SOLUTION TO PROBLEMS 13 – 16 (LECTURE 4 PROBLEM SET)

P13 (a.) use Euclidean Algo. to find gcd(1234, 542)

$$1234 = 2(542) + 150$$
$$542 = 3(150) + 92$$
$$150 = 1(92) + 58$$
$$92 = 1(58) + 34$$
$$58 = 1(34) + 24$$
$$34 = 1(24) + 10$$
$$24 = 2(10) + 4$$
$$10 = 2(4) + \boxed{2} \leftarrow \boxed{\gcd(1234, 542)}$$
$$4 = 2(2)$$

(b.) $1001 = 18(53) + 47$

$$53 = 1(47) + 6$$
$$47 = 7(6) + 5$$
$$6 = 1(5) + \boxed{1} \leftarrow \gcd(1001, 53) = 1.$$
$$5 = 1(5)$$

$$\begin{aligned} 1 = 6 - 5 &= 6 - [47 - 7(6)] \\ &= -47 + 8(53 - 47) \\ &= 8(53) - 9(47) \\ &= 8(53) - 9[1001 - 18(53)] \\ &= 170(53) - 9(1001) \end{aligned}$$

Thus $\boxed{1 = 1001(-9) + 53(170) \quad (x = -9,\ y = 170)}$

(c.) $1000 = 9(111) + 1$ thus $1 = 9(-111) + 1000$

$\Rightarrow 9^{-1} = -111$ as $1000 \equiv 0 \mod 1000$

$\Rightarrow \boxed{9^{-1} = 889}$

PROBLEM 14

Let $d = \gcd(a,b)$. If $a = da'$ and $b = db'$ then show $\gcd(a', b') = 1$

By Bezout's Identity, $\exists x, y \in \mathbb{Z}$ for which $ax + by = d$. If $a = da'$ and $b = db'$ then

$$da'x + db'y = d \Rightarrow a'x + b'y = 1 \overset{*)}{\Rightarrow} \gcd(a', b') = 1.$$

(*) Suppose a', b' have common divisor $k > 1$ then $a' = ka''$ and $b' = kb''$. thus

$$ka''x + kb''y = 1 \Rightarrow k(a''x + b''y) = 1$$

But, $k > 1 \Rightarrow a''x + b''y \notin \mathbb{Z}$ which is impossible.

Thus $k \not> 1$ and we find $\gcd(a', b') = 1$.

Remark: the argument (*) can be invoked whenever we have $ax + by = 1$ for $a, b, x, y \in \mathbb{Z}$ it follows $\gcd(a,b) = 1$ or $\gcd(x,y) = 1$ etc...

PROBLEM 15

$$X = (a_k \cdots a_2 a_1 a_0) = a_0 + a_1 \times 10 + a_2 \times 10^2 + \cdots + a_k \times 10^k$$

But, notice $9 / X$ iff $X = 9j$ for some $j \in \mathbb{Z}$ which means $9 | X$ iff $X \equiv 0$ modulo 9.

Notice, $10 \equiv 1 \mod 9 \Rightarrow 10^j \equiv 1 \mod 9$ for $j = 1, 2, \ldots$

Hence
$$\begin{aligned} X &= a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k \\ &\equiv a_0 + a_1(1) + a_2(1) + \cdots + a_k(1) \\ &\equiv a_0 + a_1 + a_2 + \cdots + a_k \end{aligned}$$

That is, $X \equiv 0 \mod 9$ only if $a_0 + a_1 + a_2 + \cdots + a_k \equiv 0 \mod 9$. Thus $9/X$ only if $9 / (a_0 + a_1 + a_2 + \cdots + a_k)$.

//

Likewise, $10 \equiv -1 \mod (11)$ or $10 \equiv 2 \mod (8)$

$\Rightarrow 10^n \equiv (-1)^n \mod (11)$ or $10^n \equiv 2^n \mod (8)$

For example, modulo 11,

$$\begin{aligned} 3{,}817 &= 3 \times 10^3 + 8 \times 10^2 + 1 \times 10^1 + 7 \\ &\equiv 3(-1)^3 + 8(-1)^2 + 1(-1) + 7 \\ &= -3 + 8 - 1 + 7 \\ &= 11 \\ &\equiv 0 \quad \Rightarrow 11 / 3817 \end{aligned}$$

mod (8),

$$\begin{aligned} 3{,}817 &= 3 \times 10^3 + 8(10^2) + 10 + 7 \\ &\equiv 3(2)^3 + 8(2)^2 + 2 + 7 \\ &= 3(8) + 4(8) + 9 \\ &\equiv 9 \\ &\equiv 1. \end{aligned}$$

thus $8 \nmid 3817$

(which you knew w/o this calculation as 3817 is odd!)

PROBLEM 16

$$D_4 = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\} \text{ with } \begin{array}{l} x^4 = 1 \\ y^2 = 1 \\ (xy)^2 = 1 \end{array}$$

(a.)

	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	1	x^3	x^2	x
xy	xy	y	x^3y	x^2y	x	1	x^3	x^2
x^2y	x^2y	xy	y	x^3y	x^2	x	1	x^3
x^3y	x^3y	x^2y	xy	y	x^3	x^2	x	1

Notice, $(xy)(xy) = 1 \Rightarrow (xy)^{-1} = xy$ or $y^{-1}x^{-1} = xy$
but, $y^2 = 1$ so $y^{-1} = y$ and thus $yx^{-1} = xy$. ~~Too~~ Also,
calculate $yyx^{-1}y = yxyy \Rightarrow \underline{x^{-1}y = yx}$.

Hence, $yx = x^{-1}y = x^3y$ $\quad (x\,x^3 = 1 \Rightarrow x^{-1} = x^3)$

Likewise $xyx = xx^{-1}y = y$

$x^2yx = x^2(x^{-1}y) = xy$

$x^3yx = x^3(x^{-1}y) = x^2y$

$yx^2 = yxx = x^{-1}yx = x^{-1}x^{-1}y = x^3x^3y = x^2y.$

$xyx^2 = xx^{-2}y = x^{-1}y = x^3y.$

$x^2yx^2 = x^2x^{-2}y = y$

$x^3yx^2 = x^3x^{-2}y = xy$

Continuing Calculations for PROBLEM 16

$$yx^3 = x^{-3}y = (x^{-1})^3 y = (x^3)^3 y = x^9 y = xy.$$

$$xyx^3 = xx^{-3}y = x^{-2}y = x^2 y$$

$$x^2yx^3 = x^2x^{-3}y = x^{-1}y = x^3 y$$

$$x^3yx^3 = x^3x^{-3}y = y.$$

$$yy = 1$$

$$xy\cancel{y} = x$$

$$x^2yy = x^2$$

$$x^3yy = x^3$$

$$yxy = x^{-1}yy = x^{-1} = x^3$$

$$xyxy = 1$$

$$x^2y\,xy = x^2x^{-1}yy = x$$

$$x^3y\,xy = x^3x^{-1}yy = x^2$$

$$yx^2y = x^{-2}yy = x^{-2} = x^2$$

$$xy\,x^2y = xx^{-2}yy = x^{-1} = x^3$$

$$x^2y\,x^2y = x^2x^{-2}yy = (1)(1) = 1$$

$$x^3y\,x^2y = x^3x^{-2}yy = x$$

$$yx^3y = x^{-3}yy = x$$

$$xy\,x^3y = xx^{-3}yy = x^{-2} = x^2$$

$$x^2y\,x^3y = x^2x^{-3}yy = x^{-1} = x^3$$

$$x^3y\,x^3y = x^3x^{-3}yy = 1.$$

Comment: I hope we all see by now that $(xy)(xy) = 1 \implies yx^n = x^{-n}y$ for $n \geq 1$. We can use this to push y to the right.

PROBLEM 16 continued

(b.)

$1^{-1} = 1$ $\qquad$ $(xy)^{-1} = xy$

$x^{-1} = x^3$ $\qquad$ $(x^2y)^{-1} = x^2y$

$x^{-2} = x^2$ $\qquad$ $(x^3y)^{-1} = x^3y$

$x^{-3} = x$ $\qquad$ $y^{-1} = y.$

(c.) $\underline{|x^2| = |y| = |xy| = |x^2y| = |x^3y| = 2}$.

any time $g = g^{-1}$ we have $g^2 = e$ and if $g \neq e$ this means $|g| = 2$.

Also, $\underline{|1| = 1}$. and $\underline{|x| = |x^3| = 4}$.

To see that $|x^3| = 4$, note

$$x^3(x^3) = x^6 = x^2 \Rightarrow (x^3)^4 = (x^2)^2 = 1$$

Also $(x^3)^3 = x^9 = x$ hence $\underline{|x^3| = 4}$.

(we have another way to see this later, it has to do with $\gcd(3,4) = 1 \ldots$)

(d.) find distinct cyclic subgroups of D_4,

$\langle 1 \rangle = \{1\}$

$\langle x \rangle = \langle x^3 \rangle = \{1, x, x^2, x^3\}$

$\langle x^2 \rangle = \{1, x^2\}$

$\langle xy \rangle = \{1, xy\}$

$\langle x^2y \rangle = \{1, x^2y\}$

$\langle x^3y \rangle = \{1, x^3y\}$.

PROBLEM 16 continued

(e.) find $Z(D_4) = \{ g \in D_4 \mid gh = hg \ \forall h \in D_4 \}$

we can determine this by examining the Cayley Table, look for matching row & column,

$$Z(D_4) = \{1, x^2\}.$$

(f.) simplify,

$$x^6 y^{-3} x^3 y^8 x^{-5} y x y = x^2 y x^{-1} x^{-5} y x y$$
$$= x^2 x y x^{-5} y x y$$
$$= x^3 x^5 y y x y$$
$$= x^3 x x y$$
$$= \boxed{xy}$$

Again, to check work,

$$x^6 \underset{y}{y^{-3}} x^3 \underset{1}{y^8} x^{-5} y x y = x^6 x^{-3} y x^{-5} y x y$$
$$= x^3 x^5 y y x y$$
$$= x^8 x y$$
$$= \boxed{xy}.$$

$\left(\begin{array}{l} 1 = 1^4 = (y^2)^4 = y^8 \\ y x^3 = x^{-3} y \end{array} \right)$