Today's plan is to review for midterm on Monday

You may bring 1 $8\frac{1}{2} \times 11$ sheet of paper, written on 1 side only

No calculators, phones, etc.

Bring a blue book or enough blank paper to write on.

Today I will reveal my secret method for writing exams, this will not be in the notes!

$a, b \in \mathbb{Z}$ $\gcd(a,b)$ = greatest common divisor

$$\gcd(a,b) = \max\{c > 0 : c \in \mathbb{Z},\ c \mid a \text{ and } c \mid b\}$$
$$= \min\{as + bt > 0 : s, t \in \mathbb{Z}\}$$

Ex 1. Find $\gcd(2^3 \times 5^{10} \times 7^{11},\ 2^2 \times 5^5 \times 11^{14})$

Ans: $2^2 \times 5^5$

Ex 2. Find $\gcd(123, 55)$

Ans: $55 = 5 \times 11$, $5 \nmid 123$, $11 \nmid 123$

$\therefore \gcd(123, 55) = 1.$

Ex 3. Find s, t so that $123s + 55t = 1$

Ans There is a method to do this, using the division algorithm:

$$123 = 2 \times 55 + 13 \quad (*)$$
$$55 = 4 \times 13 + 3 \quad (**)$$
$$55 = 18 \times 3 + 1 \quad (***)$$

Now substitute back!

$123 \times 4 = 2 \times 4 \times 55 + 4 \times 13$ by (*) mult. by 4

$123 \times 4 = 8 \times 55 + 55 - 3$ by subst. (**)

$123 \times 4 = 9 \times 55 - 3$

$123 \times 4 \times 18 = 55(9 \times 18) - 3 \times 18$ mult by 18

$123 \times 4 \times 18 = 55(9 \times 18) + 1 - 55$ by subst. (**)

$123 \times 4 \times 18 = 55(9 \times 18 - 1) + 1$

$\therefore$ may take $s = +4 \times 18$

$t = -9 \times 18 + 1$

to get $123s + 55t = 1$

other methods will also work!

Modular arithmetic

Ex 1. Find $5^{1001} \bmod 26$ (without consulting Google)

Ans. Look for some trick!

$5^2 = 25$ & $25 \bmod 26 = 26 - 1$

so $5^{1001} \bmod 26 = (5^2)^{500} \cdot 5 \bmod 26$

$= (-1)^{500} \cdot 5 \bmod 26 = 5$

Ex 2. A USPS money order has id #
1020305078
Find its check digit

Ans: $1020305078 \bmod 9$

$= 1+2+3+5+7+8 \bmod 9$ since $10^n \bmod 9 = 1$

$= 8$

Ex 3. Does the check digit detect all errors in which exactly 1 digit is copied wrong? If not, give example.

Ans. 1920305078 has same check digit, so error will not be detected.

Ex 4 Show that $\{1,2,3,4,5,6,7,8,9\}$ is not a group under multiplication mod 10

Ans. Some numbers have no inverse mod 10

e.g. 2. Suppose $2x \bmod 10 = 1$

Then $10x \bmod 10 = 5$,

which is impossible, since

$10x \bmod 10 = 0$,

Equivalence relations

Ex 1 $\mathbb{R}^*$ nonzero real numbers.

Put aRb if $ab > 0$. Prove that R is an equivalence relation

Ans. $ab > 0 \iff a > 0 \text{ \& } b > 0$ or $a < 0, b < 0$.

Reflexive $a^2 > 0 \ \forall \ a \in \mathbb{R}^* \ \therefore \ aRa$

Symmetric. $ab > 0 \iff ba > 0$

Transitive a, b, c if $ab > 0$ & $bc > 0$

Then either a, b, c are all > 0

or a, b, c are all < 0.

$\therefore \ ac > 0$.

$\therefore$ R is an equiv. relation on $\mathbb{R}^*$

Ex 2. What are the equiv classes in Ex 1?

Ans. $[1]$ & $[-1]$

If $a > 0$, then $a \cdot 1 > 0$ so $aR1$

If $a < 0$ then $a(-1) > 0$ so $aR(-1)$.

Ex 3. For $\mathbb{Z}$, put aRb if $ab \geq 0$. Is R an equivalence relation?

Ans. No $a \cdot 0 = 0 \ \forall \ a \ \therefore \ aR0 \ \forall \ a$.

By transitivity, $aRb \ \forall \ a, b \in \mathbb{Z}$. But if $a > 0, b < 0$, then $ab < 0$. (if R were an equiv. relation)

D_n as a group.

Ex 1. If R is a rotation, and F is a reflection in D_n, prove that

$$FRF = R^{-1}$$

Ans. $FRF = R^{-1} \iff FRFR = I = R_0$

Since FR is a reflection, $(FR)^2 = I$

$\therefore FRFR = I$

Ex 2. In D_4, simplify $FR^{-2}FR^5$, R, F as in Ex 1.

Ans.
$$\begin{aligned} FR^{-2}FR^5 &= FR^2FR \quad \text{since } R^4 = I \text{ in } D_4 \text{ \& } R^{-2} = R^2 \\ &= FRF\,FRFR \\ &= (FRF)(FRF)R \\ &= R^{-2}R \quad \text{by Ex. 1} \\ &= R^{-1} \end{aligned}$$

Ex 1. Find $|GL(2, \mathbb{Z}_2)|$ $\mathbb{Z}_2 = \{0, 1\}$ addition mod 2

Ans. Entries are all 0 or 1

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0 \iff a = d = 1 \text{ or } b = c = 1$$

but not both

$\begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}1&1\\1&0\end{bmatrix}, \begin{bmatrix}1&0\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&0\end{bmatrix}, \begin{bmatrix}1&1\\0&1\end{bmatrix}, \begin{bmatrix}0&1\\1&1\end{bmatrix}$

at most 3 ones

$$|GL(2, \mathbb{Z}_2)| = 6$$

Ex 2. Find $\left|\begin{bmatrix}1&1\\1&0\end{bmatrix}\right|$

Ans. $\begin{bmatrix}1&1\\1&0\end{bmatrix}\begin{bmatrix}1&1\\1&0\end{bmatrix} = \begin{bmatrix}0&1\\1&1\end{bmatrix}$

$$\begin{bmatrix}1&1\\1&0\end{bmatrix}^3 = \begin{bmatrix}0&1\\1&1\end{bmatrix}\begin{bmatrix}1&1\\1&0\end{bmatrix} = \begin{bmatrix}1&0\\0&1\end{bmatrix}$$

$$\therefore \left|\begin{bmatrix}1&1\\1&0\end{bmatrix}\right| = 3.$$

Ex. Prove that if G is a group, and $x, y \in G$ with $x^2 = y^2 = (xy)^2 = e$, then $xy = yx$.

Ans.

$y^2 = e \Leftrightarrow y = y^{-1}$

$x^2 = e \Leftrightarrow x = x^{-1}$

$(xy)^2 = e$

$\Rightarrow xyxy = e$

$yxy = x^{-1} = x$

$xy = y^{-1}x = yx$