Ques: Choose a number, eg 35
factors of 35, other than itself are : 1, 5, 7.

$D_1 = \{ 1 \leq a < 35 \mid \gcd(a, 35) = 5 \}$

set of   s.t

$D_1 = \{ 5, 10, 15, 20, 25, 30 \}$

* $|D|$ is Cardinality of set D i.e no. of elements in D.

$D_2 = \{ 1 \leq a < 35 \mid \gcd(a, 35) = 7 \}$

$D_2 = \{ 7, 14, 21, 28 \}$

$|D_1| = 6 \quad |D_2| = 4$

How to find $|D|$?

Euler function : $\phi(n)$. Let $n = 7^3 \times 5^2 \times 11^3$, n written as product of primes
Find $\phi(n)$

$\phi(n) = 6 \times 7^2 \times 4 \times 5 \times 10 \times 11^2$

↳ no. of all numbers below and has gcd = 1 with n.

eg: let $n = 5^3 \times 7^2 \times 13$

$\phi(n) = (5-1) \cdot 5^{3-1} \times (7-1) \cdot 7^{2-1} \times (13-1)\, 13^{1-1}$

$= 4 \times 5^2 \times 6 \times 7 \times 12 \times 1$

$\phi(n) = \underline{50400}$

What does $\phi(n) = 50400$ mean ?
No. of positive integers below n, s.t each has gcd with n = 1 is : 50400
Creates a set $D = \{ 1 \leq a < n \mid \gcd(a, n) = 1 \}$
and so the cardinality, $|D| = \phi(n) = 50400$

eg: $n = 302$. Find $\phi(n)$.

$n = 2 \times 151$

$\phi(n) = 1 \times 2^0 \times 150 \times 151^0$

$= 150.$

Meaning, if $D = \{ 1 \leq a < 302 \mid a \in N^*, \gcd(a, n) = 1 \}$,
then $|D| = \cancel{150}\ 150$

eg: let $n = 75$. Find $F = \{ 1 \leq a < n \mid \gcd(a, n) = 5 \}$. Find $|F|$

Answer: $|F| = \phi\left(\frac{n}{5}\right)$

$= \phi\left(\frac{75}{5}\right) = \phi(15)$

$15 = 3 \times 5$

$\phi(15) = 2 \times 4 = 8$

Hence $|F| = 8$. There are exactly 8 numbers below 75 where $\gcd(a, 75) = 5$

Check: $F = \{ 5, 10, 20, 35, 40, 55, 65, 70 \}$
number of elements = 8.

General result:

let $n \in \mathbb{N}^*$.
Take $F = \{ 1 \leq a < n \mid \gcd(a,n) = k \}$
Then $|F| = \varphi\left(\frac{n}{k}\right)$

recall if $\gcd(a,n) = k$ then $k \mid a$ and $k \mid n$.
$\frac{n}{k}$ will always be an integer.

* By convention: $\varphi(1) = 1$.

Suppose $n = 8$
Factors of n are:

1 $\quad \varphi(1) = 1$

2 $\quad \varphi(2) = 1$

4 $\quad \varphi(4) = 2$

8 $\quad \varphi(8) = 4$

Adding $\varphi(1) + \varphi(2) + \varphi(4) + \varphi(8) = 8$

Big result: $\sum_{d \mid n} \varphi(d) = n$

i.e if $d_1, d_2, d_3, \dots, d_k$ are all factors of n
then $\phi(d_1) + \phi(d_2) + \dots + \phi(d_k) = n$.

eg: $n = 34$.
Factors of 34:

$1 = d_1$
$2 = d_2$
$17 = d_3$
$34 = d_4$

now, $\underset{1}{\underset{\downarrow}{\phi(1)}} + \underset{1}{\underset{\downarrow}{\phi(2)}} + \underset{16}{\underset{\downarrow}{\phi(17)}} + \underset{16}{\underset{\downarrow}{\phi(34)}} = 34$.

observe $\phi(17) = \phi(34)$

True: $\phi(n) = \phi(2n)$
given that n is odd (i.e $n \bmod 2 = 1$)

can conclude with examples: $\phi(30) = \phi(15)$
$\phi(50) = \phi(25)$
but
$\phi(8) \neq \phi(4)$

* also, if $n = 2^k$
and $\phi(n) = 2^{k-1}$

also $\phi(n) = 2 \times \phi(2^{k-1})$
$= 2 \times 2^{k-2}$
$= 2^{k-1}$

Euler - Fermat Result:

let $n, a \in \mathbb{N}^*$, and $\gcd(a,n) = 1$.
Then $a^{\phi(n)} = 1$ in planet $\mathbb{Z}_n$

i.e $a^{\phi(n)} \equiv 1 \pmod{n}$
i.e $n \mid a^{\phi(n)} - 1$, $\quad a^{\phi(n)} = qn + 1$ for some $q \in \mathbb{Z}$

all equivalent statements (goes both ways)

let $n = 15 = 3 \times 5$
$\phi(n) = 8$

now $\gcd(7,15) = 1 \rightarrow 7$ valid for a
$\gcd(101, 15) = 1 \rightarrow 101$ valid for a
$\gcd(77, 15) = 1 \rightarrow 77$ valid for a

So
$7^8 \pmod{15} = 1$
$101^8 \pmod{15} = 1$
$77^8 \pmod{15} = 1$

$\Leftrightarrow$

$15 \mid (7^8 - 1)$
$15 \mid (101^8 - 1)$
$15 \mid (77^8 - 1)$

Homework questions:

1 Let $n = 84$

i. Find all factors of 84.

ans:

1	84
2	42
3	28
4	21
6	14
7	12

ii. Say $d_1, d_2, \dots d_k$ are all factors of n. Find $\phi(d_i)$ for each $1 \leq i \leq k$.

ans:
$d_1 = 1$, $\phi(1) = 1$.
$d_2 = 2$, $\phi(d_2) = 1$
$d_3 = 3$, $\phi(3) = 2$
$d_4 = 4 = 2^2$, $\phi(2^2) = 2$

$d_5 = 6 = 3 \times 2$, $\phi(3 \times 2) = 2$
$d_6 = 7$, $\phi(7) = 6$
$d_7 = 12 = 2^2 \times 3$, $\phi(d_7) = 4$
$d_8 = 14 = 7 \times 2$, $\phi(14) = 6$

$d_9 = 21 = 7 \times 3$, $\phi(21) = 12$
$d_{10} = 28 = 2^2 \times 7$, $\phi(28) = 12$
$d_{11} = 42 = 2 \times 21$, $\phi(42) = \phi(21) = 12$
$d_{12} = 84$, $\phi(d_{12}) = 24$

iii. Find $\phi(d_1) + \phi(d_2) + \dots + \phi(d_k)$

ans: $1 + 1 + 2 + 2 + 2 + 6 + 4 + 6 + 12 + 12 + 12 + 24$
$= 84 = n$

iv. Let $F = \{ 1 \leq a < 88 \mid \gcd(a, 88) = 11 \}$. Find $|F|$.

ans: $n = 88$, $k = 11$.
Then $|F| = \phi\left(\frac{n}{k}\right) = \phi\left(\frac{88}{11}\right) = \phi(8) = 4$.

2 i. Find $17^{41} \bmod 41$. Justify your answer. (note that $\phi(41) = 40$.) So $17^{40} = 1$ in planet $\mathbb{Z}_{41}$. Multiply both sides with 17, we get $17^{41} = 17$ in $\mathbb{Z}_{41}$.

ii. Give me some meaning to (i).

ans. $17^{41} = 17$ in $\mathbb{Z}_{41}$

This also means that $17^{41} \equiv 17 \pmod{41}$

and also $41 \mid 17^{41} - 17$: i.e 41 is a factor of $17^{41} - 17$

or even $17^{41} = q41 + 17$ for some $q \in \mathbb{Z}$

iii. Assume that $\gcd(a, 15) = 1$. Convince me that $a^{27} \pmod{15} = a^3 \pmod{15}$

ans: assume $n = 15$.

then $\phi(n) = 8$

By Euler - Fermat Result, $a^8 \pmod{15} = 1$, for any $a \in N^*$

now, $a^{27} = a^{8+8+8+3}$

$= a^8 \cdot a^8 \cdot a^8 \cdot a^3$

$a^{27} \pmod{15} = a^8 a^8 a^8 a^3 \pmod{15}$

Recall $xy \pmod{n} = x \pmod{n} \cdot y \pmod{n}$

Hence $a^{27} \pmod{15} = a^8 \pmod{15} \cdot a^8 \pmod{15} \cdot a^8 \pmod{15} \cdot a^3 \pmod{15}$

$= 1 \times 1 \times 1 \times a^3 \pmod{15}$

$\therefore \quad a^{27} \pmod{15} = a^3 \pmod{15}$

iv. Convince me that $2^{165} \pmod{15} = 2$. (note that $\phi(15) = 8$ and $165 = 8 \times 20 + 5$ and $\gcd(2,15) = 1$)

ans: let $a = 2$ and $n = 15$,

$\gcd(2,15) = 1$. and $\phi(15) = 8$

So by Euler - Fermat result, $2^8 \equiv 1 \pmod{15}$

now, $2^{165} = 2^{8 \times 20} 2^5$ ~~mod~~

$2^{165} \pmod{15} = 2^{8 \times 20} \pmod{15} \cdot 2^5 \pmod{15}$

$= 1 \times 2^5 \pmod{15}$

$= 2$.

~~26~~ 27/02/18

* gcd of non-positive integers such as $\gcd(-30, 2)$.

it is understood; gcd(positive, positive)

⇒ you are working in planet N

$\gcd(2,8)$ over N is 2.

$\gcd(2,8)$ over $\mathbb{Z}$ is 2 and -2

Definition: a, b in set A.

$d = \gcd(a,b)$ if

$\boxed{1}$ $d \mid a$ and $d \mid b$

$\boxed{2}$ if $m \mid a$ and $m \mid b$, ~~then~~ then $m \mid d$.

eg: $\gcd(2,4)$ over $\mathbb{Z}$ is 2 or -2.

Suppose $d = 2$, then $-2 \mid 2$ in $\mathbb{Z}$ i.e $-2 \times -1 = 2$

and also $-2 \mid 4$ in $\mathbb{Z}$

Similarly, it is understood that prime numbers are over N.

eg, 2, 3, 5, 7 ....

prime numbers can also be over $\mathbb{Z}$

$\therefore$ ..., $-11, -7, -5, -3, -2, 2, 3, 5, \ldots$