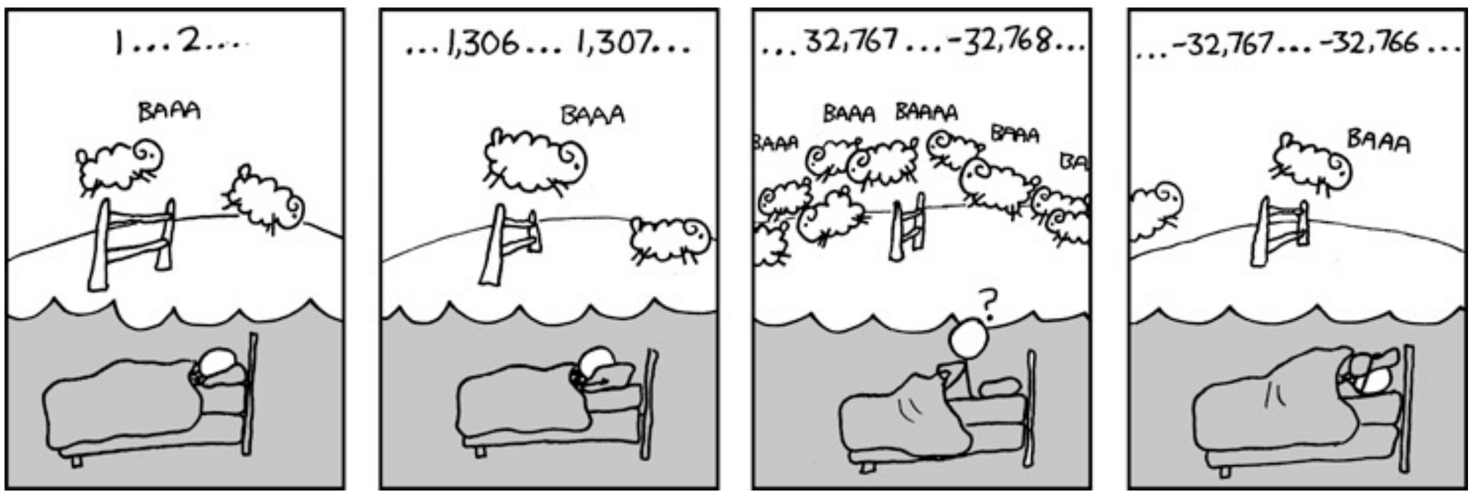
CSE 311: Foundations of Computing

Lecture 12: Modular Arithmetic and Applications



Administrivia

- HW3 solutions after class

- HW4 released on Saturday
- Remember to start early!
  - most problems require a formal proof and then a translation into an English proof
  - English proofs going forward

- Never hear people say "I can write 64-bit ARM assembly but not Java"

Last Class: Divisibility

Definition: "b divides a"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $b \neq 0$:

$$b \mid a \leftrightarrow \exists q \in \mathbb{Z}\ (a = qb)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

Recall: Elementary School Division

For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide b into a.

If $b \mid a$, then, by definition, we have $a = qb$ for some $q \in \mathbb{Z}$.
The number q is called the quotient.

Dividing both sides by b, we can write this as

$$\frac{a}{b} = q$$

(We want to stick to integers, though, so we'll write $a = qb$.)

Recall: Elementary School Division

For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide b into a.

If $b \nmid a$, then we end up with a *remainder* $r \in \mathbb{Z}$ with $0 < r < b$.
Now,

instead of $\dfrac{a}{b} = q$ we have $\dfrac{a}{b} = q + \dfrac{r}{b}$

Multiplying both sides by b gives us $a = qb + r$
(A bit nicer since it has no fractions.)

Recall: Elementary School Division

For $a, b \in \mathbb{Z}$ with $b > 0$, we can divide b into a.

If $b \mid a$, then we have $a = qb$ for some $q \in \mathbb{Z}$.
If $b \nmid a$, then we have $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 < \mathrm{r} < \mathrm{b}$.

In general, we have $a = qb + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < b$, where $r = 0$ iff $b \mid a$.

Division Theorem

Division Theorem

For $a, b \in \mathbb{Z}$ with $b > 0$
there exist *unique* integers q, r with $0 \leq r < b$
such that $a = qb + r$.

To put it another way, if we divide *b* into *a*, we get a unique quotient *q* = *a* **div** *b*
and non-negative remainder *r* = *a* **mod** *b*

Note: r ≥ 0 even if a < 0.
Not quite the same as `a%d`.

Division Theorem

Division Theorem

For $a, b \in \mathbb{Z}$ with $b > 0$
there exist *unique* integers *q*, *r* with $0 \leq r < b$
such that $a = qb + r$.

To put it another way, if we divide *b* into *a*, we get a unique quotient *q* = *a* **div** *b*
and non-negative remainder *r* = *a* **mod** *b*

```
public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}
```

```
 ----jGRASP exec: java Test2
-1

 ----jGRASP: operation complete.
```

Note: r ≥ 0 even if a < 0.
Not quite the same as **a%d.**

Division Theorem

Division Theorem

For $a, b \in \mathbb{Z}$ with $b > 0$
there exist *unique* integers q, r with $0 \leq r < b$
such that $a = qb + r$.

q = a **div** b

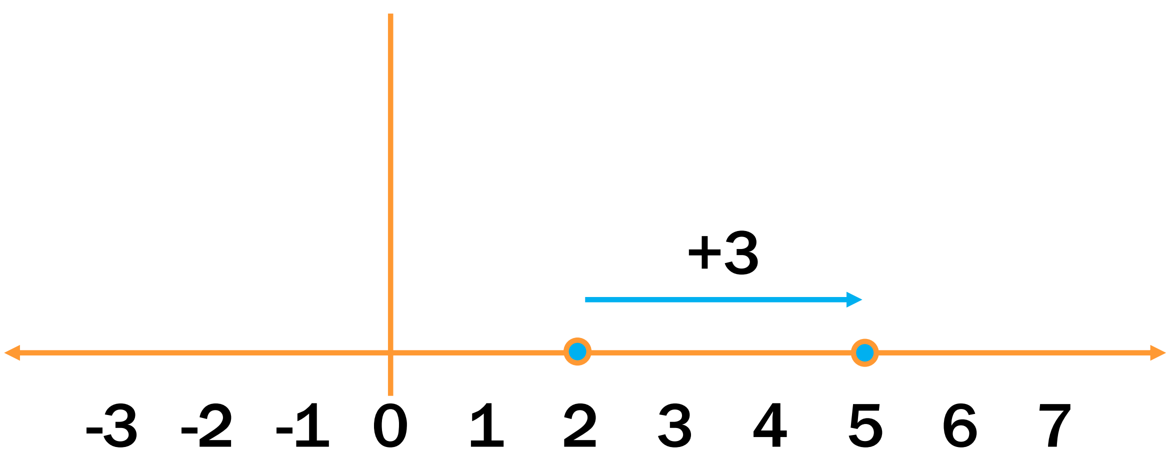
r = a **mod** b

While div is more familiar, our focus is on mod:

- **provides a bound on the size** $(0 \leq r < b)$
- **need to connect that somehow to arithmetic…**

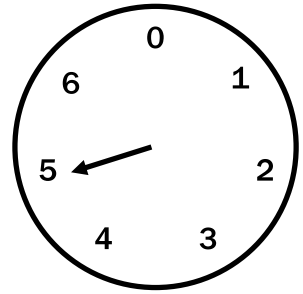
Ordinary arithmetic

$$2 + 3 = 5$$

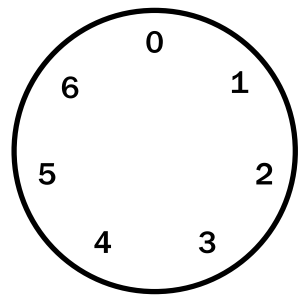


Arithmetic on a Clock

$2 + 3 = 5$



$23 = 3 \cdot 7 + 2$

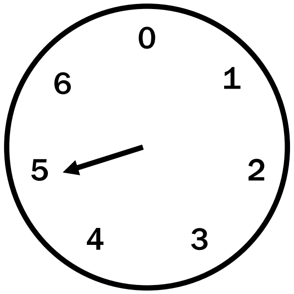


If $a = qb + r$, then $r \ (= a \bmod b)$ is
where you <u>stop</u> after taking a steps on the clock

Arithmetic, mod 7

$(a + b) \bmod 7$

$(a \times b) \bmod 7$



+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

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

New notion of "sameness" that will help us understand modular arithmetic

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

$$a \equiv_m b \;\leftrightarrow\; m \mid (a - b)$$

The standard math notation is

$$a \equiv b \pmod{m}$$

A chain of equivalences is written

$$a \equiv b \equiv c \equiv d \pmod{m}$$

Many students find this confusing,
so we will use $\equiv_m$ instead.

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

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

Check Your Understanding. What do each of these mean? When are they true?

$x \equiv_2 0$

This statement is the same as saying "x is even"; so, any x that is even (including negative even numbers) will work.

$-1 \equiv_5 19$

This statement is true. 19 - (-1) = 20 which is divisible by 5

$y \equiv_7 2$

This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form 2+7k for k an integer.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \bmod \boldsymbol{m} = \boldsymbol{b} \bmod \boldsymbol{m}$.

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q, s.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \textbf{ mod } \boldsymbol{m} = \boldsymbol{b} \textbf{ mod } \boldsymbol{m}$.

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$ since $a \bmod m = b \bmod m$

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q,s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$ since $a \bmod m = b \bmod m$

Therefore, $m \mid (a - b)$ and so $a \equiv_m b$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \mathbf{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \operatorname{\mathbf{mod}} \boldsymbol{m} = \boldsymbol{b} \operatorname{\mathbf{mod}} \boldsymbol{m}$.

Suppose that $a \equiv_m b$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

Modular Arithmetic: A Property

Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{m}$ be integers with $\boldsymbol{m} > \boldsymbol{0}$.
Then, $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ if and only if $\boldsymbol{a} \ \mathbf{mod} \ \boldsymbol{m} = \boldsymbol{b} \ \mathbf{mod} \ \boldsymbol{m}$.

Suppose that $a \equiv_m b$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$,
where $0 \leq (a \bmod m) < m$.

Modular Arithmetic: A Property

Let $\boldsymbol{a, b, m}$ be integers with $\boldsymbol{m > 0}$.
Then, $\boldsymbol{a \equiv_m b}$ if and only if $\boldsymbol{a \bmod m = b \bmod m}$.

Suppose that $a \equiv_m b$.

Then, $m \mid (a - b)$ by definition of congruence.
So, $a - b = km$ for some integer k by definition of divides.
Therefore, $a = b + km$.

By the Division Theorem, we have $a = qm + (a \bmod m)$,
where $0 \leq (a \bmod m) < m$.

Combining these, we have $qm + (a \bmod m) = a = b + km$
or equiv., $\mathrm{b} = qm - km + (a \bmod m) = (q - k)m + (a \bmod m)$.
By the Division Theorem, we have $b \bmod m = a \bmod m$.

The $\mathrm{mod}\ m$ function vs the $\equiv_m$ predicate

- What we have just shown
  - The $\mathrm{mod}\ m$ function takes any $a \in \mathbb{Z}$ and maps it to a remainder $a \mathrm{mod}\ m \in \{0,1,..,m-1\}$.

  - Imagine grouping together all integers that have the same value of the $\mathrm{mod}\ m$ function

    That is, the same remainder in $\{0,1,..,m-1\}$.

  - The $\equiv_m$ predicate compares $a, b \in \mathbb{Z}$. It is true if and only if the $\mathrm{mod}\ m$ function has the same value on a and on b.

    That is, a and b are in the same group.

Recall: Familiar Properties of "="

- **If $a = b$ and $b = c$, then $a = c$.**
  - **i.e., if $a = b = c$, then $a = c$**

- **If $a = b$ and $c = d$, then $a + c = b + d$.**
  - **in particular, since $c = c$ is true, we can "$+ c$" to both sides**

- **If $a = b$ and $c = d$, then $ac = bd$.**
  - **in particular, since $c = c$ is true, we can "$\times c$" to both sides**

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

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$.

Modular Arithmetic: Basic Property

Let $\boldsymbol{m}$ be a positive integer.
If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{b \equiv_m c}$, then $\boldsymbol{a \equiv_m c}$.

Suppose that $a \equiv_m b$ and $b \equiv_m c$. Then, by the previous property, we have $a \bmod m = b \bmod m$ and $b \bmod m = c \bmod m$.

Putting these together, we have $a \bmod m = c \bmod m$, which says that $a \equiv_m c$, by the previous property.

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Modular Arithmetic: Addition Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{a + c \equiv_m b + d}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$. Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some $k, j \in \mathbb{Z}$.

Adding the equations together gives us
$(a + c) - (b + d) = m(k + j)$.

By the definition of congruence, we have $a + c \equiv_m b + d$.

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$.

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$.

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$. Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some $k, j \in \mathbb{Z}$ or equivalently, $a = km + b$ and $c = jm + d$.

Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$.

Modular Arithmetic: Multiplication Property

Let $\boldsymbol{m}$ be a positive integer. If $\boldsymbol{a \equiv_m b}$ and $\boldsymbol{c \equiv_m d}$, then $\boldsymbol{ac \equiv_m bd}$.

Suppose that $a \equiv_m b$ and $c \equiv_m d$. Unrolling the definitions, we can see that $a - b = km$ and $c - d = jm$ for some $k, j \in \mathbb{Z}$ or equivalently, $a = km + b$ and $c = jm + d$.

Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + bjm + bd$. Re-arranging, this becomes $ac - bd = m(kjm + kd + bj)$.

This says $ac \equiv_m bd$ by the definition of congruence.

Modular Arithmetic: Properties

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{b} \equiv_{\boldsymbol{m}} \boldsymbol{c}$, then $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{c}$.

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{d}$.

Corollary: If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$, then $\boldsymbol{a} + \boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{b} + \boldsymbol{c}$.

If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$ and $\boldsymbol{c} \equiv_{\boldsymbol{m}} \boldsymbol{d}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bd}$.

Corollary: If $\boldsymbol{a} \equiv_{\boldsymbol{m}} \boldsymbol{b}$, then $\boldsymbol{ac} \equiv_{\boldsymbol{m}} \boldsymbol{bc}$.

Modular Arithmetic: Properties

If $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

If $a \equiv_m b$, then $a + c \equiv_m b + c$.

If $a \equiv_m b$, then $ac \equiv_m bc$.

"$\equiv_m$" allows us to solve problems in modular arithmetic, e.g.

- **add / subtract numbers from both sides of equations**
- **chains of "$\equiv_m$" values shows first and last are "$\equiv_m$"**
- **substitute "$\equiv_m$" values in equations (not proven yet)**

Example

Let $\boldsymbol{n}$ be an integer. Prove that $\boldsymbol{n^2 \equiv_4 0}$ or $\boldsymbol{n^2 \equiv_4 1.}$

Let's start by looking a a small example:

$0^2 = 0 \quad \equiv_4 \; 0$

$1^2 = 1 \quad \equiv_4 \; 1$

$2^2 = 4 \quad \equiv_4 \; 0$

$3^2 = 9 \quad \equiv_4 \; 1$

$4^2 = 16 \quad \equiv_4 \; 0$

Example

Let n be an integer. Prove that $n^2 \equiv_4 0$ or $n^2 \equiv_4 1$.

Case 1 (n is even):

Let's start by looking a a small example:

$0^2 = 0 \quad \equiv_4 \quad 0$
$1^2 = 1 \quad \equiv_4 \quad 1$
$2^2 = 4 \quad \equiv_4 \quad 0$
$3^2 = 9 \quad \equiv_4 \quad 1$
$4^2 = 16 \quad \equiv_4 \quad 0$

It looks like

$n \equiv_2 0 \rightarrow n^2 \equiv_4 0$, and
$n \equiv_2 1 \rightarrow n^2 \equiv_4 1$.

Example

Let $\boldsymbol{n}$ be an integer. Prove that $\boldsymbol{n^2 \equiv_4 0}$ or $\boldsymbol{n^2 \equiv_4 1}$.

Let's start by looking a a small example:

$0^2 = 0$	$\equiv_4$	0
$1^2 = 1$	$\equiv_4$	1
$2^2 = 4$	$\equiv_4$	0
$3^2 = 9$	$\equiv_4$	1
$4^2 = 16$	$\equiv_4$	0

Case 1 (n is even):

Suppose n is even.

Then, $n = 2k$ for some integer k.

So, $n^2 = (2k)^2 = 4k^2 = 4k^2 + 0$.

So, by the definition of congruence,

we have $n^2 \equiv_4 0$.

It looks like

$n \equiv_2 0 \rightarrow n^2 \equiv_4 0$, and

$n \equiv_2 1 \rightarrow n^2 \equiv_4 1$.

Example

Let $\boldsymbol{n}$ be an integer. Prove that $\boldsymbol{n^2 \equiv_4 0}$ or $\boldsymbol{n^2 \equiv_4 1.}$

Case 1 (n is even): Done.

Case 2 (n is odd):

Let's start by looking a a small example:

$0^2 = 0 \equiv_4 0$
$1^2 = 1 \equiv_4 1$
$2^2 = 4 \equiv_4 0$
$3^2 = 9 \equiv_4 1$
$4^2 = 16 \equiv_4 0$

It looks like

$n \equiv_2 0 \rightarrow n^2 \equiv_4 0$, and
$n \equiv_2 1 \rightarrow n^2 \equiv_4 1$.

Example

Let $\boldsymbol{n}$ be an integer. Prove that $\boldsymbol{n^2 \equiv_4 0}$ or $\boldsymbol{n^2 \equiv_4 1}$.

Case 1 (n is even): Done.

Case 2 (n is odd):

Suppose n is odd.

Then, $n = 2k + 1$ for some integer k.

So, $n^2 = (2k+1)^2$

$= 4k^2 + 4k + 1$

$= 4(k^2 + k) + 1$.

So, by definition of congruence,

we have $n^2 \equiv_4 1$.

Let's start by looking a a small example:

$0^2 = 0$	$\equiv_4$	0
$1^2 = 1$	$\equiv_4$	1
$2^2 = 4$	$\equiv_4$	0
$3^2 = 9$	$\equiv_4$	1
$4^2 = 16$	$\equiv_4$	0

It looks like

$n \equiv_2 0 \rightarrow n^2 \equiv_4 0$, and

$n \equiv_2 1 \rightarrow n^2 \equiv_4 1$.

Result follows by proof by cases since n is either even or odd