COL 202: DISCRETE MATHEMATICAL STRUCTURES

LECTURE 9

NUMBER THEORY I : GCD

JAN 19, 2024 | ROHIT VAISH

Arithmetic Assumptions

Assume usual rules for $+$, $\cdot$, $-$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{(Distributivity)}$$

$$a \cdot b = b \cdot a \quad \text{(Commutativity)}$$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{(Associativity)}$$

$$a + 0 = a \quad \text{(Additive Identity)}$$

$$a - a = 0 \quad \text{(Additive Inverse)}$$

$$a + 1 > a$$

Division Theorem

Let n and d be integers such that $d \neq 0$.

Then, there exists a unique pair of integers q and r s.t.

$$n = q \cdot |d| + r \quad \text{and} \quad 0 \leq r < |d|.$$

Division Theorem

Let n and d be integers such that $d \neq 0$.

Then, there exists a unique pair of integers q and r s.t.

$$n = q \cdot |d| + r \quad \text{and} \quad 0 \leq r < |d|.$$

q: quotient (n, d)

r: remainder (n, d)

DIVISION THEOREM

Let n and d be integers such that $d \neq 0$.

Then, there exists a unique pair of integers q and r s.t.

$$n = q \cdot |d| + r \quad \text{and} \quad 0 \leq r < |d|.$$

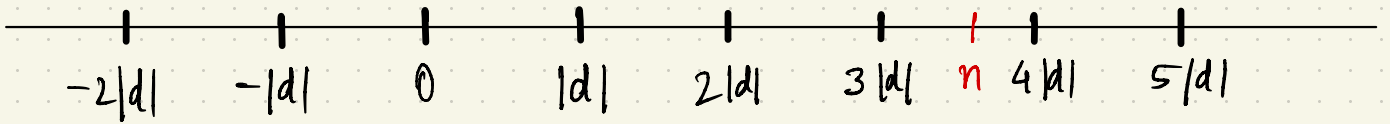
Eg., Say $d=3$. Then, for any n, there is a unique q such that $n=3q$ or $n=3q+1$ or $n=3q+2$.

Division Theorem

Let n and d be integers such that $d \neq 0$.

Then, there exists a unique pair of integers q and r s.t.

$$n = q \cdot |d| + r \quad \text{and} \quad 0 \leq r < |d|.$$

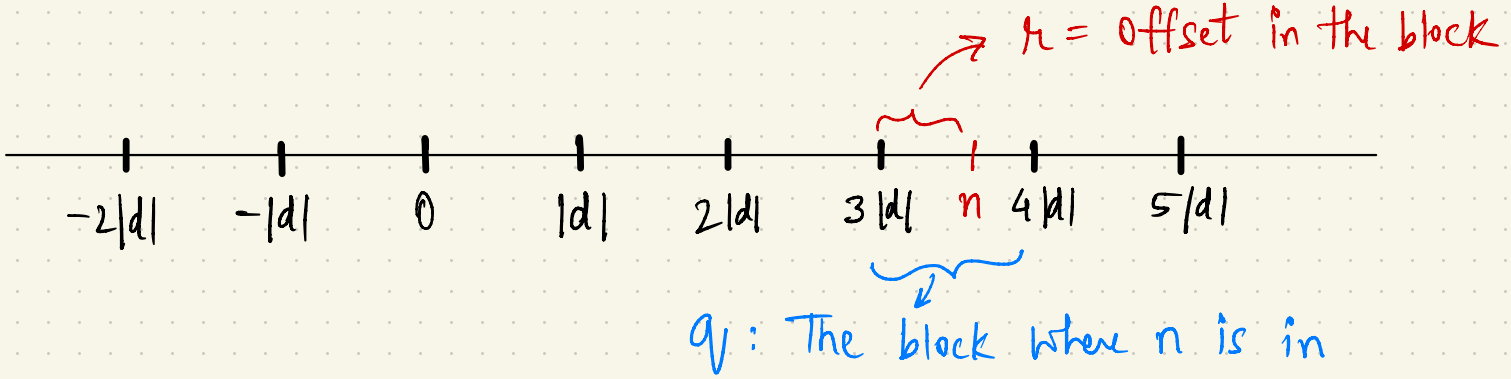


Division Theorem

Let n and d be integers such that $d \neq 0$.

Then, there exists a unique pair of integers q and r s.t.

$$n = q \cdot |d| + r \quad \text{and} \quad 0 \leq r < |d|.$$



DIVISIBILITY

d divides n if $n = q \cdot d$ for some q

DIVISIBILITY

integers

d divides n if $n = q \cdot d$ for some q

DIVISIBILITY

integers

d divides n if $n = q \cdot d$ for some q

E.g., 2 divides -6 $\quad 2 \mid -6$

a.k.a. -6 is a multiple of 2.

a.k.a. 2 is a divisor of -6.

DIVISIBILITY

integers

d divides n if $n = q \cdot d$ for some q

E.g., 2 divides -6 $\quad 2 \mid -6$

a.k.a. -6 is a multiple of 2.

a.k.a. 2 is a divisor of -6.

$n \mid 0$ for every n because $0 = 0 \cdot n$

Divisibility Facts

Divisibility Facts

1. $d \mid n \implies d \mid k \cdot n$

Divisibility Facts

1. $d \mid n \Rightarrow d \mid k \cdot n$

2. $d \mid n$ and $d \mid m \Rightarrow d \mid (n+m)$

Divisibility Facts

1. $d \mid n \Rightarrow d \mid k \cdot n$

2. $d \mid n$ and $d \mid m \Rightarrow d \mid (n+m)$

3. $d \mid n$ and $d \mid m \Rightarrow d \mid (s \cdot n + t \cdot m)$

Divisibility Facts

1. $d \mid n \Rightarrow d \mid k \cdot n$

2. $d \mid n$ and $d \mid m \Rightarrow d \mid (n+m)$

3. $d \mid n$ and $d \mid m \Rightarrow d \mid (s \cdot n + t \cdot m)$

integer linear combination

Divisibility Facts

1. $d \mid n \Rightarrow d \mid k \cdot n$

2. $d \mid n$ and $d \mid m \Rightarrow d \mid (n+m)$

3. $d \mid n$ and $d \mid m \Rightarrow d \mid (s \cdot n + t \cdot m)$

integer linear combination

d is a common divisor of n and m

Greatest Common Divisor

$\gcd(n, m)$:= greatest common divisor of n and m

GREATEST COMMON DIVISOR

$gcd(n, m)$:= greatest common divisor of n and m

Eg; $gcd(8, 10) = 2$

$gcd(7, 8) = 1$

GREATEST COMMON DIVISOR

$gcd(n, m)$:= greatest common divisor of n and m

Eg; $gcd(8, 10) = 2$

$gcd(7, 8) = 1$

$gcd(0, n) =$ for $n > 0$

Greatest Common Divisor

$gcd(n, m)$:= greatest common divisor of n and m

Eg; $gcd(8, 10) = 2$

$gcd(7, 8) = 1$

$gcd(0, n) = n$ for $n > 0$

GREATEST COMMON DIVISOR

$gcd(n, m)$:= greatest common divisor of n and m

Eg; $gcd(8, 10) = 2$

$gcd(7, 8) = 1$

$gcd(0, n) = n$ for $n > 0$

If p is prime, then $gcd(p, n) =$

Greatest Common Divisor

$\gcd(n, m)$:= greatest common divisor of n and m

Eg; $\gcd(8, 10) = 2$

$\gcd(7, 8) = 1$

$\gcd(0, n) = n$ for $n > 0$

If p is prime, then $\gcd(p, n) = 1$ or p.

Only divisors of p are $\pm 1, \pm p$.

Greatest Common Divisor

$\gcd(n,m)$:= greatest common divisor of n and m

Eg; $\gcd(8,10) = 2$

$\gcd(7,8) = 1$

$\gcd(0,n) = n$ for $n > 0$

If p is prime, then $\gcd(p,n) = 1$ or p.

Only divisors of p are $\pm 1, \pm p$.

$\gcd(n,m)$ always exists and is unique (Exercise)

Finding The GCD

Finding The GCD

Can try every number $1, 2, \ldots, \min\{|m|, |n|\}$

Finding The GCD

Can try every number $1, 2, \ldots, \min\{|m|, |n|\}$

Is there a better way?

FINDING THE GCD

Recall division theorem: Unique $0 \leq r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

FINDING THE GCD

Recall division theorem: Unique $0 \leq r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof:

Finding The GCD

Recall division theorem: Unique $0 \leq r < |m|$ s.t. $n = q|m| + r$

Remainder Lemma: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof: Suffices to show that for any integer p,

$p|n$ and $p|m \iff p|m$ and $p|r$

FINDING THE GCD

Recall division theorem: Unique $0 \leq r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Why?

Proof: Suffices to show that for any integer p,

$p|n$ and $p|m \iff p|m$ and $p|r$

FINDING THE GCD

Recall division theorem: Unique $0 \leq r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof: Suffices to show that for any integer p,

$p|n$ and $p|m \iff p|m$ and $p|r$

Why? same set of common divisors

FINDING THE GCD

Recall division theorem: Unique $0 \leq r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof: Suffices to show that for any integer p,

$p|n$ and $p|m \iff p|m$ and $p|r$

Why? same set of common divisors

$\Downarrow$

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

FINDING THE GCD

Recall division theorem: Unique $0 \le r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof: Suffices to show that for any integer p,

$p|n$ and $p|m \iff p|m$ and $p|r$

Why? Same set of common divisors

$\Downarrow$

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

* $p|m \iff p \,|\, |m|$

FINDING THE GCD

Recall division theorem: Unique $0 \le r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof: Suffices to show that for any integer p,

$p|n$ and $p|m \iff p|m$ and $p|r$

Why? same set of common divisors

$\Downarrow$

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

* $p|m \iff p||m|$
* Linear combination $n = q|m| + r$

FINDING THE GCD

Recall division theorem: Unique $0 \le r < |m|$ s.t. $n = q|m| + r$

REMAINDER LEMMA: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof: Suffices to show that for any integer p,

$p|n$ and $p|m \iff p|m$ and $p|r$

Why? Same set of common divisors

$\Downarrow$

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

* $p|m \iff p||m|$
* Linear combination $n = q|m| + r$

$\Rightarrow$ Common divisor of any two of n, m, r divides the third.

Finding The GCD

Recall division theorem: Unique $0 \le r < |m|$ s.t. $n = q|m| + r$

Remainder Lemma: $\gcd(n, m) = \gcd(m, r)$ for $m \neq 0$

Proof: Suffices to show that for any integer p,

$$p|n \text{ and } p|m \iff p|m \text{ and } p|r$$

* $p|m \iff p||m|$
* Linear combination $n = q|m| + r$

$\Rightarrow$ Common divisor of any two of n, m, r divides the third.

Why? Same set of common divisors

$\Downarrow$

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

∎

Finding The GCD

E.g., $n = 899$ $m = 493$

$\gcd(899, 493)$

Finding The GCD

E.g., $n = 899$ $m = 493$

$\gcd(899, 493)$

$= \gcd(493, 406)$

Finding The GCD

E.g., $n = 899$ $m = 493$

$\gcd(899, 493)$

$= \gcd(493, 406)$

$= \gcd(406, 87)$

Finding The GCD

E.g., $n = 899$ $m = 493$

$\gcd(899, 493)$

$= \gcd(493, 406)$

$= \gcd(406, 87)$

$= \gcd(87, 58)$ because $406 = 4 \times 87 + 58$

Finding The GCD

E.g., $n = 899$ $m = 493$

$\gcd(899, 493)$

$= \gcd(493, 406)$

$= \gcd(406, 87)$

$= \gcd(87, 58)$

$= \gcd(58, 29)$

because $406 = 4 \times 87 + 58$

Finding The GCD

E.g., $n = 899$ $m = 493$

$gcd(899, 493)$

$= gcd(493, 406)$

$= gcd(406, 87)$

$= gcd(87, 58)$

$= gcd(58, 29)$

$= gcd(29, 0)$

because $406 = 4 \times 87 + 58$

Finding The GCD

E.g., $n = 899$ $m = 493$

$\gcd(899, 493)$

$= \gcd(493, 406)$

$= \gcd(406, 87)$

$= \gcd(87, 58)$

$= \gcd(58, 29)$

$= \gcd(29, 0)$

$= 29$

because $406 = 4 \times 87 + 58$

Finding The GCD

Euclidean Algorithm

Finding The GCD

Euclidean Algorithm

```
gcd (n, m)

if m = 0
    return n
else
    n = qm + r
    return gcd (m, r)
```

Finding The GCD

Euclidean Algorithm

```
gcd (n, m)
if m = 0
    return n
else
    n = qm + r
    return gcd (m, r)
```

Termination

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if m = 0

    return n

else

    n = qm + r

    return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if m = 0

    return n

else

    n = qm + r

    return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
* if $m > \frac{n}{2}$,

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if m = 0

    return n

else

    n = qm + r

    return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
* if $m > \frac{n}{2}$, gcd (n, m) $\longrightarrow$ gcd (m, n-m)

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if m = 0

    return n

else

    n = qm + r

    return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
* if $m > \frac{n}{2}$, gcd (n, m) → gcd (m, n-m) = gcd (n-m, m)

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if $m = 0$

return n

else

$n = qm + r$

return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
* if $m > \frac{n}{2}$, gcd (n, m) $\longrightarrow$ gcd (m, n-m) = gcd (n-m, m) $< \frac{n}{2}$

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if m = 0

    return n

else

    n = qm + r

    return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
* if $m > \frac{n}{2}$, gcd (n, m) → gcd (m, n−m) = gcd (n−m, m) $< \frac{n}{2}$

again, "n" is (at least) halved

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if m = 0

    return n

else

    n = qm + r

    return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
* if $m > \frac{n}{2}$, gcd (n, m) → gcd (m, n−m) = gcd (n−m, m) $< \frac{n}{2}$

again, "n" is (at least) halved

$O\left(\log_2(\min(n, m))\right)$ steps

Correctness

Finding The GCD

Euclidean Algorithm

gcd (n, m)

if m = 0

    return n

else

    n = qm + r

    return gcd (m, r)

Termination

At each step

* if $m \leq \frac{n}{2}$, then "n" is (at least) halved
* if $m > \frac{n}{2}$, gcd (n, m) → gcd (m, n-m) = gcd (n-m, m) $< \frac{n}{2}$

again, "n" is (at least) halved

$O\left(\log_2(\min(n, m))\right)$ steps

Correctness

Invariant maintained by algo

due to remainder theorem

LINEAR COMBINATION V/S COMMON DIVISOR

LINEAR COMBINATION V/S COMMON DIVISOR

Greatest common divisor

$\gcd(n, m)$ = largest number d such that $d \mid n$ and $d \mid m$.

LINEAR COMBINATION V/S COMMON DIVISOR

Greatest common divisor

$gcd(n,m)$ = largest number d such that d/n and d/m.

Smallest positive integer linear combination

$spc(n,m)$ = smallest positive integer d such that $d = s \cdot n + t \cdot m$

s, t integers

LINEAR COMBINATION V/S COMMON DIVISOR

Greatest common divisor

$gcd(n,m)$ = largest number d such that d/n and d/m.

Smallest positive integer linear combination

$spc(n,m)$ = smallest positive integer d such that $d = s \cdot n + t \cdot m$

s, t integers

Theorem: $gcd(n,m) = spc(n,m)$

Linear combination v/s Common divisor

Greatest common divisor

$\gcd(n,m)$ = largest number d such that d/n and d/m.

Smallest positive integer linear combination

$spc(n,m)$ = smallest positive integer d such that $d = s \cdot n + t \cdot m$

s, t integers

Theorem: $\gcd(n,m) = spc(n,m)$

gcd is the smallest positive number that can be constructed by taking linear combinations.

Linear combination v/s Common divisor

Greatest common divisor

$\gcd(n,m)$ = largest number d such that d/n and d/m.

Smallest positive integer linear combination

$spc(n,m)$ = smallest positive integer d such that $d = s \cdot n + t \cdot m$

s, t integers

Theorem: $\gcd(n,m) = spc(n,m)$

Corollary: Any multiple of $\gcd(n,m)$ is a linear combination of n and m and vice versa.