with(*LinearAlgebra*) :

COMP 367- MAST 332
Final Examination
April 2014

INSTRUCTIONS:

This is a closed-book examination, no printed or electronic material other than this file is allowed

1. Save this file on the desktop under the name: **YourID-Lastname-C367-M332-FinalExam**

2. Write here your **ID:**___xxx_____

Name:_____xxx_____

3. There are 10 regular sections and one Bonus section for extra 5 marks.

4. Each regular section contains 1 or 2 questions; the total for each section is worth 10 marks.

5. Clear verbal explanations/answers in your solutions must be provided for full marks.

Total:_____

Question 1: Numbers, *Bezout's Identity*

Q1.1 (5 *marks*):

The Division Theorem states that if $a > b$ are two natural numbers then $a = b \cdot q + r$ for some

integers q **and** r,
where the remainder $r < b$. Prove that if the greatest common divisor $(a, b) = d$, then also $(a, r) = (b, r) = d$:

Proof:

for example:
5 = 2k+ 1
gcd(a,b) = d
gcd(5,2) = 1

then $(a, r) = (b, r) = d$:
gcd(5, 1) = 1 = gcd(2,1) = 1 = 1

Q1.2 (5 *marks*):

Bezout's Identity states that if the greatest common divisor $(a, b) = d$, then $d = a \cdot s + b \cdot t$ for some integers s **and** t.
True or False ? Justify your answer.
The numbers s **and** t solving the Bzout's Identity $d = a \cdot s + b \cdot t$ are coprime.

Solution:

true , if a = 5, b = 4 , then gcd(5,4) =1
5*-3 + 4*4 = 1

and -3 and 4 are coprime.

Question 2: Diophantine Equations

Q2 (10 *marks*):

Consider the following two equations with integer variables x **and** y :

(1) $27x \equiv 33 \pmod{18}$:

(2) $66x = 105y + 12$:

(***a***) Determine which one of these two equations is inconsistent, and explain why it (or both) does not have a solution.

(b) Find a solution of the equation which is consistent.

(c) Find all solutions $\{x, y\}$ of that equation.

(***d***) Identify now the solution $\{x, y\}$ with the smallest $x \geq 0$.

Solution:

(**a**)

1) 27x = 18k + 33
27x - 18k = 33

```
> gcd(27, 18)
```

9 **(2.1)**

9 can not be divide by 33, so its inconsistent.

2) 66x - 105y = 12

```
> gcd(66, 105);
```

3 **(2.2)**

3 can be divde by 12, so there is a solution.

(***b***)
66x - 105y = 12
66x - 105y = 12
using EEA matrix:

[105, 0 , 1]
[66, 1, 0]
[39, -1, 1]
[27, 2 , -1]
[12, -3, 2]
[3, 8, -5]
we can stop here.

```
> 2·105 + -3·66;
```

12 **(2.3)**

so x = -3. and y = -2.

(**c**)

there is only 2 solutions:

$2 \cdot 105 + -3 \cdot 66$; where x = -3. and y = -2.

66*32 + 105*20 = 12; where x = 32 and y = 20

(d)

looking at the EEA matrix above:

66*8 + -105*-5 = 3
66*32 + 105*20 = 12

x = 32 and y = 20

Question 3: Congruence Classes $\mathbb{Z}/m\mathbb{Z}$

```
> restart:
```

Question 3.1 (5 *marks*):

Consider the ring of congruence classes R=$\mathbb{Z}$/18$\mathbb{Z}$:

(***a***) Identify the set *S* of all zero divisors of *R* and the set *U* of all units in R (***explain***).

(***b***) For the element [12], find all complementary zero divisors or all inverses, whichever exists. Explain.

(***c***) Find the order of the element [5] or explain why this is impossible.

Note: you can use any Maple operation to help calculations, but you have to explain your calculations .

Solution:

(***a***)

if the gcd of x and 18 is not 1, then it's a zero divisor, else units.

```
> seq(gcd(x, 18), x = 1 ..17);
```

1, 2, 3, 2, 1, 6, 1, 2, 9, 2, 1, 6, 1, 2, 3, 2, 1 **(3.1.1)**

units: {1,5,7,11,13, 17}

zerodivisor: {2,3,4,6,8,9,10,12,14,15,16}

(***b***)

[12][x] = 18k

[12][3] =18*2

x= 3k + 3.
so [3], [6], [9] and more are all complementary zero divisors of [12].

(*c*)

trying to find the order of 5 mod 18.

```
> seq(5^i mod 18, i = 1..17);
```

5, 7, 17, 13, 11, 1, 5, 7, 17, 13, 11, 1, 5, 7, 17, 13, 11 **(3.1.2)**

```
> 5^6 mod 18;
```

1 **(3.1.3)**

the order of 5 in R=ℤ/18ℤ is 6.

Question 3.2 (5 marks):

In the ring R=ℤ/236ℤ :

(*a*) Calculate the number of units and the number of zero divisors using Euler's phi-function $\phi(m)$. Explain.

(Hint: Note that the modulus $m = 236$ is factored as *ifactor*(236))

$(2)^2\ (59)$ **(3.2.1)**

(*b*) Use the Euler's Theorem to find the inverse of [33].

(*c*) Find ***all*** solutions of the equation
[33]·*X* = [12]

(you can use ***any*** method.)

Solution:

(*a*)

the number of unit is :
(2^2 - 2^1)*(59-1)

```
> 2·58;
```

116 **(3.2.2)**

the number of zero divisor:
m- 1 - units

```
> 236 − 1 − 116;
```

119 **(3.2.3)**

the number of units is 116 and the number of zero divisors is 119.

(***b***)

now we find the order, but we need the inverse:

```
> 33^116 mod 236;
```

$$1 \qquad \textbf{(3.2.4)}$$

according to the theorem, m-1.

```
> 33^115 mod 236;
```

$$93 \qquad \textbf{(3.2.5)}$$

to check:

```
> 33·93 mod 236;
```

$$1 \qquad \textbf{(3.2.6)}$$

93 is inverse of [33]

(***c***)
$\mathbb{Z}/236\mathbb{Z}$:

$[33]\cdot X = [12]$

[33]x = 236k + 12

33x - 236k = 12
33x + -236k = 12

```
> gcd(33, 236);
```

$$1 \qquad \textbf{(3.2.7)}$$

so we have a solution.

[236, 0 ,1]
[33, 1, 0]
[5, -7, 1]
[3, 43, -6]
[2, -50, 7]
[1, 93, -13]

to check:

```
> -13·236 + 33·93;
```

$$1 \qquad \textbf{(3.2.8)}$$

```
> -13·12;
```

$$-156 \qquad \textbf{(3.2.9)}$$

```
> 93·12;
```

$$1116 \qquad \textbf{(3.2.10)}$$

x = 1116

to check

```
> 33·1116 mod 236;
```

12 **(3.2.11)**

```
>
```

Question 4: Primes

Question 4.1 Sieve of Eratosthenes (7 *marks*):

Apply the Sieve of Eratosthenes algorithm to find the set *P* of all primes in the interval [100,200].

Solution:

```
> sieve := {seq(i, i = 100 ..200)};
```

$$sieve := \{100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200\} \quad \textbf{(4.1.1)}$$

now we have to minus the mutiple of 2 between [100,200]

```
> multi2 := {seq(i·2, i = 50 ..100)};
```

$$multi2 := \{100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192, 194, 196, 198, 200\} \quad \textbf{(4.1.2)}$$

```
> sieve := sieve minus multi2;
```

$$sieve := \{101, 103, 105, 107, 109, 111, 113, 115, 117, 119, 121, 123, 125, 127, 129, 131, 133, 135, 137, 139, 141, 143, 145, 147, 149, 151, 153, 155, 157, 159, 161, 163, 165, 167, 169, 171, 173, 175, 177, 179, 181, 183, 185, 187, 189, 191, 193, 195, 197, 199\} \quad \textbf{(4.1.3)}$$

now we have to minus the mutiple of 3 between [100,200]

```
> multi3 := {seq(i·3, i = 30 ..70)};
```

$$multi3 := \{90, 93, 96, 99, 102, 105, 108, 111, 114, 117, 120, 123, 126, 129, 132, 135, 138, 141, 144, 147, 150, 153, 156, 159, 162, 165, 168, 171, 174, 177, 180, 183, 186, 189, 192, 195, 198, 201, 204, 207, 210\} \quad \textbf{(4.1.4)}$$

```
> sieve := sieve minus multi3;
```

$$sieve := \{101, 103, 107, 109, 113, 115, 119, 121, 125, 127, 131, 133, 137, 139, 143, 145, 149, 151, 155, 157, 161, 163, 167, 169, 173, 175, 179, 181, 185, 187, 191, 193, 197, 199\} \quad \textbf{(4.1.5)}$$

now we have to minus the mutiple of 5 between [100,200]

```
> multi5 := {seq(i·5, i = 20 ..40)};
```

$$multi5 := \{100, 105, 110, 115, 120, 125, 130, 135, 140, 145, 150, 155, 160, 165, 170, 175, 180, 185, 190, 195, 200\} \quad \textbf{(4.1.6)}$$

```
> sieve := sieve minus multi5;
```

$$sieve := \{101, 103, 107, 109, 113, 119, 121, 127, 131, 133, 137, 139, 143, 149, 151, 157, 161, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199\} \quad \textbf{(4.1.7)}$$

now we have to minus the mutiple of 7 between [100,200]

```
> multi7 := {seq(i·7, i = 13 ..30)};
```

$$multi7 := \{91, 98, 105, 112, 119, 126, 133, 140, 147, 154, 161, 168, 175, 182, 189, 196, 203, 210\} \quad \textbf{(4.1.8)}$$

```
> sieve := sieve minus multi7;
```

$$sieve := \{101, 103, 107, 109, 113, 121, 127, 131, 137, 139, 143, 149, 151, 157, 163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199\} \quad \textbf{(4.1.9)}$$

now we have to minus the mutiple of 11 between [100,200]

```
> multi11 := {seq(i·11, i = 9 ..20)};
```

$$multi11 := \{99, 110, 121, 132, 143, 154, 165, 176, 187, 198, 209, 220\} \quad \textbf{(4.1.10)}$$

```
> sieve := sieve minus multi11;
```

$$sieve := \{101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 169, 173, 179, 181, 191, 193, 197, 199\} \quad \textbf{(4.1.11)}$$

now we have to minus the mutiple of 13 between [100,200]

```
> multi13 := {seq(i·13, i = 7 ..17)};
```
$$multi13 := \{91, 104, 117, 130, 143, 156, 169, 182, 195, 208, 221\} \quad \textbf{(4.1.12)}$$
```
> sieve := sieve minus multi13;
```
$$sieve := \{101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199\} \quad \textbf{(4.1.13)}$$

now we have to minus the mutiple of 17 between [100,200]

```
> multi17 := {seq(i·17, i = 5 ..15)};
```
$$multi17 := \{85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255\} \quad \textbf{(4.1.14)}$$
```
> sieve := sieve minus multi17;
```
$$sieve := \{101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199\} \quad \textbf{(4.1.15)}$$

now we have to minus the mutiple of 23 between [100,200]

```
> multi23 := {seq(i·23, i = 4 ..10)};
```
$$multi23 := \{92, 115, 138, 161, 184, 207, 230\} \quad \textbf{(4.1.16)}$$
```
> sieve := sieve minus multi23;
```
$$sieve := \{101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199\} \quad \textbf{(4.1.17)}$$

we can stop now, now this is the sieve that doesn't have any prime number between [100,200].

Question 4.2 (3 *marks*):

Prove that the number of primes is infinite.

Proof:

since the prime number starts as 1,2,3,5,7,
and it goes until N, then the number of prime is also going to
N, therefore it's infinite.

Question 5: Chinese Remainder (*numbers*)

Q5 (10 *marks*):

Consider the sytem of congruences
$x \equiv 21 \pmod 3$
$x \equiv 1 \pmod 7$
$x \equiv -4 \pmod 5$:

(***a***) Argue why this system is consistent, and find a solution for this system.

(***b***) Write the set of all solutions as the solution to a single congruence.
Identify the solution closest to 0 (NOTE: it could be either positive or negative).

Solution:

(*a*)

first $x \equiv 21 \pmod 3$
$x \equiv 0 \pmod 3$

x = 3k
x = 7n + 1
x = 5y - 4

3k = 7x +1
20 = 7x - 3k

```
> gcd(7, 3);
```

1 **(5.1)**

1 can be divide by 20, so there is a solution.

3k = 7n +1
3k ≡ 1 (mod 7)
3k ≡ 15 (mod 7)
k ≡ 5 (mod 7)
k = 7n + 5

now we plug into the original:
3*(7n + 5)
=21n + 15

to check:

```
> 15 mod 3;
```

0 **(5.2)**

```
> 15 mod 7;
```

1 **(5.3)**

```
> 36 mod 3;
```

0 **(5.4)**

```
> 36 mod 7;
```

1 **(5.5)**

so this is correct.

$x \equiv -4 \pmod 5$
we can write it

$x \equiv 1 \pmod 5$
x = 5y + 1

21n + 15 = 5y + 1
14 = 5y - 21n

```
> gcd(5, 12);
```

1 **(5.6)**

1 can be divide by 14, so there is a solution.

21n + 15 = 5y + 1
21n + 15 ≡ 1 (mod 5)
n ≡1 (mod 5)
n = 5y + 1

21(5y+1) + 15
=105y + 21 + 15
= 105y + 36

to check:

```
> 36 mod 3;
```

0 **(5.7)**

```
> 36 mod 7;
```

1 **(5.8)**

```
> 36 mod 5;
```

1 **(5.9)**

36 or 105 is one of the solutions.

(***b***)

x = 105y + 36 is the final solutions.

to check:

```
> (105 + 36) mod 3;
```

$$0 \quad \textbf{(5.10)}$$

```
> (105 + 36) mod 7;
```

$$1 \quad \textbf{(5.11)}$$

```
> (105 + 36) mod 5;
```

$$1 \quad \textbf{(5.12)}$$

```
> (105·2 + 36) mod 3;
```

$$0 \quad \textbf{(5.13)}$$

```
> (105·2 + 36) mod 7;
```

$$1 \quad \textbf{(5.14)}$$

```
> (105·2 + 36) mod 5;
```

$$1 \quad \textbf{(5.15)}$$

```
> (-105 + 36) mod 3;
```

$$0 \quad \textbf{(5.16)}$$

```
> (-105 + 36) mod 7;
```

$$1 \quad \textbf{(5.17)}$$

```
> (-105 + 36) mod 5;
```

$$1 \quad \textbf{(5.18)}$$

above, we have -69, 36, 141 and more. 36 is the closest one to 0, and x = 105y + 36 is the final solutions.

Question 6: RSA code

Q6.1 (7 marks):

Peter wants to set up RSA system to get secure coded messages fromAlice. He chooses the primes p=31 and q=47 for the modulus $m = p \cdot q = 1457$, and the encoding exponent $e = 5$ for Alice. He finds the decoding exponent d, and sends e **and** m to Alice.
Alice wants to send the word $w := 1109$: to Peter.

Use Maple (***any command*** you want) to answer the following questions:

(***a***) Find the decoding exponent d that Peter keeps for himself.

(***b***) Find the encoded word c that Alice should send to Peter.

(***c***) Show what should Peter calculate to recover the word w from this c .
Note that you can use ***direct*** calculations by Maple without solving a Chinese Remainder type system.

(d) Set up now the Chinese Remainder type system that Peter can use in order to make his calculations faster,
and explain why in this way he can perform his calculations faster.
(**Note** that you do NOT need to solve this system, only explain the idea behind that method).

Solution:

(***a***)

to find the exponent d:

```
> ifactor(1457);
```

$$(31)\,(47) \qquad \textbf{(6.1.1)}$$

```
> 30·46;
```

$$1380 \qquad \textbf{(6.1.2)}$$

7*d ≡ 1 (mod 1380)

7d = 1380k + 1
7d - 1380k = 1

[1380, 0 , 1]
[7, 1, 0]
[1, -197, 1]

```
> -197·7 + 1380
```

$$1 \qquad \textbf{(6.1.3)}$$

```
> 1183·7 mod 1380;
```

$$1 \qquad \textbf{(6.1.4)}$$

d = 1183.

(***b***)

to encode the word: w^e **mod** m :

```
> c := 1109^7 mod 1457;
```

$$c := 158 \quad \textbf{(6.1.5)}$$

therefore 801 is the encoded word sent to peter.
(***c***)

now peter need to decode it:

```
> 158^1183 mod 1457;
```

$$1109 \quad \textbf{(6.1.6)}$$

now he can get the original word.

(***d***)

instead he can use the chinese remainder which need: mod p and mod q individual

```
> 158^1183 mod 31;
```

$$24 \quad \textbf{(6.1.7)}$$

```
> 158^1183 mod 47;
```

$$28 \quad \textbf{(6.1.8)}$$

to find:
x = 24 (mod 31)
x = 28 (mod 47)

to solve the entire system, it will be faster.

Q6.2 (3 marks):

Calculate the least non-negative residue of $(57)^{1043}$ modulo m = 207 by the method of converting the exponent 1043 to binary form and using it in the algorithm of squaring the base modulo *m*.
Use appropriate Maple commands to help your calculations.
Check at the end that your answer is correct by directly computing this number using Maple.

Solution:

turn the exp into binary:

```
> convert(1043, binary);
```

$$10000010011 \quad \textbf{(6.2.1)}$$

```
> a1 := 57 :
```

$a2 := a1^2$:
$a3 := a2^2$:
$a4 := a3^2$:
$a5 := a4^2$:
$a6 := a5^2$:
$a7 := a6^2$:
$a8 := a7^2$:
$a9 := a8^2$:
$a10 := a9^2$:
$a11 := a10^2$:
$result := a1 \cdot a2 \cdot a5 \cdot a11 \bmod 207;$

$$result := 180 \quad \textbf{(6.2.2)}$$

```
> 57^1043 mod 207;
```

$$180 \quad \textbf{(6.2.3)}$$

now we get the exactly the same thing.

Question 7: Hamming Code

Q7 (10 marks):

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

Peter wants to communicate with Alice using Hamming code system to ensure the correctness of the transmitted texts. They use the following encoding and decoding matrices:

```
> G := <<1, 1, 1, 1, 0, 0, 0, 0>|<1, 1, 0, 0, 1, 1, 0, 0>|<1, 0, 1, 0, 1, 0, 1, 0>|<0, 1, 1, 0, 1, 0, 0,
       1>>;
  H := <<1, 0, 0, 0>|<1, 1, 0, 0>|<1, 0, 1, 0>|<1, 1, 1, 0>|<1, 0, 0, 1>|<1, 1, 0, 1>|<1, 0, 1, 1>|<1,
       1, 1, 1>>;
```

$$G := \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$H := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \qquad \textbf{(7.1)}$$

(***a***) Assume Peter wants to send to Alice the sequence $(1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1)$. Find the sequence of vectors that Peter should transmit.

(***b***) Explain what is the specific property of matrices H and G that allows Alice to identify vectors transmitted without an error.

(***c***) Let Alice receive the vectors :
$v1, v2, v3, v4 := \langle 0, 1, 1, 0, 1, 1, 0, 1\rangle, \langle 1, 1, 0, 0, 1, 0, 1, 1\rangle, \langle 0, 0, 1, 1, 0, 1, 1, 0\rangle,$
$\langle 1, 1, 1, 1, 0, 0, 0, 0\rangle;$

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad \textbf{(7.2)}$$

Assuming there is not more than 2 errors in the transmission, determine which ones are transmitted correctly, which ones can be corrected, and whether Peter will have to resend some vector(s) again. Explain your solution.

(***d***) Explain what will happen if there are 3 errors in the transmitted vector.

Solution:

(***a***)

now he should sent it in

(***b***)

```
> H.G mod 2;
```

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \tag{7.3}$$

if all the vector are 0-vectors, then it's no error.

(***c***)

```
> w := ⟨v1|v2|v3|v4⟩;
```

$$w := \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \tag{7.4}$$

```
> H.w mod 2;
```

$$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \tag{7.5}$$

in the first vector:

1+1+4 = 6, 6th position is wrong, and the correct one is

```
> v1 := ⟨0, 1, 1, 0, 1, 0, 0, 1⟩;
```

$$v1 := \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{7.6}$$

in the second vector:
the error is at position 1 + 4 = 5, we need to correct it:

```
> v2 := ⟨1, 1, 0, 0, 0, 0, 1, 1⟩;
```

$$v2 := \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} \tag{7.7}$$

the third vector, it's 0 in the first digital, therefore we can not determinate the position of the errors.

in the fourth vector, it's a all-zero vectors, there it's correct.

(*d*)

```
>
```

if there is 3 errors in the transmitted vector, the receiver can not tell if there is 3 or 1 errors.

Question 8: Irreducible Polynomials

```
> restart:
```

Q8 (10 marks):

(***a***) Find all irreducible polynomials of degree 2 in $F_5[x]$.
(HINT: find first the set of all irreducible ***monic*** polynomials, then expand the set to associates).

(***b***) Decide whether the polynomial of degree 3, $q := x^3 + x + 1$: in $F_5[x]$ is irreducible or not, and factor it if it is reducible.

Solution:

(***a***)

we try to find all the set of degre 2:

```
> m := [1, x, x + 1, x + 4] :
```

```
> [seq(seq(m[i]·j, j = 1 ..4), i = 1 ..4)];
```

$$[1, 2, 3, 4, x, 2x, 3x, 4x, x+1, 2x+2, 3x+3, 4x+4, x+4, 2x+8, 3x+12, 4x+16] \quad \textbf{(8.1)}$$

(***b***)

now we try to find if it's irreducible or not

```
> seq(x^3 + x + 1 mod 5, x = 0 ..4) ;
```

$$1, 3, 1, 1, 4 \quad \textbf{(8.2)}$$

this is irreducible.

Question 9: Polynomial GCD & Chinese Remainder

Q9 (10 *marks*):

```
> restart:
```

Consider polynomials
$f := x^5 + x^4 + 1$:
$g := x^3 + 2x$:

in the field $F_3[x]$.

(***a***) Apply the Extended Euclid's Algorithm to find a greatest common divisor of f **and** g.

(***b***) Is this common divisor monic? If not, identify the monic greatest common divisors of f **and** g or explain why it is impossible.

(***c***) Assume now that you have a system of congruences

$q \equiv x^2 \pmod{f}$:

$q \equiv x \pmod{g}$:

On the basis of the results you found in (***a***) and (***b***) above, decide (***without*** trying to solve the system) whether this system is consistent or not.

Solution:

(***a***)

to find the gcd, we need to use EEA matrix:

```
> FEEA := (r1, r2) → (r1 − expand(quo(r1[1], r2[1], x)·r2)) mod 3 :
> r0 := [f, 0 , 1] :
  r1 := [g, 1, 0] :
```

```
> r2 := FEEA(r0, r1);
```

$$r2 := [x^2 + x + 1, 2x^2 + 2x + 2, 1] \quad \textbf{(9.1)}$$

```
> r3 := FEEA(r1, r2);
```

$$r3 := [2x + 1, x^3, 2x + 1] \quad \textbf{(9.2)}$$

```
> r4 := FEEA(r2, r3);
```

$$r4 := [0, x^4 + 2x^3 + 2x^2 + 2x + 2, 2x^2 + 2x] \quad \textbf{(9.3)}$$

the greatest common divisors is 2x+ 1.

(***b***)

yes, it's monic because

(***c***)

this system is consistency because

$q = x^2 + f \cdot k$:

$q = x + g \cdot k$:

gcd(f,g) = 2x+ 1 can be divide by $x^2 + x$.

```
>
```

Question 10: Congruence classes F[x]/m(x)

Q10 (10 *marks*):

```
> restart
```

Consider the ring of congruence classes $R = F_5[x]/(x^3 + 1)$.

(***a***) Give an argument, without doing Maple calculations, why the congruence class of
$f := 2x^3 + 1$:
is a unit in R, and apply then Maple (Extended Euclids Algorithm) to find the inverse of f in the complete set of least degree residues.
Is the inverse of f in R unique?

(***b***) Give an argument why the congruence class $g := (x + 1)$ is a zero divisor, and find a complementary zero divisor of g.
Is the complementary zero diviser of g unique? Argue why it is, or give an example of another complementary zero diviser if it is not unique.

Solution:

(***a***)

we try to find the inverse:

```
> m := x^3 + 1 :
  f := 2 x^3 + 1 :
  g := rem(f, m, x) mod 5;
```

$$g := 4 \qquad \textbf{(10.1)}$$

```
>
```

g*x + m*y = 1

using the EEA matrix to find inverse:

```
> r0 := [m, 0 , 1] :
  r1 := [g, 1, 0] :
> r2 := FEEA(r0, r1);
```

$$r2 := [0, 2x^3 + 2, 1] \qquad \textbf{(10.2)}$$

```
>
```

$2x^3 + 2$ is the inverse.

yes the inverse is unique.

(***b***)

```
> seq( (x^3 + 1) mod 5, x = 0..4);
```

1, 2, 4, 3, 0 **(10.3)**

```
>
```

therefore there is a factor x -4 ≡ x + 1.

it has zero divisors like x+ 1, 2x+ 2, 3x+3, 4x + 4.

it's complementary zero divisor will be 1,2,3,4.

Bonus Question: Rings

(5 *marks*)

True or False? Justify

In any ring $\mathbb{Z}/m\mathbb{Z}$, the order d of any unit a divides the number of units $\phi(m)$ in the ring.

(HINT: use Euiler's Theorem).

Solution:

true, because a can divide $\phi(m)$, *since it's a unit.*