Lecture 23, Oct. 24

Woman in Pure Math/Math Finance Lunch

Tuesday 12:30-1:20 MC5417

23.1 Theorem.

1. *if* $b \neq 0$ *and* $a \mid b$ *then* $|a| \leq |b|$
2. $a \mid a$
3. *if* $a \mid b$ *and* $b \mid a$ *then* $a = b$
4. *if* $a \mid b$ *and* $b \mid c$ *then* $a \mid c$
5. *if* $a \mid b$ *and* $a \mid c$ *then*
$$\forall x, y \in \mathbb{Z} \ a \mid (bx + cy)$$

Proof.

1. Let $a, b \in \mathbb{Z}$. Suppose $b \neq 0$ and $a \mid b$. Since $a \mid b$ we can choose $k \in \mathbb{Z}$ so that $b = ak$. Note that $k \neq 0$ because if $k = 0$ then $b = 0$ but $b \neq 0$. Since $k \neq 0$ we have $|k| \geq 1$. So we have
$$\begin{aligned} b =& ak \\ |b| =& |ak| \\ =& |a|\,|k| \\ \geq& |a| \cdot 1 \\ =& |a| \end{aligned}$$
2. Let $a \in \mathbb{Z}$. Since $a = a \cdot 1$, it follows that $a \mid a$.
$$\begin{aligned} \{\forall x \ x \cdot 1 = x\} \vDash& \forall x \ x \cdot 1 = x \\ \vDash& a \cdot 1 = a \\ \vDash& \exists x \ a \cdot x = a \end{aligned}$$
3. Let $a, b \in \mathbb{Z}$. Suppose $a \mid b$ and $b \mid a$. Choose $k \in \mathbb{Z}$ so that $b = ak$. Choose $l \in \mathbb{Z}$ sp that $a = bl$. Then $b = ak = (nl)k = b(lk)$
$$\begin{aligned} b - b(lk) =& 0 \\ b \cdot 1 - b(lk) =& 0 \\ b(1 - lk) =& 0 \end{aligned}$$
So $b = 0$ or $(1 - lk) = 0$ (Since $\mathbb{Z}$ has no zero divisors.)

   Case 1: Suppose $b = 0$, then $a = bl = 0 \cdot l = 0$, so we have $b = a = 0$, hence $b = \pm a$.

   Case 2: Suppose $1 - lk = 0$, then $lk = 1$ and so either $l = k = 1$ or $l = k = -1$. When $l = k = 1$, we have $b = ak = a \cdot 1 = a$, then $b = \pm a$. When $l = k = -1$, we have $b = ak = a(-1) = (-1)a = -a$, then $b = \pm a$.

   In all cases we have $b = \pm a$ as required.

4. $cdots$
5. Let $a, b, c \in \mathbb{Z}$. Suppose $a \mid b$ and $a \mid c$. Say $b = ak$ and $c = al$ with $k, l \in \mathbb{Z}$. Let $x, y \in \mathbb{Z}$.

$$\begin{aligned} bx + cy =& (ak)x + (al)y \\ =& a(kx) + a(ly) \\ =& a(kx + ly) \end{aligned}$$

$\therefore a \mid bx + cy$ as required.

$\square$

Remark. $a \mid b$ means $\exists x\ b = ax$. $a \mid c$ means $\exists x\ c = ax$.

$$\begin{aligned} & [\exists x\ b = ax]_{b \mapsto bx+cy} \\ \equiv & [\exists u\ b = au]_{b \mapsto bx+cy} \\ \equiv & \exists u\ (bx + cy) = au \end{aligned}$$

$a \mid (bx + cy)$ means $\exists u\ (bx + cy) = au$

Remark. Recall that when $b \neq 0$, if $a \mid b$ then $|a| \leq |b|$. So b has finitely many divisors (and the greatest divisor is $|b|$).

23.2 Definition. For $a, b, d \in \mathbb{Z}$, we say that d is a **common divisor** of a and b when $d \mid a$ and $d \mid b$. When a and b are not both zero, there are only finitely many common divisor of a and b, and ± 1 are common divisors, so a and b do have a greatest common divisor and we denote it by $gcd(a, b)$.

For convenience, we also write $gcd(0, 0) = 0$

23.3 Theorem. (Properties of the GCD) *Let $a, b, c \in \mathbb{Z}$.*

1. $gcd(a, b) = gcd(b, a)$
2. $gcd(a, b) = gcd(|a|, |b|)$
3. *if $a \mid b$ then $gcd(a, b) = |a|$, in particular, $gcd(a, 0) = |a|$*
4. $gcd(a, b) = gcd(a + tb, b)$ *for all $t \in \mathbb{Z}$.*
5. *if $a = qb + r$ where $q, r \in \mathbb{Z}$, then $gcd(a, b) = gcd(b, r)$*

Proof. 4 To show that $gcd(a, b) = gcd(a + tb, b)$ we shall show that the common divisor of a and b is exactly the same as the common divisor of $a + tb$ and b.

Let $a, b, t \in \mathbb{Z}$. Let $d \in \mathbb{Z}$. Suppose $d \mid a$ and $d \mid b$ then $d \mid ax + by$ for all $x, y \in \mathbb{Z}$. In particular, $d \mid (a \cdot 1 + bt)$, so $d \mid (a + td)$. Thus $d \mid (a + tb)$ and $d \mid b$.

Conversely, suppose $d \mid (a + tb)$ and $d \mid b$. Then $d \mid (a + tb)x + by$ for all $x, y \in \mathbb{Z}$. In particular, $d \mid (a + tb) \cdot 1 + b \cdot (-1)$, so $d \mid a$. Thus $d \mid a$ and $d \mid a$.

$\square$