Chapter 4: The Structure of $U(\mathbb{Z}/n\mathbb{Z})$

Lemma (Generators of a cyclic group). *Let $G = \langle g \rangle$ be a finite cyclic group of order n. Then $G = \langle h \rangle$ iff $h \in \{g^a \mid (a, n) = 1\}$.*

Proof. Suppose that $h = g^a$ with $(a, n) = 1$. Then clearly $\langle h \rangle \subseteq \langle g \rangle$ as a subset. For the reverse containment ($\supseteq$), write $ra + sn = 1$ where $r, s \in \mathbb{Z}$. Then $h^r = g^{ar} = g^{1-sn} = g \cdot (g^n)^{-s} = g \cdot 1 = g$. Then again $\langle g \rangle \subseteq \langle h \rangle$ as a subset.

Now suppose that $\langle g \rangle = \langle h \rangle$. Then $h = g^a$ for some $a \in \mathbb{Z}$. Also, $g = h^r$ for some $r \in \mathbb{Z}$. So $g = h^r = g^{ar}$ or $g^{ar-1} = 1$. So $n|(ar - 1)$, or $ar + ns = 1$ for some $s \in \mathbb{Z}$, that is, $(a, n) = 1$. $\square$

Corollary. *Let G be a finite cyclic group of order n. Then G has exactly $\phi(n)$ generators.*

Theorem 1. *$U(\mathbb{Z}/p\mathbb{Z})$ is a cyclic group.*

Proof. Let $p - 1 = q_1^{e_1} q_2^{e_2} \cdots q_t^{e^t} = \prod_q q^e$ be the prime decomposition of $p - 1$. Consider the congruences

(1) $x^{q^{e-1}} \equiv 1(p)$

(2) $x^{q^e} \equiv 1(p)$

Therefore,

(1) Every solution to $x^{q^{e-1}} \equiv 1(p)$ is a solution of $x^{q^e} \equiv 1(p)$.

(2) $x^{q^e} \equiv 1(p)$ has more solutions than $x^{q^{e-1}} \equiv 1(p)$. In fact, $x^{q^{e-1}} \equiv 1(p)$ has q^{e-1} solutions and $x^{q^e} \equiv 1(p)$ has q^e solutions by Proposition 4.1.2.

Therefore, there exists $g_i \in \mathbb{Z}/p\mathbb{Z}$ generating a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $q_i^{e_i}$ for all $i = 1, ..., t$. Pick $g = g_1 g_2 \cdots g_t \in \mathbb{Z}/p\mathbb{Z}$ generating a subgroup of $U(\mathbb{Z}/p\mathbb{Z})$ of order $q_1^{e_1} q_2^{e_2} \cdots q_t^{e^t} = p - 1$. That is, $\langle g \rangle = U(\mathbb{Z}/p\mathbb{Z})$. $\square$

Corollary. *$U(\mathbb{Z}/p\mathbb{Z})$ has exactly $\phi(p - 1)$ generators.*

Exercise 4.1. *Show that 2 is a primitive root module 29.*

Proof. $2^1 \equiv 2(29)$, $2^2 \equiv 4(29)$, $2^3 \equiv 8(29)$, $2^4 \equiv 16(29)$, $2^5 \equiv 3(29)$, $2^6 \equiv 6(29)$, $2^7 \equiv 12(29)$, $2^8 \equiv 24(29)$, $2^9 \equiv 19(29)$, $2^{10} \equiv 9(29)$, $2^{11} \equiv 18(29)$, $2^{12} \equiv 7(29)$, $2^{13} \equiv 14(29)$, $2^{14} \equiv 28(29)$, $2^{15} \equiv 27(29)$, $2^{16} \equiv 25(29)$, $2^{17} \equiv 21(29)$, $2^{18} \equiv 13(29)$, $2^{19} \equiv 26(29)$, $2^{20} \equiv 23(29)$, $2^{21} \equiv 17(29)$, $2^{22} \equiv 5(29)$, $2^{23} \equiv 10(29)$, $2^{24} \equiv 20(29)$, $2^{25} \equiv 11(29)$, $2^{26} \equiv 22(29)$, $2^{27} \equiv 15(29)$, $2^{28} \equiv 1(29)$. Thus $U(\mathbb{Z}/29\mathbb{Z}) = \langle 2 \rangle$. $\square$