Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

LEC4 Number Theory I 3.1

study of integers 0, 1, 2, 3, ...

Def $m \mid a$ (m divides a) (m: Greastest common factor)

iff $\exists k$, $a = k \cdot m$

ex 3|6 $a = 0 = 0 \cdot m$ $m \mid 0$ ✓

Suppose a-gallon jug, b-gallon jug, $a \le b$

($a = 3$) ($b = 5$)

Theorem $m \mid a$ & $m \mid b$, then $m \mid$ any result that I can get with the pouring and emptying and filling those jugs

State machine

states: pairs (x, y), x = # gal in the "a-jug"

y = # gal in the "b-jug"

start-state: $(0, 0)$

Transitions: & emptying: $(x, y) \to (0, y)$

$(x, y) \to (x, 0)$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

* filling

$(x, y) \to (a, y)$

$(x, y) \to (x, b)$

* pouring

① $(x, y) \to (0, x+y)$, if $x+y \le b$

② $(x, y) \to (x-(b-y), b)$

$= (x+y-b, b)$

$x+y \ge b$

③ $(x, y) \to (x+y, 0)$, $x+y \le a$

④ $(x, y) \to (a, y-(a-x)) = (a, x+y-a)$, $x+y \ge a$

in $a=3$, $b=5$

$(0,0) \to (0,5) \to (3,2) \to (0,2) \to (2,0)$

$\to (2,5) \to (3,4)$

↑ get 4 gal

PF (by induction) Assume $m|a$, $m|b$

invariant: $P(n)$ = "IF (x,y) is the state after n transitions, then $m|x$, $m|y$"

Base case: $(0,0)$, $m|0 \Rightarrow P(0)$ ✓

inductive step: Assume $P(n)$

Suppose that (x,y) state after n transitions

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

P(n) ⇒ m|x and m|y lemma 4.1.3

After another transition$: each of the jugs are filled with either (from state machine)

↓

0, a, b, x, y, x+y-b, x+y-a gallons

m|0, m|a, m|b, m|x, m|y known

⇒ m|x+y-b, m|x+y-a ✓ ⇒ P(n+1) ✓

⇒ P(n), check

4.2 The ~~Great~~ Greatest Common Divisor (factor)

Def gcd(a,b) = greatest common divisor of a and b

ex. a=3, b=5, → gcd(3,5)=1, gcd(52,44)=4

☆ **Def** a and b are relatively prime if gcd(a,b) =1

Coroller: gcd(a,b) | any result |a≤b

Thm Any linear combination (L = sa + tb) of a and b with 0 ≤ L ≤ b can be reached

↑ we want to prove next

ex: 4 = (-2)·3 + 2·5 or 5·3 - 3·5 + 3·3 - 2·5 = 4

s t s' ≥ 0

s' = (s+3) = 5

t' = -4

Mo Tu We Th Fr Sa Su

Memo No.

Date / /

Pf Notice $L = sa + tb = \overbrace{(s+mb)}^{s'}a + \overbrace{(t-ma)}^{t'}b$

So $\exists s' t'$ $L = s'a + t'b$ with $s' > 0$

Assume $0 < L < b$

Algorithm

To obtain L gallons, repeat s' times

- Fill the "a-jug"
- Pour into "b-jug"

when it becomes full, empty it out

and continue pouring until a-jug empty

example as get 4 gallons in (3,5), need repeat 3 tim

↓

First loop $(0,0) \to (3,0) \to (0,3) \to$

second loop $(3,3) \to (\cancel{4},5) \to (1,0) \to (0,1) \to$

second loop $(3,1) \to (0,4)$ getted 4 gallons!

$\Rightarrow$ Filled then 'a-jug' s' times (↓ s' need >0)

Suppose that 'b-jug' is emptyed u times

Let r be the remainder in the 'b-jug'

$(0 \le r \le b, \quad 0 < L < b)$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

so $r = s' \cdot a - u \cdot b$ $\quad L = s'a + t'b$

$\Rightarrow r = \underbrace{s'a + t'b}_{L} - t'b - ub = L - (t'+u)b$

$(t'+u)b$: ↑ integer!

if $t'+u \neq 0 \Rightarrow [r<0 \vee r>b]$, but $0 \leq r \leq b$

$\Rightarrow t'+u = 0 \Rightarrow r = L$ ✓

① $= 2 \cdot 3 - 1 \cdot 5$, so we can reach any gallons ≤ 5

in this case $\gcd(3,5) = 1$ (devisor)

There exists a unique q and r such that $b = qa + r$ with $0 \leq r < a$.

reminder ← rem(b,a)

↑ the quotient

$(b > a)$

Euclid's Alg

≤

lemma: the $\gcd(a,b) = \gcd(\text{rem}(b,a), a)$

$225 = 105 \cdot 2 + 14$

ex:

$\gcd(105, 224) = \gcd(\text{rem}(225, 105), 105)$

$= \gcd(14, 105)$

$= \gcd(\text{rem}(105, 14), 14) = \gcd(7, 14)$

$105 = 7 \cdot 14 + 7$

$= \gcd(\text{rem}(14, 7), 7) = \gcd(0, 7) = 7$

$14 = 7 \cdot 2$

Memo No. _____

Date / /

Pf ① $[m|a \wedge m|b] \Rightarrow [m|b-qa = rem(b,a) \wedge m|a]$

② If $rem(b,a) \neq 0$ then $[m|rem(b,a) = b-qa$ and $m|a] \Rightarrow [m|a \wedge m|b]$

③ If $rem(b,a) = 0 = b-q\cdot a \Rightarrow b = qa \Rightarrow m|b$

$m|a \Rightarrow m|b$, check (lemma)

Thm: gcd(a,b) is a linear combination of a and b

Pf (by induction) euclid's

Invariant: P(n) = "If Euclid's Alg reaches gcd(x,y) after n steps, then x and y are linear combination of a and b, $\Rightarrow$ gcd(a,b) = gcd(x,y).

Base case: P(0) true

Inductive steps: Assume P(n), n+1 steps

Notice that $\exists q$ $rem(y,x) = y-qx$ $m|y-qx$, $rem(y,x)$ $y-qx$ → lin comb of a and b $\Rightarrow$ P(n+1) ✓ (lemma)

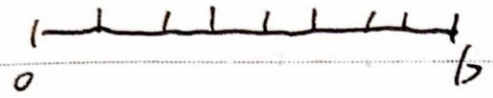
last step gcd(0,y) = y → linear comb of a & b

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

⇒ Thm. gcd(a,b) is actually the smallest positive linear combination of A and B



↑ Theorem 4.2.1 prove by well ordering Principle assume m is the smallest

$m \le \gcd(a,b)$

$\gcd(a,b) \le m$

$m = \gcd(a,b)$

the proof of Euclid's Algorithm

Ex: $\gcd(52,44) = 4 = 6 \cdot 52 + (-7) \cdot 44 = 4$

↑ the smallest positive

Corollary 4.2.2 An integer is linear combination of a and b iff it is a multiple of gcd(a,b)

1. every common divisor of a and b divides gcd(a,b)
2. $\gcd(ka, kb) = k \cdot \gcd(a,b)$ for all $k > 0$
3. if $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, then $\gcd(a, bc) = 1$
4. if $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$
5. $\gcd(a,b) = \gcd(b, \text{rem}(a,b))$.

Any multiply of gcd(a,b) is a linear combination of a and b, $= s \cdot a + t \cdot b$

Mo Tu We Th Fr Sa Su

Memo No. _____

Date / /

Back to LEC 4

text book read 3.2

the way to find $L = s'a + t' \cdot b$

ex: $a = 259$, $b = 70$. find $\gcd(a,b) = s'a + t'b$

a	b	(rem(a,b))	= a − qb
259	70	49	= 259 − 3·70
70	49	21	= 70 − 1·49
			= 70 − (259 − 3·70)
			= 4·70 − 259
49	21	7	= 49 − 2·21
			= ~~49~~ (259 − 3·70) − 2·(4·70 − 259)
21	7		

$\Rightarrow \gcd(a,b) = 7 = 3 \cdot (259) - 11 \cdot (70)$

(0, a, b)

known as "~~the~~ extended Euclidean GCD algorithm"

Summary of Number Theory II

① gcd(a,b) is ~~the least~~ smallest linear comb of a & b

~~go to next page~~

② gcd(a,b) ~~imply~~ multiply any integer is a linear comb of a & b

③ a & b is a relatively prime if gcd(a,b) = 1

④ Remember the Euclid's Alg and extend ↑