

§1.11

Given 20 and 7: $\underline{20} = 2 \cdot \underline{7} + 6$

Thm (Division Theorem)

let $a, b \in \mathbb{N}$, $a > 0 \Rightarrow \exists q, r \in \mathbb{N}$

$$0 \leq r < a \quad \text{and} \quad b = q \cdot a + r$$

"quotient"

"remainder"

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 element. Say

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

If $r \geq a$ then $r - a \geq 0$ and $-2-$
 $r - a \in D$. So r is not the smallest.
Hence, $r < a$. and.

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

□

• Definition a divides 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.
 $\uparrow$ "g.c.d."

• $d|a$ $d|b$

• If $c|a$ $c|b$ then $c|d$.

Pf | let

$$D = \left\{ \begin{matrix} as + bt \\ > 0 \end{matrix} \mid s, t \in \mathbb{Z} \right\}.$$

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

- 3 -

So $D \neq \emptyset$.

let $d = \min D$, say

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

• Claim: $c|a \quad c|b \Rightarrow c|d$.

• Pf $c|a \Rightarrow a = cq$
 $c|b \Rightarrow b = ch$.

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

Claim: $d|a$.

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 $r < d$. $\downarrow \cdot \square$.

$\square$.

Examples

$$\gcd(30, 12) = 6$$

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

$$(37, 0) = 37$$

lem $b \geq a \neq 0$ -4-

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

• Hence $(a, r) \mid (b, a)$ (2)

(1), (2) $\implies (b, a) = (a, r)$

□

Euclidean Algorithm

$b \geq a \neq 0$

• $a \mid b \implies (b, a) = a$

• $a \nmid b$: $b = aq_1 + r_1$ $0 \leq r_1 < a$

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

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

⋮

⋮

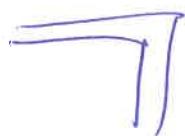
(r_{n-1}, r_n)

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

$(r_n, 0) = r_n$

↑ $\gcd(b, a) = r_n$

Ex) ~~171~~ (171, 30)



- 5 -

$$171 = 5 \cdot 30 + 21$$

$$30 = 1 \cdot 21 + 9$$

$$21 = 2 \cdot 9 + 3$$

$$9 = 3 \cdot 3 + 0$$

$$(\del{30}, 21)$$

"

$$(21, 9)$$

"

$$(9, 3)$$

"

$$(3, 0) = 3$$

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

$$34 = 1 \cdot 21 + 13$$

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

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

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

7 steps

$$\text{Ex) } (1321, 1320) = (1320, 1) = (1, 0) = 0$$

- 6 -

$$1321 = 1 \cdot 1320 + 1$$

2 steps

$$1320 = 1320 \cdot 1 + 0$$

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

$$r_{k-1} \geq q_k r_k$$

$$r_k \leq \frac{r_{k-1}}{q_k}$$

$$r_n < \frac{r_1}{\prod q_k}$$

$$r_{k-1} = q_k r_k + r_{k+1} < (q_{k+1}) r_k$$

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

$$r_n > \frac{r_1}{\prod (q_{k+1})}$$

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

$$r_k > \frac{r_1}{\prod (q_{k+1})} \geq \frac{\tilde{r}_1}{\prod \tilde{q}_k} > \tilde{r}_k$$



§1.2 Fibonacci Numbers.

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

$$\begin{array}{ccccccc} \parallel & \parallel & & & \parallel & * & \parallel \\ x_0 & x_1 & & & x_{n-1} & x_n & x_{n+1} \end{array}$$

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

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

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

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

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

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

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

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

continued fraction

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

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

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

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

Induction trick:

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

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

(Then you would be done for all n).

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

$$\text{let } v \mid x_{n+1} \quad v \mid x_n.$$

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

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

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

$$\text{So } v = 1$$

$$\text{Indeed } (x_{n+1}, x_n) = 1$$



Thm (Induction Principle) -4-

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

Suppose

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

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

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

Pf) ~~let~~ 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 $n^* - 1 \in F$ and

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

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

~~applies.~~ $\left. \begin{array}{l} P(n^* - 1) \implies P(n^*) \\ P(n^* - 1) \text{ true} \end{array} \right\}$ So $P(n^*)$ true

Contradiction.

□

Example

-5-

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

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

Suppose $(*)$ holds for n .

Show it holds for $n+1$

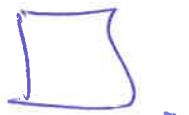
$$\frac{1}{3} + \frac{1}{15} + \dots + \frac{1}{(2(n+1)-1)(2(n+1)+1)} =$$

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

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

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

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



$$(42, 12)$$

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

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

$$(42, 12) =$$

$$(12, 6) =$$

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

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

$$(255, 251)$$

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

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

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

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

$$(255, 251)$$

$$\overset{''}{(251, 4)}$$

$$\overset{''}{(62, 3)}$$

$$\overset{''}{(3, 1)}$$

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

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

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

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

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

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

$$2 = 2 \cdot 1 + 0$$

$$(21, 13)$$

$$(13, 8)$$

$$(8, 5)$$

$$(5, 3)$$

$$(3, 2)$$

$$(2, 1)$$

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

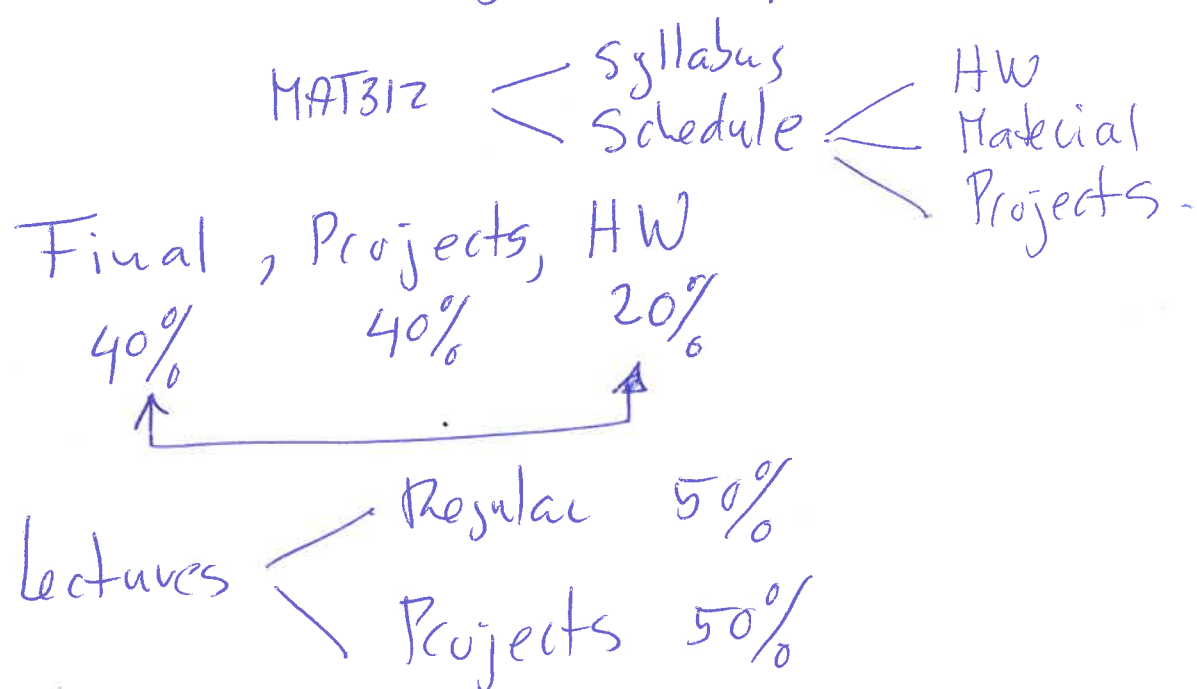
If you want the algorithm to be fast you need the quotients to be big

~~Step 1~~

Question 2 of Project

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

www.math.stonybrook.edu/~marco



§1.1

Given 20 and 7: $\underline{20} = 2 \cdot \underline{7} + 6$

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"

"remainder"

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 element. Say

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

If $r \geq a$ then $r - a \geq 0$ and $-2-$
 $r - a \in D$. So r is not the smallest.
Hence, $r < a$. and.

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

□.

• Definition a divides 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.
 $\uparrow$ "g.c.d."

• $d|a$ $d|b$

• If $c|a$ $c|b$ then $c|d$.

Pf let

$$D = \left\{ \begin{matrix} as + bt \\ > 0 \end{matrix} \mid s, t \in \mathbb{Z} \right\}.$$

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

- 3 -

So $D \neq \emptyset$.

let $d = \min D$, say

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

● Claim: $c|a \quad c|b \Rightarrow c|d$.

● Pf $c|a \Rightarrow a = cq$
 $c|b \Rightarrow b = ch$.

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

Claim: $d|a$.

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 $r < d$. $\downarrow \quad \square$.

$\square$.

Examples

$$\gcd(30, 12) = 6$$

$$(37, 0) = 37$$

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

lem $b \geq a \neq 0$ -4-

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

• Hence $(a, r) \mid (b, a)$ (2)

(1), (2) $\implies (b, a) = (a, r)$

□

Euclidean Algorithm

$b \geq a \neq 0$

• $a \mid b \implies (b, a) = a$

• $a \nmid b$: $b = aq_1 + r_1$ $0 \leq r_1 < a$

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

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

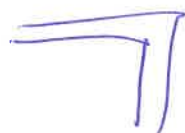
(r_{n-1}, r_n)

$(r_n, 0) = r_n$

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

$\uparrow$
 $\text{gcd}(b, a) = r_n$

Ex) ~~171~~ (171, 30)



- 5 -

$$171 = 5 \cdot 30 + 21$$

$$30 = 1 \cdot 21 + 9$$

$$21 = 2 \cdot 9 + 3$$

$$9 = 3 \cdot 3 + 0$$

$$(\del{30}, 21)$$

"

$$(21, 9)$$

"

$$(9, 3)$$

"

$$(3, 0) = 3$$

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

$$34 = 1 \cdot 21 + 13$$

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

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

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

7 steps

$$\text{Ex) } (1321, 1320) = (1320, 1) = (1, 0) = 0$$

- 6 -

$$1321 = 1 \cdot 1320 + 1$$

2 steps

$$1320 = 1320 \cdot 1 + 0$$