Another corollary of Lagrange's theorem is:

**Corollary** let $G$ be a finite group, and $a \in G$. Then $\lvert a \rvert \mid \lvert G \rvert$.

**Proof** a previous corollary says $o(a) \mid \lvert G \rvert$, where $o(a) = \lvert \langle a \rangle \rvert$ is the order of $a$. We also know $o(a)$ is the smallest positive integer such that $a^m = e$.

So $a^o(a) = e$.

Now write $\lvert G \rvert = o(a) \cdot m$, then

$$\lvert G \rvert = a^m = (a^{o(a)})^m = e^m = e.$$

A nice application of this fact is Euler's theorem in number theory. Recall $[a] \in \mathbb{Z}_n$ has a multiplicative inverse if and only if $\gcd(a, n) = 1$.

$$\mathbb{Z}_n^* = \{ [a] \mid [a] \text{ has a multiplicative inverse } \}$$

is a group under multiplication.

Define $\varphi(n) = \lvert \mathbb{Z}_n^* \rvert = \lvert \{ k \mid 0 < k < n \text{ and } \gcd(k, n) = 1 \} \rvert$

this is called Euler's totient function $\varphi$.

$$\begin{align*}
\mathbb{Z}_2^* &= \{ [1] \} & \varphi(2) &= 1 \\
\mathbb{Z}_3^* &= \{ [1], [2] \} & \varphi(3) &= 2 \\
\mathbb{Z}_4^* &= \{ [1], [3] \} & \varphi(4) &= 2 \\
\mathbb{Z}_5^* &= \{ [1], [2], [3], [4] \} & \varphi(5) &= 4 \\
\mathbb{Z}_6^* &= \{ [1], [5] \} & \varphi(6) &= 2
\end{align*}$$
**Euler's Theorem** if \( \gcd(a,n) = 1 \), then
\[
a^{\varphi(n)} \equiv 1 \pmod{n}
\]

**Proof** \( \mathbb{Z}_n^* \) is a group, and \([a] \in \mathbb{Z}_n^* \) since \( \gcd(a,n) = 1 \).

So by the corollary of Lagrange's theorem,
\[
[a]^{\varphi(n)} = [1] \quad \text{in } \mathbb{Z}_n^*, \text{ which is equivalent to } a^{\varphi(n)} \equiv 1 \pmod{n}.
\]

If \( p \) is a prime number, every \( a \) with \( 0 < a < p \) satisfies \( \gcd(a,p) = 1 \). Thus \( \mathbb{Z}_p^* = \{[1],[2],\ldots,[p-1]\} \) and \( \varphi(p) = p-1 \)

**Fermat's Little Theorem:** For any integer \( a \) and prime \( p \),
\[
a^p \equiv a \pmod{p}
\]

**Proof** if \( a \equiv 0 \pmod{p} \), then \( a^p \equiv 0 \pmod{p} \), and so \( a^p \equiv 0 \equiv a \pmod{p} \)

If \( a \not\equiv 0 \pmod{p} \), then \( \gcd(a,p) = 1 \), so by Euler's theorem,
\[
a^{\varphi(p)} \equiv 1 \pmod{p}
\]

But \( \varphi(p) = p-1 \), so \( a^{p-1} \equiv 1 \pmod{p} \)

Multiplying both sides by \( a \), \( a^p \equiv a \pmod{p} \) in this case as well \( \Box \)

E.g. 3457 is prime. So \( 2^{3457} \equiv 2 \pmod{3457} \)