The Fermat-Euler Theorem

**Corollary 54** For all \( a \in \Phi(n) \), \( a^{\phi(n)} = 1 \mod n \).

- The proof is similar to that of Lemma 53 (p. 360).
- Consider \( a\Phi(n) = \{am \mod n : m \in \Phi(n)\} \).
- \( a\Phi(n) = \Phi(n) \).
  - \( a\Phi(n) \subseteq \Phi(n) \) as a remainder must be between 0 and \( n - 1 \) and relatively prime to \( n \).
  - Suppose \( am = am' \mod n \) for \( m' < m < n \), where \( m, m' \in \Phi(n) \).
  - That means \( a(m - m') = 0 \mod n \), and \( n \) divides \( a \) or \( m - m' \), which is impossible.

---

\(^{a}\)Proof by Mr. Wei-Cheng Cheng (R93922108) on November 24, 2004.
The Proof (concluded)

- Multiply all the numbers in $\Phi(n)$ to yield $\prod_{m \in \Phi(n)} m$.
- Multiply all the numbers in $a\Phi(n)$ to yield $a^{\Phi(n)} \prod_{m \in \Phi(n)} m$.
- As $a\Phi(n) = \Phi(n)$,

$$\prod_{m \in \Phi(n)} m = a^{\Phi(n)} \left( \prod_{m \in \Phi(n)} m \right) \mod n.$$ 

- Finally, $a^{\Phi(n)} = 1 \mod n$ because $n \not| \prod_{m \in \Phi(n)} m$. 