

Announcements

1) HW 6 due Thursday

Question #5 - for all ODD n

2) Office hours slightly changed today
to 4-5

The GCD

(Section 8.1)

Definition: Let $m, n \in \mathbb{N}$. The greatest common divisor of m and n , denoted $\gcd(m, n)$ or (m, n) , is the largest $k \in \mathbb{N}$ such that

$$k \mid m \text{ and } k \mid n$$

Q: How to find the GCD?

A: The Euclidean Algorithm!

Example 1: Find $\gcd(10446, 210, 742)$

1) Divide smaller number into bigger number

$$210, 742 = 20 \cdot (10446) + 1822$$

2) Repeat procedure, with smaller number and remainder

$$10446 = 5 \cdot 1822 + 1336$$

keep on going until there is no remainder

$$1822 = 1336 + 486$$

$$1336 = 2 \cdot 486 + 364$$

$$486 = 364 + 122$$

$$364 = 2 \cdot 122 + 120$$

$$122 = 120 + 2$$

GCD

$$\leftarrow \frac{122}{120} = \textcircled{2} \cdot 60$$

Stop.

Prime Factorization

(Section 8.2)

Definition: (relatively prime)

If $m, n \in \mathbb{N}$, we say m and n
are relatively prime if

$$\gcd(m, n) = 1$$

Example 2: 28 and 15 are

relatively prime.

Run Euclidean algorithm:

$$28 = 15 + 13$$

$$15 = 13 + 2$$

$$13 = 6 \cdot 2 + 1$$

$$2 = 2 \cdot 1$$

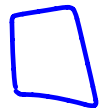
gcd

Lemma:

If m and n are relatively prime and $m \mid n \cdot b$ for some $b \in \mathbb{N}$, then $m \mid b$.

Corollary: If p is a prime,
 p does not divide m ,
and $p \mid m \cdot b$, then
 $p \mid b$.

Proof: If p does not divide m ,
since the only divisors of
 p are 1 and p ,
 $\gcd(p, m) = 1$. The
result follows from the lemma.



Corollary: If p is prime and p divides $m \cdot n$, then either $p \mid m$ or $p \mid n$.

Proof: If $p \nmid m$, then by the previous corollary, $p \mid n$.
Conversely, if $p \nmid n$, then again by the corollary, $p \mid m$.



Corollary: Let $n \geq 2$, $n \in \mathbb{N}$. If p is prime and

$$p \mid b_1 b_2 \cdots b_n \text{ for}$$

$b_i \in \mathbb{N}$, $1 \leq i \leq n$, then

$$\exists k, 1 \leq k \leq n, p \mid b_k.$$

proof: By induction.

Base case $n=2$ is the previous corollary. Now assume $\forall m < n$, $n > 2$, that the result holds.

Write

$$b_1 b_2 \cdots b_{n-1} = a.$$

Then $p \mid a b_n$. By induction,

the base case,

$$p \mid a \text{ or } p \mid b_n.$$

If $p \mid b_n$, then $n=k$ and we are done.

If $p \mid a$, then by the inductive

hypothesis, $\exists k, 1 \leq k \leq n-1$,

$p \mid b_k$, and we are done. \square

The Fundamental Theorem of Arithmetic

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

1) We have that either n is prime
or is a product of primes.

2) (Unique factorization)

If we can write, for $k, m \in \mathbb{N}$,
 $a_i, 1 \leq i \leq k$, $x_j, 1 \leq j \leq m$ prime
numbers and

$$n = a_1 a_2 \cdots a_k = x_1 x_2 \cdots x_m,$$

then $k = m$ and, up to reordering,

$$a_i = x_i \quad \forall 1 \leq i \leq k.$$

Up to reordering:

$$6 = 2 \cdot 3 = 3 \cdot 2$$

Proof: 1) By induction on n .

If $n=2$, then 2 is prime.

Now suppose $n > 2$.

Either

1) n is prime, and we are done

2) n is not prime. Then \exists
prime p , $p < n$, $p | n$.

So we can write

$$n = p \cdot b \text{ for } b < n.$$

By induction, b is either prime
or a product of primes

$\Rightarrow n$ is a product of primes.

2) Proof by inducting on n .

$n=2$ is a prime.

Show: given $n > 2$, if

$$\begin{aligned} n &= a_1 a_2 \cdots a_k \\ &= x_1 x_2 \cdots x_m \end{aligned} \left. \vphantom{\begin{aligned} n &= a_1 a_2 \cdots a_k \\ &= x_1 x_2 \cdots x_m \end{aligned}} \right\} \text{all primes}$$

then $k=m$ and, up to reordering,

$$x_i = a_i \quad \forall \quad 1 \leq i \leq k.$$

Since a_1 is a prime and

$$a_1 \mid n, \quad a_1 \mid x_1 x_2 \cdots x_m.$$

Therefore, by our corollaries, \exists

$$j, \quad 1 \leq j \leq m, \quad \text{with}$$

$$a_1 \mid x_j. \quad \text{But } x_j$$

is prime, and so $a_1 = x_j$.

Reordering the product of the x_i 's, we may assume $j=1$.

Then

$$n = a_1 a_2 \cdots a_k$$

$$= a_1 x_2 \cdots x_m, \text{ so}$$

$$\frac{n}{a_1} = a_2 a_3 \cdots a_k$$

$$= x_2 x_3 \cdots x_m$$

By induction, since $\frac{n}{a_1} < n$,

we have $k = m$ and, up to

reordering, $x_i = a_i \quad \forall 2 \leq i \leq k$.

This immediately implies the result for

n since $a_1 = x_1$

