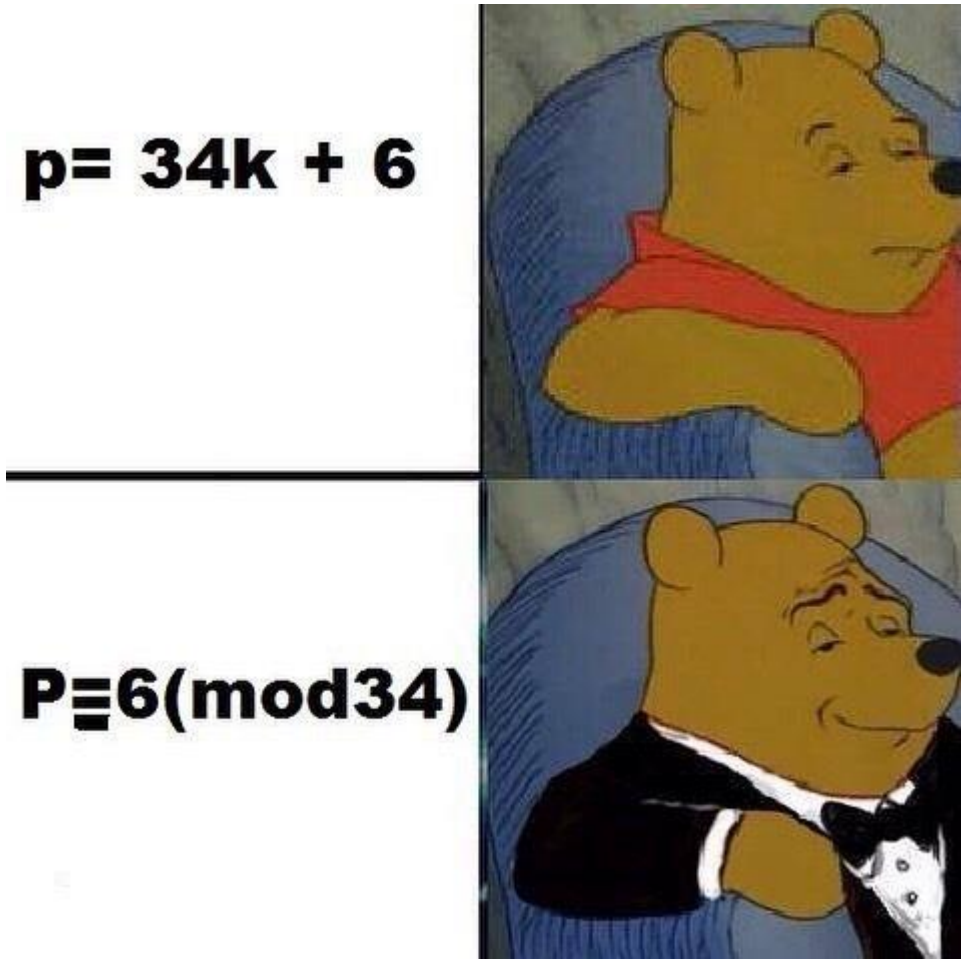


Number Theory

CSE 311: Foundations of Computing I
Lecture 9

Announcements

- HW2 solutions are at the front, grades will be published tonight
- HW3 is due Wednesday at 11:59 pm

Proof Style

We use predicate logic to make the proof claim very precise. However, please write the actual proofs in English, not logic!

E.g. for all integers x, if x is odd then $x + 1$ is even.

Good: Let x be arbitrary. Suppose x is odd. Then $x = 2k + 1$ for some integer k …

Bad: Let x be arbitrary. Suppose $\mathbf{Odd}(x)$. Then $\exists k\ (x = 2k + 1)$…

Proof Tip: Without Loss of Generality

If you're writing a proof with 2+ **very similar** cases, you can use the phrase:

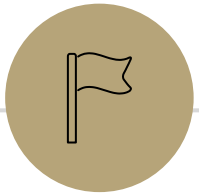
Assume without loss of generality that we are in Case 1….

For example:

Case 1: x is red and y is blue, we want to show $x + y$ is purple.

Case 2: x is blue, y is red, we want to show $x + y$ is purple.

In my proof: "Observe that there are two cases. We can assume without loss of generality that x is red and y is blue"



Number Theory: Motivation

Number Theory

- Branch of mathematics that deals with the properties and relationships of numbers 🤡
  - E.g. can we efficiently test if an integer is prime?
  - E.g. can we efficiently factor an integer?

- Many significant applications in computing
  - Cryptography & Security
  - Hashing

- Playground for practicing proof-writing

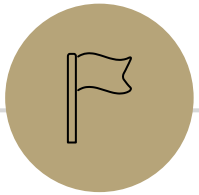
Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

Modular Arithmetic

```
public class Test {
        final static int SEC_IN_YEAR = 365*24*60*60;
        public static void main(String args[]) {
                System.out.println( “I will be alive for at least ” +  SEC_IN_YEAR * 100 + “ seconds.” );
        }
}
```

```
I will be alive for -1141367296 seconds.
```



Divisibility

Divisibility

Definition:

_____

_____.

Informally: _____

Examples: _____

Divisibility

Definition
$a \mid b \coloneqq \exists k \in \mathbb{Z}\,(b = ka)$

Which of these is true?

$5 \mid 1$ $\quad$ $25 \mid 5$ $\quad$ $7 \mid 0$ $\quad$ $-2 \mid 4$

$1 \mid 5$ $\quad$ $5 \mid 25$ $\quad$ $0 \mid 7$ $\quad$ $4 \mid -2$

Division Theorem

Division Theorem:

_____

_____.

Division Theorem

Division Theorem:

For any integer a and positive integer d, there exist unique integers q, r with $0 \leq r < d$ such that $a = qd + r$.

q is referred to as the _____

r is referred to as the _____

Division Theorem

Division Theorem:

For any integer a and positive integer d, there exist unique integers q, r with $0 \leq r < d$ such that $a = qd + r$.

In Java, q is the result of the operation _____

In Java, r is the result of the operation _____

Warning
When dealing with negative numbers, Java's % may behave differently!

The mod (%) operator

Division Theorem
$a = qd + r$ with $0 \leq r < d$

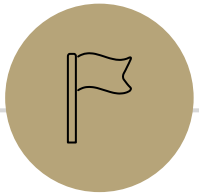
- The % operator is often referred to as "mod"
- $a \,\%\, d$ returns the remainder r when you divide a by d

$22 \,\%\, 5 =$

$25 \,\%\, 5 =$

$0 \,\%\, 5 =$

$-1 \,\%\, 4 =$

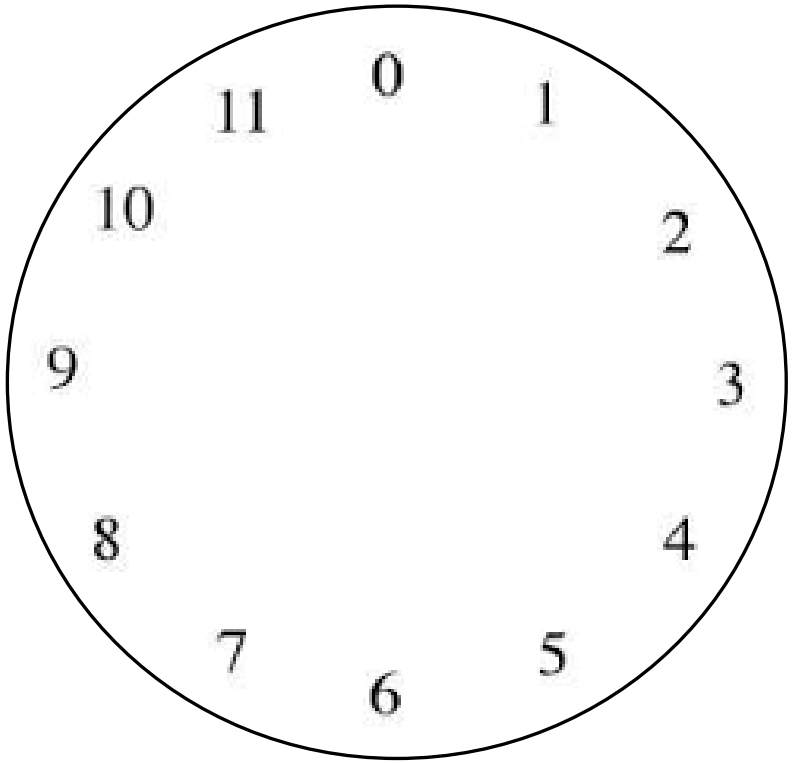


Modular Arithmetic

Modular Arithmetic: Like a Clock

Imagine you can only represent numbers $0, \ldots, 11$. We call this "arithmetic mod 12".

What's $8 + 7$?

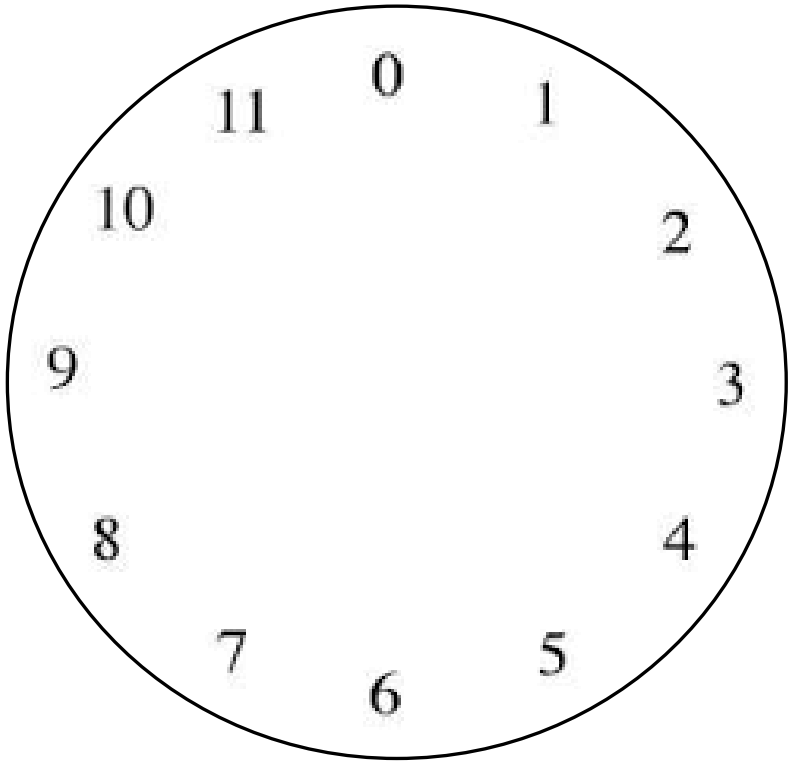


Observation
The solution is $a \% 12$.

Modular Arithmetic: Like a Clock

Imagine you can only represent numbers $0, \ldots, 11$. We call this "arithmetic mod 12".

What's $3 - 5$?

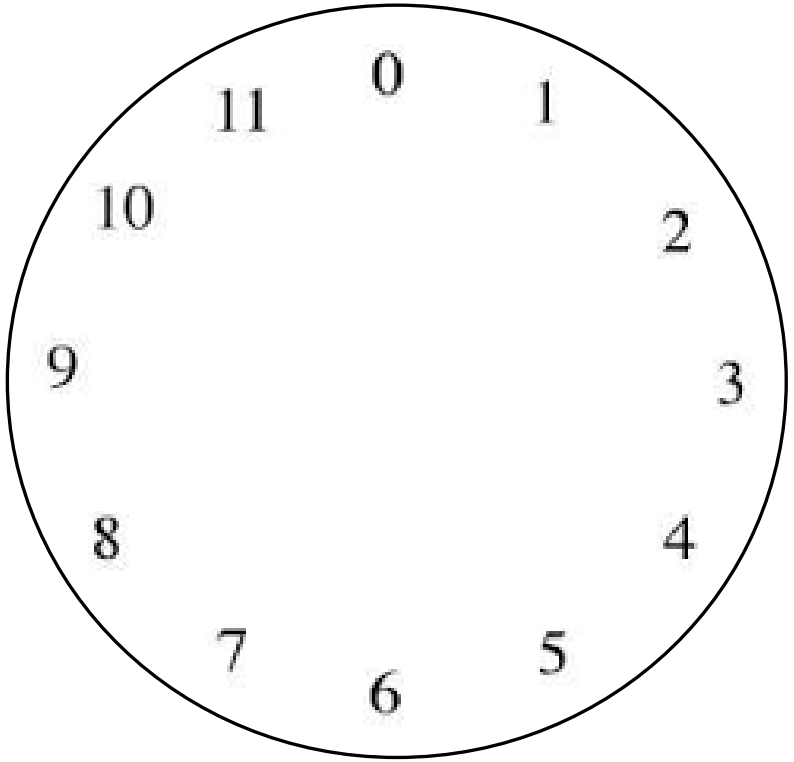


Observation
The solution is $a \% 12$.

Modular Arithmetic: Like a Clock

Imagine you can only represent numbers $0, \ldots, 11$. We call this "arithmetic mod 12".

What's $3 \cdot 7$?

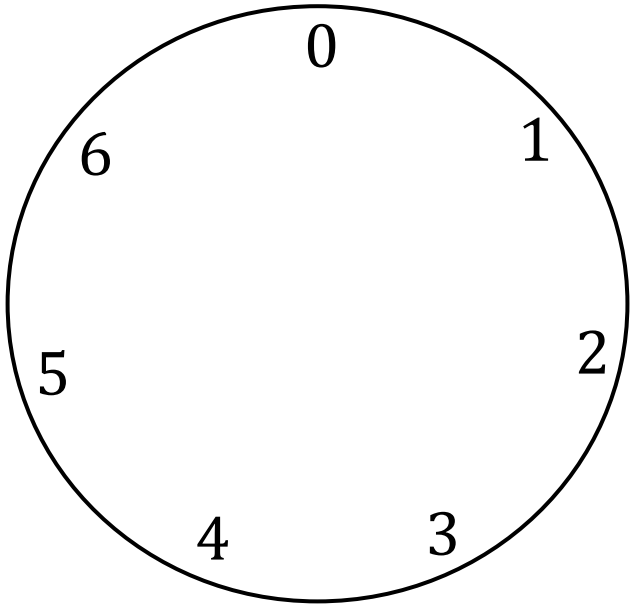


Observation
The solution is $a \,\%\, 12$.

Modular Arithmetic: Generalizing

We can extend modular arithmetic to clocks of any positive integer size.

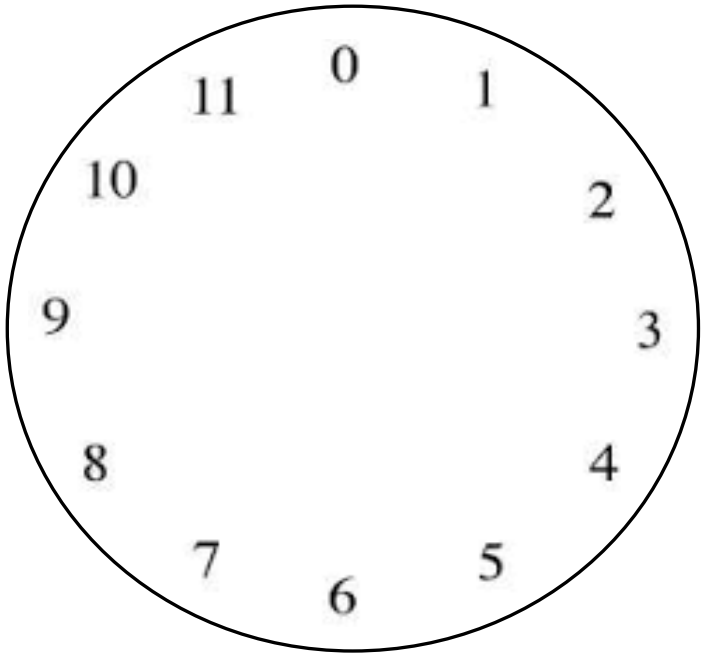
E.g. $3 + 6$ in arithmetic mod 7



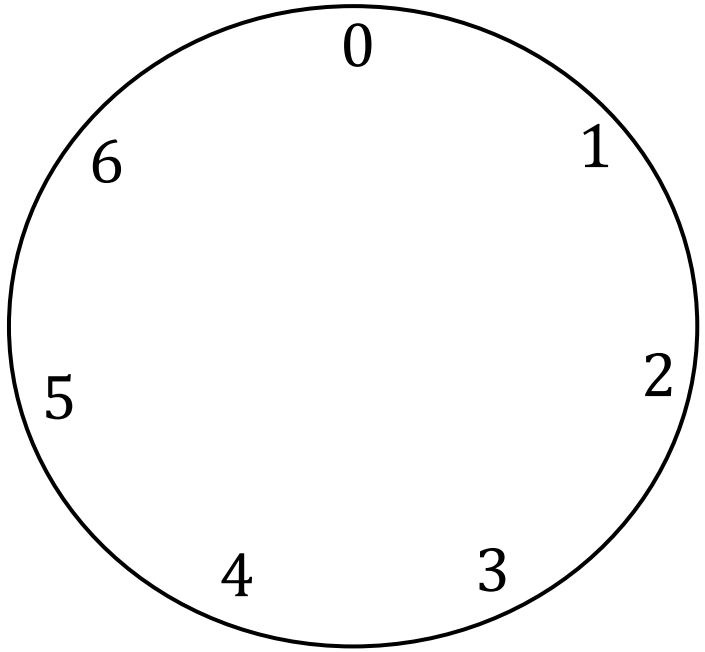
“Sameness”

In modular arithmetic, many numbers have a notion of “sameness”.

Arithmetic mod 12:



Arithmetic mod 7:



"Sameness"

In modular arithmetic, many numbers have a notion of "sameness".

- To say "the same", we don't to use the $=$ symbol.

  E.g. $13 = 1$ is wrong…

- To say same in arithmetic mod m, we use the symbol $\equiv_m$
  - Pronounced "congruent mod m"
  - $13 \equiv_{12} 1$ $\quad 13 \equiv_{12} 25$ $\quad 2 \equiv_{12} 14$
  - $3 \equiv_7 10$ $\quad 0 \equiv_7 7$

Congruence

We need a formal definition of $a \equiv_m b$.

We can't just say "a and b are on the same place in the m clock ☺"

Definition:

For integers a, b and positive integer m, we say $a \equiv_m b$ iff

_____.

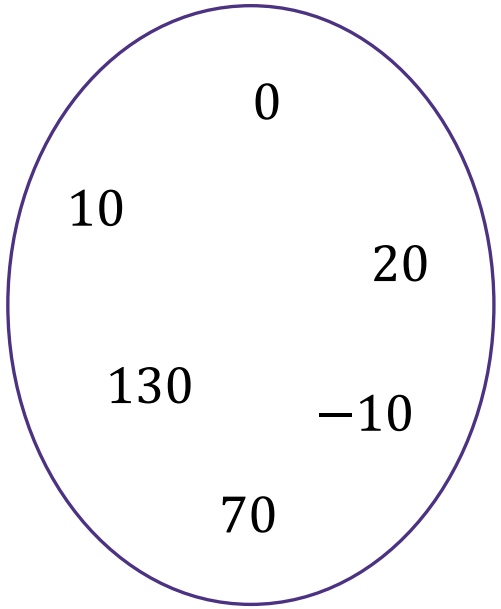
Note: $a \equiv_m b$ is equivalent to _____.

Intuition

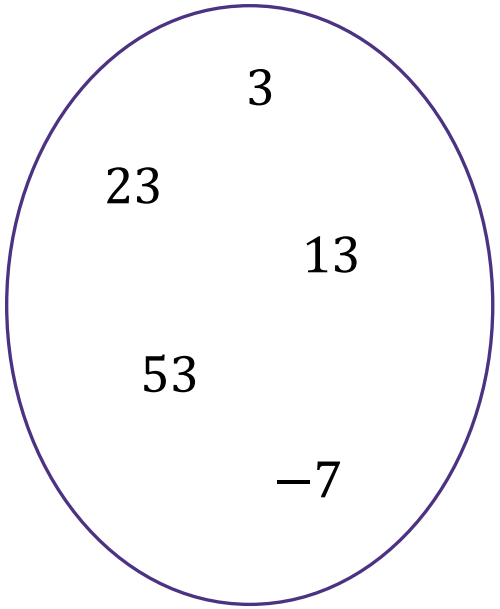
Definition: $a \equiv_m b$ is defined as $m \mid (a - b)$

Intuition: Equivalently, $a \equiv_m b$ means $a \,\%\, m = b \,\%\, m$

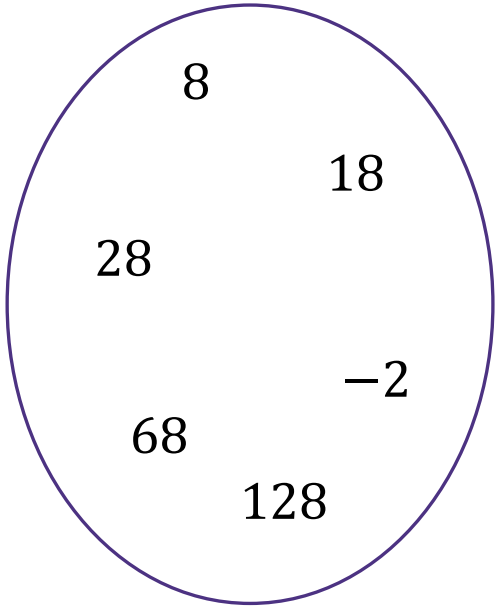
Here we have some groups of numbers that are congruent mod 10.



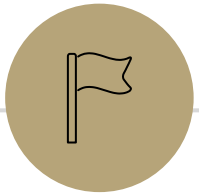
Congruent to 0



Congruent to 3



Congruent to 8



Properties of Congruence

Recall: Familiar Properties of $=$ in algebra

- If $a = b$, then $b = a$.
- If $a = b$ and $c = d$, then $a + c = b + d$.
- If $a = b$ and $c = d$, then $ac = bd$.
- If $a = b$ and $b = c$, then $a = c$.

These are the facts that allow us to use algebra to solve problems.

We will prove analogous facts for modular arithmetic.

Claim 1

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$

$a \equiv_m b$ iff $m \mid (a - b)$

Claim 1: For integers a, b and positive integer m, if $a \equiv_m b$ then $b \equiv_m a$.

Proof

Note on Claim 1

- You'll see $a \equiv_m b$ defined as $m \mid (a - b)$ or $m \mid (b - a)$ depending on where you look.
- Claim 1 proves these definitions are equivalent. From now on, you can use either definition in your proofs.
- In general, once we have proved claims in class, you can use those claims in your homework without proof.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$

$a \equiv_m b$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv_m b$ and $c \equiv_m d$ then $a + c \equiv_m b + d$.

Intuition

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$

$a \equiv_m b$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv_m b$ and $c \equiv_m d$ then $a + c \equiv_m b + d$.

Proof

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$

$a \equiv_m b$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv_m b$ and $c \equiv_m d$ then $ac \equiv_m bd$.

Intuition

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$

$a \equiv_m b$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv_m b$ and $c \equiv_m d$ then $ac \equiv_m bd$.

Proof

Claim 4

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z}\ (b = ka)$

$a \equiv_m b$ iff $m \mid (a - b)$

Claim 4: For integers a, b, c and positive integer m, if $a \equiv_m b$ and $b \equiv_m c$ then $a \equiv_m c$.

Proof

Let a, b, c and $m > 0$ be arbitrary integers. Suppose that $a \equiv_m b$ and $b \equiv_m c$. Then by definition of congruence, $m \mid (a - b)$ and $m \mid (b - c)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $b - c = mj$. Adding the expressions, we have:

$$(a - b) + (b - c) = mk + mj$$

$$a - c = m(k + j)$$

Since k, j are integers, $k + j$ is an integer. Thus by definition of divides, $m \mid a - c$. Then by definition of congruence, $a \equiv_m c$. Since a, b, c, m were arbitrary, the claim holds.