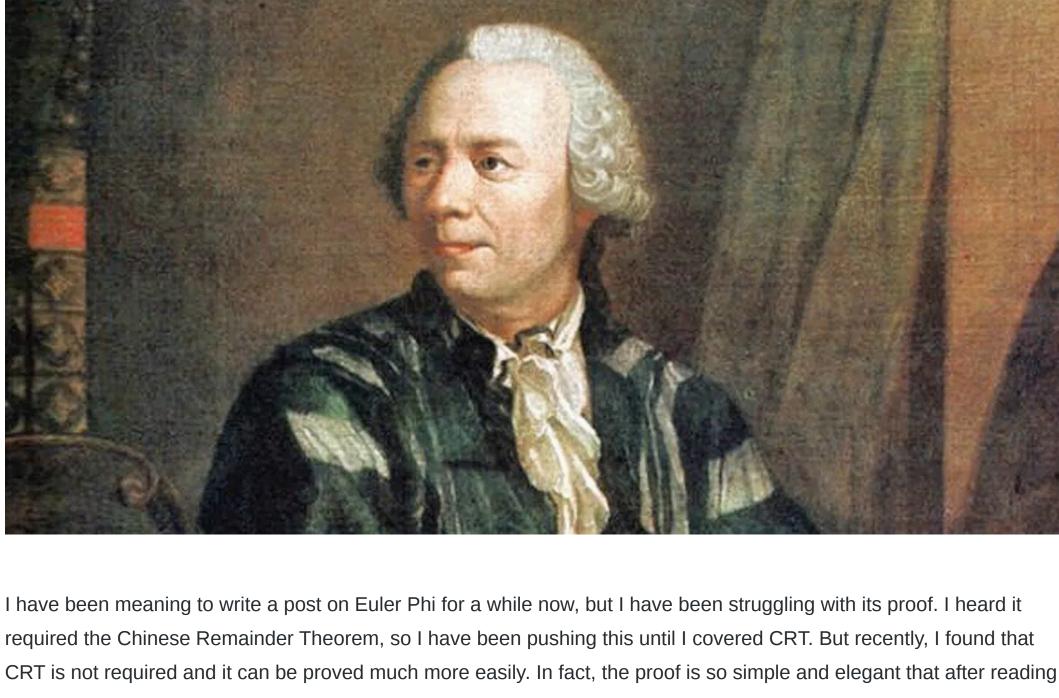
Euler Totient or Phi Function Is forthright 48 on September 4, 2015



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.

Euler Phi Function

phi() function. If we are finding Euler Phi of $N=p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$, then:

Proof of Euler Phi Function

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.

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

Next, we will consider the case when n = p. Here p is any prime number. When n is prime, it is coprime to all

When n is a Prime – $\phi(p)$

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

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,

unfolding in front of your eyes.

Base Case – $\phi(1)$

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

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 $p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$. Now, obviously p_i nad p_j are coprime to each other. Since ϕ

Proof for Multiplicity of Euler Phi Function

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.

We are trying to prove the following theorem: Theorem 1: If m and n are coprime, then $\phi(m imes n) = \phi(m) imes \phi(n)$ But in order to prove Theorem 1, we will need to prove few other theorems first. **Theorem Related to Arithmetic Progression** 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.

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-1We performed modulo operations on each element by n. So this is also obvious.

Suppose there are two numbers which have the same remainder. That means a+pm has same remainder as

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,

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

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.

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.

them. Hence, there is a contradiction. Hence, the theorem is proved.

2

2+m

2 + (n-1)m

We are now ready to tackle proving Theorem 1.

1

1+m

1 + (n-1)m

which are coprime to both m and n.

Factorization of Integer Number" to handle Euler Phi.

int eulerPhi (int n) {

int sqrtn = sqrt (n);

2. Euler Phi Divisor Sum Theorem: $\sum_{d|n} \phi(d) = n$.

int res = n;

Code

2

3

4

Integer.

Conclusion

for (int i = 0; i < prime.size() && prime[i] <= sqrtn; i++) {</pre> 5 if (n % prime[i] == 0) { 6 while (n % prime[i] == 0) { 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; res *= n - 1; 16 17 18 return res; 19

Your comment..

1. SPOJ ETF - Euler Totient Function

4. UVA 10299 - Relatives

Previous:

Bit Manipulation

2. SPOJ ETFS - Euler Totient Function Sieve

3. SPOJ ETFD - Euler Totient Function Depth

Add Anycomment to your site

Sort by newest 17

Next:

Segmented Sieve of Eratosthenes

it I went ahead and played Minecraft for 5 hours to celebrate. **Problem** 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? 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 $\phi(n) = n imes rac{p_1-1}{p_1} imes rac{p_2-1}{p_2} \ldots imes rac{p_k-1}{p_k}$ 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.

Hence, $\phi(n)=\phi(p^a)=n-rac{n}{n}=p^a-rac{p^a}{n}=p^a(1-rac{1}{n})=p^a imes(rac{p-1}{n})$ It's starting to look like the equation above, right?

this condition are called Multiplicative Functions.

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

 $\phi(n) = \phi(p_1^{a_1}) imes \phi(p_2^{a_2}) \ldots imes \phi(p_{\iota}^{a_k}).$

We can already calculate $\phi(p^a)=p^a imes rac{p-1}{p}$. So our equationg becomes: $\phi(n) = \phi(p_1^{a_1}) imes \phi(p_2^{a_2}) \ldots imes \phi(p_k^{a_k})$ $\phi(n)=p_1^{a_1} imesrac{p_1-1}{p_1} imes p_2^{a_2} imesrac{p_2-1}{p_2}\ldots imes p_k^{a_k} imesrac{p_k-1}{p_k}$ $\phi(n)=(p_1^{a_1} imes p_2^{a_2}\ldots imes p_k^{a_k}) imes rac{p_1-1}{p_1} imes rac{p_2-1}{p_2}\ldots imes rac{p_k-1}{p_k}$

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

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.

I hope that now it's clear what the Theorem claims. Now we will look into the proof. **Proof of Theorem 2**

modulus of each element, we get (1, 2, 0).

remember that m and n are coprime.

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.

a+qm, where p and q are two integer numbers such that $0 \leq p < q \leq n-1$.

Therefore, $(a+qm)-(a+pm)\equiv 0\mod n$

 $(a+qm-a-pm)\equiv 0\mod n$

 $m(q-p) \equiv 0 \mod n$

the quotient and r is the remainder.

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

2 3 m 2 3 m 1

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.

III Post Views: 1,004 **Category:** CPPS, Number Theory **Tag:** code, problem-list, proof, theorem

Now, notice that each column is an arithmetic progression with n terms and has a common difference of m. Also, mand 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 nthen 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 nis 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-1occurring 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 1

2 3 m 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 mand in each column there are $\phi(n)$ values which are coprime to n. Therefore, there are $\phi(n) \times \phi(n)$ elements

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

Since we have to factorize n in order to calculate $\phi(n)$, we can modify our factorize() function from post "Prime"

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**

 $p,2p,3p\dots p^2,(p+1)p,(p+2)p\dots (p^2)p,(p^2+1)p\dots (p^{a-1})p$. There are exactly $rac{p^a}{p}=p^{a-1}$ numbers which are divisible by p. So, there are $n-p^{a-1}$ numbers which are coprime to n. 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 So how do we prove that Euler Phi is multiplicative and how does Euler Phi being multiplicative helps us? function is multiplicative, we can simply rewrite the function as:

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? $a+0m, a+1m, a+2m, a+3m \dots a+(n-1)m$ 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.

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

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

Proof for Multiplicity of Euler Phi Function Continued

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

3

3+m

3 + (n-1)m

m

2m

3m

mn

2+2m 3+2m 1+2m

1

Properties, Extensions, and Related Theorems 1. Euler Phi Extension Theorem: Number of elements e, such that gcd(e,n)=d is equal to $\phi(\frac{n}{d})$.

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

That was a long post with lots of theorems and equations, but hopefully, they were easy to understand. Even though

3. For n>2, $\phi(n)$ is always even. For proof, read Sum of Co-prime Numbers of an Integer.

B $I \cup 99 \equiv \otimes T_x$ Login with

Comments: 5

© 2015-2019 Mohammad Samiul Islam

LCMSUM – LCM Sum

Archives Categories Recent Comments May 2019 (1) **CPPS** (45) My Shopee Interview – Shadman Protik on My Interview Experience with Shopee / Combinatorics (4) April 2019 (1) Garena / Sea Group Data Structure (1) March 2019 (1) Istiad Hossain Akib on SPOJ LCMSUM – Number Theory (36) LCM Sum December 2018 (2) Rifat Chowdhury on MyStory#02 -Meta (1) November 2018 (4) Deciding Where to Study CS Misc (4) September 2018 (2) Salman Farsi on Leading Digits of February 2018 (1) **Factorial** January 2018 (1) Learning Notes on Multiplicative Functions, Dirichlet Convolution, Mobius November 2017 (2) Inversion, etc – RobeZH's Blog on SPOJ September 2015 (7) August 2015 (13) July 2015 (15)