MATH 437/537
Elementary Number Theory
professor: Greg Martin

Tuesday, September 10, 2024

Notation:
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$
- $\mathbb{N} = \{1, 2, 3, \ldots\}$ "natural numbers"
- $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$

Definition: Let $a, b \in \mathbb{Z}$ with $a \neq 0$.
We say a divides b, and write $a \mid b$, when there exists $c \in \mathbb{Z}$ with $b = ac$.
We also say b is a multiple of a.

Properties: For all $a, b, c \in \mathbb{Z}$ with $a \neq 0$:
- If $a \mid b$ then $-a \mid b$ and $a \mid (-b)$.
- $1 \mid b$ and $a \mid a$ and $a \mid 0$, always.
- If $c \neq 0$ then $a \mid b$ if and only if $ca \mid cb$.
- If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.

Prove: By definition, there exists m and n with $b = am$ and $c = an$.
Then $bx + cy = (am)x + (an)y$
$= a(mx + ny)$.
So $a \mid (bx + cy)$. //

$bx + cy$: integer linear combination of b and c.

- If $a>0$ and $b>0$ and $a|b$, then $a \le b$.
- If $a|b$ and $b|a$, then $a = \pm b$.

Theorem ("Division algorithm"): Let $a \in \mathbb{N}$, $b \in \mathbb{Z}$. There exist unique $q, r \in \mathbb{Z}$ such that:

- $b = aq + r$,
- $0 \le r < a$.

Ex: $a=5$, $b=37$
$37 = 7 \cdot 5 + 2$.
$a=5$, $b=-37$
$-37 = -8 \cdot 5 + 3$.

Corollary: In this notation, $a|b \iff r=0$.

Pf: $\Leftarrow$: If $r=0$, then $b = aq + r = aq$, so $a|b$.

$\Rightarrow$: If $a|b$ then $b = ac + 0$; but then $r=0$ by uniqueness.

Proof of Theorem:

- Existence: Consider

$$R = \{b - an : n \in \mathbb{Z}\} \cap \mathbb{N}_0.$$

R has a least element by well-ordering of $\mathbb{N}_0$; call it r. So $r = b - aq$ for some $q \in \mathbb{Z}$, and $r \ge b$.

If $r \ge a$, then $0 \le r - a < r$ and $r - a = (b - aq) - a = b - a(q+1) \in R$; so $r-a$ would be less than the minimal element of R, contradiction.

Thus $r < a$.

- Uniqueness: Suppose $b = aq + r = aq' + r'$ where $0 \le r' \le r < a$. Then
(WLOG.)

$$r - r' = (b - aq) - (b - aq') = a(q' - q),$$

so $a | (r - r')$.

• Uniqueness: Suppose $b = aq + r = aq' + r'$ where $0 \le r' \le r < a$. (WLOG.) Then

$r - r' = (b - aq) - (b - aq') = a(q' - q)$,

so $a \mid (r - r')$.

But $0 \le r - r' \le r < a$. If $r - r' > 0$ then $a \le (r - r')$, contradiction; hence $r - r' = 0$. Thus $r = r'$ $\therefore$ $q = q'$. //

Definition: Given $a, b \in \mathbb{Z}$, not both 0, their **greatest common divisor** (or gcd) is the largest $d \in \mathbb{N}$ such that $d \mid a$ and $d \mid b$. We write $d = (a, b)$.

Ex: Positive Divisors of 537 are 1, 3, 179, 537

↑ Positive divisors of 105 are 1, 3, 5, 7, 15, 21, 35, 105. Thus $(537, 105) = 3$. ← Note: $9 \cdot 532 + (-48) \cdot 105 = 4833 - 4830 = 3$.

Remark: 1 is always a common divisor, and a has at most $|a|$ positive divisors. Hence the gcd always exists. //

Theorem: Let $a, b \in \mathbb{Z}$, not both 0.

Define $S = \{ax + by : x, y \in \mathbb{Z}\}$.

(1) If $n \in S$ then $(a, b) \mid n$.

(2) (a, b) is the smallest positive element of S.

(3) If $n \in \mathbb{Z}$ and $(a, b) \mid n$, then $n \in S$.

(4) If $c \mid a$ and $c \mid b$ then $c \mid (a, b)$.

Remark:

- (2) $(a, b) = ax + by$ — Bézout's identity
- (1) & (3): $S = \{$all multiples of $(a, b)\}$.

The ideal $\langle a, b \rangle$ in $\mathbb{Z}$ equals $\langle (a, b) \rangle$.

Theorem: Let $a, b \in \mathbb{Z}$, not both 0.

Define $S = \{ax+by : x, y \in \mathbb{Z}\}$.

(1) If $n \in S$ then $(a,b) \mid n$.

(2) (a,b) is the smallest positive element of S.

(3) If $n \in \mathbb{Z}$ and $(a,b) \mid n$, then $n \in S$.

(4) If $c \mid a$ and $c \mid b$ then $c \mid (a,b)$.

Proof: (1) Since $(a,b) \mid a$ and $(a,b) \mid b$, we know (a,b) divides any $ax+by$.

(2) Let $m = \min(S \cap \mathbb{N})$, and write $m = au+bv$. By (1), $(a,b) \mid m$ and so $(a,b) \le m$.

We claim $m \mid a$: by division algorithm, with $0 \le r < m$ ($a = mq+r$). If $m \nmid a$, then $r > 0$. Then

$$r = a - mq = a - (au+bv)q$$
$$= a(1-uq) + b(-vq) \in S.$$

But then $r \in S \cap \mathbb{N}$ would be smaller than the minimal m, contradiction.

So $m \mid a$; in the same way, $m \mid b$.

Thus m is a common divisor of a and b; so $m \le (a,b)$.

Thus $m = (a,b)$.

(3) If $(a,b) \mid n$, then we can write

$$n = (a,b) \cdot c = (au+bv) \cdot c$$
$$= a(uc) + b(vc) \in S.$$

(4) If $c \mid a$ and $c \mid b$, then

$$c \mid (au+bv) = (a,b).$$

Proposition: For $a, b \in \mathbb{Z}$, not both 0, and $m \in \mathbb{N}$: $(ma, mb) = m(a, b)$.

Proof: Set $g = (a, b)$. First, $g \mid a$ implies $mg \mid ma$, and $g \mid b$ implies $mg \mid mb$; so $mg \leq (ma, mb)$. Second, write $g = ax + by$; then

$mg = (ma)x + (mb)y$ is a positive linear combination $\Rightarrow ma$ and mb; then $mg \geq (ma, mb)$ by (2) of the previous theorem.

Corollary: If $m \mid c$ and $m \mid d$, then

$$\left(\frac{c}{m}, \frac{d}{m}\right) = \frac{1}{m}(c, d).$$

In particular,

$$\left(\frac{c}{(c,d)}, \frac{d}{(c,d)}\right) = 1.$$

Ex. $(18, 15) = 3$; and so

$$\left(\frac{18}{3}, \frac{15}{3}\right) = (6, 5) = 1.$$

Note that

$$\left(\frac{18}{(18,15)}, 15\right) = \left(\frac{18}{3}, 15\right)$$

(PITFALL) $= (6, 15) = 3.$

Definition: We say a and b are relatively prime, or coprime, if $(a, b) = 1$.

Proposition: If $(a,n)=1$ and $(b,n)=1$, then $(ab,n)=1$.

Proof: Write (by Bézout)

$$1=(a,n)=au+nv$$

$$1=(b,n)=bx+ny.$$

Then:

$$1=1\cdot 1=(au+nv)(bx+ny)$$

$$=ab(ux)+n(vbx+auy+nvy)$$

So 1 is (the smallest) positive linear combination of ab and n;

hence $1=(ab,n)$. //