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

Exercise 4.11.

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, $\langle g \rangle = U(\mathbb{Z}/p\mathbb{Z})$. $\square$