Problem Set #5

CMSC/Math 456
Instructor: Daniel Gottesman

Due on Gradscope, Thursday, Oct. 5, noon (before start of class)

General instructions: If you collaborate or use any outside resources, remember to cite them in your solutions.

Note: This problem set has 3 problems; the last parts of problem 2 and problem 3 are on page 2.

Problem #1. Modular Arithmetic Practice (40 points)

Calculate the following in modular arithmetic. Show your work (an integer operation or modular reduction counts as one step).

a) (6 points) $(15 + 23) \bmod 31$

b) (6 points) $(15 - 23) \bmod 31$

c) (6 points) $(15 * 23) \bmod 31$

d) (10 points) $(15/23) \bmod 31$

e) (12 points) $15^{23} \bmod 31$

Problem #2. Mathemagician Trick (40 points)

A mathemagician is giving a cryptography class. He writes on the board:

$$N = 12d + 31m,$$

and asks his students to think about their own birthdays and calculate N, where $d \in \{1, ..., 31\}$ corresponds to the day, and $m \in \{1, .., 12\}$ to the month. (For instance, if the birthday is May 15, then $N = 12(15)+31(5) = 335$). Then he asks them to tell their N, but not their birthdays. One by one he tells them their own birthdays: "$N = 136$," says one student. "April 1st," the mathemagician replies. "$N = 265$," proclaims another student. "You must have a lot of fun in your birthday, because you were born on July 4th," the mathemagician replies. And so on.

a) (10 points) If $N = 465$, compute its corresponding birthday (d, m). Show your work.

Hint:(for parts a and b) Try considering N mod q for useful values of q to simplify the formula for N.

b) (10 points) Suppose this were taking place in a world where there were 12^s months in the year and 31^s days in a month, and the formula was instead $N = 12^s d + 31^s m$. Describe an algorithm (in words, pseudocode, or if you prefer Python code) that will compute (d, m) given N. Your algorithm should run in a time polynomial in s. Give a basic explanation for why your algorithm works.

If you are presenting your algorithm in words or pseudocode, you may invoke subroutines for algorithms we described in class, such as Euclid's algorithm, without further detail about how those algorithms work.

c) (10 points) Prove for the original version of the problem (with $N = 12d + 31m$ and months and days as in our world) that there cannot be two (day, month) pairs (d, m) that produce the same number N.

Note: This is not quite the same as part b, besides the difference in the formula. In part b, you need to justify why your algorithm produces one of the correct answers, even if there are multiple possibilities. In part c, you must prove that there is only ever at most one possibility.

d) (10 points) If we change the formula, is it possible to have

$$N = 12d + 30m$$

for $N = 256$ and some integers d, m? If yes, find some pair (d, m). If not, explain why.

Problem #3. Group or Not a Group? (40 points)

For each of the following pairs of sets and operations, say whether they form a group or not. If the pair does form a group, justify why it is closed under the group operation, give the identity, and list or give a formula for the inverses of all elements. If the pair does not form a group, say which group property is not satisfied and prove that the property is not satisfied, for example by giving an example of elements where the property fails.

a) (10 points) The set $\{0, 2, 4, 6, 8\}$ over *addition modulo 9*.

b) (10 points) The set $\{0, 2, 4, 6, 8\}$ over *multiplication modulo 10*.

c) (10 points) The set $\{1, 3, 5, 7, 9\}$ over *multiplication modulo 11*.

d) (10 points) The set $\{A, B, C, D\}$ with group operation defined by the following table:

$*$	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

(This operation is associative; you do not need to check that.)