www.math.stonybrook.edu/~marco

MAT312 < Syllabus
Schedule < HW
Material
Projects.

Final, Projects, HW
40% 40% 20%

lectures < Regular 50%
Projects 50%

LNI a

§1.1 Given 20 and 7: $20 = 2 \cdot 7 + 6$

Thm (Division Theorem)

- Let $a, b \in \mathbb{N}$, $a > 0 \Rightarrow \exists\, q, r \in \mathbb{N}$
- $0 \leq r < a$ and $b = q \cdot a + r$

"quotient" → q

"remainder" → r

Pf If $a > b$ then $q = 0$ and $r = b$.

- Suppose $b \geq a$.
- Let

$$D = \{ b - ak \mid b - ak \geq 0 \text{ and } k \geq 0 \}.$$

$D \neq \emptyset$. So D contains a smallest elemt. Say

$$\min D = r = b - q \cdot a.$$

If $r \geq a$ then $r - a \geq 0$ and $r - a \in D$. So r is not the smallest.

Hence, $r < a$. and.

$$b = q \cdot a + r$$

□.

- Definition a devides b : $(a|b)$
- if $b = q \cdot a$

  Ex: $7 | 42$.

  Obseive: $a|b \iff r = 0$.

Greatest Common Divisor

- Thm $\forall a, b > 0$ $\exists!$ $d > 0$ s.t. ← "g.c.d."
- . $d|a$ $d|b$
  . If $c|a$ $c|b$ then $c|d$.

Pf| let

$$D = \{ as + bt \;(>0) \mid s, t \in \mathbb{Z} \}.$$

$a = 1 \cdot a + 0 \cdot b \in D.$

So $D \neq \phi$.

let $d = \min D$, say

$$d = as + bt. < a.$$

Claim: $c \mid a \quad c \mid b \Rightarrow c \mid d.$

Pf $c \mid a \Rightarrow a = cq$

$c \mid b \Rightarrow b = ch.$

So $\frac{d}{c} = [cq \cdot s + ch \cdot t] \cdot \frac{1}{c} = qs + ht \in \mathbb{Z}$. □.

Claim: $d \mid a$.

Pf Div Thm $\Rightarrow$ $a = dq + r \quad 0 \leq r < d.$

$0 \leq r = a - dq = a - (as+bt)q \in D.$

If $r > 0$ then $r \in D$ and $r < d$. ↯. □.

□

Examples

$\gcd(30, 12) = 6$ $\qquad (37, 0) = 37$

$\gcd(521, 30) = \ldots ?$

Lem $b \geq a \neq 0$

If $b = q \cdot a + r$ then $(b,a) = (a,r)$

Pf $r = b - q \cdot a$. So $(b,a) \mid r$ $(b,a) \mid a$

Hence, $(b,a) \mid (a,r)$ (1)

- $b = aq + r$. So $(a,r) \mid b$ $(a,r) \nmid a$
- Hence $(a,r) \mid (b,a)$ (2)

(1), (2) $\Longrightarrow$ $(b,a) = (a,r)$ □

Euclidean Algorithm

$b \geq a \neq 0$

- $a \mid b \Longrightarrow (b,a) = a$
- ~~$a \mid b$~~ :

$$b = aq_1 + r_1 \quad 0 \leq r_1 < a$$

$(b,a) =$
$(a,r_1) =$
$$a = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$$

$(r_1,r_2) =$
$$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$$

$$\vdots$$

(r_{n-1}, r_n)
$$r_{n-1} = r_n q_{n+1} + 0$$

$(r_n, 0) = r_n$ ← $\gcd(b,a) = r_n$

Ex) $\gcd(171, 30)$

$171 = 5 \cdot 30 + 21$

$30 = 1 \cdot 21 + 9$

$21 = 2 \cdot 9 + 3$

$9 = 3 \cdot 3 + 0$

$(30, 21)$

$=$

$(21, 9)$

$=$

$(9, 3)$

$=$

$(3, 0) = 3$.

3 steps

Ex) $(25, 15) = (15, 10) = (10, 5) = (5, 0) = 5$.

$25 = 1 \cdot 15 + 10$

$15 = 1 \cdot 10 + 5$

$10 = 2 \cdot 5 + 0$

3 steps

Ex) $(34, 21) = (21, 13) = (13, 8) = (8, 5)$

$= (5, 3) = (3, 2)$

$= (2, 1) = (1, 0) = 1$.

$34 = 1 \cdot 21 + 13$

$21 = 1 \cdot 13 + 8$

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

7 steps

Ex) $(1321, 1320) = (1320, 1) = (1, 0) = 0$

$1321 = 1 \cdot 1320 + 1$

$1320 = 1320 \cdot 1 + 0$

2 steps

$$r_{k-1} = q_k r_k + r_{k+1}$$

$$r_{k-1} \geq q_k r_k \qquad r_k < \frac{r_{k-1}}{q_k}$$

$$r_k < \frac{r_1}{\prod q_k}.$$

$$r_{k-1} = q_k r_k + r_{k+1} \leq (q_k+1) r_k.$$

$$r_k > \frac{r_{k-1}}{q_{k+1}}$$

$$r_k > \frac{r_1}{\prod (q_k+1)}$$

$$\tilde{r}_1 < r_1$$

$$r_k > \frac{r_1}{\prod (q_k+1)} \geq \frac{\tilde{r}_1}{\prod \tilde{q}_k} > \tilde{r}_k \qquad \square$$

LNIb

§1.2 Fibonacci Numbers.

$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

$x_0\ x_1 \qquad x_{n-1}\ x_n\ x_{n+1}$

$$x_{n+1} = x_n + x_{n-1}$$

These numbers appear in many situations. Also in nature. Let's look at consecutive ratios

$$\frac{x_{n+1}}{x_n} = 1 + \frac{1}{\frac{x_n}{x_{n-1}}}$$

Suppose

$$\frac{x_{n+1}}{x_n} \longrightarrow \rho$$

$$\rho = 1 + \frac{1}{\rho}$$

$$\rho^2 - \rho - 1 = 0 \qquad \rho = \frac{1+\sqrt{5}}{2}$$

$$\rho = 1 + \frac{1}{\rho} = 1 + \frac{1}{1 + \frac{1}{\rho}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{\rho}}}$$

$$\rho = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}}}}$$

continued fraction

Every irrational has a similar continued fraction. $x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$

$\rho = \frac{1+\sqrt{5}}{2}$ golden ratio is the simplest

Lemma: $(x_{n+1}, x_n) = 1$.
(relative Prime)

Pf: $(x_0, x_1) = (1,1) = 1$.

Induction tick:

Suppose $(x_n, x_{n-1}) = 1$

Show $(x_{n+1}, x_n) = 1$.

(Then you would be done for all n).

$x_{n+1} = x_n + x_{n-1}$

Let $v \mid x_{n+1}$ $v \mid x_n$.

$x_{n-1} = x_{n+1} - x_n = sv - t \cdot v = (s-t)v$.

So $v \mid x_{n-1}$ and $v \mid x_n$.

But $(x_n, x_{n-1}) = 1$

So $v = 1$

Indeed $(x_{n+1}, x_n) = 1$ □

Thm (Induction Principle)

Let $P(n)$ be a statement, $n \geq 1$

Suppose

a) $P(1)$ is true (base Ind.)

b) $P(n) \Longrightarrow P(n+1)$. (Ind. Step)

Then $P(n)$ is true for all n.

Pf) Suppose Thm is wrong: $\exists n_0$ $P(n_0)$ false.

Let $F = \{n \mid P(n) \text{ False}\}$.

Then $n_0 \in F \neq \emptyset$, $1 \notin F$

Let $n^* = \min F$.

Then $n^* > 1$

So $n^* - 1 \notin F$ and

$P(n^*-1)$ is true.

So ~~$P(n^*) = P(n^*-1+1)$~~ by says

~~Applies~~. $P(n^*-1) \Longrightarrow P(n^*)$ } So $P(n^*)$ true

$P(n^*-1)$ true

Contradiction. □

Example

$$\circledast \quad \frac{1}{3}+\frac{1}{15}+\frac{1}{35}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{n}{2n+1}$$

Proof $n=1$: $\frac{1}{3}=\frac{1}{3}$ (basis)

- Suppose $\circledast$ holds for n.
- Show it holds for $n+1$

$$\frac{1}{3}+\frac{1}{15}+\cdots+\frac{1}{(2(n+1)-1)(2(n+1)+1)}=$$

$$\underbrace{\frac{1}{3}+\cdots+\frac{1}{(2n-1)(2+1)}}+\frac{1}{(2(n+1)-1)(2(n+1)+1)}=$$

$$\frac{n}{2n+1}+\frac{1}{(2(n+1)-1)(2(n+1)+1)}=$$

$$\frac{n}{2n+1}+\frac{1}{(2n+1)(2n+3)}=\frac{n(2n+3)+1}{(2n+1)(2n+3)}=$$

$$\frac{2n^2+3n+1}{(2n+1)(2n+3)} \Downarrow = \frac{(2n+1)(n+1)}{(2n+1)(2n+3)}=\frac{n+1}{2n+3}$$

□

$(42, 12)$

$42 = \boxed{3} \cdot 12 + 6$

$12 = \boxed{2} \cdot 6 + 0$

$(42,12) =$

$(12,6) =$

$(2,0) = 2.$

$b = \boxed{q} a + r$

$(255, 251)$

$255 = \boxed{1} \cdot 251 + 4$

$251 = \boxed{62} \cdot 4 + 3$

$4 = \boxed{1} \cdot 3 + 1$

$3 = \boxed{3} \cdot 1 + 0$

$(255, 251)$
$=$
$(251, 4)$
$=$
$(62, 3)$
$=$
$(3, 1)$

$(1, 0) = 1.$

$(21, 13)$

$21 = \boxed{1} \cdot 13 + 8$

$13 = \boxed{1} \cdot 8 + 5$

$8 = \boxed{1} \cdot 5 + 3$

$5 = \boxed{1} \cdot 3 + 2$

$3 = \boxed{1} \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$(13, 8)$

$(8, 5)$

$(5, 3)$

$(3, 2)$

$(2, 1)$

$(1, 0) = 1.$

If you want the algorithm to be fast you need the quotients to be big

Question 2 of Project

$$\tilde{q}_n > q_n \implies \#(b,\tilde{a}) < \#(b,a)$$

www.math.stonybrook.edu/~marco

MAT312 < Syllabus
Schedule < HW
Material
Projects.

Final, Projects, HW
40% 40% 20%

lectures < Regular 50%
Projects 50%

LNI a

§1.1 Given 20 and 7: $20 = 2 \cdot 7 + 6$

Thm (Division Theorem)

- Let $a, b \in \mathbb{N}$, $a > 0 \Rightarrow \exists\, q, r \in \mathbb{N}$
- $0 \leq r < a$ and $b = q \cdot a + r$

"quotient" → q

"remainder" → r

Pf If $a > b$ then $q = 0$ and $r = b$.

- Suppose $b \geq a$.
- Let

$$D = \{ b - ak \mid b - ak \geq 0 \text{ and } k \geq 0 \}.$$

$D \neq \emptyset$. So D contains a smallest elemt. Say

$$\min D = r = b - q \cdot a.$$

If $r \geq a$ then $r - a \geq 0$ and $r - a \in D$. So r is not the smallest.

Hence, $r < a$. and.

$$b = q \cdot a + r$$

□.

- Definition a devides b : $(a|b)$
- if $b = q \cdot a$

  Ex: $7 | 42$.

  Observe: $a|b \iff r = 0$.

Greatest Common Divisor

- Thm $\forall a, b > 0$ $\exists!$ $d > 0$ s.t. ← "g.c.d."
- . $d|a$ $d|b$
  . If $c|a$ $c|b$ then $c|d$.

Pf| let

$$D = \{ as + bt \;(>0) \mid s, t \in \mathbb{Z} \}.$$

$a = 1 \cdot a + 0 \cdot b \in D$.

So $D \neq \phi$.

let $d = \min D$, say

$$d = as + bt < a.$$

Claim: $c \mid a \quad c \mid b \Rightarrow c \mid d$.

Pf $c \mid a \Rightarrow a = cq$

$c \mid b \Rightarrow b = ch$.

So $\frac{d}{c} = [cq \cdot s + ch \cdot t] \cdot \frac{1}{c} = qs + ht \in \mathbb{Z}$. □

Claim: $d \mid a$.

Pf Div Thm $\Rightarrow$ $a = dq + r \quad 0 \leq r < d$.

$0 \leq r = a - dq = a - (as+bt)q \in D$.

If $r > 0$ then $r \in D$ and $r < d$. ↯. □

□

Examples

$\gcd(30, 12) = 6$ $\quad (37, 0) = 37$

$\gcd(521, 30) = \ldots ?$

Lem $b \geq a \neq 0$

If $b = q \cdot a + r$ then $(b,a) = (a,r)$

Pf $r = b - q \cdot a$. So $(b,a) \mid r$ $(b,a) \mid a$

Hence, $(b,a) \mid (a,r)$ (1)

- $b = aq + r$. So $(a,r) \mid b$ $(a,r) \nmid a$
- Hence $(a,r) \mid (b,a)$ (2)

(1), (2) $\Longrightarrow$ $(b,a) = (a,r)$ □

Euclidean Algorithm

$b \geq a \neq 0$

- $a \mid b \Longrightarrow (b,a) = a$
- $a \nmid b$: $b = aq_1 + r_1$ $0 \leq r_1 < a$

$(b,a) =$
$(a,r_1) =$ $a = r_1 q_2 + r_2$ $0 \leq r_2 < r_1$

$(r_1,r_2) =$ $r_1 = r_2 q_3 + r_3$ $0 \leq r_3 < r_2$

⋮

(r_{n-1}, r_n) $r_{n-1} = r_n q_{n+1} + 0$

$(r_n, 0) = r_n$ ⟵ $\gcd(b,a) = r_n$

Ex) $\gcd(171, 30)$

$171 = 5 \cdot 30 + 21$ $\quad (30, 21)$

$30 = 1 \cdot 21 + 9$ $\quad (21, 9)$ $\quad$ 3 steps

$21 = 2 \cdot 9 + 3$ $\quad (9, 3)$

$9 = 3 \cdot 3 + 0$ $\quad (3, 0) = 3$.

Ex) $(25, 15) = (15, 10) = (10, 5) = (5, 0) = 5$.

$25 = 1 \cdot 15 + 10$

$15 = 1 \cdot 10 + 5$ $\quad$ 3 steps

$10 = 2 \cdot 5 + 0$

Ex) $(34, 21) = (21, 13) = (13, 8) = (8, 5)$

$34 = 1 \cdot 21 + 13$ $\quad = (5, 3) = (3, 2)$

$21 = 1 \cdot 13 + 8$ $\quad = (2, 1) = (1, 0) = 1$.

$13 = 1 \cdot 8 + 5$

$8 = 1 \cdot 5 + 3$ $\quad$ 7 steps

$5 = 1 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Ex) $(1321, 1320) = (1320, 1) = (1, 0) = 0$

$1321 = 1 \cdot 1320 + 1$

$1320 = 1320 \cdot 1 + 0$

2 steps