2005

Bounds on Element Order in Rings Z(m) With Divisors of Zero

C. H. Cooke
Old Dominion University

Original Publication Citation

Cooke, C. H. (2005). Bounds on element order in rings Z_m with divisors of zero. *Computers & Mathematics with Applications, 49*(11-12), 1643-1645. doi:10.1016/j.camwa.2005.02.004

Available online at www.sciencedirect.com
SCIENCE DIRECT®
An International Journal
computers & mathematics with applications
ELSEVIER Computers and Mathematics with Applications 49 (2005) 1643–1645
www elsevier com/locate/camwa

Bounds On Element Order in Rings 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 Z_p has exactly $\phi(\phi(p))$ generating elements ω, 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 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

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), $i = 1, 2, \dots R$ are equivalent to $X = a$, Mod (m), where $m =$ l.c.m. $(m_1, m_2, \dots, m_R)$.

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

EULER'S THEOREM. If $(a, m) = 1$, $a^{\phi(m)} = 1$, Mod (m) => $k = I_m(a) \mid \phi(m)$.

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 Z_m. By Euler's

0898-1221/05/$ - see front matter Typeset by AMS-TEX
doi:10 1016/j.camwa.2005.02 004

theorem, each invertible element $a \in Z_m$ 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 Z_m^* of invertible elements has a generating element, or exactly when Z_m^* is a cyclic group.

The purpose of this research is to carefully consider integer rings Z_m, where Z_m^* may not be cyclic. We shall determine bounds on the order τ_m of the maximal cyclic subgroup possessed by Z_m^*. In some cases, the bound on τ_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 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 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 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 τ_m

THEOREM 2. *Let integer $\underline{a}$ and modulus $\underline{m}$ be relatively prime, i.e., $(a,m) = 1$. If $L =$ l.c.m. $\{\phi(P_J^{\alpha_J}) : P_J$ is a divisor of m, α_J times, integer $\alpha_J \geq 1\}$, then $a^L = 1$, Mod (m). Therefore,*

(a) *L is an upper bound on the index of each $a \in Z_m^*$, 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 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 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 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 l.c.m. 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 $m = 2^K P^\alpha$, when is Z_m^* 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 $m = 2^K P^\alpha$ is an integer and $(a,m) = 1$, a necessary condition that a be a generator of 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 Z_m^*, and $m = 2^K P^\alpha$. 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 $\underline{a}$ being a generator: $a^{2J} = 1$, Mod (m) is impossible, since

$2J = \phi(m) - 2K < \phi(m)$, and $a^{2J} = a^{\phi(m)+2K} = a^{2K} = 1$, Mod (m), with $2K < \phi(m)$ is likewise impossible.

PROOF OF SUFFICIENCY. Suppose that conditions

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

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

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

COMMENT. For large composite m, the use of brute force to decide whether or not $a \in Z_m^*$ is a primitive element becomes computationally intensive. However, Theorem 2 significantly reduces the computation required.

4. NUMERICAL EXAMPLES

EXAMPLE 1. Consider the ring Z_m where $m = 32760 = 2^3 3^2 5(7)13$, with $\phi(m) = 4(6)4(6)12$. Since $L = \phi(13) = \text{l.c.m.}\{\phi(K_J) : J = 1,2,3,4,5\} = 12$, $\tau_m = 12 = \phi(13)$ is a strict bound on element index for 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 $Z_{71 \bullet 31}^*$ has no generating element, as also does Corollary 1.

EXAMPLE 3. It is well known that Z_{25}^* possesses a generating element. In this case,

$$L = \phi(m) = \tau_m.$$

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

REFERENCES

1. K.H Rosen, *Elementary Number Theory*, Addison-Wesley, New York, (2000).
2. J.K. Streyer, *Elementary Number Theory*, PWS Publishing Company, Boston, MA, (1994).