Rev For Mid1: Proofs

Review of Mods and GCD

Mods

The symbol $\mid$ means **divides**.

Mods

The symbol $|$ means **divides**.
Two equivalent definitions of Mod

Mods

The symbol $|$ means **divides**.

Two equivalent definitions of Mod

1. $a \equiv b \pmod{m}$ means m divides $b - a$.

Mods

The symbol $|$ means **divides**.
Two equivalent definitions of Mod

1. $a \equiv b \pmod{m}$ means m divides $b - a$.
2. The remainder when you divide a by m or b by m is the same.

Mods

The symbol $|$ means **divides**.

Two equivalent definitions of Mod

1. $a \equiv b \pmod{m}$ means m divides $b - a$.
2. The remainder when you divide a by m or b by m is the same.

We usually think of $a \equiv b \pmod{m}$ to mean that

Mods

The symbol $\mid$ means **divides**.
Two equivalent definitions of Mod

1. $a \equiv b \pmod{m}$ means m divides $b - a$.
2. The remainder when you divide a by m or b by m is the same.

We usually think of $a \equiv b \pmod{m}$ to mean that
a is **large** and

Mods

The symbol $\mid$ means **divides**.
Two equivalent definitions of Mod

1. $a \equiv b \pmod{m}$ means m divides $b - a$.
2. The remainder when you divide a by m or b by m is the same.

We usually think of $a \equiv b \pmod{m}$ to mean that
a is **large** and
$0 \le b \le m - 1$ (so **small**).

Do Examples of Mods

I ask random people in the class what a is congruent to mod m.

Addition and Mult with Mods

Theorem Assume
$a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.

Addition and Mult with Mods

Theorem Assume
$a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.

Then:

Addition and Mult with Mods

Theorem Assume
$a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.

Then:

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

Addition and Mult with Mods

Theorem Assume
$a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$.

Then:

1. $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.
2. $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod{7}]$.

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod{7}]$.
Note The theorem is about ALL $a \in \mathbb{N}$.

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod{7}]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$.

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod 7]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod 7]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 7$. All $\equiv$ are mod 7.

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod 7]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 7$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod 7]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 7$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.
0) $0^7 \equiv 0$. YES

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod 7]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 7$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.
0) $0^7 \equiv 0$. YES
1) $1^7 \equiv 1$. YES

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod{7}]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{7}$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.
0) $0^7 \equiv 0$. YES
1) $1^7 \equiv 1$. YES
2) $2^7 \equiv 2^3 \times 2^3 \times 2 \equiv 1 \times 1 \times 2 \equiv 2$. YES

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod{7}]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{7}$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.
0) $0^7 \equiv 0$. YES
1) $1^7 \equiv 1$. YES
2) $2^7 \equiv 2^3 \times 2^3 \times 2 \equiv 1 \times 1 \times 2 \equiv 2$. YES
3) $3^7 \equiv 3^3 \times 3^3 \times 3 \equiv -1 \times -1 \times 3 \equiv 3$. YES

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod{7}]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{7}$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.
0) $0^7 \equiv 0$. YES
1) $1^7 \equiv 1$. YES
2) $2^7 \equiv 2^3 \times 2^3 \times 2 \equiv 1 \times 1 \times 2 \equiv 2$. YES
3) $3^7 \equiv 3^3 \times 3^3 \times 3 \equiv -1 \times -1 \times 3 \equiv 3$. YES
4) $4^7 \equiv 4^3 \times 4^3 \times 4 \equiv 1 \times 1 \times 4 \equiv 4$. YES

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod 7]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod 7$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.
0) $0^7 \equiv 0$. YES
1) $1^7 \equiv 1$. YES
2) $2^7 \equiv 2^3 \times 2^3 \times 2 \equiv 1 \times 1 \times 2 \equiv 2$. YES
3) $3^7 \equiv 3^3 \times 3^3 \times 3 \equiv -1 \times -1 \times 3 \equiv 3$. YES
4) $4^7 \equiv 4^3 \times 4^3 \times 4 \equiv 1 \times 1 \times 4 \equiv 4$. YES
5) $5^7 \equiv 5^3 \times 5^3 \times 5 \equiv -1 \times -1 \times 5 \equiv 5$. YES

Using $\equiv$ in Easy Proofs

Theorem $(\forall a \in \mathbb{N})[a^7 \equiv a \pmod{7}]$.
Note The theorem is about ALL $a \in \mathbb{N}$.
Do we have to consider **all** $a \in \mathbb{N}$. That would be **insane!**
Only consider $a \equiv 0, 1, 2, 3, 4, 5, 6 \pmod{7}$. All $\equiv$ are mod 7.
We'll need: $2^3 \equiv 1$, $3^3 \equiv -1$, $4^3 \equiv 1$, $5^3 \equiv -1$, $6^3 \equiv 1$.
0) $0^7 \equiv 0$. YES
1) $1^7 \equiv 1$. YES
2) $2^7 \equiv 2^3 \times 2^3 \times 2 \equiv 1 \times 1 \times 2 \equiv 2$. YES
3) $3^7 \equiv 3^3 \times 3^3 \times 3 \equiv -1 \times -1 \times 3 \equiv 3$. YES
4) $4^7 \equiv 4^3 \times 4^3 \times 4 \equiv 1 \times 1 \times 4 \equiv 4$. YES
5) $5^7 \equiv 5^3 \times 5^3 \times 5 \equiv -1 \times -1 \times 5 \equiv 5$. YES
6) $6^7 \equiv 6^3 \times 6^3 \times 6 \equiv 1 \times 1 \times 6 \equiv 6$. YES

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2\log n$ steps.

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2\log n$ steps.
$3^{100} \pmod{13}$.

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2 \log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2\log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2 \log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2 \log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring
$3^{2^0} \equiv 3$

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2\log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring
$3^{2^0} \equiv 3$
$3^{2^1} \equiv 9$

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2 \log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring
$3^{2^0} \equiv 3$
$3^{2^1} \equiv 9$
$3^{2^2} \equiv (3^{2^1})^2 \equiv 9^2 \equiv 81 \equiv 3$.

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2\log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring
$3^{2^0} \equiv 3$
$3^{2^1} \equiv 9$
$3^{2^2} \equiv (3^{2^1})^2 \equiv 9^2 \equiv 81 \equiv 3$.
$3^{2^4} \equiv (3^{2^2})^2 \equiv 3^2 \equiv 9$.

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2\log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring
$3^{2^0} \equiv 3$
$3^{2^1} \equiv 9$
$3^{2^2} \equiv (3^{2^1})^2 \equiv 9^2 \equiv 81 \equiv 3$.
$3^{2^4} \equiv (3^{2^2})^2 \equiv 3^2 \equiv 9$.
$3^{2^5} \equiv (3^{2^3})^2 \equiv 9^2 \equiv 81 \equiv 3$.

Powering Fast

Can compute $a^n \pmod{m}$ in $\leq 2\log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring
$3^{2^0} \equiv 3$
$3^{2^1} \equiv 9$
$3^{2^2} \equiv (3^{2^1})^2 \equiv 9^2 \equiv 81 \equiv 3$.
$3^{2^4} \equiv (3^{2^2})^2 \equiv 3^2 \equiv 9$.
$3^{2^5} \equiv (3^{2^3})^2 \equiv 9^2 \equiv 81 \equiv 3$.
$3^{2^6} \equiv (3^{2^5})^2 \equiv 3^2 \equiv 9$.

Powering Fast

Can compute $a^n \pmod{m}$ in $\le 2\log n$ steps.
$3^{100} \pmod{13}$. DO WITH YOUR NEIGHBOR.
Step One $100 = 2^6 + 2^5 + 2^2$. So $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2}$.
Step Two Repeated Squaring
$3^{2^0} \equiv 3$
$3^{2^1} \equiv 9$
$3^{2^2} \equiv (3^{2^1})^2 \equiv 9^2 \equiv 81 \equiv 3.$
$3^{2^4} \equiv (3^{2^2})^2 \equiv 3^2 \equiv 9.$
$3^{2^5} \equiv (3^{2^3})^2 \equiv 9^2 \equiv 81 \equiv 3.$
$3^{2^6} \equiv (3^{2^5})^2 \equiv 3^2 \equiv 9.$
Step Three $3^{100} = 3^{2^6} \times 3^{2^5} \times 3^{2^2} \equiv 9 \times 3 \times 3 \equiv 27 \times 3 \equiv 3.$

Greatest Common Divisor (GCD)

Definition The **Greatest Common Divisor** of x, y is the largest number that divides both x and y. We denote this $\mathrm{GCD}(x, y)$.

Greatest Common Divisor (GCD)

Definition The **Greatest Common Divisor** of x, y is the largest number that divides both x and y. We denote this $\mathrm{GCD}(x, y)$.

Do Examples with the class.

Computing GCD

Assume $x < y$. Then

Computing GCD

Assume $x < y$. Then

$$\mathrm{GCD}(x, y) = \mathrm{GCD}(x, y - x)$$

Computing GCD

Assume $x < y$. Then

$$\mathrm{GCD}(x, y) = \mathrm{GCD}(x, y - x)$$

Better Remove the largest multiple of x that is $\leq y$.

Computing GCD

Assume $x < y$. Then

$$\mathrm{GCD}(x, y) = \mathrm{GCD}(x, y - x)$$

Better Remove the largest multiple of x that is $\leq y$.
Have class do an example.

Proof by Example

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Theorem $(\exists x)[\neg(\exists a, b, c)[x = a^2 + b^2 + c^2]]$

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Theorem $(\exists x)[\neg(\exists a, b, c)[x = a^2 + b^2 + c^2]]$
To prove a $\exists x$ give x and prove the thm for x.

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Theorem $(\exists x)[\neg(\exists a, b, c)[x = a^2 + b^2 + c^2]]$
To prove a $\exists x$ give x and prove the thm for x.
$x = 7$. We show 7 is not the sum of 3 squares. Cases.

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Theorem $(\exists x)[\neg(\exists a, b, c)[x = a^2 + b^2 + c^2]]$
To prove a $\exists x$ give x and prove the thm for x.
$x = 7$. We show 7 is not the sum of 3 squares. Cases.
Case 1 At least one of a, b, c is ≥ 3. Then $a^2 + b^2 + c^2 \geq 9 > 7$.

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Theorem $(\exists x)[\neg(\exists a, b, c)[x = a^2 + b^2 + c^2]]$
To prove a $\exists x$ give x and prove the thm for x.
$x = 7$. We show 7 is not the sum of 3 squares. Cases.
Case 1 At least one of a, b, c is ≥ 3. Then $a^2 + b^2 + c^2 \geq 9 > 7$.
Case 2 At least two of a, b, c are ≥ 2. Then $a^2 + b^2 + c^2 \geq 8 > 7$.

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Theorem $(\exists x)[\neg(\exists a, b, c)[x = a^2 + b^2 + c^2]]$
To prove a $\exists x$ give x and prove the thm for x.
$x = 7$. We show 7 is not the sum of 3 squares. Cases.
Case 1 At least one of a, b, c is ≥ 3. Then $a^2 + b^2 + c^2 \geq 9 > 7$.
Case 2 At least two of a, b, c are ≥ 2. Then $a^2 + b^2 + c^2 \geq 8 > 7$.
Case 3 The only case left: at most 1 of a, b, c is 2. Then
$a^2 + b^2 + c^2 \leq 4 + 1 + 1 = 6 < 7$.

Proving a $\exists x$ Theorem over $\mathbb{Z}$

Theorem $(\exists x)[\neg(\exists a, b, c)[x = a^2 + b^2 + c^2]]$
To prove a $\exists x$ give x and prove the thm for x.
$x = 7$. We show 7 is not the sum of 3 squares. Cases.
Case 1 At least one of a, b, c is ≥ 3. Then $a^2 + b^2 + c^2 \geq 9 > 7$.
Case 2 At least two of a, b, c are ≥ 2. Then $a^2 + b^2 + c^2 \geq 8 > 7$.
Case 3 The only case left: at most 1 of a, b, c is 2. Then
$a^2 + b^2 + c^2 \leq 4 + 1 + 1 = 6 < 7$.
Upshot For $\exists x$ Theorems SHOW THE x. (Nonconstructive proofs are possible though rare for this course.)

Irrationals

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.

Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases
$n \equiv 1 \rightarrow n^3 \equiv 1 \neq 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases
$n \equiv 1 \rightarrow n^3 \equiv 1 \neq 0$.
$n \equiv 2 \rightarrow n^3 \equiv 8 \equiv 1 \neq 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases
$n \equiv 1 \rightarrow n^3 \equiv 1 \neq 0$.
$n \equiv 2 \rightarrow n^3 \equiv 8 \equiv 1 \neq 0$.
$n \equiv 3 \rightarrow n^3 \equiv 27 \equiv 6 \neq 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases
$n \equiv 1 \rightarrow n^3 \equiv 1 \neq 0$.
$n \equiv 2 \rightarrow n^3 \equiv 8 \equiv 1 \neq 0$.
$n \equiv 3 \rightarrow n^3 \equiv 27 \equiv 6 \neq 0$.
$n \equiv 4 \rightarrow n^3 \equiv (-3)^3 \equiv -3^3 \equiv -6 \equiv 1 \not\equiv 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases
$n \equiv 1 \rightarrow n^3 \equiv 1 \neq 0$.
$n \equiv 2 \rightarrow n^3 \equiv 8 \equiv 1 \neq 0$.
$n \equiv 3 \rightarrow n^3 \equiv 27 \equiv 6 \neq 0$.
$n \equiv 4 \rightarrow n^3 \equiv (-3)^3 \equiv -3^3 \equiv -6 \equiv 1 \neq 0$.
$n \equiv 5 \rightarrow n^3 \equiv (-2)^3 \equiv -2^3 \equiv -1 \equiv 6 \neq 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases
$n \equiv 1 \rightarrow n^3 \equiv 1 \neq 0$.
$n \equiv 2 \rightarrow n^3 \equiv 8 \equiv 1 \neq 0$.
$n \equiv 3 \rightarrow n^3 \equiv 27 \equiv 6 \neq 0$.
$n \equiv 4 \rightarrow n^3 \equiv (-3)^3 \equiv -3^3 \equiv -6 \equiv 1 \not\equiv 0$.
$n \equiv 5 \rightarrow n^3 \equiv (-2)^3 \equiv -2^3 \equiv -1 \equiv 6 \not\equiv 0$.
$n \equiv 6 \rightarrow n^3 \equiv (-1)^3 \equiv -1 \equiv 6 \not\equiv 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods

Want $7^{1/3} \notin \mathbb{Q}$. We need the Lemma. All $\equiv$ is mod 7.
Lemma $(\forall n)[n^3 \equiv 0 \pmod 7 \rightarrow n \equiv 0 \pmod 7]$.
Take Contrapositive:
$(\forall n)[n \not\equiv 0 \pmod 7 \rightarrow n^3 \not\equiv 0 \pmod 7]$. 7 cases
$n \equiv 1 \rightarrow n^3 \equiv 1 \neq 0$.
$n \equiv 2 \rightarrow n^3 \equiv 8 \equiv 1 \neq 0$.
$n \equiv 3 \rightarrow n^3 \equiv 27 \equiv 6 \neq 0$.
$n \equiv 4 \rightarrow n^3 \equiv (-3)^3 \equiv -3^3 \equiv -6 \equiv 1 \not\equiv 0$.
$n \equiv 5 \rightarrow n^3 \equiv (-2)^3 \equiv -2^3 \equiv -1 \equiv 6 \not\equiv 0$.
$n \equiv 6 \rightarrow n^3 \equiv (-1)^3 \equiv -1 \equiv 6 \not\equiv 0$.
Proof of Lemma is done. Next slide is proof of irrationality.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$. By Lemma $a \equiv 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$. By Lemma $a \equiv 0$. $a = 7c$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$. By Lemma $a \equiv 0$. $a = 7c$.
$7b^3 = a^3 = (7c)^3 = 7^3c^3$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$. By Lemma $a \equiv 0$. $a = 7c$.
$7b^3 = a^3 = (7c)^3 = 7^3c^3$.
$b^3 = 7^2c^3$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$. By Lemma $a \equiv 0$. $a = 7c$.
$7b^3 = a^3 = (7c)^3 = 7^3c^3$.
$b^3 = 7^2c^3$. By Lemma $b \equiv 0$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$. By Lemma $a \equiv 0$. $a = 7c$.
$7b^3 = a^3 = (7c)^3 = 7^3c^3$.
$b^3 = 7^2c^3$. By Lemma $b \equiv 0$.
AH-HA! 7 divides both a and b. So a, b not in lowest terms.

Proving $7^{1/3} \notin \mathbb{Q}$ Using Mods (cont)

Want $7^{1/3} \notin \mathbb{Q}$. Assume BWOC that $7^{1/3} \in \mathbb{Q}$.
So there exists a, b **in lowest terms** such that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
$a^3 \equiv 0$. By Lemma $a \equiv 0$. $a = 7c$.
$7b^3 = a^3 = (7c)^3 = 7^3c^3$.
$b^3 = 7^2c^3$. By Lemma $b \equiv 0$.
AH-HA! 7 divides both a and b. So a, b not in lowest terms.
Contradiction!

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x - 1$ cases.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x - 1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x-1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x - 1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x - 1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x-1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x - 1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$. $a = xc$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x - 1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$. $a = xc$.
$b^z x = a^z = (xc)^z = x^z c^z$

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x-1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$. $a = xc$.
$b^z x = a^z = (xc)^z = x^z c^z$
$b^z = x^{z-1} c^z$

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x-1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$. $a = xc$.
$b^z x = a^z = (xc)^z = x^z c^z$
$b^z = x^{z-1} c^z$
$b \equiv 0 \pmod{x}$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x-1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$. $a = xc$.
$b^z x = a^z = (xc)^z = x^z c^z$
$b^z = x^{z-1} c^z$
$b \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x-1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$. $a = xc$.
$b^z x = a^z = (xc)^z = x^z c^z$
$b^z = x^{z-1} c^z$
$b \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$.
AH-HA! x divides both a and b. So a, b not in lowest terms.

Irrationality Using Mods-Generalized

The above proof is a template for these kinds of proofs.
To show $x^{1/z} \notin \mathbb{Q}$.
Step 1 Prove $(\forall n)[n^z \equiv 0 \pmod{x} \rightarrow n \equiv 0 \pmod{x}]$.
Take Contrapositive $(\forall n)[n \not\equiv 0 \pmod{x} \rightarrow n^z \not\equiv 0 \pmod{x}]$.
Prove by $x-1$ cases.

Step 2 Assume, BWOC, that $x^{1/z} = \frac{a}{b}$: a, b in lowest terms.
$bx^{1/z} = a$
$b^z x = a^z$
$a \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$. $a = xc$.
$b^z x = a^z = (xc)^z = x^z c^z$
$b^z = x^{z-1} c^z$
$b \equiv 0 \pmod{x}$. By Lemma $a \equiv 0 \pmod{x}$.
AH-HA! x divides both a and b. So a, b not in lowest terms.
Contradiction!

The Hard Part is The Lemma

For proofs of irrationality using mods:

The Hard Part is The Lemma

For proofs of irrationality using mods:

1. The lemma is the only part that is not a template.

The Hard Part is The Lemma

For proofs of irrationality using mods:

1. The lemma is the only part that is not a template.
2. The lemma may have a lot of cases.

The Hard Part is The Lemma

For proofs of irrationality using mods:

1. The lemma is the only part that is not a template.
2. The lemma may have a lot of cases.
3. If you are trying to prove a rational is irrational, the proof will fall apart in the lemma.

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
Factor both sides. $p_1, \ldots, p_L$ is the set of primes that divide a or b.

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
Factor both sides. $p_1, \ldots, p_L$ is the set of primes that divide a or b.
$b = p_1^{b_1} \cdots p_L^{b_L}$

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
Factor both sides. $p_1, \ldots, p_L$ is the set of primes that divide a or b.
$b = p_1^{b_1} \cdots p_L^{b_L}$
$a = p_1^{a_1} \cdots p_L^{a_L}$

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that

$7^{1/3} = \frac{a}{b}$

$b7^{1/3} = a$

$7b^3 = a^3$

Factor both sides. $p_1, \ldots, p_L$ is the set of primes that divide a or b.

$b = p_1^{b_1} \cdots p_L^{b_L}$

$a = p_1^{a_1} \cdots p_L^{a_L}$

$7p_1^{3b_1} \cdots p_L^{3b_L} = p_1^{3a_1} \cdots p_L^{3a_L}$

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
Factor both sides. $p_1, \ldots, p_L$ is the set of primes that divide a or b.
$b = p_1^{b_1} \cdots p_L^{b_L}$
$a = p_1^{a_1} \cdots p_L^{a_L}$
$7p_1^{3b_1} \cdots p_L^{3b_L} = p_1^{3a_1} \cdots p_L^{3a_L}$
The number of 7's on the LHS is $\equiv 1 \pmod 3$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
Factor both sides. $p_1, \ldots, p_L$ is the set of primes that divide a or b.
$b = p_1^{b_1} \cdots p_L^{b_L}$
$a = p_1^{a_1} \cdots p_L^{a_L}$
$7p_1^{3b_1} \cdots p_L^{3b_L} = p_1^{3a_1} \cdots p_L^{3a_L}$
The number of 7's on the LHS is $\equiv 1 \pmod 3$.
The number of 7's on the RHS is $\equiv 0 \pmod 3$.

Proving $7^{1/3} \notin \mathbb{Q}$ Using UFT

Want $7^{1/3} \notin \mathbb{Q}$. Assume, BWOC that
$7^{1/3} = \frac{a}{b}$
$b7^{1/3} = a$
$7b^3 = a^3$
Factor both sides. $p_1, \ldots, p_L$ is the set of primes that divide a or b.
$b = p_1^{b_1} \cdots p_L^{b_L}$
$a = p_1^{a_1} \cdots p_L^{a_L}$
$7p_1^{3b_1} \cdots p_L^{3b_L} = p_1^{3a_1} \cdots p_L^{3a_L}$
The number of 7's on the LHS is $\equiv 1 \pmod{3}$.
The number of 7's on the RHS is $\equiv 0 \pmod{3}$.
Contradiction.

Proving Irrationality Using UFT

These proofs also have a very definite template.

Proving Irrationality Using UFT

These proofs also have a very definite template.

On HW05 you will do this proof for $\sqrt{p}$.

Primes

Primes are Infinite

Theorem The number of primes is infinite.
Assume, BWOC, that the number of primes is finite.

Primes are Infinite

Theorem The number of primes is infinite.
Assume, BWOC, that the number of primes is finite.
Let $p_1, \ldots, p_L$ be ALL of the primes.

Primes are Infinite

Theorem The number of primes is infinite.
Assume, BWOC, that the number of primes is finite.
Let $p_1, \ldots, p_L$ be ALL of the primes.
Consider the number $N = p_1 \cdots p_L + 1$.

Primes are Infinite

Theorem The number of primes is infinite.
Assume, BWOC, that the number of primes is finite.
Let $p_1, \ldots, p_L$ be ALL of the primes.
Consider the number $N = p_1 \cdots p_L + 1$.
Case 1 N is prime. Then since $(\forall i)[p_i < N]$ N is a prime NOT on the list of ALL primes. Contradiction.

Primes are Infinite

Theorem The number of primes is infinite.
Assume, BWOC, that the number of primes is finite.
Let $p_1, \ldots, p_L$ be ALL of the primes.
Consider the number $N = p_1 \cdots p_L + 1$.
Case 1 N is prime. Then since $(\forall i)[p_i < N]$ N is a prime NOT on the list of ALL primes. Contradiction.
Case 2 N is not prime. Let p be a prime factor of N.

Primes are Infinite

Theorem The number of primes is infinite.
Assume, BWOC, that the number of primes is finite.
Let $p_1, \ldots, p_L$ be ALL of the primes.
Consider the number $N = p_1 \cdots p_L + 1$.
Case 1 N is prime. Then since $(\forall i)[p_i < N]$ N is a prime NOT on the list of ALL primes. Contradiction.
Case 2 N is not prime. Let p be a prime factor of N.
p cannot be any of the p_i since none of them divide N.

Primes are Infinite

Theorem The number of primes is infinite.
Assume, BWOC, that the number of primes is finite.
Let $p_1, \ldots, p_L$ be ALL of the primes.
Consider the number $N = p_1 \cdots p_L + 1$.
Case 1 N is prime. Then since $(\forall i)[p_i < N]$ N is a prime NOT on the list of ALL primes. Contradiction.
Case 2 N is not prime. Let p be a prime factor of N.
p cannot be any of the p_i since none of them divide N.
p is a prime NOT on the list of ALL primes. Contradiction.