Number Theory\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Modular Arithmetic\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Euler’s Totient Function

|  |
| --- |
| The totient function phi(n), also called Euler's totient function, is defined as the number of [positive integers](http://mathworld.wolfram.com/PositiveInteger.html) <=n that are [relatively prime](http://mathworld.wolfram.com/RelativelyPrime.html) to (i.e., do not contain any factor in common with) n, where 1 is counted as being [relatively prime](http://mathworld.wolfram.com/RelativelyPrime.html) to all numbers. Since a number less than or equal to and [relatively prime](http://mathworld.wolfram.com/RelativelyPrime.html) to a given number is called a [totative](http://mathworld.wolfram.com/Totative.html), the totient function phi(n) can be simply defined as the number of [totatives](http://mathworld.wolfram.com/Totative.html) of n. For example, there are eight [totatives](http://mathworld.wolfram.com/Totative.html) of 24 (1, 5, 7, 11, 13, 17, 19, and 23), so phi(24)=8. |

Φ(n) = n(1-1/P1) (1-1/P2) (1-1/P3)…

    Where P1, P2 … are the unique prime factors of **n** (don’t count the duplicates, could include n if n is prime).

|  |
| --- |
| Examples:  Φ(24) = 24(1-1/2)(1-1/3) = 8  Φ(13) = 13(1-1/13) = 12 |

|  |
| --- |
| Review coprime:  In **number** theory, two integers a and b are said to be **relatively prime**, mutually prime, or **coprime** (also spelled **co-prime**) if the only positive integer that divides both of them is 1. That is, the only common positive factor of the two **numbers** is 1 |

|  |
| --- |
| Review prime factor:  In [number theory](https://en.wikipedia.org/wiki/Number_theory), the **prime factors** of a positive [integer](https://en.wikipedia.org/wiki/Integer) are the [prime numbers](https://en.wikipedia.org/wiki/Prime_number) that divide that integer exactly. 1 is not a prime number |

Euler’s Totient Theorem

    Any positive integer **a** **coprime to n** satisfies this theorem.

https://lh6.googleusercontent.com/i19F46YEuhS8ECirejwJav_KB5y5w1cmnfwuk4n-kq4LSz7CYmDaNcAGKxmmhS0wUt9fjDvpbBV_hdLRcnf6CqdedDJfbCxFUYx7yWtXNbLFuKnYF4j81X8ES-BwhivhD3BRcbvM

Chinese Remainder Theorem

    Given an integer **n** which satisfies multiple modulo congruencies

https://lh6.googleusercontent.com/K2F7xkwjWfKe2mwLUd0BToxKaZCFy9AzMrAwF_yntHd32-1PHDAjlZEwncVZMImMeUMTKzMnKfb_NAEyk-uFB8tNbbPTVS52Uf1_vZNXOfSZDShImZRWgZBPE0Lmu606OrRxpW27

**n** can be determined through the following formula

https://lh4.googleusercontent.com/UtCygSGkr7riwtMlVWz-032sdyviDyJTIGAVO0XvhYY5Dx_KAZnmkDm3O6HQbiHe-4rkxT6QIkzMethfNCYlSbOrfpFIQN-jpc-9gHs1wEZD4mgekBhwAEz3UdFDnr387_MA6T58

    Where **b** is defined as

https://lh3.googleusercontent.com/esAZG-g82tUKeUsWQQQC5L48qiYsIPSU8BFEx2jzgB5O7KKjIIuPsNkYvdnT8nttXST3WX-4VIOLF_H0f6GMeuHbXhF3A3pMVcXlj3h_ViWtbbEZW-GH0b_4hQ_jHxx4CcXJqXbX

    And **M** is

https://lh5.googleusercontent.com/IJaGG2QRnzyVk_7fNZvoRRPFSWxhrhMb2iPlNzy92r6Jjo4staQCnP1uwXDio1z3oePTIoEyRwjOFeuH61t8Tguo1ao3EiGoRm1XWnqwQg0Rs6n7NTCeL68wr0pr1OunFJMF7ou-

**An example problem using Chinese Reminder therom and Euler’s totient:**

|  |
| --- |
| Find redminder of 2345 when divided by 400.  M = 400 = m1  m2  = 16 x 25  a1 = 2345 Mod(16) = 0  a2 = 2345 Mod(25), to find this we can use euler’s totient.  Φ (25) = 25 ( 1 – 1/5) = 20, so 220 = 1 Mod(25), thus 2345 Mod(25) = 25 Mod(25) = 7  b1: 25b1 = 1 Mod(16), so b1 = 9 (in fact we don’t need to find this because a1 is 0)  b2: 16b2 = 1Mod(25), b2 = 11  result = (a2 x b2 x 16) Mod(400) = (7 x 11 x 16) Mod(400) = 32 Mod(400) |

|  |
| --- |
| The way to find out 16b2 = 1Mod(25)  Add 25 to the right: 16b2 = 26Mod(25)  Divided by 2: 8b2 = 13Mod(25)  Add 25 again: 8b2 = 38Mod(25)  Divide by 2: 4b2 = 19Mod(25)  …………… b2 = 11Mod(25) |