CSE 311 Section 3

Number Theory & Induction

Announcements & Reminders

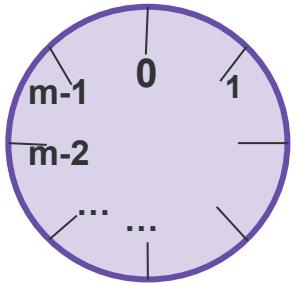
- HW3 Part 1 due today @ 6:00 pm on Cozy
- HW3 Part 2 due Friday @ 6:00 pm on Gradescope
  - Use late days if you need to!
  - Make sure you tagged pages on gradescope correctly

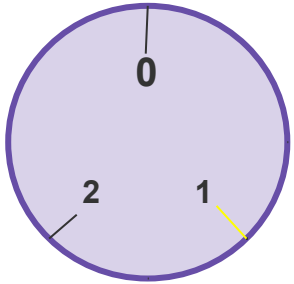
- Quiz next Tuesday
  - Remember to review feedback in homework!

Mod and Proving Divisibility

a ≡ b (mod m)

Imagine a clock with m numbers

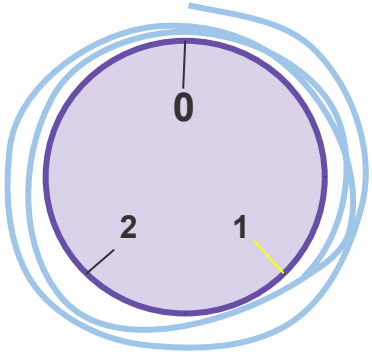




1 (mod 3)

≡

VS



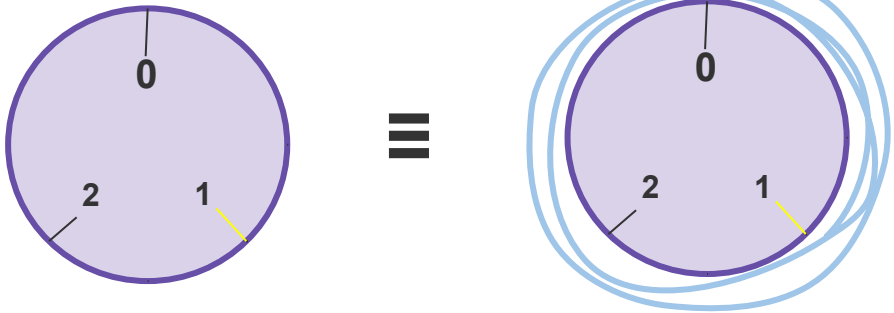
10 (mod 3)

We can say that **a ≡ b (mod m)** where a and b are in the same position in the mod clock

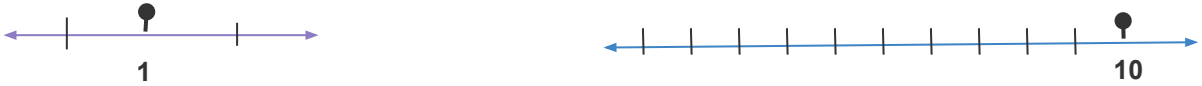
1 ≡ 10 (mod 3)

Divides

What if we “unroll” this clock?

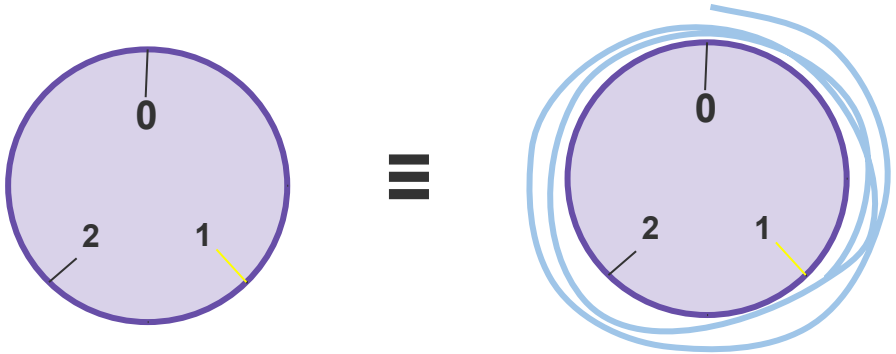


1 (mod 3) **VS** 10 (mod 3)

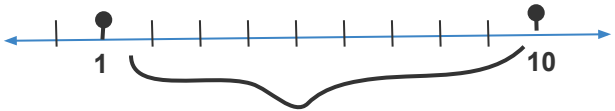


Divides

What if we “unroll” this clock?



1 (mod 3) **VS** 10 (mod 3)

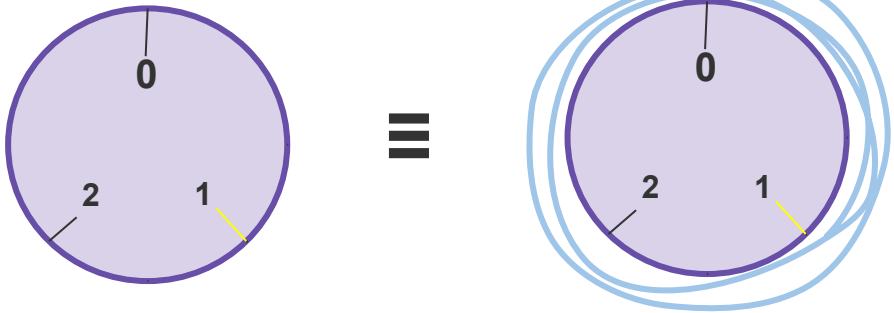


(10-1) = 9
9 ÷ 3 = 3 so 3 | 9

3 ∤ 10 and 3 ∤ 1 BUT 3 | 9

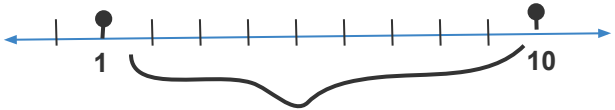
Divides

What if we “unroll” this clock?



1 (mod 3) **VS** 10 (mod 3)

So m divides the <u>difference</u> between a and b!



(10-1) = 9
9 ÷ 3 = 3 so 3 | 9

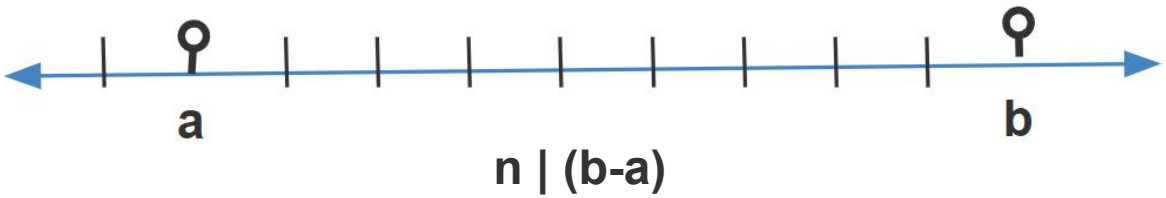
3∤10 and 3∤1 BUT 3|9

Formalizing Mod and Divides

Definition: "a is congruent to b modulo m"

For a, b, m with $m > 0$

$$a \equiv_m b \quad := \quad m \mid (a - b)$$



“Unwrapping”

This expression is generally easier to deal with

$a \equiv_n b$ ⟺ $n \mid (b-a)$ ⟺ $(b-a) = n * k$

Definition: “a is congruent to b modulo m”

For a, b, m with $m > 0$

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

Divides

For integers x, y we say $x|y$ (“x divides y”) iff there is an integer z such that $xz = y$.

Divides is an operation that outputs true/false! It is not the same as divided by!

Task 1b – Formal Proof Translations

Translate this formal proof to English

1. $n \mid m$ — Given
2. $\exists k, m = k\,n$ — Def of Divides: 1
3. $m = j\,n$ — Elim $\exists$: 2

   Let a and b be arbitrary.

   4.1.1. $a \equiv_m b$ — Assumption

   4.1.2. $m \mid a - b$ — Def of Congruent: 4.1.1

   4.1.3. $\exists k, a - b = k\,m$ — Def of Divides: 4.1.2

   4.1.4. $a - b = k\,m$ — Elim $\exists$: 4.1.3

   4.1.5. $a - b = k\,j\,n$ — Algebra: 3, 4.1.4

   4.1.7. $\exists k, a - b = k\,n$ — Intro $\exists$: 4.1.5

   4.1.8. $n \mid a - b$ — Undef Divides: 4.1.6

   4.1.9. $a \equiv_n b$ — Undef Congruent: 4.1.7

   4.1. $a \equiv_m b \rightarrow a \equiv_n b$ — Direct Proof

4. $\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$ — Intro $\forall$

Work on translating this formal proof to English with the people around you

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim $\exists$: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim $\exists$: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro $\exists$: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \rightarrow a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$	Intro $\forall$

Task 1b – Formal Proof Translations

Translate this formal proof to English

We are given that $n \mid m$

1. $n \mid m$ — Given
2. $\exists k, m = k\,n$ — Def of Divides: 1
3. $m = j\,n$ — Elim $\exists$: 2

   Let a and b be arbitrary.

   4.1.1. $a \equiv_m b$ — Assumption
   4.1.2. $m \mid a - b$ — Def of Congruent: 4.1.1
   4.1.3. $\exists k, a - b = k\,m$ — Def of Divides: 4.1.2
   4.1.4. $a - b = k\,m$ — Elim $\exists$: 4.1.3
   4.1.5. $a - b = k\,j\,n$ — Algebra: 3, 4.1.4
   4.1.7. $\exists k, a - b = k\,n$ — Intro $\exists$: 4.1.5
   4.1.8. $n \mid a - b$ — Undef Divides: 4.1.6
   4.1.9. $a \equiv_n b$ — Undef Congruent: 4.1.7

   4.1. $a \equiv_m b \rightarrow a \equiv_n b$ — Direct Proof

4. $\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$ — Intro $\forall$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1. $n \mid m$ — Given
2. $\exists k, m = k\,n$ — Def of Divides: 1
3. $m = j\,n$ — Elim $\exists$: 2

Let a and b be arbitrary.

- 4.1.1. $a \equiv_m b$ — Assumption
- 4.1.2. $m \mid a - b$ — Def of Congruent: 4.1.1
- 4.1.3. $\exists k, a - b = k\,m$ — Def of Divides: 4.1.2
- 4.1.4. $a - b = k\,m$ — Elim $\exists$: 4.1.3
- 4.1.5. $a - b = k\,j\,n$ — Algebra: 3, 4.1.4
- 4.1.7. $\exists k, a - b = k\,n$ — Intro $\exists$: 4.1.5
- 4.1.8. $n \mid a - b$ — Undef Divides: 4.1.6
- 4.1.9. $a \equiv_n b$ — Undef Congruent: 4.1.7

4.1. $a \equiv_m b \rightarrow a \equiv_n b$ — Direct Proof

4. $\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$ — Intro $\forall$

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim $\exists$: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim $\exists$: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro $\exists$: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \to a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \to a \equiv_n b$	Intro $\forall$

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim $\exists$: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim $\exists$: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro $\exists$: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \to a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \to a \equiv_n b$	Intro $\forall$

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Suppose $a \equiv_m b$

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim $\exists$: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim $\exists$: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro $\exists$: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \rightarrow a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$	Intro $\forall$

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Suppose $a \equiv_m b$

By definition of congruence, $m \mid a - b$

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim $\exists$: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim $\exists$: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro $\exists$: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \rightarrow a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$	Intro $\forall$

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Suppose $a \equiv_m b$

By definition of congruence, $m \mid a - b$

By definition of divides, $a - b = km$ for some integer k

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim $\exists$: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim $\exists$: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro $\exists$: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \rightarrow a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$	Intro $\forall$

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Suppose $a \equiv_m b$

By definition of congruence, $m \mid a - b$

By definition of divides, $a - b = km$ for some integer k

We have $a-b = km$ and $m = jn$, so with substitution, we get $a-b = kjn$

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim $\exists$: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim $\exists$: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro $\exists$: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \rightarrow a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$	Intro $\forall$

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Suppose $a \equiv_m b$

By definition of congruence, $m \mid a - b$

By definition of divides, $a - b = km$ for some integer k

We have $a-b = km$ and $m = jn$, so with substitution, we get $a-b = kjn$
Since integers are closed under multiplication, kj is an integer
So $a - b$ is n times some integer

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim ∃: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim ∃: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro ∃: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \rightarrow a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$	Intro ∀

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Suppose $a \equiv_m b$

By definition of congruence, $m \mid a - b$

By definition of divides, $a - b = km$ for some integer k

We have $a-b = km$ and $m = jn$, so with substitution, we get $a-b = kjn$
Since integers are closed under multiplication, kj is an integer
So $a - b$ is n times some integer
This is exactly the definition of divides, so n divides $a - b$

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

1.	$n \mid m$	Given
2.	$\exists k, m = k\,n$	Def of Divides: 1
3.	$m = j\,n$	Elim ∃: 2
	Let a and b be arbitrary.	
	4.1.1. $a \equiv_m b$	Assumption
	4.1.2. $m \mid a - b$	Def of Congruent: 4.1.1
	4.1.3. $\exists k, a - b = k\,m$	Def of Divides: 4.1.2
	4.1.4. $a - b = k\,m$	Elim ∃: 4.1.3
	4.1.5. $a - b = k\,j\,n$	Algebra: 3, 4.1.4
	4.1.7. $\exists k, a - b = k\,n$	Intro ∃: 4.1.5
	4.1.8. $n \mid a - b$	Undef Divides: 4.1.6
	4.1.9. $a \equiv_n b$	Undef Congruent: 4.1.7
4.1.	$a \equiv_m b \rightarrow a \equiv_n b$	Direct Proof
4.	$\forall a, \forall b, a \equiv_m b \rightarrow a \equiv_n b$	Intro ∀

We are given that $n \mid m$

By definition of divides, this means $m = jn$ for some integer j

Let a, b be arbitrary integers

Suppose $a \equiv_m b$

By definition of congruence, $m \mid a - b$

By definition of divides, $a - b = km$ for some integer k

We have $a-b = km$ and $m = jn$, so with substitution, we get $a-b = kjn$

Since integers are closed under multiplication, kj is an integer

So $a - b$ is n times some integer

This is exactly the definition of divides, so n divides $a - b$

This is exactly the definition of congruence, so $a \equiv_n b$

Since a, b were arbitrary integers, it must mean that for all integers, if $a \equiv_m b$ and $n \mid m$, then $a \equiv_n b$

Task 1b – Formal Proof Translations

Translate this formal proof to English

Let a and b be arbitrary integers.

Suppose that $a \equiv_m b$. Then, by definition of congruence, we can see that $m \mid (a-b)$. By the definition of divides, this means that $a - b = km$ for some integer k. We are also given that $n \mid m$. By the definition of divides, this tells us that $m = jn$ for some integer j. Substituting the latter equation into the earlier one, we find that $a-b = km = k(jn) = (kj)n$. This last equation shows, by the definition of divides, that $n \mid a - b$, which tells us that $a \equiv_n b$, by the definition of congruence.

Since a and b were arbitrary, the claim holds

Mod Algebra vs Mod Properties

- Notice how our formal proof utilized unwrapping
- Proofs should not use mod algebra. Even the simplest mod algebra statements must be proven
  - $a \equiv_m a$ (need to use unwrapping to show $(a = 1 * a) \rightarrow \exists k\ (a=ka) \rightarrow (a \mid a) \rightarrow a \equiv_m a$)
  - $4a \equiv_4 0$ (need to use unwrapping to show $(4a = a * 4) \rightarrow \exists k\ (4a=k*4) \rightarrow (4 \mid 4a) \rightarrow 4a \equiv_4 0$)
  - If $a \equiv_m 0$, then $a + 1 \equiv_m 1$ (need to also show $1 \equiv_m 1$ holds to use the addition property of congruences)
- 3 mod properties you can use without proof:
  - Let a, b, c, d, m be integers with $m > 0$
    - If $a \equiv_m b$ and $c \equiv_m d$, then $a + c \equiv_m b + d$ (Addition property of congruences)
    - If $a \equiv_m b$ and $c \equiv_m d$, then $ac \equiv_m bd$ (Multiplication property of congruences)
    - $(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Extended Euclid

Problem 2 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of $7 \bmod 33$. That is, find y such that $7y \equiv 1 \ (mod \ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

Problem 2 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of $7 \bmod 33$. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

First, we find the gcd:

```
gcd(33,7)   = gcd(7,5)      33 = 4 • 7 + 5
            = gcd(5,2)      7  = 1 • 5 + 2
            = gcd(2,1)      5  = 2 • 2 + 1
            = gcd(1,0)      2  = 2 • 1 + 0
```

Problem 2 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of $7 \bmod 33$. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

First, we find the gcd:

```
gcd(33,7)   = gcd(7,5)
            = gcd(5,2)
            = gcd(2,1)
            = gcd(1,0)
```

```
33 = 4 • 7 + 5
7  = 1 • 5 + 2
5  = 2 • 2 + 1
2  = 2 • 1 + 0
```

Next, we re-arrange the equations by solving for the remainder:

```
1 = 5 - 2 • 2
2 = 7 - 1 • 5
5 = 33 - 4 • 7
```

Problem 2 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of $7 \bmod 33$. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

First, we find the gcd:

```
gcd(33,7)   = gcd(7,5)
            = gcd(5,2)
            = gcd(2,1)
            = gcd(1,0)
```

```
33 = 4 • 7 + 5
7  = 1 • 5 + 2
5  = 2 • 2 + 1
2  = 2 • 1 + 0
```

Next, we re-arrange the equations by solving for the remainder:

```
1 = 5 − 2 • 2
2 = 7 − 1 • 5
5 = 33 − 4 • 7
```

Now, we backward substitute into the boxed numbers using the equations:

$$
\begin{aligned}
1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (7 - 1 \cdot 5) \\
&= 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (33 - 4 \cdot 7) - 2 \cdot 7 \\
&= 3 \cdot 33 + -14 \cdot 7
\end{aligned}
$$

Problem 2 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

First, we find the gcd:

$$\begin{aligned} \gcd(33,7) &= \gcd(7,5) \\ &= \gcd(5,2) \\ &= \gcd(2,\mathbf{1}) \\ &= \gcd(\mathbf{1},0) \end{aligned}$$

$$\begin{aligned} 33 &= 4 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + \mathbf{1} \\ 2 &= 2 \cdot \mathbf{1} + 0 \end{aligned}$$

Next, we re-arrange the equations by solving for the remainder:

$$\begin{aligned} \mathbf{1} &= 5 - 2 \cdot 2 \\ 2 &= 7 - 1 \cdot 5 \\ 5 &= 33 - 4 \cdot 7 \end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned} \mathbf{1} &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (33 - 4 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 33 + -14 \cdot 7 \end{aligned}$$

So, **1** = **3** • 33 + **−14** • 7. Thus, 33 **− 14** = **19** is the multiplicative inverse of 7 mod 33

Problem 2 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of $7 \bmod 33$. That is, find y such that $7y \equiv 1 \ (mod \ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

b) Now, solve $7z \equiv 2 \ (\mathrm{mod}\ 33)$ for all of its integer solutions z.

Try this problem with the people around you, and then we'll go over it together!

Problem 2 – Extended Euclidean Algorithm

b) Now, solve $7z \equiv 2 \pmod{33}$ for all of its integer solutions z.

Problem 2 – Extended Euclidean Algorithm

b) Now, solve $7z \equiv 2 \pmod{33}$ for all of its integer solutions z.

If we have $7z \equiv 2 \pmod{33}$, multiplying both sides by 19, we get:

$19 \cdot 7z \equiv 19 \cdot 2 \pmod{33}$

$z \equiv 5 \pmod{33}$

Thus $z = 5 + 33k$

This means that the set of solutions is $\{5 + 33k \mid k \in Z\}$

Introducing Induction (kind of)

Climb the ladder!

You are scared of heights and there is a prize at the top of a very very tall ladder.

You do not want to climb this ladder…

Climb the ladder!

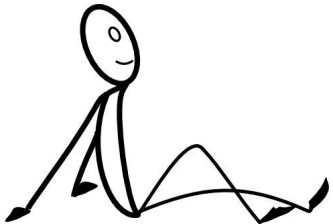
You are scared of heights and there is a prize at the top of a very very tall ladder.

You do not want to climb this ladder…

Lets convince your friend to climb it instead!!!

Climb the ladder!

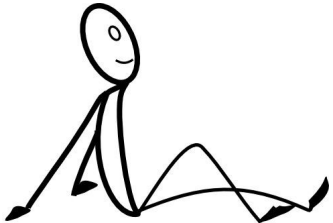
Claim: “You can climb a ladder with n steps” for n >=1



Climb the ladder!

Claim: “You can climb a ladder with n steps” for n >=1

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

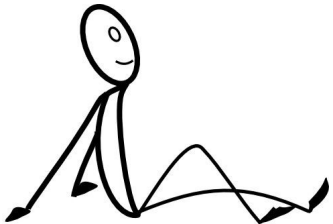


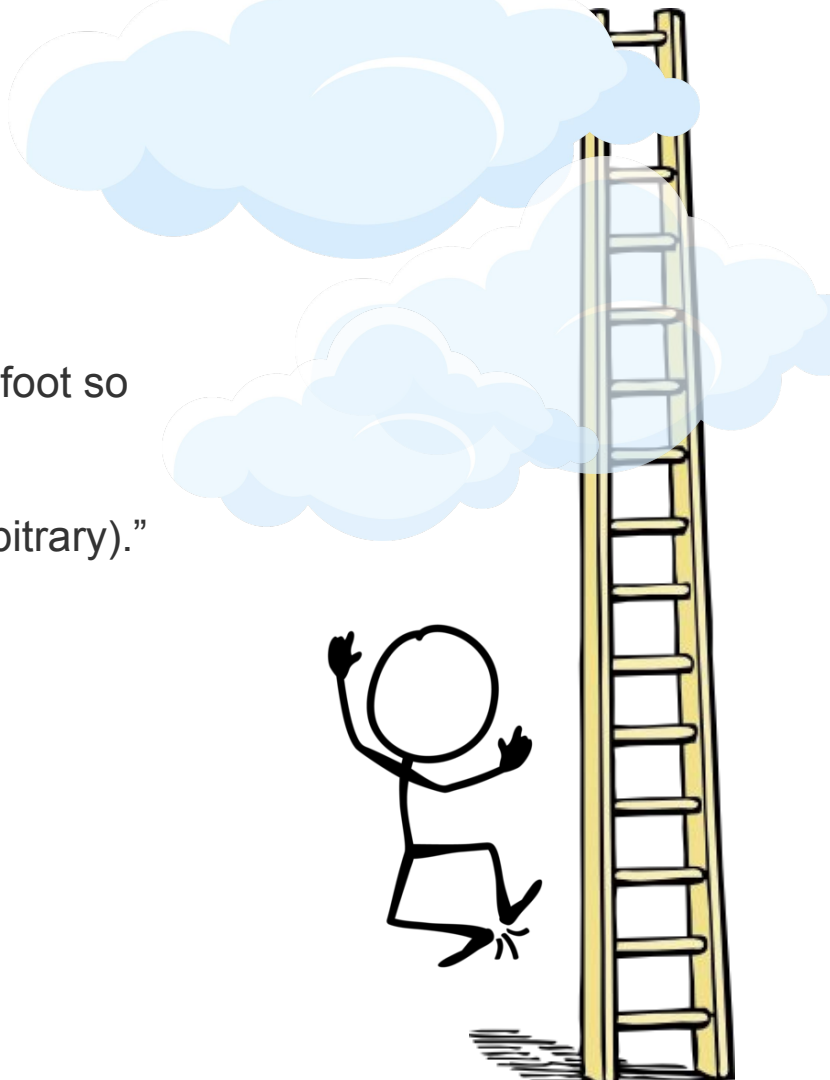
Climb the ladder!

Claim: “You can climb a ladder with n steps” for n >=1

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with k steps (k is arbitrary).”





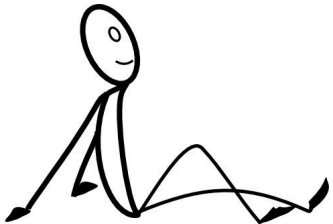
Climb the ladder!

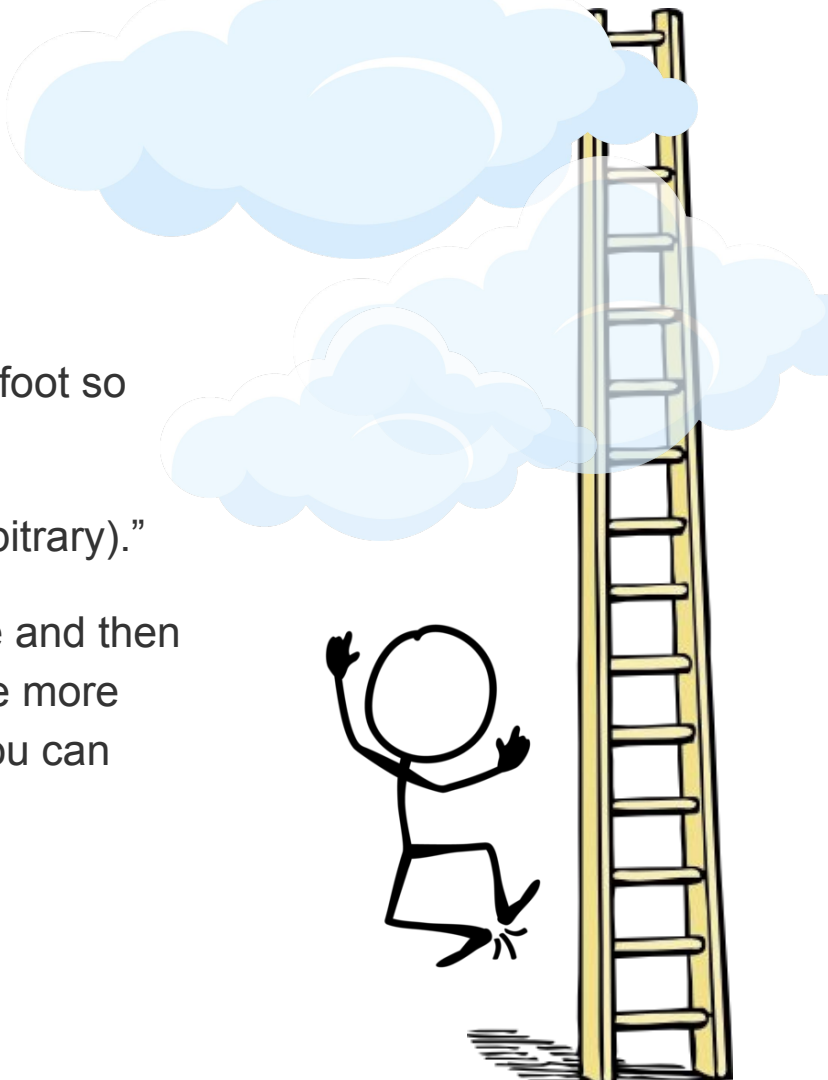
Claim: “You can climb a ladder with n steps” for n >=1

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with k steps (k is arbitrary).”

“Since you can climb to the kth step, climb up to there and then after your reach the kth step, you can lift your foot one more step to reach the k+1 step of the ladder. Therefore, you can climb a ladder with k+1 steps.”





Climb the ladder!

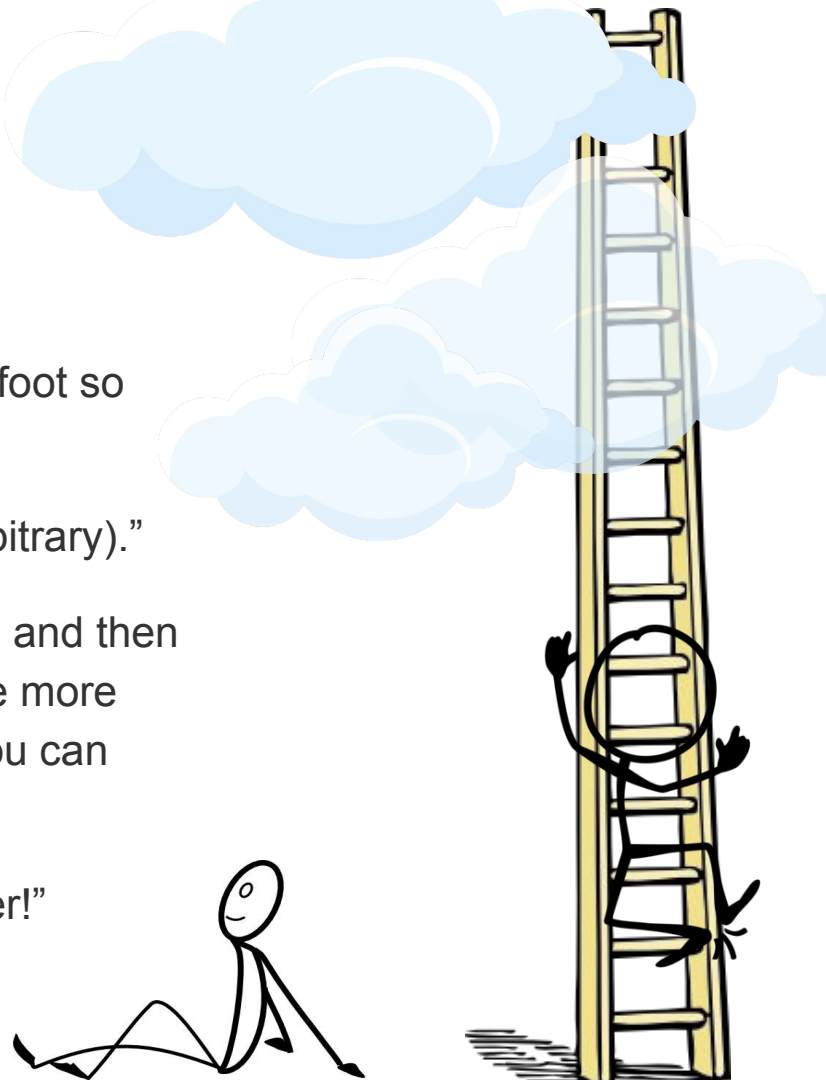
Claim: “You can climb a ladder with n steps” for n >=1

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with k steps (k is arbitrary).”

“Since you can climb to the kth step, climb up to there and then after your reach the kth step, you can lift your foot one more step to reach the k+1 step of the ladder. Therefore, you can climb a ladder with k+1 steps.”

“By the principle of induction, you can climb any ladder!”



Why does it work?

Claim: “You can climb a ladder with n steps” for n >=1

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with k>=1 steps (k is arbitrary).”

“Since you can climb to the kth step, climb up to there and then after your reach the kth step, you can lift your foot one more step to reach the k+1 step of the ladder. Therefore, you can climb a ladder with k+1 steps.”

“By the principle of induction, you can climb any ladder!”

Base Case: You were able to start climbing at some point

Inductive Step: k was arbitrary, so no matter how far you go, you can always go one step higher

Induction Proof Structure

Claim: “You can climb a ladder with n steps” for n >=1

P(n)

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

Base Case

“Suppose you can climb a ladder with k>=1 steps (k is arbitrary).”

Inductive Hypothesis:
Suppose P(k) holds

“Since you can climb to the kth step, climb up to there and then after your reach the kth step, you can lift your foot one more step to reach the k+1 step of the ladder. Therefore, you can climb a ladder with k+1 steps.”

Inductive Step:
Show P(k+1) holds

“By the principle of induction, you can climb any ladder!”

Conclusion:
P(n) holds for all n!

Why k>=1? Why not just k>1?

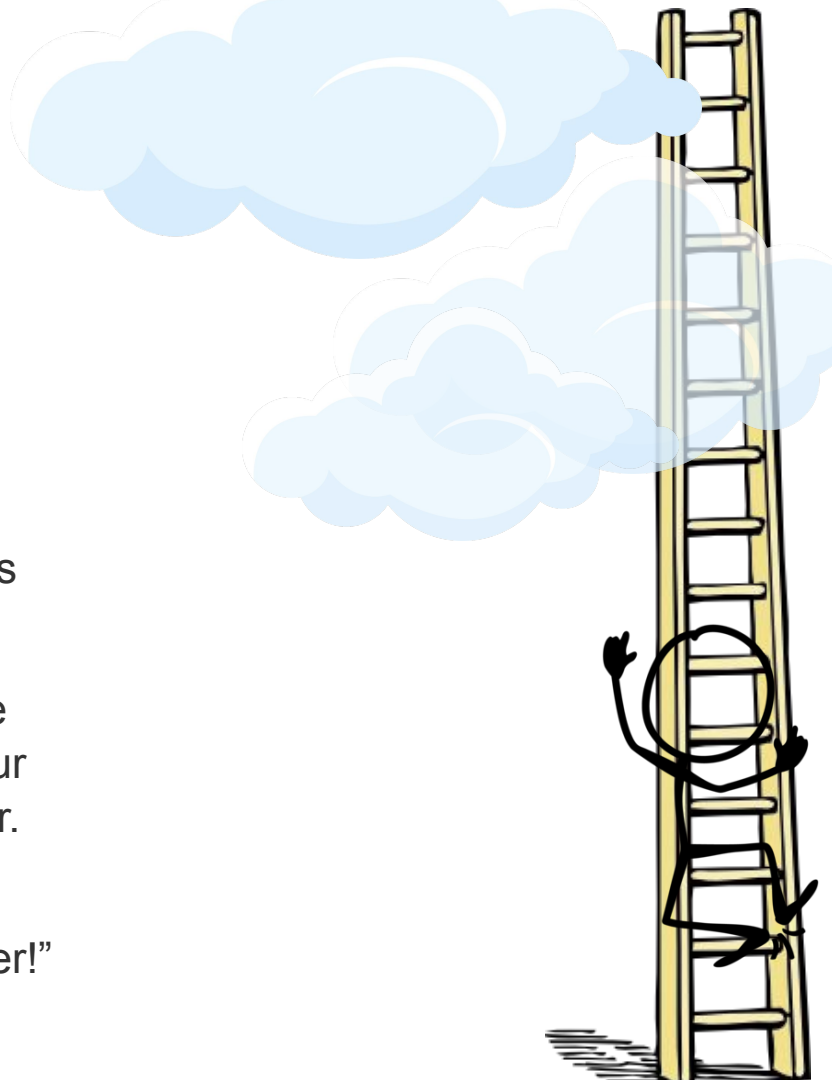
Claim: “You can climb a ladder with n steps” for n >=1

“If a ladder has just one step, I know you can lift your foot so after one step you will reach the top of the ladder.”

“Suppose you can climb a ladder with **k>=1** steps (k is arbitrary).”

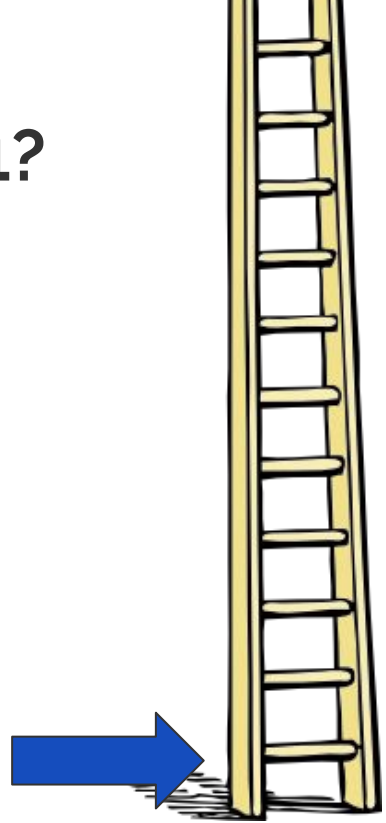
“Since you can climb to the kth step, climb up to there and then after your reach the kth step, you can lift your foot one more step to reach the k+1 step of the ladder. Therefore, you can climb a ladder with k+1 steps.”

“By the principle of induction, you can climb any ladder!”

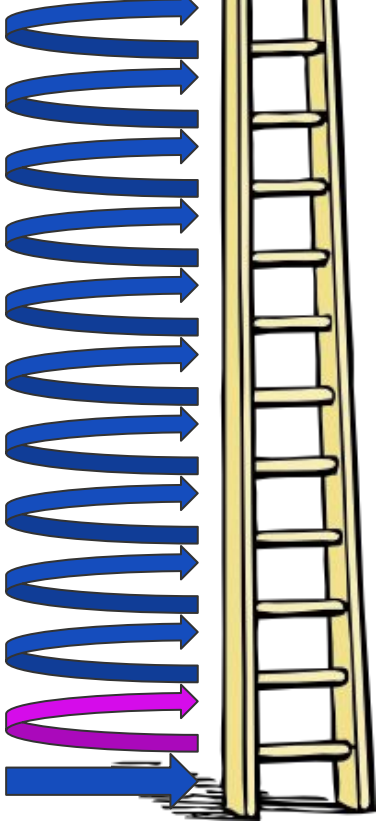


Why k>=1? Why not just k>1?

Base Case: You can climb to the first rung



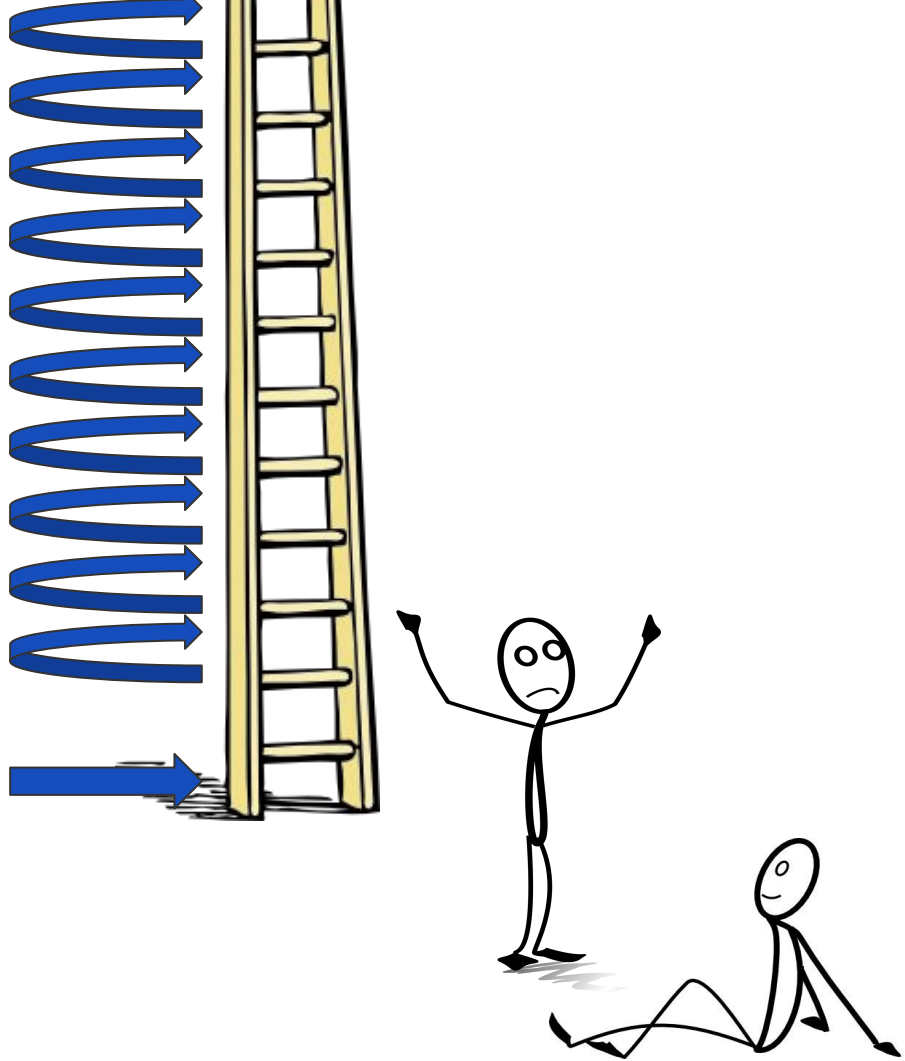
Why k>=1? Why not just k>1?



Inductive Step: If you can climb to rung k>=1, then you can climb to rung k+1. k can be as small as 1, so inductive step handles the case of going from rung 1 to rung 2

Why k>=1? Why not just k>1?

If k>1, then the smallest k can be is 2. So if you can climb to rung 2, then you can climb to rung 3. But how can you climb to rung 2?



Induction: How it actually works

(Weak) Induction Template

Let $P(n)$ be "(whatever you're trying to prove)".
We show $P(n)$ holds for all $n \in$ N by induction on n

Base Case: Show $P(b)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$.

Inductive Step: Show $P(k+1)$ (i.e. get $P(k) \rightarrow P(k+1)$)

Conclusion: Therefore, $P(n)$ holds for all n by the principle of induction.

(Weak) Induction Template

Let $P(n)$ be "(whatever you're trying to prove)".
We show $P(n)$ holds **for all n** $\in$ N by induction on n

Note: often you will condition n here, like "all natural numbers n" or "$n \geq 0$"

Base Case: Show $P(b)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$.

Inductive Step: Show $P(k+1)$ (i.e. get $P(k) \rightarrow P(k+1)$)

Conclusion: Therefore, $P(n)$ holds **for all n** by the principle of induction.

Match the earlier condition on n in your conclusion!

(Weak) Induction Template

P(n) IS A PREDICATE, IT HAS A BOOLEAN VALUE NOT A NUMERICAL ONE

Let $P(n)$ be "(whatever you're trying to prove)".
We show $P(n)$ holds **for all n** $\in$ N by induction on n

Base Case: Show $P(b)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$.

Inductive Step: Show $P(k+1)$ (i.e. get $P(k) \rightarrow P(k+1)$)

Conclusion: Therefore, $P(n)$ holds **for all n** by the principle of induction.

(Weak) Induction Template

P(n) IS A PREDICATE, IT HAS A BOOLEAN VALUE NOT A NUMERICAL ONE

YOU MUST INTRODUCE AN <u>ARBITRARY</u> VARIABLE IN YOUR IH

Let $P(n)$ be "(whatever you're trying to prove)".
We show $P(n)$ holds **for all n** $\in$ N by induction on n

<u>Base Case:</u> Show $P(b)$ is true.

<u>Inductive Hypothesis:</u> Suppose $P(k)$ holds for an arbitrary $k \geq b$.

<u>Inductive Step:</u> Show $P(k+1)$ (i.e. get $P(k) \rightarrow P(k+1)$)

<u>Conclusion:</u> Therefore, $P(n)$ holds **for all n** by the principle of induction.

(Weak) Induction Template

P(n) IS A PREDICATE, IT HAS A BOOLEAN VALUE NOT A NUMERICAL ONE

YOU MUST INTRODUCE AN ARBITRARY VARIABLE IN YOUR IH

START WITH LHS OF EXPRESSION AND END WITH RHS (FOR BASE CASE AND IS)

Let $P(n)$ be "(whatever you're trying to prove)".
We show $P(n)$ holds **for all n** $\in$ N by induction on n

Base Case: Show $P(b)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$.

Inductive Step: Show $P(k+1)$ (i.e. get $P(k) \rightarrow P(k+1)$)

Conclusion: Therefore, $P(n)$ holds **for all n** by the principle of induction.

Weak Induction

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case.

$$\sum_{i=0}^{n} i^2 =$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case.

$$\sum_{i=0}^{n} i^2 = 0^2$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case.

$$\sum_{i=0}^{n} i^2 = 0^2$$

$$= \frac{1}{6}(0)(0+1)(2(0)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case.

$$\sum_{i=0}^{n} i^2 = 0^2$$

$$= \frac{1}{6}(0)(0+1)(2(0)+1)$$

Thus P(0) is true.

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case.

$$\sum_{i=0}^{n} i^2 = 0^2$$

$$= \frac{1}{6}(0)(0+1)(2(0)+1)$$

Thus P(0) is true.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$ (i.e. $\sum_{i=0}^{k} i^2 = \frac{1}{6}k(k+1)(2(k)+1).$)

Task 4

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Let $P(n)$ be the statement "$\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case.

$$\sum_{i=0}^{n} i^2 = 0^2$$

$$= \frac{1}{6}(0)(0+1)(2(0)+1)$$

Thus P(0) is true.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$ (i.e. $\sum_{i=0}^{k} i^2 = \frac{1}{6}k(k+1)(2(k)+1).$)

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$ (i.e. $\sum_{i=0}^{k} i^2 = \frac{1}{6}k(k+1)(2(k)+1)$.)

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$ (i.e. $\sum_{i=0}^{k} i^2 = \frac{1}{6}k(k+1)(2(k)+1).$)

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$ (i.e. $\sum_{i=0}^{k} i^2 = \frac{1}{6}k(k+1)(2(k)+1).$)

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{N}$ (i.e. $\sum_{i=0}^{k} i^2 = \frac{1}{6}k(k+1)(2(k)+1).$)

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \qquad \text{by the I.H.}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \qquad \text{by the I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) \qquad \text{using common factor } (k+1)$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \qquad \text{by the I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) \qquad \text{using common factor } (k+1)$$

$$= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right)$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \qquad \text{by the I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) \qquad \text{using common factor } (k+1)$$

$$= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right)$$

$$= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right)$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \qquad \text{by the I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) \qquad \text{using common factor } (k+1)$$

$$= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right)$$

$$= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right)$$

$$= \frac{1}{6}(k+1)(k+2)(2k+3) \qquad \text{factoring the quadratic term}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\sum_{i=0}^{k+1} i^2 = \sum_{i=0}^{k} i^2 + (k+1)^2 \qquad \text{by definition}$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \qquad \text{by the I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) \qquad \text{using common factor } (k+1)$$

$$= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right)$$

$$= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right)$$

$$= \frac{1}{6}(k+1)(k+2)(2k+3) \qquad \text{factoring the quadratic term}$$

$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

Thus, we can conclude that $P(k+1)$ is true.

Task 3

For all $n \in \mathbb{N}$, prove that $\sum_{i=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$.

Inductive Step. Goal: P(k+1) i.e. $\sum_{i=0}^{k+1} i^2 = \frac{1}{6}(k+1)(k+2)(2(k+1)+1)$

$$\begin{aligned}
\sum_{i=0}^{k+1} i^2 &= \sum_{i=0}^{k} i^2 + (k+1)^2 && \text{by definition} \\
&= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by the I.H.} \\
&= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) && \text{using common factor } (k+1) \\
&= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right) \\
&= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right) \\
&= \frac{1}{6}(k+1)(k+2)(2k+3) && \text{factoring the quadratic term} \\
&= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}$$

Thus, we can conclude that $P(k+1)$ is true.

Conclusion: Therefore, $P(n)$ is true for all $n \in \mathbb{N}$ by induction.

Strong Induction

Why Strong Induction?

In **weak induction**, the inductive hypothesis only assumes that $P(k)$ is true and uses that in the inductive step to prove the implication $P(k) \to P(k+1)$.

In **strong induction**, the inductive hypothesis assumes the predicate holds for every step from the base case(s) up to $P(k)$. This usually looks something like $P(b_1) \wedge P(b_2) \wedge \cdots \wedge P(k)$. Then it uses this stronger inductive hypothesis in the inductive step to prove the implication $P(b_1) \wedge \cdots \wedge P(k) \to P(k+1)$.

Strong induction is necessary when we have multiple base cases, or when we need to go back to a smaller number than k in our inductive step.

Strong Induction Template

Let $P(n)$ be "(whatever you're trying to prove)".
We show $P(n)$ holds for all $n \geq b_{min}$ by induction on n.

Base Case: Show $P(b_{min}), P(b_{min+1}), \ldots, P(b_{max})$ are all true.

Inductive Hypothesis: Suppose $P(b_{min}) \wedge \cdots \wedge P(k)$ hold for an arbitrary $k \geq b_{max}$.

Inductive Step: Show $P(k+1)$ (i.e. get $P(b_{min}) \wedge \cdots \wedge P(k) \rightarrow P(k+1)$)

Conclusion: Therefore, $P(n)$ holds for all $n \geq b_{min}$ by the principle of induction.

Task 4: Strong Induction

Consider the function $a(n)$ defined for $n \geqslant 1$ recursively as follows.

$$a(1) = 1$$

$$a(2) = 3$$

$$a(n) = 2a(n-1) - a(n-2) \text{ for } n \geqslant 3$$

Use strong induction to prove that $a(n) = 2n - 1$ for all $n \geqslant 1$.

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Inductive Hypothesis:
Suppose that *P(j)* is true for all integers $1 \leq j \leq k$ for some arbitrary $k \geq 2$.

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Inductive Hypothesis:
Suppose that *P(j)* is true for all integers $1 \leq j \leq k$ for some arbitrary $k \geq 2$.
Inductive Step:
We will show *P(k + 1)* holds.
$a(k + 1) =$

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Inductive Hypothesis:
Suppose that *P(j)* is true for all integers $1 \leq j \leq k$ for some arbitrary $k \geq 2$.
Inductive Step:
We will show *P(k + 1)* holds.
$a(k + 1) = 2a(k) - a(k - 1)$ [Definition of *a*]

$= 2(k + 1) - 1$

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Inductive Hypothesis:
Suppose that *P(j)* is true for all integers $1 \leq j \leq k$ for some arbitrary $k \geq 2$.
Inductive Step:
We will show *P(k + 1)* holds.

$a(k + 1) = 2a(k) - a(k - 1)$ [Definition of *a*]

$= 2(2k - 1) - (2(k - 1) - 1)$ [Inductive Hypothesis]

$= 2(k + 1) - 1$

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Inductive Hypothesis:
Suppose that *P(j)* is true for all integers $1 \leq j \leq k$ for some arbitrary $k \geq 2$.
Inductive Step:
We will show *P(k + 1)* holds.

$a(k + 1) = 2a(k) - a(k - 1)$ [Definition of *a*]
$= 2(2k - 1) - (2(k - 1) - 1)$ [Inductive Hypothesis]
$= 2k + 1$ [Algebra]

$= 2(k + 1) - 1$

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Inductive Hypothesis:
Suppose that *P(j)* is true for all integers $1 \leq j \leq k$ for some arbitrary $k \geq 2$.
Inductive Step:
We will show *P(k + 1)* holds.

$a(k+1) = 2a(k) - a(k-1)$ [Definition of *a*]
$= 2(2k - 1) - (2(k - 1) - 1)$ [Inductive Hypothesis]
$= 2k + 1$ [Algebra]
$= 2(k + 1) - 1$ [Algebra]

Strong Induction

Let ***P(n)* be "*a(n) = 2n − 1*".** We will show that *P(n)* is true for all $n \geq 1$ by strong induction.

Base Cases ($n = 1, n = 2$):
($n = 1$)
$a(1) = 1 = 2 \cdot 1 - 1$
($n = 2$)
$a(2) = 3 = 2 \cdot 2 - 1$
So, *P(1)* and *P(2)* hold.

Inductive Hypothesis:
Suppose that *P(j)* is true for all integers $1 \leq j \leq k$ for some arbitrary $k \geq 2$.
Inductive Step:
We will show *P(k + 1)* holds.

$a(k+1) = 2a(k) - a(k-1)$	[Definition of *a*]
$= 2(2k - 1) - (2(k - 1) - 1)$	[Inductive Hypothesis]
$= 2k + 1$	[Algebra]
$= 2(k + 1) - 1$	[Algebra]

So, *P(k + 1)* holds.

Conclusion:
Therefore, *P(n)* holds for all integers $n \geq 1$ by the principle of strong induction.

That's All, Folks!

Thanks for coming to section this week!
Any questions?