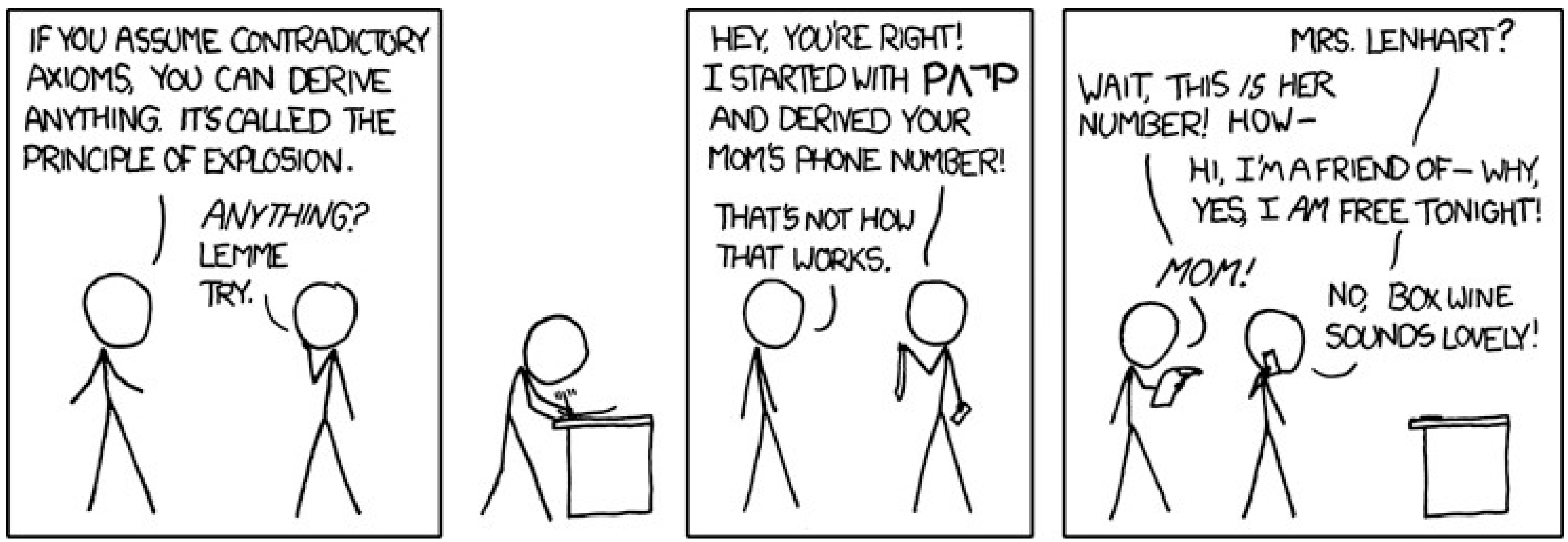


Number Theory

CSE 311
Lecture 9

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Step 1 (Compute GCD & Keep Tableau Information):

a b b a mod b = r b r

$$\gcd(35, 27) = \gcd(27, 35 \bmod 27) = \gcd(27, 8)$$

a = q * b + r

$$35 = 1 * 27 + 8$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Step 1 (Compute GCD & Keep Tableau Information):

a b b a mod b = r b r

$$\begin{aligned}
\gcd(35, 27) &= \gcd(27, 35 \bmod 27) = \gcd(27, 8) \\
&= \gcd(8, 27 \bmod 8) = \gcd(8, 3) \\
&= \gcd(3, 8 \bmod 3) = \gcd(3, 2) \\
&= \gcd(2, 3 \bmod 2) = \gcd(2, 1) \\
&= \gcd(1, 2 \bmod 1) = \gcd(1, 0)
\end{aligned}$$

a = q * b + r

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

Extended Euclidean algorithm

- **Can use Euclid's Algorithm to find s, t such that**

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

Step 2 (Solve the equations for r):

a = q * b + r

$$35 = 1 * 27 + 8$$
$$27 = 3 * 8 + 3$$
$$8 = 2 * 3 + 2$$
$$3 = 1 * 2 + 1$$

r = a -- q * b

$$8 = 35 - 1 * 27$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Step 2 (Solve the equations for r):

a = q * b + r	r = a – q * b
$35 = 1 * 27 + 8$	$8 = 35 - 1 * 27$
$27 = 3 * 8 + 3$	$3 = 27 - 3 * 8$
$8 = 2 * 3 + 2$	$2 = 8 - 2 * 3$
$3 = 1 * 2 + 1$	$1 = 3 - 1 * 2$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Step 3 (Backward Substitute Equations):

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$1 = 3 - 1 * 2$$

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Step 3 (Backward Substitute Equations):

$$8 = 35 - 1 * 27$$

$$3 = 27 - 3 * 8$$

$$2 = 8 - 2 * 3$$

$$1 = 3 - 1 * 2$$

Plug in the def of 2

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

Re-arrange into 3's and 8's

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Step 3 (Backward Substitute Equations):

$8 = 35 - 1 * 27$

$3 = 27 - 3 * 8$

$2 = 8 - 2 * 3$

$1 = 3 - 1 * 2$

Plug in the def of 2

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

Re-arrange into 3's and 8's

Plug in the def of 3

$$\begin{aligned} &= (-1) * 8 + 3 * (27 - 3 * 8) \\ &= (-1) * 8 + 3 * 27 + (-9) * 8 \\ &= 3 * 27 + (-10) * 8 \end{aligned}$$

Re-arrange into 8's and 27's

Extended Euclidean algorithm

- Can use Euclid's Algorithm to find s, t such that

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

Step 3 (Backward Substitute Equations):

$8 = 35 - 1 * 27$

$3 = 27 - 3 * 8$

$2 = 8 - 2 * 3$

$1 = 3 - 1 * 2$

Plug in the def of 2

$$1 = 3 - 1 * (8 - 2 * 3)$$
$$= 3 - 8 + 2 * 3$$
$$= (-1) * 8 + 3 * 3$$

Re-arrange into 3's and 8's

Plug in the def of 3

$$= (-1) * 8 + 3 * (27 - 3 * 8)$$
$$= (-1) * 8 + 3 * 27 + (-9) * 8$$
$$= 3 * 27 + (-10) * 8$$

Re-arrange into 8's and 27's

$$= 3 * 27 + (-10) * (35 - 1 * 27)$$
$$= 3 * 27 + (-10) * 35 + 10 * 27$$
$$= 13 * 27 + (-10) * 35$$

Re-arrange into 27's and 35's

Multiplicative inverse mod m

Let $0 \leq a, b < m$. Then, b is the *multiplicative inverse of* a *(modulo* m*)* iff $ab \equiv_m 1$.

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

mod 7

x	0	1	2	3	4	5	6	7	8	9
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

mod 10

Multiplicative inverse $\mathrm{mod}\ m$

Suppose $\gcd(a, m) = 1$

By Bézout's Theorem, there exist integers s and t
such that $sa + tm = 1$.

s is the multiplicative inverse of a (modulo m):

$$1 = sa + tm \equiv_m sa$$

So... we can compute multiplicative inverses with the extended Euclidean algorithm

These inverses let us solve modular equations...

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$

Find multiplicative inverse of 7 modulo 26

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$

Find multiplicative inverse of 7 modulo 26

$$\gcd(26, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$ **Find multiplicative inverse of 7 modulo 26**

$$\gcd(26, 7) = \gcd(7, 5) = \gcd(5, 2) = \gcd(2, 1) = 1$$

$$26 = 3 * 7 + 5$$
$$7 = 1 * 5 + 2$$
$$5 = 2 * 2 + 1$$

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$

Find multiplicative inverse of 7 modulo 26

$$\gcd(26,7) = \gcd(7,5) = \gcd(5,2) = \gcd(2,1) = 1$$

$$26 = 3 * 7 + 5 \qquad 5 = 26 - 3 * 7$$

$$7 = 1 * 5 + 2 \qquad 2 = 7 - 1 * 5$$

$$5 = 2 * 2 + 1 \qquad 1 = 5 - 2 * 2$$

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$

Find multiplicative inverse of 7 modulo 26

$$\gcd(26,7) = \gcd(7,5) = \gcd(5,2) = \gcd(2,1) = 1$$

$$26 = 3 * 7 + 5 \qquad 5 = 26 - 3 * 7$$

$$7 = 1 * 5 + 2 \qquad 2 = 7 - 1 * 5$$

$$5 = 2 * 2 + 1 \qquad 1 = 5 - 2 * 2$$

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

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$

Find multiplicative inverse of 7 modulo 26

$$\gcd(26,7) = \gcd(7,5) = \gcd(5,2) = \gcd(2,1) = 1$$

$$26 = 3 * 7 + 5 \qquad 5 = 26 - 3 * 7$$
$$7 = 1 * 5 + 2 \qquad 2 = 7 - 1 * 5$$
$$5 = 2 * 2 + 1 \qquad 1 = 5 - 2 * 2$$

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

Now $(-11) \bmod 26 = 15.$

"the" multiplicative inverse

(-11 is also "a" multiplicative inverse)

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$

Find multiplicative inverse of 7 modulo 26**… it's** 15**.**

Multiplying both sides by 15 **gives**

$$15 \cdot 7\text{x} \equiv_{26} 15 \cdot 3$$

Simplify on both sides to get

$$\text{x} \equiv_{26} 15 \cdot 7\text{x} \equiv_{26} 15 \cdot 3 \equiv_{26} 19$$

So, <u>all</u> solutions of this congruence are numbers of the form $x = 19 + 26k$ **for some** $k \in \mathbb{Z}$**.**

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$

Conversely, suppose that $x \equiv_{26} 19$.

Multiplying both sides by 7 gives

$$7\mathrm{x} \equiv_{26} 7 \cdot 19$$

Simplify on right to get

$$7\mathrm{x} \equiv_{26} 7 \cdot 19 \equiv_{26} 3$$

So, <u>all</u> numbers of form $x = 19 + 26k$ for any $k \in \mathbb{Z}$ are solutions of this equation.

Example: Solve a Modular Equation

Solve: $7x \equiv_{26} 3$ **(on HW or exams)**

Step 1. Find multiplicative inverse of 7 modulo 26

$$1 \;=\; \dots \;=\; (-11) * 7 \;+\; 3 * 26$$

Since $(-11) \bmod 26 = 15$**, the inverse of** 7 **is** 15**.**

Step 2. Multiply both sides and simplify

Multiplying by 15**, we get** $x \equiv_{26} 15 \cdot 7x \equiv_{26} 15 \cdot 3 \equiv_{26} 19.$

Step 3. State the full set of solutions

So, the solutions are $19 + 26k$ **for any** $k \in \mathbb{Z}$

(must be of the form $a + mk$ **for all** $k \in \mathbb{Z}$ **with** $0 \le a < m$**)**

Math mod a prime is especially nice

$\gcd(a, m) = 1$ if m is prime and $0 < a < m$ so can always solve these equations mod a prime.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

mod 7

Multiplicative Inverses and Algebra

Adding to both sides easily reversible:

$-c$ $\quad$ $+c$

$$x \equiv_m y$$

$$x + c \equiv_m y + c$$

The same is not true of multiplication…

unless we have a multiplicative inverse $cd \equiv_m 1$

$\times\, d$ $\quad$ $\times\, c$

$$x \equiv_m y$$

$$cx \equiv_m cy$$

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

Small Multiplications

Since $b = qm + (b \bmod m)$, we have $b \bmod m \equiv_m b$.

And since $c = tm + (c \bmod m)$, we have $c \bmod m \equiv_m c$.

Multiplying these gives $(b \bmod m)(c \bmod m) \equiv_m bc$.

By the Lemma from a few lectures ago, this tells us
$bc \bmod m = (b \bmod m)(c \bmod m) \bmod m$.

Okay to mod b and c by m before multiplying if we are planning to mod the result by m

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

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} mod m=

$(\ldots(((((a^{2^{16}}$ mod m $\cdot$

$a^{2^{13}}$ mod m) mod m $\cdot$

$a^{2^{12}}$ mod m) mod m $\cdot$

$a^{2^{11}}$ mod m) mod m $\cdot$

$a^{2^{10}}$ mod m) mod m $\cdot$

$a^{2^{9}}$ mod m) mod m $\cdot$

$a^{2^{5}}$ mod m) mod m $\cdot$

$a^{2^{3}}$ mod m) mod m $\cdot$

$a^{2^{2}}$ mod m) mod m $\cdot$

$a^{2^{0}}$ mod m) mod 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

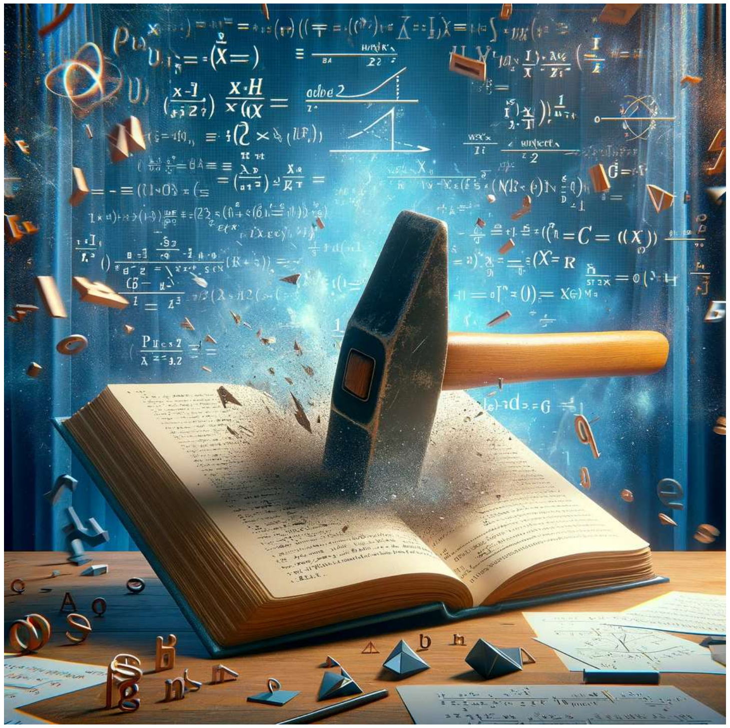
```
public static int FastModExp(int a, int k, int modulus) {

        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;
                }
}
```

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

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

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 $\boldsymbol{p}, \boldsymbol{q}$ and 512/1024-bit exponent $\boldsymbol{e}$. Computes $\boldsymbol{m} = \boldsymbol{p} \cdot \boldsymbol{q}$
  - Vendor broadcasts $(\boldsymbol{m}, \boldsymbol{e})$
  - To send $\boldsymbol{a}$ to vendor, you compute $\boldsymbol{C} = \boldsymbol{a}^{\boldsymbol{e}} \bmod \boldsymbol{m}$ using *fast modular exponentiation* and send $\boldsymbol{C}$ to the vendor.
  - Using secret $\boldsymbol{p}, \boldsymbol{q}$ the vendor computes $\boldsymbol{d}$ that is the *multiplicative inverse* of $\boldsymbol{e}$ mod $(\boldsymbol{p} - \mathbf{1})(\boldsymbol{q} - \mathbf{1})$.
  - Vendor computes $\boldsymbol{C}^{\boldsymbol{d}} \bmod \boldsymbol{m}$ using *fast modular exponentiation*.
  - Fact: $\boldsymbol{a} = \boldsymbol{C}^{\boldsymbol{d}} \bmod \boldsymbol{m}$ for $\mathbf{0} < \boldsymbol{a} < \boldsymbol{m}$ unless $\boldsymbol{p} | \boldsymbol{a}$ or $\boldsymbol{q} | \boldsymbol{a}$
  - Great Resource



Proof By Contradiction

In real life!

- Claim: My Tire is Leaking
- Suppose that this tire was not leaking
- This means the tire pressure should be constant
- I observe the pressure is dropping at a moderate rate
- But there should be constant pressure if it was not leaking
- Therefore, it must be leaking

Proof by Contradiction Skeleton

Claim: p is true.

- Suppose for the sake of contradiction $\neg p$.
- ...
- Then some statement s must hold.
- ...
- And some statement $\neg s$ must hold.
- But s and $\neg s$ is a contradiction. So p must be true.

My tire is leaking

Suppose my tire is not leaking

The tire pressure must be constant

The tire pressure is decreasing

My Tire is leaking

Why does this work?

Let's say the claim you are trying to prove is p.

A proof by contradiction shows the following implication:

$$\neg p \rightarrow False$$

Why does this implication show p?

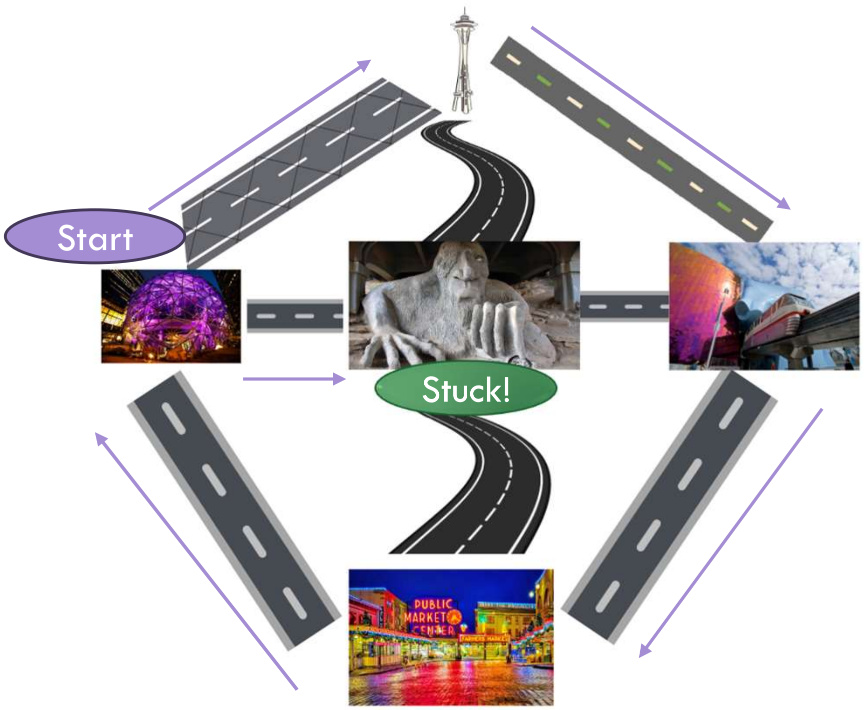
Hint think contrapositive

The contrapositive is $True \rightarrow p$ which simplifies to just p.

This means that by proving $\neg p \rightarrow False$, you have proved p is True!

Graph Example

Can we travel on every road, without going on a road twice*?



There is no path, let's prove it!

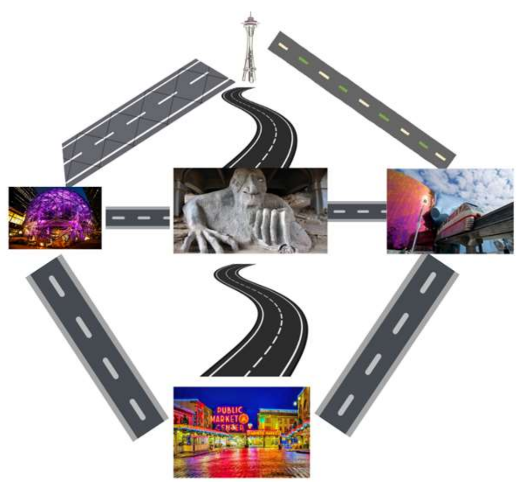
*Starting and ending at a different place

Graph Example

Claim: it is impossible to travel on every road visiting each road exactly once

Proof: Suppose that it is *possible* to travel on every road visiting each road exactly once.

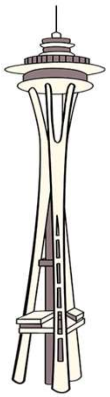
Consider how many times each landmark would be passed through on this path.



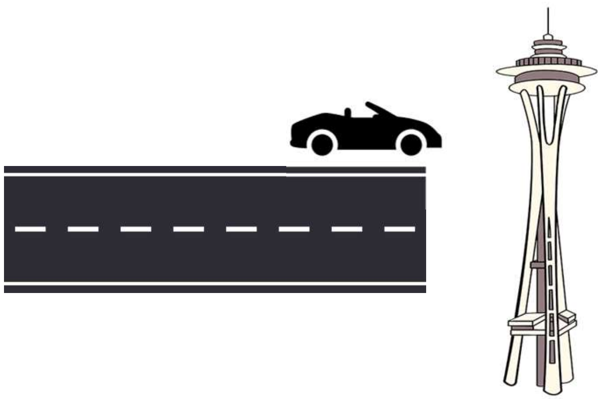
However [] is a contradiction!

Therefore, it must be impossible to visit every road exactly once

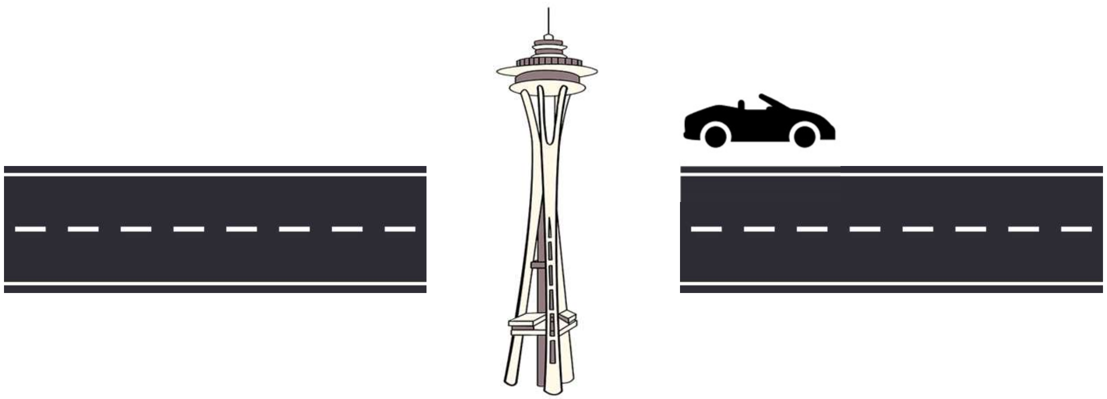
We enter and exit a landmark



Graph Example

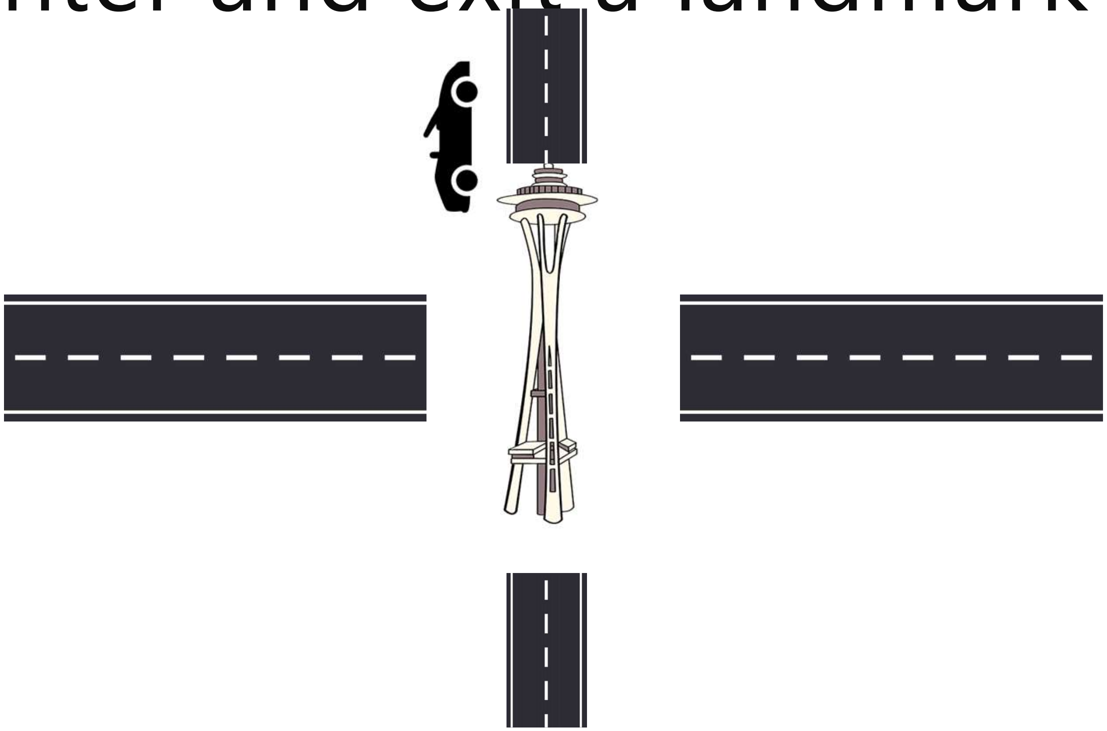


We enter and exit a landmark



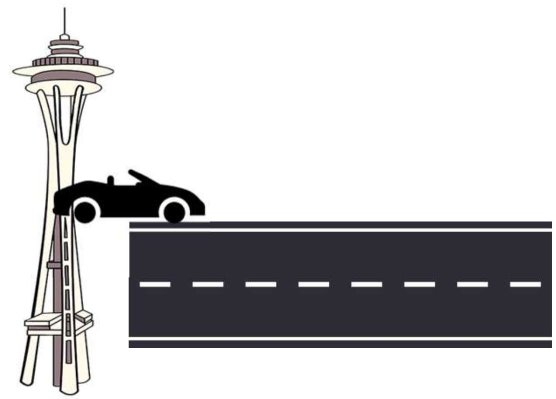
Notice that this means there are an even number of roads that we drove on connected to this landmark

We enter and exit a landmark



Even if we go through it again on new roads, this holds

We Start at the Landmark



Notice we drove on only one road, (as we *started* in the landmark) making it have an odd number of roads that connect to it

We End at the Landmark

Notice we drove on only one road, (as we *ended* in the landmark) making it have an odd number of roads that connect to it

Graph Example

Claim: it is impossible to travel on every road visiting each road exactly once

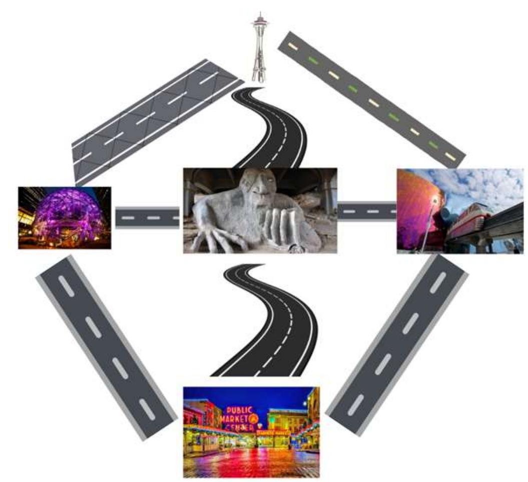
Proof: Suppose that it is *possible* to travel on every road visiting each road exactly once.

Consider how many times each landmark would be passed through on this path.

As we observed, all of the landmarks on our path must have an even number of roads, except for the starting and ending one, making us have exactly 2 landmarks with an odd number of connecting roads.

However [] is a contradiction!

Therefore, it must be impossible to visit every road exactly once



Graph Example

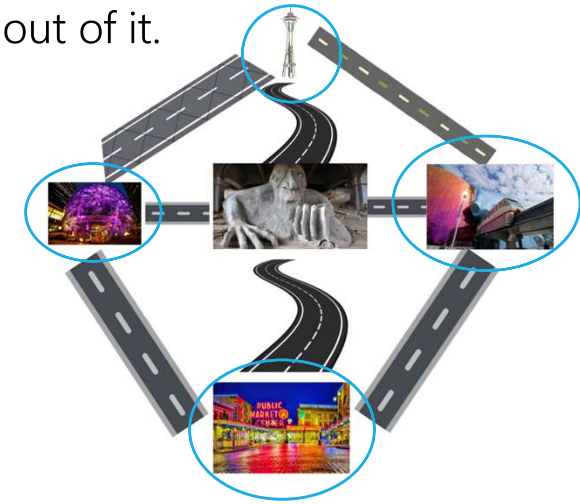
Claim: it is impossible to travel on every road visiting each road exactly once

Proof: Suppose that it is *possible* to travel on every road visiting each road exactly once.

Consider how many times each landmark would be passed through on this path.

As we observed, all of the landmarks on our path must have an even number of roads, except for the starting and ending one, making us have exactly 2 landmarks with an odd number of connecting roads.

However, our graph has 4 landmarks with an odd number of roads coming out of it.



However [] is a contradiction!

Therefore, it must be impossible to visit every road exactly once

Graph Example

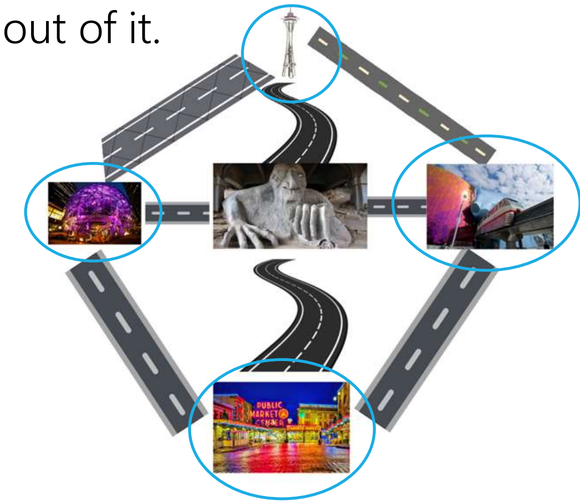
Claim: it is impossible to travel on every road visiting each road exactly once

Proof: Suppose that it is *possible* to travel on every road visiting each road exactly once.

Consider how many times each landmark would be passed through on this path.

As we observed, all of the landmarks on our path must have an even number of roads, except for the starting and ending one, making us have exactly 2 landmarks with an odd number of connecting roads.

However, our graph has 4 landmarks with an odd number of roads coming out of it.



But since 2 is not 4, this is a contradiction!

Therefore, it must be impossible to visit every road exactly once

Proof by Contradiction Examples

Proof By Contradiction

If a^2 is even, then a is even

- Claim: $\sqrt{2}$ is irrational (i.e not rational)
- Proof:

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational

Notice target is unknown

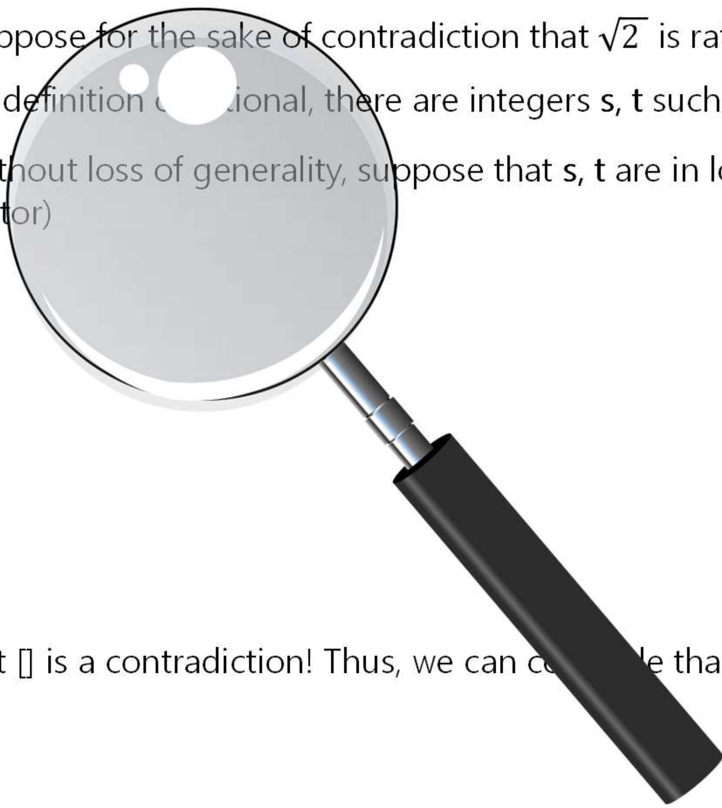
But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:



Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

What is “Without Loss of Generality”?

You can use this when it looks like you are introducing a new assumption, but you are not, and the claim is still general. Only use if it would be immediately obvious to the reader why it is the case

In this case: if s and t share a factor other than 1, i.e k, we can just cancel out their common factor and continue the proof. (i.e $\frac{s\prime k}{t\prime k} = \frac{s}{t}$)

Another example:

Let x,y be integers; without loss of generality, assume $x \geq y$.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$$\sqrt{2} = \frac{s}{t}$$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2\mathrm{t}^2 = 4k^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2t^2 = 4k^2$

Dividing both sides by two, we get $t^2 = 2k^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2\text{t}^2 = 4k^2$

Dividing both sides by two, we get $\text{t}^2 = 2k^2$, making t^2 is even, making t even by our lemma.

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2t^2 = 4k^2$

Dividing both sides by two, we get $t^2 = 2k^2$, making t^2 is even, making t even by our lemma.

But if both s and t are even, they must have a common factor of 2. But we said that the fraction $\frac{s}{t}$ was irreducible.

This is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof by Contradiction

Proof by contradiction is a strategy for proving statements of any form.

- The general strategy to prove p is to assume $\neg p$ and derive False.

Examples:

- The strategy to prove $p \rightarrow q$ is to assume $p \land \neg q$ and derive False.
- The strategy to prove $p \lor q$ is to assume $\neg p \land \neg q$ and derive False.

- The strategy to prove $\forall x(P(x))$ is to assume $\exists x\big(\neg P(x)\big)$ and derive False.
- The strategy to prove $\exists x(P(x))$ is to assume $\forall x(\neg P(x))$ and derive False.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Where can we find a contradiction?

- Show our list is non inclusive (i.e create a different prime number)
- Show one of the numbers in our list is not prime
- Create a contradiction with facts about prime factorization
- Show 1 = 2
- Show p is odd and even at the same time
- Proof by cases with a mix of the above

But [] is a contradiction! So, there must be infinitely many primes.

Proof by Contradiction: Remarks

- Unlike other proof techniques, we don't know *where* we're going.
  We're trying to find any contradiction. That can make it harder.
- Contradiction is a sledge-hammer.
  It can be used to prove many things. But it makes a mess.
- You can find a contradiction directly with your assumption

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q.

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q. This means that $q \% p_i = 0$.

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.

Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q,

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.

Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \ \%\, p_i$ using the definition of q, which gives us:

$$\mathrm{q} \,\%\, p_i =$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

> Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.
>
> Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q, which gives us:
>
> $$\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \,\%\, p_i =$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

> Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.
>
> Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q, which gives us:

$$\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \,\%\, p_i = (p_1 \cdot \dots p_i \cdot \dots \cdot p_k) + 1 \,\%\, p_i$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

> Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.
>
> Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q, which gives us:

$$\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \,\%\, p_i = (p_1 \cdot \dots p_i \cdot \dots \cdot p_k) + 1 \,\%\, p_i = 1$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

> Since q is composite, we know that some prime p_i must divide q. This means that $q \% p_i = 0$.
>
> Also, notice that $\mathrm{q} \% p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \ \% p_i$ using the definition of q, which gives us:
>
> $$\mathrm{q} \% p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \% p_i = (p_1 \cdot \dots p_i \cdot \dots \cdot p_k) + 1 \% p_i = 1$$
>
> This means that $q \% p_i$ equals both 1 and 0, which is impossible!

In both cases, this is a contradiction! So, there must be infinitely many primes.

Bonus Proof!

Claim: if a^2 is even, than a is even.

Proof:

Suppose for the sake of contradiction that a^2 is even *and* a is odd for some integer a.

This means that $\mathrm{a} = 2k + 1$ for some k.

Substituting this in, we have $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

Since $2k^2 + 2k$ is an integer, we have that a^2 is odd!

This is a contradiction however as a^2 cannot be both even and odd. Therefore through proof by contradiction, if a^2 is even, than a is even.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q. This means that $q \ \% \ p_i = 0$.

Also, notice that $\mathrm{q} \ \% \ p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \ \% \ p_i$ using the definition of q, which gives us:

$$\mathrm{q} \ \% \ p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \ \% \ p_i$$

In both cases, this is a contradiction! So, there must be infinitely many primes.