MAST 332 - COMP 367
Final Examination Sample
(Based on the Final of April 2016)
SOLUTIONS

(N.B. the final exam can include *ANY* question within the topics learned in this course!)

==========

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-M332C367-Winter2016-Final**

2. Write here your **ID:**_____ **Name:**_____

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

5. ***Short (but clear) explanations of your solutions must be provided for full marks.***

Total:_____

Question 1: Diophantine Equations

(10 *marks*)

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

(1) $99\,x + 225\,y = 18$:
(2) $27\,x + 45\,y = 33$:

(***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.

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

Solution:

(***a***)
The GCD of the pair of coefficients of each of these equations is 9.

```
> gcd(99, 225);
  gcd(27, 45);
```

$$9$$
$$9 \qquad \textbf{(1.1)}$$

9 divides 18, but it does not divide 33. Therefore the equation (1) is consistent but the equation (2) is not.

(***b***)

Define the function acting on two consequtive lists to help Extended Euclid's Algorithm calculations:

```
> FEEA :=(r1,r2)-> r1-iquo(r1[3],r2[3])*r2;
```

$$FEEA := (r1, r2) \rightarrow r1 - iquo\left(r1_3, r2_3\right)\, r2 \qquad \textbf{(1.2)}$$

Now define the initial two lists for the EEA algorithm for Diophantine equation $99\,X + 225\,Y = R$: starting with the list r0=[X=0,Y=1,R=225], and apply it to reduce the row lists until either the right side element of the resulting list is 0, or until the right-side element divides 18.

```
> r0:=[0,1,225]:
  r1:=[1,0,99]:
  r2:=FEEA(r0,r1);
```

$$r2 := [-2, 1, 27] \qquad \textbf{(1.3)}$$

Continue:

```
> r3 := FEEA(r1, r2);
  r4 := FEEA(r2, r3);
  r5 := FEEA(r3, r4);
```

$$r3 := [7, -3, 18]$$
$$r4 := [-9, 4, 9]$$
$$r5 := [25, -11, 0] \quad \textbf{(1.4)}$$

So the GCD (225,99)=9, and r4 corresponds to equation

$$-9 \cdot 99 + 4 \cdot 225 = 9;$$
$$9 = 9 \quad \textbf{(1.5)}$$

This can be multipolied by 2 to get a solution to the equation (1). Another solution, however, can be found directly from the r3, which implies {x=7,y=-3}
Check:

```
> 7·99 − 3·225 = 18;
```
$$18 = 18 \quad \textbf{(1.6)}$$

(c) To find all solutions, solve the homogeneous equation $99 \cdot x0 + 225 \cdot y0 = 0$:
for $(x0, y0)$ and add it to the found solution of the equation (1).
The homogenous equation, after cancelling by GCD(99,225)=9 both coefficients, gives
$11\ x0 = -25\ y0 \Rightarrow$
$x0 = 25 \cdot k, y0 = -11\ k, k \in \mathbb{Z}.$

Thus, the set of all solutions of the Eq.(1) is
$x = 7 + 25\ k$:
$y = -3 - 11\ k$:

(d)
The solution with smalles positive y will be produced by k=-1. So $\{x = -18, y = 8\}$

Check

```
> -18·99 + 8·225 = 18;
```
$$18 = 18 \quad \textbf{(1.7)}$$

▶ Question 2: Congruence Classes ℤ/mℤ

▶ Question 3: Rings & Fields

▶ Question 4: Hamming Code

▶ **Question 5: Chinese Remainder (*numbers*)**

▶ **Question 6: RSA code**

▶ **Question 7: Hill Cryptosystem**

▶ **Question 8: Irreducible Polynomials**

▶ **Question 9: Polynomial GCD & Chinese Remainder**

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

▶ **Bonus Question: Rings**