Modular inverses

Modular inverses

Google Classroom Facebook Twitter Email

What is an inverse?

Recall that a number multiplied by its inverse equals 1. From basic arithmetic we know that:

- The inverse of a number A is 1/A since A * 1/A = 1 (e.g. the inverse of 5 is 1/5)
- All real numbers other than 0 have an inverse
- Multiplying a number by the inverse of A is equivalent to dividing by A (e.g. 10/5 is the same as 10* 1/5)

What is a modular inverse?

In modular arithmetic we do not have a division operation. However, we do have modular inverses.

- The modular inverse of A (mod C) is A^-1

- (A * A^-1) ≡ 1 (mod C) or equivalently (A * A^-1) mod C = 1

- Only the numbers coprime to C (numbers that share no prime factors with C) have a modular inverse (mod C)

How to find a modular inverse

A naive method of finding a modular inverse for A (mod C) is:

step 1. Calculate A * B mod C for B values 0 through C-1

step 2. The modular inverse of A mod C is the B value that makes A * B mod C = 1

Note that the term B mod C can only have an integer value 0 through C-1, so testing larger values for B is redundant.

Example: A=3, C=7

Step 1. Calculate A * B mod C for B values 0 through C-1

$3 * 0 \equiv 0 \pmod{7}$

$3 * 1 \equiv 3 \pmod{7}$

$3 * 2 \equiv 6 \pmod{7}$

$3 * 3 \equiv 9 \equiv 2 \pmod{7}$

$3 * 4 \equiv 12 \equiv 5 \pmod{7}$

$3 * 5 \equiv 15 \pmod{7} \equiv \underline{1} \pmod{7}$ <------ FOUND INVERSE!

$3 * 6 \equiv 18 \pmod{7} \equiv 4 \pmod{7}$

Step 2. The modular inverse of A mod C is the B value that makes A * B mod C = 1

5 is the modular inverse of 3 mod 7 since 5*3 mod 7 = 1

Simple!

Let's do one more example where we don't find an inverse.

Example: A=2 C=6

Step 1. Calculate A * B mod C for B values 0 through C-1

2 * 0 ≡ 0 (mod 6)

2 * 1 ≡ 2 (mod 6)

2 * 2 ≡ 4 (mod 6)

2 * 3 ≡ 6 ≡ 0 (mod 6)

2 * 4 ≡ 8 ≡ 2 (mod 6)

2 * 5 ≡ 10 ≡ 4 (mod 6)

Step 2. The modular inverse of A mod C is the B value that makes A * B mod C = 1

No value of B makes A * B mod C = 1. Therefore, A has no modular inverse (mod 6).
This is because 2 is not coprime to 6 (they share the prime factor 2).

This method seems slow...

There is a much faster method for finding the inverse of A (mod C) that we will discuss in the next articles on the Extended Euclidean Algorithm.

Sort by:

Want to join the conversation?

gunwati.rules5 years ago

Why is it that A has to be coprime to C to have a modular inverse?

(10 votes)

Cameron5 years ago

Suppose A has an inverse mod C.
We will call this inverse X. (X is an integer)
A * X mod C = 1
We can equivalently write:
(A * X) = Q * C + 1
where Q is some integer
we can rearrange this to:
A * X + C * Y = 1

(where Y=-Q, Y is an integer)

Now we can label the product of ALL the prime factors that A and C share as S.
e.g. if A = 70 = 2 * 5 * 7 and B= 42 = 2 * 3 * 7 then S= 14 = 2 * 7
If A and C are coprime (no shared prime factors) then S=1
Note: S is positive

We can write:
A = F * S
C = G * S
where F and G are integers

Then:
A * X + C * Y= 1
Becomes:
(F * S) * X + (G * S) * Y = 1
S * (F * X + G * Y) = 1
(F * X + G * Y) = 1/S
But (F * X + G * Y) is the sum of products of integers, and thus must be an integer
(this is a property of integers)
Thus the right hand side of the equation, 1/S, must also be an integer
But the only possible integer for S that could make 1/S an integer are -1 and 1.
S is positive so S must be 1.
But S is the product of ALL the prime factors that A and C share.
But S is 1, so A and C must be coprime.

Thus:
If A has an inverse mod C, then A and C must be coprime.

Equivalently:
If A and C are not coprime, then A does not have an inverse mod C.

As a side note, when one calculates the modular inverse using the Extended Euclidean Algorithm, we solve for X and Y in the equation:
A * X + C * Y = GCD(A,C)
If GCD(A,C) is 1 (A,C are coprime) then X is the modular inverse of A, otherwise it is not.

Hope this makes sense

(38 votes)

The4thdimentionpro6 years ago

Wait, I thought you could divide by any number in modular arithmetic as long as the number inside the modulus was relatively prime to the number you were dividing by. Do you always have to use modular inverses?

I will find the faster method before Brit Cruise posts it up...
EDIT:
a mod b
a^2 mod b
a^3 mod b
...
Eventually, one of these expressdions will get to 1. If b is prime, then a^(b-1) mod b will be congruent to 1.
a^n mod b=1
a^(n-1)*a mod b=1
a^(n-1) mod b is the modular inverse of a mod b and if b is prime, a^(b-2) is the modular inverse of a mod b.

That's as close as I got.

This was edited just before the Extended Euclidean Algorithm was posted.

(7 votes)

Cameron6 years ago

Division doesn't exist in modular arithmetic. However, many of the things we can do with modular inverses act the same as or similar to division.

e.g.
if we have a * k ≡ b * k (mod C) where k is coprime to C we can eliminate the k from each side and say:
a ≡ b (mod C)

How did we eliminate k ?
We know that k has an inverse mod C since k is coprime to C. (We don't need to know what the value of the inverse is. We just need to know an inverse exists.)
So when we have a * k ≡ b * k (mod C) , we multiply both sides by k^-1
a * k * k^-1 ≡ b * k * k^-1 (mod C)
but since k * k^-1 = 1 we have
a * 1 ≡ b * 1 (mod C)
a ≡ b (mod C)

So as you can see, we are not dividing, but instead using modular inverses. The end result looks like we are dividing and intuitively what we are doing is similar, but is important to note that we don't have division in modular arithmetic, but in some cases we do have inverses.

Hope this makes sense

(10 votes)

Chris Torrence6 years ago

Did the Extended Euclidean Algorithm articles ever get published? These modular arithmetic articles have been fantastic, and I'm really looking forward to the next articles!

(8 votes)

bs.baniya5 years ago

Still not up article of Extended Euclidean Algorithm?

(2 votes)

Tjon Lichy5 years ago

Wait a second! *There is a much faster method for finding the inverse of A (mod C) that we will discuss in the next articles on the Extended Euclidean Algorithm. First, let's do some exercises!* But where are the exercises? The next stop is "The Euclidean Algorithm".

(8 votes)

rupertlihero3 years ago

There aren't any yet...

(1 vote)

Armin Roüshan5 years ago

I want to know how can you show if a number has an inverse or not.
Example: show the number 6 does not have a multiplication inverse modulo 15.

(2 votes)

Cameron5 years ago

For: A mod C
A only has an inverse mod C, if A and C are coprime i.e. gcd(A,C)=1
gcd(6,15)=3 thus 6 has no inverse mod 15

(2 votes)

AmiNe Sos4 years ago

Cameron said there is no division in modular arithmetic. But my problem sais:
Solve: 11x ≡ 11 mod33
Now the only way I can think of it is to devide by 11 both sides plus the mod
So we get x ≡ 1 mod3
And its correct! But if theres no division how would I solve it??
Please clarify to me, thanks in advance

(2 votes)

Cameron4 years ago

There is no division in modular arithmetic.

Suppose we had an equation like:
A * x ≡ B mod C

If A was coprime to C
i.e. gcd(A,C)=1
To solve for x we would multiply both sides by the modular inverse of A mod C

A * A^-1 * x ≡ B * A^-1 mod C
But A * A^-1 mod C = 1
1 * x ≡ B * A^-1 mod C
And 1 * x mod C = x
x ≡ B * A^-1 mod C

e.g.
5 * x ≡ 2 mod 14
5 is coprime with 14, so 5 has an inverse mod 14
5 * 5^-1 * x ≡ 2 * 5^-1 mod 14
1 * x ≡ 2 * 5^-1 mod 14
x ≡ 2 * 5^-1 mod 14

5^-1 mod 14 is 3, since 3 * 5 mod 14 = 15 mod 14 = 1
x ≡ 2 * 3 mod 14
x ≡ 6 mod 14

****But what do we do if A is NOT coprime to C****
i.e. gcd(A,C) != 1 ?
To solve for x, we need to convert the expression to an equivalent form
A * x ≡ B mod C
is equivalent to:
A * x = K * C + B where K is an integer
This is just a regular equation, so we can use divide here.
If A,B and C are ALL divisible by D then we can divide both sides of the equation to get:
(A/D) * x = K * (C/D) + (B/D) where K is an integer
Note that:(A/D) , (C/D), and (B/D) will all be integers
We can then convert this new equation into a congruence to get:
(A/D) * x ≡ (B/D) mod (C/D)

So, it only seems like we can divide by D when A,B and C are ALL divisible by D
(but it isn't really division, it only looks similar to division)

But you need to be careful !! If you solve for x now, you will have an answer mod (C/D)
You will need to find all the possible values where 0 <= x < C to be able to express your answer mod C

e.g.
12 * x ≡ 15 mod 45
is equivalent to:
12 * x = K * 45 + 15
Divide both sides by 3
4 * x = K * 15 + 5
is equivalent to:
4 * x ≡ 5 mod 15
This new expression can then be solved using the method for A coprime to C
4 * x ≡ 5 mod 15
4 * 4^-1 * x ≡ 5 * 4^-1 mod 15
4^-1 mod 15 is 4 since 4 * 4 mod 15 = 16 mod 15 = 1
x ≡ 5 * 4 mod 15
x ≡ 20 mod 15
x ≡ 5 mod 15

(But this answer is mod 15, we need our answer to be mod 45)
our expression is equivalent to $x = K * 15 + 5$ where K is an integer
So the possible values of $0 <= x < 45$ are:
5,20,35
So our answer is:
$x \equiv 5, 20$, or $35 \mod 45$

So, as far as $11 * x \equiv 11 \mod 33$ goes, you can obtain $x \equiv 1 \mod 3$ from it.
This only works because all of the terms are divisible by 11. Again, what's happening is not really division (it only seems similar).
Additionally, the solution needs to be converted to mod 33.
i.e. $x \equiv 1,4,7,10,13,16,19,22,25,28$, or $31 \mod 33$

Hope this makes sense

(2 votes)

azmatshah983 years ago

if $ab \equiv 1 \mod n$, and $b<n$, how do I prove that b is unique.

(2 votes)

Cameron3 years ago

Typically, when you have some thing with some property and you want to prove it is unique, you do the following:
Suppose that both b and c have that property.
Show that $b = c$.
This shows that everything that has that property is b, i.e. there isn't anything with that property that is not b.

This case is similar:
- we would assume that both b and c have the same property i.e. both b and c are inverses of a (mod n)
- we need to show that $b \equiv c \pmod n$

Proof:
Suppose b and c are inverses of a (mod n)
Since b is an inverse of a (mod n):
$a * b \equiv 1 \pmod n$
Since c is an inverse of a (mod n):

a * c ≡ 1 (mod n)

a * b ≡ 1 (mod n)
subsitute (a * c) into right hand side
a * b ≡ a * c (mod n)
multiply both sides by a^-1
a * a^-1 * b ≡ a * a^-1 * c (mod n)
1 * b ≡ 1 * c (mod n)
b ≡ c (mod n)

Hope this makes sense

(1 vote)

bassam.ahmed324 years ago

how can i proof that if: k =a*b mod n
then
k^-1 = a^-1 * b^-1 mod n

(2 votes)

Cameron4 years ago

Here's a big hint:

Start from this congruence
K * K^-1 ≡ 1 (mod N)
Then try to reach this congruence:
K^-1 ≡ A^-1 * B^-1 (mod N)

You will need to use this: K ≡ A * B (mod N)
and the property that: X * X^-1 ≡ 1 (mod N)

Good Luck

(1 vote)

Reshab Gupta3 years ago

a equivalence b%c is equivalent to a = c*K + b for some integer K.How can we use equals to(=) here?

(2 votes)

Cameron3 years ago

A ≡ B (mod C) is equivalent to A = C * K + B (where K is some integer)

It is not clear what concept that you are struggling with. Perhaps you could provide more detail.

(1 vote)

Vic3 years ago

Can this same idea be used when finding the inverse of a matrix with mod 26 for example?

(2 votes)

Cameron3 years ago

Inverse of a matrix mod N is found the same way you would find any matrix inverse. But here is the catch:
You can't divide in modular arithmetic, you can only multiply by a mod inverse.

Here's why that is important :
We know that the solution for the inverse of a matrix is:
A^-1 = 1 / det(A) * C^T
where:
- A^-1 is the inverse of matrix A
- det(A) is the determinant of A
- C^T is the transpose of the cofactor matrix of A

So if we are working with the matrix (mod N) we need to replace:
1 / det(A) with the modular inverse of det(A) mod A.
If gcd(det(A), N) = 1 then that modular inverse exists, otherwise it does not.
If the modular inverse doesn't exist then the matrix can't be inverted.
So this should be the first thing you check before trying to calculate an inverse matrix mod N.

Hope this makes sense

(1 vote)