OLD DOMINION UNIVERSITY

CS 463

Homework 2

Madelene McFarlane

8/30/2023

#01096496

CS 463
HW2

Madeleine McFarlane

:work : answer

Q1)

i) $150 \cdot 92 \bmod 14$

$((150 \bmod 14) \cdot (92 \bmod 14) \bmod 14)$

$10 \cdot 8$

$80 (\bmod 14) \rightarrow \frac{80}{14} : 5 \; r\,10$

$\boxed{10}$

ii) $6 \cdot (4/11) \bmod 14$

$a/b \bmod c$ $a=4,\ b=11,\ c=14,\ d=8$

$(b \cdot d) \bmod c = a \bmod c$ $(11 \cdot 8) \bmod 14 = 4$

$4 \bmod 14 = 14$

$\boxed{6}$

$(4/11) \bmod 14 = 8$

$(6 (4/11)) \bmod 14 \rightarrow (6 \cdot 8) \bmod 14 = 48 \bmod 14 = 6$

iii) $24/17 \bmod 14$

$\boxed{8}$

$((24 \bmod 14) \cdot (17^{-1} \bmod 14) \bmod 14) \rightarrow ((10 \bmod 14) \cdot (3^{-1} \bmod 14) \bmod 14)$

$((10 \bmod 14) \cdot (5 \bmod 14) \bmod 14)$ $10 \cdot 5 \bmod 14$

iv) $4^8 \cdot 5^{12} \bmod 14$

$((4^8 \bmod 14) \cdot (5^{12} \bmod 14)) \bmod 14) \rightarrow ((4^2 \bmod 14)^4 \cdot (5^3 \bmod 14)^4 \bmod 14)$

$(2 \bmod 14)^4 \cdot (-1 \bmod 14)^4 \bmod 14) \rightarrow ((16 \bmod 14) \cdot (1 \bmod 14) \bmod 14)$

$2 \cdot 1 \bmod 14$ $2 \bmod 14$ $\boxed{2}$

v) $5^{10} \cdot 6^8 \bmod 14$

$((5^5 \cdot 6^4)(\bmod 14))^2 \bmod 14) \cdot ((4{,}050{,}000 \bmod 14)^2 \bmod 14)$ $^{\wedge 10}$

$((10)^2 \bmod 14)$ $100 \bmod 14 = 2$

$\boxed{2}$

4,050,000
28
125
112
130
126
40
28
120
112
80
70
10

CS 463 Madeleine McFarlane

HW2

■ : work ■ : answer

i) elements of Z_{13} + Z_{13^*}

13 is prime therefore all non-zero elements are multiplicatively invertible.

$Z_{13} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{12}\} \rightarrow \boxed{Z_{13^*} = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{12}\}}$

ii) elements of Z_{18} + Z_{18^*}

$Z_{18} \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \ldots, \overline{17}\}$ $Z_{18} \neq$ prime therefore invertible elements are

$Z_{18} \{\bar{x} \mid \gcd(x, 18) = 1, 0 \leq x \leq 18\} - \boxed{\{\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}\}}$

iii) order of 5 in Z_{13}

$5^2 = 25 = (-1) \bmod 13 \Rightarrow 5^3 \equiv (-5) \bmod 13 \equiv 8 \bmod 13$

$5^4 \equiv 40 \bmod 13 \equiv 1 \bmod 13 \Rightarrow 5^4 \equiv 1 \bmod 13$ $\boxed{4}$

order of 5 = 4

iv) Multiplicative inverse of $5 \in Z_{13}$

$(5^4 \equiv 1 \bmod 13) \Rightarrow 5 \cdot 5^3 \equiv 1 \bmod 13 \Rightarrow 5^{-1} \equiv 5^3 \bmod 13$

$5^3 = 8 \bmod 13$ $\boxed{5^{-1} = 8}$

v) Z_{13} cyclic group? order? generator element?

$Z_{13} \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{12}\}$

Yes Z_{13} is a cycle group

Group order 12

$\bar{1}$ = generator element