(ii) We have that

$$x_1x_2 = (y_1 + k_1n)(y_2 + k_2n) = y_1y_2 + (k_1y_2 + k_2y_1 + k_1k_2n)\,n.$$

□

Theorem 12.7. *Take $n \in \mathbb{N}$ and let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, with*

$$a_i \in \mathbb{Z}\,\forall i \in \{0, 1, \ldots, n-1, n\}.$$

If $x \equiv y \pmod{n}$, then $f(x) \equiv f(y) \pmod{n}$.

Proof This follows from repeated application of Lemma 12.6. □

Lemma 12.8. *Let $x, y, n \in \mathbb{N}$ be such that $x \equiv y \pmod{n}$. Then x and y have the same remainder when divided by n.*

Proof Since $x \equiv y \pmod{n}$, we have that $n \mid x - y$ and hence that $\exists k \in \mathbb{Z}$ such that $x - y = kn$.

Let $q, r \in \overline{\mathbb{N}}$ satisfy $0 \leq r < n$ and $x = qn + r$ (the existence and uniqueness of such q, r is given by Lemma 10.5). It follows that

$$y = x - kn = (qn + r) - kn = (q - k)\,n + r.$$

Since $y > 0$, it follows that $q - k \geq 0$. □

Example 12.9. We have that $81 \equiv 56 \pmod{5}$. Furthermore, both 81 and 56 have remainder 1 when divided by 5:

$$81 = 16 \cdot 5 + 1, \quad 56 = 11 \cdot 5 + 1.$$

Definition 12.10. Take $n \in \mathbb{N}$. The integers $a_0, a_1, \ldots, a_{n-1}$ form a *complete set of residues (CSR) modulo n* if they comprise one element from each equivalence (congruence) class, i.e. if $a_i \not\equiv a_j \pmod{n}$ for $i \neq j$.

Example 12.11. Both $10, -4, 2, -2, -6$ and $-2, -1, 0, 1, 2$ are CSRs modulo 5.

Example 12.12. (1) Suppose that we wish to know the last two digits in the decimal expansion of 2^{1000}.

This means that we need to find $n \in \mathbb{N}$ such that $0 \leq n \leq 99$ and $2^{1000} \equiv n \pmod{100}$. We have

$$\begin{aligned} &2^5 = 32, \\ \Rightarrow\ &2^{10} = 32^2 = 1024 \equiv 24 \pmod{100}, \\ \Rightarrow\ &2^{20} \equiv 24^2 \pmod{100} \equiv 576 \pmod{100} \equiv -24 \pmod{100}, \end{aligned}$$