Euler's φ-function

$\varphi(n) :=$ # integers $\leq n$ that are relatively prime to n

n	$\varphi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4

NOTE: p prime $\iff \varphi(p) = p-1$

n composite $\iff \varphi(n) < n-1$

FACT: $\gcd(a, bc) = 1$ iff $\gcd(a,b) = \gcd(a,c) = 1$.

__Theorem__ φ is multiplicative.

__pf.__ let m, n be relatively prime integers, $m, n > 1$.

$$\begin{array}{cccccccc}
1 & 2 & \cdots & r & \cdots & m & \longleftarrow & \exists\ \varphi(m) \text{ integers rel. prime to } m \\
m+1 & m+2 & \cdots & m+r & \cdots & 2m & & \text{let } r \text{ be one of them.} \\
\vdots & \vdots & \ddots & \vdots & & \vdots & & \gcd(qm+r, m) = \gcd(r, m) = 1 \\
\underline{(n-1)m+1} & (n-1)m+2 & \cdots & \underbrace{(n-1)m+r}_{\text{everything here is relatively prime to } m} & \cdots & nm & &
\end{array}$$

$km + r \equiv qm + r \pmod{n} \implies km \equiv qm \pmod{n}$
$\implies k \equiv q \pmod{n} \implies k = q.$

$\implies$ The n integers in this column are congruent (in some unknown order) to $0, 1, \ldots, (n-1) \pmod{n}$.

$\implies \varphi(n)$ of them are rel. prime to $n \implies \varphi(m)\varphi(n) = \varphi(mn)$.

$\blacksquare$

p prime, $k \geq 1$

$$\boxed{\varphi(p^k) = p^k - p^{k-1}}$$

$\gcd(m, p^k) \neq 1 \Longrightarrow p \mid m$

$p, 2p, \ldots, (p^{k-1})p = p^k$, so $\exists$ p^{k-1} integers

m s.t. $\gcd(m, p^k) \neq 1$.

example: $\varphi(9) = \varphi(3^2)$

$= 6$

$= 3^2 - 3$.

$\varphi(81) = 3^4 - 3^3 = \underline{\underline{54}}$

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \Longrightarrow \varphi(n) = \varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r})$$

$$= (p_1^{k_1} - p_1^{k_1 - 1}) \cdots (p_r^{k_r} - p_r^{k_r - 1})$$

$$= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \cdots p_r^{k_r}\left(1 - \frac{1}{p_r}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

example: $12 = 2^2 \cdot 3$

$\varphi(12) = \varphi(2^2)\varphi(3)$

$= (2^2 - 2)(2)$

$= (2)(2)$

$= \underline{\underline{4}}$

7.2 **#4** $\varphi(2n)$: if n is odd, then

$$\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n).$$

if n is even, then $n = 2^k m$,

~~for~~ where $\gcd(2, m) = 1$. Then

$$\begin{aligned}
\varphi(2n) = \varphi(2^{k+1} m) &= \varphi(2^{k+1})\varphi(m) \\
&= (2^{k+1} - 2^k)\varphi(m) \\
&= 2(2^k - 2^{k-1})\varphi(m) \\
&= 2\varphi(2^k)\varphi(m) \\
&= 2\varphi(n).
\end{aligned}$$

Euler's Generalization of Fermat's Little Theorem

If a and n are relatively prime, then

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

__pf.:__ let $a_1, a_2, \ldots, a_{\varphi(n)}$ be the $\varphi(n)$ integers $< n$ that are rel. prime to n. Multiply them by a:

$$\underbrace{aa_1, \; aa_2, \ldots, \; a \cdot a_{\varphi(n)}}.$$

all incongruent mod n: $aa_i \equiv aa_j \pmod{n}$

$$\Longrightarrow a_i \equiv a_j \pmod{n} \Longrightarrow a_i = a_j.$$

Then $(aa_1)(aa_2) \cdot \ldots \cdot (aa_{\varphi(n)}) \equiv a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}$

$$\Longrightarrow a^{\varphi(n)} \equiv 1 \pmod{n}. \quad \boxtimes$$

<u>7.3</u> #2 $\underbrace{51 \mid 10^{32n+9} - 7}$ for any $n \geq 0$.

$$10^{32n+9} \equiv 7 \pmod{51}.$$

$$51 = 3 \cdot 17, \quad \text{so } \varphi(51) = \varphi(3)\varphi(17)$$
$$= 2 \cdot 16 = 32.$$

Euler's Thm: $10^{32} \equiv 1 \pmod{51}$

$$\left.\begin{aligned} &\Longrightarrow 10^{32n} \equiv 1 \pmod{51}. \\ &\text{Finally: } 10^{9} \equiv 7 \pmod{51} \end{aligned}\right\} \; 10^{32n+9} \equiv 7 \pmod{51}.$$

If $\gcd(n_i, n_j) = 1$ when $i \neq j$, we can solve the system $x \equiv a_i \pmod{n_i}$ using Euler's Thm!

Define $N_i = \dfrac{\prod n_j}{n_i}$; then $\gcd(N_i, n_i) = 1$.

$$N_i^{\varphi(n_i)} \equiv 1 \pmod{n_i} \implies a_i N_i^{\varphi(n_i)} \equiv a_i \pmod{n_i}$$

Thus, $\sum_i a_i N_i^{\varphi(n_i)}$ solves the system!

Euler's Theorem a, n integers s.t. $\gcd(a,n)=1$.

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

---

pf. #2 via induction & Fermat's Little Theorem

Fermat: p prime, $\gcd(a,p)=1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.
Thus, if n is prime, $a^{\varphi(n)} \equiv 1 \pmod{n}$ since $\varphi(n) = n-1$ in this case. $\Big\}$ base case

Now suppose that $n = p^k$, and suppose that $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$. Then $a^{\varphi(p^k)} = 1 + qp^k$ for some $q \in \mathbb{N}$.

Also, $\varphi(p^{k+1}) = p^{k+1} - p^k = p(p^k - p^{k-1}) = p\,\varphi(p^k)$, so

$$a^{\varphi(p^{k+1})} = \left(a^{\varphi(p^k)}\right)^p = (1+qp^k)^p = 1 + p(qp^k) + \binom{p}{2}(qp^k)^2 + \dots + (qp^k)^p$$

$$= 1 + p^{k+1}(\text{integer}) \equiv 1 \pmod{p^{k+1}}.$$

Then, by induction, $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$ $\forall\, k \in \mathbb{N}$.

In general, $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, and we know that

$$a^{\varphi(p_i^{k_i})} \equiv 1 \pmod{p_i^{k_i}}, \quad i = 1, \ldots, r.$$

Also, $\varphi(p_i^{k_i}) \mid \varphi(n) \implies \dfrac{\varphi(n)}{\varphi(p_i^{k_i})}$ is an integer. Raising the congruence to this power yields

$$a^{\varphi(n)} \equiv 1 \pmod{p_i^{k_i}}.$$

$$\implies \quad a^{\varphi(n)} \equiv 1 \pmod{n}. \quad \boxtimes$$

example $13x \equiv 2 \pmod{40}$

$$x = 2 \cdot 13^{\varphi(40)-1} = \underline{\underline{2 \cdot 13^{15}}}.$$

$$\varphi(40) = \varphi(8 \cdot 5) = \varphi(2^3)\varphi(5) = (2^3 - 2^2) \cdot 4 = \underline{\underline{16}}$$

$$13^2 \equiv 9 \pmod{40} \Longrightarrow 13^3 \equiv 9 \cdot 13 = 117 \equiv -3 \pmod{40}$$

$$13^3 \equiv -3 \pmod{40}$$

$$13^4 \equiv 1 \pmod{40}$$

$$\Longrightarrow 13^{12} \equiv 1 \pmod{40} \Longrightarrow 2 \cdot 13^{12} \equiv 2 \pmod{40}$$

$$\Longrightarrow 13^{15} \equiv -3 \pmod{40} \qquad \underline{x = 2 \cdot 13^{11}}$$

$$2 \cdot 13^{15} \equiv -6 \pmod{40}$$

$$\equiv 34 \pmod{40}.$$

$$\boxed{x = 34}$$

Theorem $n = \sum_{d|n} \varphi(d)$. (due to Gauss)

pf. #1 φ multiplicative, so the function $F(n) := \sum_{d|n} \varphi(d)$ is multiplicative, too. So just check when $n = p^k$:

$$F(p^k) = \sum_{d|p^k} \varphi(d) = \varphi(1) + \varphi(p) + \varphi(p^2) + \dots + \varphi(p^k)$$
$$= \cancel{1} + (p - \cancel{1}) + (p^2 - \cancel{p}) + \dots + (p^k - \cancel{p^{k-1}})$$
$$= p^k = n. \implies F(p^k) = p^k.$$

$\boxtimes$

---

d is a divisor of n.

pf. #2 $S_d := \{ m \in [1,n] : \gcd(m,n) = d \}$

$S_1 = \{a_1, a_2, \dots, a_{\varphi(n)}\}$ etc.

NOTE: $\gcd(m,n) = d$ iff $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$

$\implies \# S_d = \varphi(\frac{n}{d})$.

$$\implies \sum_{d|n} \varphi(\tfrac{n}{d}) = n \implies \sum_{d|n} \varphi(d) = n.$$

$\boxtimes$

FACT: $n \in \mathbb{N}$; $a_1, a_2, \ldots, a_{\varphi(n)}$ relatively prime to n

$$\sum_{i=1}^{\varphi(n)} a_i = \frac{n\varphi(n)}{2}.$$

pf.: $\gcd(a, n) = 1 \iff \gcd(n-a, n) = 1$

$$\Rightarrow a_1 + a_2 + \ldots + a_{\varphi(n)} = (n - a_1) + (n - a_2) + \ldots + (n - a_{\varphi(n)})$$

$$\Rightarrow \sum_{i=1}^{\varphi(n)} a_i = n\varphi(n) - \sum_{i=1}^{\varphi(n)} a_i \Rightarrow \sum_{i=1}^{\varphi(n)} a_i = \frac{n\varphi(n)}{2}.$$

example: $n = p$, prime $\Rightarrow \displaystyle\sum_{i=1}^{p-1} i = \frac{p(p-1)}{2}$.

Note: $\varphi(n)$ is even for any $n > 2$.

$$n = \sum_{d \mid n} \varphi(d) \xrightarrow[\text{Möbius}]{} \varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d} = n \sum_{d \mid n} \frac{\mu(d)}{d}.$$

<u>#3, 7.4</u> $$\sum_{d \mid n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}.$$

$n = p^k$: $$\sum_{d \mid p^k} \frac{\mu^2(d)}{\varphi(d)} = \frac{\mu^2(1)}{\varphi(1)} + \frac{\mu^2(p)}{\varphi(p)} + 0$$

$$= 1 + \frac{1}{p-1} = \frac{p}{p-1} = \frac{p^k}{\varphi(p^k)}$$

$$= \frac{n}{\varphi(n)}.$$

$\boxtimes$