Thursday, September 17, 2015

Euler's Theorem and Fermat's Little Theorem

We will be looking into two theorems at the same time today, Fermat's Little Theorem and Euler's Theorem. Euler's Theorem is just a generalized version of Fermat's Little Theorem, so they are quite similar to each other. We will focus on Euler's Theorem and its proof. Later we will use Euler's Theorem to prove Fermat's Little Theorem.

Euler's Theorem

> **Theorem** - Euler's Theorem states that, if a and n are coprime, then $a^{\phi(n)} \equiv 1 (\text{mod n})$ - Wikipedia

Here $\phi(n)$ is Euler Phi Function. Read more about Phi Function on this post - Euler Totient or Phi Function.

Proof

Let us consider a set $A = \{b_1, b_2, b_3 \ldots, b_{\phi(n)}\} \ (\text{mod n})$, where b_i is coprime to n and distinct. Since there are $\phi(n)$ elements which are coprime to n, A contains $\phi(n)$ integers.

Now, consider the set $B = \{ab_1, ab_2, ab_3 \ldots ab_{\phi(n)}\} \ (\text{mod n})$. That is, B is simply set A where we multiplied a with each element. Let a be coprime to n.

> **Lemma** - Set A and set B contains the same integers.

We can prove the above lemma in three steps.

Follow by Email

Email address... Submit

Labels

Analysis Arithmetic Function Backtrack Big Int Binary Bitwise Combinatorics Complexity Contest CPPS D&C Divisors Factorial Factorization GCD Graph Language LCM Logarithm Math Modular Arithmetic Number Theory Optimization Primality Test Prime Proof Repeated Squaring Sequence Sieve SPOJ Theorem Tree UVa

Blog Archive

- ► 2018 (2)
- ► 2017 (2)
- ▼ 2015 (35)
  - ▼ Sep (7)
    - Modular Inverse from 1 to N
    - Euler Phi Extension and Divisor Sum Theorem
    - Modular Multiplicative Inverse

1. **A and B has the same number of elements**
   Since B is simply every element of A multiplied with a, it contains the same number of elements as A. This is obvious.
2. **Every integer in B is coprime to n**
   An integer in B is of form $a \times b_i$. We know that both b_i and a are coprime to n, so ab_i is also coprime to n.
3. **B contains distinct integers only**
   Suppose B does not contain distinct integers, then it would mean that there is such a b_i and b_j such that:

   $$ab_i \equiv ab_j \pmod{n}$$
   $$b_i \equiv b_j \pmod{n}$$

   But this is not possible since all elements of A are distinct, that is, b_i is never equal to b_j. Hence, B contains distinct elements.

With these three steps, we claim that, since B has the same number of elements as A which are distinct and coprime to n, it has same elements as A.

Now, we can easily prove Euler's Theorem.

$$ab_1 \times ab_2 \times ab_3 \ldots \times ab_{\phi(n)} \equiv b_1 \times b_2 \times b_3 \ldots \times b_{\phi(n)} \pmod{n}$$
$$a^{\phi(n)} \times b_1 \times b_2 \times b_3 \ldots \times b_{\phi(n)} \equiv b_1 \times b_2 \times b_3 \ldots \times b_{\phi(n)} \pmod{n}$$

$$\therefore a^{\phi(n)} \equiv 1 \pmod{n}$$

Fermat's Little Theorem

Fermat's Little Theorem is just a special case of Euler's Theorem.

> **Theorem** - Fermat's Little Theorem states that, if a and p are coprime and p is a prime, then $a^{p-1} \equiv 1 \pmod{p}$ - Wikipedia

As you can see, Fermat's Little Theorem is just a special case of Euler's Theorem. In Euler's Theorem, we worked with any pair of value for a and n where they are coprime, here n just needs to be prime.

We can use Euler's Theorem to prove Fermat's Little Theorem.

Let a and p be coprime and p be prime, then using Euler's Theorem we can say that:

Typesetting math: 100%

$$\phi(n) \ldots 1 \pmod{p}$$ (But we know that for any prime p, $\phi(p) = p - 1$)

Follow me on Twitter

$a^{p-1} \equiv 1 \pmod p$

Conclusion

Both theorems have various applications. Finding Modular Inverse is a popular application of Euler's Theorem. It can also be used to reduce the cost of modular exponentiation. Fermat's Little Theorem is used in Fermat's Primality Test.

There are more applications but I think it's better to learn them as we go. Hopefully, I will be able to cover separate posts for each of the applications.

Reference

1. Wiki - Euler's Theorem
2. forthright48 - Euler Totient or Phi Function
3. Wiki - Fermat's Little Theorem

Posted by Mohammad Samiul Islam

Labels: Modular Arithmetic, Number Theory, Proof, Theorem

No comments:

Post a Comment

Leave comments for Queries, Bugs and Hugs.

Enter your comment...

Comment as: Google Accoun

Publish Preview

Typesetting math: 100%

Tweets by @forthright48

MohammadSamiul Islam
@forthright48

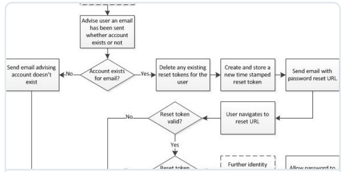
I don't know why I have been using default bash shell all these years :| ohmyz.sh Glad I found @ohmyzsh

oh my zsh
Oh-My-Zsh is a d…
ohmyz.sh

Jul 19, 2018

MohammadSamiul Islam
@forthright48

Resetting password is such a headache! Maybe I should dump basic auth and just move to third party auth service.troyhunt.com/everything-you…



Embed View on Twitter

Tweets by @forthright48

Followers

Subscribe to: Post Comments (Atom)

Followers (16)

Follow

Total Pageviews

71093

Popular Posts

SPOJ LCMSUM - LCM Sum
Problem Problem Link - SPOJ LCMSUM Given n, calculate the sum $LCM(1,n) + LCM(2,n) + \ldots + LCM(n,n)$, where $LCM(i,n)$ denotes the ...

Euclidean Algorithm - Greatest Common Divisor
Problem Given two number A and B, find the greatest number that divides both A and B. What we are trying to find here is the Greatest Comm...

Extended Euclidean Algorithm
Extended Euclidean Algorithm is an extension of Euclidean Algorithm which finds two things for integer a and b: It finds the value of...

Chinese Remainder Theorem Part 1 - Coprime Moduli
Second part of the series can be found on: Chinese Remainder Theorem Part 2 - Non Coprime Moduli Wow. It has been two years since I pub...

Prufer Code: Linear Representation of a Labeled Tree
I guess this is going to be my first post (apart from the contest analysis') which is not about Number Theory! It's not about graph ...

Segmented Sieve of Eratosthenes
Problem Given two integers A and B, find number of primes inside the range of A and B inclusive. Here, $1 \leq A \leq B \leq 10^{...

Sieve of Eratosthenes - Generating Primes
Problem Given an integer N, generate all primes less than or equal to N. Sieve of Eratosthenes - Explanation Sieve of Eratosthenes ...

Number of Digits of Factorial
Problem Given an integer N, find number of digits in $N!$. For example, for $N = 3$, number of digits in $N! = 3! = 3\times 2\times 1...

Typesetting math: 100%

Euler Totient or Phi Function

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 Chinese Rem...

Chinese Remainder Theorem Part 2 - Non Coprime Moduli

As promised on the last post, today we are going to discuss the "Strong Form" of Chinese Remainder Theorem, i.e, what do we do whe...