# 5
# The Structure of $(\mathbb{Z}/p)^\times$

This chapter is about the structure of the group $(\mathbb{Z}/p)^\times$ of units modulo $p$. The main result is that this group is always cyclic.

**Definition 5.0.5 (Primitive root).** A *primitive root* modulo an integer $n$ is an element of $(\mathbb{Z}/n)^\times$ of order $\varphi(n)$.

We prove that there is a primitive root modulo every prime $p$. Since $(\mathbb{Z}/p)^\times$ has order $p-1$, this implies that $(\mathbb{Z}/p)^\times$ is a cyclic group, a fact this will be extremely useful, since it completely determines the structure of $(\mathbb{Z}/p)^\times$ as an abelian group.

If $n$ is an odd prime power, then there is also a primitive root modulo $n$ (see the exercises), but there is no primitive root modulo the even prime power $2^3$.

Section 5.1 is the key input in our proof that $(\mathbb{Z}/p)^\times$ is cyclic; here we show that for every divisor $d$ of $p-1$ there are exactly $d$ elements of $(\mathbb{Z}/p)^\times$ whose order divides $d$. We then use this result in Section 5.2 to produce an element of $(\mathbb{Z}/p)^\times$ of order $q^r$ when $q^r$ is a prime power that exactly divides $p-1$, and combine together these to obtain an element of $(\mathbb{Z}/p)^\times$ of order $p-1$.

## 5.1 Polynomials over $\mathbb{Z}/p$

**Proposition 5.1.1.** *Let $f \in (\mathbb{Z}/p)[x]$ be a nonzero polynomial over the ring $\mathbb{Z}/p$. Then there are at most $\deg(f)$ elements $\alpha \in \mathbb{Z}/p$ such that $f(\alpha) = 0$.*

*Proof.* We induct on $\deg(f)$. The cases with $\deg(f) \leq 1$ are clear. Write $f = a_n x^n + \cdots a_1 x + a_0$. If $f(\alpha) = 0$ then

$$\begin{aligned}
f(x) &= f(x) - f(\alpha) \\
&= a_n(x^n - \alpha^n) + \cdots a_1(x - \alpha) + a_0(1 - 1) \\
&= (x - \alpha)(a_n(x^{n-1} + \cdots + \alpha^{n-1}) + \cdots + a_2(x + \alpha) + a_1) \\
&= (x - \alpha)g(x),
\end{aligned}$$

for some polynomial $g(x) \in (\mathbb{Z}/p)[x]$. Next suppose that $f(\beta) = 0$ with $\beta \neq \alpha$. Then $(\beta - \alpha)g(\beta) = 0$, so, since $\beta - \alpha \neq 0$, we have $g(\beta) = 0$. By our inductive hypothesis, $g$ has at most $n - 1$ roots, so there are at most $n - 1$ possibilities for $\beta$. It follows that $f$ has at most $n$ roots. □

**Proposition 5.1.2.** *Let $p$ be a prime number and let $d$ be a divisor of $p - 1$. Then $f = x^d - 1 \in (\mathbb{Z}/p)[x]$ has exactly $d$ solutions.*

*Proof.* Let $e = (p - 1)/d$. We have

$$\begin{aligned}
x^{p-1} - 1 &= (x^d)^e - 1 \\
&= (x^d - 1)((x^d)^{e-1} + (x^d)^{e-2} + \cdots + 1) \\
&= (x^d - 1)g(x),
\end{aligned}$$

where $g \in (\mathbb{Z}/p)[x]$ and $\deg(g) = de - d = p - 1 - d$. Theorem 3.3.14 implies that $x^{p-1} - 1$ has exactly $p - 1$ roots in $\mathbb{Z}/p$, since every nonzero element of $\mathbb{Z}/p$ is a root! By Proposition 5.1.1, $g$ has *at most* $p - 1 - d$ roots and $x^d - 1$ has at most $d$ roots. Since a root of $(x^d - 1)g(x)$ is a root of either $x^d - 1$ or $g(x)$ and $x^{p-1} - 1$ has $p - 1$ roots, $g$ must have exactly $p - 1 - d$ roots and $x^d - 1$ must have exactly $d$ roots, as claimed. □

The analogue of Proposition 5.1.2 is false when $p$ is replaced by a composite integer $n$, since a root mod $n$ of a product of two polynomials need not be a root of either factor. For example, if $n = n_1 \cdot n_2$ with $n_1, n_2 \neq 1$, then $f = n_1 x$ has at least *two* distinct zeros, namely $0$ and $n_2 \neq 0$.

## 5.2 Existence of Primitive Roots

In this section, we prove that $(\mathbb{Z}/p)^\times$ is cylic by using the results of Section 5.2 to produce an element of $(\mathbb{Z}/p)^\times$ of order $d$ for each prime power divisor $d$ of $p - 1$, then multiply these together to obtain an element of order $p - 1$.

The following lemma will be used to assemble together elements of orders dividing $p - 1$ to produce an element of order $p - 1$.

**Lemma 5.2.1.** *Suppose $a, b \in (\mathbb{Z}/n)^\times$ have orders $r$ and $s$, respectively, and that* $\gcd(r, s) = 1$. *Then $ab$ has order $rs$.*

*Proof.* This is a general fact about commuting elements of any finite group. Since

$$(ab)^{rs} = a^{rs} b^{rs} = 1,$$

the order of $ab$ is a divisor of $rs$. Write this divisor as $r_1 s_1$ where $r_1 \mid r$ and $s_1 \mid s$. Raise both sides of

$$a^{r_1 s_1} b^{r_1 s_1} = (ab)^{r_1 s_1} = 1.$$

to the power $r_2 = r/r_1$ to obtain

$$a^{r_1 r_2 s_1} b^{r_1 r_2 s_1} = 1.$$

Since $a^{r_1 r_2 s_1} = (a^{r_1 r_2})^{s_1} = 1$, we have

$$b^{r_1 r_2 s_1} = 1,$$

so $s \mid r_1 r_2 s_1$. Since $\gcd(s, r_1 r_2) = \gcd(s, r) = 1$, it follows that $s = s_1$. Similarly $r = r_1$, so the order of $ab$ is $rs$. $\square$

**Theorem 5.2.2.** *There is a primitive root modulo any prime $p$.*

*Proof.* Write $p - 1$ as a product of distinct prime powers $q_i^{n_i}$:

$$p - 1 = q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}.$$

By Proposition 5.1.2, the polynomial $x^{q_i^{n_i}} - 1$ has exactly $q_i^{n_i}$ roots, and the polynomial $x^{q_i^{n_i - 1}} - 1$ has exactly $q_i^{n_i - 1}$ roots. There are $q_i^{n_i} - q_i^{n_i - 1} = q_i^{n_i - 1}(q_i - 1)$ elements $a \in \mathbb{Z}/p$ such that $a^{q_i^{n_i}} = 1$ but $a^{q_i^{n_i - 1}} \neq 1$; each of these elements has order $q_i^{n_i}$. Thus for each $i = 1, \ldots, r$, we can choose an $a_i$ of order $q_i^{n_i}$. Then, using Lemma 5.2.1 repeatedly, we see that

$$a = a_1 a_2 \cdots a_r$$

has order $q_1^{n_1} \cdots q_r^{n_r} = p - 1$, so $a$ is a primitive root modulo $p$. $\square$

*Example* 5.2.3. We illustrate the proof of Theorem 5.2.2 when $p = 13$. We have

$$p - 1 = 12 = 2^2 \cdot 3.$$

The polynomial $x^4 - 1$ has roots $\{1, 5, 8, 12\}$ and $x^2 - 1$ has roots $\{1, 12\}$, so we may take $a_1 = 5$. The polynomial $x^3 - 1$ has roots $\{1, 3, 9\}$, and we set $a_2 = 3$. Then $a = 5 \cdot 3 = 15 \equiv 2$ is a primitive root. To verify this, note that the successive powers of 2 modulo 13 are

$$2,\ 4,\ 8,\ 3,\ 6,\ 12,\ 11,\ 9,\ 5,\ 10,\ 7,\ 1.$$

*Example* 5.2.4. Theorem 5.2.2 is false if, e.g., $p$ is replaced by a power of 2 bigger than 4. For example, the four elements of $(\mathbb{Z}/8)^\times$ each have order dividing 2, but $\varphi(8) = 4$.

**Theorem 5.2.5.** *Let $p^n$ be a power of an odd prime. Then there is a primitive root modulo $p^n$.*

The proof is left as Exercise 3.

**Proposition 5.2.6.** *If there is a primitive root modulo $n$, then there are exactly $\varphi(\varphi(n))$ primitive roots modulo $n$.*

*Proof.* The primitive roots modulo $n$ are the generators of $(\mathbb{Z}/n)^\times$, which by assumption is cyclic of order $\varphi(n)$. Thus they are in bijection with the generators of any cyclic group of order $\varphi(n)$. In particular, the number of primitive roots modulo $n$ is the same as the number of elements of $\mathbb{Z}/\varphi(n)$ with additive order $\varphi(n)$. An element of $\mathbb{Z}/\varphi(n)$ has additive order $\varphi(n)$ if and only if it is coprime to $\varphi(n)$. There are $\varphi(\varphi(n))$ such elements, as claimed. □

For example, there are $\varphi(\varphi(17)) = \varphi(16) = 2^4 - 2^3 = 8$ primitive roots mod 17, namely $3, 5, 6, 7, 10, 11, 12, 14$. The $\varphi(\varphi(9)) = \varphi(6) = 2$ primitive roots modulo 9 are 2 and 5. There aren't any primitive roots modulo 8, even though $\varphi(\varphi(8)) = \varphi(4) = 2 > 0$.

## 5.3 Artin's Conjecture

**Conjecture 5.3.1 (Emil Artin).** *Suppose $a \in \mathbb{Z}$ is not $-1$ or a perfect square. Then there are infinitely many primes $p$ such that $a$ is a primitive root modulo $p$.*

There is no single integer $a$ such that Artin's conjecture is known to be true. For any given $a$, Pieter [Mor93] proved that there are infinitely many $p$ such that the order of $a$ is divisible by the largest prime factor of $p-1$.

Hooley [Hoo67] proved that the Generalized Riemann Hypothesis implies Conjecture 5.3.1. This Generalized Riemann Hypothesis is, as its name suggests, a generalization of the Riemann Hypothesis; it asserts that certain functions, called "zeta functions", have zeros only on the vertical line $\mathrm{Re}(s) = \frac{1}{2}$.

*Remark* 5.3.2. Artin conjectured more precisely that if $N(x,a)$ is the number of primes $p \le x$ such that $a$ is a primitive root modulo $p$, then $N(x,a)$ is asymptotic to $C(a)\pi(x)$, where $C(a)$ is a positive constant that depends only on $a$ and $\pi(x)$ is the number of primes up to $x$.

EXERCISES

5.1 Prove that there is no primitive root modulo $2^n$ for any $n \ge 3$. [Hint: Relate the statement for $n = 3$ to the statement for $n > 3$.]

5.2 Characterize the integers $n$ such that there is a primitive root modulo $n$ in terms of their prime factorization.

5.3 Let $p$ be an odd prime.

(a) Prove that there is a primitive root modulo $p^2$. [Hint: Write down an element of $(\mathbb{Z}/p^2)^\times$ that looks like it might have order $p$, and prove that it does. Recall that if $a, b$ have orders $n, m$, with $\gcd(n,m) = 1$, then $ab$ has order $nm$.]

(b) Prove that for any $n$, there is a primitive root modulo $p^n$.

5.4 Search the literature for what is known about Artin's conjecture on primitive roots, and write a short survey of these results.