Sabbir Ahmed

DATE: March 3, 2018

MATH 407: HW 04

1.3 **1** Solve the following congruence

d $19x \equiv 1 \pmod{36}$

Ans □

4 Solve the following congruence: $20x \equiv 12 \pmod{72}$

Ans □

7 The smallest positive solution of the congruence $ax \equiv 0 \pmod{n}$ is called the additive order of a modulo n. Find the additive orders of each of the following elements, by solving the appropriate congruences.

b 7 modulo 12

Ans □

d 12 modulo 18

Ans □

14 Find the units digit of $3^{29} + 11^{12} + 15$.
Hint: Choose an appropriate modulus n, and then reduce modulo n.

Ans □

16 Solve the following congruences by trial and error.

a $x^3 + 2x + 2 \equiv 0 \pmod{5}$

Ans □

20 Solve the following system of congruences.

$$2x \equiv 5 \pmod{7} \qquad 3x \equiv 4 \pmod{8}$$

Ans □

1.4 **2** Make multiplication tables for the following sets.

b $\mathbb{Z}_7$

Ans $\square$

c $\mathbb{Z}_8$

Ans $\square$

6 Let m and n be positive integers such that $m \mid n$. Show that for any integer a, the congruence class $[a]_m$ is the union of the congruence classes $[a]_n, [a+m]_n, [a+2m]_n, \ldots, [a+n-m]_n$

Ans $\square$

9 Let $(a, n) = 1$. The smallest positive integer k such that a $a^k \equiv 1$ (mod n) is called the **multiplicative order** of $[a]$ in $\mathbb{Z}_n^\times$

b Find the multiplicative orders of $[2]$ and $[5]$ in $\mathbb{Z}_{17}^\times$.

Ans $\square$

10 Let $(a, n) = 1$. If $[a]$ has multiplicative order k in $\mathbb{Z}_n^\times$, show that $k \mid \varphi(n)$.

Ans $\square$

13 An element $[a]$ of is said to be **idempotent** if $[a]^2[a]$.

b Find all idempotent elements of $\mathbb{Z}_{10}^\times$ and $\mathbb{Z}_{30}^\times$.

Ans $\square$

15 If n is not a prime power, show that $\mathbb{Z}_n$ has an idempotent element different from $[0]$ and $[1]$.
Hint: Suppose that $n = bc$, with $(b, c) = 1$. Solve the simultaneous congruences $x \equiv 1$ (mod b) and $x \equiv 0$ (mod c).

Ans $\square$

20 Show that $\varphi(1)+\varphi(p)+\ldots+\varphi(p^\alpha) = \varphi^\alpha$ for any prime number p and any positive integer α.

Ans $\square$

26 Let $p = 2k + 1$ be a prime number. Show that if a is an integer such that $p \nmid a$, then either $a^k \equiv 1$ (mod p) or $a^k \equiv -1$ (mod p)

Ans □