**Prop ①** If $p \mid q_1 \cdots q_n$ and $p, q_1, \ldots, q_n$ are all primes, then $p = q_i$ for some $i$. ①

**Pf** We argue by induction on $n$.

**Base case** $(n=1)$: Given $p \mid q_1$ where $p, q_1$ are both primes.

Now $q_1$ prime $\Rightarrow$ the only positive divisors of $q_1$ are $1$ and $q_1$

$p \mid q_1 \Rightarrow p = 1$ or $p = q_1$

But $p$ prime $\Rightarrow p \geq 2 \Rightarrow p \neq 1$.

Thus $\boxed{p = q_1}$, and the base case is established.

---

**Induction Step** (true for $n=k \longrightarrow$ true for $n=k+1$)

Assume that whenever $p \mid q_1 \cdots q_k$ $p, q_i$ all primes

then $p = q_i$ for some $i$.

Now given $p \mid q_1 \cdots q_{k+1}$. We can write

$q_1 \cdots q_{k+1} = (q_1 \cdots q_k)(q_{k+1})$ as a product

of two integers.

There are 2 cases to consider: $p \mid (q_1 \cdots q_k)$ and $p \nmid (q_1 \cdots q_k)$.

CASE $p \mid (q_1 \cdots q_k)$.

In this case the Induction hypothesis (case $n=k$) applies & we conclude $p = q_i$ for some $i$.

$\Rightarrow p = q_i$ for some $i$ in the range $1 \leq i \leq k+1$.

CASE $p \nmid (q_1 \cdots q_k)$.

In this case the proposition on page 9 of the Least Principle handout (with $(q_1 \cdots q_k) = b$ and $q_{k+1} = c$) implies that $p \mid q_{k+1}$.

But then $p = q_{k+1}$ (by the base case argument).

$\Rightarrow p = q_i$ for some $i$ in the range $1 \leq i \leq k+1$.

In each case, $p = q_i$ for some $1 \leq i \leq p+1$, & so the statement is true for $n = k+1$.

---

By the Principle of Induction, the statement is true for all $n \in \mathbb{N}$. $\boxtimes$

**Prop 2** If $p_1 \cdots p_n = q_1 \cdots q_m$

where
- $n \leq m$
- $p_i$ and $q_j$ are all primes,

<u>then</u>
- $m = n$ and
- $p_i = q_i$ for all $i$ (possibly after rearranging the $q$'s).

<u>Proof</u>: We argue by induction on $n$.

<u>Case</u>: ($n = 1$) Given $p_1 = q_1 \cdots q_m$ ($m \geq 1$)

$p_1, q_i$ all primes.

If $m \geq 2$, then we obtain more $\oplus$ divisors of $p_1$ than $1, p_1$. This contradicts the fact that $p_1$ is prime.

Thus $m = 1$ and $p_1 = q_1$. done!

---

<u>Induction Step</u> (true for $n=k$ $\longrightarrow$ true for $n=k+1$)

We assume that if

$$p_1 \cdots p_k = q_1 \cdots q_m \quad \text{---} (*)$$

with $m \geq k$, $p_i, q_j$ all primes, then

$m = k$ & $p_i = q_i$ for all $i$ (possibly after rearranging the $q$'s).

4

Given $p_1 \cdots p_{k+1} = q_1 \cdots q_m$ (**) where

$m \geq k+1$ and $p_i, q_j$ are all primes.

$p_{k+1} \mid LHS \Rightarrow p_{k+1} \mid RHS$

$\Rightarrow p_{k+1} \mid q_1 \cdots q_m$

Prop (1) above $\Rightarrow$ $p_{k+1} = q_j$ for some $j$

By rearranging the $q$'s (if necessary) we can assume

$$p_{k+1} = q_m \longrightarrow (A)$$

Now divide both sides of (**) by $p_{k+1}$ $(= q_m)$ to get

$$p_1 \cdots p_k = q_1 \cdots q_{m-1}$$

Since $m \geq k+1$, then $m-1 \geq k$ and the Induction hypothesis (*) applies to give

$$m-1 = k$$

and $p_i = q_i$ for $1 \leq i \leq k$ (possibly after rearranging the $q$'s)

(B)

Combing (A) & (B) we get - - -

$M = k+1$ and

$p_i = q_i \qquad 1 \le i \le k$ (possibly after rearranging the $q$'s)

$p_{k+1} = q_{k+1}$

i.e. $M = k+1$ and $p_i = q_i \quad 1 \le i \le k+1$

Thus the statement is true for $n = k+1$.

By the principle of Induction, the statement is true for all $n \in \mathbb{N}$.

$\boxed{}$

**Fundamental Th$^{\underline{m}}$ of Arithmetic** Every positive integer greater than 1 can be written uniquely as a product of primes, with the prime factors in the product written in non decreasing order.

---

**Existence** → we gave a proof of this using strong induction (see strong Induction examples online).

**Uniqueness** → This follows from Prop ② above.

If $p_1 \text{---} p_n = q_1 \text{---} q_m$ $(m \geq n)$

& the $p_i, q_i$ are primes written in non decreasing order

then $m = n$ & $p_i = q_i$ for each $i$.

by Prop ②.

---

"nondecreasing order" ensures that no rearranging of the $q$'s is necessary for $p_i = q_i$ for each $i$.

# Applications of Fund Th$^{\underline{m}}$

Application ① With ($\equiv$ mod $m$), we get efficient proofs of irrationality. Example...

Prop $\sqrt[36]{12}$ is irrational

Proof Argue by contradiction. Assume $\sqrt[36]{12} = p/q$ for some $p, q \in \mathbb{N}$.

Then $12 = \dfrac{p^{36}}{q^{36}}$

$$\Rightarrow \quad (3)(2)(2)\, q^{36} = p^{36} \qquad \text{———} (*)$$

Fund Th$^{\underline{m}}$ $\Rightarrow$ each of $p, q$ has unique decomposition into product of primes. This gives decomp of LHS & RHS of $(*)$ as a product of primes.

\# occurrences of 3 in LHS of $(*)$ $\equiv 1 \pmod{36}$

\# occurrences of 3 in RHS of $(*)$ $\equiv 0 \pmod{36}$

But this contradicts the uniqueness part of the Fund. Theorem for the integer $p^{36}$ $(= 12 q^{36})$.

Contradiction arose because we assumed $\sqrt[36]{12}$ ~~was~~ is rational.

$\Rightarrow \sqrt[36]{12}$ is irrational. $\boxed{/\!/}$

**Exercise** (1) Prove $\sqrt[5]{\frac{3}{4}}$ is irrational.

---

**Exercise** (2) Prove that if the positive integer $a$ is <u>not</u> the $m$-th power of another integer, then $\sqrt[m]{a}$ is irrational.

---

## Application (2) Determination of $\gcd(a,b)$, $\operatorname{lcm}(a,b)$.

**Step (1)** Write down unique prime factorizations for $a$ and for $b$. Let $p_1, \ldots, p_k$ be a list of the <u>distinct</u> primes arising in these factorizations.

So $a = p_1^{\alpha_1} \cdots\cdots p_k^{\alpha_k}$ $\quad \alpha_i \in \mathbb{Z}$, $\alpha_i \geq 0$

($\alpha_i = 0$ if $p_i$ did not appear in factorization of $a$)

$b = p_1^{\beta_1} \cdots\cdots p_k^{\beta_k}$ $\quad \beta_i \in \mathbb{Z}$, $\beta_i \geq 0$

($\beta_j = 0$ if $p_j$ did not occur in factorization of $b$).

**Step (2)**

$$\gcd(a,b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots\cdots p_k^{\min\{\alpha_k, \beta_k\}}$$

$$\operatorname{lcm}(a,b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdots\cdots p_k^{\max\{\alpha_k, \beta_k\}}.$$