Fermat's Little Theorem

Theorem 6 (Fermat, 1640): Let p be a prime. Then:

$$n^p \equiv n \pmod{p}, \quad \text{for all } n \in \mathbb{Z}.$$

Corollary 1: If p is a prime and $p \nmid n$ then

$$n^{p-1} \equiv 1 \pmod{p}.$$

Corollary 2: Suppose p and n are prime and

$$a \not\equiv 1 \pmod{p}.$$

If $p | (a^n - 1)$, then $n | (p - 1)$, so p is of the form $p = 1 + kn$.

Remark. This applies in particular to the Mersenne numbers $M_n = 2^n - 1$, where n is a prime.

Corollary 3: Let $p \neq q$ be two distinct primes and put $n = pq$ and $k = (p-1)(q-1)$. Then for any integer $a \equiv 1 \pmod{k}$ we have

$$m^a \equiv m \pmod{n}.$$

In particular, for any $e \in \mathbb{Z}$ with $\gcd(e, k) = 1$, there is an integer $d \in \mathbb{Z}$ such that $ed \equiv 1 \pmod{k}$, and we have for all $m \in \mathbb{Z}$:

$$m^{ed} \equiv m \pmod{n}.$$