Section 5

CSE 311AC - WI 2022
Allie Pfleger
Kasper Lindberg

Announcements and Reminders

- Check feedback and regrade requests for HW3
- HW 4 due yesterday EOD on Gradescope
- HW 5 out:
    - Part 2 will be graded first!
- Midterm will be next weekend (Friday 2/11 - Sunday 2/13)

References

- Equivalence Reference Sheet
  - https://courses.cs.washington.edu/courses/cse311/21wi/resources/reference-logical_equiv.pdf
- Boolean Algebra Reference Sheet
  - https://courses.cs.washington.edu/courses/cse311/21wi/resources/reference-boolean-alg.pdf
- Inference Reference Sheet
  - https://courses.cs.washington.edu/courses/cse311/19au/docs/InferenceRules.pdf
- Set Definitions
  - https://courses.cs.washington.edu/courses/cse311/19au/docs/SetDefinitions.pdf
- Modular Arithmetic Definitions and Properties
  - https://courses.cs.washington.edu/courses/cse311/20wi/documents/NumberTheoryDefinitions.pdf
- Induction Templates
  - https://courses.cs.washington.edu/courses/cse311/22wi/resources/induction-templates.pdf

Warm-Up

Warm-Up: 1

(a) Calculate gcd(100, 50).

(b) Calculate gcd(17, 31)

(c) Find the multiplicative inverse of 6 (mod 7).

(d) Does 49 have an multiplicative inverse (mod 7)?

Warm-Up: 1

(a) Calculate gcd(100, 50).

50

(a) Calculate gcd(17, 31)

(a) Find the multiplicative inverse of 6 (mod 7).

(a) Does 49 have an multiplicative inverse (mod 7)?

Warm-Up: 1

(a) Calculate gcd(100, 50).

50

(a) Calculate gcd(17, 31)

1

(a) Find the multiplicative inverse of 6 (mod 7).

(a) Does 49 have an multiplicative inverse (mod 7)?

Warm-Up: 1

(a) Calculate gcd(100, 50).

50

(a) Calculate gcd(17, 31)

1

(a) Find the multiplicative inverse of 6 (mod 7).

6

(a) Does 49 have an multiplicative inverse (mod 7)?

Warm-Up: 1

(a) Calculate gcd(100, 50).

50

(a) Calculate gcd(17, 31)

1

(a) Find the multiplicative inverse of 6 (mod 7).

6

(a) Does 49 have an multiplicative inverse (mod 7)?

It does not. Intuitively, this is because 49x for any x is going to be 0 mod 7, which means it can never be 1.

Extended Euclidian Algorithm

Euclid’s Algorithm

```
while(n != 0) {
     int rem = m % n;
     m=n;
     n=rem;
}
```

gcd(660,126)

Euclid’s Algorithm

```
while(n != 0) {
     int rem = m % n;
     m=n;
     n=rem;
}
```

$$
\begin{aligned}
\gcd(660,126) \quad &= \gcd(126, 660 \bmod 126) &&= \gcd(126, 30) \\
&= \gcd(30, 126 \bmod 30) &&= \gcd(30, 6) \\
&= \gcd(6, 30 \bmod 6) &&= \gcd(6, 0) \\
&= 6
\end{aligned}
$$

Tableau form

$$
\begin{aligned}
\boxed{660} &= 5 \cdot \boxed{126} + 30 \\
126 &= 4 \cdot 30 + \textcircled{6} \\
30 &= 5 \cdot 6 + 0
\end{aligned}
$$

$\boxed{\text{Starting Numbers}}$

$\textcircled{\text{Final answer}}$

Bézout’s Theorem

Bézout’s Theorem

If a and b are positive integers, then there exist integers s and t such that

gcd(a,b)$= sa + tb$

We’re not going to prove this theorem…

But we’ll show you how to find s,t for any positive integers a, b.

Extended Euclidian Algorithm

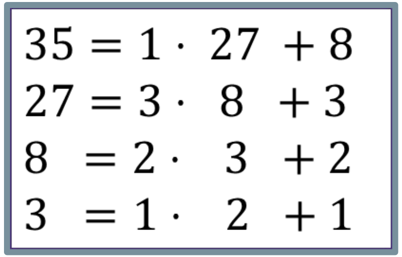
- **Step 1 compute gcd(a,b); keep tableau information.**
- Step 2 solve all equations for the remainder.
- Step 3 substitute backward

gcd(35,27)

Extended Euclidian Algorithm

- **Step 1 compute gcd(a,b); keep tableau information.**
- Step 2 solve all equations for the remainder.
- Step 3 substitute backward

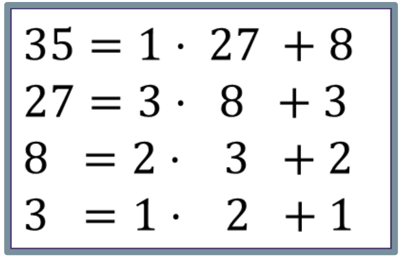
gcd(35,27) = gcd(27, 35%27) = gcd(27,8)
= gcd(8, 27%8) = gcd(8, 3)
= gcd(3, 8%3) = gcd(3, 2)
= gcd(2, 3%2) = gcd(2,1)
= gcd(1, 2%1) = gcd(1,0)



$$\begin{aligned} 35 &= 1 \cdot 27 + 8 \\ 27 &= 3 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Extended Euclidian Algorithm

- Step 1 compute gcd(a,b); keep tableau information.
- **Step 2 solve all equations for the remainder.**
- Step 3 substitute backward



$$\begin{aligned} 35 &= 1 \cdot 27 + 8 \\ 27 &= 3 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

Extended Euclidian Algorithm

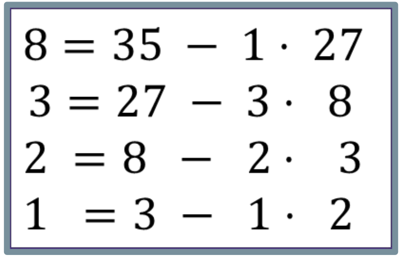
- Step 1 compute gcd(a,b); keep tableau information.
- **Step 2 solve all equations for the remainder.**
- Step 3 substitute backward

$$\begin{aligned}
35 &= 1\cdot 27 + 8\\
27 &= 3\cdot 8 + 3\\
8 &= 2\cdot 3 + 2\\
3 &= 1\cdot 2 + 1
\end{aligned}$$

$$\begin{aligned}
8 &= 35 - 1\cdot 27\\
3 &= 27 - 3\cdot 8\\
2 &= 8 - 2\cdot 3\\
1 &= 3 - 1\cdot 2
\end{aligned}$$

Extended Euclidian Algorithm

- Step 1 compute gcd(a,b); keep tableau information.
- Step 2 solve all equations for the remainder.
- **Step 3 substitute backward**



$$\begin{aligned}8 &= 35 - 1 \cdot 27\\ 3 &= 27 - 3 \cdot 8\\ 2 &= 8 - 2 \cdot 3\\ 1 &= 3 - 1 \cdot 2\end{aligned}$$

Extended Euclidian Algorithm

- Step 1 compute gcd(a,b); keep tableau information.
- Step 2 solve all equations for the remainder.
- **Step 3 substitute backward**

$$\begin{aligned} 8 &= 35 - 1 \cdot 27 \\ 3 &= 27 - 3 \cdot 8 \\ 2 &= 8 - 2 \cdot 3 \\ 1 &= 3 - 1 \cdot 2 \end{aligned}$$

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= -1 \cdot 8 + 2 \cdot 3 \end{aligned}$$

Extended Euclidian Algorithm

- Step 1 compute gcd(a,b); keep tableau information.
- Step 2 solve all equations for the remainder.
- **Step 3 substitute backward**

$$\boxed{\begin{array}{l} 8 = 35 - 1 \cdot 27 \\ 3 = 27 - 3 \cdot 8 \\ 2 = 8 - 2 \cdot 3 \\ 1 = 3 - 1 \cdot 2 \end{array}}$$

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= -1 \cdot 8 + 3 \cdot 3 \\ &= -1 \cdot 8 + 3(27 - 3 \cdot 8) \\ &= 3 \cdot 27 - 10 \cdot 8 \\ &= 3 \cdot 27 - 10(35 - 1 \cdot 27) \\ &= 13 \cdot 27 - 10 \cdot 35 \end{aligned}$$

When substituting back, you keep the larger of m, n and the number you just substituted.
Don't simplify further! (or you lose the form you need)

gcd(27,35) = $13 \cdot 27 + (-10) \cdot 35$

Try it: 2

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

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

Try it: 2

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

Try it: 2

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

First, we find the gcd:

$\gcd(33, 7) = \gcd(7, 5)$ $\quad 33 = 7 \bullet 4 + 5$
$\quad = \gcd(5, 2)$ $\quad 7 = 5 \bullet 1 + 2$
$\quad = \gcd(2, 1)$ $\quad 5 = 2 \bullet 2 + 1$
$\quad = \gcd(1, 0)$ $\quad 2 = 1 \bullet 2 + 0 \ (4) = 1$

Try it: 2

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

First, we find the gcd:

$\gcd(33, 7) = \gcd(7, 5)$
$= \gcd(5, 2)$
$= \gcd(2, 1)$
$= \gcd(1, 0)$

$33 = 7 \bullet 4 + 5$
$7 = 5 \bullet 1 + 2$
$5 = 2 \bullet 2 + 1$
$2 = 1 \bullet 2 + 0$ (4) = 1

Next, we rearrange equations (1) - (3) by solving for the remainder:

$1 = 5 - 2 \bullet 2$ (6)
$2 = 7 - 5 \bullet 1$ (7)
$5 = 33 - 7 \bullet 4$

Try it: 2

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

First, we find the gcd:

$\gcd(33, 7) = \gcd(7, 5)$
$= \gcd(5, 2)$
$= \gcd(2, 1)$
$= \gcd(1, 0)$

$33 = 7 \bullet 4 + 5$
$7 = 5 \bullet 1 + 2$
$5 = 2 \bullet 2 + 1$
$2 = 1 \bullet 2 + 0$ (4) $= 1$

Next, we rearrange equations (1) - (3) by solving for the remainder:

$1 = 5 - 2 \bullet 2$ (6)
$2 = 7 - 5 \bullet 1$ (7)
$5 = 33 - 7 \bullet 4$

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

$1 = 5 - 2 \bullet 2$
$= 5 - (7 - 5 \bullet 1) \bullet 2$
$= 3 \bullet 5 - 7 \bullet 2$
$= 3 \bullet (33 - 7 \bullet 4) - 7 \bullet 2$
$= 33 \bullet 3 + 7 \bullet -14$

Try it: 2

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

First, we find the gcd:

$\gcd(33, 7) = \gcd(7, 5)$ $\quad 33 = 7 \bullet 4 + 5$

$\quad = \gcd(5, 2)$ $\quad 7 = 5 \bullet 1 + 2$

$\quad = \gcd(2, 1)$ $\quad 5 = 2 \bullet 2 + 1$

$\quad = \gcd(1, 0)$ $\quad 2 = 1 \bullet 2 + 0$ (4) $= 1$

Next, we rearrange equations (1) - (3) by solving for the remainder:

$1 = 5 - 2 \bullet 2$ (6)

$2 = 7 - 5 \bullet 1$ (7)

$5 = 33 - 7 \bullet 4$

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

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

So, $1 = 33 \bullet 3 + 7 \bullet -14$.
Thus, $33 - 14 = 19$ is the multiplicative inverse of 7 mod 33

Try it: 2

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

Try it: 2

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

If $7y \equiv 1 \pmod{33}$, then

$$2 \cdot 7y \equiv 2 \pmod{33}.$$

So, $z \equiv 2 \times 19 \pmod{33} \equiv 5 \pmod{33}$. This means that the set of solutions is $\{5 + 33k \mid k \in Z\}$

Induction

Induction Template

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

Base Case: Show ***P(b)*** is true

Inductive Hypothesis: Suppose ***P(k)*** holds for an arbitrary ***k ≥ b***

Inductive Step: Show ***P(k + 1)*** (i.e. get ***P(k) → P(k + 1)***)

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

Induction Template

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

Note: often you will condition ***n*** here, like "all natural numbers ***n***" or "***n* ≥ *0***"

Base Case: Show ***P(b)*** is true

Inductive Hypothesis: Suppose ***P(k)*** holds for an arbitrary ***k* ≥ *b***

Inductive Step: Show ***P(k + 1)*** (i.e. get ***P(k) → 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!

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

We’re going to fill in the template to construct our proof by induction. Yay fun!

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in N$

Let *P(n)* be “”
We show *P(n)* holds for all *n* by induction on *n*.

We need to plug in the thing we want to prove as our *P(n)* and constrain *n* appropriately

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

Let $P(n)$ be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in \mathbb{N}$
We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in N$

Let *P(n)* be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in N$
We show *P(n)* holds for all $n \in N$ by induction on *n*.

Base Case:

Show that the statement we want to prove is true for our base case.

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in$ N

Let *P(n)* be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all n $\in$ N
We show *P(n)* holds for all $n \in$ N by induction on *n*.

<u>Base Case:</u> *P(0)*: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

CAUTION!!! It is easy to accidentally use backwards reasoning in induction proofs, so we try to be very explicit to show ourselves and our readers that we are only proving forwards!

One good way to help avoid backwards reasoning in our base case is to simplify the left side, simplify the right side, and show they are equal to each other.

Let's Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

Let *P(n)* be "$0 + 1 + 2 + \cdots + n = n(n+1)/2$" for all $n \in \mathbb{N}$
We show *P(n)* holds for all $n \in \mathbb{N}$ by induction on *n*.

Base Case: *P(0)*: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis:

This step is pretty much always the same!

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in N$

Let $P(n)$ be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in N$
We show $P(n)$ holds for all $n \in N$ by induction on n.

Base Case: $P(0)$: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

This step is pretty much always the same!

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in N$

Let $P(n)$ be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in N$
We show $P(n)$ holds for all $n \in N$ by induction on n.

Base Case: $P(0)$: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

Inductive Step:

NOW we get to the real meat of the proof.

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in N$

Let *P(n)* be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in N$
We show *P(n)* holds for all $n \in N$ by induction on *n*.

<u>Base Case:</u> *P(0)*: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

<u>Inductive Hypothesis:</u> Suppose *P(k)* holds for some arbitrary integer $k \geq 0$.

<u>Inductive Step:</u> Goal: Show *P(k + 1)*: $0 + 1 + \cdots + (k + 1) = (k + 1)(k + 2)/2$

It can be really helpful to list the goal for this step, to remind yourself where you need to go!

Now, we start with the algebraic manipulation! To avoid backwards reasoning here, remember to start with the left side, and keep going until you reach the right. If it all goes well, you’ll use the IH somewhere, and that’s induction!

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in N$

Let *P(n)* be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in N$
We show *P(n)* holds for all $n \in N$ by induction on n.

Base Case: *P(0)*: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose *P(k)* holds for some arbitrary integer $k \geq 0$.

Inductive Step: Goal: Show *P(k + 1)*: $0 + 1 + \cdots + (k + 1) = (k + 1)(k + 2)/2$
$0 + 1 + \cdots + k + (k + 1) =$

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

Let $P(n)$ be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in \mathbb{N}$
We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

Inductive Step: Goal: Show $P(k+1)$: $0 + 1 + \cdots + (k + 1) = (k + 1)(k + 2)/2$

$$0 + 1 + \cdots + k + (k + 1) = (0 + 1 + \cdots + k) + (k + 1)$$

Let's Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

Let $P(n)$ be "$0 + 1 + 2 + \cdots + n = n(n+1)/2$" for all $n \in \mathbb{N}$
We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

Inductive Step: Goal: Show $P(k+1)$: $0 + 1 + \cdots + (k+1) = (k+1)(k+2)/2$

$$
\begin{aligned}
0 + 1 + \cdots + k + (k+1) &= (0 + 1 + \cdots + k) + (k+1) \\
&= k(k+1)/2 + (k+1) && \text{by I.H.}
\end{aligned}
$$

This step is KEY! We're able to substitute that whole messy part with the … for a closed expression BECAUSE we use our inductive hypothesis.

Make sure you ALWAYS point out when you use that I.H., so you keep things clear for your reader and yourself!

Let's Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

Let *P(n)* be "$0 + 1 + 2 + \cdots + n = n(n+1)/2$" for all $n \in \mathbb{N}$
We show *P(n)* holds for all $n \in \mathbb{N}$ by induction on *n*.

Base Case: *P(0)*: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose *P(k)* holds for some arbitrary integer $k \geq 0$.

Inductive Step: Goal: Show *P(k + 1)*: $0 + 1 + \cdots + (k + 1) = (k + 1)(k + 2)/2$

$$\begin{aligned} 0 + 1 + \cdots + k + (k + 1) &= (0 + 1 + \cdots + k) + (k + 1) \\ &= k(k + 1)/2 + (k + 1) && \text{by I.H.} \\ &= k(k + 1)/2 + 2(k + 1)/2 \end{aligned}$$

Let’s Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

Let *P(n)* be “$0 + 1 + 2 + \cdots + n = n(n+1)/2$” for all $n \in \mathbb{N}$
We show *P(n)* holds for all $n \in \mathbb{N}$ by induction on *n*.

<u>Base Case:</u> *P(0)*: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

<u>Inductive Hypothesis:</u> Suppose *P(k)* holds for some arbitrary integer $k \geq 0$.

<u>Inductive Step:</u> Goal: Show *P(k + 1)*: $0 + 1 + \cdots + (k + 1) = (k + 1)(k + 2)/2$

$$\begin{aligned}
0 + 1 + \cdots + k + (k + 1) &= (0 + 1 + \cdots + k) + (k + 1) \\
&= k(k + 1)/2 + (k + 1) && \text{by I.H.} \\
&= k(k + 1)/2 + 2(k + 1)/2 \\
&= (k(k + 1) + 2(k + 1))/2
\end{aligned}$$

Let's Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in N$

Let $P(n)$ be "$0 + 1 + 2 + \cdots + n = n(n+1)/2$" for all $n \in N$
We show $P(n)$ holds for all $n \in N$ by induction on n.

<u>Base Case:</u> $P(0)$: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

<u>Inductive Hypothesis:</u> Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

<u>Inductive Step:</u> Goal: Show $P(k+1)$: $0 + 1 + \cdots + (k+1) = (k+1)(k+2)/2$

$$\begin{aligned}0 + 1 + \cdots + k + (k+1) &= (0 + 1 + \cdots + k) + (k+1) \\ &= k(k+1)/2 + (k+1) && \text{by I.H.} \\ &= k(k+1)/2 + 2(k+1)/2 \\ &= (k(k+1) + 2(k+1))/2 \\ &= (k+1)(k+2)/2 && \text{factoring out } (k+1)\end{aligned}$$

Let's Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathrm{N}$

Let *P(n)* be "$0 + 1 + 2 + \cdots + n = n(n+1)/2$" for all $n \in \mathrm{N}$
We show *P(n)* holds for all $n \in \mathrm{N}$ by induction on *n*.

Base Case: *P(0)*: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose *P(k)* holds for some arbitrary integer $k \geq 0$.

Inductive Step: Goal: Show *P(k + 1)*: $0 + 1 + \cdots + (k + 1) = (k + 1)(k + 2)/2$

$$\begin{aligned} 0 + 1 + \cdots + k + (k + 1) &= (0 + 1 + \cdots + k) + (k + 1) \\ &= k(k + 1)/2 + (k + 1) && \text{by I.H.} \\ &= k(k + 1)/2 + 2(k + 1)/2 \\ &= (k(k + 1) + 2(k + 1))/2 \\ &= (k + 1)(k + 2)/2 && \text{factoring out } (k+1) \end{aligned}$$

We have shown *P(k+1)*!

Let's Try it: 6a

Show using induction that
$0 + 1 + 2 + \cdots + n = n(n+1)/2$ for all $n \in \mathbb{N}$

Let $P(n)$ be "$0 + 1 + 2 + \cdots + n = n(n+1)/2$" for all $n \in \mathbb{N}$
We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: Left side: 0, Right side: $0(0+1)/2 = 0$, the two are equal so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

Inductive Step: Goal: Show $P(k+1)$: $0 + 1 + \cdots + (k + 1) = (k + 1)(k + 2)/2$

$$
\begin{aligned}
0 + 1 + \cdots + k + (k + 1) &= (0 + 1 + \cdots + k) + (k + 1) \\
&= k(k + 1)/2 + (k + 1) && \text{by I.H.} \\
&= k(k + 1)/2 + 2(k + 1)/2 \\
&= (k(k + 1) + 2(k + 1))/2 \\
&= (k + 1)(k + 2)/2 && \text{factoring out } (k+1)
\end{aligned}
$$

We have shown $P(k+1)$!

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

That’s All, Folks!

Any questions?