# Unit 4: Fermats Little Theorem and Eulers Theorem


Paul Ycay
MATH 409


December 13, 2019

The following theorems are ones to be marked. There is a separate file of handwritten notes for the rest of the theorems in this chapter

**Theorem 4.2.** Let $a$ and $n$ be natural numbers with $(a, n) = 1$. Then $(a^j, n) = 1$ for any natural number $j$.

*Proof.* Suppose $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$. Then $a = a_1^{b_1} a_2^{b_2} \dots a_c b^c$ and $n = n_1^{m_1} n_2^{m_2} \dots n_l b^l$, for $b, c, m, l \in \mathbb{N}$. Since $(a, n) = 1$, neither $a$ nor $n$ share a common factor. Let $j \in \mathbb{N}$. Then,

$$\begin{aligned} a^j &= (a_1^{b_1} a_2^{b_2} \dots a_c^{b_c})^j \\ &= a_1^{b_1 j} a_2^{b_2 j} \dots a_c^{b_c j} \end{aligned}$$

Assuming all exponents are different, then bases have not changed and thus, $a^j$ does not have a common factor with $n$. Hence, $(a^j, n) = 1$ $\square$

**Theorem 4.3.** Let $a, b, n \in \mathbb{Z}$ with $n > 0$ and $(a, n) = 1$. If $a \equiv b$ $(mod\ n)$, then $(b, n) = 1$

*Proof.* If $(a, n) = 1$, then for some $x, y \in \mathbb{Z}$, (i) $ax + ny = 1$. If $a \equiv b$ $(mod\ n)$, then for some $t \in \mathbb{Z}$, (ii) $nt = a - b$. This implies that $a = nt + b$. Substituting (ii) into (i), we have

$$\begin{aligned} (a)x + ny &= 1 \\ (nt + b)x + ny &= 1 \\ ntx + bx + ny &= 1 \\ n(tx + y) + bx &= 1 \\ nc + bx &= 1,\ c \in \mathbb{Z} \end{aligned}$$

Thus $(b, n) = 1$ $\square$

**Theorem 4.8.** Let $a$ and $n$ be natural numbers with $(a, n) = 1$ and let $k = ord_n(a)$. Then the numbers $a_1, a_2, \ldots, a_k$ are pairwise incongruent *modulo* $n$

*Proof.* By contradiction, suppose powers $i, j$, with $1 \leq j < i < k$, such that $a^i \equiv a^j (mod\ n)$. Then $a^{i-j}a^j \equiv a^j (mod\ n) \implies a^{i-j} \equiv 1 (mod\ n)$ (by right multiplying with the inverse). But $i - j < k$; this contradicts $k$ being the smallest natural number where $a^k \equiv 1 (mod\ n)$. Thus, if $(a, n) = 1$ and $k = ord_n(a)$, then $a, a^2, \ldots, a^k$ are pairwise incongruent $mod\ n$, i.e., values $mod\ n$ never repeat. □

**Theorem 4.10.** Let $a$ and $n$ be natural numbers with $(a, n) = 1$, let $k = ord_n(a)$, and let $m \in \mathbb{N}$. Then $a^m \equiv 1\ (mod\ n)$ if and only if $k|m$

*Proof.* i) Suppose $(a, n) = 1,\ k = ord_n(a), m \in \mathbb{Z}$. Suppose $a^m \equiv 1 (mod\ n)$. By division algorithm, $m = kq + r, 0 < r < k$. Then

$$\begin{aligned} a^m &\equiv a^{kq+r}\ mod\ n \\ &\equiv (a^k)^q a^r\ mod\ n \\ &\equiv 1^q a^r\ mod\ n,\ \ by\ order\ property \\ &\equiv a^r\ mod\ n \end{aligned}$$

Then $r$ has to be 0, which implies that $m = kq$. Therefore, $k = ord_n(a)|m$
ii) Assume $k = ord_n(a)|m$. Then

$$\begin{aligned} a^m &\equiv a^{kq}\ mod\ n \\ &\equiv (a^k)^q\ mod\ n \\ &\equiv 1^q\ mod\ n,\ \ by\ order\ property \\ &\equiv 1\ mod\ n \end{aligned}$$

□

**Theorem 4.13.** Let $p$ be a prime and let $a$ be an integer not divisible by $p$; that is, $(a, p) = 1$. Then $a, 2a, 3a, \ldots, pa$ is a complete residue system *modulo* $p$

*Proof.* Let $p$ be a prime and let $(a, p) = 1, a \in \mathbb{Z}$. Consider $a, 2a, 3a, \ldots, pa$. To show that this is a complete residue system, let $an \equiv am\ (mod\ p), n, m \in \mathbb{Z}$. Then $n \equiv m\ (mod\ p)$. Then, each element in $a, 2a, \ldots, pa$ are distinct *modulo* $p$; each element is congruent to one element in the complete residue system since there are $p$ distinct elements. Thus, $a, 2a, \ldots, pa$ is a complete residue system $mod\ p$. □

**Exercise 4.20.** Find the remainder upon division of $314^{159}$ by 31

*Solution.* By F.L.T, $314^{30} \equiv 1\ (mod\ 31)$, and $159 = 30 * 5 + 9$. So, we have $314^{159} \equiv (314^{30})^{5+9}\ (mod\ 31) \implies 314^{159} \equiv (1)^5 314^9\ (mod\ 31)$. We just have to find the remainder of $314^9$ divided by 31.

$$\begin{aligned} 314 &\equiv 4\ (mod\ 31) \\ 314^3 &\equiv 4^3\ (mod\ 31) \\ &\equiv 2\ (mod\ 31) \\ 314^9 &\equiv 2^3\ (mod\ 31) \end{aligned}$$

Thus, the remainder of $314^{159}$ by 31 is 8. $\square$