8.1 THE ORDER OF AN INTEGER MODULO n

In view of Euler's Theorem, we know that $a^{\phi(n)} \equiv 1 \pmod{n}$, whenever $\gcd(a, n) = 1$. However, there are often powers of a smaller than $a^{\phi(n)}$ which are congruent to 1 modulo n. This prompts the following definition:

DEFINITION 8-1. Let $n > 1$ and $\gcd(a, n) = 1$. The *order of a modulo n* (in older terminology: the *exponent to which a belongs modulo n*) is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$.

Consider the successive powers of 2 modulo 7. For this modulus, we obtain the congruences

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 1,\ 2^4 \equiv 2,\ 2^5 \equiv 4,\ 2^6 \equiv 1,\ \ldots,$$

from which it follows that the integer 2 has order 3 modulo 7.

Observe that if two integers are congruent modulo n, then they have the same order modulo n. For if $a \equiv b \pmod{n}$ and $a^k \equiv 1 \pmod{n}$, Theorem 4-2 implies that $a^k \equiv b^k \pmod{n}$, whence $b^k \equiv 1 \pmod{n}$.

It should be emphasized that our definition of order modulo n concerns only integers a for which $\gcd(a, n) = 1$. Indeed, if $\gcd(a, n) > 1$, then we know from Theorem 4-7 that the linear congruence $ax \equiv 1 \pmod{n}$ has no solution; hence, the relation

$$a^k \equiv 1 \pmod{n}, \qquad k \geq 1$$

cannot hold, for this would imply that $x = a^{k-1}$ is a solution of $ax \equiv 1 \pmod{n}$. Thus, whenever there is reference to the order of a modulo n, it is to be assumed that $\gcd(a, n) = 1$, even if it is not explicitly stated.

In the example given above, we have $2^k \equiv 1 \pmod{7}$ whenever k is a multiple of 3, the order of 2 modulo 7. Our first theorem shows that this is typical of the general situation.

THEOREM 8-1. *Let the integer a have order k modulo n. Then* $a^h \equiv 1 \pmod{n}$ *if and only if* $k \mid h$; *in particular*, $k \mid \phi(n)$.

Proof: Suppose to begin with that $k \mid h$, so that $h = jk$ for some integer j. Since $a^k \equiv 1 \pmod{n}$, Theorem 4-2 tells us that $(a^k)^j \equiv 1^j \pmod{n}$ or $a^h \equiv 1 \pmod{n}$.

Conversely, let h be any positive integer satisfying $a^h \equiv 1 \pmod{n}$. By the Division Algorithm, there exist q and r such that $h = qk + r$, where $0 \leq r < k$. Consequently,

$$a^h = a^{qk+r} = (a^k)^q a^r.$$

By hypothesis both $a^h \equiv 1 \pmod{n}$ and $a^k \equiv 1 \pmod{n}$, the implication of which is that $a^r \equiv 1 \pmod{n}$. Since $0 \leq r < k$, we end up with $r = 0$; otherwise, the choice of k as the smallest positive integer such that $a^k \equiv 1 \pmod{n}$ is contradicted. Hence $h = qk$, and $k \mid h$.

Theorem 8-1 expedites the computation when attempting to find the order of an integer a modulo n: instead of considering all powers of a, the exponents can be restricted to the divisors of $\phi(n)$. Let us obtain, by way of illustration, the order of 2 modulo 13. Since $\phi(13) = 12$, the order of 2 must be one of the integers 1, 2, 3, 4, 6, 12. From

$$2^2 \equiv 4,\ 2^3 \equiv 8,\ 2^4 \equiv 3,\ 2^6 \equiv 12,\ 2^{12} \equiv 1 \pmod{13},$$

it is seen that 2 has order 12 modulo 13.

For an arbitrarily selected divisor d of $\phi(n)$, it is not always true that there exists an integer a having order d modulo n. An example is $n = 12$. Here $\phi(12) = 4$, yet there is no integer which is of order 4 modulo 12; indeed, one finds that

$$1^2 \equiv 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

and so the only choice for orders is 1 or 2.

Here is another basic fact regarding the order of an integer.

THEOREM 8-2. *If a has order k modulo n, then $a^i \equiv a^j \pmod{n}$ if and only if $i \equiv j \pmod{k}$.*

Proof: First, suppose that $a^i \equiv a^j \pmod{n}$, where $i \geq j$. Since a is relatively prime to n, we may cancel a power of a to obtain $a^{i-j} \equiv 1 \pmod{n}$. According to Theorem 8-1, this last congruence holds only if $k \mid i - j$, which is just another way of saying that $i \equiv j \pmod{k}$.

Conversely, let $i \equiv j \pmod{k}$. Then we have $i = j + qk$ for some integer q. By the definition of k, $a^k \equiv 1 \pmod{n}$, so that

$$a^i \equiv a^{j+qk} \equiv a^j(a^k)^q \equiv a^j \pmod{n},$$

which is the desired conclusion.

COROLLARY. *If a has order k modulo n, then the integers $a, a^2, \ldots, a^k$ are incongruent modulo n.*

Proof: If $a^i \equiv a^j \pmod{n}$ for $1 \leq i \leq j \leq k$, then the theorem insures that $i \equiv j \pmod{k}$. But this is impossible unless $i = j$.

A fairly natural question presents itself: is it possible to express the order of any integral power of a in terms of the order of a? The answer is the content of

THEOREM 8-3. *If the integer a has order k modulo n and $h > 0$, then a^h has order $k/\gcd(h, k)$ modulo n.*

Proof: Let $d = \gcd(h, k)$. Then we may write $h = h_1 d$ and $k = k_1 d$, with $\gcd(h_1, k_1) = 1$. Clearly,

$$(a^h)^{k_1} = (a^{h_1 d})^{k/d} = (a^k)^{h_1} \equiv 1 \pmod{n}.$$

If a^h is assumed to have order r modulo n, then Theorem 8-1 asserts that $r \mid k_1$. On the other hand, since a has order k modulo n, the congruence

$$a^{hr} \equiv (a^h)^r \equiv 1 \pmod{n}$$

indicates that $k \mid hr$; in other words, $k_1 d \mid h_1 dr$ or $k_1 \mid h_1 r$. But $\gcd(k_1, h_1) = 1$ and therefore $k_1 \mid r$. This divisibility relation, when combined with the one obtained earlier, gives

$$r = k_1 = k/d = k/\gcd(h, k),$$

proving the theorem.

The last theorem has a corollary for which the reader may supply a proof.

COROLLARY. *Let a have order k modulo n. Then a^h also has order k if and only if* $\gcd(h, k) = 1$.

Let us see how all this works in a specific instance.

Example 8-1

The following table exhibits the orders modulo 13 of the positive integers less than 13:

integer	1	2	3	4	5	6	7	8	9	10	11	12
order	1	12	3	6	4	12	12	4	3	6	12	2

We observe that the order of 2 modulo 13 is 12, while the orders of 2^2 and 2^3 are 6 and 4, respectively; it is easy to verify that

$$6 = 12/\gcd(2, 12) \quad \text{and} \quad 4 = 12/\gcd(3, 12)$$

in accordance with Theorem 8-3. Those integers which also have order 12 modulo 13 are powers 2^k for which $\gcd(k, 12) = 1$; namely,

$$2^5 \equiv 6,\ 2^7 \equiv 11,\ 2^{11} \equiv 7 \pmod{13}.$$

If an integer a has the largest order possible, then we call it a primitive root of n.

DEFINITION 8-2. If $\gcd(a, n) = 1$ and a is of order $\phi(n)$ modulo n, then a is a *primitive root of n.*

To put it another way, n has a as a primitive root if $a^{\phi(n)} \equiv 1 \pmod{n}$, but $a^k \not\equiv 1 \pmod{n}$ for all positive integers $k < \phi(n)$.

It is easy to see that 3 is a primitive root of 7, for

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod{7}.$$

More generally, one can prove that primitive roots exist for any prime modulus, a result of fundamental importance. While it is possible for a primitive root of n to exist when n is not a prime (for instance, 2 is a primitive root of 9), there is no reason to expect that every integer n will possess a primitive root; indeed, the existence of primitive roots is more the exception than the rule.

Example 8-2

Let us show that if $F_n = 2^{2^n} + 1$, $n > 1$, is a prime, then 2 is not a primitive root of F_n. (Clearly, 2 is a primitive root of $5 = F_1$.) Since $2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1)$, we have

$$2^{2^{n+1}} \equiv 1 \pmod{F_n},$$

which implies that the order of 2 modulo F_n does not exceed 2^{n+1}. But if F_n is assumed to be prime,

$$\phi(F_n) = F_n - 1 = 2^{2^n}$$

and a straightforward induction argument confirms that $2^{2^n} > 2^{n+1}$, whenever $n > 1$. Thus the order of 2 modulo F_n is smaller than $\phi(F_n)$; referring to Definition 8-2 we see that 2 cannot be a primitive root of F_n.