> MAST 332 - COMP 367
Winter 2019
MIDTERM TEST

INSTRUCTIONS:
This is a closed-book examination, no printed or electronic material other than
this file is allowed. Save the file under your name on the desktop (add you ID
and name to the title)
Write your name here: _____

Write your student ID here: _____

There are 5 main question worth 6 marks each, + a Bonus question for additional
3 marks,
with the total not exceeding 30 marks (=100%).
Solutions must contain clear explanations for full marks.

Total:

Question 1: Diophantine Equations

Consider the following two equations with integer variables x and y

(1) 126*x+225*y = 36 (2) 45*x+30*y = 20

> (a) Determine which of these two equations is inconsistent, and explain why
> (you can use the Maple commands ifactor and/or gcd).

(b) Find a solution of the equation which is consistent. (c) Find all solutions
{x, y} of that equation. Identify then the solution {x, y} with smallest
possible absolute value of x.

>

Solution:

(a)

(b)

(c)

Question 2: Congruence Classes

> restart:

Question 2.1 (3 marks) :
Consider the ring of congruence classes $R=\mathbb{Z}/21\mathbb{Z}$:
(a) Identify the set S of all zero divisors of R and the set U of all units in
R. Explain your solution.
(b) Find all inverses or all or all complementary zero divisors, whatever
exists, of the element [30] in R.

Solution:
(a)

(b)

Question 2.2 (3 marks) :

The number m=10557 is factored as:
ifactor(10557)

$$(3)^3 (17) (23)$$

Consider the ring of congruence classes R= $\mathbb{Z}/10557\mathbb{Z}$.
(a) Use the Euler's Theorem to find the inverse of the congruence class [10] in
R, and

(b) use it to find all solutions of the equation [10]*X = [11] in R. Explain
your solution.

Solution:

(a)

(b)

Question 3: Rings Z/mZ

Find the order of the element A of the ring Z/mZ, or explain why the order does
not exist:

(a) A = 28in $\mathbb{Z}/210\mathbb{Z}$

(b) A = 36 in $\mathbb{Z}/2111\mathbb{Z}$ (Hint: use the Fermat's theorem)
Explain your solutions.

(HINT: use Maple's ifactor to find out the composition of the moduli).

Solution:

(a)

(b)

Question 4: Hill Cryptosystem

```
> restart: with(LinearAlgebra):
```

Peter receives from Alice an encripted message consisting of following 3
double-digit sequences: "c1= 10 12 02 21 13: c2= 25 23 04 26 16: c3=08 13 14 06
18:"

Peter knows that she has used the following 27 character-to-digits conversion
table
Matrix(6, 9, [[1, 2, 3, 4, 5, 6, 7, 8, 9], ["A", "B", "C", "D", "E", "F", "G",
"H", "I"], [10, 11, 12, 13, 14, 15, 16, 17, 18], ["J", "K", "L", "M", "N", "O",
"P", "Q", "R"], [19, 20, 21, 22, 23, 24, 25, 26, 27], ["S", "T", "U", "V", "W",
"X", "Y", "Z", "_"]])
so using 27-modular ring Z/27Z (using 27 for space), and that for encription
Alice might have used one of the following matrices:
A := `<|>`(`<,>`(12, 4, 2, 2, 0), `<,>`(3, 3, 3, 15, 0), `<,>`(1, 5, 3, 2, 0),
`<,>`(3, 1, 4, 5, 0), `<,>`(1, 2, 2, 1, 1)); B := `<|>`(`<,>`(1, 13, 12, 10),
`<,>`(3, 11, 7, 1), `<,>`(5, 2, 17, 1), `<,>`(5, 7, 14, 5)); C := `<|>`(`<,>`(1,
1, 3, 0, 1), `<,>`(1, 2, 1, 12, 3), `<,>`(5, 1, 2, 7, 17), `<,>`(6, 9,

11, 13,
1), `<,>`(0, 1, 19, 19, 23))

(A) Based on this information, Peter was able to make an unambiguous choice for
the matrix that Alice has used to encript the text received by Peter. Argue
which of the matrices A, B or C was used by Alice.

(B) Perform now decryption of the text received by Peter.

Solution:

(A)

(B)

Question 5: Modular algebra

Calculate the least non-negative residue of (137)"^(546)modulo m=527 " using
the 'squaring the base' algorithm. That is, convert the exponent 546 to base-2
form and use it accordingly in the algorithm. Use appropriate Maple commands to
help your calculations. Check at the end that your answer is correct by directly
computing this residue using Maple.

Solution:

Bonus Question:

Prove that a ring $R=\mathbb{Z}/m\mathbb{Z}$ cannot have a primitive root if it is not a field.
Proof: