

Corollary: Suppose $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$. If $k \in \mathbb{Z}$, $m \mid k$, $n \mid k$, then $(m \cdot n) \mid k$.

Proof:

By the previous corollary,

$\exists a, b \in \mathbb{Z}$ with

$$1 = \gcd(m, n) = am + bn.$$

Multiplying by k ,

$$k = k(am + bn) = kam + kbn.$$

But we know that $a \mid k$ and $b \mid k$, so \exists integers s and t with $k = as$, $k = bt$.

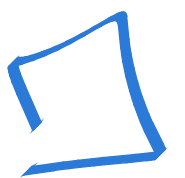
Substituting in our equality,

$$k = (bt)(am) + (as)(bn)$$

$$k = ab(tm) + ab(sn)$$

$$k = ab(tm + sn)$$

$$\Rightarrow ab \mid k$$



Proposition: Let p be prime and let
 $n \in \mathbb{Z}$, $n \neq 0$. Then either
 $p \mid n$ or $\gcd(p, n) = 1$.

proof: Suppose $\gcd(p, n) \neq 1$.

Then with $d = \gcd(p, n)$,

$d \mid p$ and $d \mid n$. But

$d \neq 1$ and p is prime, so

we must have $d = p$, and

consequently, $p \mid n$.



Proposition: Let p be prime. Let
 $m, n \in \mathbb{Z}$, $m \neq 0 \neq n$. If
 $p \mid (m \cdot n)$, then $p \mid m$ or
 $p \mid n$.

proof: Suppose $p \nmid m$. Then by
the previous proposition, p and
 n are relatively prime, so

$\exists a, b \in \mathbb{Z}$ with

$$1 = pa + nb.$$

Multiplying by n ,

$$n = npa + nnb.$$

But by assumption, $p \mid nm$,

so $\exists k \in \mathbb{Z}$, $nm = pk$.

Then

$$n = npa + pkb$$

$$n = p(na + kb)$$

$$\Rightarrow p \mid n.$$



Theorem: (other half of the Fundamental Theorem of Arithmetic)

Up to reordering of the product, the prime factorization of a natural number is unique

proof: Let $n \in \mathbb{N}$, $n \geq 2$.

Suppose \exists primes p_1, p_2, \dots, p_m

and q_1, q_2, \dots, q_k with

$p_1 \leq p_2 \leq p_3 \leq \dots \leq p_m$ and

$q_1 \leq q_2 \leq q_3 \leq \dots \leq q_k$

with

$$n = p_1 p_2 \cdots p_m$$

$$n = q_1 q_2 \cdots q_k$$

The proof proceeds by induction.

For $n=2$, 2 is prime.

Fix $n \in \mathbb{N}$, $n > 2$, and

suppose the statement of the theorem holds $\forall a \in \mathbb{N}$,

$$2 \leq a < n.$$

Either $p_1 \geq q_1$ or $q_1 \geq p_1$.

Without loss of generality, assume

$$p_1 \geq q_1.$$

Dividing out by q_1 , we
have

$$\frac{n}{q_1} = q_2 q_3 \cdots q_k \in \mathbb{N}$$

Since q_1 is prime and $q_1 | n$,

if $n = p_1 p_2 \cdots p_m$, we know

that q_1 divides p_t for some

$1 \leq t \leq m$ by the previous proposition

and your HW 3 question.

But p_1, p_2, \dots, p_m are all

prime and p_1 is the smallest,

with $q_1 \leq p_1$, so

$$q_1 \mid p_1 \Rightarrow q_1 = p_1$$

Then

$$\frac{n}{q_1} = \frac{n}{p_1} = p_2 p_3 \dots p_m \in \mathbb{N}$$

$$\frac{n}{q_1} = q_2 q_3 \dots q_k$$

Since q_1 is prime,

$$1 \leq \frac{n}{q_1} < n$$

If $\frac{n}{q_1} = 1$, then n is prime.

If $\frac{n}{q_1} > 1$, then by induction,

the factorization of $\frac{n}{q_1}$ is unique.

Therefore, the factorization of n is unique, up to reordering,



Fundamental Theorem of Arithmetic,

Full Statement:

Let $n \in \mathbb{N}$, $n \geq 2$. Then n is either prime or may be expressed uniquely (up to reordering) as a product of primes.