Euler-totient function ϕ

For $n>0$, $\phi(n) =$ count of the m, $1 \le m \le n$
and $\gcd(m, n) = 1$

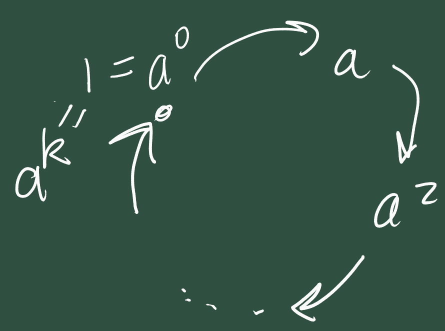
$= |U(n)|$, $U(n) =$ group of units modulo n under mult.

Important result is Euler's theorem.

- for $a \in U(n)$ $\quad a^{\phi(n)} \equiv 1 \pmod{n}$

$\Rightarrow |a| =$ order of a in $U(n)$.
$=$ least exponent k, $k \geq 1$ $\quad a^k \equiv 1 \bmod (n)$

$$k \mid \phi(n)$$



Theorem 5.1

If $n = \prod_{i=1}^{r} p_i^{a_i}$ then

$$\phi(n) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1)$$

Already proved

- $\phi(p) = p - 1$
- $\phi(p^a) = p^{a-1}(p-1)$

Once we've proved ϕ is multiplicative.

i.e. $\boxed{\gcd(a,b)=1 \Rightarrow \phi(ab)=\phi(a)\phi(b)}$

we can Th 5.1 using this.

$$\phi\left(\prod_{i=1}^{r} p_i^{a_i}\right) = \prod_{i=1}^{r} \phi(p_i^{a_i})$$

since $(p_i^{a_i}, p_j^{a_j})$ are coprime for $i \neq j$

giving us Th 5.1.

Lemma 5.3 If $a \equiv b \pmod n$

then $\gcd(a,n) = \gcd(b,n)$

Proof: Note that

$$a \equiv b \pmod n \Leftrightarrow n \mid a-b$$

$$\Leftrightarrow a-b = qn, \text{ for some } q \in \mathbb{Z}.$$

$a = qn + b$

"a as a lin. comb of n & b"

$b = a - qn$

"b as a lin. comb. of a & n"

By theorem 2.1 (3) if $c | n$ & $c | b$

then $c | a$ so $c | n$ & $c | a$

Similarly if $c | n$ & $c | a$

then $c | b$ so $c | n$ & $c | b$.

So (a,n) and (b,n) share the exact <u>same common divisors.</u>

$$\Rightarrow \quad \gcd(a,n) = \gcd(b,n) \quad \blacksquare$$

<u>Lemma 5.4</u>

$$\gcd(u, vw) = 1 \iff \left\{ \begin{array}{c} \gcd(u,v) = 1 \\ \text{AND} \\ \gcd(u,w) = 1 \end{array} \right\}$$

Proof in notes done via lin. combs.

We could also appeal to <u>F.T.A</u>.

So $\gcd(u, vw) = 1$ means <u>factorisations</u> of <u>u</u> and <u>vw</u> have no primes in common

But by the F.T.A. prime factorisation of vw

is the product of prime factorisations of v and w.

So u has no comes in common with v, or with w. ∎

Lemma 5.5 ϕ is multiplicative.

Assume i.e. $\gcd(a,b)=1$ then
$$\phi(ab)=\phi(a)\phi(b).$$

We'll prove this directly by counting the m from $1 \le m \le ab$ that are coprime to ab and see that the count is $\phi(a)\phi(b)$.

Lay out the m in an $a \times b$ grid.

$\phi(b)$

$$\begin{array}{cccccc}
1 & 2 & 3 & \cdots & b-1 & b \\
b+1 & b+2 & b+3 & \cdots & 2b-1 & 2b \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
(a-2)b+1 & & & & & (a-1)b \\
(a-1)b+1 & \cdots & \cdots & \cdots & & ab
\end{array}$$

$$\begin{array}{cccccc} \equiv & \equiv & \equiv & & \equiv & \equiv \\ 1 & 2 & 3 & & b-1 & 0 \\ (\text{mod } b) & (\text{mod } b) & & & (\text{mod } b) & (\text{mod } b) \end{array}$$

- each column is a cong. class mod b.
- in each row we see a complete set of residues modulo b.
- in each column we have a entries all of which are incongruent modulo a.

Pf By contradiction. Suppose we have

$$rb + r \equiv wb + r \pmod{a}.$$

$$\Rightarrow \quad rb \equiv wb \pmod{a}.$$

$$\Rightarrow \quad rbb^{-1} \equiv wbb^{-1} \pmod{a}$$

since b^{-1} exists mod a, as $\gcd(a,b)=1$

$$\Rightarrow \quad r \equiv w \pmod{a}$$

But $0 \le r, w \le a-1$

$$\Rightarrow \quad r = w \qquad \blacksquare$$

- so in each column we have a complete set of elements modulo a.

So now we can perform the count, with help of the lemma

$$\gcd(m, ab) = 1 \iff \begin{pmatrix} \gcd(m,a)=1 \ \& \\ \gcd(m,b)=1 \end{pmatrix}$$

There are $\phi(b)$ of the columns which contain integers m, all of which are co-prime to b.

within in any one of these columns there $\phi(a)$ entries that are also co-prime to a.

There are clearly

$\phi(b) \cdot \phi(a)$ of such m,

that co-prime to a, and coprime to b.

$\Longleftrightarrow$ coprime to ab, by lemma $\gcd(a,b)=1$.

Therefore $\phi(ab) = \phi(b)\cdot\phi(a)$.

This is the proof of Th 5.1

Last row of grid.

$(a-1)b+1$, $(a-1)b+2$, ...

. . ., $\underbrace{(a-1)b+b-1}_{ab-1}$, $\underbrace{(a-1)b+b}_{ab}$.

Applications of ϕ formula (Th. 5.1).

Ex 5.1.1

$\boxed{\text{Q2.}}$ Find all solutions to

$\phi(n)=12.$

Recall $\phi(p)=p-1$ $\quad 1\le m\le \cancel{p}$

$1\le m\le p-1$

So that top border is line $y=x-1$.

From looking at plot there appear to be a handful of solutions. six in fact

Let's prove this.

Assume $$n = \prod_{i=1}^{r} p_i^{a_i}$$ potentially infinite number of n.

and so

$$\phi(n) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1) = 12.$$

$$= 2^2 \cdot 3$$

This surely, places great restrictions on the p_i. The only p_i that might be here, none bigger 13, because of the $p-1$ factor

$$p_i = 13, 2, 3, 5, 7, \cancel{11}.$$

So know we know, any solution n has the form.

$$n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \cdot 13^e$$ finite # cases

what restrictions on exponents?

$e = 0,1$. $d = 0,1$, $c = 0,1$

$$\boxed{b = 0, 1, 2 \quad , \quad a = 0, 1, 2, 3}$$

this from the fact that $12 = 2^2 \cdot 3$

So there at most $2^3 \cdot 3 \cdot 4 = 96$ solutions. Wonderful progress.

Let's inspect them all

Supposes $e = 1$.

ie. $n = 13 \cdot m$, $\gcd(13, m) = 1$

$$\Longrightarrow \phi(n) = \phi(13 \cdot m)$$
$$= \phi(13) \cdot \phi(m) \quad , \text{ by mult. prop}$$
$$= 12 \cdot \phi(m)$$

So $\phi(n) = 12 \Longleftrightarrow \phi(m) = 1$.

$$\Longleftrightarrow m = 1, 2.$$

as any $m \geq 3$, we have 1 and $m-1$ at least, coprime to m.

So ~~若~~ we've found two such solutions $\boxed{n = 13, 26.}$

From now on. we assume $e=0$.

Now look at $d=1$ case ($e=0$)

So $n = 7 \cdot m$, $\gcd(m,7)=1$

$$\Rightarrow \phi(n) = \phi(7)\cdot\phi(m)$$

$$= 6\cdot\phi(m) = 12$$

$$\Leftrightarrow \phi(m) = 2.$$

$$\Leftrightarrow m = 3, 4, 6.$$

prime factor. $3, 2^2, 2\cdot 3$

So we've found another three solutions

$$\boxed{n = 21, 28, 42.}$$

So now can assume ($e=0$, $d=0$).

Assume $c=1$.

i.e. $n = 5\cdot m$, $\gcd(m,5)=1$

$$\Rightarrow \phi(n) = \phi(5)\phi(m)$$

$$= 4\phi(m) = 12$$

$$\Leftrightarrow \phi(m) = 3.$$

which is impossible as the factor $p^{a-1}(p-1)$ can never equal 3, as it's ≥ 6.

So no solutions here.

So now can assume $e=d=c=0$

So now left with cases

$$n = 2^a \cdot 3^b \quad , \quad a = 0,1,2,3 \quad b = 0,1,2.$$

From these twelve possibilities only one gives.

$$\phi(n) = 2^{a-1} 3^{b-1} \cdot 2 = 12.$$

$b=2,\ a=2$ i.e. $\boxed{n = 2^2 \cdot 3^2 = 36}$

So these 6 are the <u>only</u> solutions to $\phi(n) = 12$

Same approach should work for any such problem.

Eg 5.1 Q11

Claim: $\boxed{\phi(n)=\phi(2n) \text{ iff } n \text{ is odd.}}$

and $\phi(2n)=2\phi(n)$ iff even n.

Proof "$\Leftarrow$" ✓

Assume n is odd, ie. $\gcd(n,2)=1$

$$\phi(2n) = \phi(2)\phi(n), \text{ by } \phi \text{ being multiplic.}$$

$$= \phi(n).$$

"$\Rightarrow$" $\phi(n)=\phi(2n) \Rightarrow n$ is odd.

Let's consider its contrapositive

"n is even $\Rightarrow \phi(n) \neq \phi(2n)$"

Proof Assume n is even

ie. $n = 2^a \cdot m$, where m is odd and $a \geq 1$

$$\Rightarrow \phi(2n) = \phi(2^{a+1} m)$$

$$= \phi(2^{a+1})\phi(m), \quad \text{multiplicati. of } \phi.$$

$$= 2^a \cdot \phi(m)$$

$$= 2\,(2^{a-1}\phi(m))$$

$$= 2\cdot(\phi(2^a)\phi(m))$$

$$= 2\,\phi(2^a m)$$

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

So $\phi(2n) \neq \phi(n)$.

This proves the contrapositive of "$\Rightarrow$" of the claim.

Also see a proof that $2\phi(n) = \phi(2n) \Leftrightarrow n$ is even.