Lecture 27: Pigeonhole and divisibility

Monday, November 28, 2016 6:08 PM

<u>Recall</u>. For any $n \in \mathbb{Z}^+$, $a \in \mathbb{Z}$, there is a unique $r \in \{0, 1, \cdots, n-1\}$ such $a \equiv r \pmod{n}$.

<u>Problem</u>. For any $k_1, \ldots, k_{n+1} \in \mathbb{Z}$, there are $i \neq j$ such that

$$n \mid k_i - k_j.$$

<u>Solution</u>. For any i, let r_i be the remainder of k_i divided by n. So

① $k_i \overset{n}{\equiv} r_i$,

② $r_i \in \{0, 1, \cdots, n-1\}$.

Since $r_1, r_2, \cdots, r_{n+1} \in \underbrace{\{0, 1, \cdots, n-1\}}_{n \text{ possible numbers}}$, by the pigeonhole principle there are $i \neq j$ such that $r_i = r_j$.

Hence $k_i \overset{n}{\equiv} r_i = r_j \overset{n}{\equiv} k_j$, which implies $k_i \overset{n}{\equiv} k_j$. So $n \mid k_i - k_j$. ■

<u>Corollary</u>. For any $k_1, k_2, k_3 \in \mathbb{Z}$, we have

$$2 \mid (k_1 - k_2)(k_2 - k_3)(k_3 - k_1).$$

<u>Proof</u>. Using the previous problem for $n = 3$ we get that $\exists\, i \neq j$, $2 \mid k_i - k_j$. Hence $2 \mid (k_1 - k_2)(k_2 - k_3)(k_3 - k_1)$. ■

Lecture 27: gcd of two integers

Monday, November 28, 2016 6:19 PM

Definition. Let a and b be two integers such that at least one of them is non-zero. The greatest common divisor of a and b is denoted by $\gcd(a,b)$. So, if $d = \gcd(a,b)$, then

- $d \mid a$ and $d \mid b$ (d is a common divisor of a and b)
- $\left.\begin{array}{l} d' \mid a \\ d' \mid b \end{array}\right\} \Rightarrow d' \leq d$ (Any common divisor of a and b is at most d.)

Recall. If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

Lemma. For any non-zero integers a and b we have

$$1 \leq \gcd(a,b) \leq \min\{|a|, |b|\}$$

Proof. $1 \mid a$ and $1 \mid b \Rightarrow 1 \leq \gcd(a,b)$.

- Let $d = \gcd(a,b)$. So $1 \leq d$, and hence $|d| = d$.

$$\left.\begin{array}{l} \left.\begin{array}{l} d \mid a \\ a \neq 0 \end{array}\right\} \Rightarrow |d| \leq |a| \\ \left.\begin{array}{l} d \mid b \\ b \neq 0 \end{array}\right\} \Rightarrow |d| \leq |b| \end{array}\right\} \Rightarrow d = |d| \leq \min\{|a|, |b|\}.$$

■

Lecture 27: gcd and integer linear combination

Monday, November 28, 2016 6:33 PM

The following is one of the most important results that would be proved in this class:

Theorem. Let a and b be positive integers. Then there are integers r and s such that $\gcd(a,b) = ra+sb$.

Proof. In the proof we use the well-ordering principle:

If S is a non-empty subset of $\mathbb{Z}^+$, then S has a minimum.

Let $S = \{n \in \mathbb{Z}^+ \mid \exists x, y \in \mathbb{Z}, \ n = ax+by\}$. Notice that $a = a(1)+b(0) > 0$, so $a \in S$ and $S \neq \emptyset$. Hence by the well-ordering principle, S has the minimum. Let $d' = \min S$, and $d = \gcd(a,b)$. It is enough to prove $d = d'$.

Step 1. $d \le d'$.

Proof of step 1. Since $d' \in S$, there are $r, s \in \mathbb{Z}$ such that $d' = ra+sb$. On the other hand, $d = \gcd(a,b)$ is a common divisor of a and b. So

$$\left.\begin{array}{l} d \mid a \\ d \mid b \end{array}\right\} \Rightarrow d \mid ra+sb = d'$$

$$(d \mid d' \text{ and } d', d > 0) \Rightarrow d \le d'.$$

Lecture 27: gcd and integer linear combination

Thursday, December 1, 2016 9:40 PM

Step 2. $d' \leq d$.

Proof of step 2. To show this, it is enough to show d' is a common divisor of a and b since d is the greatest common divisor of a and b.

By symmetry it is enough to show $d' \mid a$. (By symmetry here means that by a similar argument one can get $d' \mid b$.)

Proof of $d' \mid a$. Suppose to the contrary that $d' \nmid a$. Let r be the remainder of a divided by d'. So for some $q \in \mathbb{Z}$, $a = d'q + r$ and $0 \leq r < d'$. Since $d' \nmid a$ (by the contrary assumption), $r \neq 0$. Hence

$$0 < r < d' \quad \text{and} \quad r = a - d'q = a - (ra + sb)q$$
$$= (1 - rq)a - (sq)b.$$

Therefore r is an integer linear combination of a and b, and r is positive. So $r \in S$. Thus $r \geq \min S = d'$ which contradicts $r < d'$. ■

Lecture 27: Some properties of gcd

Thursday, December 1, 2016 9:52 PM

<u>Corollary 1</u>. For any $a, b \in \mathbb{Z}^+$,

$$\left.\begin{array}{l} d \mid a \\ d \mid b \end{array}\right\} \Rightarrow d \mid \gcd(a,b).$$

<u>Proof</u>. By the previous theorem, there are integers r and s such that $\gcd(a,b) = ra + sb$.

$$\left.\begin{array}{l} d \mid a \\ d \mid b \end{array}\right\} \Rightarrow d \mid ra+sb \Rightarrow d \mid \gcd(a,b). \qquad \blacksquare$$

<u>Corollary 2</u>. For any $a, b, c \in \mathbb{Z}^+$,

$$\left.\begin{array}{l} a \mid bc \\ \gcd(a,b) = 1 \end{array}\right\} \Rightarrow a \mid c.$$

<u>Proof</u>.

By the previous theorem, there are integers r and s such that $ra + sb = 1$. Therefore $rac + sbc = c$.

$$\left.\begin{array}{l} a \mid a \\ a \mid bc \end{array}\right\} \Rightarrow a \mid (rc)\,a + (s)\,bc = c. \qquad \blacksquare$$