Number Theory. Class 3

Victor H. Moll
Tulane University

January 22, 2008

Unique factorization

Theorem

Every $n \in \mathbb{N}$ has a unique factorization in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

We may always assume: $p_1 < p_2 < \cdots < p_r$.

Meaning of uniqueness: if

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

then $r = s$ and

$$p_i = q_i \text{ for } 1 \leq i \leq r \text{ and } a_i = b_i \text{ for } 1 \leq i \leq r.$$

Unique factorization

Theorem

Every $n \in \mathbb{N}$ has a unique factorization in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

We may always assume: $p_1 < p_2 < \cdots < p_r$.

Meaning of uniqueness: if

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

then $r = s$ and

$$p_i = q_i \text{ for } 1 \leq i \leq r \text{ and } a_i = b_i \text{ for } 1 \leq i \leq r.$$

Unique factorization

Theorem

Every $n \in \mathbb{N}$ has a unique factorization in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

We may always assume: $p_1 < p_2 < \cdots < p_r$.

Meaning of uniqueness: if

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

then $r = s$ and

$$p_i = q_i \text{ for } 1 \le i \le r \text{ and } a_i = b_i \text{ for } 1 \le i \le r.$$

Unique factorization

Theorem

Every $n \in \mathbb{N}$ has a unique factorization in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

We may always assume: $p_1 < p_2 < \cdots < p_r$.

Meaning of uniqueness: if

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

then $r = s$ and

$$p_i = q_i \text{ for } 1 \leq i \leq r \text{ and } a_i = b_i \text{ for } 1 \leq i \leq r.$$

Unique factorization

Theorem

Every $n \in \mathbb{N}$ has a unique factorization in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

We may always assume: $p_1 < p_2 < \cdots < p_r$.

Meaning of uniqueness: if

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

then $r = s$ and

$$p_i = q_i \text{ for } 1 \leq i \leq r \text{ and } a_i = b_i \text{ for } 1 \leq i \leq r.$$

Unique factorization

Theorem

Every $n \in \mathbb{N}$ has a unique factorization in the form

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

We may always assume: $p_1 < p_2 < \cdots < p_r$.

Meaning of uniqueness: if

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

then $r = s$ and

$p_i = q_i$ for $1 \leq i \leq r$ and $a_i = b_i$ for $1 \leq i \leq r$.

Unique factorization

Theorem

Every $n \in \mathbb{N}$ *has a unique factorization in the form*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

We may always assume: $p_1 < p_2 < \cdots < p_r$.

Meaning of uniqueness: if

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

then $r = s$ and

$$p_i = q_i \text{ for } 1 \leq i \leq r \text{ and } a_i = b_i \text{ for } 1 \leq i \leq r.$$

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.

In particular, $p_1, p_2, \cdots, p_r$ *are the only primes that divide n.*

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \le b_i \le a_i$.
In particular, $p_1, p_2, \cdots, p_r$ are the only primes that divide n.

Proof.
Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.
In particular, $p_1, p_2, \cdots, p_r$ are the only primes that divide n.

Proof.
Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.

In particular, $p_1, p_2, \cdots, p_r$ *are the only primes that divide* n.

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.

In particular, $p_1, p_2, \cdots, p_r$ *are the only primes that divide n.*

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.
In particular, $p_1, p_2, \cdots, p_r$ are the only primes that divide n.

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_j. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.

In particular, $p_1, p_2, \cdots, p_r$ *are the only primes that divide n.*

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.
In particular, p_1, $p_2, \cdots, p_r$ are the only primes that divide n.

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.
In particular, $p_1, p_2, \cdots, p_r$ *are the only primes that divide n.*

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$*.*
In particular, $p_1, p_2, \cdots, p_r$ *are the only primes that divide n.*

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done.

Determination of factors

Theorem

Given

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

then m divides n if and only if

$$m = p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}$$

with $0 \leq b_i \leq a_i$.

In particular, $p_1, p_2, \cdots, p_r$ *are the only primes that divide n.*

Proof.

Assume m divides n and write $n = m \times m_1$.

Suppose $m = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r}$, then

$$p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = q_1^{c_1} q_2^{c_2} \cdots q_s^{c_r} \times m_1.$$

We conclude that every q_i must equal one of the p_i. Done. □

Irrationality proof

Theorem
$\sqrt{2} \notin \mathbb{Q}$

Proof.
Assume $\sqrt{2} = m/n$

$$m^2 = 2n^2$$

$\square$

Irrationality proof

Theorem
$\sqrt{2} \notin \mathbb{Q}$

Proof.
Assume $\sqrt{2} = m/n$

$$m^2 = 2n^2$$

□

Irrationality proof

Theorem

$\sqrt{2} \notin \mathbb{Q}$

Proof.

Assume $\sqrt{2} = m/n$

$$m^2 = 2n^2$$

□

Irrationality proof

Theorem

$\sqrt{2} \notin \mathbb{Q}$

Proof.

Assume $\sqrt{2} = m/n$

$$m^2 = 2n^2$$

□

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2 q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1 - 1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction. □

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2 q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1 - 1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction. □

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2 q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1 - 1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction.

□

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2 q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1 - 1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction.

□

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1-1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction.

□

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2 q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1-1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction.

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1-1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction.

Irrationality proof. Continuation

Proof.

Introduce the prime factorization

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \text{ and } n = q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s}$$

with $p_i \neq q_j$ and the primes are ordered.

$$p_1^{2a_1} p_2^{2a_2} \cdots p_r^{2a_r} = 2 q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $p_1 = 2$

$$2^{2a_1 - 1} p_2^{2a_2} \cdots p_r^{2a_r} = q_1^{2b_1} q_2^{2b_2} \cdots q_s^{2b_s}$$

Therefore $q_1 = 2$. Contradiction.

□

Valuation of n!

Theorem

Let $n \in \mathbb{N}$. Then

$$\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$$

and also

$$\nu_p(n!) = \frac{n - S_p(n)}{p - 1}$$

where $S_p(n)$ is the sum of the digits of n written in base p.

Valuation of n!

Theorem

Let $n \in \mathbb{N}$. Then

$$\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$$

and also

$$\nu_p(n!) = \frac{n - S_p(n)}{p - 1}$$

where $S_p(n)$ is the sum of the digits of n written in base p.

Valuation of $n!$

Theorem

Let $n \in \mathbb{N}$. Then

$$\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$$

and also

$$\nu_p(n!) = \frac{n - S_p(n)}{p - 1}$$

where $S_p(n)$ is the sum of the digits of n written in base p.

Valuation of $n!$

Theorem

Let $n \in \mathbb{N}$. Then

$$\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$$

and also

$$\nu_p(n!) = \frac{n - S_p(n)}{p - 1}$$

where $S_p(n)$ is the sum of the digits of n written in base p.

Valuation of $n!$

Theorem

Let $n \in \mathbb{N}$. Then

$$\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$$

and also

$$\nu_p(n!) = \frac{n - S_p(n)}{p - 1}$$

where $S_p(n)$ is the sum of the digits of n written in base p.

Valuation of $n!$

Theorem

Let $n \in \mathbb{N}$. Then

$$\nu_p(n!) = \sum_{k=1}^{\infty} \lfloor \frac{n}{p^k} \rfloor$$

and also

$$\nu_p(n!) = \frac{n - S_p(n)}{p - 1}$$

where $S_p(n)$ is the sum of the digits of n written in base p.