Chapter 14

Euler's and Fermat's Theorems

Definition 14.1. Take $n \in \mathbb{N}$. A *reduced set of residues (RSR) modulo* n is a set

$$x_1, x_2, \ldots, x_s \in \mathbb{N}$$

such that $(x_i, n) = 1 \, \forall i \in \{1, 2, \ldots, s\}$, $x_i \not\equiv x_j \pmod{n}$ for $i \neq j$ and

$$(x, n) = 1 \quad \Rightarrow \quad x \equiv x_i \pmod{n} \text{ for some } i \in \{1, 2, \ldots, s\}.$$

Remark 14.2. It follows that for $n \in \mathbb{N}$, an RSR modulo n comprises one element from each congruence class $\overline{x}$ such that $(x, n) = 1$.

Lemma 14.3. *Take $n \in \mathbb{N}$, and suppose that $x_1, x_2, \ldots, x_s \in \mathbb{N}$ is an RSR modulo n. Then*

(i) $s = \varphi(n)$;

(ii) $\lambda x_1, \lambda x_2, \ldots, \lambda x_s \in \mathbb{N}$ *is also an RSR modulo n for any $\lambda \in \mathbb{N}$ with* $(\lambda, n) = 1$.

Proof (i) This follows from the definition of φ.

(ii) Fix $i \in \{1, 2, \ldots, s\}$. Then $(x_i, n) = 1$.

Let $d = (\lambda x_i, n)$. Then $d \mid n$ and $d \mid \lambda x_i$. Furthermore, d can be expressed in the form $d = d_1 d_2$, where $d_1 \mid \lambda$ and $d_2 \mid x_i$. Also, it follows that $d_1 \mid n$ and $d_2 \mid n$.

Since $d_1 \mid \lambda$, $d_1 \mid n$ and $(\lambda, n) = 1$, $d_1 = 1$.

Since $d_2 \mid x_i$, $d_2 \mid n$ and $(x_i, n) = 1$, $d_2 = 1$. Hence $(\lambda x_i, n) = d = d_1 d_2 = 1$.

Suppose that $\lambda x_i \equiv \lambda x_j \pmod{n}$. Since $(\lambda, n) = 1$, it follows from Theorem 12.13 (ii) that $x_i \equiv x_j \pmod{n}$. Since $x_i \not\equiv x_j \pmod{n}$ for $i \neq j$, it follows that $\lambda x_i \not\equiv \lambda x_j \pmod{n}$ for $i \neq j$. Furthermore, it follows from above that $(\lambda x_i, n) = 1 \, \forall i \in \{1, 2, \ldots, s\}$.

Hence for each $i \in \{1, 2, \ldots, s\}$, $\exists j(i) \in \{1, 2, \ldots, s\}$ such that $\lambda x_i \equiv x_{j(i)} \pmod{n}$.