Introduction to Proofs - Number Theory
Fundamental Theorem of Arithmetic

Prof Mike Pawliuk

UTM

August 13, 2020

Slides available at: mikepawliuk.ca

Learning Objectives (for this video)

By the end of this video, participants should be able to:

1. Adapt the proof that $\sqrt{2}$ is irrational to prove related statements.
2. State the fundamental theorem of arithmetic.
3. Adapt the proof that $\log_{48}(72)$ is irrational to prove related statements.

Motivation

Motivation

"Primes are the building blocks of the integers", or "Primes are the atoms of the integers".

We will know be able to formally prove that $\sqrt{2}$ and $\log_2(3)$ are irrational.

1. Euclid's Lemma

Theorem (Euclid's Lemma)

Let a, b be natural numbers and let p be a prime. If $p|ab$, then $p|a$ or $p|b$.

1. Euclid's Lemma

Theorem (Euclid's Lemma)

Let a, b be natural numbers and let p be a prime. If $p|ab$, then $p|a$ or $p|b$.

Warning

Euclid's lemma is only true if p is prime.

Example. Let $c = 6, a = 4, b = 9$. Note $c \mid ab$ but $c \nmid a$ and $c \nmid b$.

1. Euclid's Lemma

Theorem (Euclid's Lemma)

Let a, b be natural numbers and let p be a prime. If $p|ab$, then $p|a$ or $p|b$.

Warning

Euclid's lemma is only true if p is prime.

Example. Let $c = 6, a = 4, b = 9$. Note $c \mid ab$ but $c \not| a$ and $c \not| b$.

Corollary

Let p be a prime. If p divides a product of integers, then p must divide one of those integers.

1. Euclid's Lemma

Theorem (Euclid's Lemma)

Let a, b be natural numbers and let p be a prime. If $p|ab$, then $p|a$ or $p|b$.

Warning

Euclid's lemma is only true if p is prime.

Example. Let $c = 6, a = 4, b = 9$. Note $c \mid ab$ but $c \not| a$ and $c \not| b$.

Corollary

Let p be a prime. If p divides a product of integers, then p must divide one of those integers.

Proof is by induction and Euclid's Lemma.

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational.

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$.

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.
Note $2n^2 = m^2$.

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.
Note $2n^2 = m^2$.
So $2|m^2$. So $2|m$ by

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.
Note $2n^2 = m^2$.
So $2|m^2$. So $2|m$ by Euclid's Lemma.

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.
Note $2n^2 = m^2$.
So $2|m^2$. So $2|m$ by Euclid's Lemma. Let $k \in \mathbb{Z}$ be such that $m = 2k$.
Thus $m^2 = (2k)^2 = 4k^2$.

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.
Note $2n^2 = m^2$.
So $2|m^2$. So $2|m$ by Euclid's Lemma. Let $k \in \mathbb{Z}$ be such that $m = 2k$.
Thus $m^2 = (2k)^2 = 4k^2$.
So $2n^2 = 4k^2$. i.e. $n^2 = 2k^2$.

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.
Note $2n^2 = m^2$.
So $2|m^2$. So $2|m$ by Euclid's Lemma. Let $k \in \mathbb{Z}$ be such that $m = 2k$.
Thus $m^2 = (2k)^2 = 4k^2$.
So $2n^2 = 4k^2$. i.e. $n^2 = 2k^2$.
So $2|n$. (A contradiction.)

2. Applications of Euclid's Lemma to irrationality

$\sqrt{2}$ is irrational

Suppose for the sake of contradiction that it is rational. So there are $m \in \mathbb{Z}, n \in \mathbb{N}$ with $\sqrt{2} = \frac{m}{n}$. Assume that all common positive factors of m, n have been cancelled.
Note $2n^2 = m^2$.
So $2|m^2$. So $2|m$ by Euclid's Lemma. Let $k \in \mathbb{Z}$ be such that $m = 2k$.
Thus $m^2 = (2k)^2 = 4k^2$.
So $2n^2 = 4k^2$. i.e. $n^2 = 2k^2$.
So $2|n$. (A contradiction.)

Exercises Adapt this proof to show that

1. $\sqrt{p}$ is irrational (where p is a prime).
2. $\sqrt{pq}$ is irrational (if p, q are different primes).
3. $\sqrt{n}$ is irrational when n is not a square.
4. Similar statements about cube roots.

3. Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every natural number $n \geq 2$ is either a prime, or can be expressed as a product of powers of distinct primes, in a unique way (except for re-ordering of the factors).

Note. $3^7 2^5 = 2^5 3^7$ are not considered “different enough” representations.

3. Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic)

Every natural number $n \geq 2$ is either a prime, or can be expressed as a product of powers of distinct primes, in a unique way (except for re-ordering of the factors).

Note. $3^7 2^5 = 2^5 3^7$ are not considered "different enough" representations.

Proof.

We already proved existence in the section on Strong induction. We skip the proof of uniqueness. □

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not.

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$,

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$, as $\log_{48}(72) > 0$.

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$, as $\log_{48}(72) > 0$. Thus $48^{m/n} = 72$.

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$, as $\log_{48}(72) > 0$. Thus $48^{m/n} = 72$.

$$48^{m/n} = 72$$
$$\implies 48^m = 72^n \qquad \text{and } 48 = 2^4 \cdot 3, 72 = 2^3 \cdot 3^3$$

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$, as $\log_{48}(72) > 0$. Thus $48^{m/n} = 72$.

$$\begin{aligned} & 48^{m/n} = 72 \\ \implies & 48^m = 72^n \qquad \text{and } 48 = 2^4 \cdot 3, 72 = 2^3 \cdot 3^3 \\ \implies & 2^{4m} 3^m = 2^{3n} 3^{3n} \end{aligned}$$

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$, as $\log_{48}(72) > 0$. Thus $48^{m/n} = 72$.

$$\begin{aligned} & 48^{m/n} = 72 \\ \implies & 48^m = 72^n \qquad \text{and } 48 = 2^4 \cdot 3, 72 = 2^3 \cdot 3^3 \\ \implies & 2^{4m}3^m = 2^{3n}3^{3n} \\ \implies & 4m = 3n \text{ and } m = 3n \end{aligned}$$

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$, as $\log_{48}(72) > 0$.
Thus $48^{m/n} = 72$.

$$\begin{aligned} & 48^{m/n} = 72 \\ \implies & 48^m = 72^n \qquad \text{and } 48 = 2^4 \cdot 3, 72 = 2^3 \cdot 3^3 \\ \implies & 2^{4m}3^m = 2^{3n}3^{3n} \\ \implies & 4m = 3n \text{ and } m = 3n \\ \implies & 4m = m \end{aligned}$$

4. Application of FTA to irrationality

Definition (log)

Let $a, n > 0$ be real numbers. Then $\log_a(n) = b$ if and only if $a^b = n$

$\log_{48}(72)$ is irrational

Assume not. Say $\log_{48}(72) = \frac{m}{n}$ for particular $m, n \in \mathbb{N}$, as $\log_{48}(72) > 0$. Thus $48^{m/n} = 72$.

$$
\begin{aligned}
& 48^{m/n} = 72 \\
\implies & 48^m = 72^n \qquad \text{and } 48 = 2^4 \cdot 3, 72 = 2^3 \cdot 3^3 \\
\implies & 2^{4m}3^m = 2^{3n}3^{3n} \\
\implies & 4m = 3n \text{ and } m = 3n \\
\implies & 4m = m
\end{aligned}
$$

Which is a contradiction. (Why?)

Reflection

- Can the $\log_{48}(72)$ argument be adapted to show that other things are irrational?
- Can the "$\sqrt{2}$ is irrational" proof be done without using Euclid's Lemma?
- In what ways does the FTA tell us that the primes are the building blocks of the integers?
- In what ways does Euclid's Lemma tell us that the primes are the atoms of the integers?