Notes on Number Theory and Discrete Mathematics
Vol. 19, 2013, No. 3, 66–69

Modular zero divisors of longest exponentiation cycle

Amin Witno

Department of Basic Sciences
Philadelphia University, 19392 Jordan
e-mail: awitno@gmail.com

Abstract: We show that the sequence $w^k \bmod n$, given that $\gcd(w, n) > 1$, can reach a maximal cycle length of $\phi(n)$ if and only if n is twice an odd prime power, w is even, and w is a primitive root modulo $n/2$.
Keywords: Modular exponentiation, Primitive roots.
AMS Classification: 11A05, 11A07.

In the ring $\mathbb{Z}_n$ of modular integers, the nonzero elements are partitioned into two subsets: the unit elements $w \in \mathbb{Z}_n$ with $\gcd(w, n) = 1$ and the zero divisors $w \in \mathbb{Z}_n$ for which $\gcd(w, n) > 1$. (For references, see Dummit and Foote [1, pp. 226–227] or other algebra text.) The unit elements form the multiplicative group U_n of order $\phi(n)$, where $\phi(n)$ is the Euler's totient function. The group U_n is cyclic when there exists a primitive root modulo n, i.e., an element $w \in U_n$ of maximal multiplicative order $\phi(n)$.

In this article, we consider the analog of multiplicative order for the zero divisors in $\mathbb{Z}_n$. Note that if $\gcd(w, n) > 1$, then the sequence $w^k \bmod n$ will never yield unity since the congruence $w^k \equiv 1 \pmod n$ would imply that w^{k-1} is the multiplicative inverse of w in $\mathbb{Z}_n$, and so we would have $w \in U_n$. This leads us to the following definition.

Definition. For every element $w \in \mathbb{Z}_n$, let $L = L(w, n)$ be the least positive integer such that $w^L \equiv w^K \pmod n$ for some integer K in the range $0 \leq K < L$. By the *cycle length* of w modulo n we mean the quantity $|w|_n = L - K$. In particular, when $w \in U_n$, then $|w|_n$ is just the multiplicative order of w modulo n.

With this definition, we will be able to show that $|w|_n$ divides $\phi(n)$ (a result which is already known as far as $\gcd(w, n) = 1$) for all zero divisors $w \in \mathbb{Z}_n$, implying that $|w|_n \leq \phi(n)$. Our modest goal is then to give a practical classification for the pair (w, n) for which we do have $|w|_n = \phi(n)$.

We start our observations with Table 1, which serves to illustrate the modular exponentiation with $n = 18$ and how the cycle length $|w|_{18}$ is computed for every zero divisor $w \in \mathbb{Z}_{18}$. Note that in each case, $|w|_{18}$ is a divisor of $\phi(18) = 6$.

Table 1: The zero divisors $w \in \mathbb{Z}_{18}$ and their cycle length $|w|_{18}$.

w	w^2	w^3	w^4	w^5	w^6	w^7	$\|w\|_{18}$
2	4	8	16	14	10	2	$7-1=6$
3	9	9	9	9	9	9	$3-2=1$
4	16	10	4	16	10	4	$4-1=3$
6	0	0	0	0	0	0	$3-2=1$
8	10	8	10	8	10	8	$3-1=2$
9	9	9	9	9	9	9	$2-1=1$
10	10	10	10	10	10	10	$2-1=1$
12	0	0	0	0	0	0	$3-2=1$
14	16	8	4	2	10	14	$7-1=6$
15	9	9	9	9	9	9	$3-2=1$
16	4	10	16	4	10	16	$4-1=3$

We will now present a series of results leading to our goal, which will be accomplished in Theorem 4. The interested reader may wish to compare Theorem 1 to a stronger result that has previously appeared in print [2, Theorem 4.7]. Nevertheless, it will be appropriate to make our newer theorem independent from the latter as well as minimized to suit our purposes.

Theorem 1. Suppose that $\gcd(w, n) > 1$. Let m be the largest factor of n such that $\gcd(w, m) = 1$. Then there exists a positive integer k such that $w^k \equiv w^{k+\phi(m)} \pmod{n}$.

Proof. Observe that every prime factor of n/m is a divisor of w. Hence, we can find an integer k such that $w^k \equiv 0 \pmod{n/m}$. Now if $m = 1$, then the claim is trivially true, so we assume now $m > 1$. Then by Euler's theorem, we have $w^{\phi(m)} \equiv 1 \pmod{m}$. Combine the two congruences by multiplying the moduli, and we get $w^{k+\phi(m)} \equiv w^k \pmod{n}$ as desired. □

Theorem 2. For every nonzero element $w \in \mathbb{Z}_n$, we have $|w|_n$ divides $\phi(n)$.

Proof. Assume that $\gcd(w, n) > 1$ since this is our only concern. We note that as soon as the sequence $w^k \bmod n$ yields a repeated term, say $w^K \equiv w^L \pmod{n}$ for some least possible exponent $L > K$, then the sequence becomes periodic with the earliest cycle consisting of $w^K, w^{K+1}, \ldots, w^{L-1}$. With the number m defined in Theorem 1, we see that $\phi(m)$ must then be some multiple of the cycle length $|w|_n$. And since m is a factor of n, by the property of the Euler's function, $\phi(m)$ divides $\phi(n)$; thus by transitivity, also $|w|_n$ divides $\phi(n)$. □

Theorem 3. Let $\gcd(w, n) > 1$ and let m be the largest factor of n for which $\gcd(w, m) = 1$. If $|w|_n = \phi(n)$, then $|w|_m = \phi(m)$ and w is a primitive root modulo m.

Proof. Suppose that $|w|_n = \phi(n)$. As explained in the proof of Theorem 2, we must have that $|w|_n = \phi(m) = \phi(n)$. But with m being a factor of n, this identity between the two Euler's functions is possible only when $n = 2m$ and m is odd. It follows that $\gcd(w, n) = 2$ and so, for any pair (k, l) of positive integers, the congruence

$$w^{k+l} \equiv w^k \pmod{n},$$

upon dividing both sides by w^k, is equivalent to

$$w^l \equiv 1 \pmod{n/2}.$$

If l is to be the least value for which the congruences hold, then we see why the cycle length of w modulo n must equal the multiplicative order of w modulo $n/2 = m$. In particular, we now have $|w|_m = \phi(n)$. Since $\phi(n) = \phi(m)$ and $w \in U_m$, this says that w is a primitive root modulo m. □

Theorem 4. Let $w \in \{1, 2, 3, \ldots, n-1\}$ with $\gcd(w, n) > 1$. Then $|w|_n = \phi(n)$ if and only if w is even and $n = 2m$ for some odd prime power m modulo which w is a primitive root.

Proof. For necessity, Theorem 3, together with its proof, asserts that w must be even and a primitive root modulo the odd number $m = n/2$. The primitive root theorem [2, Theorem 5.6] now requires that m be an odd prime power in order for such w to exist. (By a prime power we mean a number p^k for some prime p and integer $k \geq 1$.)

To prove sufficiency, suppose that w is an even primitive root modulo $m = n/2$. Then $\gcd(w, n) = 2$, and the same argument used in the preceding proof states that $w^{k+l} \equiv w^k \pmod{n}$ if and only if $w^l \equiv 1 \pmod{m}$. Therefore, $|w|_n = |w|_m = \phi(m)$, where $\phi(m) = \phi(2m) = \phi(n)$. □

As a further consequence of Theorem 4, we have the following fact concerning the total number of zero divisors in $\mathbb{Z}_n$ which have the maximal cycle length of $\phi(n)$. Once again, the result mirrors its analog for the number of unit elements of multiplicative order $\phi(n)$, i.e., primitive roots modulo n.

Theorem 5. For a fixed n, suppose that we can find a zero divisor $w_0 \in \mathbb{Z}_n$ such that $|w_0|_n = \phi(n)$. Then there exist exactly $\phi(\phi(n))$ zero divisors $w \in \mathbb{Z}_n$ for which $|w|_n = \phi(n)$.

Proof. We have established that $n = 2m$, $\phi(n) = \phi(m)$, and that w_0 is a primitive root modulo m. As a known fact, the existence of one primitive root means that there are exactly $\phi(\phi(m))$ primitive roots modulo m. (Incidentally, this also gives the same number of primitive roots modulo $2m$ since m is odd.) In particular, if g is a primitive root modulo m, then both g and $g + m$

are primitive roots modulo m, and exactly one of them is even. Hence, among the integers from 1 to $2m$, there are exactly $\phi(\phi(m))$ even numbers which are primitive roots modulo m. In view of the preceding Theorem 4, $\phi(\phi(m))$ is therefore the number of zero divisors w in $\mathbb{Z}_n$ with $|w|_n = \phi(n)$. $\square$

References

[1] Dummit, D. S., R. M. Foote, *Abstract Algebra*, 3rd ed., Wiley, 2003.

[2] Witno, A. *Theory of Numbers*, BookSurge Publishing, 2008.