Thursday, September 12

Checklist for all group discussions:

- Regular polygon
- Proactive balance
- Respect for differences

Observation: We saw that

(a,b) = smallest possible linear combination $ax+by$ of a and b $(x,y \in \mathbb{Z})$

In particular,

[$(a,b)=1$ if and only if there exist $x,y \in \mathbb{Z}$ such that $ax+by=1$.

Pitfall: for $k \in \mathbb{N}$, there exist $x,y \in \mathbb{Z}$ with $ax+by=k \Leftrightarrow (a,b) \mid k$.

Question: If $a \mid c$ and $b \mid c$, does $ab \mid c$?

No: $a=b=c=3$.

But:

Proposition: If $(a,b)=1$ and $a \mid c$ and $b \mid c$, then $ab \mid c$.

Proof: Write $c = am = bn$, and by Bézout write $ax+by=1$. Then

$$c = c \cdot 1 = c(ax+by)$$
$$= cax + cby$$
$$= (bn)ax + (am)by$$
$$= ab(nx+my), \text{ so } ab \mid c.$$

Thm (*): If $d \mid ab$ and $(d,b)=1$, then $d \mid a$.

Proposition: Suppose $d \mid a$. Then for any $x \in \mathbb{Z}$, we have $d \mid b \iff d \mid (b+ax)$.

Pf:- If $d \mid a$ and $d \mid b$ then $d \mid (b+ax)$ (linear combination)

Also, if $d \mid a$ and $d \mid (b+ax)$ then $d \mid ((b+ax) + a(-x))$. //

Corollary:- The common divisors of a and b are the same as the common divisors of a and $b+ax$.

- In particular $(a,b) = (a, b+ax)$ for any $x \in \mathbb{Z}$.

- Fundamental idea behind Euclidean algorithm:

Example: Let's find gcd of 537 and 105.

- Division algorithm: $537 = 5 \cdot 105 + 12$.
  So $(105, 537) = (105, 537 + 105(-5)) = (105, 12)$.
- Division alg: $105 = 8 \cdot 12 + 9$.
  So $(12, 105) = (12, 105 - 8 \cdot 12) = (12, 9)$.
- Div alg: $12 = 1 \cdot 9 + 3$, so $(9, 12) = (9, 3)$.
- " $9 = 3 \cdot 3 + 0$, so $(3, 9) = (3, 0)$.
- $(n, 0) = |n|$ for any $n \in \mathbb{Z} \setminus \{0\}$.

Can even extend the Euclidean algorithm to "solve" the Bézout equation

$$ax + by = (a, b).$$

Consider the augmented matrix

$\left(\begin{array}{cc|c} 1 & 0 & 537 \\ 0 & 1 & 105 \end{array}\right)$, corresponding to $\begin{array}{l} 1x+0y = 537 \\ 0x+1y = 105. \end{array}$

Solution: $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 537 \\ 105 \end{pmatrix}$.

Elementary row operations preserve the set of solutions:

- subtract $5\times R2$ from $R1$: $\left(\begin{array}{cc|c} 1 & -5 & 12 \\ 0 & 1 & 105 \end{array}\right)$
- subtract $8\times R1$ from $R2$: $\left(\begin{array}{cc|c} 1 & -5 & 12 \\ -8 & 41 & 9 \end{array}\right)$
- subtract $R2$ from $R1$: $\left(\begin{array}{cc|c} 9 & -46 & 3 \\ -8 & 41 & 9 \end{array}\right)$
- subtract $3\times R1$ from $R2$: $\left(\begin{array}{cc|c} 9 & -46 & 3 \\ -35 & 179 & 0 \end{array}\right)$.

equations are

$$\begin{cases} 9x - 46y = 3 & (1) \\ -35x + 179y = 0 & (2) \end{cases}$$

still has solution $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 537 \\ 105 \end{pmatrix}$.

(1): $9\cdot 537 - 46\cdot 105 = 3$

Bézout ☺ $= (537, 105)$

(2) $-35\cdot 537 + 179\cdot 105 = 0$

$\Updownarrow$ LCM(537, 105)

$\frac{179}{35} = \frac{537}{105}$

Convention: a is a divisor of b if

$a > 0$ and $a \mid b$.

Ex: $-2 \mid 6$ but -2 is not a divisor of 6.

Definition: $n \in \mathbb{N}$ is prime if n has exactly 2 divisors. (they are 1 and n)

n is composite if n has at least 3 divisors, or equivalently, n has a divisor d with $1 < d < n$.

- 1 is neither prime nor composite (it's a "unit")

Notation: In this course, p always denotes a prime.

Euclid's lemma: (Let p be prime)

If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Suppose $p \mid ab$ but $p \nmid b$.

Then $(p, b) = 1$; by Theorem (*),

$p \mid a$. //

Abstract algebra aside:

In general rings, we define

- x is irreducible if $y \mid x \Rightarrow y = x$ or $y = 1$ *
- x is prime if $x \mid ab \Rightarrow x \mid a$ or $x \mid b$.

In the ring $\mathbb{Z}$, irreducible $\Rightarrow$ prime.