giving that

$$\prod_{i=1}^{s} x_i \equiv x^{\varphi(n)} \prod_{i=1}^{s} x_i \,(\mathrm{mod}\; n)\,.$$

Since $(x_i,\, n) = 1\, \forall i \in \{1,\, 2,\, \ldots,\, s\}$, it follows that

$$\left(\prod_{i=1}^{s} x_i,\, n\right) = 1.$$

If $p \in \mathbb{N}$ is a prime number such that $p \,|\, \prod_{i=1}^{s} x_i$, then $p \,|\, x_j$ for some $j \in \{1,\, 2,\, \ldots,\, s\}$. Hence if $p \,|\, n$ also, then it follows that $p = 1$. Thus $1 \equiv x^{\varphi(n)}\,(\mathrm{mod}\; n)$. □

Lemma 14.6. *Let $n \in \mathbb{N}$, and define*

$$U_n = \{\overline{x} \mid (x,\, n) = 1\}\,.$$

Then

(i) $|U_n| = \varphi(n)$*;*

(ii) *if $\overline{x},\, \overline{y} \in U_n$, then $\overline{xy} \in U_n$;*

(iii) *if $\overline{x} \in U_n$, then $\exists \overline{y} \in U_n$ such that $\overline{xy} = \overline{1}$;*

(iv) *if $\overline{x} \in U_n$, then $\overline{x^{\varphi(n)}} = \overline{1}$.*

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

(ii) Suppose that $x,\, y \in \mathbb{N}$ satisfy $(x,\, n) = (y,\, n) = 1$. Then $(xy,\, n) = 1$.

Indeed, suppose that $p \in \mathbb{N}$ is a prime such that $p \,|\, xy$ and $p \,|\, n$. Then $p \,|\, x$ or $p \,|\, y$. If $p \,|\, x$ then, since $p \,|\, n$ and $(x,\, n) = 1$, $p = 1$. Similarly, if $p \,|\, y$ then $p = 1$.

(iii) This is an exercise.

(iv) This follows from Theorem 14.5.

□

Example 14.7. We have that $U_8 = \{\overline{1},\, \overline{3},\, \overline{5},\, \overline{7}\}$. Furthermore, multiplication modulo 8 gives the following table for $\overline{xy}$:

$\overline{x} \setminus \overline{y}$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1