

Euler's Totient Function

Dragan Marković

Euler's totient function, denoted as $\varphi(n)$, is a function which returns number of numbers less than or equal to n that are relatively prime with n .

Euler's product formula states that $\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \dots \cdot (1 - \frac{1}{p_k})$. Where p_i 's are n 's prime divisors. For example $\varphi(36) = 36 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) = 12$. Now, natural question arises, what is the easiest way to implement without dealing with doubles and precision errors?

First let's assume that we can find all of n 's prime divisors in $\mathcal{O}(\sqrt{n})$ time. This can be easily done by using the fact that at most one prime factor of n can be larger than \sqrt{n} . Here is a simple pseudocode which accomplishes that.

```
Prints all prime divisors of n:
for  $i = 1$  to  $\sqrt{n}$  do
    if  $i$  divides  $n$  then
        print( $i$ )
        while  $i$  divides  $n$  do  $n = n \setminus i$ 
        end while
    end if
end for
if  $n > 1$  then print( $n$ )           ▷ Checks for that one prime larger than  $\sqrt{n}$ 
end if
```

Having this in mind we still need an efficient way of calculating $\varphi(n)$ without using doubles. To achieve that we can use a simple programming trick, let's do the following:

$$\begin{aligned} n_0 &= n \\ n_1 &= n_0 - \frac{n_0}{p_1} = n \cdot (1 - \frac{1}{p_1}) \\ n_2 &= n_1 - \frac{n_1}{p_2} = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \\ &\vdots \\ &\vdots \\ &\vdots \\ n_k &= n_{k-1} - \frac{n_{k-1}}{p_k} = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \dots \cdot (1 - \frac{1}{p_k}) = \varphi(n) \end{aligned}$$

After this analysis it's pretty clear that all we have to do is subtract $\frac{n}{p_i}$ from n in each step of k steps in our algorithm. It can be easily shown that $k < \sqrt{n}$, since k is the number of prime divisors of n , therefore our entire algorithm has complexity of $\mathcal{O}(\sqrt{n})$.

Some useful characteristics of phi functions:

1. $\sum_{d|n} \varphi(d) = n$
2. $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m) \cdot \frac{\gcd(n, m)}{\varphi(\gcd(n, m))}$
3. $\varphi(\text{lcm}(n, m)) \cdot \varphi(\gcd(n, m)) = \varphi(n) \cdot \varphi(m)$
4. $\sum k = \frac{1}{2} \cdot n \cdot \varphi(n)$, for $n > 1$, $1 \leq k \leq n$ and $\gcd(k, n) = 1$
5. if $a|b$ then $\varphi(a)|\varphi(b)$
6. $a^{\varphi(m)} \% m = 1$, iff $\gcd(a, m) = 1$ (Euler's theorem)
7. $a^{p-1} \% p = 1$, for $1 \leq a < p$ and p is prime (Fermat's little theorem)
8. $\frac{a}{b} \% m = (a \% m) \cdot (b^{\varphi(m)-1} \% m) \% m$, if $\gcd(b, m) = 1$ and $b|a$
9. $a^b \% m = (a \% m)^{b \% \varphi(m)} \% m$, iff $\gcd(a, m) = 1$

Quick proof for number nine:

Write b like $b = k \cdot \varphi(m) + b \% \varphi(m)$, for some integer k

then $a^b \% m = a^{k \cdot \varphi(m) + b \% \varphi(m)} \% m = (a^{\varphi(m)})^k \cdot a^{b \% \varphi(m)} \% m$

if Euler's theorem holds, that is $\gcd(a, m) = 1$ then

$(a^{\varphi(m)})^k \cdot a^{b \% \varphi(m)} \% m = 1 \cdot a^{b \% \varphi(m)} \% m = (a \% m)^{b \% \varphi(m)} \% m$.