21 January 2021 10:22

Alg-2

HW $\begin{matrix} \text{pg} - 1 \\ \text{p13} - 1 \end{matrix}$ } Due 1/28

Grading

HW — 100
Midterm — 100
Final — 200
400

$85\% \leq A$
$75\% \leq B < 85\%$
$60\% \leq C < 75\%$
$50\% \leq D < 60\%$
$F < 50\%$

Three famous impossibilities

1. Doubling a cube (Delian Prob) No
2. Squaring a circle (1882) 1837
3. trisecting an arbitrary angle Gauss 60° No

using a ruler and a compass.

π is transcendental (not algebraic)

$\alpha \in \mathbb{C}$ is algebraic iff

$\alpha \in \mathbb{C}$ is algebraic iff $\exists\ p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_0, \ldots, a_n \in \mathbb{Z}$ s.t. $p(\alpha) = 0$, the smallest n is called the deg of α

Ex $\sqrt{2}$ is alg of deg 2.

$p(x) = x^2 - 2$ has $\sqrt{2}$.

Th. e is transcendental (Hermite 1872)

A $n \times n$ matrix B is

Hermitian $B^* = B$

$$B^* = \overline{B}^t = \overline{B^t}$$

WOP $\Rightarrow$ Ind. 1st form $\Rightarrow$ Ind. 2nd form $\Rightarrow$ WOP

WOP is false for $\mathbb{Z}$

Assume Induction 2nd form

to prove WOP: $\emptyset \neq S \subseteq \mathbb{Z}_+$

Want to prove that S has a least element

Suppose there $S \subseteq \mathbb{Z}_+$ without a least element. Want to show

suppose ...
a least element. Want to show
$S = \phi$.

$$T = S^c \cap \mathbb{Z}_+ = S^c = \{x \in \mathbb{Z}_+ : x \notin S\}$$

$0 \in T$ (?) $T \subseteq \mathbb{Z}_+ = T \cup S$

otherwise $0 \in S \Rightarrow 0$ is a least element.

Assume $\{0, 1, \ldots n-1\} \subseteq T$ for $n \in \mathbb{N}$

then $n \in T$, otherwise $n \in S$
& will be the smallest element of S

By 2nd form of induction

$$T = \mathbb{Z}_+$$

$\Rightarrow S = \phi$, proving our claim

WOP

Induction 1st form

$S \subseteq \mathbb{N}$ with (i) $1 \in S$
(ii) $n \in S \Rightarrow n+1 \in S$

then $S = \mathbb{N}$.

then $S = \mathbb{N}$.

2nd form of Induction: $S \subseteq \mathbb{N}$

s.t. (i) $1 \in S$

(2) $\{1, \dots, n\} \subseteq S$

$\Rightarrow n+1 \in S$

then $S = \mathbb{N}$

$\alpha \in \mathbb{C}$ is algebraic number.

then $\deg \alpha \in \mathbb{N}$ exists

Division Algorithm

Euclidean Algorithm

Thm (i) $m, n \in \mathbb{Z}$, $m > 0$, then

$\exists\ q \in \mathbb{Z}$ & $r \in \mathbb{Z}$ s.t.

$n = mq + r$.

(ii) m, r are unique if $0 \le r < m$

---

q is called quotient &

r is called remainder.

Ex $m = 3$, $n = -14$

$-14 = (-4) \cdot 3 - 2 \Rightarrow q = -4, \quad r = -2$

$= (-5 \cdot 3) + 1 \Rightarrow q = -5, \quad r = 1.$

Ex $m=3, \quad n=-14$

$-14 = (-4)\cdot 3 - 2 \Rightarrow q=-4, \quad r=-2$

$= (-5\cdot 3) + 1 \Rightarrow q=-5, \quad r=1.$

(iii) $m \neq 0$, $m, n \in \mathbb{Z}$, $\exists!\ q, r \in \mathbb{Z}$ s.t. $n = qm + r$, where $0 \leq r < |m|$

$$|m| = \begin{cases} m & \text{if } m \geq 0, \text{ integer} \\ -m & \text{if } m < 0 \end{cases}$$

Proof: Let $S = \{n - qm \geq 0 : q \in \mathbb{Z}\} \subseteq \mathbb{Z}_+$.

Claim $S \neq \phi$. If $0 \in S$ done. Otherwise, since $m > 0$

$m \geq 1 \Rightarrow |n| \leq |n|m$

and $m|n| \geq |n| \geq -n$

$\Rightarrow n + |n|m \geq 0$ i.e. $n - (-|n|)m \in S$

$q = -|n|$

$\phi \neq S \subseteq \mathbb{Z}_+$, so by WOP, $\exists$ $r \in S$ s.t. $r \leq s$ $\forall s \in S$

Then $0 \leq r = n - qm$ for some $q \in \mathbb{Z}$.

Then $0 \le r = n - qm$ "

$n = qm + r$.

Suppose $0 \le r < m$ &

$n = q_i m + r_i \quad i = 1, 2$ &

$0 \le r_i < m$

$n = q_1 m + r_1 \quad (1)$

$= q_2 m + r_2 \quad (2)$

Assume $r_1 \neq r_2$, say $0 \le r_1 < r_2$

Subtracting (1) from the (2) we

get $0 = (q_2 - q_1)m + (r_2 - r_1)$

$(q_1 - q_2)m = r_2 - r_1 > 0$

$\Downarrow$

$q_1 - q_2 > 0$ as $m > 0$

$\Rightarrow q_1 - q_2 \ge 1 \Rightarrow (q_1 - q_2)m \ge m$.

$0 \le r_1 < m \quad , -m < -r_1 \le 0$

$0 \le r_2 < m \qquad 0 \le r_2 < m$

$\Rightarrow -m < r_2 - r_1 < m$.

Also $r_2 - r_1 = (q_1 - q_2)m \ge m > r_2 - r_1$

$\Rightarrow$

$r_2 - r_1$ - (1) (2)

a contradiction $\Rightarrow$

$r_1 = r_2$

then $r_2 - r_1 = (q_1 - q_2)m$

$\Rightarrow q_1 - q_2 = 0 \Rightarrow q_1 = q_2$

(iii) $m, n \in \mathbb{Z}$. $m \neq 0$ $\exists! q, r$

s.t. $n = mq + r$, $0 \leq r < |m|$

Proof. For n, $|m|$ we have uniq

(2) $\exists!\ q_1, r$ s.t. $n = q_1|m| + r$

$0 \leq r < |m|$

Take $q = -q_1$, $n = qm + r$.

(If $m > 0$ it is (ii))

If $m < 0$, then $|m| = -m$

and $n = q_1|m| + r$

$= -q_1 m + r$, $0 \leq r < |m|$

$= qm + r$

Arithmetic of $\mathbb{Z}$.

Let $n, d \in \mathbb{Z} - \{0\}$

Def (1) d divides n, denoted $d \mid n$

iff $n = qd$ for some $q \in \mathbb{Z}$.

iff $n = qd$ for some $q \in \mathbb{Z}$.
d is also called a divisor of n.

(2) $m, n \in \mathbb{Z} - \{0\}$, $d \in \mathbb{Z} - \{0\}$
is a common divisor of m & n
iff $d \mid m \wedge d \mid n$.

(3) The greatest common divisor of
$m, n \in \mathbb{Z} - \{0\}$. denoted $gcd(m,n)$
$\in \mathbb{N} \ni d =$
iff (1) $d \mid m \wedge d \mid m$
and (2) if $c \in \mathbb{N}$ and
$c \mid m$ and $c \mid m$
then $c \mid d$ $(d \geq c)$

(4) $\ell \in \mathbb{Z} - \{0\}$ is the least common
multiple of $m, n \in \mathbb{Z} - \{0\}$,
denoted $\ell = lcm(m,n)$ iff
(i) $m \mid \ell$ and $n \mid \ell$
(ii) if $m \mid k$ and $n \mid k$ for
some $k \in \mathbb{Z} - \{0\}$
then $\ell \mid k$.

Question: Does $gcd(m,n)$ exist?

Question: Does gcd(m,n) exist ?

Ans Yes.

Thm $m, n \in \mathbb{Z} - \{0\}$. Then $\exists\, d \in \mathbb{N}$ s.t. $d = \gcd(m,n)$.

$d = 1$, then m & n are called relatively prime

Need a lemma & a defn:

Def. $J \subseteq \mathbb{Z}$ is called an ideal iff

(1) $m - n \in J \;\forall\; m, n \in J$

(2) $r \in J,\ m \in \mathbb{Z} \Rightarrow rm \in J$

or

(i) $0 \in J$

(ii) $m + n \in J \;\forall\; m, n \in J$

(iii) $rm \in J \;\forall\; r \in J \;\forall m \in \mathbb{Z}$.

Ex. Let $m_1, \ldots, m_r \in \mathbb{Z}$

$$J = \left\{ \sum_{i=1}^{r} x_i m_i : x_1, \ldots x_r \in \mathbb{Z} \right\}$$

$$= (m_1, \ldots m_r) = \langle m_1, \ldots m_r \rangle$$

$$= \{ x_1 m_1 + x_2 m_2 + \cdots + x_n m_n : x_1, \ldots x_n \in \mathbb{Z} \}$$

J is an ideal

J is an ideal

proof (1) $0 \in J$, take $x_1 = 0 \cdot 0 = x_r$

(2) $a \in J$, $b \in J$

$a = x_1 m_1 + \cdots + x_r m_r$, $x_1 \cdots x_r \in \mathbb{Z}$

$b = y_1 m_1 + \cdots + y_r m_r$, $y_1 \cdots y_r$

$a + b = (x_1 + y_1) m_1 + \cdots + (x_r + y_r) m_n \in J$

$s \in \mathbb{Z}$, $a \in J$

$sa = s(x_1 m_1 + \cdots + x_r m_r)$

$= (sx_1) m_1 + \cdots + (sx_r) m_r \in J$

$\Rightarrow$ J is an ideal of $\mathbb{Z}$, i.e. subring

(in ch 3 for more

Ex $J = \{0\}$ is a ring, called the zero ring

2 $\mathbb{Z} = J$ is an ideal is generated by 1

Def $J = \left\{ \sum_{j=1}^{r} x_j m_j : x_1 \cdots x_r \in \mathbb{Z} \right\}$

is an ideal & the set $\{m_1 \cdots m_r\}$ is called a generators for J or of J.

Thm $m, n \in \mathbb{Z} - \{0\}$

$J = \langle m, n \rangle = \{ am + bn : a, b \in \mathbb{Z} \}$

$\cdots \quad \gcd(m, n) \leq t.$

$J = \langle m, n, \ldots \rangle$

Then $\exists\ d \in \mathbb{N}$ s.t.
$J = \langle d \rangle$

More generally

Thm Let $J \subseteq \mathbb{Z}$ be an ideal
then $\exists\ d \in \mathbb{Z}_+$ s.t.
$J = \langle d \rangle$

Or $J \neq \{0\}$, $\exists\ d \geq 1$ intgrs
s.t. $J = \langle d \rangle$

Proof If $J = \{0\}$. take $d = 0$
$J = \langle 0 \rangle = \{m \cdot 0 : m \in \mathbb{Z}\}$

Assume $J \neq \{0\}$ ideal. Then
$\exists\ n \in J$ s.t. $n \neq 0$,

$\{0\} \subsetneq J$ ($A \subseteq B$
means $a \in A \Rightarrow a \in B$
$A \subsetneq B$, $\exists b \in B$
s.t $b \notin A$)

Can assume $n \in J$ is positive
if $n < 0$, $-n > 0$ &
$-n = (-1)n \in J$

So $S = J \cap \mathbb{N}$ is

nonempty as $n \in S$ &

$S \subseteq \mathbb{N}$. So by WOP

$\exists\ d \in S$ & smallest i.e.

$d \leq s\ \forall\ s \in J \cap \mathbb{N} = S$

To show $J = \langle d \rangle$.

$md \in \langle d \rangle \Rightarrow md \in J$

as J is an ideal

& $m \in \mathbb{Z}$

$\langle d \rangle \subseteq J$

Let $m \in J$ & can take $m > 0$

$m \in J \cap \mathbb{N} = S$

By division alg. $m = qd + r$.

$0 \leq r < d$

Now $r = m - qd \in S$

Since d is smallest

$r = 0 \Rightarrow m = qd$

$\Rightarrow J \subseteq \langle d \rangle$ &

hence $J = \langle d \rangle$.

Every ideal of J is generated by a single element i.e. a principle ideal of $\mathbb{Z}$. ($J = \langle d \rangle$)

Thm $J = \langle m_1 \cdots m_r \rangle$

$= \langle d \rangle$

then $d \mid m_i$, $i = 1 \cdots r$

& if $c \mid m_i$, $i = 1 \cdots r$

then $c \mid d$.

ie. $d = \gcd(m_1 \cdots m_r)$

Proof $m_i \in J$ as $m_i = 0m_1 + 0m_2 + \cdots + 1m_i + 0m_{i+1} + 0m_r$

$\Rightarrow m_i \in \langle d \rangle$ ie. $m_i = q_i d$

$\Rightarrow d \mid m_i$

Also $d \in J = \langle m_1 \cdots m_r$

so $d = x_1 m_1 + \cdots + x_r m_r$.

for some $x_1 \cdots x_r \in \mathbb{Z}$

Suppose $c \mid m_i$, then

$m_i = q_i c$ for some $q_i \in \mathbb{Z}$

$$d = \sum_{i=1}^{r} x_i m_i = \sum_{i=1}^{r} x_i (q_i c)$$

$$= \left(\sum x_i q_i \right) c$$

$\Rightarrow c \mid d$.

Thus given $m, n \in \mathbb{Z} - \{0\}$
$d = \gcd(m,n)$ exists in $\mathbb{N}$
& $d = am + bn$ for some
$a, b \in \mathbb{Z}$.

Ex Find the gcd of 78 and 326 &
write as $a78 + b326$

Sol $d = \gcd(78, 326)$
$= a78 + b326$.

$78 \overline{)326}\ 4$, 312, 14

$326 = 4 \cdot 78 + 14$ (1)
$78 = 5 \cdot 14 + 8$ (2)
$14 = 1 \cdot 8 + 6$ (3)
$8 = 1 \cdot 6 + 2$ (4)

$6 = 3 \cdot 2$

$2 = \gcd(78, 326)$

from (4) $2 = 8 - (1) \cdot 6$ from (4)
$= 8 - (1)(14 - 1 \cdot 8)$ from (3)
$= 2 \cdot 8 - 1 \cdot 14$
$= 2(78 - 5 \cdot 14) - 14$ from (2)
$= 11 \cdot 14$

$= 2.78 - 11.14$

$= 2.78 - 11(326 - 4.78)$

$= (146)78 - 11.326$

$a = 46, \quad b = -11$

$15 = 3.5$

$8 = 2.2.2$

$10 = 2.5$

Freshman's Dream thm

$$(x+y)^p = x^p + y^p \pmod{p}$$

Cell

718-688-9445