Math 531 Homework 2

Theo Koss

February 2021

1 Section 1.3

- Problem 4: Solve: $20x \equiv 12 \mod 72$.

$$20x = 12 + 72q; q = -1, x = [-3]$$

- Problem 5: Solve: $25x \equiv 45 \mod 60$.

$$25x = 45 + 60q; q = -2, x = [-3]$$

- Problem 7: Find additive orders of:

  a. $8 \mod 12 : \quad 3$
  b. $7 \mod 12 : \quad 12$
  c. $21 \mod 28 : \quad 3$
  d. $12 \mod 18 : \quad 3$

- Problem 27: Let p be prime and $a, b \in \mathbb{Z}$. Prove,

$$(a+b)^p \equiv a^p + b^p \mod p$$

Proof. By the Binomial Thm., it holds that:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

Where $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Then it is easy to see that

$$k = 0, p \implies \binom{p}{k} = 1$$

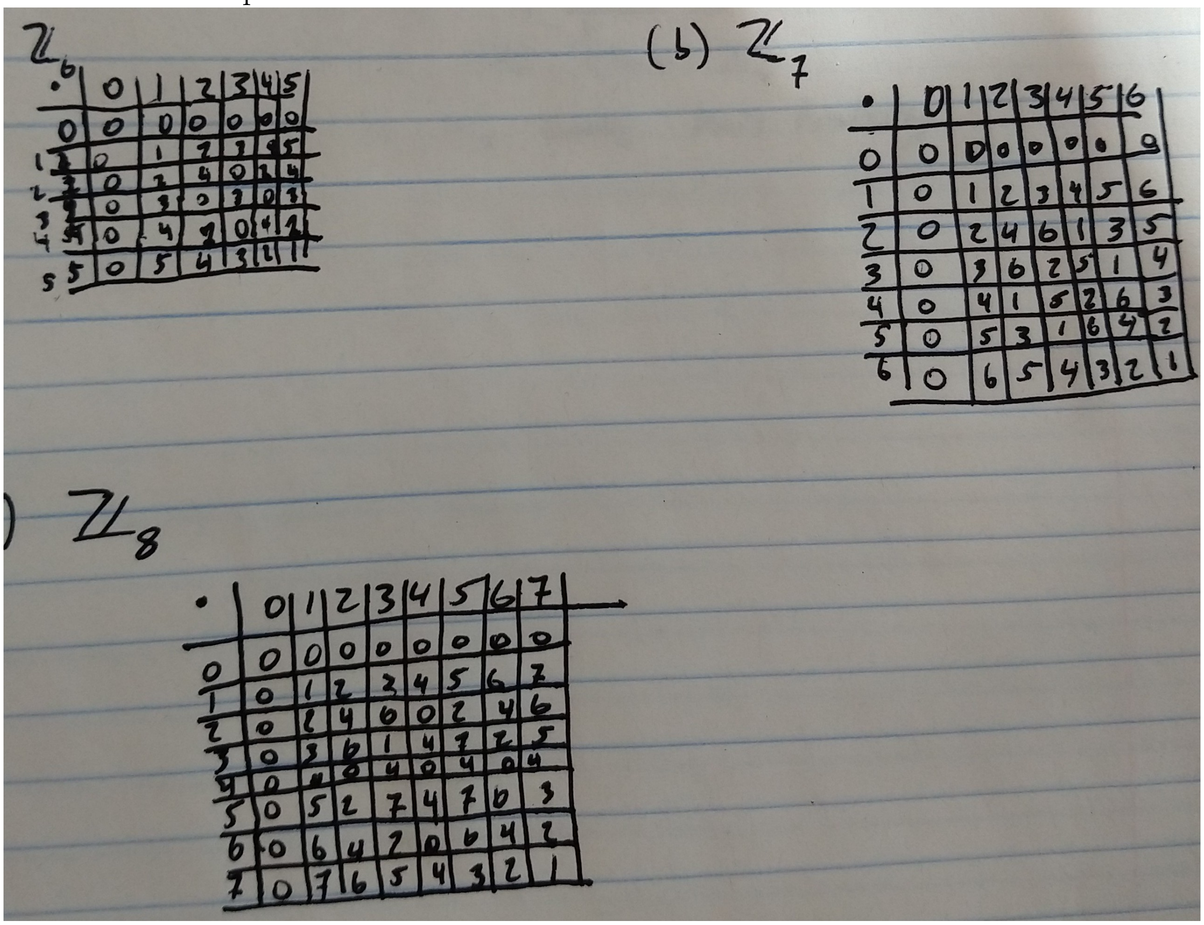
Suppose $k \in \{1, 2, ..., p-1\}$ Then

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p \cdot l_k$$

for some $l_k \in \mathbb{Z}$. Then, by definition, $\binom{p}{k} \equiv 0 \mod p$.
Thus, all $\binom{p}{k}$ such that $k \in \{1, 2, ..., p-1\}$ are equivalent to $0 \mod p$.
Therefore, $(a+b)^p = a^p + b^p$ for prime p and $a, b \in \mathbb{Z}$. QED

2 Section 1.4

- Problem 2: Multiplication tables:



$\mathbb{Z}_6$

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b) $\mathbb{Z}_7$

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

) $\mathbb{Z}_8$

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	7	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

- Problem 9:

  a. Find multiplicative orders of [5] and [7] in $\mathbb{Z}_{16}^x$.
  $5^4 \equiv 1 \mod 16; 7^2 \equiv 1 \mod 16$. Mult. orders, 4 and 2 respectively.

  b. Find multiplicative orders of [2] and [5] in $\mathbb{Z}_{17}^x$.
  $2^8 \equiv 1 \mod 17; 5^{16} \equiv 1 \mod 17$.

- Problem 12: In $\mathbb{Z}_9^x$ each element is equal to a power of [2]. Can you find a congruence class in $\mathbb{Z}_8^x$ such that each element of $\mathbb{Z}_8^x$ is equal to

some power of that class? Answer the same question for $\mathbb{Z}_7^x$.
$[3] \in \mathbb{Z}_8^x$ is a generator. As is $[3] \in \mathbb{Z}_7^x$.

- Problem 13: Show that $\mathbb{Z}_{10}^x$ and $\mathbb{Z}_{11}^x$ are cyclic, but $\mathbb{Z}_{12}^x$ is not.

  Proof. By some guy on wikipedia, The group $\mathbb{Z}_n^x$ is cyclic iff $n \in \{1, 2, 4, p^k, 2p^k\}$. Where p is an odd prime and $k \in \mathbb{N}$. Since $10 = 2 \cdot \underbrace{5}_{\text{odd prime}}$ and $11 = \underbrace{11^1}_{\text{odd prime}}$, $\mathbb{Z}_{10}^x$ and $\mathbb{Z}_{11}^x$ are cyclic. However, 12 is not of that form, therefore it is not cyclic. (I call this one, "proof by wikipedia.") QED