2005

Bounds on Element Order in Rings $\mathbb{Z}(m)$ With Divisors of Zero

C. H. Cooke

Old Dominion University

Follow this and additional works at: https://digitalcommons.odu.edu/mathstat_fac_pubs

Part of the Applied Mathematics Commons

Repository Citation
https://digitalcommons.odu.edu/mathstat_fac_pubs/69

Original Publication Citation
Bounds On Element Order in Rings $\mathbb{Z}_m$ With Divisors of Zero

C. H. Cooke
Department of Mathematics, Old Dominion University
Norfolk, VA 23529, U.S.A.

(Received and accepted February 2005)

Abstract—If $p$ is a prime, integer ring $\mathbb{Z}_p$ has exactly $\phi(p)$ generating elements $\omega$, each of which has maximal index $I_p(\omega) = \phi(p) = p - 1$. But, if $m = \prod_{j=1}^{R} p_j^{\alpha_j}$ is composite, it is possible that $\mathbb{Z}_m$ does not possess a generating element, and the maximal index of an element is not easily discernible. Here, it is determined when, in the absence of a generating element, one can still with confidence place bounds on the maximal index. Such a bound is usually less than $\phi(m)$, and in some cases the bound is shown to be strict. Moreover, general information about existence or nonexistence of a generating element often can be predicted from the bound © 2005 Elsevier Ltd. All rights reserved.

1. NUMBER THEORETIC PRELIMINARIES

Some results from number theory which form a base for what follows are now given. These results can be found in number theory texts such as [1,2].

Merged Congruence. The system of simultaneous congruences, $X = a$, Mod $(m_i)$, $i = 1, 2, \ldots R$ are equivalent to $X = a$, Mod $(m)$, where $m = \text{l.c.m.}(m_1, m_2, \ldots, m_R)$.

Element Index. If $Z^*_m$ is the set of invertible elements of integer ring $\mathbb{Z}_m$, the order $k = I_m(a)$ of element $a \in Z^*_m$ is the smallest integer $k$, such that $a^k = 1$, Mod$(m)$. Element $a$ is invertible iff $(a, m) = 1$.

Euler’s Theorem. If $(a, m) = 1$, $a^{\phi(m)} = 1$, Mod$(m) \Rightarrow k = I_m(a) | \phi(m)$.

Euler Totient Function. $\phi(m)$ is the number of nonnegative integers, $a$, not exceeding $m$, such that $(a, m) = 1$. $\phi(m)$ is always even, for $m > 2$.

Generating Elements. If $I_m(a) = \phi(m)$, element $a$ is called a generator of $Z^*_m$. If $a$ is a generator, every element of $Z^*_m$ can be expressed as an integer power of $a$.

For prime modulus $\phi(\phi(p)) = \phi(p - 1)$ generators exist [1,2]. But, rarely is it the case that a generator exists when $m$ is a composite modulus.

2. MAXIMAL INDEX FOR RINGS POSSESSING DIVISORS OF ZERO

Suppose $m = \prod_{j=1}^{R} p_j^{\alpha_j}$ has factors determined by primes $p_1 < p_2 < \cdots < p_R$, with $\alpha_j > 0$. If $\phi(x)$ is the Euler Totient function, there are $\phi(m)$ invertible elements in ring $\mathbb{Z}_m$. By Euler’s
theorem, each invertible element \( a \in \mathbb{Z}_m \) has index \( I_m(a) \) which divides \( \phi(m) \). Thus, \( \phi(m) \) emerges as an upper bound on the maximal index. This is a strict bound if and only if the set \( \mathbb{Z}_m^* \) of invertible elements has a generating element, or exactly when \( \mathbb{Z}_m^* \) is a cyclic group.

The purpose of this research is to carefully consider integer rings \( \mathbb{Z}_m \), where \( \mathbb{Z}_m^* \) may not be cyclic. We shall determine bounds on the order \( \tau_m \) of the maximal cyclic subgroup possessed by \( \mathbb{Z}_m^* \). In some cases, the bound on \( \tau_m \) is strict.

An additional benefit of such a bound is that in many cases it can be used to declare the existence or nonexistence of a generating element. This is valuable information, as little is known about when integer rings \( \mathbb{Z}_m \) with composite modulus \( m \) have a generating element, although instances where this occurs are known \([1,2]\).

A result of the present research shows one can be assured that \( \mathbb{Z}_m^* \) is not a cyclic group when integer \( m \) has at least two distinct, odd prime divisors, as then it has no generator. A necessary condition that \( \mathbb{Z}_m^* \) be cyclic is determined, as well as a concomitant set of sufficient conditions, which cut down the work required if a brute force approach to answering the question were employed.

### 3. A CHARACTERIZATION OF \( \tau_m \)

**Theorem 2.** Let integer \( a \) and modulus \( m \) be relatively prime, i.e., \( (a, m) = 1 \). If \( L = \text{l.c.m.} \{\phi(P_j^{\alpha_j}) : P_j \text{ is a divisor of } m, \alpha_j \text{ times, integer } \alpha_j \geq 1\} \), then \( a^L = 1 \), Mod \( m \). Therefore,

(a) \( L \) is an upper bound on the index of each \( a \in \mathbb{Z}_m^* \), and

(b) if there is at least one integer \( J, 1 \leq J \leq R \), such that \( L = \phi(P_j^{\alpha_j}) \), then \( L \) is a strict upper bound on \( I_m(a) \);

(c) always \( \tau_m \leq L \); this is a strict bound iff (b) holds;

(d) thus, when \( L < \phi(m) \) a generating element for \( \mathbb{Z}_m^* \) does not exist.

**Proof.** Since \( (a, m) = 1 \) implies \( (K_j, m) = 1 \), where \( K_j = (p_j^{\alpha_j}) \), by Euler’s theorem \( a^{\phi(K_j)} = 1 \), Mod \( K_j \). Therefore, \( a^L = 1 \), Mod \( K_j \), since \( \phi(K_j) \mid L \). Since \( a^{\phi(K_j)} = 1 \), Mod \( K_j \) is true for each integer \( 1 \leq J \leq R \), the theory of merged congruences assures that \( a^L = 1 \), Mod \( m \). Clearly, \( \tau_m \leq L \), and equality holds iff \( \phi(K_j) = L \), for some integer \( J \) in the range \( 1 \leq J \leq R \). If \( L < \phi(m) \), a generating element for \( \mathbb{Z}_m^* \) cannot exist, as \( \tau_m = \phi(m) \) is a necessary and sufficient for the existence of a generator.

**Corollary 1.** If integer \( m \) has at least two distinct odd prime divisors, then \( \mathbb{Z}_m^* \) is not a cyclic group, as \( \tau_m \leq \phi(m)/2 \).

**Proof.** If \( m \) has at least two distinct odd prime divisors, the \lcm. calculated in determining the bound \( L \) of Theorem 1 will satisfy \( \tau_m \leq \phi(m)/2 \), since \( \phi(m) \) will be divisible at least by 4, with two 2s occurring distributed between two distinct divisors of \( \phi(m) \), causing at least one 2 divisor of \( \phi(m) \) to be dropped when forming the least common multiple, \( L \).

The chief remaining question is: for integer \( m = 2^K \cdot P^\alpha \), when \( \mathbb{Z}_m^* \) is a cyclic group, and when does it fail to be such? Further research may be required. However, the following can be established.

**Theorem 2.** If \( m = 2^K \cdot P^\alpha \) is an integer and \( (a, m) = 1 \), a necessary condition that \( a \) be a generator of \( \mathbb{Z}_m^* \) is that \( a^{\phi(m)/2} = -1 \), Mod \( m \). This necessary condition, in conjunction with \( a^J \neq \pm 1 \), Mod \( m \) for \( 1 \leq J < \phi(m)/2 \), is also sufficient to guarantee that \( a \) is a generator.

**Proof of Necessity.** Suppose \( a \) is a generator of \( \mathbb{Z}_m^* \), and \( m = 2^K \cdot P^\alpha \). By definition of a generator, there must be some integer \( J < \phi(m) \), such that \( a^J = -1 \), Mod \( m \), as \(-1\) is invertible. If \( J = \phi(m)/2 \pm K \) is true for any nonzero integer \( K \) which satisfies \( 0 < K < \phi(m)/2 \), one arrives at a contradiction to \( a \) being a generator: \( a^{2J} = 1 \), Mod \( m \) is impossible, since
2J = \phi(m) - 2K < \phi(m), and \ a^{2J} = a^{\phi(m)+2K} = a^{2K} = 1, \ \text{Mod} (m), \ with \ 2K < \phi(m) \ is \ likewise \ impossible.

**Proof of Sufficiency.** Suppose that conditions

(i) \ a^{\phi(m)/2} = -1, \ \text{Mod} (m) \ and

(ii) \ a^J \neq \pm 1, \ \text{Mod} (m), \ for \ 1 \leq J < \phi(m)/2

are satisfied by element \ a \in \mathbb{Z}_m^*\). If integer \ K = \phi(m)/2 + J \ with \ 1 \leq J < \phi(m)/2, then \ a^K = a^{\phi(m)/2}a^J = -a^J, \ \text{Mod} (m). \ Clearly, \ if \ \pm 1 \ are \ excluded \ values \ for \ a^J, \ likewise \ these \ are \ excluded \ values \ for \ a^K. \ Hence, \ a^J \neq 1, \ \text{Mod} (m), \ for \ 1 \leq J < \phi(m), \ but \ a^{\phi(m)} = 1, \ \text{Mod} (m) \Rightarrow \ a \ is \ primitive.

**Comment.** For large composite \ m, \ the use of brute force to decide whether or not \ a \in \mathbb{Z}_m^*\ is a primitive element becomes computationally intensive. However, Theorem 2 significantly reduces the computation required.

4. **Numerical Examples**

**Example 1.** Consider the ring \ \mathbb{Z}_m\ where \ m = 32760 = 2^33^25(7)13, with \ \phi(m) = 4(6)4(6)12. \ Since \ \tau \ = \phi(13) = \text{l.c.m.} \{\phi(K_j) : J = 1, 2, 3, 4, 5\} = 12, \ \tau_m = 12 = \phi(13) \ is \ a \ strict \ bound \ on \ element \ index \ for \ \mathbb{Z}_{32760}. \ No \ generating \ element \ exists, \ as \ \tau_m < \phi(m).

**Example 2.** For \ m = 71(31), \ \phi(m) = 70(30), \ so \ \tau_m \leq L = 7(3)10 < \phi(m). \ Here, \ Theorem 2 \ does \ not \ guarantee \ a \ strict \ bound. \ It \ does \ establish \ that \ \mathbb{Z}_{71*31} \ has \ no \ generating \ element, \ as \ also \ does \ Corollary 1.

**Example 3.** It is well known that \ \mathbb{Z}_{25}^*\ possesses a generating element. In this case,

\[ L = \phi(m) = \tau_m. \]

Moreover, \ 3^{10} = -1, \ \text{Mod} (20), \ whereas \ 3^J \neq \pm 1, \ \text{Mod} (20), \ for \ 1 < J < 10.

**References**