ELEN 162
A. I. Zecevic

Homework 3

NOTE: For all problems in this assignment, you must *show your work*. If you simply produce a number that was obtained by a software package and don't provide the intermediate steps, you will get no credit.

1. (a) Compute
$$a_1 = (6 + 8) \bmod 5 \tag{1}$$
$$a_2 = (3 - 15) \bmod 7 \tag{2}$$
and
$$a_3 = (6 \cdot 5) \bmod 9 \tag{3}$$
(b) Determine whether
$$a_4 = (11/5) \bmod 9 \tag{4}$$
and
$$a_5 = (215/91) \bmod 14 \tag{5}$$
are properly defined. If they are, calculate these values. If not, explain.

2. (a) Use Euclid's method to compute $\gcd(969, 1785)$ and $\gcd(57, 833)$.
(b) Based on the results obtained in part (a), determine whether equations
$$x \cdot 1,785 = 1 \pmod{969} \tag{6}$$
and
$$x \cdot 833 = 1 \pmod{57} \tag{7}$$
have a solution. If they do, compute the *smallest positive* integer x that satisfies them.

3. Find a positive integer x that satisfies equation
$$(1,585)^x = 1 \pmod{29} \tag{8}$$
Is the solution that you obtained unique? Explain. (**Hint:** Think how Lemma 5.10 can help you answer this question).

4. Compute
$$(4,108)^{31} \bmod 168 \tag{9}$$
and
$$(18)^{126} \bmod 79 \tag{10}$$
using Lemmas 5.10 and 5.11.

5. Express $x = 0.25366064$ as $x = p/q$, where p and q are positive integers. Show the sequence of convergents that arises in the process of continued fraction expansion, and calculate the approximation error

$$\varepsilon^{(n)} = \left| \frac{p_n}{q_n} - 0.25366064 \right| \tag{11}$$

in each step. The process should terminate at the point when $\varepsilon^{(n)} = 0$. **Note:** Since accuracy is important in this problem, avoid rounding, and use Matlab's full precision for all your calculations.

6. Let Z_n^* denote a group whose elements are all positive integers that are smaller than n and are co-prime with it. Given two elements $a, b \in Z_n^*$ we will define operation $a \circ b$ as

$$a \circ b = ab \bmod n \tag{12}$$

and denote the k-th power of a as

$$f_k(a) = a \circ a \circ \ldots \circ a \tag{13}$$

(a) Find the elements that constitute groups Z_7^*, Z_8^* and Z_{14}^*.

(b) Using the fact that

$$f_k(a) = a^k \bmod n \tag{14}$$

for any element $a \in Z_n^*$ (see Lemma 7.1), determine whether or not each of these three groups is cyclic. Can we guarantee that one (or more) of them will possess this property without checking their elements explicitly? Explain.

(c) Identify *all* the generators for the groups that you found to be cyclic in part (b).

(d) For each group Z_n^* ($n = 7, 8, 14$) find the order modulo n of *every* element that belongs to it (except for $g_0 = 1$, which is trivial). Which of these elements have order equal to $\varphi(n)$? Do you notice a pattern? Explain.