\gcd(\mathcal{O}_{n_2}(a),n_2)}$$
$$= \gcd\left(\frac{\mathcal{O}_{n_2}(a)}{\gcd(\mathcal{O}_{n_2}(a),n_2)}, \frac{n_2}{\gcd(\mathcal{O}_{n_2}(a),n_2)} \cdot \frac{\gcd(n_1,\mathcal{R}_{n_2}(a))}{n_2}\right).$$

Finally, since we have

$$\gcd\left(\frac{\mathcal{O}_{n_2}(a)}{\gcd(\mathcal{O}_{n_2}(a),n_2)}, \frac{n_2}{\gcd(\mathcal{O}_{n_2}(a),n_2)}\right) = \frac{\gcd(\mathcal{O}_{n_2}(a),n_2)}{\gcd(\mathcal{O}_{n_2}(a),n_2)} = 1,$$

it follows that

$$\frac{\alpha_{n_2}(a)}{\alpha_{n_1}(a)} = \gcd\left(\frac{\mathcal{O}_{n_2}(a)}{\gcd(\mathcal{O}_{n_2}(a),n_2)}, \frac{\gcd(n_1,\mathcal{R}_{n_2}(a))}{n_2}\right) = \gcd\left(\alpha_{n_2}(a), \frac{\gcd(n_1,\mathcal{R}_{n_2}(a))}{n_2}\right).$$

□

Thus, the determination of α_n is reduced to the case where n is square-free.

Corollary 9. *Let n be a positive integer such that $v_2(n) \leqslant 1$. Then, for every integer a, coprime to n, we have*

$$\alpha_n(a) = \frac{\alpha_{\operatorname{rad}(n)}(a)}{\gcd\left(\alpha_{\operatorname{rad}(n)}(a), \frac{\gcd(n,\mathcal{R}_{\operatorname{rad}(n)}(a))}{\operatorname{rad}(n)}\right)}.$$

Corollary 10. *Let n be a positive integer such that $v_2(n) \geqslant 2$. Then, for every integer a, coprime to n, we have*

$$\alpha_n(a) = \frac{\alpha_{2\operatorname{rad}(n)}(a)}{\gcd\left(\alpha_{2\operatorname{rad}(n)}(a), \frac{\gcd(n,\mathcal{R}_{2\operatorname{rad}(n)}(a))}{2\operatorname{rad}(n)}\right)}.$$

3 The arithmetic function β_n

First, we can observe that, by definition of the functions α_n and β_n, we have

$$\alpha_n(a) = \beta_n(a) = 0$$

for every integer a not coprime to n and

$$\frac{\alpha_n(a)}{\beta_n(a)} \in \{1,2\}$$

for every integer a coprime to n. There is no general formula known to compute $\alpha_n(a)/\beta_n(a)$ but, however, we get the following proposition.

Proposition 11. *Let n_1 and n_2 be two positive integers such that* $\mathrm{rad}(n_1) = \mathrm{rad}(n_2)$. *Let a be an integer coprime to n_1 and n_2. If $v_2(n_1) \leqslant 1$, then we have*

$$\frac{\alpha_{n_1}(a)}{\beta_{n_1}(a)} = \frac{\alpha_{n_2}(a)}{\beta_{n_2}(a)}.$$

If $v_2(n_1) \geqslant 2$, then we have

$$\alpha_{n_1}(a) = \beta_{n_1}(a).$$

Proof. Let n_1 be a positive integer such that $v_2(n_1) \leqslant 1$ and a be an integer coprime to n_1. Let p be an odd prime factor of n_1 such that $v_p(n_1) \geqslant 2$. We will prove that

$$\frac{\alpha_{n_1}(a)}{\beta_{n_1}(a)} = \frac{\alpha_{n_1/p}(a)}{\beta_{n_1/p}(a)}.$$

If $\alpha_{n_1}(a) = 2\beta_{n_1}(a)$, then

$$a^{\beta_{n_1}(a)\cdot n_1} \equiv -1 \pmod{n_1}$$

and thus

$$a^{\beta_{n_1}(a)\cdot p\cdot \frac{n_1}{p}} \equiv -1 \pmod{\frac{n_1}{p}}.$$

This implies that $\alpha_{n_1/p}(a) = 2\beta_{n_1/p}(a)$. Conversely, if $\alpha_{n_1/p}(a) = 2\beta_{n_1/p}(a)$, then we have

$$a^{\beta_{n_1/p}(a)\cdot \frac{n_1}{p}} \equiv -1 \pmod{\frac{n_1}{p}}.$$

Since $v_p(n_1) \geqslant 2$, it follows that

$$a^{\beta_{n_1/p}(a)\cdot \frac{n_1}{p}} \equiv -1 \pmod{p}$$

and thus

$$a^{\beta_{n_1/p}(a)\cdot n_1}+1 = 1-\left(-a^{\beta_{n_1/p}(a)\cdot \frac{n_1}{p}}\right)^p = \left(1+a^{\beta_{n_1/p}(a)\cdot \frac{n_1}{p}}\right)\sum_{k=0}^{p-1}\left(-a^{\beta_{n_1/p}(a)\cdot \frac{n_1}{p}}\right)^k \equiv 0 \pmod{n_1}.$$

This implies that $\alpha_{n_1}(a) = 2\beta_{n_1}(a)$. Continuing this process we have

$$\frac{\alpha_{n_1}(a)}{\beta_{n_1}(a)} = \frac{\alpha_{\mathrm{rad}(n_1)}(a)}{\beta_{\mathrm{rad}(n_1)}(a)}$$

and since $\mathrm{rad}(n_1) = \mathrm{rad}(n_2)$,

$$\frac{\alpha_{n_1}(a)}{\beta_{n_1}(a)} = \frac{\alpha_{n_2}(a)}{\beta_{n_2}(a)}.$$

Now, let n_1 be a positive integer such that $v_2(n_1) \geqslant 2$, and let a be a non-zero integer. Suppose that we have $\alpha_{n_1}(a) = 2\beta_{n_1}(a)$. Since

$$a^{\beta_{n_1}(a)\cdot n_1} \equiv -1 \pmod{n_1}$$

it follows that

$$\left(a^{\beta_{n_1}(a)\cdot\frac{n_1}{4}}\right)^4 \equiv -1 \pmod 4$$

in contradiction with

$$\left(a^{\beta_{n_1}(a)\cdot\frac{n_1}{4}}\right)^4 \equiv 1 \pmod 4.$$

Thus $\alpha_{n_1}(a) = \beta_{n_1}(a)$. □

If n is a prime power, then $\beta_n = \beta_{\mathrm{rad}(n)}$, in analogy with Proposition 3 for α_n.

Proposition 12. *Let p be a prime number and let a be an integer. Then we have*

$$\beta_{p^k}(a) = \beta_p(a)$$

for every positive integer k.

Proof. This result is trivial for every integer a not coprime to p. Suppose now that a is coprime to p. For $p = 2$, then, by Proposition 11, we have

$$\beta_{2^k}(a) = \alpha_{2^k}(a) = 1$$

for every positive integer k. For an odd prime number $p \geqslant 3$, Proposition 11 and Proposition 3 lead to

$$\beta_{p^k}(a) = \frac{\alpha_{p^k}(a)}{\alpha_p(a)} \cdot \beta_p(a) = \beta_p(a)$$

for every positive integer k. This completes the proof. □

Let n_1 and n_2 be two positive integers such that

$$\begin{cases} \mathrm{rad}(n_1)|n_2 \text{ and } n_2|n_1, & \text{if } v_2(n_1) \leqslant 1; \\ 2\,\mathrm{rad}(n_1)|n_2 \text{ and } n_2|n_1, & \text{if } v_2(n_1) \geqslant 2. \end{cases}$$

It immediately follows that $\beta_{n_1}(a) = \beta_{n_2}(a) = 0$ for every integer a not coprime to n_1 and n_2. Finally, we determine the relationship between $\beta_{n_1}(a)$ and $\beta_{n_2}(a)$ for every integer a coprime to n_1 and n_2.

Theorem 13. *Let n_1 and n_2 be two positive integers such that*

$$\begin{cases} \mathrm{rad}(n_1)|n_2 \textit{ and } n_2|n_1, & \textit{if } v_2(n_1) \leqslant 1; \\ 2\,\mathrm{rad}(n_1)|n_2 \textit{ and } n_2|n_1, & \textit{if } v_2(n_1) \geqslant 2. \end{cases}$$

Let a be an integer coprime to n_1 and n_2. Then, we have

$$\beta_{n_1}(a) = \frac{\beta_{n_2}(a)}{\gcd\left(\beta_{n_2}(a), \frac{\gcd(n_1, \mathcal{R}_{n_2}(a))}{n_2}\right)}.$$

Proof. If $v_2(n_1) \leqslant 1$, then Theorem 6 and Proposition 11 lead to

$$\frac{\beta_{n_2}(a)}{\beta_{n_1}(a)} = \frac{\alpha_{n_2}(a)}{\alpha_{n_1}(a)} = \gcd\left(\alpha_{n_2}(a), \frac{\gcd(n_1, \mathcal{R}_{n_2}(a))}{n_2}\right).$$

Since $v_2(n_2) = v_2(n_1) \leqslant 1$, it follows that $\gcd(n_1, \mathcal{R}_{n_2}(a))/n_2$ is odd and hence, we have

$$\frac{\beta_{n_2}(a)}{\beta_{n_1}(a)} = \gcd\left(\alpha_{n_2}(a), \frac{\gcd(n_1, \mathcal{R}_{n_2}(a))}{n_2}\right) = \gcd\left(\beta_{n_2}(a), \frac{\gcd(n_1, \mathcal{R}_{n_2}(a))}{n_2}\right).$$

If $v_2(n_1) \geqslant 2$, then $\beta_{n_1}(a) = \alpha_{n_1}(a)$ and $\beta_{n_2}(a) = \alpha_{n_2}(a)$ by Proposition 11 and the result follows from Theorem 6. □

Thus, as for α_n, the determination of β_n is reduced to the case where n is square-free.

Corollary 14. *Let n be a positive integer such that $v_2(n) \leqslant 1$. Then, for every integer a, coprime to n, we have*

$$\beta_n(a) = \frac{\beta_{\mathrm{rad}(n)}(a)}{\gcd\left(\beta_{\mathrm{rad}(n)}(a), \frac{\gcd(n, \mathcal{R}_{\mathrm{rad}(n)}(a))}{\mathrm{rad}(n)}\right)}.$$

Corollary 15. *Let n be a positive integer such that $v_2(n) \geqslant 2$. Then, for every integer a, coprime to n, we have*

$$\beta_n(a) = \frac{\beta_{2\,\mathrm{rad}(n)}(a)}{\gcd\left(\beta_{2\,\mathrm{rad}(n)}(a), \frac{\gcd(n, \mathcal{R}_{2\,\mathrm{rad}(n)}(a))}{2\,\mathrm{rad}(n)}\right)}.$$

4 Acknowledgments

The author would like to thank Shalom Eliahou for his help in preparing this paper. He also thanks the anonymous referee for his/her useful remarks.

References

[1] Jonathan Chappelon, On a problem of Molluzzo concerning Steinhaus triangles in finite cyclic groups, *Integers* **8** (2008), #A37.

[2] John C. Molluzzo, Steinhaus graphs, *Theory and Applications of Graphs*, Springer, volume **642** of *Lecture Notes in Mathematics*, Berlin / Heidelberg, 1978, pp. 394–402.

[3] Melvyn B. Nathanson, *Elementary Methods in Number Theory*, Springer, 2000, pp. 92–93.

2000 *Mathematics Subject Classification*: Primary 11A05; Secondary 11A07, 11A25.
Keywords: multiplicative order, projective multiplicative order, balanced Steinhaus triangles, Steinhaus triangles, Molluzzo's problem.

Received October 16 2009; revised version received January 20 2010. Published in *Journal of Integer Sequences*, January 27 2010.

Return to Journal of Integer Sequences home page.