DEPARTMENT OF MATHEMATICS

MACQUARIE UNIVERSITY
FACULTY OF SCIENCE

NAME: Nassif-Haynes Christian
Student Id: 42510023
Tutorial Group: B, Mon 14:00, E8A 188
Tutor: Mitch Buckley

DMTH237 S113
Discrete Mathematics II
Assignment 5

Due 14:00 31/05 2013

Please sign the declaration below, and staple this sheet to the front of your solutions. Your assignment must be submitted at the Science Centre, E7A Level 1.

Your assignment must be STAPLED, please do not put it in a plastic sleeve.

PLAGIARISM Plagiarism involves using the work of another person and presenting it as one's own. For this assignment, the following acts constitute plagiarism:

a) Copying or summarizing another person's work.

b) Where there was collaborative preparatory work, submitting substantially the same final version of any material as another student.

Encouraging or assisting another person to commit plagiarism is a form of improper collusion and may attract the same penalties.

STATEMENT TO BE SIGNED BY STUDENT

1. I have read the definition of plagiarism that appears above.
2. In my assignment I have carefully acknowledged the source of any material which is not my own work.
3. I am aware that the penalties for plagiarism can be very severe.
4. If I have discussed the assignment with another student, I have written the solutions independently.

SIGNATURE.....

---

1. Find the general solution to each of the following recurrence relations.
   (a) $a_{n+2} - 7\,a_{n+1} + 12\,a_n = 2^n$ (b) $a_{n+2} - 7\,a_{n+1} + 12\,a_n = n^2$
   (c) $a_{n+2} - 7\,a_{n+1} + 12\,a_n = n^2\,2^n$ (d) $a_{n+1} - 2\,a_n = \cos n$ (e) $a_{n+2} - 6\,a_{n+1} + 5\,a_n = n$.

2. To calculate the *computational complexity* — a measure for the maximal possible number of steps needed in a computation — of the 'mergesort' algorithm (an algorithm for sorting natural numbers into non-decreasing order) one can proceed by solving the following recurrence relation:

$$a_n = 2\,a_{n-1} + 2^n - 1\,, \qquad \text{with } a_0 = 0\,.$$

   (a) Use the method of generating functions to solve this recurrence relation.

   (b) The relation between the number t_m of computations needed to sort m numbers, and the solution a_m of the recurrence relation, is given by $t_{2^m} = a_m$. Use this to find an expression for t_n, where $n = 2^m$ (or $\log_2 n = m$), explicitly as a function of n, and conclude that $t_n \sim n \log_2 n$ for large n.

(assignment continued on next page)

3. Let POWER be the 16-state Turing machine that calculates 2^n in Chris Cooper's notes (repeated as Example 13 of Ross Moore's 'Turing Machines' notes), and let EXP be the following 23-state Turing machine.

	0	**1**
0	0R1	1R0
1	1L2	
2	0L3	
3	0R4	1L3
4	0R23	0R5
5	0R6	1R5
6 ⋮ 21	POWER	
22	0L3	1L22

It is not hard to see that EXP calculates $2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\Big\}n$ 2s, for $n \geq 1$, and for $n = 0$ it calculates 1.
For example, $2^{2^2} = 2^4 = 16$, $2^{2^{2^2}} = 2^{16} = 65536$.

Now, if INC is the 1-state Turing machine that calculates $n + 1$, namely:

	0	**1**
0	1R1	1L0

then show that

$$\text{INC} + \text{INC} + \text{INC} + \text{INC} + \text{INC} + \text{EXP}$$

is a 28-state Turing machine that calculates $2^{2^{2^{2^2}}} = 2^{65536}$.
Use this fact to show that $\beta(28) > 2 \times 10^{19728}$.

4. You can do the following sub-questions without a calculator.

   (a) Find the inverse of 135 in $\mathbb{Z}_{211}$.

   (b) Use Fermat's theorem to find the remainder when 27^{68} is divided by 31.
   [HINT: rewrite 27 as a negative number modulo 31.]

   (c) Use Euler's theorem to find the remainder when 11^{4805} is divided by 48.

   (d) Find the remainder when 38! is divided by 41. State any theorems that you use.

5. In an RSA Public Key system, Eve's modulus is 746003, which is the product of two primes, and her encoding key is 17. Bob sends Eve a message, represented by the number 31.

   (a) What is the encoded message?

   (b) Eve's decoding key is 218873. Use this information to find the two prime factors of 746003.

   (c) Hence find $\varphi(746003)$.

   (d) This particular RSA system has not been set up securely, so that Alice has the same modulus as Eve. If Alice's public encoding key is 7, use Eve's information to find Alice's secret decoding key.

   (e) Eve intercepts a message being sent to Alice, as the number 242435. What number represents the original content of this message?

[for bonus marks]

Your task, should you choose to accept it, is to decode the personalised message represented by the following set of numbers, resulting from an RSA encoding as described on the next page. You will know that you have successfully decoded the message, since your own student ID appears at some place within the message surrounded by a pair of colons (:), starting at character k say. Your answer should consist of the text of the message, along with the number k at which character the colon preceding the student ID appears, as well as a description of how you obtained it. You are free to use any software that you like in attempting to decode your message.

Your personalised encoded message is as follows.

227687, 284014, 158099, 194429, 236685, 41444, 28087, 265481, 95112, 78580, 134546, 131400

Messages are built using the 40 characters comprising digits, capital letters, space character and some punctuation as shown in the following ordered list — the space character is at position 11 (shown in quotes), with 'A' at position 12.

0 1 2 3 4 5 6 7 8 9 ' ' A B C D E F G H I J K L M N O P Q R S T U V W X Y Z , : .

Let ind(c) denote the position of character c within the above list — starting at 1, so ind(0) = 1. Three characters are combined to form a single number using base 41; e.g. 'ABC' corresponds to $41^2 \times \text{ind(A)} + 41 \times \text{ind(B)} + \text{ind(C)}$. Or is it $\text{ind(A)} + 41 \times \text{ind(B)} + 41^2 \times \text{ind(C)}$?
(Nevermind, only one of these works correctly with your message!)

The 36 characters in the message (of which 10 are devoted to the student ID) are split into groups of three successive characters, with each group converted to a number as above. These 12 numbers are then each encoded using RSA with a modulus of $m = p\,q = 295927$ (with p and q being primes) and encoding exponent of 11, to produce your given encoded message.

What is the corresponding decoding exponent?

You must work this out, given that $\{1019, 136859\}$ is a valid encoding–decoding pair for the given modulus. Use this information, or other means, to determine $\phi(m)$ and the primes p and q.
Then determine the required decoding exponent, and decode each of the 12 numbers to recover the numbers for 3-letter groups in the original message. Use base 41 to convert those numbers back into characters. Finding your student ID confirms having done everything correctly.

Successful completion of this optional task is worth a bonus of up to 5 marks for this assignment.