Modular Arithmetic

Modular arithmetic is a system of arithmetic for integers, which considers the remainder. In modular arithmetic, numbers "w around" upon reaching a given fixed quantity (this given quantity is known as the modulus) to leave a remainder. Modular arithmetic is often tied to prime numbers, for instance, in Wilson's theorem, Lucas's theorem, and Hensel's lemma, and generally appears in fields like cryptography, computer science, and computer algebra.

An intuitive usage of modular arithmetic is with a 12-hour clock. If it is 10:00 now, then in 5 hours the clock will show 3:00 inste of 15:00. 3 is the remainder of 15 with a modulus of 12.

A number $x \bmod N$ is the equivalent of asking for the remainder of x when divided by N. Two integers a and b are said to b congruent (or in the same equivalence class) modulo N if they have the same remainder upon division by N. In such a case, say that $a \equiv b \pmod{N}$.

Contents

Modular Arithmetic as Remainders

The easiest way to understand modular arithmetic is to think of it as finding the remainder of a number upon division by another number. For example, since both 15 and -9 leave the same remainder 3 when divided by 12, we say that

$$15 \equiv -9 \pmod{12}.$$

This allows us to have a simple way of doing modular arithmetic: first perform the usual arithmetic, and then find the remain For example, to find $123 + 321 \pmod{11}$, we can take

$$123 + 321 = 444$$

and divide it by 11, which gives us

$$123 + 321 \equiv 4 \pmod{11}.$$

However, this could get messy when the numbers get larger. One approach that we could take is to first find the remainders 123 and 321 when divided by 11 (the remainders are both 2), perform the usual arithmetic, and find the remainder again. In thi

example, since $123 \equiv 2 \pmod{11}$ and $321 \equiv 2 \pmod{11}$, we can conclude that

$$\begin{aligned} 123 + 321 &\equiv 2 + 2 \pmod{11} \\ &\equiv 4 \pmod{11}. \end{aligned}$$

Congruence

For a positive integer n, the integers a and b are congruent $\bmod n$ if their remainders when divided by n are the same.

EXAMPLE

$$52 \equiv 24 \pmod{7}$$

As we can see above, 52 and 24 are congruent (mod 7) because $52 \pmod{7} = 3$ and $24 \pmod{7} = 3$.

Note that $=$ is different from $\equiv$.

Another way of defining this is that integers a and b are congruent $\bmod n$ if their difference $(a - b)$ is an integer multiple o that is, if $\frac{a-b}{n}$ has a remainder of 0.

EXAMPLE

$$36 \equiv 10 \pmod{13}$$

36 and 10 are said to be congruent (mod 13) because their difference $36 - 10 = 26$ is an integer multiple of $n = 13$, that i $26 = 2 \times 13$.

Addition

Properties of addition in modular arithmetic:

1. If $a + b = c$, then $a \pmod{N} + b \pmod{N} \equiv c \pmod{N}$.
2. If $a \equiv b \pmod{N}$, then $a + k \equiv b + k \pmod{N}$ for any integer k.
3. If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then $a + c \equiv b + d \pmod{N}$.
4. If $a \equiv b \pmod{N}$, then $-a \equiv -b \pmod{N}$.

EXAMPLE

It is currently 7:00 PM. What time (in AM or PM) will it be in 1000 hours?

Time "repeats" every 24 hours, so we work modulo 24. Since

$$1000 \equiv 16 + (24 \times 41) \equiv 16 \pmod{24},$$

the time in 1000 hours is equivalent to the time in 16 hours. Therefore, it will be 11:00 AM in 1000 hours. □

EXAMPLE

Find the sum of 31 and 148 in modulo 24.

Solution 1:
31 in modulo 24 is equivalent to 7. If we use the first modular addition rule stated in this wiki, we find that $31 + 148 \equiv 7 + 148 \equiv 155 \pmod{24}$. 155 in modulo 24 is 11. □

Solution 2:
As stated previously, 31 in modulo 24 is 7. Instead of using the first rule, we'll use the second rule. 148 is 4 in modulo 24. So now, all we need to find is 7+4, which is 11. □

EXAMPLE

Find the remainder when $123 + 234 + 32 + 56 + 22 + 12 + 78$ is divided by 3.

We know that $123 \equiv 0 \pmod{3}$, $234 \equiv 0 \pmod{3}$, $32 \equiv 2 \pmod{3}$, $56 \equiv 2 \pmod{3}$, $22 \equiv 1 \pmod{3}$, $12 \equiv 0 \pmod{3}$, and $78 \equiv 0 \pmod{3}$. From property 3, we have

$$123 + 234 + 32 + 56 + 22 + 12 + 78 \equiv 0 + 0 + 2 + 2 + 1 + 0 + 0 \equiv 5 \pmod{3}.$$

Since 5 has a remainder of 2 when divided by 3, so does $123 + 234 + 32 + 56 + 22 + 12 + 78$, and thus the answer is 2 □

Multiplication

Modular multiplication appears in many fields of mathematics and has many far-ranging applications, including cryptograph computer science, and computer algebra.

Properties of multiplication in modular arithmetic:

1. If $a \cdot b = c$, then $a \pmod{N} \cdot b \pmod{N} \equiv c \pmod{N}$.
2. If $a \equiv b \pmod{N}$, then $ka \equiv kb \pmod{N}$ for any integer k.
3. If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then $ac \equiv bd \pmod{N}$.

EXAMPLE

What is $(8 \times 16) \pmod{7}$?

Since $8 \equiv 1 \pmod{7}$ and $16 \equiv 2 \pmod{7}$, we have

$$(8 \times 16) \equiv (1 \times 2) \equiv 2 \pmod{7}.$$ □

EXAMPLE

Find the remainder when $124 \cdot 134 \cdot 23 \cdot 49 \cdot 235 \cdot 13$ is divided by 3.

We did a similar problem above, where the signs were all $+$ instead of $\times$. In that case, manually adding the numbers up wouldn't take that much time, though the modular arithmetic solution was faster.

In this example, multiplying the numbers would be very tedious. Instead, we use property 3 repeatedly. We know that $124 \equiv 1$, $134 \equiv 2$, $23 \equiv 2$, $49 \equiv 1$, $235 \equiv 1$, and $13 \equiv 1$. Therefore,

$$124 \cdot 134 \cdot 23 \cdot 49 \cdot 235 \cdot 13 \equiv 1 \cdot 2 \cdot 2 \cdot 1 \cdot 1 \cdot 1 \equiv 4 \equiv 1 \pmod 3,$$

implying the product, upon division by 3, leaves a remainder of 1. □

EXAMPLE

Prove property 3 of multiplication in modular arithmetic as stated below:

If $a \equiv b \pmod N$ and $c \equiv d \pmod N$, then $ac \equiv bd \pmod N$.

By the definition of equivalence, $a - b$ is a multiple of N and $c - d$ is a multiple of N. That is,

$$a - b = k_1 N, \quad c - d = k_2 N$$

for constants k_1 and k_2. Then

$$\begin{aligned} ac - bd &= ac - bd + bc - bc \\ &= c(a - b) + b(c - d) \\ &= c(k_1 N) + b(k_2 N) \\ &= (ck_1 + bk_2)N. \end{aligned}$$

This implies $ac - bd$ is a multiple of N and therefore $ac - bd \equiv 0 \pmod N$, or $ac \equiv bd \pmod N$. □

TRY IT YOURSELF

What is the last digit when

$$1234 \times 5678$$

is multiplied out?

- ◯ 2
- ◯ 4
- ◯ 6
- ◯ 8

Exponentiation

Since exponentiation is repeated multiplication, we have the following:

Property of Exponentiation in Modular Arithmetic:

If $a \equiv b \pmod{N}$, then $a^k \equiv b^k \pmod{N}$ for any positive integer k.

PROOF

We can write a in the form of $a = Np + b$, where p is some integer. Then we have

$$a^k = (Np+b)^k = \sum_{i=0}^{k} \binom{k}{i} (Np)^{k-i} b^i.$$

Now notice how all the terms of this sum are multiples of N, except the last when $i = k$. Hence

$$a^k \equiv 0 + 0 + \cdots + 0 + b^k = b^k \pmod{N}. \ \square$$

EXAMPLE

What is $3^{16} \pmod{4}$?

We observe that

$$3^2 \equiv 9 \equiv 1 \pmod{4}.$$

Then by the property of exponentiation, we have

$$\begin{aligned} 3^{16} \pmod{4} &\equiv \left(3^2\right)^8 \pmod{4} \\ &\equiv (1)^8 \pmod{4} \\ &\equiv 1 \pmod{4}. \ \square \end{aligned}$$

In the above example, we do not need to find the exact value of 3^{16}, which is very large

EXAMPLE

What is the last digit of 17^{17}?

The last digit of a number is equivalent to the number taken modulo 10. Working modulo 10, we have

$$\begin{aligned} 17^{17} &\equiv 7^{17} &&\equiv \left(7^2\right)^8 \cdot 7 &&\pmod{10} \\ &\equiv (49)^8 \cdot 7 &&\equiv 9^8 \cdot 7 &&\pmod{10} \\ &\equiv \left(9^2\right)^4 \cdot 7 &&\equiv (81)^4 \cdot 7 &&\pmod{10} \\ &\equiv 1^4 \cdot 7 &&\equiv 7 &&\pmod{10}. \ \square \end{aligned}$$

EXAMPLE

Find the last three digits of 2^{40}.

We have

$$\begin{aligned} 2^{40} &= \left(2^{10}\right)^4 \\ &= 1024^4 \\ &\equiv 24^4 \\ &\equiv 576^2 \pmod{1000}. \end{aligned}$$

We can write 576^2 as

$$\begin{aligned} (500+76)(500+76) &= 250000 + 2\times 500 \times 76 + 76 \times 76 \\ &= 250000 + 76000 + 5776 \\ &\equiv 0 + 5776 \\ &\equiv 776 \pmod{1000}. \end{aligned}$$

Since 2^{40} leaves a remainder of 776 when divided by 1000, its last three digits are 776. □

TRY IT YOURSELF

What is the remainder when $2^{123456789}$ is divided by 7?

Submit your answer

EXAMPLE

Find an example of integers a, x, y, n, where $x \equiv y \pmod{n}$, but $a^x \not\equiv a^y \pmod{n}$.

Many combinations of a, x, y, n will work here. We present the case with $n = 3, a = 2, x = 2$ and $y = 5$, where we get $2 \equiv 5 \pmod{3}$, but $2^2 \equiv 1 \pmod{3}$ while $2^5 \equiv 2 \pmod{3}$. □

The important takeaway is that the exponentiation property only works on the base. If you want to work with the powers, you need Euler's theorem.

Division

This is tricky. Consider $4 \equiv 8 \pmod{4}$. Note that we cannot simply divide both sides of the equation by 2, since $2 \not\equiv 4 \pmod{4}$. This shows that, in general, division is not well defined. As the following property shows, if we add the condition th k, N are coprime, then division becomes well defined.

THEOREM

Property of division in modular arithmetic:

If $\gcd(k, N) = 1$ and $ka \equiv kb \pmod{N}$, then $a \equiv b \pmod{N}$.

This property is true because if $k(a-b)$ is a multiple of N and $\gcd(k, N) = 1$, then N must divide $a-b$, or equivalently, $a \equiv b \pmod{N}$.

Multiplicative Inverses

The modular inverse of a in the ring of integers modulo m is an integer x such that

$$ax \equiv 1 \pmod{m}.$$

From the Euclidean division algorithm and Bézout's identity, we have the following result about the existence of multiplicativ inverses in modular arithmetic:

DEFINITION

If a and N are integers such that $\gcd(a, N) = 1$, then there exists an integer x such that $ax \equiv 1 \pmod{N}$.

x is called the **multiplicative inverse** of a modulo N.

The following Python code shows how we can calculate the modulo inverse by implementing the extended Euclidean algoritl

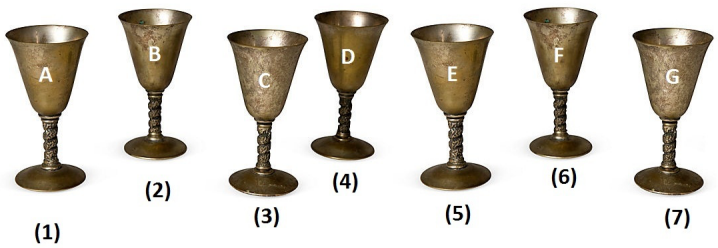
Python Implementation

Python

```
def egcd(a, b):
    x,y, u,v = 0,1, 1,0
    while a != 0:
        q, r = b//a, b%a
        m, n = x-u*q, y-v*q
        b,a, x,y, u,v = a,r, u,v, m,n
    gcd = b
    return gcd, x, y
def modinv(a, m):
    gcd, x, y = egcd(a, m)
    if gcd != 1:
        return None
    else:
        return x % m
```

Word Problems

TRY IT YOURSELF



- A
- B
- C
- D
- E
- F

One of the seven goblets above is made of real gold. If you start counting at A and wind

back and forth while counting (A, B, C, D, E, F, G, F, E, D, ...), then the golden goblet would be the 1000^{th} one that you count.

Which one is the golden goblet?

- G

TRY IT YOURSELF

Aditya is excited for his birthday party on Saturday, March 2, 2013. He is turning 16 years old. What day of the week was Aditya born?

Submit your answer

Details and Assumptions:

- The recent leap years are 2012, 2008, 2004, 2000, 1996, ... If your answer is Monday, type 1. If your answer is Tuesday, type 2, and so on and so forth. If your answer is Sunday, type 7.

TRY IT YOURSELF

Ashley went to the movies nine days ago. If Thursdays are the only day of the week that Ashley goes to the movies, then what day of the week is today?

- Tuesday
- Wednesday
- Friday
- Saturday

Problem Solving - Basic

TRY IT YOURSELF

$$6^{6^{6^{6^{6^{6}}}}}$$

What is the remainder when the above number is divided by 7?

Clarification: There are a total of seven 6's.

- 0
- 1
- 2
- 3
- 5
- 8

TRY IT YOURSELF

What is the remainder when

$$1! + 2! + 3! + \cdots + 50!$$

- 0
- 22

is divided by $5!$?

- 11
- 33

TRY IT YOURSELF

$$a^x \equiv a-2 \pmod{(a-1)}$$

Submit your answer

If a and x are positive integers greater than 2, what is the value of a?

TRY IT YOURSELF

$$\underbrace{1111111\ldots1}_{\text{number of 1's} = 124} \pmod{271} = ?$$

Submit your answer

Problem Solving - Intermediate

EXAMPLE

Mark Hennings

Is there a positive integer n for which $n^7 - 77$ is a Fibonacci number?

If p is a prime of the form $7k+1$, then there are $k+1$ seventh powers (where the +1 accounts for 0). This gives a fighting chance of the residues being distinct from the Fibonacci residues. So, we try the smallest prime of the form $7k+1$, which i 29.

We can check that $n^7 \equiv 0, 1, 12, 17, 28 \pmod{29}$, which gives us

$$n^7 - 77 \equiv 9, 10, 11, 22, 27 \pmod{29}.$$

When looking at the remainder of the Fibonacci numbers taken modulo 29, we obtain the repeating sequence

$$1, 1, 2, 3, 5, 8, 13, 21, 5, 26, 2, 28, 1, 0, \ldots.$$

A quick check shows us that no number appears in both sequences, and thus the answer is no. □

TRY IT YOURSELF

$$n^3 - 3n + 7 \equiv 0 \pmod{n-5}$$
$$2n^2 - n + 2 \equiv 0 \pmod{n+6}$$

Submit your answer

What integer $n \geq 5$ satisfies the above system of congruence equations?

TRY IT YOURSELF

$$1 \times 10^1 + 2 \times 10^2 + 3 \times 10^3 + \cdots + 2015 \times 10^{2015}$$

What is the remainder when the number above is divided by 11?

Submit your answer

TRY IT YOURSELF

Bogdan divides 2015 successively by 1, 2, 3, ..., all the way up to include 1000. He writes down the remainder for each division. What is the largest remainder he writes down?

Submit your answer

TRY IT YOURSELF

$$\begin{cases} x^2 + 3x - 7 & \equiv 0 \pmod{71} \\ x^2 - 5x - 16 & \equiv 0 \pmod{89} \end{cases}$$

Let x be a positive integer satisfying the system of equations above. What is the least possible value of x?

Submit your answer

See Also

- Chinese Remainder Theorem
- Finding the Last Digit of a Power