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) |

Bijection:

|  |
| --- |
| Review Injection:  Injection (1-1): Let *f* : *A**B* . If for each *y**f* (*A*) there exists a unique  (pre-image) *x**A* such that *f* *x**y* , the function *f* is called an injection (or  simply one-to-one1). |

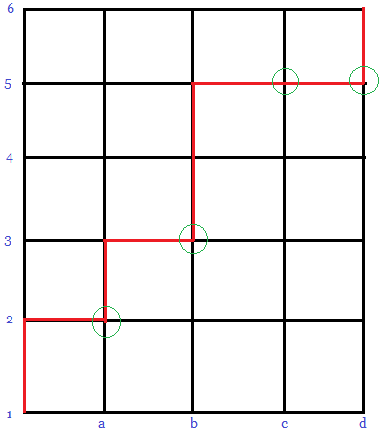
|  |
| --- |
| Review Surjection:  Surjection (onto): Let *f* : *A**B* . If the set of images *f* (*A*) is equal to the  codomain *B* (i.e. *f* *A**B* ) the function *f* is called a surjection (or simply  onto) and we say “ *f* is from *A* onto B .” In other words, for each *y**B* there  exists an *x**A* (called a pre-image of *y* ) such that *f* (*x*) *y* |

|  |
| --- |
| Review Bijection  (1-1 correspondence): If *f* : *A**B* is both an injection and  surjection, then *f* is called a bijection (or one-to-one correspondence).    Bijection is actually both Surjection and Injection. |

|  |
| --- |
| Example 1:  **2006 AIME II Problem 4**  **Problem**  Let $(a_1,a_2,a_3,\ldots,a_{12})$be a permutation of $(1,2,3,\ldots,12)$for which  $a_1>a_2>a_3>a_4>a_5>a_6 \mathrm{\  and \ } a_6<a_7<a_8<a_9<a_{10}<a_{11}<a_{12}.$  An example of such a permutation is $(6,5,4,3,2,1,7,8,9,10,11,12).$Find the number of such permutations.  Example 2: 2001 AIME I Problem 6Problem A fair die is rolled four times. The [probability](https://www.artofproblemsolving.com/wiki/index.php?title=Probability) that each of the final three rolls is at least as large as the roll preceding it may be expressed in the form $\frac{m}{n}$where $m$ and $n$ are [relatively prime](https://www.artofproblemsolving.com/wiki/index.php?title=Relatively_prime) [positive](https://www.artofproblemsolving.com/wiki/index.php?title=Positive) [integers](https://www.artofproblemsolving.com/wiki/index.php?title=Integer). Find $m + n$. |

Block Walking:

There are m steps and each step could have one of n values, each step must be at least as big as previous step.

[](https://wiki-images.artofproblemsolving.com/2/26/AIME01IN6.png)

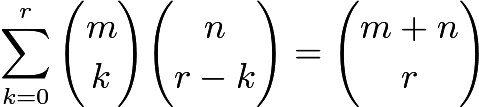
Here we have 4 steps and 6 values. The number of paths are:

(steps + values – 1) choose (steps or [values – 1])

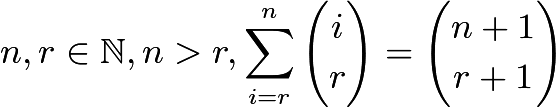
|  |
| --- |
|  |

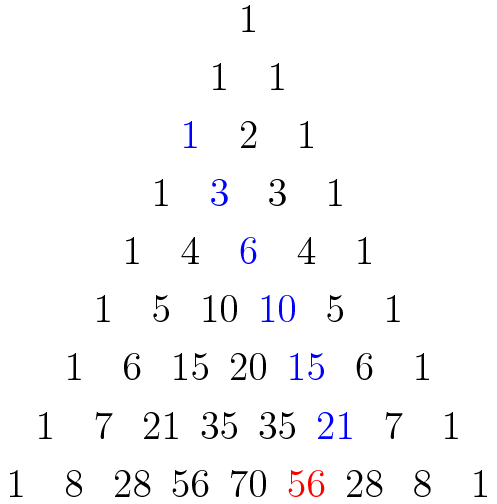
Combinatorial identity (see problem from block walking)

Vandermonde's Identity:

Vandermonde's Identity states that , which can be proven combinatorially by noting that any combination of $r$objects from a group of $m+n$objects must have some $0\le k\le r$objects from group $m$and the remaining from group $n$

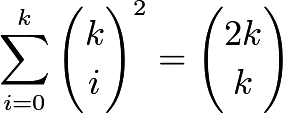
Hockey-Stick Identity:

For .

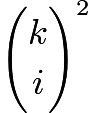
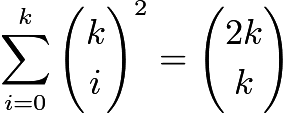


This identity is known as the *hockey-stick* identity because, on Pascal's triangle, when the addends represented in the summation and the sum itself are highlighted, a hockey-stick shape is revealed.

Another Identity:



### Hat Proof

We have $2k$different hats. We split them into two groups, each with k hats: then we choose $i$hats from the first group and $k-i$hats from the second group. This may be done in ways. Evidently, to generate all possible choices of $k$hats from the $2k$hats, we must choose $i=0,1,\cdots,k$hats from the first $k$and the remaining $k-i$hats from the second $k$; the sum over all such $i$is the number of ways of choosing $k$hats from $2k$. Therefore , as desired.

### Proof 2

This is a special case of Vandermonde's identity, in which we set $m=n$and $r=m$.

|  |
| --- |
| Examples:  (1)The polynomial $1-x+x^2-x^3+\cdots+x^{16}-x^{17}$may be written in the form $a_0+a_1y+a_2y^2+\cdots +a_{16}y^{16}+a_{17}y^{17}$, where $y=x+1$and thet $a_i$'s are constants. Find the value of $a_2$. (1986 AIME P2)  (2)Given that  $\frac 1{2!17!}+\frac 1{3!16!}+\frac 1{4!15!}+\frac 1{5!14!}+\frac 1{6!13!}+\frac 1{7!12!}+\frac 1{8!11!}+\frac 1{9!10!}=\frac N{1!18!}$  find the greatest integer that is less than $\frac N{100}$.(2000 AIME ii P7)  (3) Consider all 1000-element subsets of the set {1, 2, 3, ... , 2015}. From each such subset choose the least element. The arithmetic mean of all of these least elements is $\frac{p}{q}$, where $p$and $q$are relatively prime positive integers. Find $p + q$.(2015 AIME I p12) |