

**MATH 332 - ALGEBRA AND NUMBER THEORY :
HOMEWORK 4**

DUE FRIDAY, SEPTEMBER 21ST (NO LATER THAN **12PM**)

NOTE: This document contains two pages, please see next page for additional problems.

CHAPTER 2: CONGRUENCES

Solve the following exercises from Adler & Coury:

Exercises (pages 65, 66): 31, 32, 36, 38, 41.

CHAPTER 3: THE THEOREMS OF FERMAT AND WILSON

Solve the following exercises from Adler & Coury:

Exercises (pages 94): 1, 3, 5, 11, 12, 13.

Also:

(1) **Five Pirates and a Monkey.**

Five pirates and a monkey are shipwrecked on an island. The pirates have collected a pile of coconuts which they plan to divide equally among themselves the next morning. Not trusting the others, one pirate wakes up during the night and divides the coconuts into five equal parts with one left over, which he gives to the monkey. The pirate then hides his portion of the pile. During the night, each of the other pirates does exactly the same thing by dividing the pile he finds into five equal parts leaving one coconut for the monkey and hiding his portion. In the morning, the pirates gather and split the remaining pile of coconuts into five equal parts and again one is left over for the monkey. What is the smallest number of coconuts the pirates could have collected for their original pile?

(2) Read the section of the book “An Application: Finding the Day of the Week” (page 47) and the solved problems (page 59).

Then solve problems 43 and 45 (page 66).

- (3) **Definition:** A group G is a mathematical system consisting of a non-empty set G and an operation $*$ such that $a*b$ is in G , for any two a, b elements of G . G and $*$ must verify the following properties:

- (a) The operation $*$ is associative. For all a, b, c in G :

$$a * (b * c) = (a * b) * c.$$

- (b) There is a (neutral) element e in G such that, for all a in G :

$$a * e = e * a = a.$$

- (c) For each $a \in G$ there is an element a' in G such that

$$a * a' = a' * a = e.$$

Examples: The integers \mathbb{Z} with the operation of addition form a group ($*$ = + and the neutral element is zero, $e = 0$ in this case). The non-zero real numbers $\mathbb{R} - \{0\}$ with the operation of multiplication is a group ($*$ = \times and the neutral element is 1, $e = 1$ in this case).

Problem 3.1: Let m be a positive integer. Let U_m be the set of all elements of $\mathbb{Z}/m\mathbb{Z}$ which have a multiplicative inverse (i.e. U_m is the set of all $a \pmod m$ such that there is an element a^{-1} in $\mathbb{Z}/m\mathbb{Z}$ such that $a \cdot a^{-1} \equiv 1 \pmod m$). Prove that U_m is a group with respect to multiplication.

Example: Let $p = 7$. Then $U_7 = \{1, 2, 3, 4, 5, 6 \pmod 7\}$. Let $g \equiv 3 \pmod 7$. Then $g^1 = g \equiv 3 \pmod 7$ and the powers are:
 $g^2 \equiv 3^2 \equiv 2 \pmod 7$, $g^3 \equiv 6$, $g^4 \equiv 4$, $g^5 \equiv 5$, $g^6 \equiv 1 \pmod 7$

and so, the powers of 3 go through every element of U_7 .

Let $(G, *)$ be a group and let $g \in G$ which satisfies that for every $a \in G$ there is n such that $g^n = a$ in G (here $g^2 = g * g$). Then we say that g is a *generator* of G . If $g \pmod m$ is a generator of (U_m, \times) then we also say that $g \pmod m$ is a *primitive root* of modulo m . The previous example shows that 3 is a primitive root modulo 7.

Problem 3.2: Are there other primitive roots modulo 7 (i.e. generators of U_7)? Which are they? Are there primitive roots modulo 11 and 13? If so, find them.