Lecture 4 - Number Theory 1

Number Theory 1 ⇒ Study of the integers

Def $m|a$ (m divides a) iff $\exists k \quad a = k \cdot m$

an interesting exception; $0 = 0 = 0 \cdot m$
$m|0$ (any number can divide 0)

Example Problem Suppose a-gallon jug, b-gallon jug $\quad a \le b$
($a=3$) ($b=5$)

Thm $m|a$ and $m|b$, then $m|$ any result

State Machine

States: pairs (x,y), where:
x = # gallons in the a-jug
y = # gallons in the b-jug

start-state: $(0,0)$

Transitions:

*emptying:
- $(x,y) \to (0,y)$
- $(x,y) \to (x,0)$

*Filling:
- $(x,y) \to (a,y)$
- $(x,y) \to (x,b)$

*Pouring:
- $(x,y) \to (0, x+y)$ $(x+y \le b)$
- $(x,y) \to (x-(b-y), b) = (x+y-b, b)$ $(x+y \ge b)$

*Pouring:
- $(x,y) \to (0, x+y)$ $(x+y \le b)$
- $(x,y) \to (x-(b-y), b) = (x+y-b, b)$ $(x+y \ge b)$
- $(x,y) \to (x+y, 0)$ $(x+y \le a)$
- $(x,y) \to (a, y-(a-x)) = (a, x+y-a)$ $(x+y \ge a)$

Ex $a=3, b=5$ $(0,0) \to (0,5) \to (3,2) \to (0,2) \to (2,0) \to (2,5) \to (3,4)$ ||

Proof of Thm. By induction

Assume $m|a$ and $m|b$
Invariant: $P(n) ::=$ "If (x,y) is the state after n transitions, then $m|x$ and $m|y$"

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

Inductive step: Assume $P(n)$
Suppose that (x,y) is the state after n transitions
$P(n) \Rightarrow m|x$ and $m|y$

After another transition, each of the jugs are filled with
$0, a, b, x, y, x+y, x+y-a, x+y-b$ gallons
$m|0, m|a, m|b, m|x, m|y \Rightarrow m$ divides any combinations of these i.e. any of above

This implies $P(n+1)$ is true so we proved the thm. ■

* Can we get 4 gallons by using $a=33$-gallon and $b=55$-gallon jugs
  - a and b are both divisible by 11
  - So any configuration has to be divisible by 11
  - 4 is not divisible by 11

  So no, we can't get 4-gallons by using a and b

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

$a=3, b=5 \rightarrow gcd(a,b)=1$
$gcd(52,44)=4$

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

Thm $m|a$ and $m|b$, then $m|$ any result

cor $gcd(a,b)|$ any result

Thm Any linear combination $L = s\cdot a + t\cdot b$, of a and b with $a \le L \le b$ can be reached.

$4 = (-2)\cdot 3 + 2\cdot 5$
$5\cdot 3 - 3\cdot 5 +$
$3\cdot 3 - 1\cdot 5$
$\rightsquigarrow s' > 0$

Proof Notice $L = sa + tb = (s+mb)a + (t-ma)b$
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

First Loop: $(0,0) \to (3,0) \to (0,3)$

Second Loop: $(0,3) \to (3,3) \to (1,5) \to (1,0) \to (0,1)$

Third Loop: $(0,1) \to (3,1) \to (0,4)$

Let's try to formalize this process

Filled the 'a-Jug' s' times

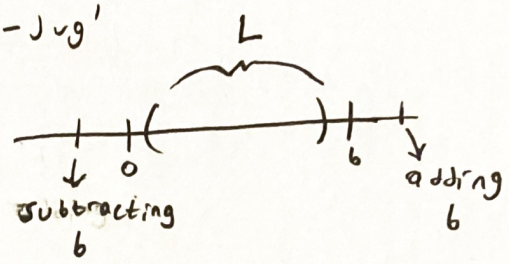
Suppose that 'b-Jug' is emptied u times

Let r be the remainer in the 'b-Jug'

$0 \le r \le b$ $\quad$ $0 < L < b$

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

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



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

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

** There exists a unique q (quotient) and r (remainder (rem(b,a))) such that $b = q.a + r \quad (0 \le r < a)$

Euclid's algorithm

Lemma: $gcd(a,b) = gcd(rem(b,a), a)$

Ex: $gcd(105,224) = gcd(rem(224,105), 105) = gcd(14,105)$ ($224 = 2*105 + 14$)

$= gcd(rem(105,14), 14) = gcd(7,14)$ ($105 = 7 \cdot 14 + 7$)

$= gcd(rem(14,7), 7) = gcd(0,7)$ ($14 = 2*7$)

$= gcd(0,7) = 0$

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

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

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

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

Proof By induction

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

$gcd(x,y) = gcd(a,b)$

Base case: $P(0)$ is true because $x=a$ and $y=b$

Inductive step: Assume $P(n)$

Notice that $\exists q$ $rem(y,x) = y - q \cdot x \rightarrow$ Lin. comb. of a and b

$\Rightarrow P(n+1)$ ✓

Last step $gcd(0,y) = y$

Thm $gcd(a,b)$ is the smallest positive linear combination of a and b