SOLUTIONS TO PROBLEMS 17 – 20 (FROM LECTURE 5)

PROBLEM 17 Gallian #40 from Chpt. 0

Given $0-716X-2841-9$ what is X?

THE ISBN DIGIT CHECK GIVEN IN #39 is

$$10a_1 + 9a_2 + 8a_3 + 7a_4 + \cdots + 2a_9 + a_{10} \equiv 0 \pmod{11}$$

for ISBN $a_1 - a_2a_3a_4a_5 - a_6a_7a_8a_9 - a_{10}$. We need

$$10(0) + 9(7) + 8(1) + 7(6) + 6X + 5(2) + 4(8) + 3(4) + 2(1) + 9 \equiv 0$$

$$63 + 8 + 42 + 6X + 10 + 32 + 12 + 11 \equiv 0 \pmod{11}$$

$$-3 - 3 + 9 + 6X + 44 + 11 - 1 \equiv 0$$

$$6X \equiv 1 + 6 - 9$$

$$6X \equiv -2 \implies 2(6X) \equiv 2(-2) \pmod{11}$$

$$\implies 12X \equiv -4 \pmod{11}$$

$$\implies X \equiv 7 \pmod{11}$$

$$\therefore \boxed{X = 7}$$

PROBLEM 18 (mod 14)

(a.) find additive inverse and order of each element in $\mathbb{Z}_{14} = \{0, 1, 2, \ldots, 13\}$

$|0| = 1$.

$|11| = |13| = |5| = |9| = |11| = |13| = 14$.

$|2| = 7$

and, $\gcd(3,7) = \gcd(4,7) = \gcd(2,7) = \gcd(5,7) = \gcd(6,7) = 1$

so $2(2), 3(2), 4(2), 5(2), 6(2)$ also generate $\langle 2 \rangle$

hence have order 7.

$|4| = |6| = |8| = |10| = |12| = |2| = 7$.

– (I'm using Cyclic Lecture to guide calculation, of course, at this point, you would reasonably just calculate brute force) –

(b.) In $\mathbb{Z}_{14}$ multiplicative inverses do not exist for $0, 2, 4, 6, 8, 10, 12, 7$

$U(14) = \{1, 3, 5, 9, 11, 13\}$

$3(5) = 15 = 1 \quad \therefore \; 3^{-1} = 5 \;\&\; 5^{-1} = 3$.

$3^2 = 9, \; 3^3 = 27 = -1, \; 3^4 = -3, \; 3^5 = -9 = 5$

$3^6 = 15 = 1$

$\therefore \; |3| = 6$ in $U(14)$

(once we found $3^3 = -1 \Rightarrow (3^3)^2 = (-1)^2 = 1$)

Likewise, $5^2 = 25 = -3 \Rightarrow 5^3 = -15 = -1 \Rightarrow 5^6 = 1$

$\therefore \; |5| = 6$ in $U(14)$.

P18 continued

(b.) $9(11) = 99 \equiv 1$ since $98 = 7(14)$.

$\underline{9^{-1} = 11}$ and $\underline{11^{-1} = 9}$.

$9 = 3^2 \Rightarrow 9^3 = 3^6 = 1 \therefore \underline{|9| = 3}$

Likewise $|11| = |9^{-1}| = |9|$ so $\underline{|11| = 3}$.

Finally, $(13)(13) = 169 \equiv 1 \mod (14)$

$\therefore \underline{13^{-1} = 13}$ and $\underline{|13| = 2}$.

(c.) Calculate mod 14,

$5^{-2} \cdot (4-10) \cdot 13^{999} + 11 =$

$\hookrightarrow = (5^{-1})^2 \cdot (4+4) \cdot (-1)^{999} + 11$

$= 3^2 \cdot 8 \cdot (-1) + 11$

$= 9 \cdot 8 \cdot (-1) + 11$

$= (-5)(-6)(-1) + 11$

$= -30 + 11$

$= -19$

$= \boxed{9}$.

(d.) $\begin{bmatrix} 1 & 5 \\ 4 & 9 \end{bmatrix}^{-1} = (9-20)^{-1} \begin{bmatrix} 9 & -5 \\ -4 & 1 \end{bmatrix}$

$= 3^{-1} \begin{bmatrix} 9 & -5 \\ -4 & 1 \end{bmatrix} = \left[5 \begin{bmatrix} 9 & -5 \\ -4 & 1 \end{bmatrix} = \begin{bmatrix} 45 & -25 \\ -20 & 5 \end{bmatrix} = \boxed{\begin{bmatrix} 3 & 3 \\ 8 & 5 \end{bmatrix}}\right.$

P19 Let $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$, $B = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}_9) = GL(2, \mathbb{Z}_9)$

(a.) $A^{-1} = [4-6]^{-1} \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix} = 7^{-1} \begin{bmatrix} 4 & 7 \\ -3 & 1 \end{bmatrix} = 4 \begin{bmatrix} 4 & 7 \\ -3 & 1 \end{bmatrix} = \begin{bmatrix} 16 & 28 \\ -12 & 4 \end{bmatrix}$

$\Rightarrow$ $\underline{A^{-1} = \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix}}$. you can check, $AA^{-1} = \begin{bmatrix} 19 & 9 \\ 45 & 19 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Hence, $A^{-1}B^2 = \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$

$= \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix}\begin{bmatrix} 11 & 8 \\ 4 & 3 \end{bmatrix}$

$= \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix}\begin{bmatrix} 2 & -1 \\ 4 & 3 \end{bmatrix}$

$= \left[\begin{array}{c|c} 14+4 & -7+3 \\ \hline 12+16 & -6+12 \end{array}\right]$

$= \boxed{\begin{bmatrix} 0 & 5 \\ 1 & 6 \end{bmatrix}}$.

Remark: all these calculations are done in $\mathbb{Z}_9$

(b.) find cyclic subgroup generated by A.

$A^2 = \begin{bmatrix} -1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 10 \\ 15 & 22 \end{bmatrix} = \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix} = A^{-1}$

thus $A^3 = I$ and we find $\boxed{|A| = 3}$ and

$\boxed{\langle A \rangle = \{ I, A, A^2 \}}$

$= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, \begin{bmatrix} 7 & 1 \\ 6 & 4 \end{bmatrix} \right\}$.

P20

(a.) Let $f: \mathbb{Z} \longrightarrow \mathbb{Z}$ be defined by $f(x) = 2x^2 - 3$

(i.) $f(1) = f(-1)$ as $2(1)^2 - 3 = -1 = 2(-1)^2 - 3$

yet $1 \neq -1$ $\therefore$ f is not 1-1.

(ii.) preparation: Consider $f(0) = -3$, $f(\pm 1) = -1$, $f(\pm 2) = 5$, $f(\pm 3) = 2(9) - 3) = 15$ etc. It is clear that f is not onto (but, none of this yet proves it!)

proof: Pick $2 \in \mathbb{Z}$ and consider $f(x) = 2$

this gives $2x^2 - 3 = 2 \Rightarrow 2x^2 = 5 \Rightarrow x^2 = \frac{5}{2}$

thus $x = \pm\sqrt{\frac{5}{2}} \notin \text{dom}(f)$ $\therefore$ $2 \notin \text{range}(f)$

which proves f is not onto.

(iii) Let $A = \{-1, 0, 1, 2, 3\}$

$$f(A) = \{ f(x) \mid x \in A \} = \boxed{\{-1, -3, 5, 15\}}$$

(iv.) $$f^{-1}(A) = \{ x \in \mathbb{Z} \mid f(x) \in A \}$$

$$= \{ x \in \mathbb{Z} \mid 2x^2 - 3 \in \{-1, 0, 1, 2, 3\} \}$$

$$= \boxed{\{-1, 1\}} = \underbrace{f^{-1}\{-1\}}_{\text{called the "fiber" over } -1}$$

To find $f^{-1}(A)$ we needed to see if $2x^2 - 3 = -1$, $2x^2 - 3 =$ etc have integer sol^{n}s.

$2x^2 - 3 = -1 \Rightarrow 2x^2 = 2 \Rightarrow x^2 = 1 \therefore x = \pm 1$

$2x^2 - 3 = 0 \Rightarrow 2x^2 = 3 \Rightarrow$ no sol^{n} in $\mathbb{Z}$.

$2x^2 - 3 = 1 \Rightarrow 2x^2 = 4 \Rightarrow x^2 = 2 \Rightarrow x = \pm\sqrt{2} \notin \mathbb{Z}$.

$2x^2 - 3 = 2 \Rightarrow 2x^2 = 5 \Rightarrow$ no sol^{n} in $\mathbb{Z}$.

$2x^2 - 3 = 3 \Rightarrow 2x^2 = 6 \Rightarrow x^2 = 3 \Rightarrow x = \pm\sqrt{3} \notin \mathbb{Z}$

P20 continued

(6.) Let $g: X \to Y$, prove g is onto iff $g^{-1}(B) \neq \emptyset$ for all non-empty subsets B of Y $(\emptyset \neq B \subseteq Y)$

$\Rightarrow$ Suppose g is onto where $g: X \to Y$ a function. Consider $B \subseteq Y$ with $B \neq \emptyset$. By definition of nonempty, $\exists x \in B$ and as $B \subseteq Y$ we have $x \in Y$ thus by surjectivity of g there exists $a \in X$ for which $g(a) = x$. Observe, $a \in g^{-1}(B)$ since $g^{-1}(B) = \{z \in X \mid g(z) \in B\}$. Thus $g^{-1}(B) \neq \emptyset$.

$\Leftarrow$ suppose $g^{-1}(B) \neq \emptyset$ for <u>all</u> $\emptyset \neq B \subseteq Y$. Consider $y \in Y$ and note $y \in \{y\} \subseteq Y$ hence $g^{-1}\{y\} \neq \emptyset$ for each $y \in Y$. But,

$$g^{-1}\{y\} = \{x \in X \mid g(x) \in \{y\}\}$$
$$= \{x \in X \mid y = g(x)\}$$

thus $\exists x \in X$ for which $g(x) = y$. Thus g is onto. //