Euler-Fermat Theorem: Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$, $\gcd(a,m)=1$. Then

$$a^{\varphi(m)} \equiv 1 \pmod m.$$

Proof. Let $R = \{r_1, r_2, \ldots, r_{\varphi(m)}\}$ be a reduced system of residues mod m

By proposition $aR = \{ar_1, ar_2, \ldots, ar_{\varphi(m)}\}$ is also a reduced system.

$\Rightarrow$ $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ are congruent to $r_1, r_2, \ldots, r_{\varphi(m)}$ in some order.

$$\Rightarrow r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \equiv (ar_1)\cdot(ar_2)\cdot \ldots (ar_{\varphi(m)}) \pmod m$$
$$\equiv a^{\varphi(m)} \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \pmod m$$

$\Rightarrow 1 \equiv a^{\varphi(m)} \pmod m$ $\boxtimes$

Corollary (Fermat Little Theorem): Let p be prime and $a \not\equiv 0 \pmod p$. Then $a^{p-1} \equiv 1 \pmod p$.

Proof: consequence of $\varphi(p) = p-1$ and $a \not\equiv 0 \pmod p \Rightarrow \gcd(a,p) = 1$. $\boxtimes$

Example: What weekday will be 1 million days from today?

$10^6 \equiv 1 \pmod 7 \Rightarrow$ 1 million days from today will be the same weekday as tomorrow (Thursday).

Recall: $\operatorname{ord}_m(a)$ is the smallest $d \in \mathbb{Z}^+$ such that $a^d \equiv 1 \pmod m$

Proposition. Let $m \in \mathbb{Z}^+$, $a \in \mathbb{Z}$ with $\gcd(a,m)=1$. Then $\operatorname{ord}_m(a) \mid \varphi(m)$.

Proof. denote $d = \operatorname{ord}_m(a)$

$$\varphi(m) = q \cdot d + r \quad \text{where } 0 \le r < d$$

By E-FT, $1 \equiv a^{\varphi(m)} \equiv a^{qd+r} \equiv \underbrace{(a^d)}_{\equiv 1}{}^{q} \cdot a^r$

$$\equiv a^r \pmod m.$$

Since d is smallest positive with $a^d \equiv 1 \pmod m$ we have $r = 0$.

$\Rightarrow d \mid \varphi(m)$. $\boxtimes$

Example: $m=14$, Reduced system is $\{1,3,5,9,11,13\}$, $\varphi(14)=6$

a	1	3	5	9	11	13
$\mathrm{ord}_{14}(a)$	1	6	6	3	3	2

$3^2 \equiv 9$, $3^3 \equiv 27 \equiv -1 \pmod{14}$, $3^6 \equiv (-1)^2 \equiv 1 \pmod{14}$

$5^2 \equiv -3$, $5^3 \equiv -15 \equiv -1 \pmod{14}$, $5^6 \equiv 1 \pmod{14}$

$9 = 3^2$, $9^3 \equiv (3^2)^3 \equiv 1 \pmod{14}$

$11 \equiv -3 \pmod{14}$, $11^3 \equiv (-3)^3 \equiv 1 \pmod{14}$

§5.3 The case $\gcd(a,m)>1$.

Theorem (FLT v.2) Let p be prime, $a \in \mathbb{Z}$, arbitrary. Then

$$a^p \equiv a \pmod{p}$$

Proof: If $a \not\equiv 0 \pmod{p}$ then

$$a^p \equiv a^{p-1} \cdot a \equiv [\text{FLT}] \equiv a \pmod{p}.$$

If $a \equiv 0 \pmod{p}$ then $a^p \equiv 0 \equiv a \pmod{p}$ ☒

Q: Can we reformulate E-FT in a similar way? (i.e. is $a^{\varphi(m)+1} \equiv a \pmod{m}$ for all a?)

A: Not always. Take $m=4$, $a=2$

$$2^{\varphi(m)+1} \equiv 2^3 \equiv 0 \pmod 4 \not\equiv 2.$$

However we can do that for $m = pq$ where p, q are two distinct primes.

Proposition: $\varphi(pq) = (p-1)(q-1)$.

Proof. Standard complete system:

$$\{a \in \mathbb{Z} : 0 \le a \le pq-1\}.$$

Possibilities for $\gcd(a, pq)$ are $1, p, q, pq$.

If $\gcd(a, pq) = pq$ then $a = 0$

$\gcd(a, pq) = p$: $a = p, 2p, \ldots, (q-1)p$

$\gcd(a, pq) = q$: $a = q, 2q, \ldots, (p-1)q$

$$\Rightarrow \varphi(pq) = pq - 1 - (q-1) - (p-1) = pq - p - q + 1$$
$$= (p-1)(q-1)$$

$\boxtimes$

Proposition: Let $m = pq$ as before. Then

$$a^{\varphi(m)+1} \equiv a \pmod m \text{ for all } a \in \mathbb{Z}.$$

Proof. If $\gcd(a, m) = 1$. Then by E-FT:

$$a^{\varphi(m)+1} \equiv a^{\varphi(m)} \cdot a \equiv a \pmod m.$$

If $\gcd(a, m) = m$ then $a \equiv 0 \pmod m$

$$\Rightarrow a^{\varphi(m)+1} \equiv 0 \equiv a \pmod m.$$

If $\gcd(a, pq) = p$. then $\gcd(a, q) = 1$

$\Rightarrow a^{q-1} \equiv 1 \pmod q$

$\Rightarrow a^{\varphi(m)+1} \equiv a^{(p-1)(q-1)+1} \equiv 1 \cdot a \equiv a \pmod q$

$a \equiv 0 \pmod p$. Then $a^{\varphi(m)+1} \equiv 0 \equiv a \pmod p$

We have: $\left.\begin{array}{l} p \mid a^{\varphi(m)+1} - a \\ q \mid a^{\varphi(m)+1} - a \end{array}\right\} \Rightarrow pq \mid a^{\varphi(m)+1} - a$

$\Rightarrow a^{\varphi(m)+1} \equiv a \pmod m$

If $\gcd(a, pq) = q$ - Ex.

Theorem ("RSA-theorem"). Let $m = pq$ as before. Then

$$a^{k\varphi(m)+1} \equiv a \pmod m \quad \text{for all } a \in \mathbb{Z},\ k \in \mathbb{Z},\ k \geq 0.$$