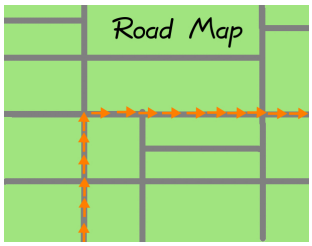
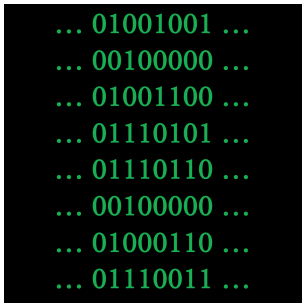
Module 10.3: All about Modular Inverses



Earlier, we saw that there is no division operation in modular arithmetic, a point we will quickly revisit in this module. Then, we will learn about the replacement of division, which is the modular inverse. We will also use modular inverses to solve some simple equations in modular arithmetic.

Along the way, we will have the chance to discover some cool theorems about modular inverses. There are many applications of modular inverses in mathematics, but we cannot explore them here. Instead, we will see some in the next module (about historical ciphers), and we will see that the modular inverse is very important in the RSA cryptosystem. If you're unfamiliar with the RSA cryptosystem, I'll describe it briefly, in the next box.



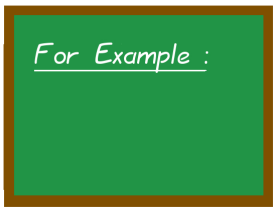
Whenever you use your web browser in `https://` mode, instead of `http://` mode, you're actually using a protocol called SSL or TLS (the Secure Sockets Layer, or Transport Layer Security). The early versions of the protocol were called SSL, but the committee in charge of it decided to rename it TLS, yet many people still say "SSL" out of habit. Others, like myself, will say SSL/TLS.

When your web browser uses SSL/TLS, the encrypted link uses either the RSA Cryptosystem, or the Diffie-Helman Key-Exchange protocol. Both RSA and Diffie-Hellman are based on modular arithmetic.

The letters RSA stand for Rivest-Shamir-Adleman, the last names of the inventors: Ron Rivest, Adi Shamir, and Leonard Adleman. All three are still alive as of the year 2020, so etiquette forbids that I put a biography of them in a textbook.

In order to understand this module, it is vital to grasp that division and fractions from the ordinary rational numbers will not make sense in the environment of modular arithmetic. For example, we should never write something like $15 \div 5$ or $3/5$ when working in modular arithmetic.

The next two examples will explain why.



10-3-1

When we write $15 \div 5 = 3$ in the ordinary integers, what we're really saying is that 3 is a solution to the equation $5x = 15$. Dividing both sides by 5 will reveal that $x = 15 \div 5 = 3$.

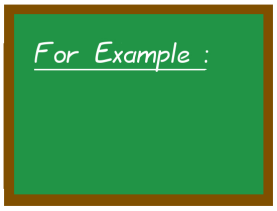
In contrast, consider working mod 25, and the equation $5x \equiv 15$. Any $x \in \{3, 8, 13, 18, 23\}$ is a solution to $5x \equiv 15 \bmod 25$. Consider

$$\begin{aligned} 5(3) &= 15\checkmark \\ 5(8) &= 40 = 25 + 15 \equiv 15 \bmod 25\checkmark \\ 5(13) &= 65 = 50 + 15 = 2(25) + 15 \equiv 15 \bmod 25\checkmark \\ 5(18) &= 90 = 75 + 15 = 3(25) + 15 \equiv 15 \bmod 25\checkmark \\ 5(23) &= 115 = 100 + 15 = 4(25) + 15 \equiv 15 \bmod 25\checkmark \end{aligned}$$

The symbols $15 \div 5$ make sense in the ordinary integers because there is a unique solution to $5x = 15$. That means that the symbols $15 \div 5$ refer to one integer. In the world of mod 25 arithmetic, you must not write $15 \div 5$, because if you did, no one would know which of the five solutions from $\{3, 8, 13, 18, 23\}$ you mean.

An alternative way of finding the solution set in the previous example involves the Cayley table for mod 25. (Such a table has been provided in the appendix "Modular Arithmetic Tables.") One can look in the row for multiplication by 5, and search for 15s. We see 15s in the columns for 3, 8, 13, 18, and 23.

For small moduli, this can be a fast way of finding solution sets. For the size moduli that are used in practice with RSA, the Cayley table would be larger than the solar system, because the moduli are hundreds of digits long, if not longer.



10-3-2

When we write $3/5$ in the ordinary rational numbers, what we're really trying to indicate is the single rational number that is a solution to the equation $5x = 3$. Dividing both sides by 5 will reveal that $x = 3/5$.

In contrast, working mod 25, there are no solutions to the equation $5x \equiv 3 \bmod 25$. This is most easily seen by looking at the Cayley table for mod 25. When we find the row for multiplication by 5, we see that this row does not contain any 3s. Therefore, there is no solution to $5x \equiv 3 \bmod 25$.

Furthermore, this means that we cannot write $3/5$ in the world of mod 25 arithmetic, because we would be talking about a number that does not exist (in that world).

Another way to see that $5x \equiv 3 \bmod 25$ has no solutions is to cut-and-paste the following code (below this box) into Sage. This code runs a for-loop through all 25 numbers in the world of "mod 25 arithmetic." For each number, it multiples by 5, and prints the output. We obtain this output. As you can see, the result is never 3.

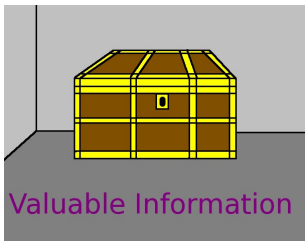
```
0 ---> 0; 1 ---> 5; 2 ---> 10; 3 ---> 15; 4 ---> 20; 5 ---> 0; 6 ---> 5; 7
---> 10; 8 ---> 15; 9 ---> 20; 10 ---> 0; 11 ---> 5; 12 ---> 10; 13 ---> 15;
14 ---> 20; 15 ---> 0; 16 ---> 5; 17 ---> 10; 18 ---> 15; 19 ---> 20; 20
---> 0; 21 ---> 5; 22 ---> 10; 23 ---> 15; 24 ---> 20;
```

The careful reader will note the use of the `%` sign to indicate mod 25 arithmetic.

```
for k in range(0, 25):
    output = (5*k) % 25
    print(k, "--->", output, end="; ")
```

Now we've established that we must never write something like $15 \div 5$ or $3/5$ when working with modular arithmetic. Instead, we will replace division with a new operation, called the modular inverse.

Let's start with a formal definition, given in the next box.

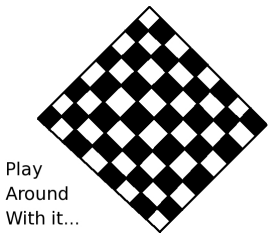


We shall use the following five "abbreviations" for $ab \equiv 1 \bmod N$.

- a and b are inverses mod N.
- a is the inverse of b mod N.
- b is the inverse of a mod N.
- $a \equiv b^{-1} \bmod N$.
- $b \equiv a^{-1} \bmod N$.

Remember, these bullets are just alternative ways of writing "$ab \equiv 1 \bmod N$."

Please reread the previous box. It is extremely important.

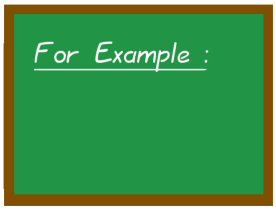


10-3-3

Please determine whether or not the following statements are true.

1. $41^{-1} \equiv 48 \bmod 96$.
2. $17^{-1} \equiv 5 \bmod 21$.
3. $7^{-1} \equiv 36 \bmod 251$.
4. $11^{-1} \equiv 17 \bmod 37$.
5. $13^{-1} \equiv 61 \bmod 75$.

The solutions will be given on Page 615 of this module.



10-3-4

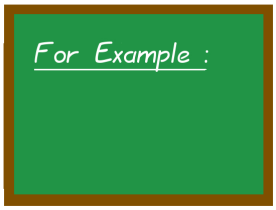
Suppose we might like to know 2^{-1}, 3^{-1}, 4^{-1}, 5^{-1}, 6^{-1}, 7^{-1}, and 8^{-1}, all taken mod 15.

- Because $(2)(8) = 16 = 15 + 1 \equiv 1$, 2 and 8 are inverses, so we write $2^{-1} \equiv 8 \bmod 15$.
- Because $(7)(13) = 91 = 90 + 1 = (15)(6) + 1 \equiv 1$, we know that 7 and 13 are inverses, so $7^{-1} \equiv 13 \bmod 15$.
- Because $(4)(4) = 16 = 15 + 1 \equiv 1$, 4 is its own inverse, so we write $4^{-1} \equiv 4 \bmod 15$.
- Earlier, we found out that 8 and 2 are inverses, so we can also write $8^{-1} \equiv 2 \bmod 15$.
- Similarly, while we were not asked about 13^{-1}, we could write $13^{-1} \equiv 7 \bmod 15$, if we wanted to.

Later in this module, you will see several different methods of computing a modular inverse. Therefore, let's not focus just yet on *how* I figured out the 8 in $(2)(8) \equiv 1$ and the 13 in $7(13) \equiv 1$. We'll get to that shortly and in detail. For the moment, just make sure that you follow the rest of the reasoning.

If you are fully awake, then you will have already noticed that I have not addressed 3^{-1}, 5^{-1}, nor 6^{-1} in the previous box.

As it turns out, these numbers do not have inverses mod 15. Some numbers in the integers modulo 15 have inverses, and some do not. We will continue to discuss this in the next box.



10-3-5

How do we know that 3 has no inverse mod 15? How do we know that 5 and 6 have no inverse mod 15? One option is to look at the Cayley table for the integers modulo 15. (Such a table has been provided in the appendix "Modular Arithmetic Tables.")

Take a moment to verify that the row for multiplication by 5 has no entry equal to 1. Similarly, the rows for multiplication by 3 and multiplication by 6 have no entry equal to 1.

Continuing with the previous box, we were trying to figure out whether or not 3 has an inverse mod 15. If we do not have a Cayley table on hand, then we can instead check all the integers modulo 15.

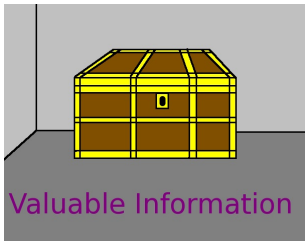
$$\begin{array}{lll} (0)(3) \equiv 0 & (5)(3) \equiv 0 & (10)(3) \equiv 0 \\ (1)(3) \equiv 3 & (6)(3) \equiv 3 & (11)(3) \equiv 3 \\ (2)(3) \equiv 6 & (7)(3) \equiv 6 & (12)(3) \equiv 6 \\ (3)(3) \equiv 9 & (8)(3) \equiv 9 & (13)(3) \equiv 9 \\ (4)(3) \equiv 12 & (9)(3) \equiv 12 & (14)(3) \equiv 12 \end{array}$$

That's a very pleasing pattern, isn't it? In any case, since there does not exist any b such that $3b \equiv 1 \bmod 15$, we conclude that 3 has no inverse mod 15.

In summary, not every member of the integers mod N will have an inverse.

In my experience with teaching this course, two misconceptions about modular inverses frequently cause harm to students. The biggest misconception is that some students assume that every member of the integers mod N has an inverse. They do not consider the possibility that some members might not be invertible.

Luckily, there is a shortcut for determining whether b has an inverse mod N or not. We'll see that on Page 614.



If there does exist an inverse of b mod N, then we can say "b is *invertible* mod N," or "b is a *unit* mod N."

If there does not exist an inverse of b mod N (that is to say, if there does not exist any a such that $ab \equiv 1 \bmod N$), then we will say that "b has no inverse mod N" or "b is not invertible mod N."

You might be wondering what the second misconception is, when it comes to students learning about modular inverses. Some students do not grasp the dependence of modular inverses on the choice of N.

- For example, because $(2)(4) = 8 = 7 + 1$, we see that $(2)(4) \equiv 1 \bmod 7$, and therefore $2^{-1} \equiv 4 \bmod 7$.
- However, we earlier saw (in an example on Page 597) that $2^{-1} \equiv 8 \bmod 15$.

If you change the modulus, the value of 2^{-1} changes, and it might not even exist at all. For example, 2 has no inverse mod 10.

You might be surprised to find the *reciprocity of modular inverses*, namely that if a is the inverse of b mod N, then b is the inverse of a mod N. In the previous example, we saw that 2 and 8 are inverses of each other, and also that 7 and 13 are inverses of each other.

However, we must recall that $a^{-1} \equiv b \bmod N$ and $b^{-1} \equiv a$ are both abbreviations for $ab \equiv 1 \bmod N$. Since these statements are both logically equivalent to $ab \equiv 1$, they must be logically equivalent to each other. That's why it is nice to sometimes say "a and b are inverses mod N," to draw attention to the reciprocity.

Here is a natural question to ask: can a member of the integers mod N have several inverses? At first glance, it might seem that it could be possible that several different members of the integers mod N might be inverses of some particular member.

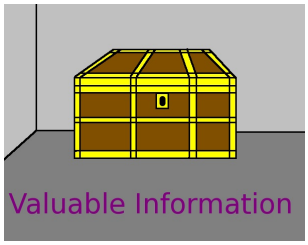
In other words, is it possible that there are $b \in \mathbb{Z}_N$ and $c \in \mathbb{Z}_N$, with $b \not\equiv c$, and $ab \equiv 1 \mod N$ as well as $ac \equiv 1 \mod N$? (Remember, the symbol $\mathbb{Z}_N$ represents "the integers modulo N.")

It turns out that the answer is no. Modular inverses are unique. Formally, if $ab \equiv 1 \mod N$ and $ac \equiv 1 \mod N$, then $b \equiv c \mod N$. We could also write that as if a and b are inverses mod N, and a and c are inverses mod N, then $b \equiv c$.

The proof of this theorem is very short and cute, so I will provide it in the next box.

Here is the proof that if $ab \equiv 1 \mod N$ and $ac \equiv 1 \mod N$, then $b \equiv c \mod N$.

- Suppose that $ab \equiv 1 \mod N$ and $ac \equiv 1 \mod N$.
  - We know that $1 \equiv 1$, thus $ab \equiv ac$.
  - Let's multiply both sides by b, obtaining $bab \equiv bac$.
  - Since $ab \equiv 1$ and since multiplication is commutative, $ba \equiv 1$.
  - Substituting 1 for ba, we obtain $1b \equiv 1c$.
  - Since $1b = b$ and since $1c = c$, we can simplify to $b \equiv c$.
- Therefore, if $ab \equiv 1 \mod N$ and $ac \equiv 1 \mod N$, then $b \equiv c \mod N$.



We have seen that a member of the integers mod N can have an inverse, or can have no inverses. Moreover, we have proven that a member of the integers mod N cannot have multiple distinct inverses.

The concise way of summarizing this is to say that "every element of the integers mod N has at most one inverse."

Other textbooks will say "For a fixed N, modular inverses are unique when they exist," but I much prefer my own concise summary.

Let's further analyze the remark, "For a fixed N, modular inverses are unique when they exist." We really do need to say "for a fixed N" in that remark.

That's because the inverse of 3 mod 7 is 5, but the inverse of 3 mod 11 is 4. Moreover, 3 doesn't even have an inverse mod 15. So if we say "the inverse of 3" without specifying a modulus, no one could possibly have any idea what we are referring to.

As mentioned earlier, the inverse of a number mod N can change if you change N. In other words, the phrase "x is the inverse of y" only has meaning in modular arithmetic if it is clear what the modulus is.

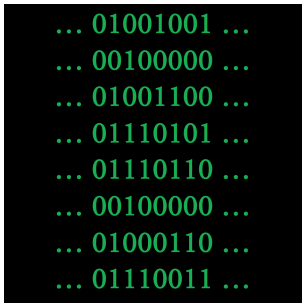
Sometimes it is nice to have a modular inverse table. For example, here is one for working in the integers mod 97.

1^{-1}	=	1	2^{-1}	=	49	3^{-1}	=	65	4^{-1}	=	73	5^{-1}	=	39	6^{-1}	=	81
7^{-1}	=	14	8^{-1}	=	85	9^{-1}	=	54	10^{-1}	=	68	11^{-1}	=	53	12^{-1}	=	89
13^{-1}	=	15	14^{-1}	=	7	15^{-1}	=	13	16^{-1}	=	91	17^{-1}	=	40	18^{-1}	=	27
19^{-1}	=	46	20^{-1}	=	34	21^{-1}	=	37	22^{-1}	=	75	23^{-1}	=	38	24^{-1}	=	93
25^{-1}	=	66	26^{-1}	=	56	27^{-1}	=	18	28^{-1}	=	52	29^{-1}	=	87	30^{-1}	=	55
31^{-1}	=	72	32^{-1}	=	94	33^{-1}	=	50	34^{-1}	=	20	35^{-1}	=	61	36^{-1}	=	62
37^{-1}	=	21	38^{-1}	=	23	39^{-1}	=	5	40^{-1}	=	17	41^{-1}	=	71	42^{-1}	=	67
43^{-1}	=	88	44^{-1}	=	86	45^{-1}	=	69	46^{-1}	=	19	47^{-1}	=	64	48^{-1}	=	95
49^{-1}	=	2	50^{-1}	=	33	51^{-1}	=	78	52^{-1}	=	28	53^{-1}	=	11	54^{-1}	=	9
55^{-1}	=	30	56^{-1}	=	26	57^{-1}	=	80	58^{-1}	=	92	59^{-1}	=	74	60^{-1}	=	76
61^{-1}	=	35	62^{-1}	=	36	63^{-1}	=	77	64^{-1}	=	47	65^{-1}	=	3	66^{-1}	=	25
67^{-1}	=	42	68^{-1}	=	10	69^{-1}	=	45	70^{-1}	=	79	71^{-1}	=	41	72^{-1}	=	31
73^{-1}	=	4	74^{-1}	=	59	75^{-1}	=	22	76^{-1}	=	60	77^{-1}	=	63	78^{-1}	=	51
79^{-1}	=	70	80^{-1}	=	57	81^{-1}	=	6	82^{-1}	=	84	83^{-1}	=	90	84^{-1}	=	82
85^{-1}	=	8	86^{-1}	=	44	87^{-1}	=	29	88^{-1}	=	43	89^{-1}	=	12	90^{-1}	=	83
91^{-1}	=	16	92^{-1}	=	58	93^{-1}	=	24	94^{-1}	=	32	95^{-1}	=	48	96^{-1}	=	96

If you'd like to make a human-readable table of modular inverses, the following Sage code will make a nice table.

```
for k in range(1, 97):
    print("The inverse of", k, "is", inverse_mod(k, 97) )

    if ((k % 4)==0):
        print()
```



In the code above, you can see another use of modular arithmetic in computer programming. If we have a `for` loop, in this case with iterator variable `k`, and if we want something to happen every 4 iterations—instead of every iteration—then observe what `k % 4` will do.

If `k` takes on the values

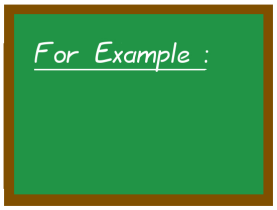
$$1, 2, 3, 4, 5, 6, 7, 8, 9, \ldots, 92, 93, 94, 95, 96$$

then `(k % 4)` takes on the values

$$1, 2, 3, 0, 1, 2, 3, 0, 1, \ldots, 0, 1, 2, 3, 0$$

As you can see, when we use an `if` statement to cause something to occur when `k % 4` equals zero, then it will happen once every four iterations.

Sorry, something here was deleted.



10-3-6

Suppose you wanted to solve

$$37x + 54 \equiv 71x + 88 \bmod 97$$

using the previously provided table of modular inverses for the integers modulo 97.

You can proceed as follows:

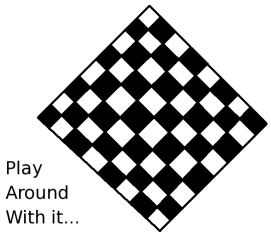
$$\begin{aligned}
37x + 54 &\equiv 71x + 89 \\
37x &\equiv 71x + 89 - 54 \\
37x &\equiv 71x + 35 \\
37x - 71x &\equiv 35 \\
(37 - 71)x &\equiv 35 \\
(-34)x &\equiv 35 \\
(97 - 34)x &\equiv 35 \\
63x &\equiv 35 \\
(77)(63x) &\equiv (77)(35) \\
4851x &\equiv 2695 \\
(4850 + 1)x &\equiv 2619 + 76 \\
(50(97) + 1)x &\equiv 27(97) + 76 \\
(0 + 1)x &\equiv 0 + 76 \\
x &\equiv 76
\end{aligned}$$

We will now check our work in the next box.

To check our solution to the previous example, we merely need to take $x \equiv 76$, and plug it into $37x + 54$ as well as $71x + 89$, and hope to get the same output in both cases.

$$37(76) + 54 = 2812 + 54 \quad = 2866 = \quad 2813 + 53 = 29(97) + 53 \equiv 0 + 53 = 53$$
$$71(76) + 89 = 5396 + 89 \quad = 5485 = \quad 5432 + 53 = 56(97) + 53 \equiv 0 + 53 = 53$$

However, it is worth noting that almost no one would show as many steps as I did in the previous box, when solving such a simple equation. Perhaps typically, 1/2 to 1/3 as many steps would be shown. I merely provided all those steps to make sure that all readers could follow the argument.



10-3-7

Using the modular inverses tables that have already been provided for working mod 97, solve these four equations:

- $92x + 60 \equiv 17x + 31 \bmod 97$
- $69x + 89 \equiv 90x + 3 \bmod 97$
- $58x + 54 \equiv 69x + 43 \bmod 97$
- $59x + 78 \equiv 24x + 55 \bmod 97$

The answers will be given on Page 615.

If you are curious, here is the Sage code that I used to generate those examples:

```
def random_nonzero_field_element():
    random_real = random()*(modulus-1)
    return floor( random_real+1 )
##########################################
modulus=97
m1=0
m2=0
b1=0
b2=0

while (m1==m2):
    m1=random_nonzero_field_element()
    m2=random_nonzero_field_element()

while (b1==b2):
    b1=random_nonzero_field_element()
    b2=random_nonzero_field_element()

m_diff = m1 - m2
b_diff = b2 - b1
multiplier = pow( m_diff, -1, modulus )
answer = multiplier*b_diff % modulus

print(answer, "is the unique solution to the equation:")
print(m1, "* x +", b1, "==", m2, "* x +", b2, "mod", modulus)

left_check = (m1*answer+b1) % modulus
right_check = (m2*answer+b2) % modulus

print("Left Side =", left_check, "... Right Side =", right_check)
```

A typical output might look like:

```
35 is the unique solution to the equation:
47 * x + 84 == 23 * x + 51 mod 97
Left Side = 80 ... Right Side = 80
```

Sometimes students ask me about the inverse of the inverse of b. For example, does the inverse of the inverse always exist? Is it useful? Is it easily calculated? What does it mean?

To explore this point, we can use the table of inverses mod 97 (provided above) to make some observations, and then we can form a hypothesis.

- The inverse of the inverse of 2, is the inverse of 49, which is 2.
- The inverse of the inverse of 3, is the inverse of 65, which is 3.
- The inverse of the inverse of 4, is the inverse of 73, which is 4.
- The inverse of the inverse of 5, is the inverse of 39, which is 5.
- The inverse of the inverse of 6, is the inverse of 81, which is 6.
- The inverse of the inverse of 7, is the inverse of 14, which is 7.

You can feel free to verify the remaining 90 cases yourself, if you like. Alternatively, a proof of the fact that "if b is invertible mod N, then b equals the inverse of the inverse of b" is given in the next box.

For Example :

10-3-8

Assume b is invertible mod N. What is the inverse of the inverse of b mod N?

Suppose b is invertible mod N. Then there must be some c such that $b^{-1} \equiv c$. This means that the words "the inverse of the inverse of b" are equivalent to "the inverse of c." Yet, since $b^{-1} \equiv c$, we know by reciprocity that $c^{-1} \equiv b$. That means the words "the inverse of c" mean just b itself. Therefore the words "the inverse of the inverse of b" is just a very long name for b.

In conclusion, $(b^{-1})^{-1} = b$. ■

For Example :

10-3-9

One way to find all the modular inverses for a modulus is called "searching for ones." You have to have the Cayley table, and make sure you're looking at the multiplication table. Then, search for 1s on the inside of the table. Whenever you find a 1, the integer associated with that row and the integer associated with that column are inverses of each other. For example, let's do this for the integers mod 11.

- We see that $1(1) \equiv 1$, so 1 is its own inverse.
- We see that $2(6) \equiv 1$, so 2 and 6 are inverses.
- We see that $3(4) \equiv 1$, so 3 and 4 are inverses.
- We already know that the inverse of 4 is 3, so we don't need to search.
- We see that $5(9) \equiv 1$, so 5 and 9 are inverses.
- We already know that the inverse of 6 is 2, so we don't need to search.
- We see that $7(8) \equiv 1$, so 7 and 8 are inverses.
- We already know that the inverse of 8 is 7, so we don't need to search.
- We already know that the inverse of 9 is 5, so we don't need to search.
- We see that $10(10) \equiv 1$, so 10 is its own inverse.

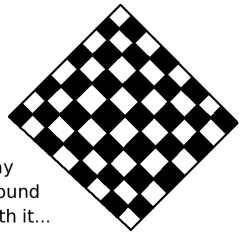
By the way, 1 is always its own inverse mod N, and $(N-1)$ is always its own inverse mod N, for any modulus $N > 1$. Let's explore why.

Since $1(1) = 1$, for all integers $N > 1$, it will always be the case that $1(1) \equiv 1$. Remembering that "a is the inverse of b mod N" is just shorthand for "$ab \equiv 1$ mod N," we can see that 1 is the inverse of 1 mod N, for any N.

Similarly, for all integers $N > 1$, it is true that $(N-1)^{-1} \equiv (N-1)$. The following calculation shows why.

$$(N-1)(N-1) = N^2 - 2N + 1 \equiv 0 - 0 + 1 \equiv 1 \bmod N$$

These properties can save you some time if you have to compute all the modular inverses for some modulus.

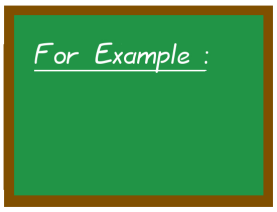


10-3-10

In the appendix "Modular Arithmetic Tables," you will find the Cayley tables for the integers mod 26. Use the technique of "finding 1s" to create a list of modular inverses for working mod 26, similar to the previous example.

For reasons that will be explained on Page 612, you can skip all the even integers, and only do the odd ones. (In short, no even integer k has an inverse mod N, for any even N.)

The answer will be given on Page 616 of this module.



10-3-11

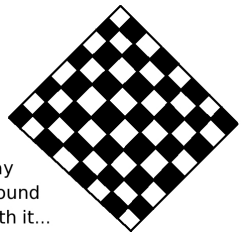
Suppose we are asked to find the inverse of 11 working mod 19. A common technique for both doing this mentally and on paper is called "counting up."

$$\begin{aligned} 11(2) &= 22 = 19+3 \equiv 3 \\ 11(3) &= 33 = 19+14 \equiv 14 \\ 11(4) &= 44 = 38+6 = 2(19)+6 \equiv 6 \\ 11(5) &= 55 = 38+17 = 2(19)+17 \equiv 17 \\ 11(6) &= 66 = 57+9 = 3(19)+9 \equiv 9 \\ 11(7) &= 77 = 76+1 = 4(19)+1 \equiv 1 \leftarrow \text{ We got it!} \end{aligned}$$

Also, I should note that when I do this mentally, I'm repeatedly adding 11 to get 22, 33, 44, 55, 66, and 77. I'm not performing a mental multiplication. I do find that mental addition is faster than mental multiplication. To be specific, I'm mentally computing:

$3{+}11 = 14;\ 14{+}11 = 25 \equiv 6;\ 6{+}11 = 17;\ 17{+}11 = 28 \equiv 9;\ 9{+}11 = 20 \equiv 1 \leftarrow$ There it is!

Next, I have another trick to share with you, but we need to prove a theorem first, otherwise my trick won't make any sense.



10-3-12

Let's practice the "counting up" method of finding a modular inverse.

- What is the inverse of 4 mod 23?
- What is the inverse of 14 mod 23?
- What is the inverse of 8 mod 23?

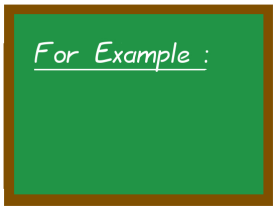
The answers will be given on Page 616 of this module.

This theorem can significantly speed up the "counting up" method. Suppose that $ab \equiv N-1$ modulo N. Then $a^{-1} \equiv N-b$ modulo N.

Suppose that $ab \equiv N-1$ modulo N. Then we can compute

$$a(N-b) = aN - ab \equiv 0 - ab \equiv 0 - (N-1) \equiv 0 - N + 1 \equiv -N + 1 \equiv 1 \bmod N$$

Since $a(N-b) \equiv 1$ modulo N, then a and $N-b$ are inverses modulo N.
In conclusion, if $ab \equiv N-1$ modulo N, then $a^{-1} \equiv N-b$ modulo N.



10-3-13

In the previous example, we were asked to compute the inverse of 11, working mod 19. This time, let's suppose we are asked to compute the inverse of 6, again working mod 19. We'll use the "counting up" method.

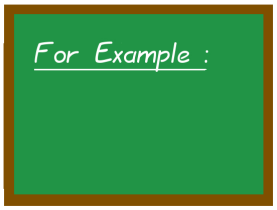
$$\begin{aligned} 6(2) &= 12 \equiv 12 \\ 6(3) &= 18 \leftarrow \text{ Hey! That's } N-1\text{, isn't it?!} \end{aligned}$$

Since $6(3) = 18 = 19 - 1$, we know that the inverse of 6 is $19 - 3 = 16$. Nonetheless, let's check our work. We'll do that in the next box.

Let's check our work from the previous box. To verify that $6^{-1} \equiv 16 \bmod 19$, we must compute $6(16)$, hoping that it equals 1. We obtain

$$6(16) = 96 = 95 + 1 = 5(19) + 1 \equiv 1 \bmod 19$$

Now you can see how powerful it is that we can stop whenever we see either 1 or $19 - 1 = 18$, when trying to find modular inverses mod 19 by counting up. If we didn't know about stopping when you get $N - 1 = 19 - 1 = 18$, then we would have had 13 additional lines of computation, because we would have to keep counting up until we had checked 16. However, because we knew about this theorem, we only had to check 2 and 3, saving us 13 lines of computation.



10-3-14

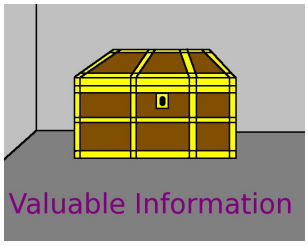
Let's try to find all the modular inverses for the integers modulo 7. We will make use of the fact that 1 is always its own inverse, and $(N - 1)$ is always its own inverse. We should use the method of "counting up" and stop whenever we see either 1 or $7 - 1 = 6$.

- We know that 1 is always its own inverse.
- For 2, we first try $2(2) = 4$, and then try $2(3) = 6 = 7 - 1$, which is good. So we know that the inverse of 2 is $7 - 3 = 4$.
- For 3, we first try $3(2) = 6 = 7 - 1$, getting lucky on our first try. So we know that the inverse of 3 is $7 - 2 = 5$. Indeed, $3(5) = 15 = 14 + 1 = 2(7) + 1 \equiv 1$.
- For 4, we already know that 4 and 2 are inverses. If you didn't remember this, you'd get $4(2) = 8 = 7 + 1 \equiv 1$ on the first try.
- For 5, we already know that 5 and 3 are inverses. If you didn't remember this, you'd get $5(2) = 10 = 7 + 3 \equiv 3$ on the first try, but $5(3) = 15 = 14 + 1 = 2(7) + 1 \equiv 1$ on the second try.
- For 6, we realize that $6 = 7 - 1$, so 6 is its own inverse.

Let's check our work from the previous box.

- To verify that $2^{-1} \equiv 4 \bmod 7$, we compute $2(4) = 8 = 7 + 1 \equiv 1$ ✓.
- To verify that $3^{-1} \equiv 5 \bmod 7$, we compute $3(5) = 15 = 14 + 1 = 2(7) + 1 \equiv 1$ ✓.
- We don't need to verify that $4^{-1} \equiv 2 \bmod 7$, because we already checked that $2^{-1} \equiv 4 \bmod 7$.
- We don't need to verify that $5^{-1} \equiv 3 \bmod 7$, because we already checked that $3^{-1} \equiv 5 \bmod 7$.
- It turns out that $(N-1)^{-1} \equiv N - 1 \bmod N$ for all integers N. However, if you wanted to check anyway, then you would compute

$$6(6) = 36 = 35 + 1 = 5(7) + 1 \equiv 1 \bmod 7 ✓$$



This next theorem will cut your work in half when you have to find all the modular inverses for some N. Suppose that $a^{-1} \equiv b$ modulo N. Then $(N-a)^{-1} \equiv (N-b)$ modulo N.

That's because

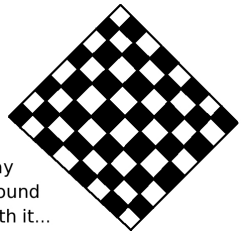
$$(N-a)(N-b) = N^2 - Nb - Na + ab \equiv 0 - 0 - 0 + ab = ab$$

Since $a^{-1} \equiv b$, we know that $ab \equiv 1$, which means that $(N-a)(N-b) \equiv 1$. Therefore, $(N-a)$ and $(N-b)$ are inverses.

In conclusion, if $a^{-1} \equiv b \bmod N$, then $(N-a)^{-1} \equiv (N-b) \bmod N$.

A good memory hook for the previous box is to think of non-zero rational numbers.

- You can think of $(N-a) \equiv -a$ and $(N-b) \equiv -b$.
- In the rational numbers, if b is the reciprocal of a, then $-b$ is the reciprocal of $-a$.
- Working mod N, if b is the modular inverse of a, then $-b$ is the modular inverse of $-a$.
- That's equivalent to (when working mod N), if b is the modular inverse of a, then $N-b$ is the modular inverse of $N-a$.



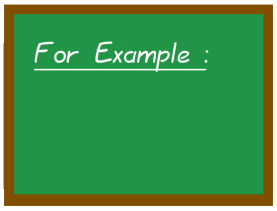
10-3-15

Using the method called "counting up," compute all the modular inverses that exist when working mod 17. However, only do this for 2, 3, 4, . . . , 8, and then I will show you a neat trick—we will use the theorem that we just proved to complete the modular inverse table.

The solution is given in the next box, but don't peek. It is good to actually perform this mental exercise.

- 1 is always its own inverse.
- $2(2) \equiv 4$, $2(3) \equiv 6$, $2(4) \equiv 8$, $2(5) \equiv 10$, $2(6) \equiv 12$, $2(7) \equiv 14$, $2(8) \equiv 16 = 17 - 1$ so we can stop early. This means $2^{-1} \equiv 17 - 8 \equiv 9$.
- $3(2) \equiv 6$, $3(3) \equiv 9$, $3(4) \equiv 12$, $3(5) \equiv 15$, $3(6) \equiv 1$. This means $3^{-1} \equiv 6$.
- $4(2) \equiv 8$, $4(3) \equiv 12$, $4(4) \equiv 16 = 17 - 1$ so we can stop early. This means $4^{-1} \equiv 17 - 4 \equiv 13$.
- $5(2) \equiv 10$, $5(3) \equiv 15$, $5(4) \equiv 3$, $5(5) \equiv 8$, $5(6) \equiv 13$, $5(7) \equiv 1$. This means $5^{-1} \equiv 7$.
- Since $3^{-1} \equiv 6$, then $6^{-1} \equiv 3$.
- Since $5^{-1} \equiv 7$, then $7^{-1} \equiv 5$.
- $8(2) = 16 = 17 - 1$, we got lucky on the first try, so we can stop early. This means $8^{-1} \equiv 17 - 2 \equiv 15$.

We will now compute the remaining modular inverses in the next box.



10-3-16

It is extremely rapid to compute the rest of the modular inverse table, because of the theorem that we proved earlier. If ab are inverses mod N, then $N - a$ and $N - b$ are inverses mod N.

- Since $17 - 8 = 9$, and since $8^{-1} \equiv 15$, then $9^{-1} \equiv 17 - 15 = 2$.
- Since $17 - 7 = 10$, and since $7^{-1} \equiv 5$, then $10^{-1} \equiv 17 - 5 = 12$.
- Since $17 - 6 = 11$, and since $6^{-1} \equiv 3$, then $11^{-1} \equiv 17 - 3 = 14$.
- Since $17 - 5 = 12$, and since $5^{-1} \equiv 7$, then $12^{-1} \equiv 17 - 7 = 10$.
- Since $17 - 4 = 13$, and since $4^{-1} \equiv 13$, then $13^{-1} \equiv 17 - 13 = 4$.
- Since $17 - 3 = 14$, and since $3^{-1} \equiv 6$, then $14^{-1} \equiv 17 - 6 = 11$.
- Since $17 - 2 = 15$, and since $2^{-1} \equiv 9$, then $15^{-1} \equiv 17 - 9 = 8$.
- Since $17 - 1 = 16$, and since $1^{-1} \equiv 1$, then $16^{-1} \equiv 17 - 1 = 16$.

Note: Of course, $N - 1$ is always its own inverse, so we didn't really need that last step.

The following remarkably useful theorem has an easy proof. Suppose that a is invertible mod N and that b is invertible mod N. Then ab is invertible mod N, and $b^{-1}a^{-1}$ is the inverse of ab.

Proof: Assume that a is invertible mod N and that b is invertible mod N. Then

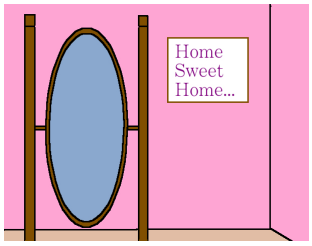
$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b \equiv b^{-1}(1)b = b^{-1}b \equiv 1$$

Since $(b^{-1}a^{-1})(ab) \equiv 1 \bmod N$, the inverse of ab is $b^{-1}a^{-1}$. ■

The theorem in the previous box can also be applied to functions. If $a(x)$ and $b(x)$ are invertible functions, then $a(b(x))$ is invertible, and its inverse is $b^{-1}(a^{-1}(x))$. Similarly, it can be applied to matrices as well. If A and B are invertible matrices (of the same size) then AB is invertible and $(AB)^{-1} = B^{-1}A^{-1}$.

In modular arithmetic, $xy \equiv yx$ mod any integer, so we can write either $b^{-1}a^{-1}$ or $a^{-1}b^{-1}$, as they are the same thing. However, for functions and for matrices, the order does matter, and we should take pains to get it correctly.

The reversal of the order for functions and matrices can be easily remembered as follows. In the morning, when you get dressed, you put your socks on first (a), and your shoes on second (b). However, when you undress, the shoes come off first (b^{-1}), and then your socks come off (a^{-1}), reversing the order. For these reasons, many instructors use the term "socks-shoes theorem" to describe the equation $(AB)^{-1} = B^{-1}A^{-1}$.

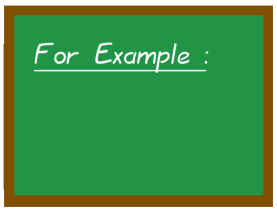


A Pause for Reflection...

Many theorems, formulas, and methods in mathematics are the hyphenated last names of two (or more) mathematicians. For example, consider the Cauchy–Schwartz theorem, the Abel–Ruffini theorem, the Newton–Cotes formulas for numerical integration, and the Newton–Raphson method for numerically finding roots of differentiable functions. (If you are curious, the following URL gives a list of theorems that are also the names of articles on Wikipedia.) `https://en.wikipedia.org/wiki/List_of_theorems`

Once in the Spring of 2016,while teaching MSCS-580: *Cryptography* at UW Stout one of my students, Jared Siverling, referred to the socks-shoes theorem. I knew the theorem, of course, because it is very central in abstract algebra. However, I didn't know this funny name for it. Therefore, I thought there must be two mathematicians, perhaps Zocks and Shoos, and I thought it was the Zocks-Shoos theorem.

Some confusion and much laughter ensued, once the name of the theorem was explained.

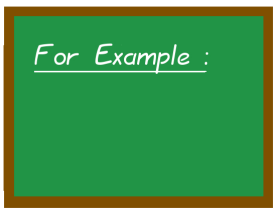


10-3-17

If you're curious how the "socks-shoes theorem" can be used to help us find modular inverses with less effort, suppose that working mod some N, we discover that 2, 3, and 5 are all invertible, and that their inverses mod N are x, y, and z. What can we conclude?

- We know that $2(3) = 6$ is invertible mod N, and the inverse of 6 is xy mod N.
- We know that $2(5) = 10$ is invertible mod N, and the inverse of 10 is xz mod N.
- We know that $3(5) = 15$ is invertible mod N, and the inverse of 15 is yz mod N.

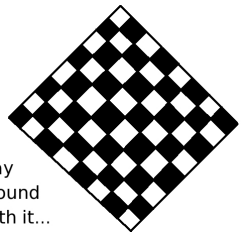
Yet, we actually know more than that, as we'll see in the next box.



10-3-18

We can actually do better than the previous example. Continuing with all the data from the previous box...

- Since $4 = (2)(2)$, we know that 4 is invertible mod N, and that the inverse of 4 mod N is x^2.
- Furthermore, since $9 = (3)(3)$, we know that 9 is invertible mod N, and that the inverse of 9 mod N is y^2.
- Similarly, since $25 = (5)(5)$, we know that 25 is invertible mod N, and that the inverse of 25 mod N is z^2.



10-3-19

Let's see if you can generalize the results of the previous box.

- What do we learn if we plug in $a = c$ and $b = c$ into the socks-shoes theorem?
- What do we learn if we plug in $a = c^2$ and $b = c$ into the socks-shoes theorem, and the answer to the previous sub-problem?
- What do we learn if we plug in $a = c^3$ and $b = c$ into the socks-shoes theorem, and the answer to the previous sub-problem?
- What do we learn if we plug in $a = c^4$ and $b = c$ into the socks-shoes theorem, and the answer to the previous sub-problem?

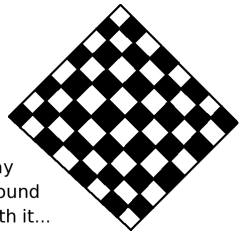
To maintain the flow of the conversation, I'm going to put the solutions to this checkerboard box immediately below, and not at the end of the module.

Here are the solutions to question of the previous box.

- What do we learn if we plug in $a = c$ and $b = c$ into the socks-shoes theorem?
  [Answer: $(c^2)^{-1} = (c^{-1})^2$.]
- What do we learn if we plug in $a = c^2$ and $b = c$ into the socks-shoes theorem, and the answer to the previous sub-problem?
  [Answer: $(c^3)^{-1} = (c^{-1})^3$.]
- What do we learn if we plug in $a = c^3$ and $b = c$ into the socks-shoes theorem, and the answer to the previous sub-problem?
  [Answer: $(c^4)^{-1} = (c^{-1})^4$.]
- What do we learn if we plug in $a = c^4$ and $b = c$ into the socks-shoes theorem, and the answer to the previous sub-problem?
  [Answer: $(c^5)^{-1} = (c^{-1})^5$.]

It is not hard to prove, using mathematical induction, that $(c^n)^{-1} = (c^{-1})^n$. This is why we will abbreviate both $(c^n)^{-1}$ and $(c^{-1})^n$ with c^{-n}. That's permissible because (for any invertible c), we know that

$$(c^n)^{-1} = (c^{-1})^n$$

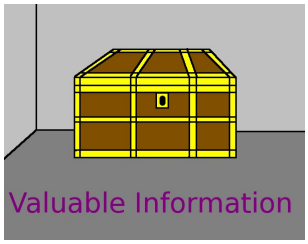


10-3-20

The following exercise might sound as though it is going to be very tedious, but actually it is a beautiful example of how we can avoid work by being clever. I want you to find all the modular inverses working mod 21. You could do this by counting up.

As it turns out, you only need to find the inverses of 2 and of 5 by counting up. For every other case, some use of some theorem will save you the effort of counting up. Several theorems from this module will play a role.

My solution will begin on Page 617 of this module.



Let's summarize the ways in which we can compute a modular inverse.

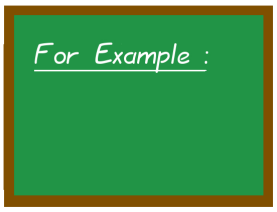
- We can use technology, such as Maple, MATLAB, Mathematica, MAGMA, or Sage. However, we then would wonder about how the technology manages to find the inverse.
- If you're given a Cayley table, you could try searching for 1s in the Cayley table, as explained earlier. However, even for $N = 101$, the Cayley table is too large to be of practical use, so this is only an option for very small moduli.
- You might be given a modular inverse table. As we saw earlier, for moderately large moduli, the modular inverse table might be of tolerable size, but the full Cayley table might be too large to be practical. For cryptographic sized moduli, having hundreds of digits, your computer would not have enough memory to store such a table.
- We have learned the method called "counting up," looking for 1 or $N - 1$, as explained earlier.

As it comes to pass, there is another method, and I'll explain that in the next box.

If we have (or can find) an equation of the form $k(b) + c(N) = 1$ in the ordinary integers, then we can conclude $b^{-1} \equiv k \bmod N$. This is not obvious, and requires some explanation. We'll explain it in the next example.

Equations of the form $k(b) + c(N) = 1$ are sometimes called Bezout equations. Bezout showed how to use equations of that type to solve all sorts of problems about the integers, including the solving of Diophantine equations. (Those are equations where we only care about integer-valued solutions, even though there might be many easy-to-find real-valued solutions.) Actually, Bezout's real contribution was showing how to do this when b and N are polynomials, not integers, and how to use this to solve some very advanced problems that eventually led to a topic called elimination theory. The integer-only version was already proven by Claude Gaspard Bachet de Méziriac (1581–1638).

The Extended Euclidean Algorithm can always provide us with an equation of the form $k(b) + c(N) = 1$ whenever b is invertible mod N. That's how computer-algebra systems such as Maple, MATLAB, Mathematica, MAGMA, or Sage will compute modular inverses.



10-3-21

It happens to be true (in the ordinary integers) that $(-3)(31) + (2)(47) = 1$. Using this information, compute the inverse of 31 mod 47.

Keep in mind, the above equation takes place in the ordinary integers, not in modular arithmetic. So we might ask ourselves what $(-3)(31) + (2)(47)$ comes out to, working mod 47?

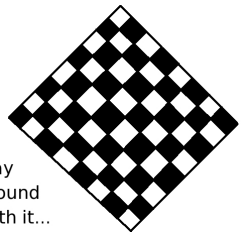
Well, we certainly can take that equation, and apply the rule in modular arithmetic that we can subtract the modulus (in this case, 47) at any moment. Of course, while doing that, we must change the $=$ into $\equiv$.

The -3 is replaced by $-3 + 47 = 44$; the 31 can remain unchanged; the 2 can remain unchanged; the 47 is replaced by 0; the 1 can remain unchanged. We have

$$\begin{aligned} (-3)(31) + (2)(47) &= 1 \\ (44)(31) + (2)(0) &\equiv 1 \end{aligned}$$

Because we know that $(44)(31) \equiv 1$, we know that $31^{-1} \equiv 44 \bmod 47$. Let's check this with

$$(31)(44) = 1364 = 1363 + 1 = 29(47) + 1 \equiv 1 \bmod 47$$

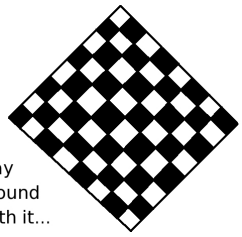


10-3-22

Let's practice with the technique of the previous box. The idea is that given some a and some N, the Extended Euclidean Algorithm (which I haven't shown you yet) will find x and y such that $xa + yN = 1$ in the ordinary integers. Such an equation is sometimes called a Bezout equation for a and N. Now imagine that you're programming a computer-algebra system like Sage or Maple, and that a colleague of yours has successfully coded the Extended Euclidean Algorithm. What we're doing here is verifying that we can use the output of that algorithm to find modular inverses.

- It happens to be true, in the ordinary integers, that $(-11)(17) + (4)(47) = 1$. What is $17^{-1} \bmod 47$?
- It happens to be true, in the ordinary integers, that $(41)(39) + (-34)(47) = 1$. What is $39^{-1} \bmod 47$?
- Using some facts we learned before, can you tell me the inverse of 36 mod 47?
- Using some facts we learned before, can you tell me the inverse of 41 mod 47?

The answers will be given on Page 619 of this module.

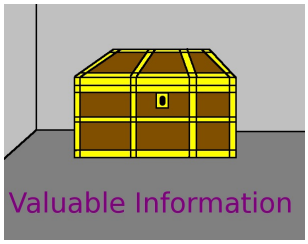


10-3-23

Using some of the theorems we studied earlier, and the information of the previous box, tell me the following modular inverses:

- What is the inverse of 30 mod 47?
- What is the inverse of 6 mod 47?
- What is the inverse of 11 mod 47?
- What is the inverse of 8 mod 47?

The answers will be given on Page 619 of this module.



We are now ready to generalize this technique. Suppose that $k(b) + c(N) = 1$ in the ordinary integers. (In other words, you know the numerical value of all four variables: b, c, k, and N.) Then

$$k^{-1} \equiv b \bmod N \text{ as well as } b^{-1} \equiv k \bmod N$$

This is easy to prove: if $k(b) + c(N) = 1$ then $k(b) = 1 - c(N)$. Reducing mod N, we obtain $k(b) \equiv 1 \bmod N$, which is another way of saying that k and b are inverses mod N. ■

(Of course, we might want to add or subtract N a few times, to put either k or b into the usual $\{0, 1, 2, 3, \ldots, N-1\}$ range.)

I'd like to prove a theorem now. This theorem is useful in its own right, but it will become a building block in a much more important theorem.

In the next box, we will prove that if there exists some prime integer p, such that p divides b and p divides N, then b is not invertible mod N.

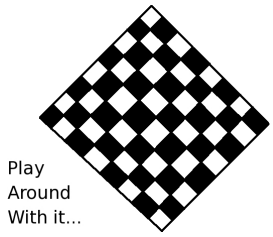
Let b and N be positive integers. Suppose there exists some prime integer p, such that p divides b and p divides N.

Assume b is invertible mod N. Then there exists some c such that $bc \equiv 1 \bmod N$. That implies there is some integer w, such that $bc = 1 + wN$, or equivalently $bc - wN = 1$.

Since p divides b and p divides N, then p divides bc and p divides wN. Thus p divides $bc - wN$, the difference of bc and wN.

However, because $bc - wN = 1$ this means that p divides 1, or equivalently that $1/p$ is an integer. That's absurd.

Therefore, our assumption (that b is invertible mod N) must be false. In conclusion, if there exists some prime integer p, such that p divides b and p divides N, then b is not invertible mod N.



10-3-24

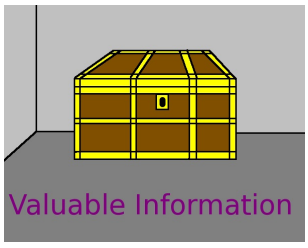
Based on the previous box, tell me why I was certain (on Page 604) that no even integer has an inverse mod 26?

My answer will be given on Page 620.

The contrapositive of the theorem that we just proved a few boxes ago is literally "if b is invertible mod N, then there does not exist any prime integer p such that p divides b and p divides N."

Of course, if there does not exist any prime integer p such that p divides b and p divides N, then the greatest common divisor of b and N is 1. We would write this as $\gcd(b, N) = 1$.

The situation of two integers having a gcd of 1 happens so often that we have a compressed way of writing it, with a single word. I'll discuss that in the next box.



For any integers x and y, we say "x is coprime to y" if and only if $\gcd(x, y) = 1$.

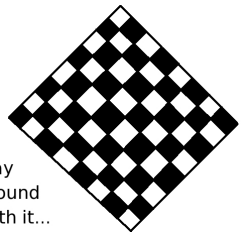
Of course, since the set of common divisors of x and y is the same thing as the set of common divisors for y and x, we know that $\gcd(x, y) = \gcd(y, x)$. This further implies that "x is coprime to y if and only if y is coprime to x."

Among other things, we can rewrite the contrapositive from the previous box much more concisely by saying "if b is invertible mod N, then b and N are coprime."

It might be very useful for us to explore the converse of that concise statement from the previous box.

Can we prove that "if b and N are coprime, then b is invertible mod N?" If we can prove that, then we can write the grand conclusion, that b and N are coprime if and only if b is invertible mod N. That would be enormously useful, because we could easily tell which members of the "world mod N" are invertible.

We will explore that proof in the next few boxes. First, let's practice with the concept of two integers being coprime, using some computational exercises.



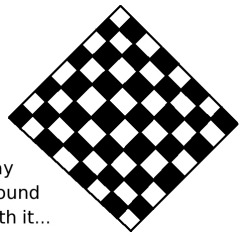
10-3-25

In this box and the next, you will find a few computational exercises to review your knowledge of factorization and the gcd, and you will explore the notion of two integers being coprime.

If you need review about gcds or prime factorizations, consider rereading Module 1.6: "Set Theory meets Number Theory." The discussion of the gcd begins on Page 208.

- What is the prime factorization of 26?
- What is the prime factorization of 169?
- Are 26 and 169 coprime? Why or why not?
- What is the prime factorization of 100?
- Are 26 and 100 coprime? Why or why not?

The answers are given on Page 620 of this module.

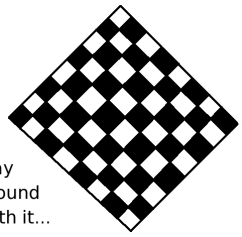


10-3-26

Continuing with the previous box, here are a few more questions about factorization and coprimality.

- Are 100 and 169 coprime? Why or why not?
- What is the prime factorization of 75?
- Are 26 and 75 coprime? Why or why not?
- Are 75 and 169 coprime? Why or why not?
- Are 75 and 100 coprime? Why or why not?

The answers are given on Page 620 of this module.

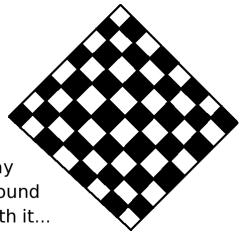


10-3-27

Continuing with the previous two boxes, here are still more questions about factorization and coprimality

- What is the prime factorization of 72?
- Are 26 and 72 coprime? Why or why not?
- Are 72 and 169 coprime? Why or why not?
- Are 72 and 100 coprime? Why or why not?
- Are 72 and 75 coprime? Why or why not?

The answers are given on Page 621 of this module.



10-3-28

Here's a question. Think about it a bit, and then commit to an answer by writing it on a piece of scrap paper. Suppose a is coprime to b and b is coprime to c. Is it always the case that a is coprime to c?

The answer will be given on Page 621 of this module.

Some books will say "a and b are relatively prime," instead of saying "a and b are coprime." Personally, I dislike the term "relatively prime." It sounds to the ear like "kind of prime," "sort of prime," or "a little bit prime." Either an integer is prime, or not. To me it sounds like saying someone is "kind of pregnant," "sort of pregnant," or "a little bit pregnant."

Therefore, this book will use the term "coprime."

We need another theorem before we can continue toward our main objective.

Suppose the gcd of b and N were some integer g with $g > 1$. Every integer greater than 1 is divisible by some prime, so let p be a prime dividing g. Since g is the greatest common divisor of b and N, it must be a common divisor of b and N. This means that g divides b and g divides N.

Since p divides g and g divides N, we know p divides N. Likewise, since p divides g and g divides b, we know that p divides b. Therefore, p divides both b and N. This means that b and N are not coprime, since there exists a prime integer dividing both b and N.

In conclusion, "if the gcd of b and N is some integer $g > 1$, b and N are not coprime." The contrapositive of that statement is "if b and N are coprime, then the gcd of b and N is 1."

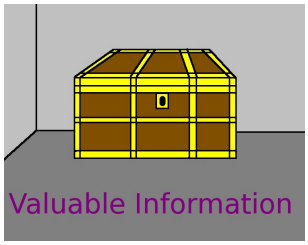
We need one more theorem.

For any integers r and s, if $\gcd(r, s) = g$, then there exist integers x and y such that $xr + ys = g$.

This is often called Bezout's theorem, or sometimes it is one clause in a very large theorem named for Bezout.

Suppose that b is coprime to N. This means that $\gcd(b, N) = 1$. By Bezout's theorem, there are integers $xb + yN = 1$. That implies $xb = 1 - yN$. Reducing mod N, we obtain $xb \equiv 1 - y0 \bmod N$, or more simply $xb \equiv 1 \bmod N$. Thus x and b are inverses mod N. This also implies that b is invertible mod N.

In conclusion, if b is coprime to N then b is invertible mod N. That allows us to make the grand conclusion, given in the next box.



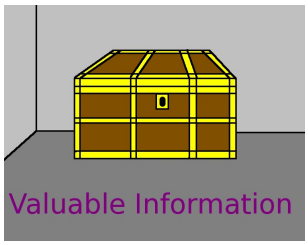
An integer b is invertible modulo N if and only if b is coprime to N.

In the special case when working mod p, for some prime p, we can say even more. Since the only positive integer divisors of a prime number p are 1 and p, we know that there are no integers x in the set

$$\{1, 2, 3, 4, \ldots, p-2, p-1\}$$

that have $\gcd(x, p) \neq 1$.

That means all such x are invertible mod p.



For any prime p, all non-zero members of the integers mod p are invertible mod p.
(Equivalently, 0 is the only non-invertible member of the integers mod p.)

This module is now complete. The solutions to various exercises now follow.

Here are the solutions to the five true/false questions from Page 597 of this module.

1. False, because $(48)(41) = 1968 = 1920 + 48 = 20(96) + 48 \equiv 48 \not\equiv 1 \bmod 96$. Thus, 41 and 48 are not inverses of each other mod 96.
2. True, because $17(5) = 85 = 84 + 1 = 4(21) + 1 \equiv 1 \bmod 21$. Thus 17 and 5 are inverses mod 21.
3. True, because $7(36) = 252 = 251 + 1 \equiv 1 \bmod 251$. Thus 7 and 36 are inverses mod 251.
4. False, because $(11)(17) = 187 = 185 + 2 = 5(37) + 2 \equiv 2 \not\equiv 1 \bmod 37$. Thus 11 and 17 are not inverses of each other mod 37.
5. False, because $13(61) = 793 = 750 + 43 = 10(75) + 43 \equiv 43 \not\equiv 1 \bmod 75$. Thus 13 and 61 are not inverses of each other mod 75.

Here are the solutions to the four equations mod 97 that I challenged you to solve, back on Page 601.

- $92x + 60 \equiv 17x + 31 \bmod 97$ [Answer: $x \equiv 41$.]
- $69x + 89 \equiv 90x + 3 \bmod 97$ [Answer: $x \equiv 78$.]
- $58x + 54 \equiv 69x + 43 \bmod 97$ [Answer: $x \equiv 1$.]
- $59x + 78 \equiv 24x + 55 \bmod 97$ [Answer: $x \equiv 52$.]

Here is the solution to the problem where you were asked to use the method of "finding 1s" in the Cayley table (from Page 604 of this module) to find all the modular inverses mod 26.

- Since $1(1) = 1$, we know that 1 is its own inverse.
- Since $3(9) = 1$, we know that 3 and 9 are inverses.
- Since $5(21) = 1$, we know that 5 and 21 are inverses.
- Since $7(15) = 1$, we know that 7 and 15 are inverses.
- We don't need to check 9, because we already know that 3 and 9 are inverses.
- Since $11(19) = 1$, we know that 11 and 19 are inverses.
- There is no k such that $13k = 1$, so we know 13 is not invertible.
- We don't need to check 15, because we already know that 7 and 15 are inverses.
- Since $17(23) = 1$, we know that 17 and 23 are inverses.
- We don't need to check 19, because we already know that 11 and 19 are inverses.
- We don't need to check 21, because we already know that 5 and 21 are inverses.
- We don't need to check 23, because we already know that 17 and 23 are inverses.
- Since $25(25) = 1$, we know that 25 is its own inverse.

As you can see, I skipped all the even integers. Do you know why? Think about it for a moment. I'll give the reason in the next box.

Because 26 is even, any even k will at least have 2 as a common divisor of k and 26. That means even ks are definitely not invertible. That means we only need to check odd integers, not even integers.

This is a special case of the general rule explained on Page 614.

Here are the solutions, from Page 604, where I asked you to practice the method of "counting up" to invert some numbers mod 23.

- What is the inverse of 4 mod 23?
  [Answer: 6, because $(4)(6) = 24 = 23 + 1 \equiv 1 \bmod 23$.]
- What is the inverse of 14 mod 23?
  [Answer: 5, because $(14)(5) = 70 = 69 + 1 = 3(23) + 1 \equiv 1 \bmod 23$.]
- What is the inverse of 8 mod 23?
  [Answer: 3, because $(8)(3) = 24 = 23 + 1 \equiv 1 \bmod 23$.]

Here is my solution to the problem of finding all the modular inverses for working mod 21, as I asked you to do on Page 609. First, we should find the modular inverses of 2, 3, 4, ..., 10..

- Recall, 1 is always its own inverse.
- We count up to $2(10) = 20 = 21 - 1 \equiv -1$ so $21 - 10 = 11$ is the inverse of 2.
- Next, 3 is a divisor of 21, so $\gcd(3, 21) = 3$. Because 3 is not coprime to 21, there is no inverse of 3.
- Happily, $4 = 2^2$, so $4^{-1} = (2^2)^{-1} = (2^{-1})^2 = 11^2 = 121 = 105 + 16 = 5(21) + 16 \equiv 16$.
- We count up to $5(4) = 20 = 21 - 1 \equiv -1$ so $21 - 4 = 17$ is the inverse of 5.

We will continue in the next box.

Continuing with the previous box...

- Next, since 3 divides 6 and 3 divides 21, we have that 3 is a common divisor of 6 and 21, so they are not coprime. Thus there is no inverse of 6.
- Of course, 7 is a divisor of 21, so $\gcd(7, 21) = 7$. Because 7 is not coprime to 21, there is no inverse of 7.
- Since $8 = 2^3$, we know that $8^{-1} = (2^3)^{-1} = (2^{-1})^3 \equiv 11^3 = 1331 = 1323 + 8 = 63(21) + 8 \equiv 8$.
- As we saw for 6, for 9 we can say that since 3 divides 9 and 3 divides 21, we have that 3 is a common divisor of 9 and 21, so they are not coprime. Therefore, there is no inverse of 9.
- For 10, we do not have to count up. Since $10 = (2)(5)$, we can use the socks-shoes theorem and say that

$$10^{-1} = (2(5))^{-1} = 2^{-1}(5^{-1}) = 11(17) = 187 = 168 + 19 = 8(21) + 19 \equiv 19$$

- At this point, since we found the inverses of all the as such that $1 \leq a \leq 10$, then the inverses of the $N - a$s can be found using $(N - a)^{-1} \equiv N - a^{-1} \bmod N$.

We will continue in the next box.

Continuing with the previous two boxes...

- You might recall that the inverse of 2 was 11. Thus the inverse of 11 is 2. If you didn't recall that, then since $11 = 21 - 10$, we can write the following:

$$11^{-1} \equiv (21 - 10)^{-1} \equiv 21 - 10^{-1} \equiv 21 - 19 \equiv 2$$

- Since 3 divides 12 and 3 divides 21, we know that 12 and 21 are not coprime, so there is no inverse of 12.
- Since $13 = 21 - 8$, $13^{-1} \equiv (21 - 8)^{-1} \equiv 21 - 8^{-1} \equiv 21 - 8 \equiv 13$.
- Since 7 divides 14 and 7 divides 21, we know that 14 and 21 are not coprime, so there is no inverse of 14.

We will continue in the next box.

Continuing with the previous three boxes...

- Since 3 divides 15 and 3 divides 21, we know that 15 and 21 are not coprime, so there is no inverse of 15.
- You might recall that the inverse of 4 was 16. Thus the inverse of 16 is 4. If you didn't recall that, then since $16 = 21 - 5$, we can write the following:

$$16^{-1} \equiv (21-5)^{-1} \equiv 21 - 5^{-1} \equiv 21 - 17 \equiv 4$$

- Since we just used the fact that the inverse of 5 is 17, we should note that the inverse of 17 is 5.
- Since 3 divides 18 and 3 divides 21, we know that 18 and 21 are not coprime, so there is no inverse of 18.
- Since 19 is the inverse of 10, we know that 10 is the inverse of 19.
- For $20 = 21 - 1$, we can either use the fact that $(N-1)$ is always its own inverse mod N, or we can compute

$$20^{-1} = (21-1)^{-1} \equiv 21 - 1^{-1} = 21 - 1 = 20$$

It is good in mathematics to be very thorough, and to check one's work. We'll do that in the next box.

We will now check the modular inverses from the previous four boxes.

- We don't have to check that 1 is its own inverse, because $(1)(1) = 1$ always.
- To check that 2 and 11 are inverses: $(2)(11) = 22 = 21 + 1 \equiv 1$.
- To check that 4 and 16 are inverses: $(4)(16) = 64 = 63 + 1 = 3(21) + 1 \equiv 1$.
- To check that 5 and 17 are inverses: $(5)(17) = 85 = 84 + 1 = 4(21) + 1 \equiv 1$.
- To check that 8 is its own inverse: $8(8) = 64 = 63 + 1 = 3(21) + 1 \equiv 1$.
- To check that 10 and 19 are inverses: $(10)(19) = 190 = 189 + 1 = 9(21) + 1 \equiv 1$.
- To check that 13 is its own inverse: $13(13) = 169 = 168 + 1 = 8(21) + 1 \equiv 1$.
- To check that 20 is its own inverse: $20(20) = 400 = 399 + 1 = 19(21) + 1 \equiv 1$.

Here is the answer to the question from Page 611, where we were given two Bezout equations, and were asked to use them to find some modular inverses, mod 47.

- It happens to be true, in the ordinary integers, that $(-11)(17) + (4)(47) = 1$. What is 17^{-1} mod 47?
  [Answer: $-11 \equiv (-11 + 47) = 36 \bmod 47$, so $17^{-1} \equiv 36 \bmod 47$.]
- It happens to be true, in the ordinary integers, that $(41)(39) + (-34)(47) = 1$. What is 39^{-1} mod 47?
  [Answer: $39^{-1} \equiv 41 \bmod 47$.]
- Using some facts we learned before, can you tell me the inverse of 36 mod 47?
  [Answer: Since $17^{-1} \equiv 36 \bmod 47$, we know $36^{-1} \equiv 17 \bmod 47$, by the reciprocity of modular inverses.]
- Using some facts we learned before, can you tell me the inverse of 41 mod 47?
  [Answer: Since $39^{-1} \equiv 41 \bmod 47$, we know $41^{-1} \equiv 39 \bmod 47$, by the reciprocity of modular inverses.]

Here are the answers from the question on Page 611, where we used some modular inverses, mod 47, to compute the modular inverses of other numbers, mod 47.

- What is the inverse of 30 mod 47?
  [Answer: Since $47 - 30 = 17$, and $17^{-1} \equiv 36$, we know that
  $$30^{-1} \equiv (-17)^{-1} \equiv -17^{-1} \equiv -36 \equiv 11$$
  thus $30^{-1} = 11$.]
- What is the inverse of 6 mod 47?
  [Answer: Since $47 - 6 = 41$, and $41^{-1} \equiv 39$, we know that
  $$6^{-1} \equiv (-41)^{-1} \equiv -41^{-1} \equiv -39 \equiv 8$$
  thus $6^{-1} = 8$.]
- What is the inverse of 11 mod 47? [Answer: It is possible that you would use the reciprocity of modular inverses, knowing that $30^{-1} = 11 \bmod 47$, to simply state that $11^{-1} = 30 \bmod 47$. Otherwise, here is another approach: Since $47 - 11 = 36$, and $36^{-1} \equiv 17$, we know that
  $$11^{-1} \equiv (-36)^{-1} \equiv -36^{-1} \equiv -17 \equiv 30$$
  thus $11^{-1} = 30$.]
- What is the inverse of 8 mod 47? [Answer: It is possible that you would use the reciprocity of modular inverses, knowing that $6^{-1} = 8 \bmod 47$, to simply state that $8^{-1} = 6 \bmod 47$. Otherwise, here is another approach: Since $47 - 8 = 39$, and $39^{-1} \equiv 41$, we know that
  $$8^{-1} \equiv (-39)^{-1} \equiv -39^{-1} \equiv -41 \equiv 6$$
  thus $8^{-1} = 6$.]

Here is my answer to the question (from Page 612) about why I was certain that "No even integer has an inverse mod 26."

Suppose an integer c is even. Then c is divisible by 2. Note that 26 is also divisible by 2. Therefore, the prime 2 divides both c and 26. Earlier, we proved that if there exists some prime integer p, such that p divides b and p divides N, then b is not invertible mod N. Therefore, c is not invertible mod 26.

Here are the solutions to the first checkerboard box of questions reviewing coprimality and prime factorization, from Page 613.

- What is the prime factorization of 26? [Answer: $26 = 2(13)$.]
- What is the prime factorization of 169? [Answer: $169 = (13)^2$.]
- Are 26 and 169 coprime? Why or why not? [Answer: No. Both 26 and 169 are divisible by 13.]
- What is the prime factorization of 100? [Answer: $100 = 2^2(5)^2$.]
- Are 26 and 100 coprime? Why or why not?
  [Answer: No. Both 26 and 100 are divisible by 2.]

Here are the solutions to the second checkerboard box of questions reviewing coprimality and prime factorization, from Page 613.

- Are 100 and 169 coprime? Why or why not? [Answer: Yes. Because 13 is the only prime that divides 169, and 13 does not divide 100.]
- What is the prime factorization of 75? [Answer: $75 = 3(5)^2$.]
- Are 26 and 75 coprime? Why or why not? [Answer: Yes. The only primes dividing 26 are 2 and 13, neither of which divides 75.]
- Are 75 and 169 coprime? Why or why not? [Answer: Yes. The only prime dividing 169 is 13, and 13 does not divide 75.]
- Are 75 and 100 coprime? Why or why not? [Answer: No. Both 75 and 100 are divisible by 5.]

Here are the solutions to the third checkerboard box of questions reviewing coprimality and prime factorization, from Page 613.

- What is the prime factorization of 72? [Answer: $72 = 2^3(3)^2$.]
- Are 26 and 72 coprime? Why or why not?
  [Answer: No. Both 26 and 72 are divisible by 2.]
- Are 72 and 169 coprime? Why or why not?
  [Answer: Yes. The only prime dividing 169 is 13, and 13 does not divide 72.]
- Are 72 and 100 coprime? Why or why not?
  [Answer. No. Both 72 and 100 are divisible by 2.]
- Are 72 and 75 coprime? Why or why not?
  [Answer: No. Both 72 and 75 are divisible by 3.]

On Page 613 of this module, I asked you to consider the following question: "Suppose a is coprime to b and b is coprime to c. Is it always the case that a is coprime to c?"

The answer is no. There are infinitely many counter-examples. I will present only one.

Consider $a = 2$, $b = 3$, and $c = 4$. Clearly, 2 and 3 are coprime, as the only positive integer which divides them both is 1. Likewise, 3 and 4 are coprime, for the same reason.

However, 2 divides both 2 and 4, so $\gcd(2, 4) = 2$ and we conclude that 2 is not coprime to 4.