CSE 311 Lecture 15: Modular Exponentiation and Induction

Emina Torlak and Sami Davies
Topics

Modular equations
   A quick review of Lecture 14.

Modular exponentiation
   A fast algorithm for computing $a^k \mod m$.

Mathematical induction
   A method for proving statements about all natural numbers.

Using induction
   Using induction in formal and English proofs.

Example proofs by induction
   Example proofs about sums and divisibility.
Modular equations

A quick review of Lecture 14.
Bézout’s theorem and multiplicative inverses

Bézout’s theorem

If $a$ and $b$ are positive integers, then there exist integers $s$ and $t$ such that $\text{GCD}(a, b) = sa + tb$.

We can compute $s$ and $t$ using the extended Euclidean algorithm.

If $\text{GCD}(a, m) = 1$, then $s \mod m$ is the multiplicative inverse of $a$ modulo $m$:

- $sa + tm = 1$ so $sa \equiv 1 \pmod{m}$, and we have
- $(s \mod m)a \equiv 1 \pmod{m}$.

These inverses let us solve modular equations.
Using multiplicative inverses to solve modular equations

Solve: $7x \equiv 1 \pmod{26}$

① Compute GCD and keep the tableau.

\[
\begin{align*}
\text{GCD}(26, 7) &= \text{GCD}(7, 5) = \text{GCD}(5, 2) \\
&= \text{GCD}(2, 1) = \text{GCD}(1, 0) \\
&= 1
\end{align*}
\]

② Solve the equations for $r$ in the tableau.

\[
\begin{align*}
a &= q \times b + r \\
26 &= 3 \times 7 + 5 \\
7 &= 1 \times 5 + 2 \\
5 &= 2 \times 2 + 1
\end{align*}
\]

③ Back substitute the equations for $r$.

\[
\begin{align*}
1 &= 5 - 2 \times (7 - 1 \times 5) \\
&= (-2) \times 7 + 3 \times 5 \\
&= (-2) \times 7 + 3 \times (26 - 3 \times 7) \\
&= 3 \times 26 + (-11) \times 7
\end{align*}
\]

④ Solve for $x$.

- Multiplicative inverse of 7 mod 26
  - $(-11) \mod 26 = 15$
- So, $x = 26k + 15$ for $k \in \mathbb{Z}$. 
Modular exponentiation

A fast algorithm for computing $a^k \mod m$. 
The modular exponentiation problem: $a^k \mod m$

How would you compute $78365^{81453} \mod 104729$?
The modular exponentiation problem: \( a^k \mod m \)

How would you compute \( 78365^{81453} \mod 104729 \)?

**Naive approach**

First compute \( 78365^{81453} \).
Then take the result modulo 104729.
The modular exponentiation problem: $a^k \mod m$

How would you compute $78365^{81453} \mod 104729$?

**Naive approach**

First compute $78365^{81453}$.
Then take the result modulo 104729.

**This works but is very inefficient …**

The intermediate result $78365^{81453}$ is a 1,324,257-bit number!
But we only need the remainder mod 104,729, which is 17 bits.
The modular exponentiation problem: \( a^k \mod m \)

How would you compute \( 78365^{81453} \mod 104729 \)?

Naive approach

First compute \( 78365^{81453} \).
Then take the result modulo 104729.

This works but is very inefficient …

The intermediate result \( 78365^{81453} \) is a 1,324,257-bit number!
But we only need the remainder mod 104,729, which is 17 bits.

To keep the intermediate results small, we use fast modular exponentiation.
Repeated squaring: $a^k \mod m$ for $k = 2^i$

If $k = 2^i$, we can compute $a^k \mod m$ in just $i$ steps.

Note that $a \mod m \equiv a \pmod{m}$ and $b \mod m \equiv b \pmod{m}$. So, we have $ab \mod m = ((a \mod m)(b \mod m)) \mod m$. 
Repeated squaring: $a^k \mod m$ for $k = 2^i$

If $k = 2^i$, we can compute $a^k \mod m$ in just $i$ steps.

Note that $a \mod m \equiv a \pmod{m}$ and $b \mod m \equiv b \pmod{m}$. So, we have $ab \mod m = ((a \mod m)(b \mod m)) \mod m$.

For example:

- $a^2 \mod m = (a \mod m)^2 \mod m$
- $a^4 \mod m = (a^2 \mod m)^2 \mod m$
- $a^8 \mod m = (a^4 \mod m)^2 \mod m$
- $a^{16} \mod m = (a^8 \mod m)^2 \mod m$
- $a^{32} \mod m = (a^{16} \mod m)^2 \mod m$
Repeated squaring: $a^k \mod m$ for $k = 2^i$

If $k = 2^i$, we can compute $a^k \mod m$ in just $i$ steps.

Note that $a \mod m \equiv a \pmod{m}$ and $b \mod m \equiv b \pmod{m}$. So, we have $ab \mod m = ((a \mod m)(b \mod m)) \mod m$.

For example:

\[
\begin{align*}
a^2 \mod m &= (a \mod m)^2 \mod m \\
a^4 \mod m &= (a^2 \mod m)^2 \mod m \\
a^8 \mod m &= (a^4 \mod m)^2 \mod m \\
a^{16} \mod m &= (a^8 \mod m)^2 \mod m \\
a^{32} \mod m &= (a^{16} \mod m)^2 \mod m
\end{align*}
\]

What if $k$ is not a power of 2? How do we solve $78365^{81453} \mod 104729$?
Fast exponentiation: $a^k \mod m$ for all $k$

Note that 81453 is 10011111000101101 in binary.

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

$$a^{81453} = a^{2^{16}} \cdot a^{2^{13}} \cdot a^{2^{12}} \cdot a^{2^{11}} \cdot a^{2^{10}} \cdot a^9 \cdot a^5 \cdot a^3 \cdot a^2 \cdot a^0$$
Fast exponentiation: $a^k \mod m$ for all $k$

Note that 81453 is 10011111000101101 in binary.

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

\[
a^{81453} = a^{2^{16}} \times a^{2^{13}} \times a^{2^{12}} \times a^{2^{11}} \times a^{2^{10}} \times a^{2^9} \times a^{2^5} \times a^{2^3} \times a^{2^2} \times a^{2^0}
\]

\[
a^{81453} \mod m = ((((((a^{2^{16}} \mod m) \mod m \times a^{2^{13}} \mod m) \mod m \times a^{2^{12}} \mod m) \mod m \times a^{2^{11}} \mod m) \mod m \times a^{2^{10}} \mod m) \mod m \times a^{2^9} \mod m) \mod m \times a^{2^5} \mod m) \mod m \times a^{2^3} \mod m) \mod m \times a^{2^2} \mod m) \mod m)
\]
Fast exponentiation: $a^k \mod m$ for all $k$

Note that 81453 is 10011111000101101 in binary.

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

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

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

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

\[
\begin{align*}
a^{2j} \mod m &= (a^j \mod m)^2 \mod m \\
a^{2j+1} \mod m &= ((a \mod m) \times (a^{2j} \mod m)) \mod m
\end{align*}
\]
The fast exponentiation algorithm

\[ a^{2j} \mod m = (a^j \mod m)^2 \mod m \]
\[ a^{2j+1} \mod m = ((a \mod m) * (a^{2j} \mod m)) \mod m \]

Example implementation:

```java
// Assumes a > 0, k >= 0, m > 1.
public static long fastModExp(long a, long k, long m) {
    if (k == 0) { // k = 0
        return 1;
    } else if (k % 2 == 0) { // k is even
        long tmp = fastModExp(a, k/2, m);
        return (tmp * tmp) % m;
    } else { // k is odd
        long tmp = fastModExp(a, k-1, m);
        return ((a % m) * tmp) % m;
    }
}
```
The fast exponentiation algorithm

\[
a^{2j} \mod m = (a^j \mod m)^2 \mod m
\]

\[
a^{2j+1} \mod m = ((a \mod m) \times (a^{2j} \mod m)) \mod m
\]

Example implementation:

```java
// Assumes \(a > 0\), \(k \geq 0\), \(m > 1\).
public static long fastModExp(long a, long k, long m) {
    if (k == 0) { // k = 0
        return 1;
    } else if (k % 2 == 0) { // k is even
        long tmp = fastModExp(a, k/2, m);
        return (tmp * tmp) % m;
    } else { // k is odd
        long tmp = fastModExp(a, k-1, m);
        return ((a % m) * tmp) % m;
    }
}
```

\(78365^{81453} \mod 104729 = 45235\)
Using fast modular exponentiation: RSA encryption

Alice chooses random 512-bit (or 1024-bit) primes $p$, $q$ and exponent $e$.  
Alice computes $m = pq$ and broadcasts $(m, e)$, which is her public key. 
She also computes the multiplicative inverse $d$ of $e \mod (p - 1)(q - 1)$, which serves as her private key.

To encrypt a message $a$ with Alice’s public key, Bob computes $C = a^e \mod m$. 
This computation uses fast modular exponentiation. 
Bob sends the ciphertext $C$ to Alice.

To decrypt $C$, Alice computes $C^d \mod m$. 
This computation also uses fast modular exponentiation. 
It works because $C^d \mod m = a$ for $0 < a < m$ unless $p | a$ or $q | a$. 

Mathematical induction

A method for proving statements about all natural numbers.
How would you prove this theorem?

Mods and exponents

For all integers $a, b, m > 0$ and $k \geq 0$, $a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}$. 
How would you prove this theorem?

Mods and exponents
For all integers \( a, b, m > 0 \) and \( k \geq 0 \), \( a \equiv b \pmod{m} \) \( \rightarrow \) \( a^k \equiv b^k \pmod{m} \).

Proof
Let \( a, b, m > 0 \in \mathbb{Z} \) and \( k \geq 0 \in \mathbb{Z} \) be arbitrary. Suppose that \( a \equiv b \pmod{m} \).
How would you prove this theorem?

**Proof**

Let \(a, b, m > 0\) and \(k \geq 0\) be arbitrary. Suppose that \(a \equiv b \pmod{m}\). By the multiplication property, we know that if \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m}\), then \(ac \equiv bd \pmod{m}\). So, taking \(c\) to be \(a\) and \(d\) to be \(b\), we have \(a^2 \equiv b^2 \pmod{m}\).
How would you prove this theorem?

**Mods and exponents**

For all integers $a, b, m > 0$ and $k \geq 0$, $a \equiv b \pmod{m} \implies a^k \equiv b^k \pmod{m}$.

**Proof**

Let $a, b, m > 0 \in \mathbb{Z}$ and $k \geq 0 \in \mathbb{Z}$ be arbitrary. Suppose that $a \equiv b \pmod{m}$.

By the multiplication property, we know that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. So, taking $c$ to be $a$ and $d$ to be $b$, we have $a^2 \equiv b^2 \pmod{m}$.

Applying this reasoning repeatedly, we have

\[
(a \equiv b \pmod{m} \land a \equiv b \pmod{m}) \implies (a^2 \equiv b^2 \pmod{m})
\]

\[
(a^2 \equiv b^2 \pmod{m} \land a \equiv b \pmod{m}) \implies (a^3 \equiv b^3 \pmod{m})
\]

\[
\vdots
\]

\[
(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \land a \equiv b \pmod{m}) \implies (a^k \equiv b^k \pmod{m}).
\]
How would you prove this theorem?

**Mods and exponents**

For all integers \(a, b, m > 0\) and \(k \geq 0\), \(a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}\).

**Proof (almost):**

Let \(a, b, m > 0 \in \mathbb{Z}\) and \(k \geq 0 \in \mathbb{Z}\) be arbitrary. Suppose that \(a \equiv b \pmod{m}\). By the multiplication property, we know that if \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m}\), then \(ac \equiv bd \pmod{m}\). So, taking \(c\) to be \(a\) and \(d\) to be \(b\), we have \(a^2 \equiv b^2 \pmod{m}\).

Applying this reasoning repeatedly, we have

\[
\begin{align*}
(a \equiv b \pmod{m} \land a \equiv b \pmod{m}) & \rightarrow (a^2 \equiv b^2 \pmod{m}) \\
(a^2 \equiv b^2 \pmod{m} \land a \equiv b \pmod{m}) & \rightarrow (a^3 \equiv b^3 \pmod{m}) \\
& \ldots \\
(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \land a \equiv b \pmod{m}) & \rightarrow (a^k \equiv b^k \pmod{m}).
\end{align*}
\]

This, uhm, completes the proof? \(\blacksquare\)
How would you prove this theorem?

### Mods and exponents

For all integers $a, b, m > 0$ and $k \geq 0$, $a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}$.

**Proof (almost):**

Let $a, b, m > 0 \in \mathbb{Z}$ and $k \geq 0 \in \mathbb{Z}$ be arbitrary. Suppose that $a \equiv b \pmod{m}$.

By the multiplication property, we know that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. So, taking $c$ to be $a$ and $d$ to be $b$, we have $a^2 \equiv b^2 \pmod{m}$.

Applying this reasoning repeatedly, we have

$$(a \equiv b \pmod{m} \land a \equiv b \pmod{m}) \rightarrow (a^2 \equiv b^2 \pmod{m})$$

$$(a^2 \equiv b^2 \pmod{m} \land a \equiv b \pmod{m}) \rightarrow (a^3 \equiv b^3 \pmod{m})$$

$$
\vdots
$$

$$(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \land a \equiv b \pmod{m}) \rightarrow (a^k \equiv b^k \pmod{m}).$$

This, uhm, completes the proof? □

We don’t have a proof rule to say “perform this step repeatedly.”
Perform a step repeatedly with induction!

\[
\begin{align*}
\text{Induction} & \quad P(0); \forall k. P(k) \rightarrow P(k + 1) \\
\therefore & \quad \forall n. P(n)
\end{align*}
\]

Domain: natural numbers (\(\mathbb{N}\)).
Perform a step repeatedly with induction!

**Induction**

\[
P(0); \forall k. P(k) \rightarrow P(k + 1) \quad \therefore \forall n. P(n)
\]

Domain: natural numbers (\(\mathbb{N}\)).

Induction is a logical rule of inference that applies (only) over \(\mathbb{N}\).

If we know that a property \(P\) holds for 0, and we know that \(\forall k. P(k) \rightarrow P(k + 1)\), then we can conclude that \(P\) holds for all natural numbers.
Perform a step repeatedly with induction!

Induction

\[ P(0); \forall k. P(k) \rightarrow P(k + 1) \]
\[ \therefore \forall n. P(n) \]

Domain: natural numbers \((\mathbb{N})\).

Induction is a logical rule of inference that applies (only) over \(\mathbb{N}\).

If we know that a property \(P\) holds for 0, and we know that \(\forall k. P(k) \rightarrow P(k + 1)\), then we can conclude that \(P\) holds for all natural numbers.

```java
// f(x) = x for all x >= 0.
public int f(int x) {
    if (x == 0) { return 0; }
    else { return f(x - 1) + 1; }
}
```

Induction is essential for reasoning about programs with loops and recursion.
Induction: how does it work?

**Induction**

\[
P(0); \forall k. P(k) \rightarrow P(k + 1)
\]

\[
\therefore \forall n. P(n)
\]

Domain: natural numbers (\(\mathbb{N}\)).

Suppose that we are given \(P(0)\) and \(\forall k. P(k) \rightarrow P(k + 1)\).

How does that give us \(P(k)\) for a concrete \(k\) such as 5?
Induction: how does it work?

\[ \frac{P(0); \forall k. P(k) \rightarrow P(k + 1)}{\therefore \forall n. P(n)} \]

Domain: natural numbers (\( \mathbb{N} \)).

Suppose that we are given \( P(0) \) and \( \forall k. P(k) \rightarrow P(k + 1) \).

How does that give us \( P(k) \) for a concrete \( k \) such as 5?

1. First, we have \( P(0) \).
Induction: how does it work?

\[
\begin{align*}
\text{Induction} \quad & P(0); \forall k. P(k) \rightarrow P(k + 1) \\
\therefore & \forall n. P(n)
\end{align*}
\]

Domain: natural numbers (\(\mathbb{N}\)).

Suppose that we are given \(P(0)\) and \(\forall k. P(k) \rightarrow P(k + 1)\).

How does that give us \(P(k)\) for a concrete \(k\) such as 5?

1. First, we have \(P(0)\).
2. Since \(P(k) \rightarrow P(k + 1)\) for all \(k\), we have \(P(0) \rightarrow P(1)\).
Induction: how does it work?

\[ P(0); \forall k. P(k) \rightarrow P(k + 1) \]
\[ \therefore \forall n. P(n) \]

Domain: natural numbers (\( \mathbb{N} \)).

Suppose that we are given \( P(0) \) and \( \forall k. P(k) \rightarrow P(k + 1) \).

How does that give us \( P(k) \) for a concrete \( k \) such as 5?

1. First, we have \( P(0) \).
2. Since \( P(k) \rightarrow P(k + 1) \) for all \( k \), we have \( P(0) \rightarrow P(1) \).
3. Applying Modus Ponens to 1 and 2, we get \( P(1) \).
Induction: how does it work?

\[
P(0); \forall k. P(k) \rightarrow P(k + 1) \quad \therefore \forall n. P(n)
\]

Domain: natural numbers (\(\mathbb{N}\)).

Suppose that we are given \(P(0)\) and \(\forall k. P(k) \rightarrow P(k + 1)\).

How does that give us \(P(k)\) for a concrete \(k\) such as 5?

1. First, we have \(P(0)\).
2. Since \(P(k) \rightarrow P(k + 1)\) for all \(k\), we have \(P(0) \rightarrow P(1)\).
3. Applying Modus Ponens to 1 and 2, we get \(P(1)\).
4. Since \(P(k) \rightarrow P(k + 1)\) for all \(k\), we have \(P(1) \rightarrow P(2)\).
Induction: how does it work?

Suppose that we are given $P(0)$ and $\forall k. P(k) \rightarrow P(k + 1)$.

How does that give us $P(k)$ for a concrete $k$ such as 5?

1. First, we have $P(0)$.
2. Since $P(k) \rightarrow P(k + 1)$ for all $k$, we have $P(0) \rightarrow P(1)$.
3. Applying Modus Ponens to 1 and 2, we get $P(1)$.
4. Since $P(k) \rightarrow P(k + 1)$ for all $k$, we have $P(1) \rightarrow P(2)$.
5. Applying Modus Ponens to 3 and 4, we get $P(2)$.
Induction: how does it work?

\[ P(0); \forall k. P(k) \rightarrow P(k + 1) \]
\[ \therefore \forall n. P(n) \]

Domain: natural numbers (\(\mathbb{N}\)).

Suppose that we are given \(P(0)\) and \(\forall k. P(k) \rightarrow P(k + 1)\).

How does that give us \(P(k)\) for a concrete \(k\) such as 5?

1. First, we have \(P(0)\).
2. Since \(P(k) \rightarrow P(k + 1)\) for all \(k\), we have \(P(0) \rightarrow P(1)\).
3. Applying Modus Ponens to 1 and 2, we get \(P(1)\).
4. Since \(P(k) \rightarrow P(k + 1)\) for all \(k\), we have \(P(1) \rightarrow P(2)\).
5. Applying Modus Ponens to 3 and 4, we get \(P(2)\).
  \[ \vdots \]
11. Applying Modus Ponens to 9 and 10, we get \(P(5)\).
Using induction

Using induction in formal and English proofs.
Using the induction rule in a formal proof

\[
\begin{align*}
\text{Induction} & \quad P(0); \forall k. P(k) \rightarrow P(k + 1) \\
& \quad \therefore \forall n. P(n)
\end{align*}
\]

1. Prove \( P(0) \)

5. \( \forall k. P(k) \to P(k + 1) \)
6. \( \forall n. P(n) \) \quad \text{Induction: 1, 5}
Using the induction rule in a formal proof

\[
\begin{align*}
\text{Induction} & \quad P(0); \forall k. P(k) \rightarrow P(k + 1) \\
& \quad \therefore \forall n. P(n)
\end{align*}
\]

1. Prove \( P(0) \)
2. Let \( k \geq 0 \) be an arbitrary integer

4. \( P(k) \rightarrow P(k + 1) \)
5. \( \forall k. P(k) \rightarrow P(k + 1) \)  Intro \( \forall \): 2, 4
6. \( \forall n. P(n) \)  Induction: 1, 5
Using the induction rule in a formal proof

\[ P(0); \forall k. P(k) \rightarrow P(k + 1) \]

∴ \( \forall n. P(n) \)

1. Prove \( P(0) \)
2. Let \( k \geq 0 \) be an arbitrary integer
   - 3.1. Assume that \( P(k) \) is true
   - 3.2. …
   - 3.3. Prove \( P(k + 1) \) is true

4. \( P(k) \rightarrow P(k + 1) \) \hspace{1cm} Direct Proof Rule
5. \( \forall k. P(k) \rightarrow P(k + 1) \) \hspace{1cm} Intro \( \forall \): 2, 4
6. \( \forall n. P(n) \) \hspace{1cm} Induction: 1, 5
Using the induction rule in a formal proof: key parts

Induction

\[ P(0); \forall k. P(k) \rightarrow P(k + 1) \]

\[ \therefore \forall n. P(n) \]

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Prove ( P(0) )</td>
<td>Base case</td>
</tr>
<tr>
<td>2.</td>
<td>Let ( k \geq 0 ) be an arbitrary integer</td>
<td>Inductive hypothesis</td>
</tr>
<tr>
<td>3.1.</td>
<td>Assume that ( P(k) ) is true</td>
<td></td>
</tr>
<tr>
<td>3.2.</td>
<td>…</td>
<td>Inductive step</td>
</tr>
<tr>
<td>3.3.</td>
<td>Prove ( P(k + 1) ) is true</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>( P(k) \rightarrow P(k + 1) )</td>
<td>Direct Proof Rule</td>
</tr>
<tr>
<td>5.</td>
<td>( \forall k. P(k) \rightarrow P(k + 1) )</td>
<td>Intro ( \forall ): 2, 4</td>
</tr>
<tr>
<td>6.</td>
<td>( \forall n. P(n) )</td>
<td>Induction: 1, 5</td>
</tr>
</tbody>
</table>
Translating to an English proof: the template

1. Let $P(n)$ be [definition of $P(n)$].
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   [Proof of $P(0)$.

3. Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

4. Inductive step:
   We want to prove that $P(k + 1)$ is true.
   [Proof of $P(k + 1)$. This proof must invoke the inductive hypothesis somewhere.]

5. The result follows for all $n \geq 0$ by induction.
Translating to an English proof: the template

① Let $P(n)$ be [definition of $P(n)$].
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):
   [Proof of $P(0)$.]

③ Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ Inductive step:
   We want to prove that $P(k + 1)$ is true.
   [Proof of $P(k + 1)$. This proof must invoke the inductive hypothesis somewhere.]

⑤ The result follows for all $n \geq 0$ by induction.

Induction dos and don’ts:
- Do write out all 5 steps.
- Do point out where you are using the inductive hypothesis in step ④.
- Don’t assume $P(k + 1)$!
Example proofs by induction

Example proofs about sums and divisibility.
What is $\sum_{i=0}^{n} 2^i$ for an arbitrary $n \in \mathbb{N}$?

Recall that $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n$. 
What is $\sum_{i=0}^{n} 2^i$ for an arbitrary $n \in \mathbb{N}$?

Recall that $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n$.

Let’s look at a few examples:

$\sum_{i=0}^{0} 2^i = 1$

$\sum_{i=0}^{1} 2^i = 1 + 2 = 3$

$\sum_{i=0}^{2} 2^i = 1 + 2 + 4 = 7$

$\sum_{i=0}^{3} 2^i = 1 + 2 + 4 + 8 = 15$

$\sum_{i=0}^{4} 2^i = 1 + 2 + 4 + 8 + 16 = 31$
What is $\sum_{i=0}^{n} 2^i$ for an arbitrary $n \in \mathbb{N}$?

Recall that $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n$.

Let’s look at a few examples:

- $\sum_{i=0}^{0} 2^i = 1$
- $\sum_{i=0}^{1} 2^i = 1 + 2 = 3$
- $\sum_{i=0}^{2} 2^i = 1 + 2 + 4 = 7$
- $\sum_{i=0}^{3} 2^i = 1 + 2 + 4 + 8 = 15$
- $\sum_{i=0}^{4} 2^i = 1 + 2 + 4 + 8 + 16 = 31$

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

Let’s use induction to prove it!
Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$
Prove \( \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \) for all \( n \in \mathbb{N} \)

1. Let \( P(n) \) be \( \sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1 \).
   We will show that \( P(n) \) is true for every integer \( n \geq 0 \) by induction.
Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

1. Let $P(n)$ be $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$. We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   $\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$ so $P(0)$ is true.
Prove \( \sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \) for all \( n \in \mathbb{N} \)

① Let \( P(n) \) be \( \sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1 \).

We will show that \( P(n) \) is true for every integer \( n \geq 0 \) by induction.

② Base case \((n = 0)\):
\[
\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1 \text{ so } P(0) \text{ is true.}
\]

③ Inductive hypothesis:
Suppose that \( P(k) \) is true for an arbitrary integer \( k \geq 0 \).
Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

1. Let $P(n)$ be $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   $\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$ so $P(0)$ is true.

3. Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

4. Inductive step: Assume $P(k)$ to prove $P(k + 1)$, not vice versa!
   We want to prove that $P(k + 1)$ is true, i.e., $\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$. Note that $\sum_{i=0}^{k+1} 2^i = (\sum_{i=0}^{k} 2^i) + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1}$ by the inductive hypothesis. From this, we have that $(2^{k+1} - 1) + 2^{k+1} = 2 \cdot 2^{k+1} - 1 = 2^{k+1+1} - 1 = 2^{k+2} - 1$, which is exactly $P(k + 1)$.
Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for all $n \in \mathbb{N}$

1. Let $P(n)$ be $\sum_{i=0}^{n} 2^i = 2^0 + 2^1 + \ldots + 2^n = 2^{n+1} - 1$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   $\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$ so $P(0)$ is true.

3. Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

4. Inductive step: Assume $P(k)$ to prove $P(k + 1)$, not vice versa!
   We want to prove that $P(k + 1)$ is true, i.e., $\sum_{i=0}^{k+1} 2^i = 2^{k+2} - 1$. Note that
   $\sum_{i=0}^{k+1} 2^i = (\sum_{i=0}^{k} 2^i) + 2^{k+1} = (2^{k+1} - 1) + 2^{k+1}$ by the inductive hypothesis. From this, we have that
   $(2^{k+1} - 1) + 2^{k+1} = 2 \cdot 2^{k+1} - 1 = 2^{k+1+1} - 1 = 2^{k+2} - 1$, which is exactly $P(k + 1)$.

5. The result follows for all $n \geq 0$ by induction.
Prove\( \sum_{i=0}^{n} i = n(n + 1)/2 \) for all \( n \in \mathbb{N} \)
Prove $\sum_{i=0}^{n} i = n(n + 1)/2$ for all $n \in \mathbb{N}$

1 Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n + 1)/2$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.
Prove $\sum_{i=0}^{n} i = n(n + 1)/2$ for all $n \in \mathbb{N}$

1. Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n + 1)/2$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   $\sum_{i=0}^{n} i = 0 = 0(0 + 1)/2$ so $P(0)$ is true.
Prove $\sum_{i=0}^{n} i = n(n + 1)/2$ for all $n \in \mathbb{N}$

1. Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n + 1)/2$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   $\sum_{i=0}^{n} i = 0 = 0(0 + 1)/2$ so $P(0)$ is true.

3. Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$. 
Prove $\sum_{i=0}^{n} i = n(n + 1)/2$ for all $n \in \mathbb{N}$

① Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n + 1)/2$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):
   $\sum_{i=0}^{n} i = 0 = 0(0 + 1)/2$ so $P(0)$ is true.

③ Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ Inductive step:
   We want to prove that $P(k + 1)$ is true, i.e., $\sum_{i=0}^{k+1} i = (k + 1)(k + 2)/2$. Note that
   $\sum_{i=0}^{k+1} i = (\sum_{i=0}^{k} i) + (k + 1) = (k(k + 1)/2) + (k + 1)$ by the inductive hypothesis.
   From this, we have that $(k(k + 1)/2) + (k + 1) = (k + 1)(k/2 + 1) = (k + 1)(k + 2)/2$, which is exactly $P(k + 1)$. 
Prove $\sum_{i=0}^{n} i = n(n + 1)/2$ for all $n \in \mathbb{N}$

1. Let $P(n)$ be $\sum_{i=0}^{n} i = 0 + 1 + \ldots + n = n(n + 1)/2$. We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   $\sum_{i=0}^{n} i = 0 = 0(0 + 1)/2$ so $P(0)$ is true.

3. Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

4. Inductive step:
   We want to prove that $P(k + 1)$ is true, i.e., $\sum_{i=0}^{k+1} i = (k + 1)(k + 2)/2$. Note that $\sum_{i=0}^{k+1} i = (\sum_{i=0}^{k} i) + (k + 1) = (k(k + 1)/2) + (k + 1)$ by the inductive hypothesis. From this, we have that $(k(k + 1)/2) + (k + 1) = (k + 1)(k/2 + 1) = (k + 1)(k + 2)/2$, which is exactly $P(k + 1)$.

5. The result follows for all $n \geq 0$ by induction.
What number divides $2^{2n} - 1$ for every $n \in \mathbb{N}$?
What number divides $2^{2n} - 1$ for every $n \in \mathbb{N}$?

Let’s look at a few examples:

$2^{2\cdot0} - 1 = 1 - 1 = 0 = 3 \cdot 0$

$2^{2\cdot1} - 1 = 4 - 1 = 3 = 3 \cdot 1$

$2^{2\cdot2} - 1 = 16 - 1 = 15 = 3 \cdot 5$

$2^{2\cdot3} - 1 = 64 - 1 = 63 = 3 \cdot 21$

$2^{2\cdot4} - 1 = 256 - 1 = 255 = 3 \cdot 85$
What number divides $2^{2n} - 1$ for every $n \in \mathbb{N}$?

Let’s look at a few examples:

$2^{2\times 0} - 1 = 1 - 1 = 0 = 3 \times 0$

$2^{2\times 1} - 1 = 4 - 1 = 3 = 3 \times 1$

$2^{2\times 2} - 1 = 16 - 1 = 15 = 3 \times 5$

$2^{2\times 3} - 1 = 64 - 1 = 63 = 3 \times 21$

$2^{2\times 4} - 1 = 256 - 1 = 255 = 3 \times 85$

It looks like $3 | (2^{2n} - 1)$.

Let’s use induction to prove it!
Prove $3|\left(2^{2n} - 1\right)$ for all $n \in \mathbb{N}$
Prove $3 | (2^{2n} - 1)$ for all $n \in \mathbb{N}$

Let $P(n)$ be $3 | (2^{2n} - 1)$.
We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.
Prove $3|(2^{2n} - 1)$ for all $n \in \mathbb{N}$

① Let $P(n)$ be $3|(2^{2n} - 1)$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):
   $2^{2*0} - 1 = 1 - 1 = 0 = 3 \times 0$ so $P(0)$ is true.
Prove $3|(2^{2n} - 1)$ for all $n \in \mathbb{N}$

1. Let $P(n)$ be $3|(2^{2n} - 1)$.
   We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

2. Base case ($n = 0$):
   $2^{2*0} - 1 = 1 - 1 = 0 = 3 \times 0$ so $P(0)$ is true.

3. Inductive hypothesis:
   Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$. 

Prove $3|(2^{2n} - 1)$ for all $n \in \mathbb{N}$

① Let $P(n)$ be $3|(2^{2n} - 1)$.
We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):
$2^{2*0} - 1 = 1 - 1 = 0 = 3 \times 0$ so $P(0)$ is true.

③ Inductive hypothesis:
Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ Inductive step:
We want to prove that $P(k + 1)$ is true, i.e., $3|(2^{2(k+1)} - 1)$. By inductive hypothesis, $3|(2^{2k} - 1)$ so $2^{2k} - 1 = 3j$ for some integer $j$. We therefore have that $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j + 1) - 1 = 12j + 3 = 3(4j + 1)$. So $3|(2^{2(k+1)} - 1)$, which is exactly $P(k + 1)$. 


Prove $3|(2^{2n} - 1)$ for all $n \in \mathbb{N}$

① Let $P(n)$ be $3|(2^{2n} - 1)$.
We will show that $P(n)$ is true for every integer $n \geq 0$ by induction.

② Base case ($n = 0$):
$2^{2*0} - 1 = 1 - 1 = 0 = 3 \times 0$ so $P(0)$ is true.

③ Inductive hypothesis:
Suppose that $P(k)$ is true for an arbitrary integer $k \geq 0$.

④ Inductive step:
We want to prove that $P(k + 1)$ is true, i.e., $3|(2^{2(k+1)} - 1)$. By inductive hypothesis, $3|(2^{2k} - 1)$ so $2^{2k} - 1 = 3j$ for some integer $j$. We therefore have that $2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 4(2^{2k}) - 1 = 4(3j + 1) - 1 = 12j + 3 = 3(4j + 1)$. So $3|(2^{2(k+1)} - 1)$, which is exactly $P(k + 1)$.

⑤ The result follows for all $n \geq 0$ by induction.
Summary

Fast modular exponentiation efficiently computes $a^k \mod m$.

Important practical applications include public-key cryptography (RSA).

Induction lets us prove statements about all natural numbers.

A proof by induction must show that $P(0)$ is true (base case).

And it must use the inductive hypothesis $P(k)$ to show that $P(k + 1)$ is true (inductive step).