Euler Totient or Phi Function

forthright48 on September 4, 2015

I have been meaning to write a post on Euler Phi for a while now, but I have been struggling with its proof. I heard it required the Chinese Remainder Theorem, so I have been pushing this until I covered CRT. But recently, I found that CRT is not required and it can be proved much more easily. In fact, the proof is so simple and elegant that after reading it I went ahead and played Minecraft for 5 hours to celebrate.

Problem

Given an integer N, how many numbers less than or equal N are there such that they are coprime to N? A number X is coprime to N if $gcd(X, N) = 1$.

For example, if $N = 10$, then there are 4 numbers, namely $1, 3, 7, 9$, which are coprime to 10.

This problem can be solved using Euler Phi Function, $phi()$. Here is the definition from Wiki:

> **In number theory, Euler's totient function (or Euler's phi function), denoted as $\phi(n)$, is an arithmetic function that counts the positive integers less than or equal to n that are relatively prime to n. – Wiki**

That's exactly what we need to find in order to solve the problem above. So, how does Euler Phi work?

Euler Phi Function

Before we go into its proof, let us first see the end result. Here is the formula using which we can find the value of the $phi()$ function. If we are finding Euler Phi of $N = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, then:

$$\phi(n) = n \times \frac{p_1 - 1}{p_1} \times \frac{p_2 - 1}{p_2} \ldots \times \frac{p_k - 1}{p_k}$$

If you want you can skip the proof and just use the formula above to solve problems. That's what I have been doing all these years. But I highly recommend that you read and try to understand the proof. It's simple and I am sure someday the proof will help you out in an unexpected way.

Proof of Euler Phi Function

Even though the proof is simple, it has many steps. We will go step by step, and slowly you will find that the proof is unfolding in front of your eyes.

Base Case – $\phi(1)$

First, the base case. Phi function counts the number of **positive** numbers less than N that are coprime to it. The keyword here is positive. Since the smallest positive number is 1, we will start with this.

$\phi(1) = 1$, since 1 itself is the only number which is coprime to it.

When n is a Prime – $\phi(p)$

Next, we will consider the case when $n = p$. Here p is any prime number. When n is prime, it is coprime to all numbers less than n. Therefore, $\phi(n) = \phi(p) = p – 1$.

When n is Power of Prime – $\phi(p^a)$

Next, we will consider n where n is a power of a single prime. In this case, how many numbers less than n are coprime to it? Instead of counting that, we will count the inverse. How many numbers are there which are **not** coprime?

Since, $n = p^a$, we can be sure that $gcd(p, n) \neq 1$. Since both n and p are divisible by p. Therefore, the following numbers which are divisible by p are not coprime to n, $p, 2p, 3p \ldots p^2, (p+1)p, (p+2)p \ldots (p^2)p, (p^2+1)p \ldots (p^{a-1})p$. There are exactly $\frac{p^a}{p} = p^{a-1}$ numbers which are divisible by p. So, there are $n – p^{a-1}$ numbers which are coprime to n.

Hence, $\phi(n) = \phi(p^a) = n – \frac{n}{p} = p^a – \frac{p^a}{p} = p^a(1 – \frac{1}{p}) = p^a \times (\frac{p-1}{p})$

It's starting to look like the equation above, right?

Assuming $\phi()$ is Multiplicative – $\phi(m \times n)$

This step is the most important step in the proof. This step claims that Euler Phi function is a multiplicative function. What does this mean? It means, if m and n are coprime, then $\phi(m \times n) = \phi(m) \times \phi(n)$. Functions that satisfy this condition are called Multiplicative Functions.

So how do we prove that Euler Phi is multiplicative and how does Euler Phi being multiplicative helps us?

We will prove multiplicity of Euler Phi Function in the next section. In this section, we will assume it is multiplicative and see how it helps us calculating Euler Phi.

Let the prime factorization of n be $p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$. Now, obviously p_i nad p_j are coprime to each other. Since ϕ function is multiplicative, we can simply rewrite the function as:

$\phi(n) = \phi(p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})$
$\phi(n) = \phi(p_1^{a_1}) \times \phi(p_2^{a_2}) \ldots \times \phi(p_k^{a_k})$.

We can already calculate $\phi(p^a) = p^a \times \frac{p-1}{p}$. So our equationg becomes:

$\phi(n) = \phi(p_1^{a_1}) \times \phi(p_2^{a_2}) \ldots \times \phi(p_k^{a_k})$
$\phi(n) = p_1^{a_1} \times \frac{p_1-1}{p_1} \times p_2^{a_2} \times \frac{p_2-1}{p_2} \ldots \times p_k^{a_k} \times \frac{p_k-1}{p_k}$
$\phi(n) = (p_1^{a_1} \times p_2^{a_2} \ldots \times p_k^{a_k}) \times \frac{p_1-1}{p_1} \times \frac{p_2-1}{p_2} \ldots \times \frac{p_k-1}{p_k}$

$$\therefore \phi(n) = n \times \frac{p_1 - 1}{p_1} \times \frac{p_2 - 1}{p_2} \ldots \times \frac{p_k - 1}{p_k}$$

This is what we have been trying to prove. This equation was derived by assuming that Euler Phi Function is multiplicative. So all we need to do now is prove Euler Phi Function is multiplicative and we are done.

Proof for Multiplicity of Euler Phi Function

We are trying to prove the following theorem:

> **Theorem 1: If m and n are coprime, then $\phi(m \times n) = \phi(m) \times \phi(n)$**

But in order to prove Theorem 1, we will need to prove few other theorems first.

Theorem Related to Arithmetic Progression

> **Theorem 2: In an arithmetic progression with a difference of m, if we take n terms and find their modulo by n, and if n and m are coprime, then we will get the numbers from 0 to $n-1$ in some order.**

Umm, looks like Theorem 2 is packed with too much information. Let me break it down.

Suppose you have an arithmetic progression (AP). Now, every arithmetic progression has two things. A starting element and a common difference. That is, arithmetic progressions are of the form $a + kb$ where a is the starting element, b is a common difference and k is any number.

So take any arithmetic progression that has a common difference of m. Then take n consecutive terms of that progression. So which terms will they be?

$a + 0m, a + 1m, a + 2m, a + 3m \ldots a + (n-1)m$ There are exactly n terms in this list.

Next, find their modulus by n. That is, find the remainder of each term after dividing by n.

Now, Theorem 2 claims that, if m and n are coprime, then the list will contain a permutation of 0 to $n-1$.

For example, let us try with $a = 1$, $m = 7$ and $n = 3$. So the 3 terms in the list will be $(1, 8, 15)$. Now, if find modulus of each element, we get $(1, 2, 0)$.

I hope that now it's clear what the Theorem claims. Now we will look into the proof.

Proof of Theorem 2

What we need to prove is that the list after modulo operation has a permutation of numbers from 0 to $n-1$. That means, all the numbers from 0 to $n-1$ occurs in the list exactly once. There are three steps to this proof. Also, remember that m and n are coprime.

1. **There are exactly n elements in the list.**
   Well, since we took n terms from the AP, this is obvious.
2. **Each element of the list has a value between 0 to $n-1$**
   We performed modulo operations on each element by n. So this is also obvious.
3. **No remainder has the same value as another.**
   Since there are n values, and each value is between 0 to $n-1$, if we can prove that each element is unique in the list, then our work is done.

Suppose there are two numbers which have the same remainder. That means $a + pm$ has same remainder as $a + qm$, where p and q are two integer numbers such that $0 \leq p < q \leq n – 1$.

Therefore, $(a + qm) – (a + pm) \equiv 0 \mod n$
$(a + qm - a – pm) \equiv 0 \mod n$
$m(q – p) \equiv 0 \mod n$

That means, n divides $m(q-p)$. But this is impossible. n and m are coprime and $q - p$ is smaller than n. So it is not possible for two numbers to have the same remainder.

Theorem Related to Remainder

> **Theorem 3: If a number x is coprime to y, then $(x \% y)$ will also be coprime to y.**

The proof for this theorem is simple. Suppose x and y are coprime. Now, we can rewrite x as $x = ky + r$, where k is the quotient and r is the remainder.

Theorem 3 claims that y and r are coprime. What happens if this claim is false? Suppose they are **not** coprime. That means there is a number $d > 1$ which divides both y and r. But then, d also divides $ky + r = a$. So $d > 1$ divides r, y and x, which is impossible cause y and x are coprime. There is no number greater than 1 that can divide both of them. Hence, there is a contradiction. Hence, the theorem is proved.

Proof for Multiplicity of Euler Phi Function Continued

We are now ready to tackle proving Theorem 1.

Suppose you have two numbers m and n, and they are coprime. We want to show that $\phi(m \times n) = \phi(m) \times \phi(n)$.

What does $\phi(m \times n)$ give us? It gives us the count of numbers which are coprime to mn. If a number x is coprime to mn, then it is also coprime to m and n separately. So basically, we need to count the number of positive numbers less than or equal to mn which are coprime to both m and n.

Now, let us build a table of with n rows and m columns. Therefore, the table will look like the following:

1	2	3	…	m
1+m	2+m	3+m	…	2m
1+2m	2+2m	3+2m	…	3m
…	…	…	…	…
1 + (n-1)m	2 + (n-1)m	3 + (n-1)m	…	mn

Now, notice that each column is an arithmetic progression with n terms and has a common difference of m. Also, m and n are coprime. This is exactly the same situation as Theorem 2.

Now, how many numbers in each column are coprime to n? In order to figure this result out, we first need to consider what happens if we modulo all table values with n. Using theorem 2, we know that each column will then contain a permutation of numbers from 0 to $n-1$. Using theorem 3, we know what if the remainder of a number is coprime to n then the number itself will also be coprime. So, how many numbers between 0 to $n-1$ is coprime to n? We can consider 0 to be same as n (cause this is modular arithmetic), so it boils down to, how many numbers between 1 to n is coprime to n? Euler Phi Function calculates this values.

So, there are exactly $\phi(n)$ numbers which are coprime to n in each column.

We need to find numbers that coprime to **both** n and m. So, we cannot take $\phi(n)$ elements from every column, cause those elements may not be coprime to m. How do we decide which columns we should be taking?

Notice that, if we find the modulus of elements of the table by m, then each row has remainder between 0 to $m-1$ occuring exactly once. If we consider 0 to be m, then each row has values between 1 to m. That is the table becomes something like this:

1	2	3	…	m
1	2	3	…	m
1	2	3	…	m
…	…	…	…	…
1	2	3	…	m

So, how many columns are there which are coprime to m? There are $\phi(m)$ columns which are coprime to m.

Now we just need to combine the two results from above. There are exactly $\phi(m)$ columns which are coprime to m and in each column there are $\phi(n)$ values which are coprime to n. Therefore, there are $\phi(m) \times \phi(n)$ elements which are coprime to both m and n.

$$\therefore \phi(m) \times \phi(n) = \phi(m \times n)$$

Code

Since we have to factorize n in order to calculate $\phi(n)$, we can modify our $factorize()$ function from post "Prime Factorization of Integer Number" to handle Euler Phi.

```
1  int eulerPhi ( int n ) {
2      int res = n;
3      int sqrtn = sqrt ( n );
4      for ( int i = 0; i < prime.size() && prime[i] <= sqrtn; i++ ) {
5          if ( n % prime[i] == 0 ) {
6              while ( n % prime[i] == 0 ) {
7                  n /= prime[i];
8              }
9              sqrtn = sqrt ( n );
10             res /= prime[i];
11             res *= prime[i] - 1;
12         }
13     }
14     if ( n != 1 ) {
15         res /= n;
16         res *= n - 1;
17     }
18     return res;
19 }
```

I highlighted the lines that are different from $factorize()$ function. Notice that in line 10 divided res before multiplying in line 11. This is an optimization that lowers the risk of overflowing.

Properties, Extensions, and Related Theorems

1. Euler Phi Extension Theorem: Number of elements e, such that $gcd(e, n) = d$ is equal to $\phi(\frac{n}{d})$.
2. Euler Phi Divisor Sum Theorem: $\sum_{d|n} \phi(d) = n$.
3. For $n > 2$, $\phi(n)$ is always even. For proof, read Sum of Co-prime Numbers of an Integer.
4. Sum of integers that are coprime to n equals to $\frac{\phi(n) \times n}{2}$. For proof, read Sum of Co-prime Numbers of an Integer.

Conclusion

That was a long post with lots of theorems and equations, but hopefully, they were easy to understand. Even though Theorem 2 and 3 were used as lemmas to prove Theorem 1, they both are important by themselves.

Leave a comment if you face any difficulty in understanding the post.

Reference

1. Wiki - Euler Totient Function

Related Problems

1. SPOJ ETF - Euler Totient Function
2. SPOJ ETFS - Euler Totient Function Sieve
3. SPOJ ETFD - Euler Totient Function Depth
4. UVA 10299 - Relatives

Category: CPPS, Number Theory **Tag:** code, problem-list, proof, theorem

Previous:
Bit Manipulation

Next:
Segmented Sieve of Eratosthenes