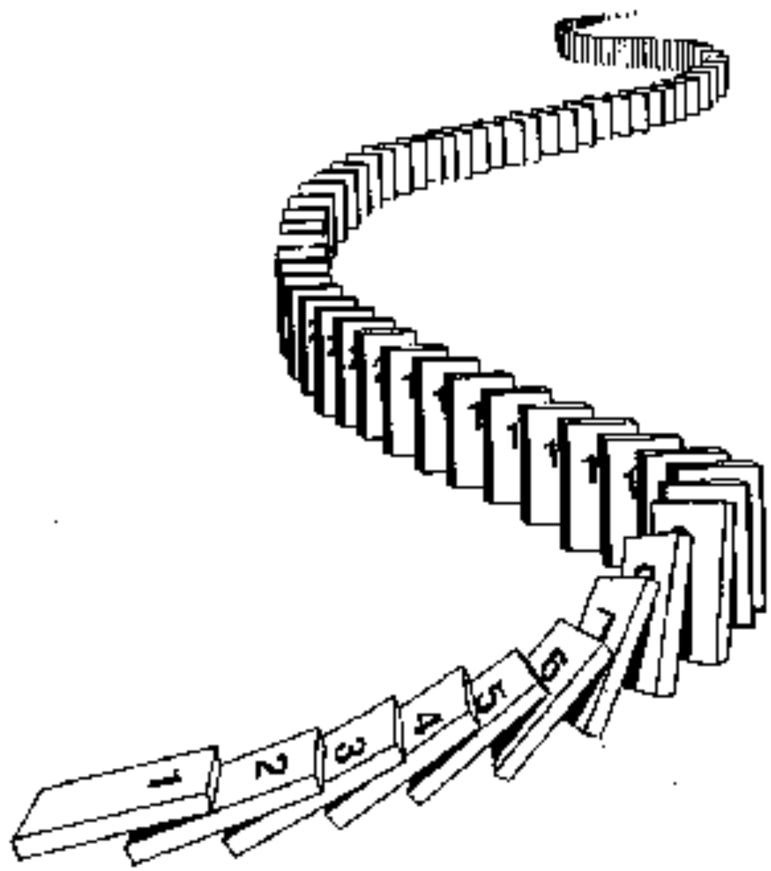
CSE 311: Foundations of Computing

Lecture 15: Induction



Modular Exponentiation mod 7

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

a	a^1	a^2	a^3	a^4	a^5	a^6
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	3	2	6	4	5	1
4	4	2	1	4	2	1
5	5	4	6	2	3	1
6	6	1	6	1	6	1

Exponentiation

- **Compute** 78365^{81453}
- **Compute** $78365^{81453} \bmod 104729$
- **Output is small**
  - need to keep intermediate results small

Repeated Squaring – small and fast

Since $b \bmod m \equiv_m b$ and $c \bmod m \equiv_m c$

we have $bc \bmod m = (b \bmod m)(c \bmod m) \bmod m$

So $\quad a^2 \bmod m = (a \bmod m)^2 \bmod m$

and $\quad a^4 \bmod m = (a^2 \bmod m)^2 \bmod m$

and $\quad a^8 \bmod m = (a^4 \bmod m)^2 \bmod m$

and $\quad a^{16} \bmod m = (a^8 \bmod m)^2 \bmod m$

and $\quad a^{32} \bmod m = (a^{16} \bmod m)^2 \bmod m$

Can compute $a^k \bmod m$ for $k = 2^i$ in only i steps

What if k is not a power of 2?

Fast Exponentiation Algorithm

81453 in binary is 10011111000101101

$81453 = 2^{16} + 2^{13} + 2^{12} + 2^{11} + 2^{10} + 2^{9} + 2^{5} + 2^{3} + 2^{2} + 2^{0}$

$a^{81453} = a^{2^{16}} \cdot a^{2^{13}} \cdot a^{2^{12}} \cdot a^{2^{11}} \cdot a^{2^{10}} \cdot a^{2^{9}} \cdot a^{2^{5}} \cdot a^{2^{3}} \cdot a^{2^{2}} \cdot a^{2^{0}}$

$a^{81453} \bmod m =$
$(\ldots(((((a^{2^{16}} \bmod m \cdot$
$a^{2^{13}} \bmod m) \bmod m \cdot$
$a^{2^{12}} \bmod m) \bmod m \cdot$
$a^{2^{11}} \bmod m) \bmod m \cdot$
$a^{2^{10}} \bmod m) \bmod m \cdot$
$a^{2^{9}} \bmod m) \bmod m \cdot$
$a^{2^{5}} \bmod m) \bmod m \cdot$
$a^{2^{3}} \bmod m) \bmod m \cdot$
$a^{2^{2}} \bmod m) \bmod m \cdot$
$a^{2^{0}} \bmod m) \bmod m$

Uses only 16 + 9 = 25 multiplications

The fast exponentiation algorithm computes $a^k \bmod m$ using $\leq 2\log k$ multiplications $\bmod m$

Fast Exponentiation: $a^k \bmod m$ for all k

Another way….

$$a^{2j} \bmod m = \left(a^j \bmod m\right)^2 \bmod m$$

$$a^{2j+1} \bmod m \ = \ \left((a \bmod m) \cdot (a^{2j} \bmod m)\right) \bmod m$$

Fast Exponentiation

```
public static int FastModExp(int a, int k, int modulus) {

        if (k == 0) {
            return 1;

        } else if ((k % 2) == 0) {
            long temp = FastModExp(a,k/2,modulus);
            return (temp * temp) % modulus;

        } else {
            long temp = FastModExp(a,k-1,modulus);
            return (a * temp) % modulus;
        }
}
```

$$a^{2j} \bmod m = \left(a^j \bmod m\right)^2 \bmod m$$

$$a^{2j+1} \bmod m \; = \; \big((a \bmod m) \cdot (a^{2j} \bmod m)\big) \bmod m$$

Using Fast Modular Exponentiation

- Your e-commerce web transactions use SSL (Secure Socket Layer) based on RSA encryption
- RSA
  - Vendor chooses random 512-bit or 1024-bit primes p, q and 512/1024-bit exponent e. Computes $m = p \cdot q$
  - Vendor broadcasts (m, e)
  - To send a to vendor, you compute $C = a^e \bmod m$ using *fast modular exponentiation* and send C to the vendor.
  - Using secret p, q the vendor computes d that is the *multiplicative inverse* of e mod $(p-1)(q-1)$.
  - Vendor computes $C^d \bmod m$ using *fast modular exponentiation*.
  - **Fact:** $a = C^d \bmod m$ for $0 < a < m$ unless $p|a$ or $q|a$

More Logic

Induction

Mathematical Induction

Method for proving statements about all natural numbers

- **A new logical inference rule!**
  - It only applies over the natural numbers
  - The idea is to **use** the special structure of the naturals to prove things more easily

- **Particularly useful for reasoning about programs!**

  ```
  for (int i=0; i < n; n++) { … }
  ```

  - Show P(i) holds after i times through the loop

Prove $\forall a, b, m > 0\ \forall\, k \in \mathbb{N}\ ((a \equiv_m b) \rightarrow (a^k \equiv_m b^k))$

Let $a, b, m > 0$ be arbitrary. Let $k \in \mathbb{N}$ be arbitrary.

Suppose that $a \equiv_m b$.

We know $((a \equiv_m b) \wedge (a \equiv_m b)) \rightarrow (a^2 \equiv_m b^2)$ by multiplying congruences. So, applying this repeatedly, we have:

$$((a \equiv_m b) \wedge (a \equiv_m b)) \rightarrow (a^2 \equiv_m b^2)$$
$$\big((a^2 \equiv_m b^2) \wedge (a \equiv_m b)\big) \rightarrow (a^3 \equiv_m b^3)$$

$$\dots$$

$$\big((a^{k-1} \equiv_m b^{k-1}) \wedge (a \equiv_m b)\big) \rightarrow (a^k \equiv_m b^k)$$

The "…"s is a problem! We don't have a proof rule that allows us to say "do this over and over".

But there such a property of the natural numbers!

Domain: Natural Numbers

$$P(0)$$

$$\forall k\ (P(k) \longrightarrow P(k+1))$$

$$\therefore \forall n\ \ P(n)$$

Induction Is A Rule of Inference

Domain: Natural Numbers

$$\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \\ \hline \therefore \forall n\ \ P(n) \end{array}$$

How do the givens prove P(3)?

Induction Is A Rule of Inference

Domain: Natural Numbers

$$\begin{array}{c} P(0) \\ \forall k \, (P(k) \longrightarrow P(k+1)) \\ \hline \therefore \forall n \;\; P(n) \end{array}$$

How do the givens prove P(5)?

$$P(0) \xrightarrow{P(0)\to P(1)} P(1) \xrightarrow{P(1)\to P(2)} P(2) \xrightarrow{P(2)\to P(3)} P(3) \xrightarrow{P(3)\to P(4)} P(4) \xrightarrow{P(4)\to P(5)} P(5)$$

First, we have P(0).

Since P(n) → P(n+1) for all n, we have P(0) → P(1).

  Since P(0) is true and P(0) → P(1), by Modus Ponens, P(1) is true.

Since P(n) → P(n+1) for all n, we have P(1) → P(2).

  Since P(1) is true and P(1) → P(2), by Modus Ponens, P(2) is true.

Using The Induction Rule In A Formal Proof

$$\frac{\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \end{array}}{\therefore \forall n\ \ P(n)}$$

Using The Induction Rule In A Formal Proof

$$\frac{\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \end{array}}{\therefore \forall n\ \ P(n)}$$

1. P(0)

4. $\forall$k (P(k) $\rightarrow$ P(k+1))
5. $\forall$n P(n) Induction: 1, 4

Using The Induction Rule In A Formal Proof

$$\frac{P(0) \qquad \forall k\ (P(k) \longrightarrow P(k+1))}{\therefore \forall n\ \ P(n)}$$

1. P(0)
2. Let k be an arbitrary integer ≥ 0

3. $P(k) \rightarrow P(k+1)$
4. $\forall k\ (P(k) \rightarrow P(k+1))$ — Intro $\forall$: 2, 3
5. $\forall n\ P(n)$ — Induction: 1, 4

Using The Induction Rule In A Formal Proof

$$\frac{\begin{array}{c} P(0) \\ \forall k\ (P(k) \longrightarrow P(k+1)) \end{array}}{\therefore \forall n\ \ P(n)}$$

1. P(0)
2. Let k be an arbitrary integer ≥ 0

3.1. P(k)	Assumption
3.2. ...	
3.3. P(k+1)	
3. $P(k) \rightarrow P(k+1)$	Direct Proof Rule
4. $\forall k\ (P(k) \rightarrow P(k+1))$	Intro $\forall$: 2, 3
5. $\forall n\ P(n)$	Induction: 1, 4

Translating to an English Proof

$$P(0)$$
$$\forall k\ (P(k) \longrightarrow P(k+1))$$
$$\therefore \forall n\ \ P(n)$$

1. Prove P(0)

Base Case

2. Let k be an arbitrary integer ≥ 0
    3.1. Suppose that P(k) is true

Inductive Hypothesis

    3.2. ...
    3.3. Prove P(k+1) is true

Inductive Step

3.	$P(k) \rightarrow P(k+1)$	Direct Proof Rule
4.	$\forall k\ (P(k) \rightarrow P(k+1))$	Intro $\forall$: 2, 3
5.	$\forall n\ P(n)$	Induction: 1, 4

Conclusion

Translating to an English Proof

Base Case
1. Prove P(0)

Inductive Hypothesis
2. Let k be an arbitrary integer ≥ 0
    3.1. Assume that P(k) is true

Inductive Step
    3.2. ...
    3.3. Prove P(k+1) is true

3.	$P(k) \rightarrow P(k+1)$	Direct Proof Rule
4.	$\forall k\, (P(k) \rightarrow P(k+1))$	Intro $\forall$: 2, 3
5.	$\forall n\, P(n)$	Induction: 1, 4

Conclusion

Induction English Proof Template

[...Define P(n)...]

We will show that $P(n)$ is true for every $n \in \mathbb{N}$ by Induction.

Base Case: *[...proof of $P(0)$ here...]*

Induction Hypothesis:

> **Suppose that $P(k)$ is true for an arbitrary $k \in \mathbb{N}$.**

Induction Step:

> *[...proof of $P(k+1)$ here...]*
>
> *The proof of $P(k+1)$ **must** invoke the IH somewhere.*

So, the claim is true by induction.

Inductive Proofs In 5 Easy Steps

Proof:

1. "Let $P(n)$ be... . We will show that $P(n)$ is true for every $n \geq 0$ by Induction."
2. "Base Case:" Prove $P(0)$
3. "Inductive Hypothesis:

   Suppose $P(k)$ is true for an arbitrary integer $k \geq 0$"
4. "Inductive Step:" Prove that $P(k+1)$ is true.

   Use the goal to figure out what you need.

   Make sure you are using I.H. and point out where you are using it. (Don't assume $P(k+1)$!!)
5. "Conclusion: Result follows by induction"

What is $1 + 2 + 4 + \ldots + 2^n$?

- $1 \quad = \quad 1$
- $1 + 2 \quad = \quad 3$
- $1 + 2 + 4 \quad = \quad 7$
- $1 + 2 + 4 + 8 \quad = \quad 15$
- $1 + 2 + 4 + 8 + 16 \quad = \quad 31$

It sure looks like this sum is $2^{n+1} - 1$

How can we prove it?

We could prove it for $n = 1, n = 2, n = 3, \ldots$ but that would literally take forever.

Good that we have induction!

Prove $1 + 2 + 4 + ... + 2^n = 2^{n+1} - 1$

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. Let $P(n)$ be "$2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$". We will show $P(n)$ is true for all natural numbers by induction.

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. **Let** P(n) **be** "$2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ **so** P(0) **is true.**

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. **Let** P(n) **be** “$2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$”. **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ **so** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$, **i.e., that** $\boxed{2^0 + 2^1 + \ldots + 2^k = 2^{k+1} - 1}$**.**

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. **Let** P(n) **be** "$2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ **so** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$**, i.e., that** $2^0 + 2^1 + \ldots + 2^k = 2^{k+1} - 1$**.**
4. **Induction Step:**

Goal: Show P(k+1)**, i.e. show** $2^0 + 2^1 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1$

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. **Let** $P(n)$ **be** "$2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$". **We will show** $P(n)$ **is true for all natural numbers by induction.**
2. **Base Case** $(n=0)$: $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ **so** $P(0)$ **is true.**
3. **Induction Hypothesis: Suppose that** $P(k)$ **is true for some arbitrary integer** $k \geq 0$**, i.e., that** $2^0 + 2^1 + \ldots + 2^k = 2^{k+1} - 1$**.**
4. **Induction Step:**

   $$2^0 + 2^1 + \ldots + 2^k = 2^{k+1} - 1 \quad \textbf{by IH}$$

   Adding 2^{k+1} **to both sides, we get:**

   $$2^0 + 2^1 + \ldots + 2^k + 2^{k+1} = 2^{k+1} + 2^{k+1} - 1$$

   Note that $2^{k+1} + 2^{k+1} = 2(2^{k+1}) = 2^{k+2}$**.**

   So, we have $2^0 + 2^1 + \ldots + 2^k + 2^{k+1} = 2^{k+2} - 1$**, which is exactly** $P(k+1)$**.**

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. **Let** $P(n)$ **be** "$2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$". **We will show** $P(n)$ **is true for all natural numbers by induction.**
2. **Base Case** $(n=0)$: $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ **so** $P(0)$ **is true.**
3. **Induction Hypothesis: Suppose that** $P(k)$ **is true for some arbitrary integer** $k \geq 0$**, i.e., that** $2^0 + 2^1 + \ldots + 2^k = 2^{k+1} - 1$**.**
4. **Induction Step:**

   We can calculate

$$
\begin{aligned}
2^0 + 2^1 + \ldots + 2^k + 2^{k+1} &= (2^0+2^1+ \ldots + 2^k) + 2^{k+1} \\
&= (2^{k+1} - 1) + 2^{k+1} && \textbf{by the IH} \\
&= 2(2^{k+1}) - 1 \\
&= 2^{k+2} - 1,
\end{aligned}
$$

   which is exactly $P(k+1)$**.**

Alternative way of writing the inductive step

Prove $1 + 2 + 4 + \ldots + 2^n = 2^{n+1} - 1$

1. **Let** P(n) **be** "$2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^0 = 1 = 2 - 1 = 2^{0+1} - 1$ **so** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$, **i.e., that** $2^0 + 2^1 + \ldots + 2^k = 2^{k+1} - 1$**.**
4. **Induction Step:**

   We can calculate

$$\begin{aligned} 2^0 + 2^1 + \ldots + 2^k + 2^{k+1} &= (2^0+2^1+ \ldots + 2^k) + 2^{k+1} \\ &= (2^{k+1} - 1) + 2^{k+1} \qquad \textbf{by the IH} \\ &= 2(2^{k+1}) - 1 \\ &= 2^{k+2} - 1, \end{aligned}$$

   which is exactly P(k+1).

5. **Thus** P(n) **is true for all** $n \in \mathbb{N}$, **by induction.**

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0. **I.e., suppose** 1 + 2 + …+ k = k(k+1)/2

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0**. I.e., suppose** 1 + 2 + …+ k = k(k+1)/2
4. **Induction Step:**

   Goal: Show P(k+1), **i.e. show** 1 + 2 + …+ k+ (k+1) = (k+1)(k+2)/2

Prove $1 + 2 + 3 + \ldots + n = n(n+1)/2$

1. **Let** P(n) **be** "0 + 1 + 2 + … + n = n(n+1)/2". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): 0 = 0(0+1)/2. **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0**. I.e., suppose** 1 + 2 + …+ k = k(k+1)/2
4. **Induction Step:**

$$
\begin{aligned}
1 + 2 + \ldots + k + (k+1) &= (1 + 2 + \ldots + k) + (k+1) \\
&= k(k+1)/2 + (k+1) \quad \textbf{by IH} \\
&= (k+1)(k/2 + 1) \\
&= (k+1)(k+2)/2
\end{aligned}
$$

   So, we have shown 1 + 2 + … + k + (k+1) = (k+1)(k+2)/2**,**

   which is exactly P(k+1)**.**

5. **Thus** P(n) **is true for all** n ∈ℕ**, by induction.**

Another example of a pattern

- $2^0 - 1 = 1 - 1 = 0 = 3 \cdot 0$
- $2^2 - 1 = 4 - 1 = 3 = 3 \cdot 1$
- $2^4 - 1 = 16 - 1 = 15 = 3 \cdot 5$
- $2^6 - 1 = 64 - 1 = 63 = 3 \cdot 21$
- $2^8 - 1 = 256 - 1 = 255 = 3 \cdot 85$
- $\dots$

Prove: $3 \mid (2^{2n}-1)$ **for all** $n \geq 0$

Prove: $3 \mid (2^{2n}-1)$ for all $n \geq 0$

1. **Let** P(n) **be** "3 | (2^{2n} – 1)". **We will show** P(n) i**s true for all natural numbers by induction.**

Prove: $3 \mid (2^{2n}-1)$ for all $n \geq 0$

1. **Let** P(n) **be** "3 | (2^{2n} – 1)". **We will show** P(n) i**s true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2\cdot 0}$-1=1-1=0=3·0 **Therefore** P(0) **is true**

Prove: $3 \mid (2^{2n}-1)$ for all $n \geq 0$

1. **Let** P(n) **be** "$3 \mid (2^{2n} - 1)$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2\cdot 0}-1=1-1=0=3\cdot 0$ **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$. $\boxed{\text{I.e., suppose that } 3 \mid (2^{2k} - 1)}$

Prove: $3 \mid (2^{2n} - 1)$ for all $n \geq 0$

1. **Let** P(n) **be** "$3 \mid (2^{2n} - 1)$". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2\cdot 0}-1=1-1=0=3\cdot 0$ **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** $k \geq 0$**. I.e., suppose that** $3 \mid (2^{2k} - 1)$
4. **Induction Step:**

Goal: Show P(k+1), **i.e. show** $3 \mid (2^{2(k+1)} - 1)$

Prove: $3 \mid (2^{2n}-1)$ for all $n \geq 0$

1. **Let** P(n) **be** "3 | (2^{2n} – 1)". **We will show** P(n) **is true for all natural numbers by induction.**
2. **Base Case** (n=0): $2^{2\cdot 0}-1=1-1=0=3\cdot 0$ **Therefore** P(0) **is true.**
3. **Induction Hypothesis: Suppose that** P(k) **is true for some arbitrary integer** k ≥ 0. **I.e., suppose that** 3 | (2^{2k} – 1)
4. **Induction Step:**

   By IH, $3 \mid (2^{2k} - 1)$ **so** $2^{2k} - 1 = 3j$ **for some integer** j

   So $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j+1) - 1$

   $= 12j+3 = 3(4j+1)$

   Therefore $3 \mid (2^{2(k+1)} - 1)$ **which is exactly** P(k+1).
5. **Thus** P(n) **is true for all** $n \in \mathbb{N}$, **by induction.**