南方科技大學
SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY

CS201 DISCRETE MATHEMATICS FOR COMPUTER SCIENCE

Dr. Qi Wang

Department of Computer Science and Engineering
Office: Room903, Nanshan iPark A7 Building
Email: wangqi@sustech.edu.cn

Number Theory and Cryptography

- Division, Primes
- Congruence
- Greatest Common Divisor (GCD)
- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $$a = dq + r$$

- Congruence
- Greatest Common Divisor (GCD)
- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \qquad q = a \; div \; d \qquad r = a \; mod \; d$

- Congruence
- Greatest Common Divisor (GCD)
- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \qquad q = a \ div \ d \qquad r = a \ mod \ d$

- Congruence

- Greatest Common Divisor (GCD)

- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \quad q = a \textit{ div } d \quad r = a \textit{ mod } d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \quad q = a \; div \; d \quad r = a \; mod \; d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \qquad q = a \textit{ div } d \qquad r = a \textit{ mod } d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

  (extended) Euclidean algorithm

- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

$$a = dq + r \qquad q = a \textit{ div } d \qquad r = a \textit{ mod } d$$

- Congruence

$$a \equiv b \pmod{m} \text{ if } m \text{ divides } a - b$$

- Greatest Common Divisor (GCD)

Find the GCD of 286 and 503.

$$\begin{aligned}
&\gcd(503, 286) && 503 = 1 \cdot 286 + 217 \\
&= \gcd(286, 217) && 286 = 1 \cdot 217 + 69 \\
&= \gcd(217, 69) && 217 = 3 \cdot 69 + 10 \\
&= \gcd(69, 10) && 69 = 6 \cdot 10 + 9 \\
&= \gcd(10, 9) && 10 = 1 \cdot 9 + 1 \\
&= 1 && 9 = 9 \cdot 1
\end{aligned}$$

$$\begin{aligned}
1 &= 10 - 1 \cdot 9 \\
1 &= 7 \cdot 10 - 1 \cdot 69 \\
1 &= 7 \cdot 217 - 22 \cdot 69 \\
1 &= 29 \cdot 217 - 22 \cdot 286 \\
1 &= 29 \cdot 503 - 51 \cdot 286
\end{aligned}$$

- E

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \qquad q = a \ \mathit{div} \ d \qquad r = a \ \mathit{mod} \ d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

  (extended) Euclidean algorithm
  find the modular inverse
  solve linear congruence $ax \equiv b \pmod{m}$ $(\gcd(a, m) = 1)$

- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \qquad q = a \text{ } div \text{ } d \qquad r = a \text{ } mod \text{ } d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

  (extended) Euclidean algorithm
  find the modular inverse
  solve linear congruence $ax \equiv b \pmod{m}$ $(\gcd(a, m) = 1)$
  Chinese Remainder Theorem / back substitution

- Euler's Theorem / Fermart's Little Theorem

Number Theory and Cryptography

- Division, Primes

  $a = dq + r \qquad q = a \ div \ d \qquad r = a \ mod \ d$

- Congruence

  $a \equiv b \pmod{m}$ if m divides $a - b$

- Greatest Common Divisor (GCD)

  (extended) Euclidean algorithm
  find the modular inverse
  solve linear congruence $ax \equiv b \pmod{m}$ $(\gcd(a, m) = 1)$
  Chinese Remainder Theorem / back substitution

- Euler's Theorem / Fermart's Little Theorem

  $x^{\phi(n)} \equiv 1 \bmod n$ if $\gcd(x, n) = 1$
  $x^{p-1} \equiv 1 \bmod p$ if $x \not\equiv 0 \bmod p$

RSA Variant

$\mathcal{Q}$: Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \mathrm{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)

RSA Variant

$\mathcal{Q}$: Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \mathrm{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)

Case I: $\gcd(M, n) = 1$

$$\begin{aligned} C^{d'} \bmod n &= M^{ed'} \bmod n = M^{k\lambda(n)+1} \bmod n \\ &= (M^{k\lambda(n)} \bmod n) M \bmod n \\ &= \left(M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod n\right)^k M \bmod n \end{aligned}$$

By Fermat's theorem, $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod p = \left(M^{(q-1)/\gcd(p-1,q-1)}\right)^{p-1} \bmod p = 1$ and $M^{(p-1)(q-1)/\gcd(p-1,q-1)} \bmod q = 1$. Then by Chinese Remainder Theorem, we have $C^{d'} \bmod n = M$.

RSA Variant

$\mathcal{Q}$: Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \mathrm{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)

Case II: $\gcd(M, n) = p$

$M = tp$ for some integer $0 < t < q$. We have $\gcd(M, q) = 1$ and $ed' = k\lambda(n) + 1$ for some integer k. By Fermat's theorem, we have

$(M^{k\lambda(n)} - 1) \bmod q = (M^{k(p-1)(q-1)/\gcd(p-1,q-1)} - 1) \bmod q = 0.$

Then

$$\begin{aligned}
(M^{ed'} - M) \bmod n &= M(M^{ed'-1} - 1) \bmod n \\
&= tp(M^{k\lambda(n)} - 1) \bmod pq \\
&= 0
\end{aligned}$$

RSA Variant

$\mathcal{Q}$: Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \mathrm{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)

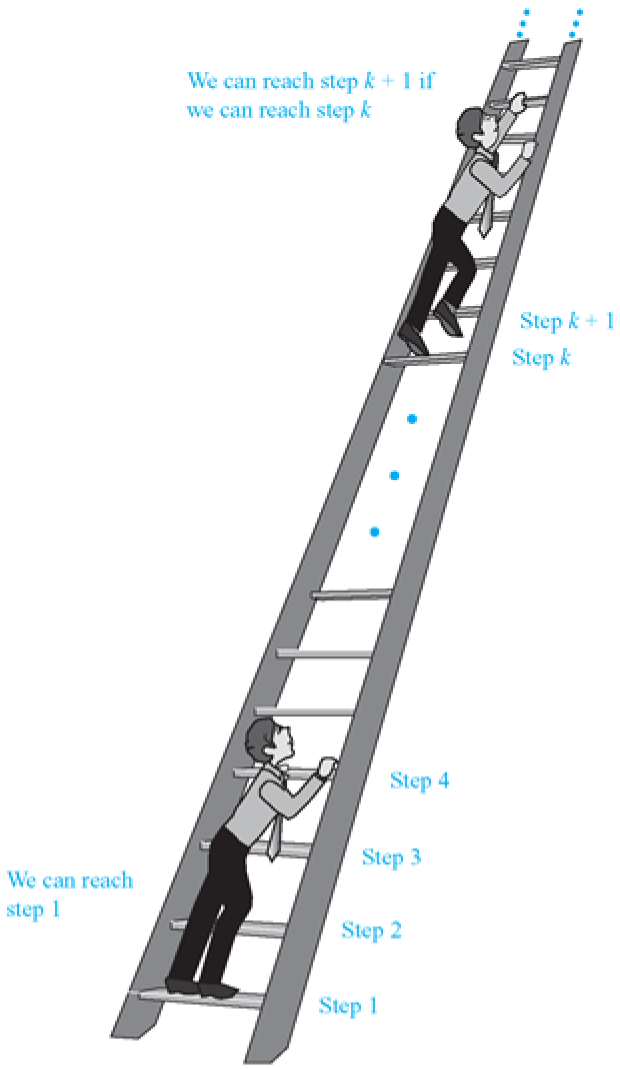
<u>Case III:</u> $\gcd(M, n) = q$

Similar to Case II.

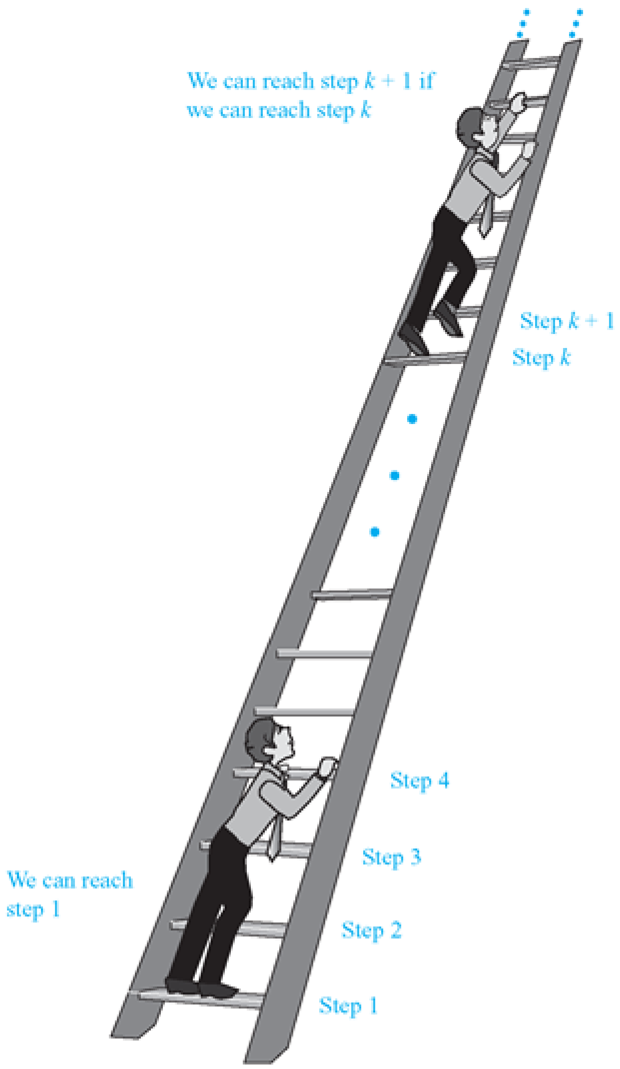
<u>Case IV:</u> $\gcd(M, n) = pq$

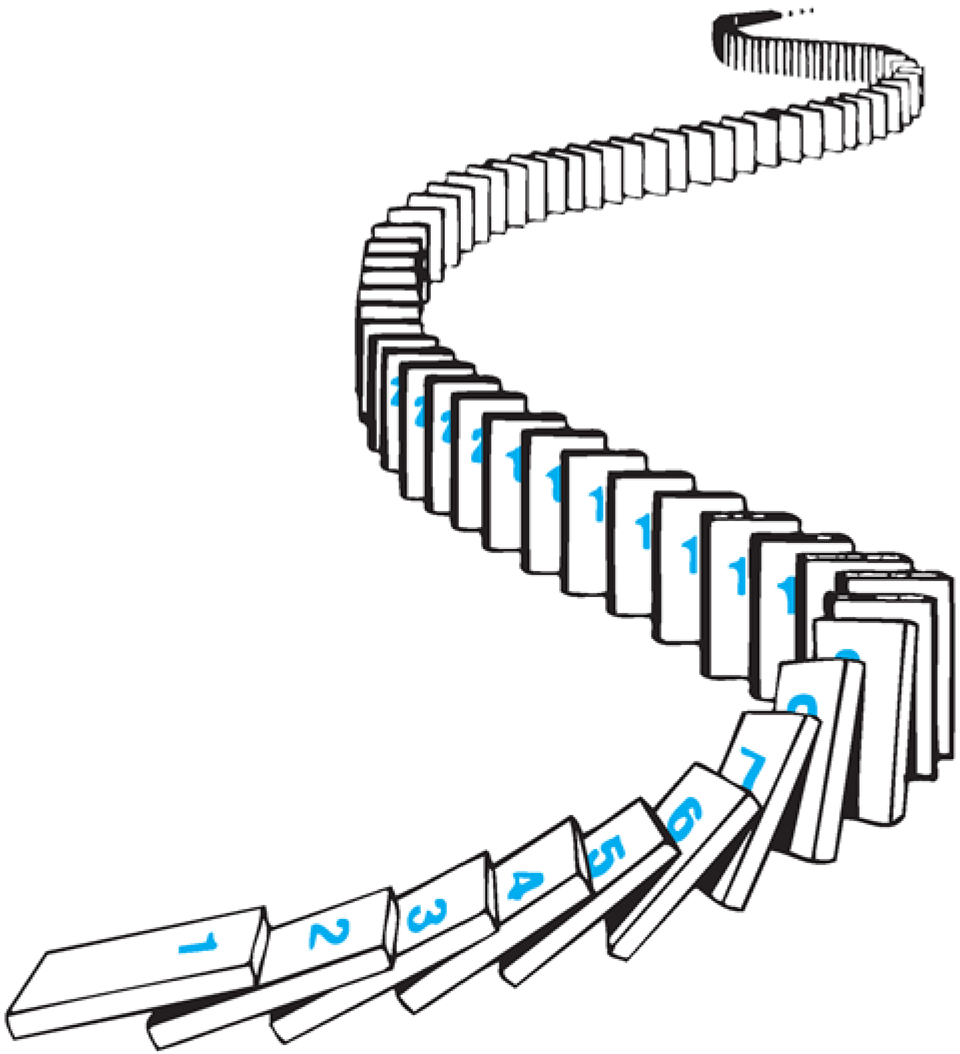
Trivial.

Mathematical Induction



Mathematical Induction





Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.

Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.
- This leads us to transform the *indirect proof* of proof by counterexample to *direct proof*. This direct proof technique will be **induction**.

Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.

- This leads us to transform the *indirect proof* of proof by counterexample to *direct proof*. This direct proof technique will be **induction**.

- We conclude by distinguishing between the *weak principle* of mathematical induction and the *strong principle* of mathematical induction.

Mathematical Induction

- We start by reviewing proof by smallest counterexample to try and understand what it is really doing.

- This leads us to transform the *indirect proof* of proof by counterexample to *direct proof*. This direct proof technique will be **induction**.

- We conclude by distinguishing between the *weak principle* of mathematical induction and the *strong principle* of mathematical induction.

  The *strong principle* can actually be derived from the *weak principle*.

Proof by Smallest Counterexample

- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

Proof by Smallest Counterexample

- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

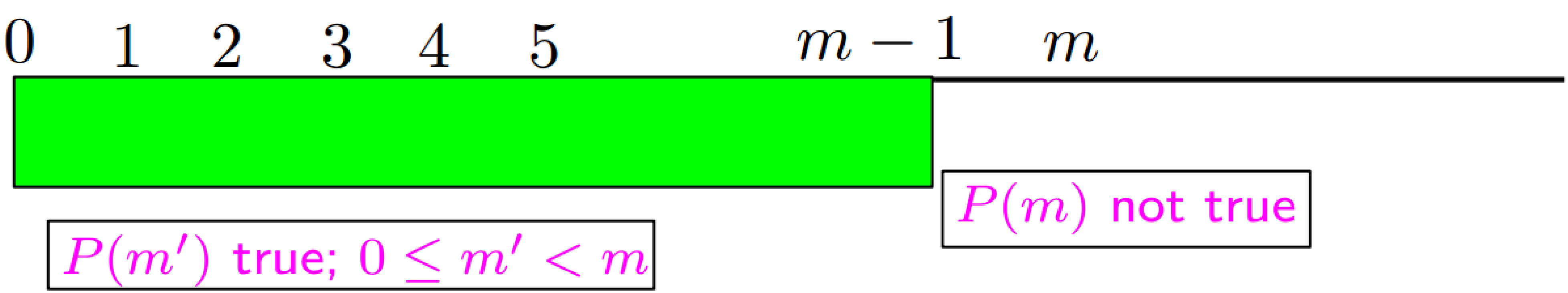
Proof by Smallest Counterexample

- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

  (ii) Let $m > 0$ be the smallest value for which $P(n)$ is false



Proof by Smallest Counterexample

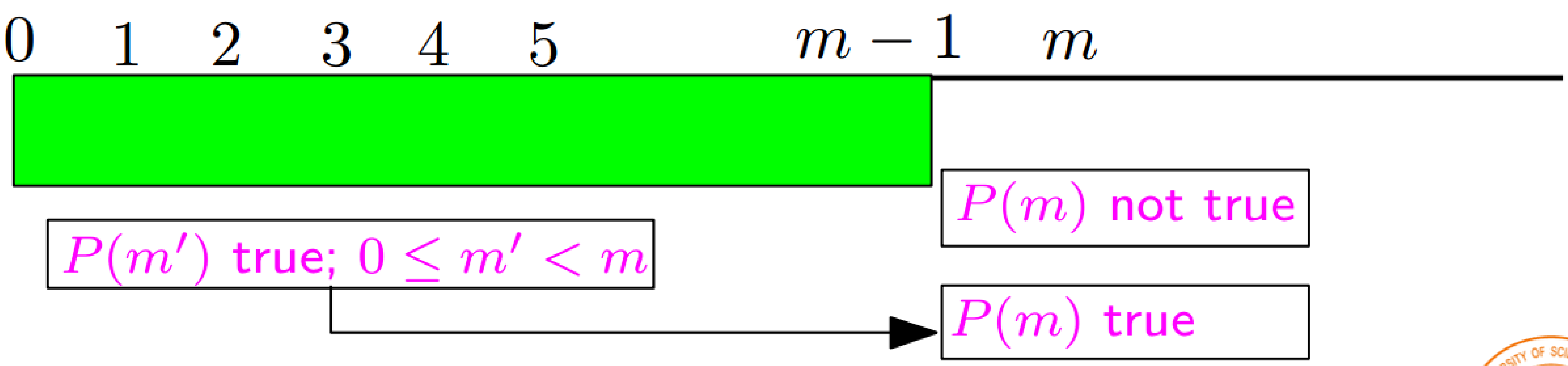
- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

  (ii) Let $m > 0$ be the smallest value for which $P(n)$ is false

  (iii) Then use the fact that $P(m')$ is true for all $0 \le m' < m$ to show that $P(m)$ is true, contradicting the choice of m.



Proof by Smallest Counterexample

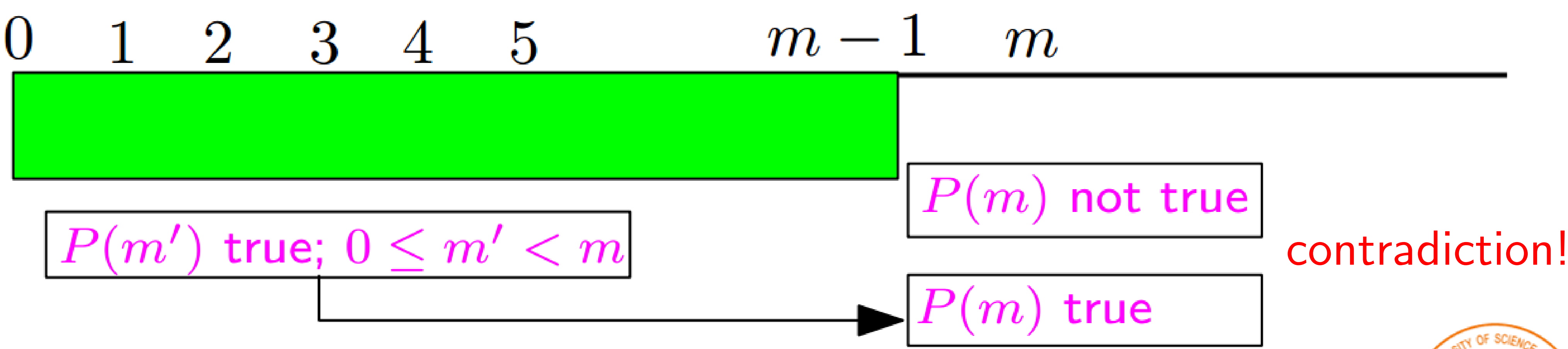
- The statement $P(n)$ is true for all $n = 0, 1, 2, \ldots$

  We prove this by

  (i) Assume that a counterexample exists, i.e., There is some $n > 0$ for which $P(n)$ is false

  (ii) Let $m > 0$ be the smallest value for which $P(n)$ is false

  (iii) Then use the fact that $P(m')$ is true for all $0 \leq m' < m$ to show that $P(m)$ is true, contradicting the choice of m.



Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

  - Suppose that $(*)$ is not always true

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0+1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

◇ Suppose that $(*)$ is not always true

◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0 + 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

◇ Suppose that $(*)$ is not always true

◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n

◇ For any nonnegative integer $i < n$,

$$1 + 2 + \cdots + i = \frac{i(i+1)}{2}$$

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0+1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

  - ◇ Suppose that $(*)$ is not always true
  - ◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n
  - ◇ For any nonnegative integer $i < n$,

$$1+2+\cdots+i=\frac{i(i+1)}{2}$$

  - ◇ Since $0 = 0 \cdot 1/2$, $(*)$ holds for $n = 0$

Example 1

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$(*) \qquad 0+1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

◇ Suppose that $(*)$ is not always true

◇ Then there must be a smallest $n \in N$ s.t. $(*)$ does not hold for n

◇ For any nonnegative integer $i < n$,

$$1+2+\cdots+i=\frac{i(i+1)}{2}$$

◇ Since $0 = 0 \cdot 1/2$, $(*)$ holds for $n = 0$

◇ The smallest counterexample n is larger than 0

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  - Substituting $n-1$ for i gives
$$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  - Substituting $n-1$ for i gives
  $$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$
  - Adding n to both sides gives
  $$1+2+\cdots+n-1+n=\frac{(n-1)n}{2}+n=\frac{n(n+1)}{2}$$

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  - Substituting $n-1$ for i gives
    $$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$
  - Adding n to both sides gives
    $$1+2+\cdots+n-1+n=\frac{(n-1)n}{2}+n=\frac{n(n+1)}{2}$$
  - Thus, n is not a counterexample. Contradiction!

Example 1

- We now have
  (i) smallest counterexample n is greater than 0, and
  (ii) $(*)$ holds for $n-1$

  - ◇ Substituting $n-1$ for i gives
  $$1+2+\cdots+n-1=\frac{(n-1)n}{2}$$
  - ◇ Adding n to both sides gives
  $$1+2+\cdots+n-1+n=\frac{(n-1)n}{2}+n=\frac{n(n+1)}{2}$$
  - ◇ Thus, n is not a counterexample. Contradiction!
  - ◇ Therefore, $(*)$ holds for all positive integers n.

Example 1

- What implication did we have to prove?

Example 1

- What implication did we have to prove?

  The key step was proving that

$$P(n-1) \to P(n)$$

  where $P(n)$ is the statement

$$1+2+\cdots+n = \frac{n(n+1)}{2}$$

Example 2

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$2^{n+1} \geq n^2 + 2.$$

Example 2

- Use proof by smallest counterexample to show that, $\forall n \in N$, $$2^{n+1} \geq n^2 + 2.$$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$. We start by assuming that the statement
  $$\forall n \in N \ P(n)$$
  is false.

Example 2

- Use proof by smallest counterexample to show that, $\forall n \in N$,

$$2^{n+1} \geq n^2 + 2.$$

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$. We start by assuming that the statement

$$\forall n \in N \ P(n)$$

is false.

When a for all quantifier is false, there must be some n for which it is false. Let n be the smallest nonnegative integer for which $2^{n+1} \ngeq n^2 + 2$.

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  This means that, for all $i \in N$ with $i < n$,
  $$2^{i+1} \geq i^2 + 2$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  This means that, for all $i \in N$ with $i < n$,
  $$2^{i+1} \geq i^2 + 2$$

  Since $2^{0+1} \geq 0^2 + 2$, we know that $n > 0$. Thus, $n - 1$ is a nonnegative integer less than n.

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  This means that, for all $i \in N$ with $i < n$,
  $$2^{i+1} \geq i^2 + 2$$

  Since $2^{0+1} \geq 0^2 + 2$, we know that $n > 0$. Thus, $n - 1$ is a nonnegative integer less than n.

  Then setting $i = n - 1$ gives
  $$2^{(n-1)+1} \geq (n-1)^2 + 2.$$

  or
  $$(*) \quad 2^n \geq n^2 - 2n + 1 + 2 = n^2 - 2n + 3$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\qquad (*)$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\quad (*)$

  Multiply both sides by 2, giving

$$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $(*)$

  Multiply both sides by 2, giving

  $$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

  To get a contradiction, we want to convert the right side into $n^2 + 2$ plus an additional nonnegative term.

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\qquad (*)$

  Multiply both sides by 2, giving
  $$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

  To get a contradiction, we want to convert the right side into $n^2 + 2$ plus an additional nonnegative term.

  Thus, we write
  $$\begin{aligned} 2^{n+1} &\geq 2n^2 - 4n + 6 \\ &= (n^2 + 2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n - 2)^2 \\ &\geq n^2 + 2. \end{aligned}$$

Example 2

- Let n be the smallest nonnegative integer for which $2^{n+1} \not\geq n^2 + 2$.

  We are now given $2^n \geq n^2 - 2n + 3$. $\quad (*)$

  Multiply both sides by 2, giving

  $$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot (n^2 - 2n + 3) = 2n^2 - 4n + 6.$$

  To get a contradiction, we want to convert the right side into $n^2 + 2$ plus an additional nonnegative term.

  Thus, we write

  $$\begin{aligned} 2^{n+1} &\geq 2n^2 - 4n + 6 \\ &= (n^2 + 2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n - 2)^2 \\ \text{contradiction!} \quad &\geq n^2 + 2. \end{aligned}$$

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \to P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \to P(n)$

  - ◇ Suppose there is some n for which $P(n)$ is false $(*)$
  - ◇ Let n be the smallest counterexample

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \to P(n)$

  - ◇ Suppose there is some n for which $P(n)$ is false $(*)$
  - ◇ Let n be the smallest counterexample
  - ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

  ◇ Let n be the smallest counterexample

  ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

  ◇ Therefore, from (b), using direct inference, $P(n)$ is true

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

  ◇ Let n be the smallest counterexample

  ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

  ◇ Therefore, from (b), using direct inference, $P(n)$ is true

  ◇ This contradicts $(*)$.

Example 2

- Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  ◇ Suppose there is some n for which $P(n)$ is false $(*)$

  ◇ Let n be the smallest counterexample

  ◇ Then, from (a) $n > 0$, so $P(n-1)$ is true

  ◇ Therefore, from (b), using direct inference, $P(n)$ is true

  ◇ This contradicts $(*)$.

  ◇ Thus, $P(n)$ is true for all $n \in N$.

Example 2

- What did we really do?

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

Example 2

- What did we really do?

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \to P(n)$

  We then used proof by smallest counterexample to derive that $P(n)$ is true for all $n \in N$.

Example 2

- What did we really do?

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  We just showed that

  (a) $P(0)$ is true

  (b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

  We then used proof by smallest counterexample to derive that $P(n)$ is true for all $n \in N$.

  This is an *indirect proof*. Is it possible to prove this fact *directly*?

Example 2

- What did we really do?

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

We just showed that

(a) $P(0)$ is true

(b) if $n > 0$, then $P(n-1) \rightarrow P(n)$

We then used proof by smallest counterexample to derive that $P(n)$ is true for all $n \in N$.

This is an *indirect proof*. Is it possible to prove this fact *directly*?

Since $P(n-1) \rightarrow P(n)$, we see that

$P(0)$ implies $P(1)$, $P(1)$ implies $P(2)$, ...

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

  This is actually **equivalent** to the *principle of mathematical induction*.

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

  This is actually **equivalent** to the *principle of mathematical induction*.

  Principle. (*the Weak Principle of Mathematical Induction*)
  (a) If the statement $P(b)$ is true
  (b) the statement $P(n-1) \to P(n)$ is true for all $n > b$,
  then $P(n)$ is true for all integers $n \geq b$

The Principle of Mathematical Induction

- The *well-ordering* principle permits us to assume that every set of nonnegative integers has a smallest element, allowing us to use the smallest counterexample.

  This is actually **equivalent** to the *principle of mathematical induction*.

  Principle. (*the Weak Principle of Mathematical Induction*)
  (a) If the statement $P(b)$ is true
  (b) the statement $P(n-1) \rightarrow P(n)$ is true for all $n > b$,
  then $P(n)$ is true for all integers $n \geq b$

  (a) – *Basic Step* *Inductive Hypothesis*

  (b) – *Inductive Step* *Inductive Conclusion*

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  (i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  (i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

  (ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2 \qquad (*)$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  (i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

  (ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2 \qquad (*)$

$$
\begin{aligned}
2^{n+1} &\geq 2(n-1)^2 + 4 \\
&= (n^2 + 2) + (n^2 - 4n + 4) \\
&= n^2 + 2 + (n-2)^2 \\
&\geq n^2 + 2
\end{aligned}
$$

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

(i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

(ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2 \qquad (*)$

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 4 \\ &= (n^2 + 2) + (n^2 - 4n + 4) \\ &= n^2 + 2 + (n-2)^2 \\ &\geq n^2 + 2 \end{aligned}$$

Hence, we've just prove that for $n > 0$, $P(n-1) \rightarrow P(n)$.

Proof by Induction

- $\forall n \geq 0,\ 2^{n+1} \geq n^2 + 2$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 2$

  (i) Note that for $n = 0$, $2^{0+1} = 2 \geq 2 = 0^2 + 2$ – $P(0)$

  (ii) Suppose that $n > 0$ and that $2^n \geq (n-1)^2 + 2$ $\qquad (*)$

$$
\begin{aligned}
2^{n+1} &\geq 2(n-1)^2 + 4 \\
&= (n^2 + 2) + (n^2 - 4n + 4) \\
&= n^2 + 2 + (n-2)^2 \\
&\geq n^2 + 2
\end{aligned}
$$

  Hence, we've just prove that for $n > 0$, $P(n-1) \rightarrow P(n)$.

  By mathematical induction, $\forall n > 0,\ 2^{n+1} \geq n^2 + 2$.

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

Proof by Induction

- $\forall n \geq 2$, $2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

  (ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

(i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

(ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 6 \\ &= n^2 + 3 + n^2 - 4n + 4 + 1 \\ &= n^2 + 3 + (n-2)^2 + 1 \\ &> n^2 + 3 \end{aligned}$$

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

  Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

  (i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

  (ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 6 \\ &= n^2 + 3 + n^2 - 4n + 4 + 1 \\ &= n^2 + 3 + (n-2)^2 + 1 \\ &> n^2 + 3 \end{aligned}$$

  Hence, we've just prove that for $n > 2$, $P(n-1) \rightarrow P(n)$.

Proof by Induction

- $\forall n \geq 2$, $2^{n+1} \geq n^2 + 3$

Let $P(n)$ – $2^{n+1} \geq n^2 + 3$

(i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

(ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

$$\begin{aligned} 2^{n+1} &\geq 2(n-1)^2 + 6 \\ &= n^2 + 3 + n^2 - 4n + 4 + 1 \\ &= n^2 + 3 + (n-2)^2 + 1 \\ &> n^2 + 3 \end{aligned}$$

Hence, we've just prove that for $n > 2$, $P(n-1) \to P(n)$.

By mathematical induction, $\forall n > 2$, $2^{n+1} \geq n^2 + 3$.

Proof by Induction

- $\forall n \geq 2,\ 2^{n+1} \geq n^2 + 3$

Let $P(n)$ – $2^{n+1} \geq n^2 + 3$ Base Step

(i) Note that for $n = 2$, $2^{2+1} = 8 \geq 7 = 2^2 + 3$ – $P(2)$

(ii) Suppose that $n > 2$ and that $2^n \geq (n-1)^2 + 3 \qquad (*)$

Inductive Hypothesis

$$
\begin{aligned}
2^{n+1} &\geq 2(n-1)^2 + 6 \\
&= n^2 + 3 + n^2 - 4n + 4 + 1 \\
&= n^2 + 3 + (n-2)^2 + 1 \\
&> n^2 + 3
\end{aligned}
$$

Inductive Step

Hence, we've just prove that for $n > 2$, $P(n-1) \rightarrow P(n)$.

By mathematical induction, $\forall n > 2,\ 2^{n+1} \geq n^2 + 3$.

Inductive Conclusion

Another Form of Induction

- We may have another form of *direct proof* as follows.

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$
  - ◇ Next suppose that we have a proof that, $\forall k > 0$,

$$P(0) \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \rightarrow P(k)$$

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$
  - ◇ Next suppose that we have a proof that, $\forall k > 0$,

$$P(0) \land P(1) \land P(2) \land \cdots \land P(k-1) \rightarrow P(k)$$

  - ◇ Then, $P(0)$ implies $P(1)$

$P(0) \land P(1)$ implies $P(2)$

$P(0) \land P(1) \land P(2)$ implies $P(3)$ ...

Another Form of Induction

- We may have another form of *direct proof* as follows.
  - ◇ First suppose that we have proof of $P(0)$
  - ◇ Next suppose that we have a proof that, $\forall k > 0$,
$$P(0) \wedge P(1) \wedge P(2) \wedge \cdots \wedge P(k-1) \rightarrow P(k)$$
  - ◇ Then, $P(0)$ implies $P(1)$
$P(0) \wedge P(1)$ implies $P(2)$
$P(0) \wedge P(1) \wedge P(2)$ implies $P(3)$ ...
  - ◇ Iterating gives us a proof of $P(n)$ for all n

Strong Induction

- **Principle** (*The Strong Principle of Mathematical Induction*)

  (a) If the statement $P(b)$ is true

  (b) for all $n > b$, the statement
  $P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \rightarrow P(n)$ is true.

  then $P(n)$ is true for all integers $n \geq b$.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.
    - ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

  ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

  ◇ Inductive Hypothesis: Suppose that every number less than n is a power of a prime or a product of powers of primes.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

  ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

  ◇ Inductive Hypothesis: Suppose that every number less than n is a power of a prime or a product of powers of primes.

  ◇ Then, if n is not a prime power, it is a product of two smaller numbers, each of which is, by the inductive hypothesis, a power of a prime or a product of powers of primes.

Example

- Prove that every positive integer is a power of a prime or the product of powers of primes.

  ◇ Base Step: 1 is a power of a prime number, $1 = 2^0$

  ◇ Inductive Hypothesis: Suppose that every number less than n is a power of a prime or a product of powers of primes.

  ◇ Then, if n is not a prime power, it is a product of two smaller numbers, each of which is, by the inductive hypothesis, a power of a prime or a product of powers of primes.

  ◇ Thus, by the strong principle of mathematical induction, every positive integer is a power of a prime or a product of powers of primes.

Mathematical Induction

- In practice, we do not usually explicitly distinguish between the weak and strong forms.

Mathematical Induction

- In practice, we do not usually explicitly distinguish between the weak and strong forms.

- In reality, they are equivalent to each other in that the weak form is a special case of the strong form, and the strong form can be derived from the weak form.

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

  1. We show that $P(b)$ is true. – Base Step

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

  1. We show that $P(b)$ is true. – Base Step
  2. We then, $\forall n > b$, show either

$$(*) \qquad P(n-1) \rightarrow P(n)$$

or

$$(**) \qquad P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \rightarrow P(n)$$

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

  1. We show that $P(b)$ is true. – Base Step
  2. We then, $\forall n > b$, show either

     $$(*) \qquad P(n-1) \to P(n)$$

     or

     $$(**) \qquad P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \to P(n)$$

     We need to make the inductive hypothesis of either $P(n-1)$ or $P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1)$.We then use $(*)$ or $(**)$ to derive $P(n)$.

Summary

- A *typical* proof by mathematical induction, showing that a statement $P(n)$ is true for all integers $n \geq b$ consists of three steps:

1. We show that $P(b)$ is true. – Base Step
2. We then, $\forall n > b$, show either

$$(*) \qquad P(n-1) \to P(n)$$

or

$$(**) \qquad P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1) \to P(n)$$

   We need to make the inductive hypothesis of either $P(n-1)$ or $P(b) \wedge P(b+1) \wedge \cdots \wedge P(n-1)$.We then use $(*)$ or $(**)$ to derive $P(n)$.

3. We conclude on the basis of the principle of mathematical induction that $P(n)$ is true for all $n \geq b$.

Recursion

- Recursive computer programs or algorithms often lead to inductive analysis.

Recursion

- Recursive computer programs or algorithms often lead to inductive analysis.

- A classical example of *recursion* is the **Towers of Hanoi** Problem.

Towers of Hanoi

Towers of Hanoi

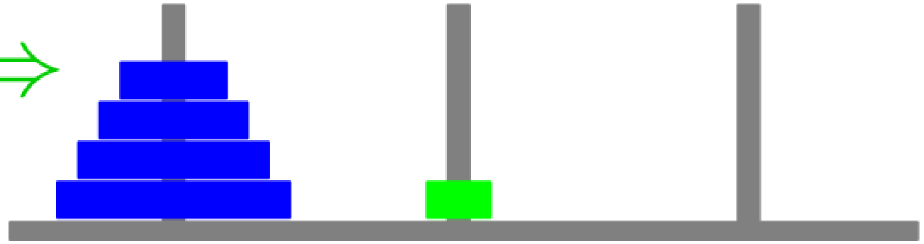
- 3 pegs; n disks of different sizes
- A *legal move* takes a disk from one peg and moves it onto another peg so that it is not on top of a smaller disk
- **Problem**: Find a (efficient) way to move all of the disks from one peg to another

Towers of Hanoi

Towers of Hanoi

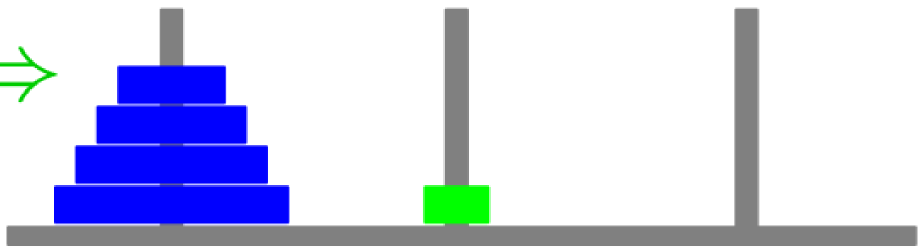
legal move

⇒

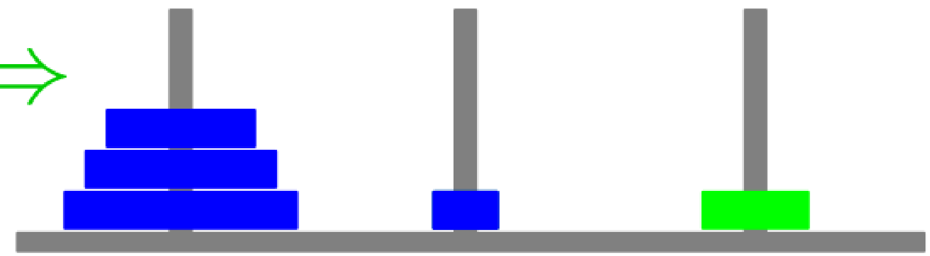


Towers of Hanoi

legal move

$\Rightarrow$ 

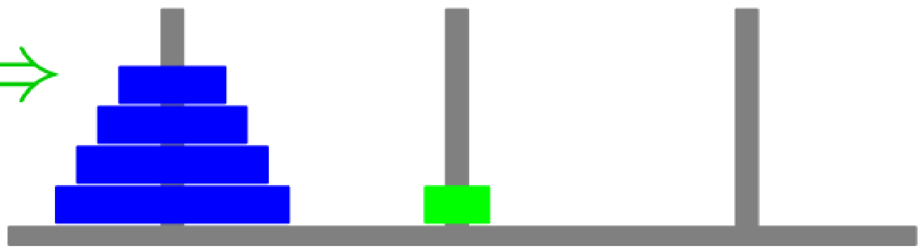
legal move

$\Rightarrow$ 

Towers of Hanoi

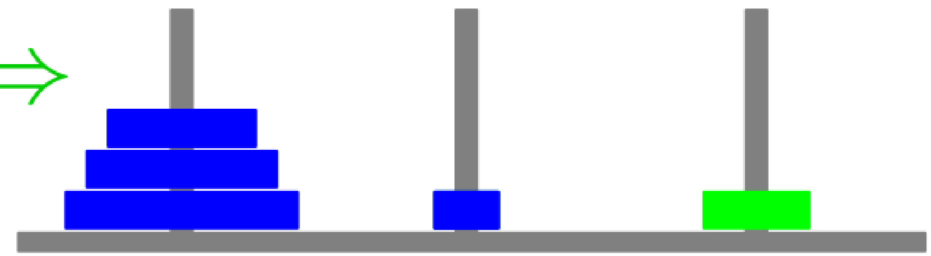
legal move

$\Rightarrow$



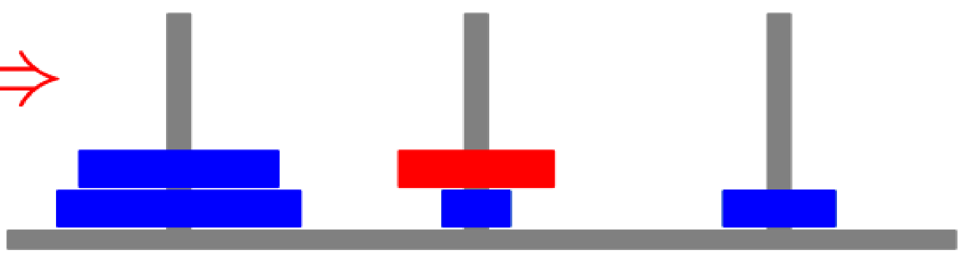
legal move

$\Rightarrow$



not legal

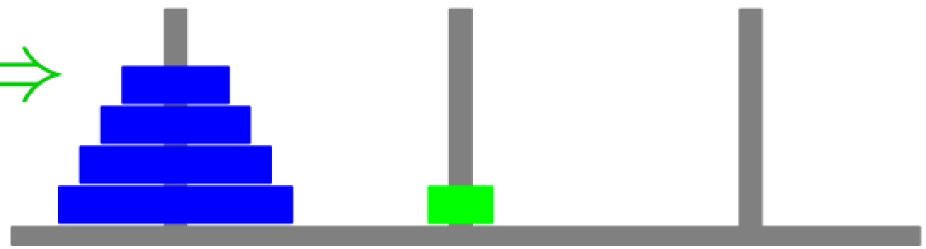
$\Rightarrow$



Towers of Hanoi

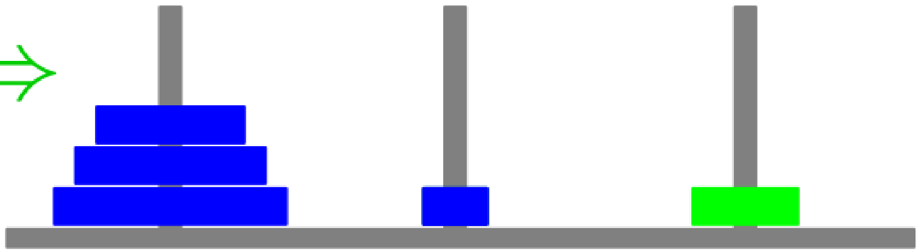
legal move

$\Rightarrow$



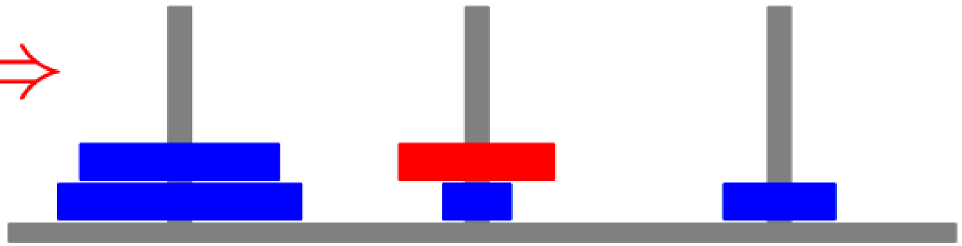
legal move

$\Rightarrow$



not legal

$\Rightarrow$



legal move

$\Rightarrow$

Towers of Hanoi

- **Problem:** Start with n disks on leftmost peg

Towers of Hanoi

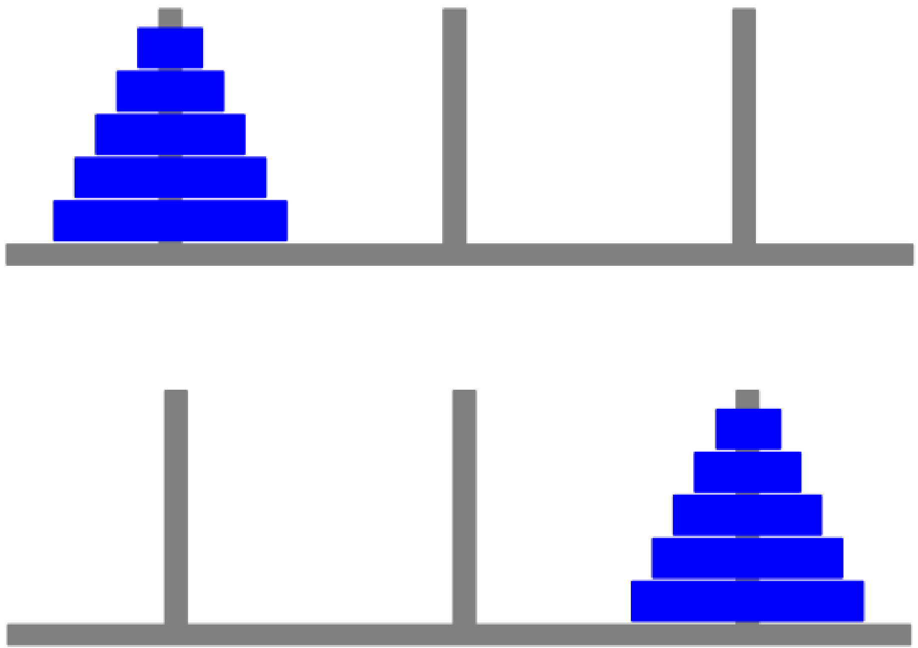
- **Problem:** Start with n disks on leftmost peg using only legal moves

Towers of Hanoi

- **Problem:** Start with n disks on leftmost peg

  using only legal moves

  move all disks to rightmost peg.

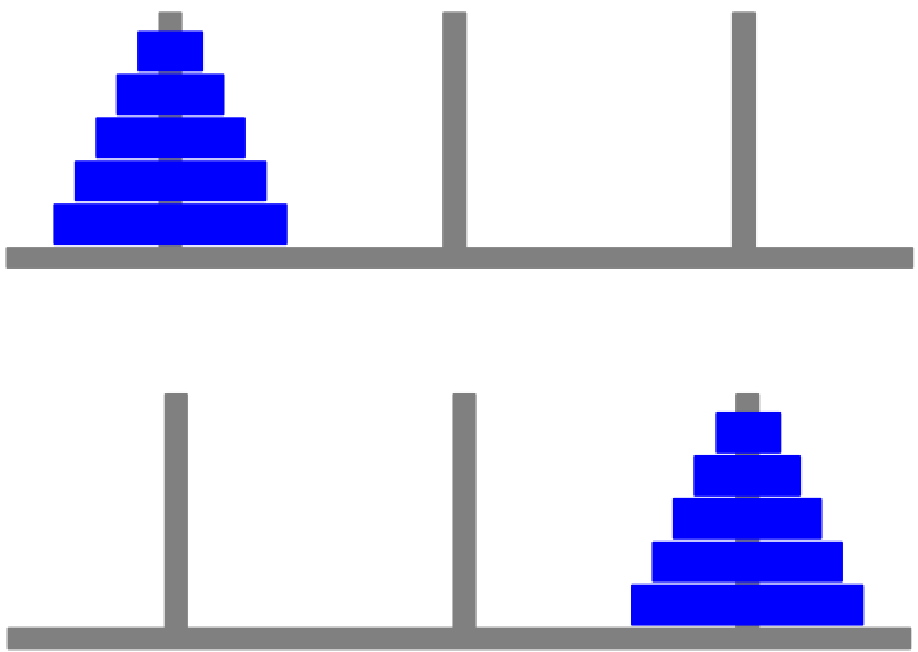


Towers of Hanoi

- **Problem:** Start with n disks on leftmost peg

  using only legal moves

  move all disks to rightmost peg.



Given $i, j \in \{1,2,3\}$, let $\overline{\{i,j\}} = \{1,2,3\} - \{i\} - \{j\}$,
i.e., $\overline{\{1,2\}} = \{3\}$, $\overline{\{1,3\}} = \{2\}$, $\overline{\{2,3\}} = \{1\}$.

Towers of Hanoi

- General solution

Towers of Hanoi

- General solution

  Recursion Base:

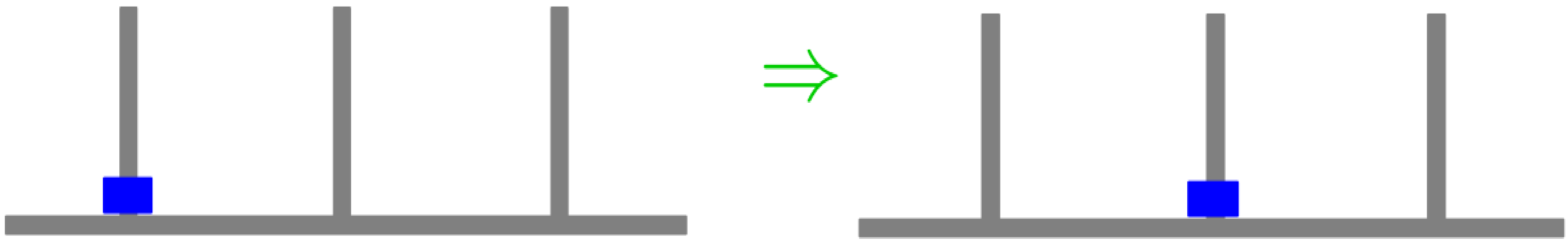
  If $n = 1$, moving one disk from i to j is easy. Just move it.

Towers of Hanoi

- General solution

  Recursion Base:

  If $n = 1$, moving one disk from i to j is easy. Just move it.



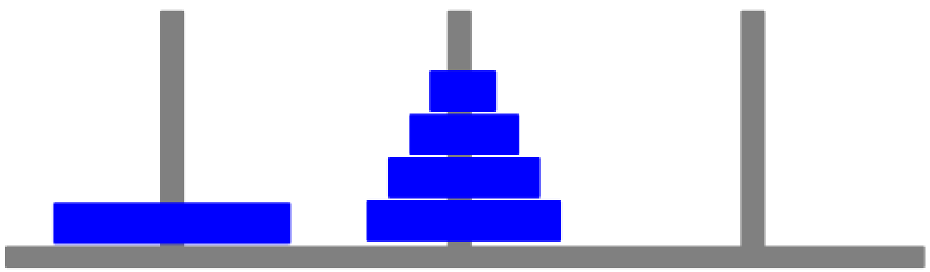
Towers of Hanoi

To move $n > 1$ disks from i to j

Towers of Hanoi

To move $n > 1$ disks from i to j

1)

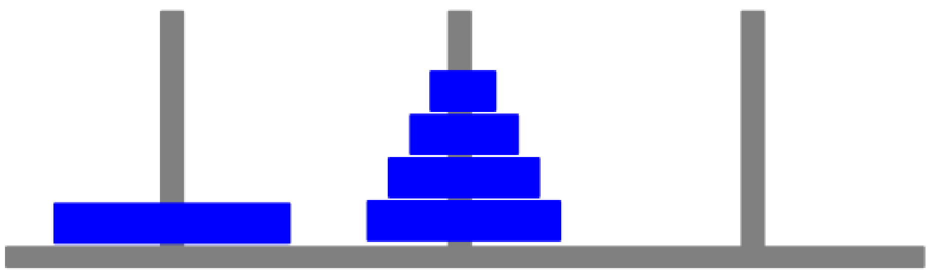


move top $n-1$ disks from i to $\overline{\{i,j\}}$

Towers of Hanoi

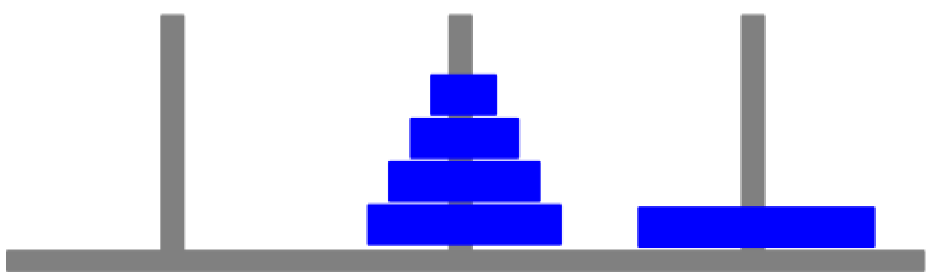
To move $n > 1$ disks from i to j

1)



move top $n-1$ disks from i to $\overline{\{i,j\}}$

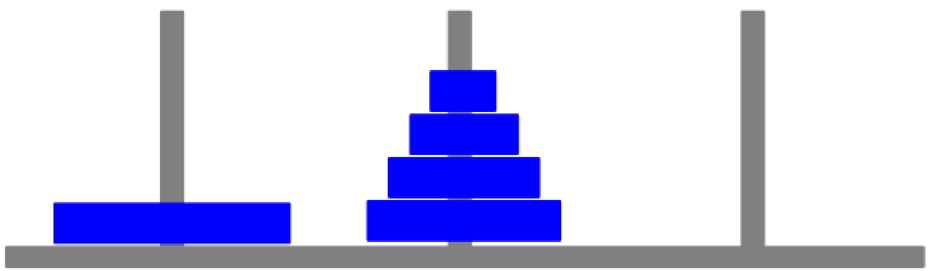
2)



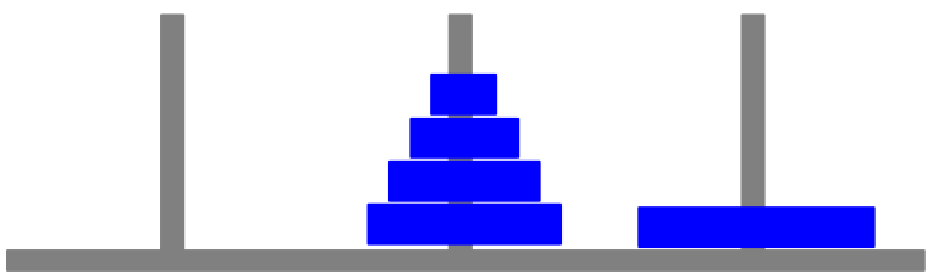
move largest disk from i to j

Towers of Hanoi

To move $n > 1$ disks from i to j

1) 

move top $n-1$ disks from i to $\overline{\{i,j\}}$

2) 

move largest disk from i to j

3) 

move top $n-1$ disks from $\overline{\{i,j\}}$ to j

Towers of Hanoi

```java
public class Hanoi
{

    public void move(int n, char a, char b, char c)
    {
        if (n == 1)
            System.out.println("plate " + n + " from " + a + " to " + c);
        else
        {
            move(n-1,a,c,b);
            System.out.println("plate " + n + " from " + a + " to " + c);
            move(n-1,b,a,c);
        }

    }

```

Towers of Hanoi

To move n disks from i to j

i) move top $n-1$ disks from i to $\overline{\{i,j\}}$

ii) move largest disk from i to j

iii) move top $n-1$ disks from $\overline{\{i,j\}}$ to j

Towers of Hanoi

- To prove Correctness of solution, we are implicitly using induction

To move n disks from i to j

i) move top $n-1$ disks from i to $\overline{\{i,j\}}$

ii) move largest disk from i to j

iii) move top $n-1$ disks from $\overline{\{i,j\}}$ to j

Towers of Hanoi

- To prove Correctness of solution, we are implicitly using induction

- $p(n)$ is statement that algorithm is correct for n

To move n disks from i to j

i) move top $n-1$ disks from i to $\overline{\{i,j\}}$

ii) move largest disk from i to j

iii) move top $n-1$ disks from $\overline{\{i,j\}}$ to j

Towers of Hanoi

- To prove Correctness of solution, we are implicitly using induction
- $p(n)$ is statement that algorithm is correct for n
- $p(1)$ is statement that algorithm works for $n = 1$ disks, which is obviously true

To move n disks from i to j

i) move top $n-1$ disks from i to $\overline{\{i,j\}}$

ii) move largest disk from i to j

iii) move top $n-1$ disks from $\overline{\{i,j\}}$ to j

Towers of Hanoi

- To prove Correctness of solution, we are implicitly using induction
- $p(n)$ is statement that algorithm is correct for n

To move n disks from i to j

i) move top $n-1$ disks from i to $\overline{\{i,j\}}$

ii) move largest disk from i to j

iii) move top $n-1$ disks from $\overline{\{i,j\}}$ to j

- $p(1)$ is statement that algorithm works for $n=1$ disks, which is obviously true
- $p(n-1) \rightarrow p(n)$ is *recursion* statement that

  if our algorithm works for $n-1$ disks, then we can build a correct solution for n disks

Towers of Hanoi

- Running time

  $M(n)$ is number of disk moves needed for n disks

To move n disks from i to j

i) move top $n-1$ disks from i to $\overline{\{i,j\}}$

ii) move largest disk from i to j

iii) move top $n-1$ disks from $\overline{\{i,j\}}$ to j

Towers of Hanoi

- Running time

  $M(n)$ is number of disk moves needed for n disks

To move n disks from i to j

i) move top $n-1$ disks from i to $\overline{\{i,j\}}$

ii) move largest disk from i to j

iii) move top $n-1$ disks from $\overline{\{i,j\}}$ to j

$M(1) = 1$

if $n > 1$, then $M(n) = 2M(n-1) + 1$

Towers of Hanoi

- We saw that $M(1) = 1$ and that
- $M(n) = 2M(n-1) + 1$ for $n > 1$

Towers of Hanoi

- We saw that $M(1) = 1$ and that
- $M(n) = 2M(n-1) + 1$ for $n > 1$

- Iterating the recurrence gives

$$M(1) = 1,\ M(2) = 3,\ M(3) = 7,$$
$$M(4) = 15,\ M(5) = 31,\ \ldots$$

Towers of Hanoi

- We saw that $M(1) = 1$ and that
- $M(n) = 2M(n-1) + 1$ for $n > 1$

- Iterating the recurrence gives

$$M(1) = 1,\ M(2) = 3,\ M(3) = 7,$$
$$M(4) = 15,\ M(5) = 31,\ \ldots$$

- We *guess* that $M(n) = 2^n - 1$

Towers of Hanoi

- We saw that $M(1) = 1$ and that
- $M(n) = 2M(n-1) + 1$ for $n > 1$

- Iterating the recurrence gives

$$M(1) = 1,\ M(2) = 3,\ M(3) = 7,$$
$$M(4) = 15,\ M(5) = 31,\ \ldots$$

- We *guess* that $M(n) = 2^n - 1$

  We'll prove this by induction

Towers of Hanoi

- We saw that $M(1) = 1$ and that
- $M(n) = 2M(n-1) + 1$ for $n > 1$

- Iterating the recurrence gives

  $$M(1) = 1,\ M(2) = 3,\ M(3) = 7,$$
  $$M(4) = 15,\ M(5) = 31,\ \ldots$$

- We *guess* that $M(n) = 2^n - 1$

  We'll prove this by induction

  Later, we'll also see how to solve without guessing

Towers of Hanoi

- Formally, given

$$M(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2M(n-1) + 1 & \text{otherwise} \end{cases}$$

We show that $M(n) = 2^n - 1$.

Towers of Hanoi

- Formally, given

$$M(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2M(n-1) + 1 & \text{otherwise} \end{cases}$$

We show that $M(n) = 2^n - 1$.

Proof. (by induction)

The base case $n = 1$ is true, since $2^1 - 1 = 1$.

For the inductive step, assume that $M(n-1) = 2^{n-1} - 1$ for $n > 1$.

- Formally, given

$$M(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2M(n-1)+1 & \text{otherwise} \end{cases}$$

We show that $M(n) = 2^n - 1$.

Proof. (by induction)

The base case $n = 1$ is true, since $2^1 - 1 = 1$.

For the inductive step, assume that $M(n-1) = 2^{n-1} - 1$ for $n > 1$.

Then $M(n) = 2M(n-1) + 1 = 2(2^{n-1} - 1) + 1 = 2^n - 1$

Towers of Hanoi

- Note that we used induction twice.

Towers of Hanoi

- Note that we used induction twice.

- The first time was to derive correctness of algorithm and the recurrence

$$M(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2M(n-1) + 1 & \text{otherwise} \end{cases}$$

Towers of Hanoi

- Note that we used induction twice.
- The first time was to derive correctness of algorithm and the recurrence

$$M(n) = \begin{cases} 1 & \text{if } n = 1 \\ 2M(n-1) + 1 & \text{otherwise} \end{cases}$$

- The second time was to derive the closed form solution $M(n) = 2^n - 1$ of the recurrence.

Next Lecture

- recurrence ...