Theorem 14.8 (Fermat). (i) *If $x \in \mathbb{N}$, $p \in \mathbb{N}$ is prime and $x \not\equiv 0 \,(\mathrm{mod}\, p)$ (i.e. $p \not| x$), then $x^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$.*

(ii) *If $x \in \mathbb{N}$ and $p \in \mathbb{N}$ is prime, then $x^p \equiv x \,(\mathrm{mod}\, p)$.*

Proof (i) It is easy to see that

$$x \not\equiv 0 \,(\mathrm{mod}\, p) \quad \Leftrightarrow \quad (x,\, p) = 1.$$

Since $\varphi(p) = p - 1$, Theorem 14.5 gives that $x^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$.

(ii) If $x \not\equiv 0 \,(\mathrm{mod}\, p)$, then (i) gives that $x^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$ and hence

$$x^p = x \cdot x^{p-1} \equiv x \cdot 1 \,(\mathrm{mod}\, p) \equiv x \,(\mathrm{mod}\, p)\,.$$

If $x \equiv 0 \,(\mathrm{mod}\, p)$, then

$$x^p \equiv 0^p \,(\mathrm{mod}\, p) \equiv 0 \,(\mathrm{mod}\, p)\,.$$

□

Example 14.9. Consider $p = 7$. We have that

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8 \equiv 1 \,(\mathrm{mod}\, 7)\,, \quad 2^4 \equiv 2 \,(\mathrm{mod}\, 7)\,, \quad 2^5 \equiv 4 \,(\mathrm{mod}\, 7)\,,$$
$$2^6 \equiv 8 \,(\mathrm{mod}\, 7) \equiv 1 \,(\mathrm{mod}\, 7)\,;$$

and

$$3^1 = 3, \quad 3^2 = 9 \equiv 2 \,(\mathrm{mod}\, 7)\,, \quad 3^3 \equiv 6 \,(\mathrm{mod}\, 7)\,, \quad 3^4 \equiv 18 \,(\mathrm{mod}\, 7) \equiv 4 \,(\mathrm{mod}\, 7)\,,$$
$$3^5 \equiv 12 \,(\mathrm{mod}\, 7) \equiv 5 \,(\mathrm{mod}\, 7)\,, \quad 3^6 \equiv 15 \,(\mathrm{mod}\, 7) \equiv 1 \,(\mathrm{mod}\, 7)\,.$$

Suppose we wish to show that $21 \,|\, 3^{91} - 3$. Then it is sufficient to show that $7 \,|\, 3^{90} - 1$. Moreover, since $3^6 \equiv 1 \,(\mathrm{mod}\, 7)$,

$$3^{90} = 3^{6 \cdot 15} = \left(3^6\right)^{15} \equiv 1^{15} \,(\mathrm{mod}\, 7) \equiv 1 \,(\mathrm{mod}\, 7)\,.$$

Definition 14.10. Let $x,\, n \in \mathbb{N}$ satisfy $(x,\, n) = 1$. Then the *order*, *period* or *exponent* of $x \,(\mathrm{mod}\, n)$ is the *smallest* natural number $r \in \mathbb{N}$ such that $x^r \equiv 1 \,(\mathrm{mod}\, n)$.

Note 14.11. The condition that $(x,\, n) = 1$ is necessary for the last definition. Indeed, suppose that $(x,\, n) = d > 1$. Then, since $d \,|\, x$, $d \,|\, x^r$ for all $r \in \mathbb{N}$.

Furthermore, since $d \,|\, n$, $d \,|\, kn$ for all $k \in \mathbb{Z}$. Hence $d \,|\, x^r - kn$ for all $r \in \mathbb{N}$ and $k \in \mathbb{Z}$. Hence for each pair $(r,\, k) \in \mathbb{N} \times \mathbb{Z}$, there exists $l\,(r,\, k) \in \mathbb{Z}$ such that $x^r - kn = l\,(r,\, k)\, d$.

Suppose that $r \in \mathbb{N}$ satisfies $x^r \equiv 1 \,(\mathrm{mod}\, n)$. Then $n \,|\, x^r - 1$. Pick $k \in \mathbb{Z}$ such that $x^r - 1 = kn$. Then $x^r - kn = 1$, and hence $l\,(r,\, k)\, d = 1$. Since $d > 1$ and $l\,(r,\, k) \in \mathbb{Z}$, this is impossible.