2/5: Structure of primitive roots in $\mathbb{F}_p^*$

Let $p$ be a prime. We have seen that $\mathbb{F}_p$ has some primitive roots. Let $a \in \mathbb{F}_p^*$ be any primitive root. Consider the map

$$a(-) : \mathbb{Z}/(p-1) \rightarrow \mathbb{F}_p^*$$

$$\bar{c} \mapsto a^c$$

This is a bijection thanks to Fermat’s little theorem $a^{p-1} = 1$ and the property of primitive roots.

**Lemma 9.1.** We have $a^c$ is a primitive root if and only if $\gcd(c, p-1) = 1$.

**Proof.** Suppose $\gcd(c, p-1) = 1$. We claim that $(a^c)^t \neq 1$ for $t = 1, \ldots, p-2$. Indeed, suppose $(a^c)^t = a^{ct} = 1$. Then $\text{ord}(a)|ct \implies p-1|ct \implies p-1|t$ as $\gcd(p-1, c) = 1$, which is impossible as $0 < t < p-1$.

Conversely, suppose $\gcd(c, p-1) = d > 1$. Take $t = (p-1)/d < p-1$. Then $d|c \implies dt|ct$. But $dt = p-1$. Thus $p-1|ct$ and thus $(a^c)^t = a^{ct} = 1$, i.e. $a^c$ is not a primitive root. \qed

We note that we saw last time that the number of invertible elements in $\mathbb{Z}/(p-1)$ is $\phi(p-1)$. Lemma 9.1 then says that these elements correspond to primitive roots in $\mathbb{F}_p^*$, the number of which we also know to be $\phi(p-1)$. In fact, Lemma 9.1 that the number of primitive roots should be $\phi(p-1)$ if non-zero, which motivates our proof of the existence of primitive roots.