

Chapter 5

Primitive roots

5.1 The order of an integer

Definition (Order of an integer) Let $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ be such that $(a, m) = 1$. The **order of a modulo m** , denoted by $\text{ord}_m a$, is the least positive integer k such that

$$(5.1) \quad a^k \equiv 1 \pmod{m}.$$

In order for this definition to make sense, there has to be at least one positive integer k for which (5.1) holds. The existence of such a k is guaranteed by Euler's Theorem (Theorem 2.13), which states that, under the same assumptions on m and a as in the definition, (5.1) holds for $k = \varphi(m)$. Thus, the order $\text{ord}_m a$ is well-defined, and it is at most equal to $\varphi(m)$.

Proposition 5.1 (Properties of an order) Let $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ be such that $(a, m) = 1$, and let $\text{ord}_m a$ be the order of a modulo m . Then:

- (i) (Periodicity) If $b \equiv a \pmod{m}$, then $\text{ord}_m b = \text{ord}_m a$.
- (ii) (Relation to Euler phi) $\text{ord}_m a$ is a divisor of $\varphi(m)$.
- (iii) (Characterization of "good" exponents) The set of positive integers k for which the congruence (5.1) holds consists exactly of the positive integer multiples of $\text{ord}_m a$.
- (iv) (Order of powers of a) For any positive integer i ,

$$\text{ord}_m a^i = \frac{\text{ord}_m a}{(\text{ord}_m a, i)}.$$

In particular, $\text{ord}_m a^i = \text{ord}_m a$ if and only if $(\text{ord}_m a, i) = 1$.

Proposition 5.2 (Number of elements of given order) Let p be an odd prime. Then the possible orders of integers modulo p are exactly the positive divisors of $p - 1 (= \varphi(p))$. Moreover, given any positive divisor $d \mid p - 1$, there exist exactly $\varphi(d)$ incongruent integers a with $\text{ord}_p a = d$.

5.2 Primitive roots

The question when the order of an integer a modulo m is equal to its maximal possible value, the “Euler order” $\varphi(m)$, motivates the following definition.

Definition (Primitive root) Let $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ be such that $(a, m) = 1$. Then a is called a **primitive root modulo m** if $\text{ord}_m a = \varphi(m)$, i.e., if the order of a is equal to the maximal possible value.

Proposition 5.3 (Primitive roots and reduced systems of residues) Let $m \in \mathbf{N}$, and suppose r is a primitive root modulo m . Then the set

$$\{r, r^2, \dots, r^{\varphi(m)}\}$$

is a system of reduced residues modulo m . That is, the elements in this set are pairwise incongruent modulo m , and every integer a with $(a, m) = 1$ is congruent modulo m to an element in the above set.

5.3 The Primitive Root Theorem

Theorem 5.4 (Existence of Primitive Roots) Let m be a positive integer. Then there exists a primitive root modulo m if and only if m has one of the following forms:

- (i) $m = p^\alpha$, where p is an odd prime and $\alpha \in \mathbf{N}$.
- (ii) $m = 2p^\alpha$, where p is an odd prime and $\alpha \in \mathbf{N}$.
- (iii) $m = 1, 2, 4$.

Theorem 5.5 (Number of primitive roots) Let m be of one of the forms in the Primitive Root Theorem, so that there exists at least one primitive root modulo m . Then there exist exactly $\varphi(\varphi(m))$ incongruent primitive roots modulo m .