3. Primitive Roots

We study the group structure of $\mathbb{Z}_m^*$ for any integer $m \geqslant 2$. In particular, we wish to know when it is a cyclic group. This leads to the notion of the primitive root.

3.1. **The cases of primes and powers of 2.** We start with the definition of primitive roots.

Definition 3.1. Let $a, m \in \mathbb{Z}$, $m \geqslant 2$, $\mathrm{hcf}(a, m) = 1$. a is said to be a *primitive root* modulo m if the group of units $\mathbb{Z}_m^*$ is cyclic and the congruence class $\overline{a}$ is a generator.

Remark 3.2. We make some comments about this definition.

(1) Assume a and m and coprime. The *order* of a modulo m is defined to be the order of $\overline{a}$ in the group of units $\mathbb{Z}_m^*$. For any integer n, $a^n \equiv 1 \pmod{m}$ iff n is a multiple of the order of a modulo m. In this terminology, a is a primitive root modulo m iff a is coprime to m and the order of a modulo m is $\phi(m)$.

(2) Knowing that a is a primitive root modulo m allows us to write

$$\mathbb{Z}_m^* = \{\, \overline{a}^{\,k} \mid k \in \mathbb{Z}, 0 \leqslant k < \phi(m) \,\}.$$

In other words, every integer coprime to m is congruent to a^k for some $k \in \mathbb{Z}$. This will be extremely helpful in many different situations. See Exercises 3.2 and 3.3.

(3) If a is a primitive root modulo m, then $\mathbb{Z}_m^*$ is cyclic of order $\phi(m)$ hence has $\phi(\phi(m))$ generators. More precisely, any primitive root modulo m lies in the congruence class $\overline{a}^{\,k}$ for some k with $0 \leqslant k < \phi(m)$ and $\mathrm{hcf}(k, \phi(m)) = 1$.

We have seen in Remark 2.20 that it is essential to understand $\mathbb{Z}_m^*$ when m is a power of a prime in order to understand the general case. We first consider the situation when m is a prime. We need the following lemma:

Lemma 3.3. *Let $f(x) \in \Bbbk[x]$ where $\Bbbk$ is a field. Suppose that $\deg f(x) = n$. Then f has at most n distinct roots in $\Bbbk$.*

Proof. The proof goes by induction on n. For $n = 0$ the assertion is trivial. Assume that the statement is true for polynomials of degree $n - 1$. If $f(x)$ has no roots in k, we are done. If α is a root, since $k[x]$ is a Euclidean domain, we can write $f(x) = (x-\alpha)q(x)+r$, where r is a constant. Setting $x = \alpha$ we see that $r = 0$. Thus $f(x) = (x - \alpha)q(x)$ and $\deg q(x) = n - 1$. If $\beta \neq \alpha$ is another root of $f(x)$, then $0 = f(\beta) = (\beta - \alpha)q(\beta)$, which implies that $q(\beta) = 0$. Since by induction $q(x)$ has at most $n - 1$ distinct roots, $f(x)$ has at most n distinct roots. □

The following theorem is useful in many situations.

Theorem 3.4. *Let K be a field and K^* the group of non-zero elements under multiplication. Suppose G is a finite subgroup of K^*, then G is cyclic.*

Proof. We prove by strong induction on $n = |G|$. If $n = 1$ there is nothing to prove. Now we assume any subgroup of K^* with order smaller than n is cyclic.

For any d with $d \mid n$ and $d < n$, we write $G_d = \{g \in G \mid g^d = 1\}$. We claim G_d is a subgroup of G. Indeed, $1 \in G_d$ because $1^d = 1$. If $g_1, g_2 \in G_d$, then $(g_1 g_2)^d = g_1^d g_2^d = 1$ because multiplication is commutative in the field K. Therefore G_d is closed under multiplication. Moreover, if $g \in G_d$, then $(g^{-1})^d = (g^d)^{-1} = 1$, hence G_d is closed under taking inverse. These conclude that G_d is a group, thus a subgroup of G. Each element of G_d is a solution to $x^d - 1 = 0$ in K, so $|G_d| \leqslant d$ by Lemma 3.3. By induction hypothesis we know G_d is a cyclic group.

Let $\psi(d)$ be the number of elements of order d in G. Each such element is contained in G_d, so $\psi(d)$ is also the number of elements of order d in G_d. If $|G_d| < d$ then $\psi(d) = 0$. Otherwise G_d is a cyclic group of order d and $\psi(d) = \phi(d)$. So we always have $\psi(d) \leqslant \phi(d)$.

On one hand $\psi(n) + \sum_{d \mid n, d<n} \psi(d) = n$ since the order of any element of G is a divisor of n. On the other hand $\phi(n) + \sum_{d \mid n, d<n} \phi(d) = n$ by Proposition 1.28. Since for each $d < n$ we have $\psi(d) \leqslant \phi(d)$, we must have $\psi(n) \geqslant \phi(n) > 0$. In other words, there are elements of order n in G, hence G is cyclic. □

The following immediate consequence has fundamental importance. It was first proved by Gauss.

Corollary 3.5. *Let p be a prime, then $\mathbb{Z}_p^*$ is a cyclic group; i.e. there exist primitive roots modulo p.*

Proof. By Proposition 2.9, $\mathbb{Z}_p$ is a field. Then the result follows from Theorem 3.4. □

Next we study the case of prime powers. We will show that primitive roots exist for powers of odd primes, but the situation is completely different for powers of 2. The necessity of treating 2 differently from the other primes occurs repeatedly in number theory.

Proposition 3.6. *Let l be a positive integer. Then $\mathbb{Z}_{2^l}^*$ is not cyclic unless $l = 1$ or 2.*

Proof. It is easy to see that 1 is a primitive root modulo 2, and 3 is a primitive root modulo 4. From now on we assume that $l \geqslant 3$. We claim that

$$a^{2^{l-2}} \equiv 1 \pmod{2^l}$$

for every odd integer a. It means that the order of every element in $\mathbb{Z}_{2^l}^*$ is strictly smaller than $\phi(2^l)$, hence $\mathbb{Z}_{2^l}^*$ cannot be cyclic.

We prove this claim by induction on l. When $l = 3$, $\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$. We can check them one by one and conclude $a^2 \equiv 1 \pmod 8$ for any odd integer a. Now we assume the claim holds for l, then we can write $a^{2^{l-2}} = 1 + b \cdot 2^l$, thus

$$a^{2^{l-1}} = (1 + b \cdot 2^l)^2 = 1 + b \cdot 2^{l+1} + b^2 \cdot 2^{2l}.$$

The last two terms are divisible by 2^{l+1}, hence $a^{2^{l-1}} \equiv 1 \pmod{2^{l+1}}$, i.e. the claim holds for $l + 1$. □

Remark 3.7. For enthusiasts: for any $l \geqslant 3$, we actually have $\mathbb{Z}_{2^l}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{l-2}}$ which is the direct product of two cyclic groups. We do not prove this fact but it is not difficult.