Suppose that $j(i_1) = j(i_2)$. Then

$$\lambda x_{i_1} \equiv x_{j(i_1)} \pmod{n} \equiv x_{j(i_2)} \pmod{n} \equiv \lambda x_{i_2} \pmod{n}.$$

Since $(\lambda, n) = 1$, it follows from Theorem 12.13 (ii) that $x_{i_1} \equiv x_{i_2} \pmod{n}$. So $i_1 = i_2$. Hence the mapping $i \in \{1, 2, \ldots, s\} \mapsto j(i) \in \{1, 2, \ldots, s\}$ is injective and thus bijective. Hence for each $j \in \{1, 2, \ldots, s\}$, $\exists i(j) \in \{1, 2, \ldots, s\}$ such that $\lambda x_{i(j)} \equiv x_j \pmod{n}$.

Suppose that $(x, n) = 1$. Then $x \equiv x_j \pmod{n}$ for some $j \in \{1, 2, \ldots, s\}$, giving that

$$x \equiv \lambda x_{i(j)} \pmod{n}.$$

□

Examples 14.4. (1) We have that 1, 3, 5, 7 is an RSR modulo 8. Since $(3, 8) = 1$,

$$3, \quad 9 \,(\equiv 1 \pmod 8), \quad 15 \,(\equiv 7 \pmod 8), \quad 21 \,(\equiv 5 \pmod 8)$$

is also an RSR modulo 8.

(2) We have that 1, 5, 7, 11 is an RSR modulo 12. Since $(5, 12) = 1$,

$$5, \quad 25 \,(\equiv 1 \pmod{12}), \quad 35 \,(\equiv 11 \pmod{12}), \quad 55 \,(\equiv 7 \pmod{12})$$

is also an RSR modulo 12.

Theorem 14.5 (Euler). *If $x, n \in \mathbb{N}$ are such that $(x, n) = 1$, then $x^{\varphi(n)} \equiv 1 \pmod{n}$.*

Proof Let $x_1, x_2, \ldots, x_s$ $(s = \varphi(n))$ be an RSR modulo n. Since $(x, n) = 1$, it follows from Lemma 14.3 that $xx_1, xx_2, \ldots, xx_s$ is also an RSR modulo n.

For each $i \in \{1, 2, \ldots, s\}$, $(x_i, n) = 1$ and hence $\exists j(i) \in \{1, 2, \ldots, s\}$ such that $x_i \equiv xx_{j(i)} \pmod{n}$. So

$$\prod_{i=1}^{s} x_i \equiv \prod_{i=1}^{s} xx_{j(i)} \pmod{n} \equiv x^s \prod_{i=1}^{s} x_{j(i)} \pmod{n} \equiv x^{\varphi(n)} \prod_{i=1}^{s} x_{j(i)} \pmod{n}.$$

As in the proof of Lemma 14.3, it can be shown that the mapping

$$i \in \{1, 2, \ldots, s\} \mapsto j(i) \in \{1, 2, \ldots, s\}$$

is bijective. Hence

$$\prod_{i=1}^{s} x_i = \prod_{i=1}^{s} x_{j(i)},$$