Jan 30th

Euclidean Algorithm
a, b divide a by b with remainder $a = bq + r$
$0 \le r < b$
the set of common divisions of a, b is the same as the set of common divisions of b and r.

$d|a$, $d|b$ $a = dx$ $b = dy \Rightarrow d|r$ also
$r = a - bq = dx - dyq = d(x - yq)$
so if $d|a$ & $d|b \Rightarrow d|r$

conversely, if $d|b$ & $d|r$
$b = dx$, $r = dy$
$a = bq + r = dxq + dy = d(xq + y)$
$\Rightarrow d|a$ & $d|b$
$\Rightarrow \gcd(a,b) = \gcd(b,r)$
① $a = bq + r$ $0 \le r < b$ divide a by b
② $b = rq_1 + r$ $0 \le r_1 < r$ divide b by r
③ $r = r_1 q_2 + r_2$ $0 \le r_2 < r_1$ divide r by r_1
④ $r_1 = r_2 q_3 + r_3$ $0 \le r_3 < r_2$ ...

$\gcd(a,b) = \gcd(b,r) = \gcd(r, r_1) = \gcd(r_1, r_3) = \cdots$
$b > r > r_1 > r_2 > \cdots \rightarrow$ remainders are getting smaller $\Rightarrow$ at some point there will be a zero remainder $r_i = r_{i+1} q_{i+2} + 0$

$\gcd(a,b) = \cdots = \gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, 0) = r_{i+1}$

$\gcd(n, 0) = n$

$\gcd(33, 9) = \gcd(9, 6) = \gcd(6, 3) = \gcd(3, 0)$
$33 = 3 \cdot 9 + 6$
$9 = 1 \cdot 6 + 3$
$6 = 2 \cdot 3 + 0$

Theorem: Given a, b natural numbers there exist integers x, y such that $ax + by = \gcd(a, b)$
ex: $a = 5$, $b = 3$ $\gcd(5, 3) = 1$ can write 1 as $1 = 5x + 3y$
$1 = 5 \times 2 + 3 \times (-3)$

$\gcd(44, 13) = 1$
want x, y s.t. $44x + 13y = 1$

$44 = 3 \cdot 13 + 5$
$13 = 2 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 1 \cdot 2 + 0$

$5 = 44 \cdot 1 + 13 \cdot (-3)$
$3 = 13 \cdot 1 + 5 \cdot (-2)$
$= 13 \cdot 1 + (44 \cdot 1 + 13 \cdot (-3))(-2) = 13 \cdot 7 - 44 \cdot 2$
$2 = 5 \cdot 1 - 3 \cdot 1 = 44(1 + 2) + 13(-3 - 7) = 44 \cdot 3 - 13 \cdot 10$
$1 = 3 \cdot 1 - 2 \cdot 1 = 13 \cdot 7 - 44 \cdot 2 - 44 \cdot 3 + 13 \cdot 10 = 44 \cdot (-5) + 17 \cdot 13$

$\gcd(44, 13) = \gcd(13, 5) = \gcd(5, 3) = \gcd(3, 2) = \gcd(2, 1) = 1$

Cor. if $\gcd(a,b)=1$ $a \mid b\cdot c \Rightarrow a \mid c$

ex: $4 \mid 36 = 3\cdot 12$

$\gcd(4,3)=1 \Rightarrow 4 \mid 12$

Recall: if $a=p$ - prime

Recall if $p \mid bc$ $p \nmid b \Rightarrow p \mid c$

p - prime

this is a special case of the cor. with $a=p$ - prime

p - prime, $p \nmid b \Rightarrow (p,b)=1$

Proof: $\gcd(a,b)=1$ - given $\Rightarrow$

can write 1 as $ax+by=1$ for some integers x,y

$ac\cdot x + b\cdot cy = c = acx + ady = a(cx+dy) \Rightarrow a \mid c$

given $a \mid bc \Rightarrow bc = ad$

HW: $\gcd(a,b)=1$

$a \mid c$, $b \mid c \Rightarrow ab \mid c$

Ex: if $2 \mid c$

$3 \mid c$ $\Rightarrow 2\cdot 3 = 6 \mid c$

Diphantine Equations:

given a,b,c - integers

want to find all integer solutions of $ax+by=c$

$5x+3y=2$, $10x+15y=7$

$10+15y=7$

$\gcd(10,15)=5$

$5 \nmid 7 \Rightarrow$ no integer solutions

$ax+by=c$

if $\gcd(a,b) \nmid c \Rightarrow$

this equation has no solutions, or,

equivalently if $ax+by=c$

has integer solutions $\Rightarrow \gcd(a,b) \mid c$

Now sps $\gcd(a,b) \mid c$ then there is always a solution of $ax+by=c$

Let $d=\gcd(a,b)$

$a = d\tilde{a}$, $b = d\tilde{b}$

$ax+by = d\tilde{a}x + d\tilde{b}y = d(\tilde{a}x+\tilde{b}y) = c$

$\Rightarrow d \mid c$

Let $d \mid c \Rightarrow c = dm$

$d=\gcd(a,b)$

can find x_0, y_0 - integers s.t

$ax_0+by_0 = d = \gcd(a,b)$

$ax_0m + by_0m = dm = c$

(x_0m, y_0m: Solution)

ex: $5x+3y=4$, $\gcd(5,3)=1$

first find x_0, y_0 s.t. $5x_0+3y_0=1$

Say $x_0=-1$, $y_0=2$ works

$4\times\ 5\cdot(-1)+3\cdot(2)=1$

$5\cdot(-1)\cdot 4 + 3\cdot(2)\cdot 4 = 4$

$5\cdot(-4)+3\cdot 8 = 4$

Theorem: $ax+by=c$ has integer solution if and only if $\gcd(a,b) \mid c$

$5x+3y=4$ $\quad x=-4$ $\quad x=-1$ $\quad \dots$

$\quad y=8$ $\quad y=3$ $\quad \dots$

Q: How to find all possible solutions of $ax+by=c$?

Claim: the general solution is
$x = x_0 + bk$
$y = y_0 - ak$
k - any integer

Theorem: $ax+by=c$
if (x_0, y_0) is a solution of $ax+by=c$
$\Rightarrow x_0+kb, y_0-ka$ is also a solution for any integer k

Claim: there are no other solutions
$\gcd(a,b)=1$ $ax_0+by_0=c$
sps $ax_1+bx_1=c$ — another solution
Claim: $x_1=x_0+kb, y_1=y_0-ka$ for some k

WHY?

$ax_0+bx_0=c$
$ax_1+bx_1=c$

$a(x_1-x_0)=b(y_0-y_1)$ $\longrightarrow$ $x_1-x_0=kb$
$\Rightarrow b \mid a(x_1-x_0)$
$\Rightarrow b \mid (x_1-x_0)$
$\Rightarrow x_1-x_0=kb$ for some k
$x_1=x_0+kb$

$akb=b(y_0-y_1)$
$ak=y_0-y_1$
$y_1=y_0-ak$ for some k

Theorem: If $\gcd(a,b)=1$
and (x_0, y_0) is a solution of $ax+by=c$
then the general solution is
$x=x_0+kb$
$y=y_0-ka$ k is any int.

What to do if $\gcd(a,b)\neq 1$?
$ax+by=c$
then if $\gcd(a,b) \nmid c \Rightarrow$ no solutions
and if $\gcd(a,b) \mid c \Rightarrow$ divide the equation by $\gcd(a,b)$ and reduce to the case when a & b are relatively prime

$4x+6y=10$ $\quad 2x+3y=5$

$\gcd(4,6)=2 \mid 10$