Recall

$$\phi(n) = \#\{1 \leqslant a \leqslant n \mid \gcd(a,n) = 1\}$$

satisfies

$$\phi(p^k) = p^k - p^{k-1} \quad \text{and} \quad \phi(mn) = \phi(m)\phi(n)$$

if p is prime, and $\gcd(m,n) = 1$.
Define

$$F(n) = \sum_{d|n} \phi(d)$$

to be the sum of ϕ applied to all of the divisors of n (including 1 and n).
Ex: The divisors of 12 are $1, 2, 3, 4, 6$, and 12, so

$$\begin{aligned} F(12) &= \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) \\ &= 1 + 1 + 2 + (4-2) + 1 * 2 + (4-2) * 2 \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12 \end{aligned}$$

$$\phi(n) = \#\{1 \leqslant a \leqslant n \mid \gcd(a,n) = 1\}$$

$$\phi(p^k) = p^k - p^{k-1} \quad \text{and} \quad \phi(mn) = \phi(m)\phi(n)$$

for p is prime, and $\gcd(m,n) = 1$.

Define $\quad F(n) = \sum_{d|n} \phi(d).$

Ex: The divisors of 12 are $1, 2, 3, 4, 6$, and 12, so

$$F(12) = \phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 12$$

Theorem

For $n \in \mathbb{Z}_{>0}$, we have $F(n) = n$.

Prove in two parts:

Lemma (1)

If p is prime, then $F(p^k) = p^k$.

Proof. The divisors of p^k are $1, p, p^2, \ldots, p^k$. So

$$F(p^k) = \sum_{i=0}^{k} \phi(p^i) = 1 + \underbrace{\sum_{i=1}^{k} (p^i - p^{i-1})}_{\text{telescoping sum!}} = 1 + p^k - 1 = p^k.$$

□

$$\phi(p^k) = p^k - p^{k-1} \quad \text{and} \quad \phi(mn) = \phi(m)\phi(n)$$

for p is prime, and $\gcd(m, n) = 1$.

Define $$F(n) = \sum_{d|n} \phi(d).$$

Theorem

For $n \in \mathbb{Z}_{>0}$, we have $F(n) = n$.

Prove in two parts:

Lemma (1)

If p is prime, then $F(p^k) = p^k$.

Lemma (2)

If $\gcd(m, n) = 1$, then $F(mn) = F(m)F(n)$.

(F, ϕ are multiplicative)

Proof. Let $d_1, \ldots, d_k$ be the divisors of m and $e_1, \ldots, e_\ell$ the divisors of n. Then $\gcd(d_i, e_j) = 1$, and the divisors of mn are

$$d_i e_j \quad \text{for } 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant \ell.$$

Compute $F(m)F(n)\ldots$

Back to Fermat's little theorem

We computed that for a prime p and integer a with $p \nmid a$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Question: What is the *least* (positive) power k with $a^k \equiv_p 1$?

$a^k \pmod{5}$: ($\leftarrow k \rightarrow$ across, $\uparrow a \downarrow$ down)

a	1	2	3	4	
1	1	1	1	1	$\lvert 1\rvert_5 = 1$
2	2	4	3	1	$\lvert 2\rvert_5 = 4$
3	3	4	2	1	$\lvert 3\rvert_5 = 4$
4	4	1	4	1	$\lvert 4\rvert_5 = 2$

$a^k \pmod{7}$: ($\leftarrow k \rightarrow$ across, $\uparrow a \downarrow$ down)

a	1	2	3	4	5	6	
1	1	1	1	1	1	1	$\lvert 1\rvert_7 = 1$
2	2	4	1	2	4	1	$\lvert 2\rvert_7 = 3$
3	3	2	6	4	5	1	$\lvert 3\rvert_7 = 6$
4	4	2	1	4	2	1	$\lvert 4\rvert_7 = 3$
5	5	4	6	2	3	1	$\lvert 5\rvert_7 = 6$
6	6	1	6	1	6	1	$\lvert 6\rvert_7 = 2$

Define: The order of $a \pmod{p}$, written $|a|$ or $|a|_p$, is the smallest positive integer k such that $a^k \equiv 1 \pmod{p}$. (Book: $e_p(a) = |a|_p$)

Order

Define: Fix n, and let a be an integer with $\gcd(a, n) = 1$. The order of $a \pmod{n}$, written $|a|$ or $|a|_n$, is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. (Book: $e_n(a) = |a|_n$)

Facts:

(1) $|a| = 1$ if and only if $a = 1$.

(2) $1 \leqslant |a|_n \leqslant \phi(n)$.

(3) $|a|_n$ divides $\phi(n)$.

(4) If $|a|_n = k$, then $1, a, a^2, \ldots, a^{k-1}$ are all pairwise distinct (mod n). In particular, for p prime, we have $|a|_p = p - 1$ if and only if

$$\{1, 2, \ldots, p-1\} \equiv_p \{1, a, a^2, \ldots, a^{p-2}\}.$$

We call a a primitive root (mod n) if $|a|_n = \phi(n)$.
Define

$$\psi_n(k) = \#\{1 \leqslant a < n \mid |a| = k\}$$

You try: Compute $\psi_p(k)$ for $1 \leqslant k \leqslant p - 1$ for $p = 3, 5$, and 7.