Euler's totient function

Here, we learn about Euler's totient function, written as $\emptyset(n)$. It is used in Euler's theorem (https://www.savitagandhi.com/articles/eulers-theorem). Recall, positive number a is relatively prime to b if $\gcd(a, b) = 1$. Euler's totient function $\emptyset(n)$ counts those positive integers $\leq n$, which are relatively prime to n. Because, it is denoted as $\emptyset(n)$, it is more commonly called Euler's phi function or Euler's $\emptyset$ – function.

Thus, it can be stated that $\emptyset(n)$ is the number of integers, $1 \leq k \leq n$, satisfying $\gcd(k, n) = 1$. Such integers k are also called totatives of n.

Example 1: Determine totatives of 12 and $\emptyset(12)$.

Solution: Now, $\gcd(2,12) = 2, \gcd(3,12) = 3, \gcd(4,12) = 4, \gcd(6,12) = 6, \gcd(8,12) = 4, \gcd(9,12) = 3, \gcd(10,12) = 2,\ \gcd(12,12) = 12$. Therefore, 2, 3, 4, 6, 8, 9, 10, 12 are not totatives of 12. As $\gcd(1,12) = 1, \gcd(5,12) = 1, \gcd(7,12) = 1, \gcd(11,12) = 1$; 1, 5, 7, 11 are relatively prime to 12, giving totatives of 12 as 1, 5, 7, 11 and number of totatives being 4, $\emptyset(12) = 4$.

Example 2: Determine totatives of 7 and $\emptyset(7)$.

Solution: 7 is prime. The only factors of 7 are 1 and 7. All the positive integers $k, 1 \leq k < 7$ are relatively prime to 7; $\gcd(k, 7) = 1\ for\ k = 1, 2, 3, 4, 5, 6$. Therefore, 1,2, 3, 4, 5, 6 are totatives of 7. Number of totatives of 7 are 6, $\emptyset(7) = 6$.

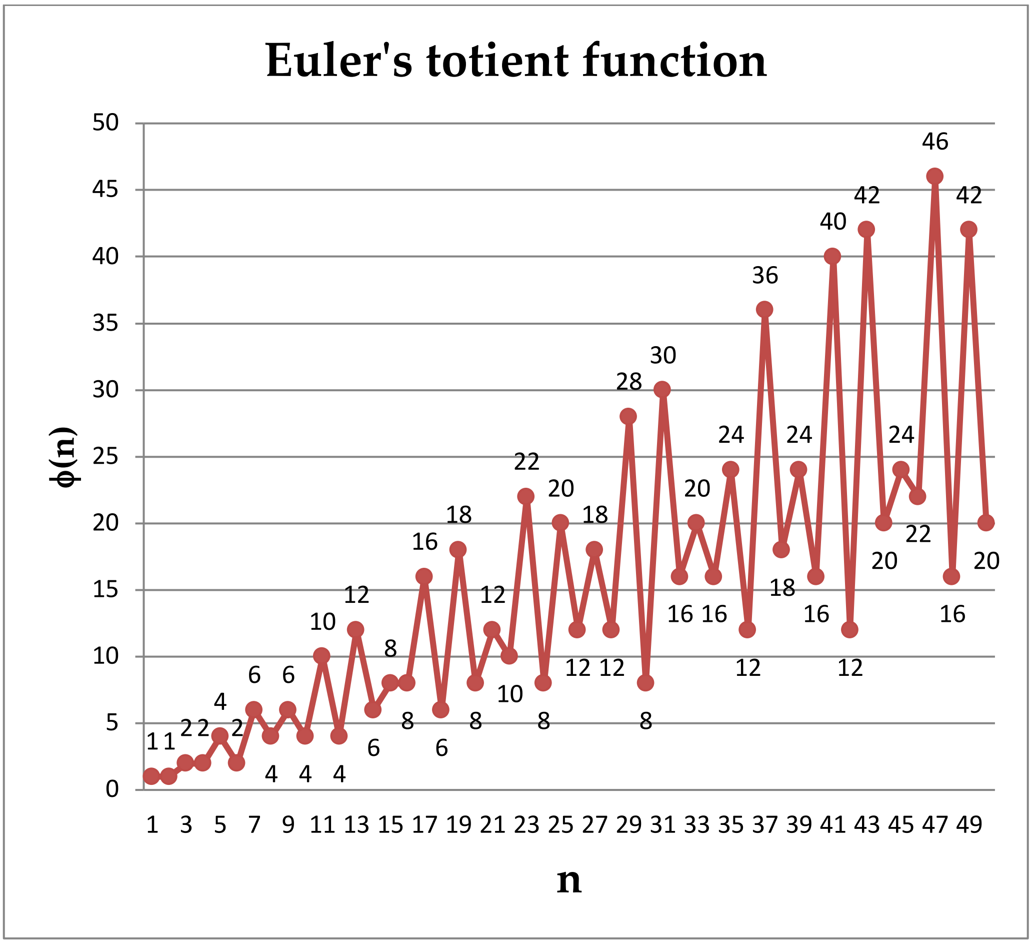
Following **Table 1** lists the Euler's totient function $\emptyset(n)$ and the set of totatives of n for $1 \leq n \leq 50$, whereas **Graph 1** shows the graph plot of n verses $\emptyset(n)$.

n	$\emptyset(n)$	Totatives of n
1	1	{1}
2	1	{1}
3	2	{1, 2}
4	2	{1, 3}
5	4	{1, 2, 3, 4}
6	2	{1, 5}
7	6	{1, 2, 3, 4, 5, 6}
8	4	{1, 3, 5, 7}
9	6	{1, 2, 4, 5, 7, 8}

10	4	{1, 3, 7, 9}
11	10	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10}
12	4	{1, 5, 7, 11}
13	12	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12}
14	6	{1, 3, 5, 9, 11, 13}
15	8	{1, 2, 4, 7, 8, 11, 13, 14}
16	8	{1, 3, 5, 7, 9, 11, 13, 15}
17	16	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16}
18	6	{1, 5, 7, 11, 13, 17}
19	18	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18}
20	8	{1, 3, 7, 9, 11, 13, 17, 19}
21	12	{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20}
22	10	{1, 3, 5, 7, 9, 13, 15, 17, 19, 21}
23	22	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22}
24	8	{1, 5, 7, 11, 13, 17, 19, 23}
25	20	{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24}
26	12	{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}
27	18	{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}
28	12	{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27}
29	28	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28}
30	8	{1, 7, 11, 13, 17, 19, 23, 29}
31	30	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30}
32	16	{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31}
33	20	{1, 2, 4, 5, 7, 8, 10, 13, 14, 16, 17, 19, 20, 23, 25, 26, 28, 29, 31, 32}
34	16	{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31,33}

35	24	{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34}
36	12	{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35}
37	36	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24,,25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36}
38	18	{1, 3, 5, 7, 9, 11, 13, 15, 17, 21, 23, 25, 27, 29, 31, 33, 35, 37}
39	24	{1, 2, 4, 5, 7, 8, 10, 11, 14, 16, 17, 19, 20, 22, 23, 25, 28, 29, 31, 32, 34, 35, 37, 38}
40	16	{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39}
41	40	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40}
42	12	{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41}
43	42	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42}
44	20	{1, 3, 5, 7, 9, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 35, 37, 39, 41 ,43}
45	24	{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44}
46	22	{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 29, 31, 33, 35, 37,39, 41, 43, 45}
47	46	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46}
48	16	{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47}
49	42	{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48}
50	20	{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49}

Table 1: Euler's totient function $\emptyset(n)$ and the set of totatives of n for $1 \leq n \leq 50$



Graph 1: Graph of $\boldsymbol{n}$ verses $\emptyset(\boldsymbol{n})$

Let us have a look at some elementary properties of Euler's phi function, which are quite useful, to mention few areas as elementary number theory, Euler's theorem, primitive roots of unity, and RSA cryptography.

Theorem: Euler's phi function $\emptyset(n)$ satisfies following properties:

(i) $\emptyset(1) = 1$.

(ii) If p is prime then $\emptyset(p) = p - 1$.

(iii) If p and q are distinct primes then $\emptyset(p \cdot q) = \emptyset(p) \cdot \emptyset(q) = (p-1) \cdot (q-1)$

Proof: (i) gcd (1, 1) = 1 and 1 is the only integer in the range $1 \leq k \leq 1$. Thus, number of totatives of 1 is 1. Therefore, $\emptyset(1) = 1$.

(ii) As p is prime, its only divisors are 1 and p. Thus, for $1 \leq k \leq p-1$, $\gcd(k,p) = 1$ and $\gcd(p,p) = p \neq 1$ (p is prime, $p \geq 2$). Therefore, number of integers in the range $1 \leq k \leq p$ such that $\gcd(k,p) = 1$ is $p - 1$. All integers in the range except, p itself, are relatively prime to p . So, we get, $\emptyset(p) = p - 1$.

Example 2, is a particular case of preceding result for $p = 7$. Also, from the Table 1, it can be verified that $\emptyset(p) = p - 1$ for primes < 50.

(iii) Let $n = p \cdot q$, where p and q are distinct primes. The positive integers $\leq n$ are $1, 2, 3, \ldots, (pq-1), (pq)$. $\emptyset(p \cdot q)$ is the number of positive integers $\leq pq$, which are relatively prime to pq, that is, number of $k's$ such that $1 \leq k \leq pq$ and $\gcd(k, pq) = 1$. $\gcd(k, pq)$ will be 1, when k has neither p nor q as one of its factors. The numbers with p as one of the factors are $p, 2p, \ldots, (q-1)p, qp$. Count of such numbers is q and the numbers with q as one of the factors are $q, 2q, \ldots, (p-1)p, pq$. Count of such number is

p. Total count of distinct numbers with p or q as one of the factors is $q + p - 1$. (pq to be counted once). Required number of positive integer relatively prime to pq are : $pq - (q + p - 1) = pq - p - q + 1$

$= p(q-1) - 1(q-1)$

$= (p-1)(q-1)$

$= \emptyset(p) \cdot \emptyset(q)$, which proves the result.

Example 3: Verify $\emptyset(p \cdot q) = \emptyset(p) \cdot \emptyset(q)$, for $n = 15 = 3 \cdot 5$

Solution: For $n = 15$, $\emptyset(15)$ is count of positive integers relatively prime to 15.
Set of numbers relative prime to 15 is {1, 2, 4, 7, 8, 11, 13, 14}, thus there are 8 natural numbers, which are relatively prime to 15. Thus, $\emptyset(15) = 8$. Now, use of property (ii) of preceding theorem: (If p is prime then $\emptyset(p) = p - 1$); gives $\emptyset(5) = 4$ *and* $\emptyset(3) = 2$.
Thus, $\emptyset(5) \cdot \emptyset(3) = 4 \cdot 2 = 8 = \emptyset(15)$.

There is general result, about $\emptyset(n)$, which can be proved using Chinese remainder theorem (https://www.savitagandhi.com/articles/chinese-remainder-theorem). This states, for any positive integer n, $\boldsymbol{\emptyset(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)}$, where the product is over **distinct** primes p dividing n. As a particular case, if $n = p \cdot q$, where p and q are distinct primes, $\emptyset(p \cdot q) = p \cdot q \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = \frac{(pq)(p-1)(q-1)}{pq} = (p-1)(q-1)$, which is same as property (iii) proved in preceding theorem. Let us solve one example using this generalized theorem.

Example 4: Determine $\emptyset(120)$.

Solution: $120 = 2^3 \cdot 3 \cdot 5$; primes dividing 120 are 2, 3 and 5. Use the result:
$\boldsymbol{\emptyset(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)}$; where the product is over **distinct** primes p dividing n.
Here $n = 120$, and distinct primes are 2, 3 and 5. Therefore,

$$\emptyset(120) = 120 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$
$$= 120 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 32$$

****