Modular Exponentiation (Power in Modular Arithmetic)

Given three numbers x, y and p, compute (x^y) % p.

Examples

```
Input:  x = 2, y = 3, p = 5
Output: 3
Explanation: 2^3 % 5 = 8 % 5 = 3.

Input:  x = 2, y = 5, p = 13
Output: 6
Explanation: 2^5 % 13 = 32 % 13 = 6.
```

We strongly recommend you to minimize your browser and try this yourself first.

We have discussed recursive and iterative solutions for power.

Below is discussed iterative solution.

```
/* Iterative Function to calculate (x^y) in O(logy) */
int power(int x, unsigned int y)
{
    int res = 1;     // Initialize result

    while (y > 0)
    {
        // If y is odd, multiply x with result
        if (y & 1)
            res = res*x;

        // n must be even now
        y = y>>1; // y = y/2
        x = x*x;  // Change x to x^2
    }
    return res;
}
```

The problem with above solutions is, overflow may occur for large value of n or x. Therefore, power is generally evaluated under modulo of a large number.

Below is the fundamental modular property that is used for efficiently computing power under modular arithmetic.

```
(a mod p) (b mod p) =  (ab) mod p

or equivalently

( (a mod p) (b mod p) ) mod p  =  (ab) mod p

For example a = 50,  b = 100, p = 13
50  mod 13  = 11
100 mod 13  = 9

11*9 = 1500 mod 13
or
11*9 mod 13 = 1500 mod 13
```

Below is C implementation based on above property.

```
// Iterative C program to compute modular power
#include <stdio.h>

/* Iterative Function to calculate (x^n)%p in O(logy) */
int power(int x, unsigned int y, int p)
{
    int res = 1;     // Initialize result

    x = x % p;  // Update x if it is more than or
                // equal to p

    while (y > 0)
    {
        // If y is odd, multiply x with result
        if (y & 1)
            res = (res*x) % p;

        // y must be even now
        y = y>>1; // y = y/2
        x = (x*x) % p;
    }
    return res;
}

// Driver program to test above functions
int main()
{
    int x = 2;
    int y = 5;
    int p = 13;
    printf("Power is %u", power(x, y, p));
    return 0;
}
```

Output:

```
Power is 6
```


Company Wise Coding Practice Topic Wise Coding Practice

14 Comments Category: Mathematical

Related Posts:

- Find Last Digit Of a^b for Large Numbers
- Reverse and Add Function
- Number of elements with odd factors in given range
- Stein's Algorithm for finding GCD
- GCD of two numbers when one of them can be very large
- Sub-string Divisibility by 11 Queries
- Sub-string Divisibility by 3 Queries
- Converting Decimal Number lying between 1 to 3999 to Roman Numerals

Previous post in category Next post in category

(Login to Rate and Mark)

2.6 Average Difficulty : 2.6/5.0 Based on 10 vote(s)

Add to TODO List
Mark as DONE

Writing code in comment? Please use code.geeksforgeeks.org, generate link and share the link here.

14 Comments GeeksforGeeks Login

Recommend 2 Share Sort by Newest

Join the discussion…

Akhil Pokle - a month ago
can this help to find powers like 2^999 if yes how?
Reply · Share ›

Tony Stark → Akhil Pokle - 22 days ago
This method will give the correct answer of 2^999 but c/c++ does not have any data type which can store such large value which will result in overflow. This method is used for computing calculation of (a^b)%c eg (2^999)%1000000007 which could be stored in long long. If you perform a naive method on (a^b)%c, loop will execute b times and b times multiplication will perform which time complex will be O(b). But above method give the result in O(log(b)) time.
Reply · Share ›

aashi - 2 months ago
its giving 1 for 0,0,1 whereas the answer should be 0
Reply · Share ›

kapil kumar → aashi - 8 days ago
That's because in that case we never go into while loop and default value of res is returned. we can use a if condition outside while loop if(x==0) return 0;
else res=1;
BTW 0^0 is not defined.
Reply · Share ›

Sridhar Addagatla - 3 months ago
simple recursive solution in c can be found here : http://ideone.com/vPt3OB
Reply · Share ›

gauri shankar gaur - 3 months ago
In the above mentioned example a=50 and b=100.Shouldn't the result be
11*9 = 5000 mod 13??
Reply · Share ›

SHALU - 4 months ago
This algorithm is not right, as it gives wrong output for bigger inputs like x=71045970 , y=41535487 and p=64735492 , the expected ans is 20805472 while its coming -5613284. I tried to solve with this algorithm n submit the solutn on different site but its showing wrong ans.
Reply · Share ›

AJAY RAJAWAT → SHALU - 3 months ago
Make your ints -> long long.
Reply · Share ›

Popular Posts

- Top 10 Algorithms and Data Structures for Competitive Programming
- Top 10 algorithms in Interview Questions
- How to begin with Competitive Programming?
- Reflection in Java
- Memory Layout of C Programs
- Push Relabel Algorithm
- Heavy Light Decomposition
- Sorted Linked List to Balanced BST
- Generics in Java
- Aho-Corasick Algorithm for Pattern Searching
- Binary Search , QuickSort , MergeSort , HeapSort

- Common Interview Puzzles
- Interview Experiences
- Advanced Data Structures
- Design Patterns
- Dynamic Programming
- Greedy Algorithms
- Backtracking
- Pattern Searching
- Divide & Conquer
- Geometric Algorithms
- Searching
- Sorting
- Hashing
- Analysis of Algorithms
- Mathematical Algorithms
- Randomized Algorithms
- Recursion

Tags

Accolite Adobe Advance Data Structures Advanced Data Structures Amazon array Bit Magic C++ CN c puzzle D-E-Shaw Directi Divide and Conquer Dynamic Programming Flipkart GATE GATE-CS-DS-&-Algo GATE-CS-Older GFacts Goldman Sachs Google Graph Greedy Algorithm Hashing Interview Experience Java MakeMyTrip MAQ Software MathematicalAlgo Matrix Microsoft Morgan Stanley Operating systems Oracle Pattern Searching puzzle Python Recursion Samsung SAP Labs SnapDeal stack Stack-Queue STL Zoho

Subscribe and Never Miss an Article
Email Address Subscribe

Like us on Facebook

Follow us on Twitter

Recent Comments

Vibhor Vaish fails for 2147395599 , returns 1073697799 (i...
Square root of an integer · 4 minutes ago

Joul does not work... see for n=11 for example.....
Generate all unique partitions of an integer · 7 minutes ago

GeeksforGeeks Thanks for pointing this out. We have updated...
Greedy Algorithms | Set 7 (Dijkstra's shortest path algorithm) · 7 minutes ago

Satyanshu First of all I would like to thank you for...
Function overloading and const keyword · 11 minutes ago

Tushar Felix awesome basic and best theoratical explanation...
Analysis of Algorithms | Set 1 (Asymptotic Analysis) · 29 minutes ago

Sumit Kesarwani i think ur code will not work if, in above...
Boundary Traversal of binary tree · 31 minutes ago

All Categories

Select Category

- GeeksQuiz
- GeeksforGeeksIDE
- GeeksforGeeks Practice
- Data Structures
- Algorithms
- C Programming
- C++ Programming
- Java Programming
- Books
- Interview Experiences
- GATE CS
- GATE CS Forum
- Android App