CSE 311 Lecture 15: Modular Exponentiation and Induction

Emina Torlak and Kevin Zatloukal

Topics

Modular equations

A quick review of Lecture 14.

Modular exponentiation

A fast algorithm for computing $a^k \bmod m$.

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 $\mathrm{GCD}(a, b) = sa + tb$.

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

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

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

These inverses let us solve modular equations.

Using multiplicative inverses to solve modular equations

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

Using multiplicative inverses to solve modular equations

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

① Compute GCD and keep the tableau.

$$\begin{aligned}\mathrm{GCD}(26, 7) &= \mathrm{GCD}(7, 5) = \mathrm{GCD}(5, 2) \\ &= \mathrm{GCD}(2, 1) = \mathrm{GCD}(1, 0) \\ &= 1\end{aligned}$$

Using multiplicative inverses to solve modular equations

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

① Compute GCD and keep the tableau.

$$\begin{aligned}\mathrm{GCD}(26, 7) &= \mathrm{GCD}(7, 5) = \mathrm{GCD}(5, 2) \\ &= \mathrm{GCD}(2, 1) = \mathrm{GCD}(1, 0) \\ &= 1\end{aligned}$$

② Solve the equations for r in the tableau.

$$\begin{aligned} a &= q * b + r \\ 26 &= 3 * 7 + 5 \\ 7 &= 1 * 5 + 2 \\ 5 &= 2 * 2 + 1 \end{aligned}$$

$$\begin{aligned} r &= a - q * b \\ 5 &= 26 - 3 * 7 \\ 2 &= 7 - 1 * 5 \\ 1 &= 5 - 2 * 2 \end{aligned}$$

Using multiplicative inverses to solve modular equations

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

① Compute GCD and keep the tableau.

$$\begin{aligned}\mathrm{GCD}(26,7) &= \mathrm{GCD}(7,5) = \mathrm{GCD}(5,2)\\ &= \mathrm{GCD}(2,1) = \mathrm{GCD}(1,0)\\ &= 1\end{aligned}$$

② Solve the equations for r in the tableau.

$$\begin{array}{r} a = q*b + r \\ 26 = 3*7 + 5 \\ 7 = 1*5 + 2 \\ 5 = 2*2 + 1 \end{array}$$

$$\begin{array}{r} r = a - q*b \\ 5 = 26 - 3*7 \\ 2 = 7 - 1*5 \\ 1 = 5 - 2*2 \end{array}$$

③ Back substitute the equations for r.

$$\begin{aligned}1 &= 5 - 2*(7 - 1*5)\\ &= (-2)*7 + 3*5\\ &= (-2)*7 + 3*(26 - 3*7)\\ &= 3*26 + (-11)*7\end{aligned}$$

Using multiplicative inverses to solve modular equations

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

① Compute GCD and keep the tableau.

$$\begin{aligned}\mathrm{GCD}(26,7) &= \mathrm{GCD}(7,5) = \mathrm{GCD}(5,2)\\ &= \mathrm{GCD}(2,1) = \mathrm{GCD}(1,0)\\ &= 1\end{aligned}$$

② Solve the equations for r in the tableau.

$a = q * b + r$	$r = a - q * b$
$26 = 3 * 7 + 5$	$5 = 26 - 3 * 7$
$7 = 1 * 5 + 2$	$2 = 7 - 1 * 5$
$5 = 2 * 2 + 1$	$1 = 5 - 2 * 2$

③ Back substitute the equations for r.

$$\begin{aligned}1 &= 5 - 2 * (7 - 1 * 5)\\ &= (-2) * 7 + 3 * 5\\ &= (-2) * 7 + 3 * (26 - 3 * 7)\\ &= 3 * 26 + (-11) * 7\end{aligned}$$

④ Solve for x.

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

Solving a more general equation

Solve: $7y \equiv 3 \pmod{26}$

Solving a more general equation

Solve: $7y \equiv 3 \pmod{26}$

We computed that 15 is the multiplicative inverse of 7 modulo 26:

That is, $7 * 15 \equiv 1 \pmod{26}$.

Solving a more general equation

Solve: $7y \equiv 3 \pmod{26}$

We computed that 15 is the multiplicative inverse of 7 modulo 26:

That is, $7 * 15 \equiv 1 \pmod{26}$.

By the multiplication property of mod, we have

That is, $7 * 15 * 3 \equiv 1 * 3 \pmod{26}$.

Solving a more general equation

Solve: $7y \equiv 3 \pmod{26}$

We computed that 15 is the multiplicative inverse of 7 modulo 26:

That is, $7 * 15 \equiv 1 \pmod{26}$.

By the multiplication property of mod, we have

That is, $7 * 15 * 3 \equiv 1 * 3 \pmod{26}$.

So, any $\mathbf{y \equiv 15 * 3 \pmod{26}}$ is a solution.

That is, $y = 19 + 26k$ for any $k \in \mathbb{Z}$ is a solution.

A useful proof technique based on modular equations

Suppose that $\mathbf{x, y} \in \mathbb{Z}$ and $(\mathbf{x, y})$ satisfies linear equations

$ax + by = c$ and $dx + ey = f$,

where a, b, c, d, e, f are integer coefficients.

Then $(\mathbf{x, y})$ also satisfies the corresponding equations mod $\mathbf{m > 0} \in \mathbb{Z}$:

$ax + by \equiv c \pmod{m}$ and $dx + ey \equiv f \pmod{m}$.

A useful proof technique based on modular equations

Suppose that $\mathbf{x, y} \in \mathbb{Z}$ and $(\mathbf{x, y})$ satisfies linear equations

$ax + by = c$ and $dx + ey = f$,

where a, b, c, d, e, f are integer coefficients.

Then $(\mathbf{x, y})$ also satisfies the corresponding equations mod $\mathbf{m > 0} \in \mathbb{Z}$:

$ax + by \equiv c \pmod{m}$ and $dx + ey \equiv f \pmod{m}$.

The reverse doesn't hold. Can you think of a counterexample?

A useful proof technique based on modular equations

Suppose that $\mathbf{x, y} \in \mathbb{Z}$ and $(\mathbf{x, y})$ satisfies linear equations

$ax + by = c$ and $dx + ey = f$,

where a, b, c, d, e, f are integer coefficients.

Then $(\mathbf{x, y})$ also satisfies the corresponding equations mod $\mathbf{m > 0} \in \mathbb{Z}$:

$ax + by \equiv c \pmod{m}$ and $dx + ey \equiv f \pmod{m}$.

The reverse doesn't hold. Can you think of a counterexample?

$(0, 0)$ is a solution to $x + y \equiv 2 \pmod{2}$ and $2x + 2y \equiv 4 \pmod{2}$.

But it's not a solution to $x + y = 2$ and $2x + 2y = 4$.

A useful proof technique based on modular equations

Suppose that $\mathbf{x, y} \in \mathbb{Z}$ and $(\mathbf{x, y})$ satisfies linear equations

$ax + by = c$ and $dx + ey = f$,

where a, b, c, d, e, f are integer coefficients.

Then $(\mathbf{x, y})$ also satisfies the corresponding equations mod $\mathbf{m > 0} \in \mathbb{Z}$:

$ax + by \equiv c \pmod{m}$ and $dx + ey \equiv f \pmod{m}$.

The reverse doesn't hold. Can you think of a counterexample?

$(0, 0)$ is a solution to $x + y \equiv 2 \pmod{2}$ and $2x + 2y \equiv 4 \pmod{2}$.

But it's not a solution to $x + y = 2$ and $2x + 2y = 4$.

The contrapositive is a useful proof technique:

You can prove that a system of linear equations with integer coefficients has *no integer solutions* by showing that those equations modulo m have no solutions.

Modular exponentiation

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

The modular exponentiation problem: $\mathbf{a^k \bmod m}$

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

The modular exponentiation problem: $\mathbf{a^k \bmod m}$

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

Naive approach

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

The modular exponentiation problem: $a^k \bmod m$

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

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: $a^k \bmod m$

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

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: $\mathbf{a^k \bmod m}$ for $\mathbf{k = 2^i}$

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

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

Repeated squaring: $\mathbf{a^k \bmod m}$ for $\mathbf{k = 2^i}$

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

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

For example:

$$a^2 \bmod m = (a \bmod m)^2 \bmod m$$
$$a^4 \bmod m = (a^2 \bmod m)^2 \bmod m$$
$$a^8 \bmod m = (a^4 \bmod m)^2 \bmod m$$
$$a^{16} \bmod m = (a^8 \bmod m)^2 \bmod m$$
$$a^{32} \bmod m = (a^{16} \bmod m)^2 \bmod m$$

Repeated squaring: $\mathbf{a^k \bmod m}$ for $\mathbf{k = 2^i}$

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

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

For example:

$$a^2 \bmod m = (a \bmod m)^2 \bmod m$$
$$a^4 \bmod m = (a^2 \bmod m)^2 \bmod m$$
$$a^8 \bmod m = (a^4 \bmod m)^2 \bmod m$$
$$a^{16} \bmod m = (a^8 \bmod m)^2 \bmod m$$
$$a^{32} \bmod m = (a^{16} \bmod m)^2 \bmod m$$

What if k is not a power of 2?

Fast exponentiation: $\mathbf{a^k \bmod m}$ for all $\mathbf{k}$

Note that 81453 is 10011111000101101 in binary.

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

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

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

Note that 81453 is 1001111000101101 in binary.

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

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

$$\begin{aligned} a^{81453} \bmod m = ((((((((((a^{2^{16}} \bmod m * \\ a^{2^{13}} \bmod m) \bmod m * \\ a^{2^{12}} \bmod m) \bmod m * \\ a^{2^{11}} \bmod m) \bmod m * \\ a^{2^{10}} \bmod m) \bmod m * \\ a^{2^9} \bmod m) \bmod m * \\ a^{2^5} \bmod m) \bmod m * \\ a^{2^3} \bmod m) \bmod m * \\ a^{2^2} \bmod m) \bmod m * \\ a^{2^0} \bmod m) \bmod m) \end{aligned}$$

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

Note that 81453 is 1001111000101101 in binary.

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

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

$$\begin{aligned} a^{81453} \bmod m = ((((((((((a^{2^{16}} \bmod m * \\ a^{2^{13}} \bmod m) \bmod m * \\ a^{2^{12}} \bmod m) \bmod m * \\ a^{2^{11}} \bmod m) \bmod m * \\ a^{2^{10}} \bmod m) \bmod m * \\ a^{2^9} \bmod m) \bmod m * \\ a^{2^5} \bmod m) \bmod m * \\ a^{2^3} \bmod m) \bmod m * \\ a^{2^2} \bmod m) \bmod m * \\ a^{2^0} \bmod m) \bmod m) \end{aligned}$$

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

The fast exponentiation algorithm

$$a^{2j} \bmod m = (a^j \bmod m)^2 \bmod m$$
$$a^{2j+1} \bmod m = ((a \bmod m) * (a^{2j} \bmod m)) \bmod m$$

The fast exponentiation algorithm

$$a^{2j} \bmod m = (a^j \bmod m)^2 \bmod m$$
$$a^{2j+1} \bmod m = ((a \bmod m) * (a^{2j} \bmod m)) \bmod m$$

Example implementation:

```
// Assumes a > 0, k >= 0, m > 0.
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 * tmp) % m;
    }
}
```

The fast exponentiation algorithm

$$a^{2j} \bmod m = (a^j \bmod m)^2 \bmod m$$
$$a^{2j+1} \bmod m = ((a \bmod m) * (a^{2j} \bmod m)) \bmod m$$

Example implementation:

```
// Assumes a > 0, k >= 0, m > 0.
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 * tmp) % m;
    }
}
```

$$78365^{81453} \bmod 104729 = 45235$$

Using fast modular exponentiation: RSA encryption

Alice chooses random 512-bit (or 1024-bit) primes $\mathbf{p}$, $\mathbf{q}$ and exponent $\mathbf{e}$.

Alice computes $m = pq$ and broadcasts (m, e), which is her public key.
She also computes the multiplicative inverse d of $e \bmod (p-1)(q-1)$,
which serves as her private key.

To encrypt a message $\mathbf{a}$ with Alice's public key, Bob computes $\mathbf{C = a^e \bmod m}$.

This computation uses fast modular exponentiation.
Bob sends the ciphertext C to Alice.

To decrypt $\mathbf{C}$, Alice computes $\mathbf{C^d \bmod m}$.

This computation also uses fast modular exponentiation.
It works because $C^d \bmod m = a$ 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?

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 $a \equiv b \pmod{m}$.
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 $k \geq 0$,
$a \equiv b \pmod{m} \rightarrow a^k \equiv b^k \pmod{m}$.

Proof

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

$$(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^2 \equiv b^2 \pmod{m})$$
$$(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^3 \equiv b^3 \pmod{m})$$
$$\dots$$
$$(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^k \equiv b^k \pmod{m}).$$

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 (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

$$(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^2 \equiv b^2 \pmod{m})$$
$$(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^3 \equiv b^3 \pmod{m})$$
$$\dots$$
$$(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^k \equiv b^k \pmod{m}).$$

This, uhm, completes the proof? □

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

$$(a \equiv b \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^2 \equiv b^2 \pmod{m})$$
$$(a^2 \equiv b^2 \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^3 \equiv b^3 \pmod{m})$$
$$\dots$$
$$(a^{(k-1)} \equiv b^{(k-1)} \pmod{m} \wedge a \equiv b \pmod{m}) \rightarrow (a^k \equiv b^k \pmod{m}).$$

This, uhm, completes the proof? □

We don't have a proof rule to say "perform this step repeatedly."

Perform a step repeatedly with induction!

Induction $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

Perform a step repeatedly with induction!

$$\textbf{Induction}\ \frac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$$

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.

Perform a step repeatedly with induction!

Induction $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

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.

```
// 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 $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

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

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

Induction: how does it work?

Induction $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

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

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

1. First, we have $P(0)$. **P(0)**

Induction: how does it work?

Induction $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

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

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

1. First, we have $P(0)$.
2. Since $P(k) \to P(k+1)$ for all k, we have $P(0) \to P(1)$.

P(0)

$\Downarrow$ **P(0)→P(1)**

Induction: how does it work?

Induction $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

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

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

1. First, we have $P(0)$. **P(0)**
2. Since $P(k) \to P(k+1)$ for all k, we have $P(0) \to P(1)$. ⇓ **P(0)→P(1)**
3. Applying Modus Ponens to 1 and 2, we get $P(1)$. **P(1)**

Induction: how does it work?

Induction $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

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

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

1. First, we have $P(0)$.
2. Since $P(k) \to P(k+1)$ for all k, we have $P(0) \to P(1)$.
3. Applying Modus Ponens to 1 and 2, we get $P(1)$.
4. Since $P(k) \to P(k+1)$ for all k, we have $P(1) \to P(2)$.

$\mathbf{P(0)}$

$\Downarrow_{\mathbf{P(0) \to P(1)}}$

$\mathbf{P(1)}$

$\Downarrow_{\mathbf{P(1) \to P(2)}}$

Induction: how does it work?

Induction $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

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

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

1. First, we have $P(0)$. **P(0)**
2. Since $P(k) \to P(k+1)$ for all k, we have $P(0) \to P(1)$. ⇓ **P(0)→P(1)**
3. Applying Modus Ponens to 1 and 2, we get $P(1)$. **P(1)**
4. Since $P(k) \to P(k+1)$ for all k, we have $P(1) \to P(2)$. ⇓ **P(1)→P(2)**
5. Applying Modus Ponens to 3 and 4, we get $P(2)$. **P(2)**

Induction: how does it work?

Induction $\dfrac{P(0); \forall k.\, P(k) \to P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

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

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

1. First, we have $P(0)$.
2. Since $P(k) \to P(k+1)$ for all k, we have $P(0) \to P(1)$.
3. Applying Modus Ponens to 1 and 2, we get $P(1)$.
4. Since $P(k) \to P(k+1)$ for all k, we have $P(1) \to P(2)$.
5. Applying Modus Ponens to 3 and 4, we get $P(2)$.

⋮

11. Applying Modus Ponens to 9 and 10, we get $P(5)$.

P(0)
⇓ P(0)→P(1)
P(1)
⇓ P(1)→P(2)
P(2)
⇓ P(k)→P(k+1)
P(5)

Using induction

Using induction in formal and English proofs.

Using the induction rule in a formal proof

Induction $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

1. Prove $P(0)$

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

Using the induction rule in a formal proof

Induction $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

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 ∀: 2, 4
6. $\forall n.\, P(n)$ — Induction: 1, 5

Using the induction rule in a formal proof

Induction $\dfrac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$

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

Using the induction rule in a formal proof: key parts

Induction $$\frac{P(0); \forall k.\, P(k) \rightarrow P(k+1)}{\therefore\ \forall n.\, P(n)}$$

1. Prove $P(0)$		**Base case**
2. Let $k \geq 0$ be an arbitrary integer		**Inductive hypothesis**
3.1. Assume that $P(k)$ is true		
3.2. …		**Inductive step**
3.3. Prove $P(k+1)$ is true		
4. $P(k) \rightarrow P(k+1)$	**Direct Proof Rule**	**Conclusion**
5. $\forall k.\, P(k) \rightarrow P(k+1)$	**Intro ∀: 2, 4**	
6. $\forall n.\, P(n)$	**Induction: 1, 5**	

Translating to an English proof: the template

① Let $\mathbf{P(n)}$ be *[definition of $P(n)$]*.

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

② Base case ($\mathbf{n = 0}$):

[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 $\mathbf{n \geq 0}$ by induction.

1. Prove $P(0)$		Base case
2. Let $k \geq 0$ be an arbitrary integer		Inductive hypothesis
3.1. Assume that $P(k)$ is true		
3.2. …		Inductive step
3.3. Prove $P(k+1)$ is true		
4. $P(k) \to P(k+1)$	Direct Proof Rule	Conclusion
5. $\forall k.\, P(k) \to P(k+1)$	Intro ∀: 2, 4	
6. $\forall n.\, P(n)$	Induction: 1, 5	

Translating to an English proof: the template

① **Let $\mathbf{P(n)}$ be** *[definition of $P(n)$]*.

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

② **Base case ($\mathbf{n = 0}$):**

[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 $\mathbf{n \geq 0}$ by induction.**

1. Prove $P(0)$		Base case
2. Let $k \geq 0$ be an arbitrary integer		Inductive hypothesis
3.1. Assume that $P(k)$ is true		
3.2. …		Inductive step
3.3. Prove $P(k+1)$ is true		
4. $P(k) \to P(k+1)$	Direct Proof Rule	Conclusion
5. $\forall k.\, P(k) \to P(k+1)$	Intro ∀: 2, 4	
6. $\forall n.\, P(n)$	Induction: 1, 5	

Induction **do**s and **don't**s:

- **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 ($n = 0$):**

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

③ **Inductive hypothesis:**

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

Prove $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ 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 $(2^{k+1} - 1) + 2^{k+1} = 2 * 2^{k+1} - 1 = 2^{k+1+1} - 1 = 2^{k+2} - 1$, 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 $(2^{k+1} - 1) + 2^{k+1} = 2 * 2^{k+1} - 1 = 2^{k+1+1} - 1 = 2^{k+2} - 1$, 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:

$$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$$
$$2^{2*1} - 1 = 4 - 1 = 3 = 3 * 1$$
$$2^{2*2} - 1 = 16 - 1 = 15 = 3 * 5$$
$$2^{2*3} - 1 = 64 - 1 = 63 = 3 * 21$$
$$2^{2*4} - 1 = 256 - 1 = 255 = 3 * 85$$

What number divides $2^{2n} - 1$ for every $n \in \mathbb{N}$?

Let's look at a few examples:

$$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$$
$$2^{2*1} - 1 = 4 - 1 = 3 = 3 * 1$$
$$2^{2*2} - 1 = 16 - 1 = 15 = 3 * 5$$
$$2^{2*3} - 1 = 64 - 1 = 63 = 3 * 21$$
$$2^{2*4} - 1 = 256 - 1 = 255 = 3 * 85$$

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

Let's use induction to prove it!

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

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.

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 ($n = 0$):**

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ 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 ($n = 0$):**

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ 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 ($n = 0$):**

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ 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 ($n = 0$):**

$2^{2*0} - 1 = 1 - 1 = 0 = 3 * 0$ 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 $\mathbf{a^k \bmod m}$.

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*).